Vigor3200 Series

Multi-WAN Security Router

Your reliable networking solutions partner

User's Guide

V1.1

Vigor3200 Series
Multi-WAN Security Router
User's Guide

Version: 1.1

Firmware Version: V3.3.7

Date: 07/04/2011

Copyright Information

Copyright Declarations

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 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

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor3200 Series Router

DrayTek Corp. declares that Vigor3200 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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.

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.

Please visit http://www.DrayTek.com/user/AboutRegulatory.php

This product is designed for 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France. Please see the user manual for the applicable networks on your product.

Table of Contents

1

2

3

1 Preface

Vigor3200 Series, a broadband router, integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly and offers several protocols (such as IPSec/PPTP/L2TP) with up to **32** VPN tunnels.

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

Object-based firewall is flexible and allows your network be safe. In addition, Vigor3200 Series supports USB interface for connecting USB printer to share printer, USB storage device for sharing files, or for 3G WAN.

Vigor3200 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.

1.1 Web Configuration Buttons Explanation

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

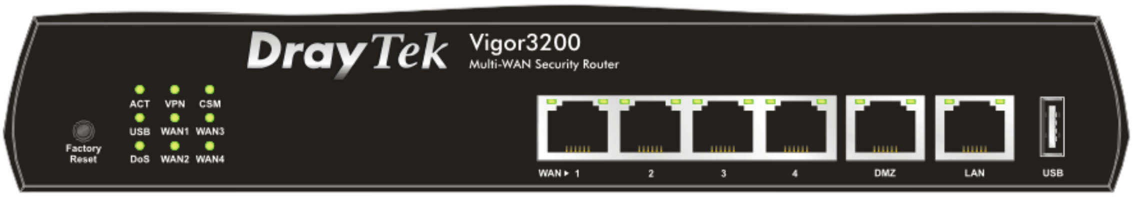
OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified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

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

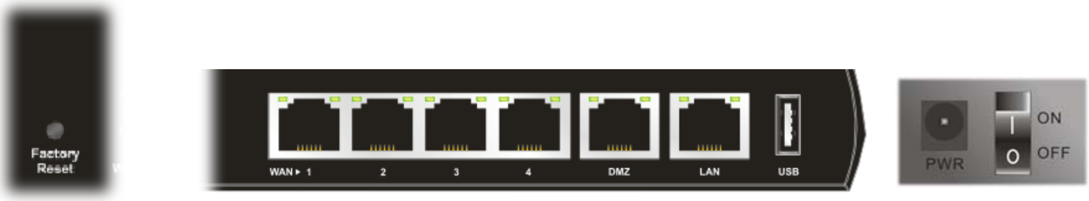
1.2 LED Indicators and Connectors

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

1.2.1 For Vigor3200

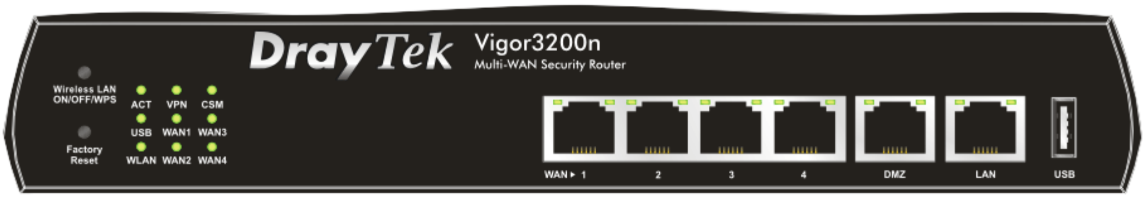


LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while detecting an attack.
VPN		On	The VPN tunnel is active.
WAN1-4		On	The WAN1 ~ WAN4 connection is ready.
		Blinking	It will blink while transmitting data.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from **Firewall >>General Setup**. (Such profile must be established under **CSM** menu).
LED on Connector			
WAN 1/2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
DMZ	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
LAN	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.

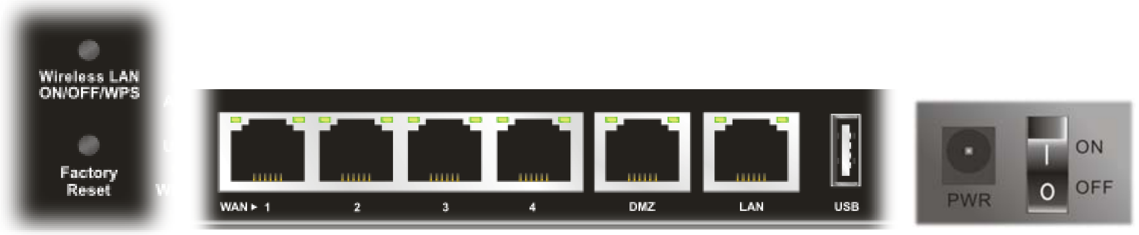


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN1- WAN4	Connecters for remote networked devices.
DMZ	Connecter for local DMZ host.
LAN	Connecter for local network devices.
USB	Connecter for 3G Modem or printer.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.2 For Vigor3200n



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
WLAN		On	Wireless access point is ready.
		Blinking	Ethernet packets are transmitting over wireless LAN.
		Off	The WLAN function is inactive.
VPN		On	The VPN tunnel is active.
WAN1-4		On	The WAN1 ~ WAN4 connection is ready.
		Blinking	It will blink while transmitting data.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from **Firewall >>General Setup**. (Such profile must be established under **CSM** menu).
LED on Connector			
WAN 1/2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
DMZ	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
LAN	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.



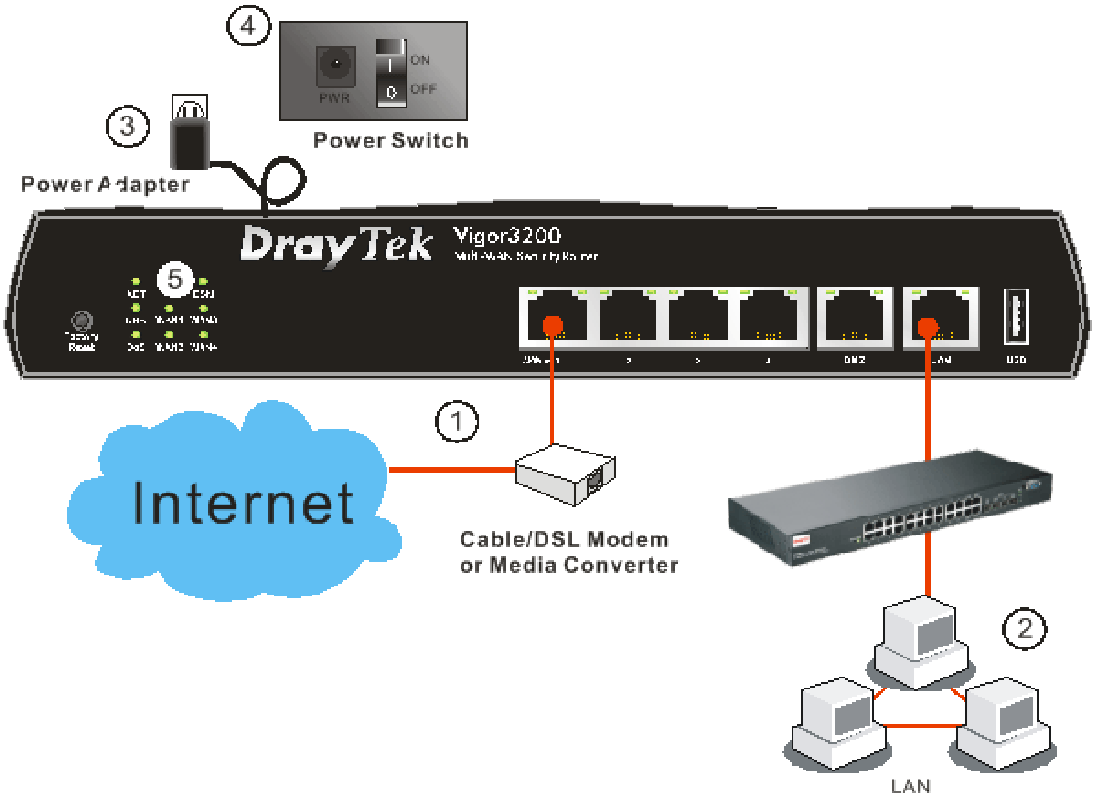
Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN1- WAN4	Connecters for remote networked devices.
DMZ	Connecter for local DMZ host.
LAN	Connecter for local network devices.
USB	Connecter for 3G Modem or printer.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.3 Hardware Installation

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

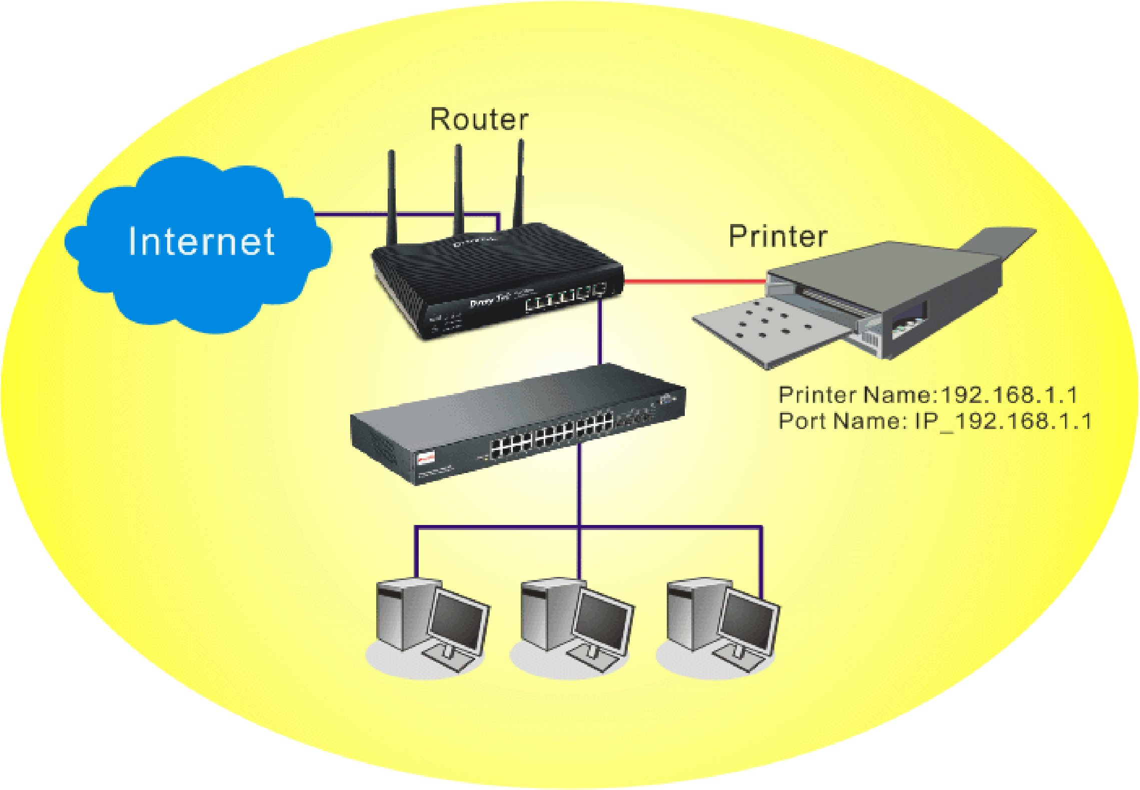
1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect one end of an Ethernet cable (RJ-45) to the **LAN** port of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer. Or, use a switch to connect Vigor router and computer(s).
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 detailed information of LED status, please refer to section 1.1.)



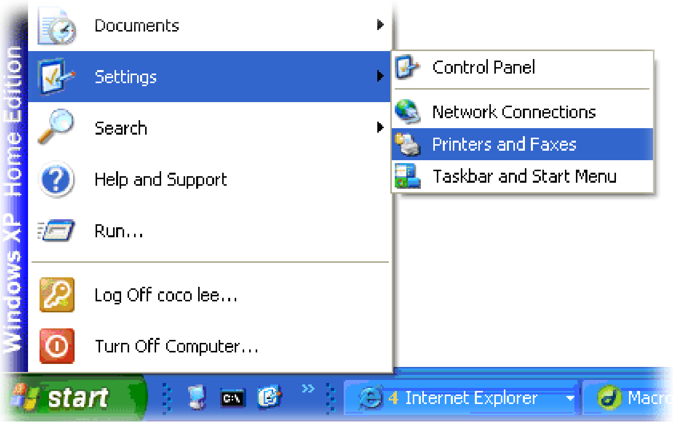
1.4 Printer Installation

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**.

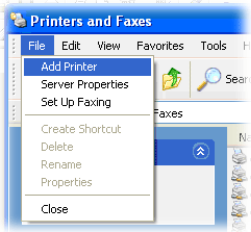


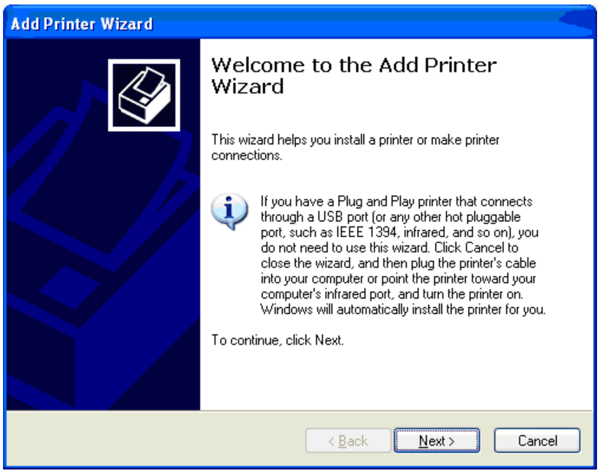
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

1. Connect the printer with the router through USB/parallel port.
2. Open **Start->Settings-> Printer and Faxes**.



3. Open **File->Add Printer**. A welcome dialog will appear. Please click **Next**.




Add Printer Wizard

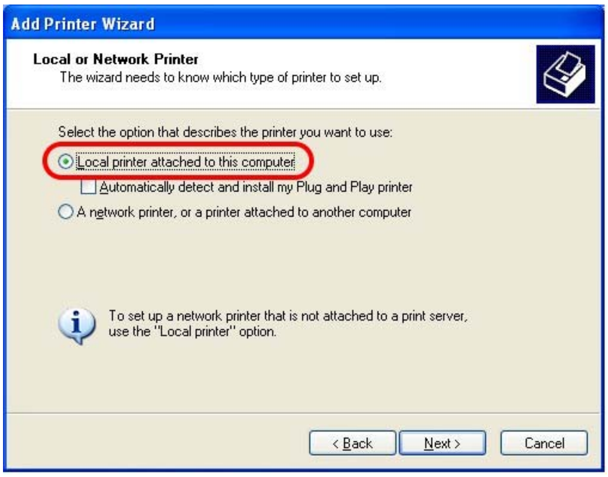
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

4. Click Local printer attached to this computer and click Next.


Add Printer Wizard

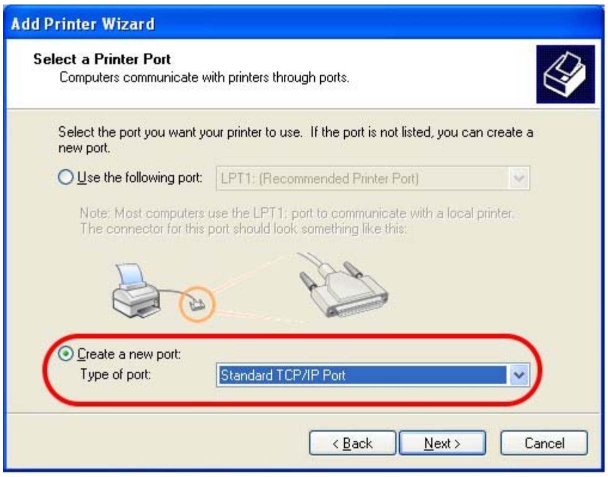
Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

- ● Local printer attached to this computer
  - □ Automatically detect and install my Plug and Play printer
- ○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.


Add Printer Wizard

Select a Printer Port
Computers communicate with printers through ports.

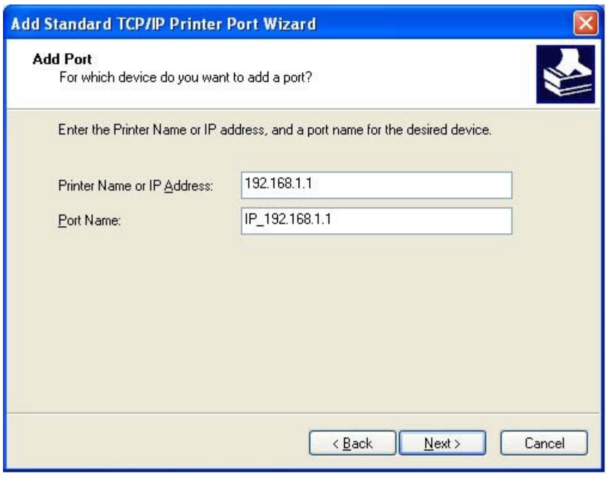
Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:
Type of port: Standard TCP/IP Port

6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.



Add Standard TCP/IP Printer Port Wizard

Add Port

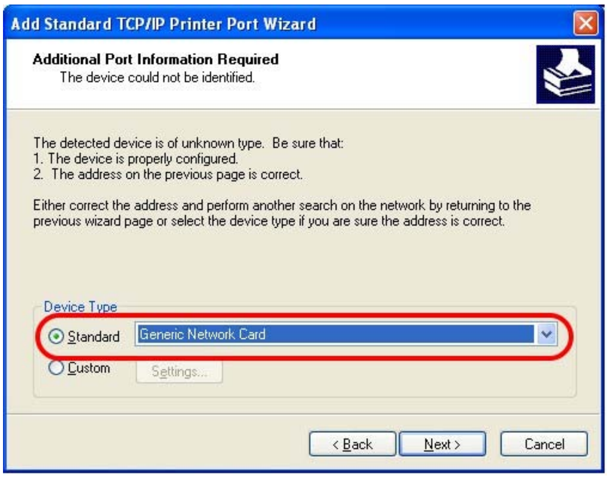
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.1.1

Port Name: IP_192.168.1.1

7. Click Standard and choose Generic Network Card.



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.

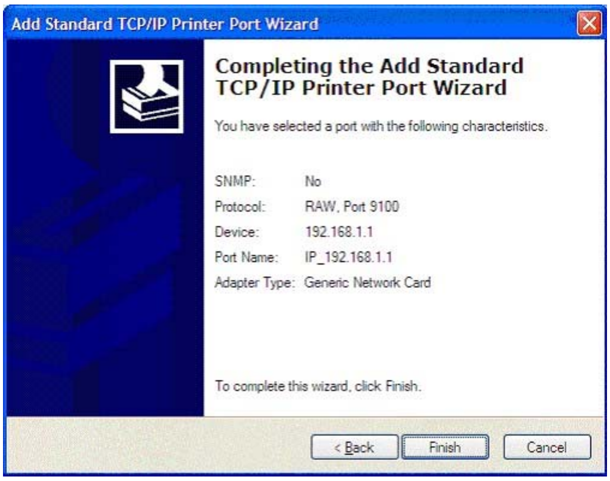
Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type

● Standard: Generic Network Card

○ Custom

8. Then, in the following dialog, click **Finish**.



Add Standard TCP/IP Printer Port Wizard

Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP: No

Protocol: RAW, Port 9100

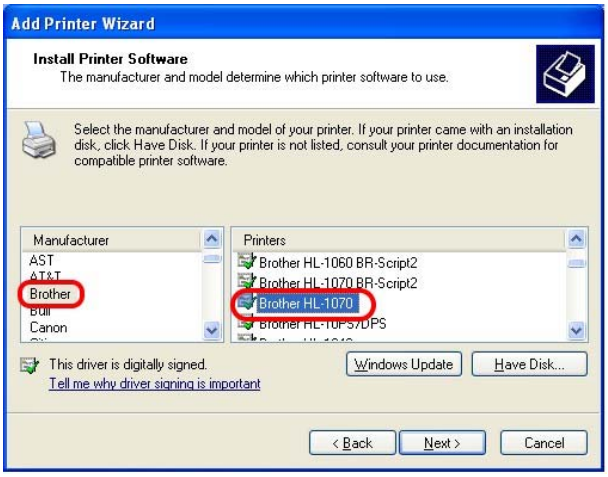
Device: 192.168.1.1

Port Name: IP_192.168.1.1

Adapter Type: Generic Network Card

To complete this wizard, click Finish.

9. 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**.



Add Printer Wizard

Install Printer Software

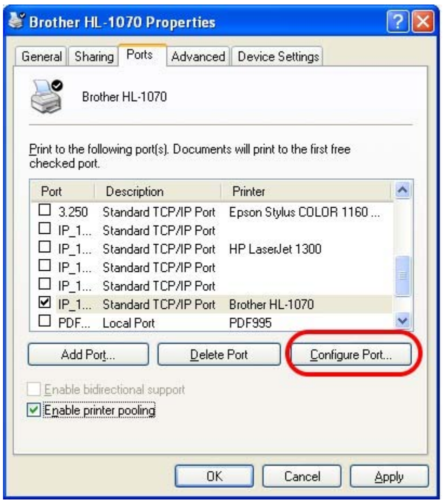
The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

Manufacturer	Printers
AST	Brother HL-1060 BR-Script2
AT&T	Brother HL-1070 BR-Script2
Brother	Brother HL-1070
Bull	Brother HL-10PS/DPS
Canon	

This driver is digitally signed.
Tell me why driver signing is important

10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.



Brother HL-1070 Properties

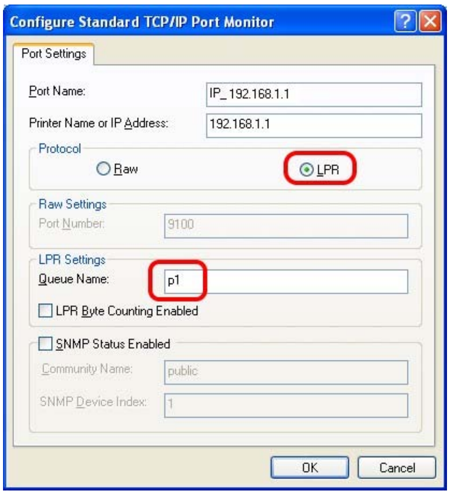
Brother HL-1070

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
□ 3.250	Standard TCP/IP Port	Epson Stylus COLOR 1160 ...
□ IP_1...	Standard TCP/IP Port	
□ IP_1...	Standard TCP/IP Port	HP LaserJet 1300
□ IP_1...	Standard TCP/IP Port	
□ IP_1...	Standard TCP/IP Port	
☑ IP_1...	Standard TCP/IP Port	Brother HL-1070
□ PDF...	Local Port	PDF995

□ Enable bidirectional support
☑ Enable printer pooling

11. 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.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol
○ Raw ● LPR

Raw Settings
Port Number: 9100

LPR Settings
Queue Name: p1

□ LPR Byte Counting Enabled

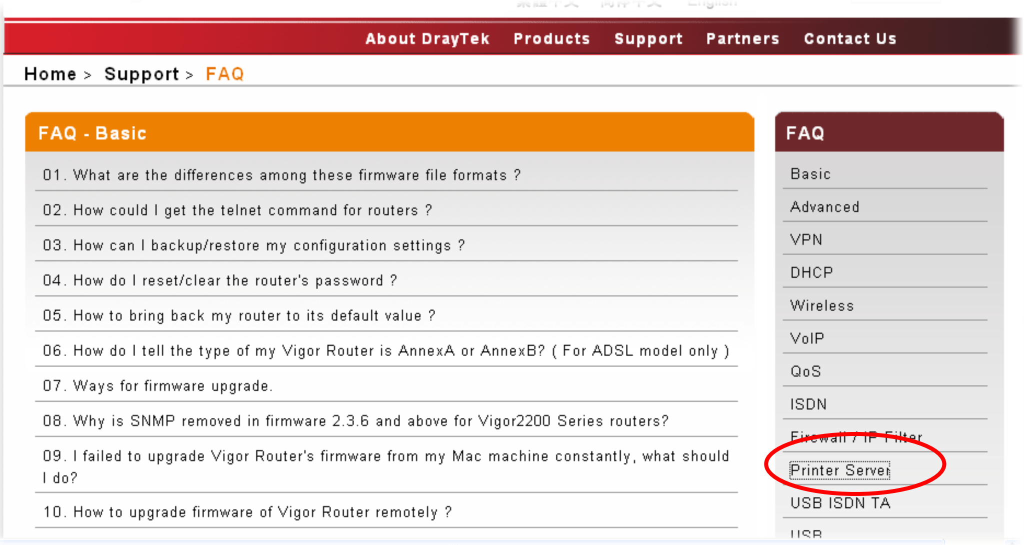
□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

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**; find out the link of **Printer Server** and click it; then choose the **What types of printers are compatible with Vigor router?**.



FAQ - Basic

01. What are the differences among these firmware file formats ?

02. How could I get the telnet command for routers ?

03. How can I backup/restore my configuration settings ?

04. How do I reset/clear the router's password ?

05. How to bring back my router to its default value ?

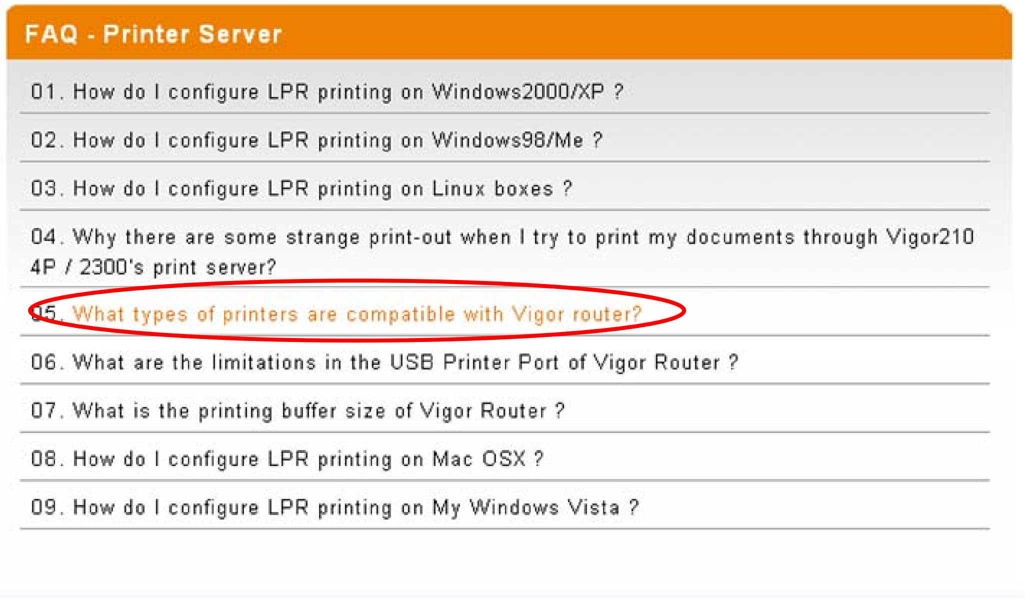
06. How do I tell the type of my Vigor Router is AnnexA or AnnexB? (For ADSL model only)

07. Ways for firmware upgrade.

08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?

09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what should I do?

10. How to upgrade firmware of Vigor Router remotely ?



FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?

02. How do I configure LPR printing on Windows98/Me ?

03. How do I configure LPR printing on Linux boxes ?

04. Why there are some strange print-out when I try to print my documents through Vigor2104P / 2300's print server?

05. What types of printers are compatible with Vigor router?

06. What are the limitations in the USB Printer Port of Vigor Router ?

07. What is the printing buffer size of Vigor Router ?

08. How do I configure LPR printing on Mac OSX ?

09. How do I configure LPR printing on My Windows Vista ?

Note 2: Vigor router supports printing request from computers via the LAN port but not WAN port.

This page is left blank.

2 Configuring Basic Settings

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

2.1 Two-Level Management

This chapter explains how to setup a password for an administrator/user and how to adjust basic/advanced settings for accessing Internet successfully.

For user mode operation, do not type any word on the window and click Login for the simple web pages for configuration.

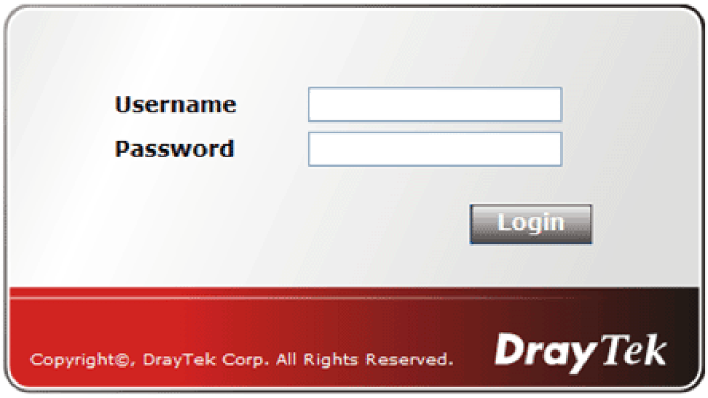
Yet, for admin mode operation, please type “admin/admin” on Username/Password and click Login for full configuration.

2.2 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.

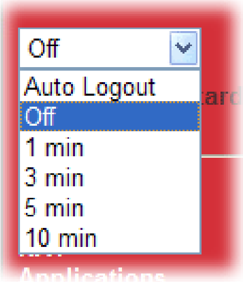
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.



3. For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type “admin/admin” on Username/Password and click **Login** for full configuration.

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

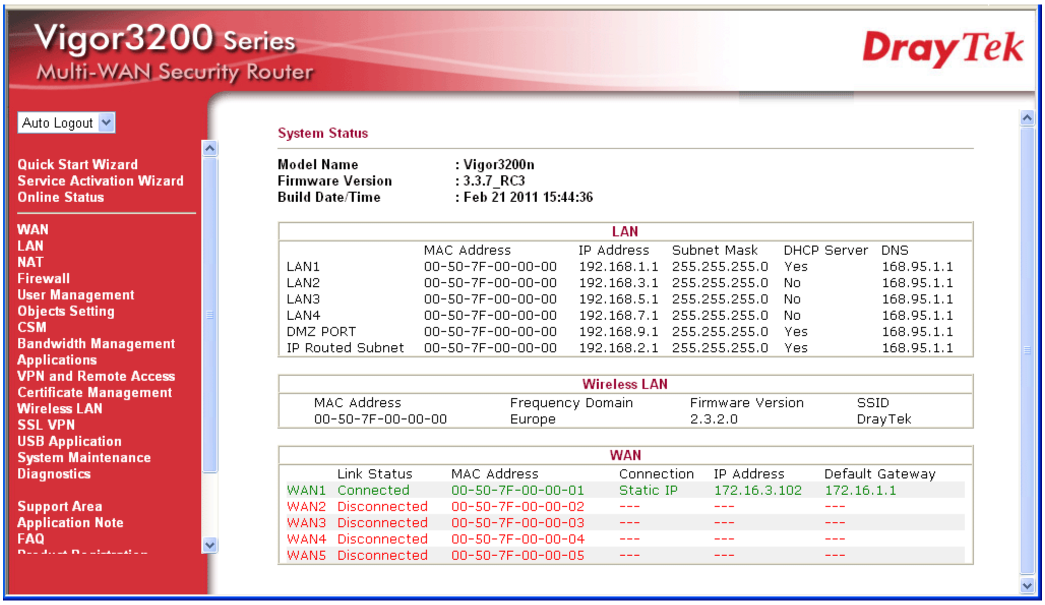
4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



2.3 Changing Password

No matter user mode operation or admin mode operation, 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" on Username/Password for admin mode. Otherwise, do not type any word (both username and password are Null for user mode) on the window and click **Login** on the window.
3. Now, the **Main Screen** will appear.



System Status

Model Name : Vigor3200n
Firmware Version : 3.3.7_RC3
Build Date/Time : Feb 21 2011 15:44:36

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-00-00-00	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-00-00-00	192.168.3.1	255.255.255.0	No	168.95.1.1
LAN3	00-50-7F-00-00-00	192.168.5.1	255.255.255.0	No	168.95.1.1
LAN4	00-50-7F-00-00-00	192.168.7.1	255.255.255.0	No	168.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.2.1	255.255.255.0	Yes	168.95.1.1

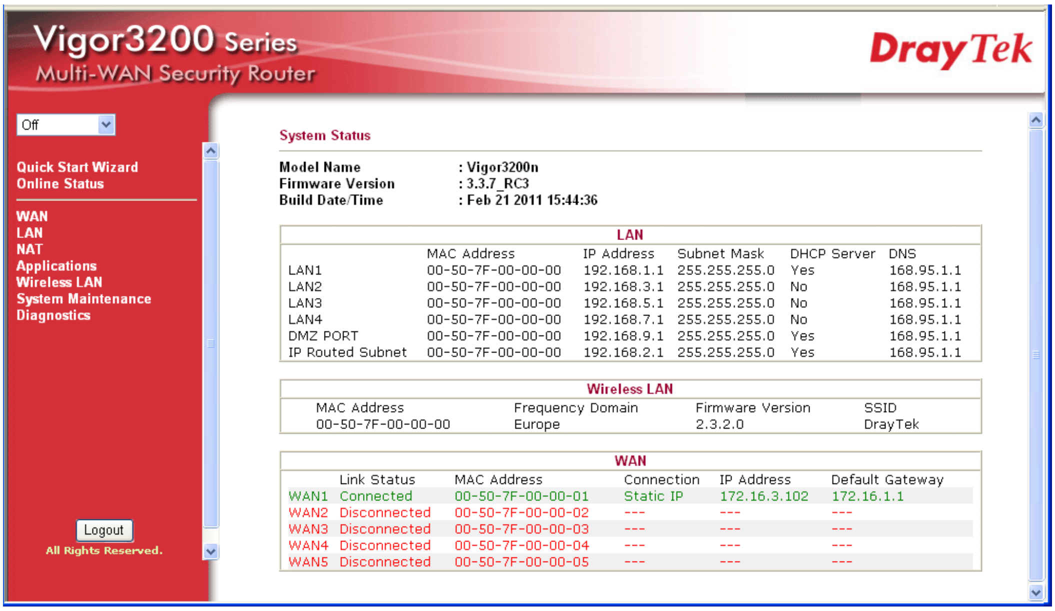
Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-00-00-00	Europe	2.3.2.0	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-00-00-01	Static IP	172.16.3.102	172.16.1.1
WAN2	Disconnected	00-50-7F-00-00-02	---	---	---
WAN3	Disconnected	00-50-7F-00-00-03	---	---	---
WAN4	Disconnected	00-50-7F-00-00-04	---	---	---
WAN5	Disconnected	00-50-7F-00-00-05	---	---	---

Main screen for admin mode operation (full configuration)



System Status

Model Name : Vigor3200n
Firmware Version : 3.3.7_RC3
Build Date/Time : Feb 21 2011 15:44:36

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-00-00-00	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-00-00-00	192.168.3.1	255.255.255.0	No	168.95.1.1
LAN3	00-50-7F-00-00-00	192.168.5.1	255.255.255.0	No	168.95.1.1
LAN4	00-50-7F-00-00-00	192.168.7.1	255.255.255.0	No	168.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.2.1	255.255.255.0	Yes	168.95.1.1

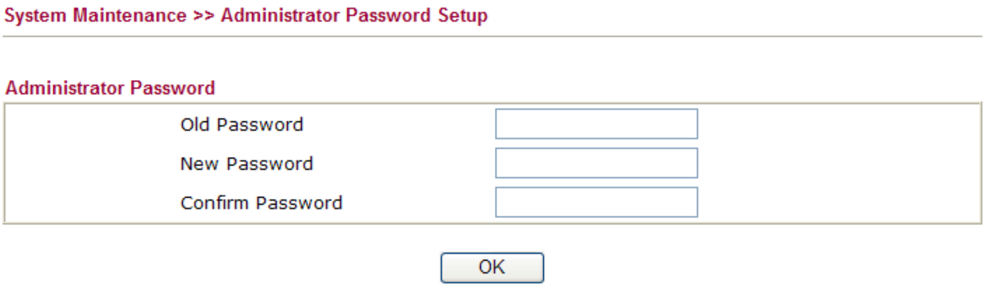
Wireless LAN			
MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-00-00-00	Europe	2.3.2.0	DrayTek

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-00-00-01	Static IP	172.16.3.102	172.16.1.1
WAN2	Disconnected	00-50-7F-00-00-02	---	---	---
WAN3	Disconnected	00-50-7F-00-00-03	---	---	---
WAN4	Disconnected	00-50-7F-00-00-04	---	---	---
WAN5	Disconnected	00-50-7F-00-00-05	---	---	---

Main screen for user mode operation (simple configuration)

> **Note:** The home page will change slightly in accordance with the type of the router you have.

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

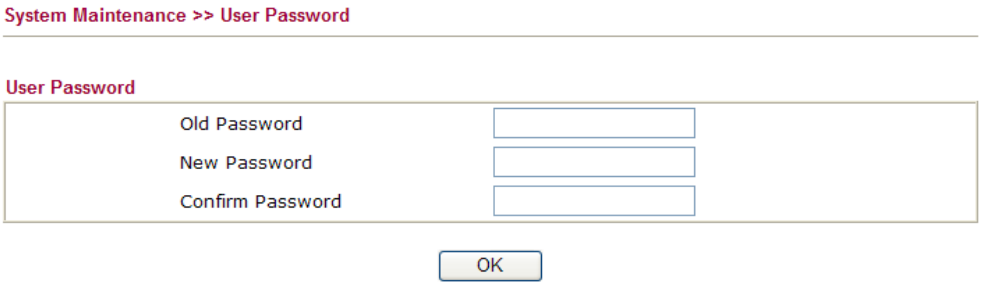


System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	
New Password	
Confirm Password	

or



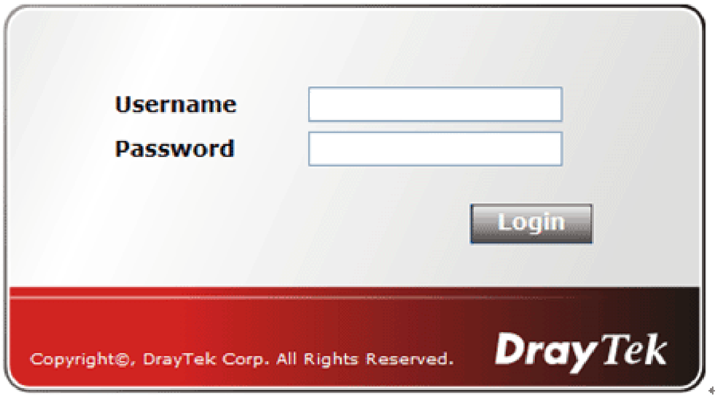
System Maintenance >> User Password

User Password

Old Password	
New Password	
Confirm Password	

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

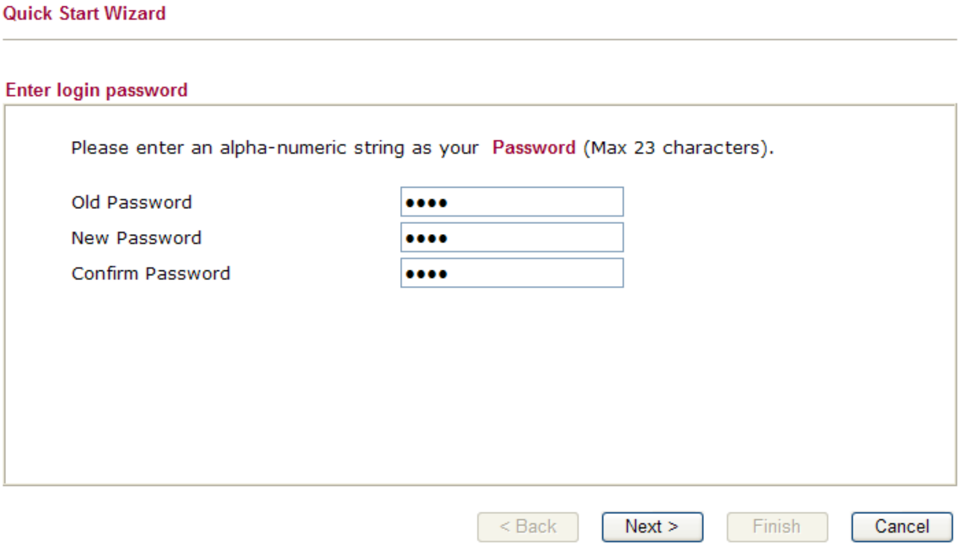
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.



2.4 Quick Start Wizard

Notice: Quick Start Wizard for user mode operation is the same as for admin mode operation.

If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.



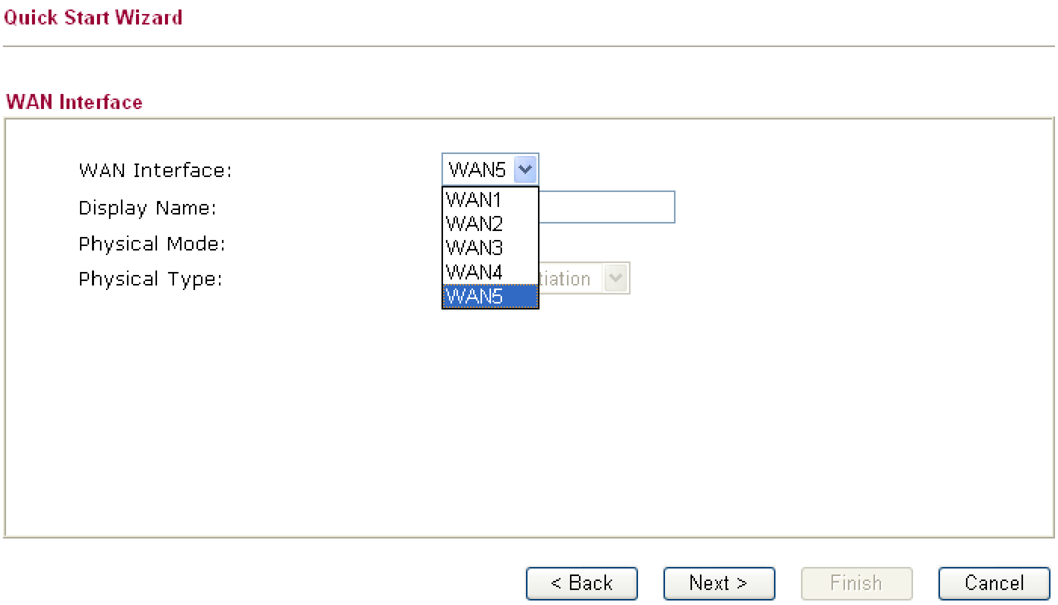
Quick Start Wizard

Enter login password

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

Old Password	••••
New Password	••••
Confirm Password	••••

On the next page as shown below, please select the WAN interface that you use. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.



Quick Start Wizard

WAN Interface

WAN Interface: WAN5

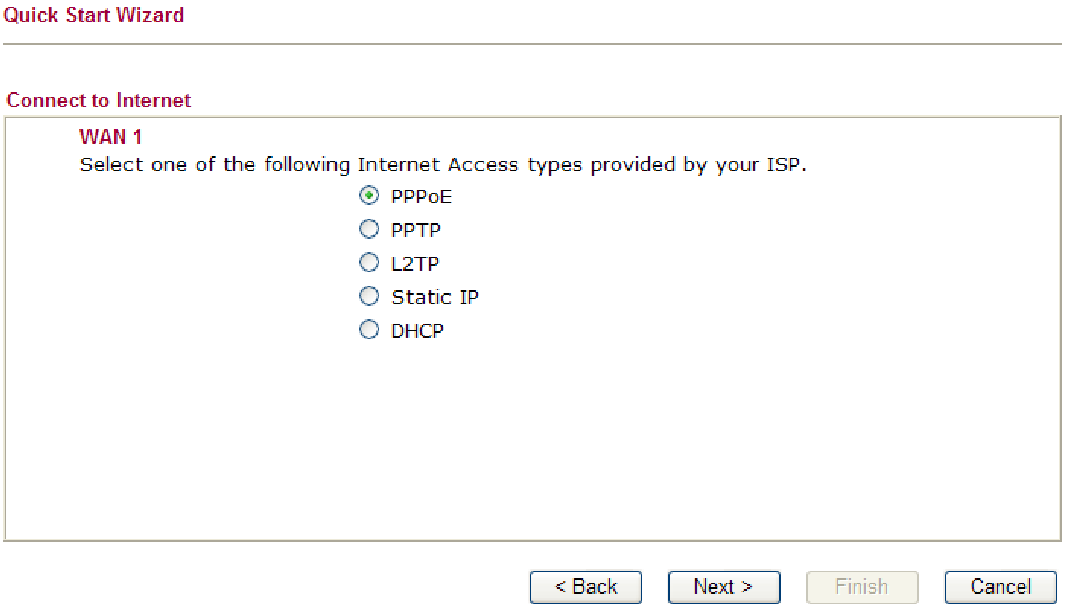
Display Name:

Physical Mode:

Physical Type:

Note: There are five WAN selections available for you to choose. In which, WAN5 is selected for 3G USB modem connection.

On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.



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

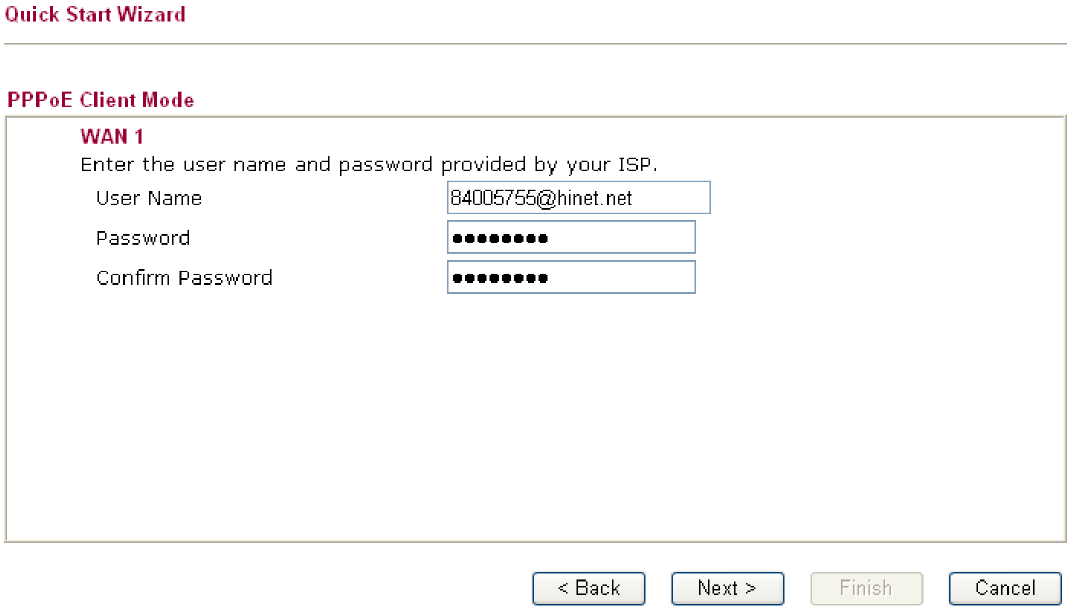
○ DHCP

2.4.1 PPPoE

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

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

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown:



Quick Start Wizard

PPPoE Client Mode

WAN 1

Enter the user name and password provided by your ISP.

User Name: 84005755@hinet.net

Password: ●●●●●●●●●

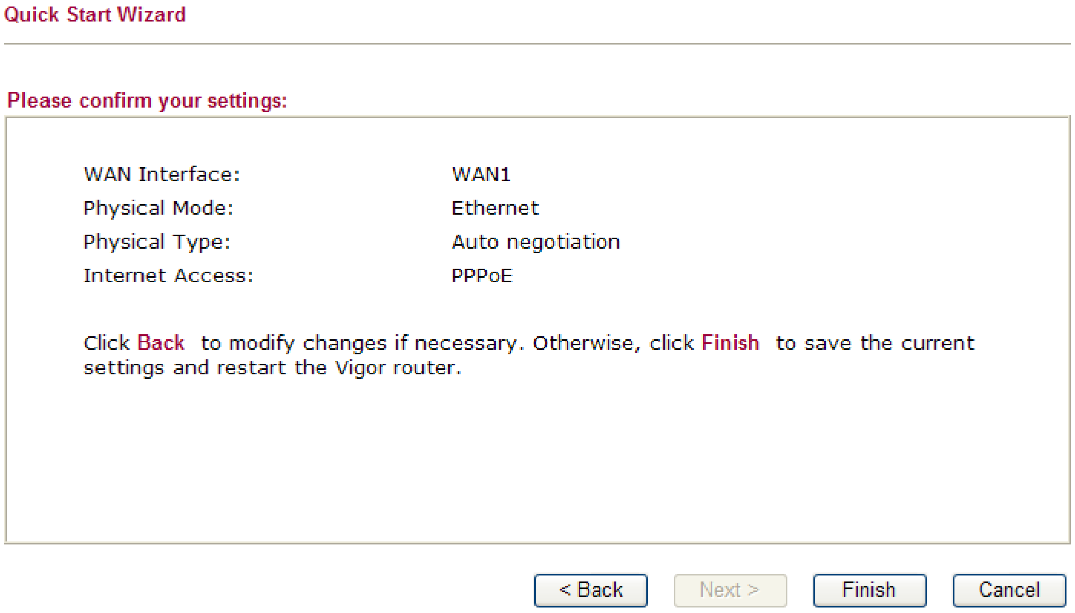
Confirm Password: ●●●●●●●●●

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.

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



Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE

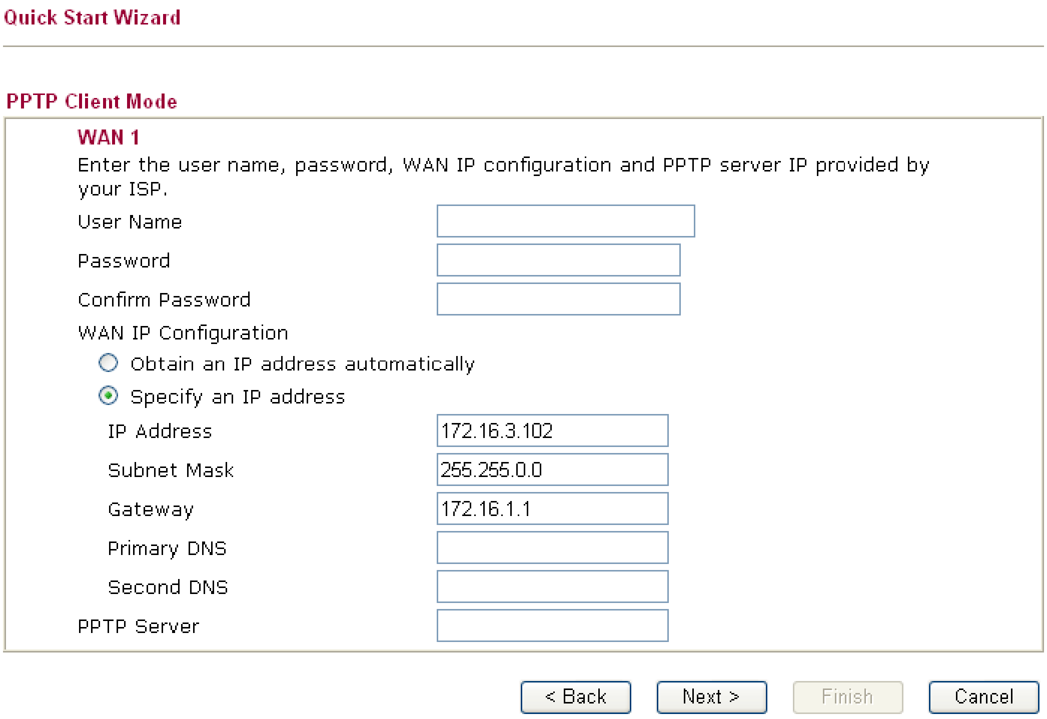
Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.4.2 PPTP/L2TP

Click **PPTP/L2TP** as the protocol. Type in all the information that your ISP provides for this protocol.



Quick Start Wizard

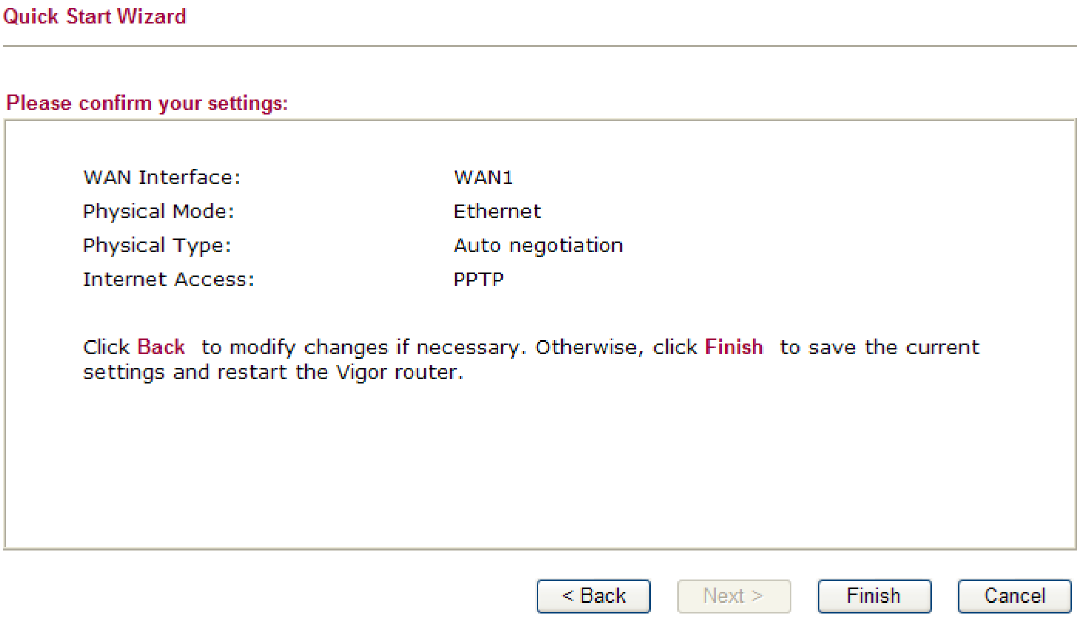
PPTP Client Mode

WAN 1

Enter the user name, password, WAN IP configuration and PPTP server IP provided by your ISP.

User Name	
Password	
Confirm Password	
WAN IP Configuration	
○ Obtain an IP address automatically	
● Specify an IP address	
IP Address	172.16.3.102
Subnet Mask	255.255.0.0
Gateway	172.16.1.1
Primary DNS	
Second DNS	
PPTP Server	

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



Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPTP

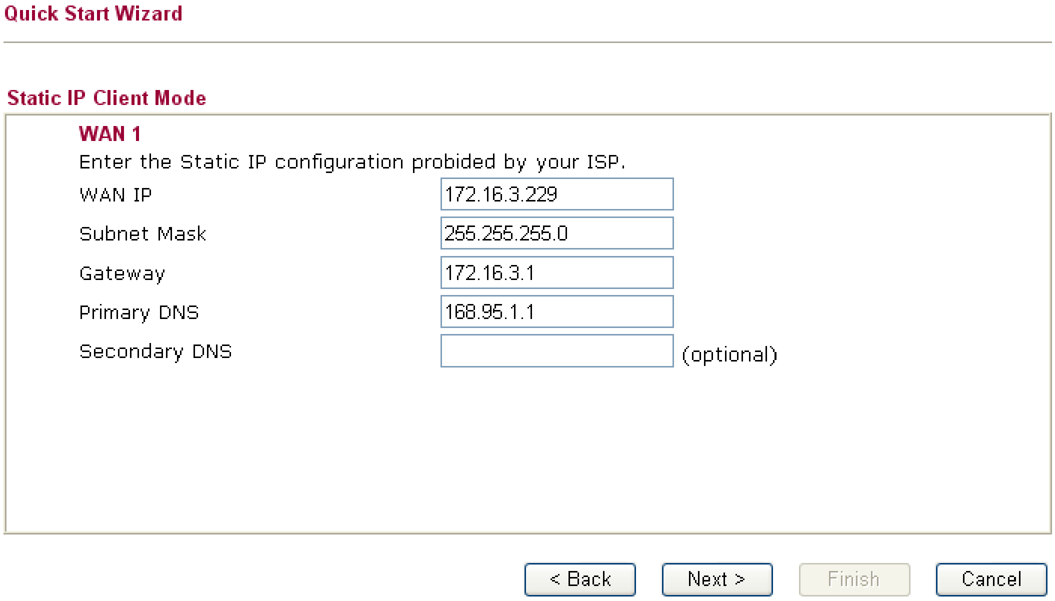
Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.4.3 Static IP

Click **Static IP** as the protocol. Type in all the information that your ISP provides for this protocol.



Quick Start Wizard

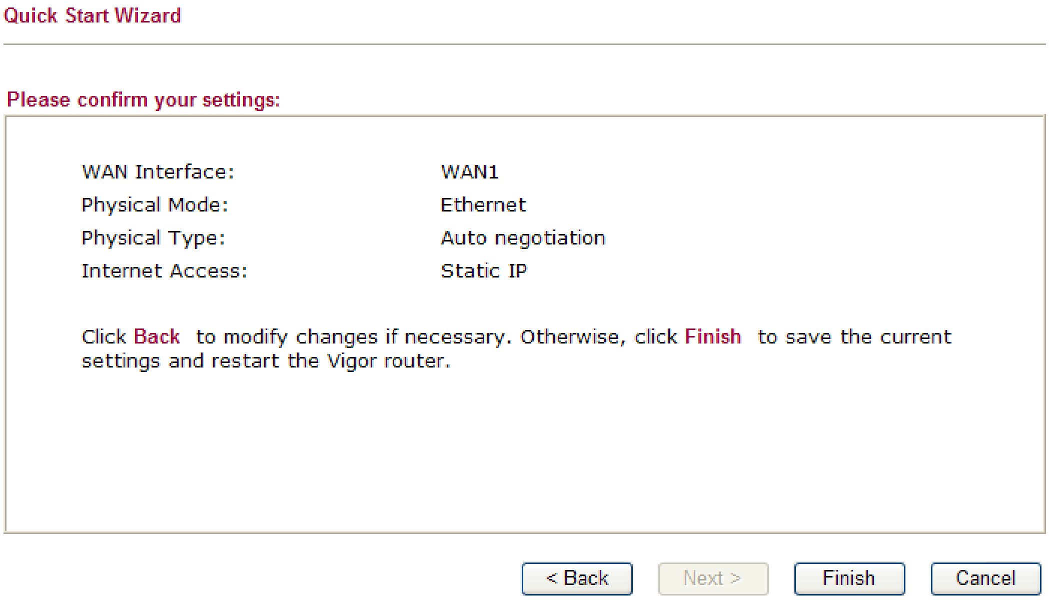
Static IP Client Mode

WAN 1

Enter the Static IP configuration probided by your ISP.

WAN IP	172.16.3.229
Subnet Mask	255.255.255.0
Gateway	172.16.3.1
Primary DNS	168.95.1.1
Secondary DNS	(optional)

After finishing the settings in this page, click **Next** to see the following page.



Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP

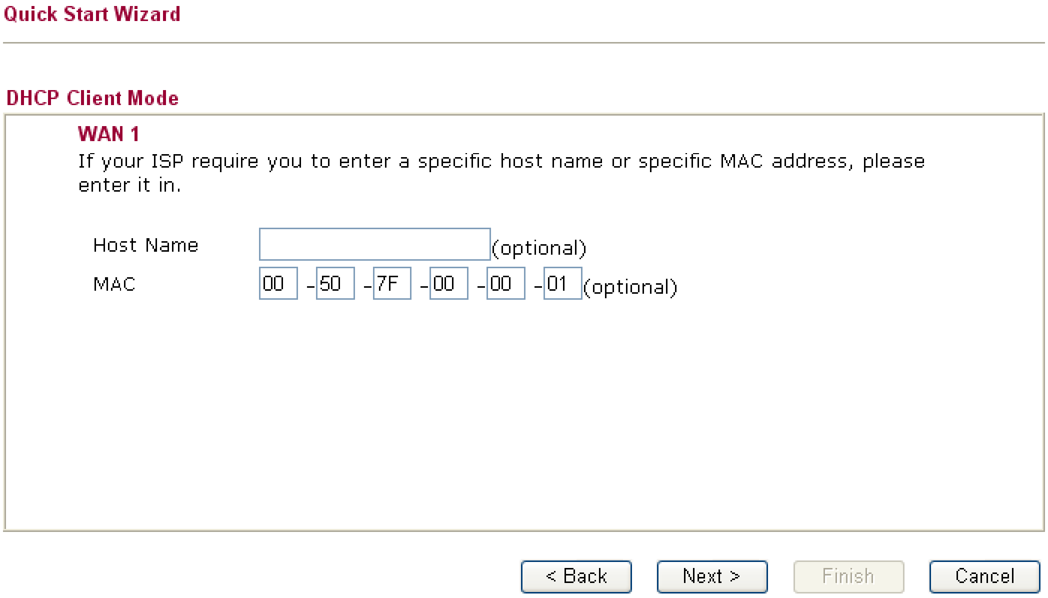
Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.4.4 DHCP

Click **DHCP** as the protocol. Type in all the information that your ISP provides for this protocol.



Quick Start Wizard

DHCP Client Mode

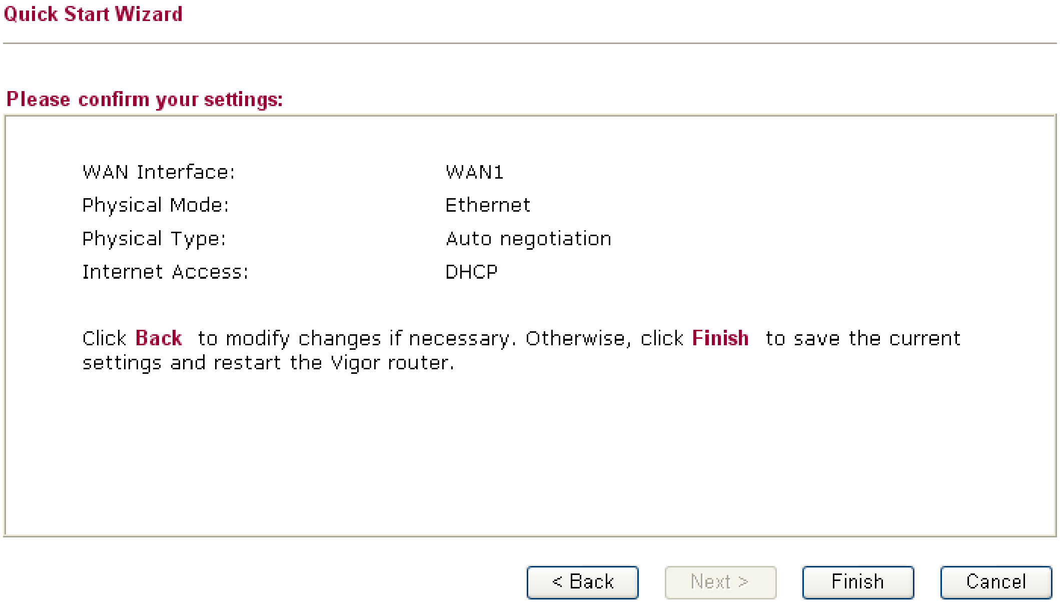
WAN 1

If your ISP require you to enter a specific host name or specific MAC address, please enter it in.

Host Name: (optional)

MAC: 00 - 50 - 7F - 00 - 00 - 01 (optional)

After finishing the settings in this page, click **Next** to see the following page.



Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP

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

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

Quick Start Wizard Setup OK !!!

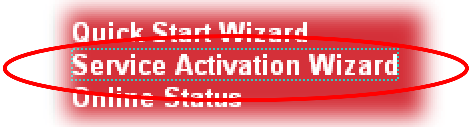
2.5 Service Activation Wizard

Service Activation Wizard can guide you to set WCF (Web Content Feature) 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 configurator.**

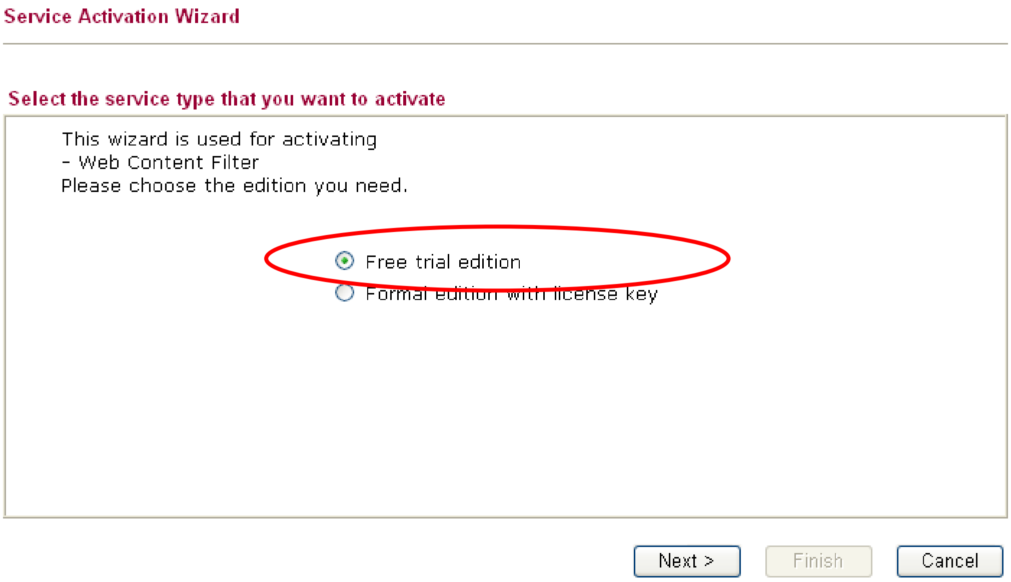
Service Activation Wizard is a tool which allows you to use trial version or update the license of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for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

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

1. Open **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.



Service Activation Wizard

Select the service type that you want to activate

This wizard is used for activating
- Web Content Filter
Please choose the edition you need.

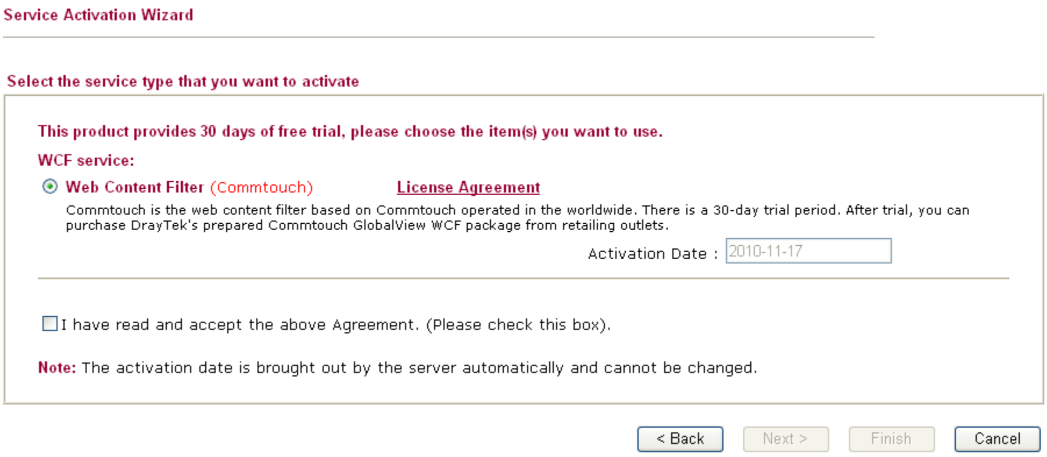
● Free trial edition
○ Formal edition with license key

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

Formal edition with license key: you can extend the license valid time manually.

Note: If you activate **Formal edition with license key** first, the free trial edition will be invalid.

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



Service Activation Wizard

Select the service type that you want to activate

This product provides 30 days of free trial, please choose the item(s) you want to use.

WCF service:

● Web Content Filter (Commtouch) License Agreement

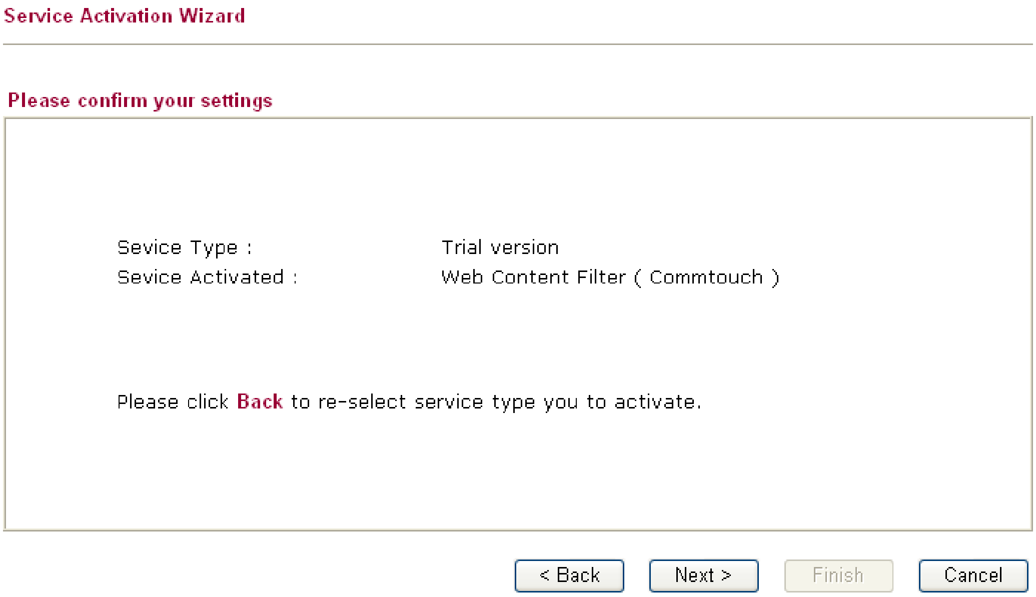
Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.

Activation Date : 2010-11-17

□ I have read and accept the above Agreement. (Please check this box).

Note: The activation date is brought out by the server automatically and cannot be changed.

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



Service Activation Wizard

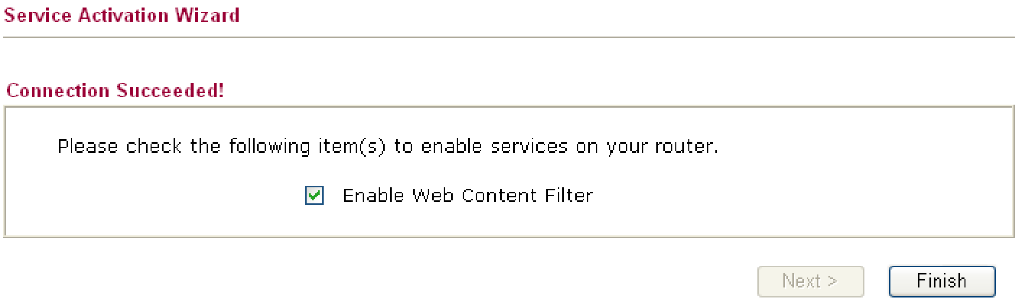
Please confirm your settings

Sevice Type : Trial version

Sevice Activated : Web Content Filter (Commtouch)

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

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



Service Activation Wizard

Connection Succeeded!

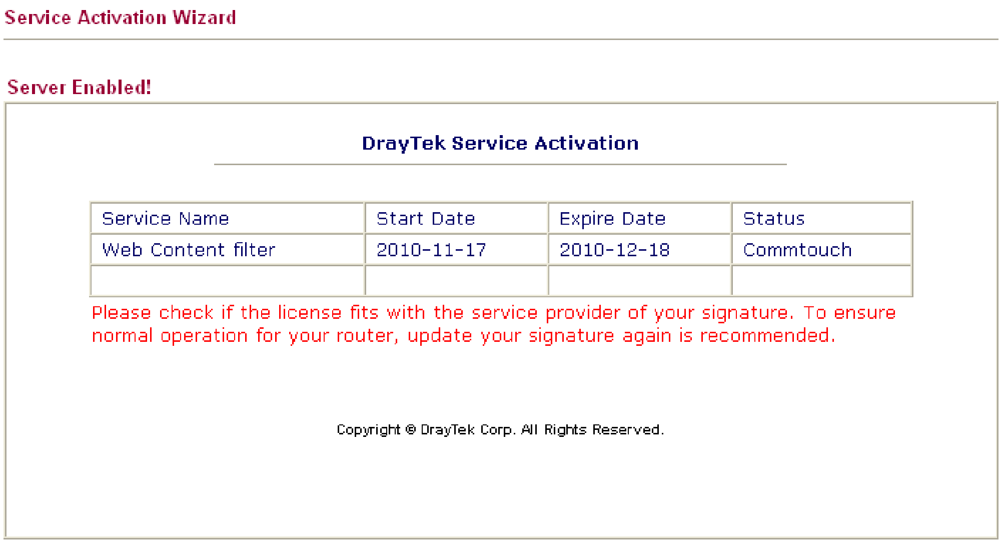
Please check the following item(s) to enable services on your router.

☑ Enable Web Content Filter

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!

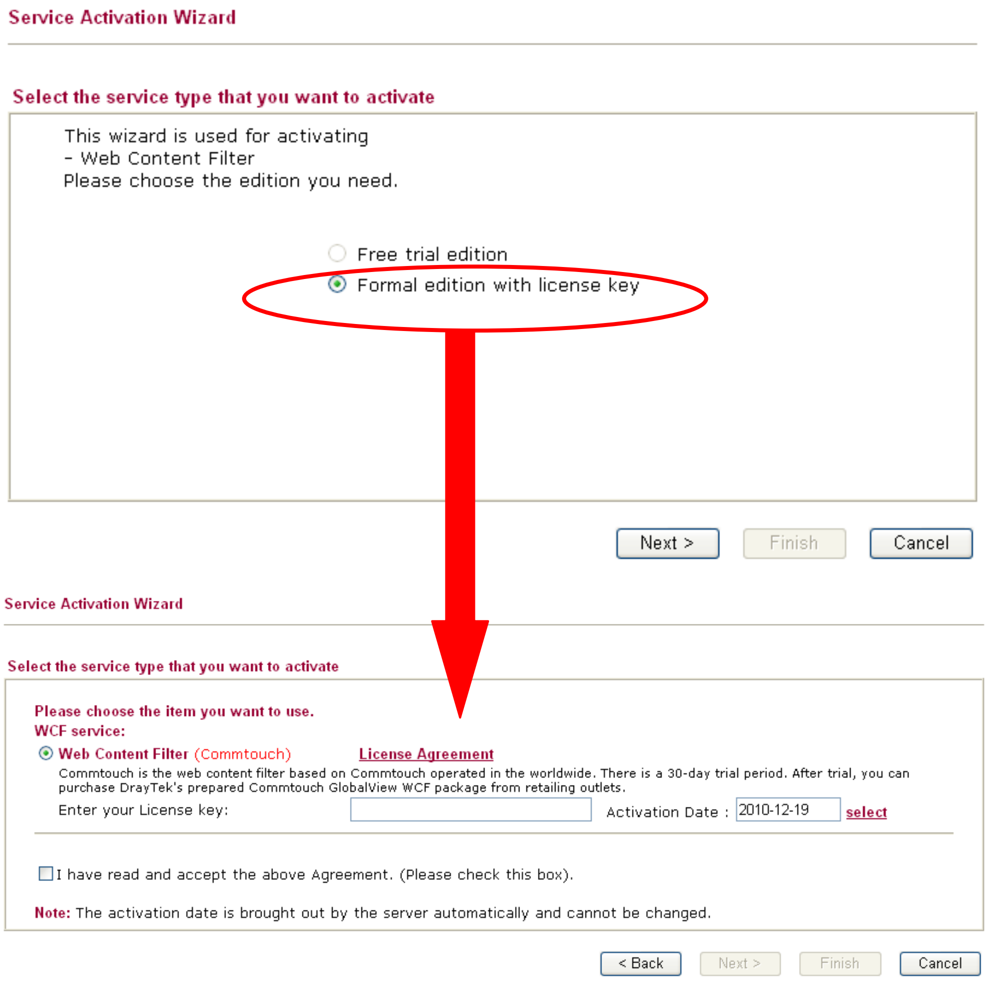
DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2010-11-17	2010-12-18	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.

Later, if you need to extend the license valid time, you can also use the **Service Activation Wizard** again to reach your goal by clicking the radio button of **Formal edition with license key** and clicking **Next.**



Service Activation Wizard

Select the service type that you want to activate

This wizard is used for activating
- Web Content Filter
Please choose the edition you need.

○ Free trial edition
● Formal edition with license key

Service Activation Wizard

Select the service type that you want to activate

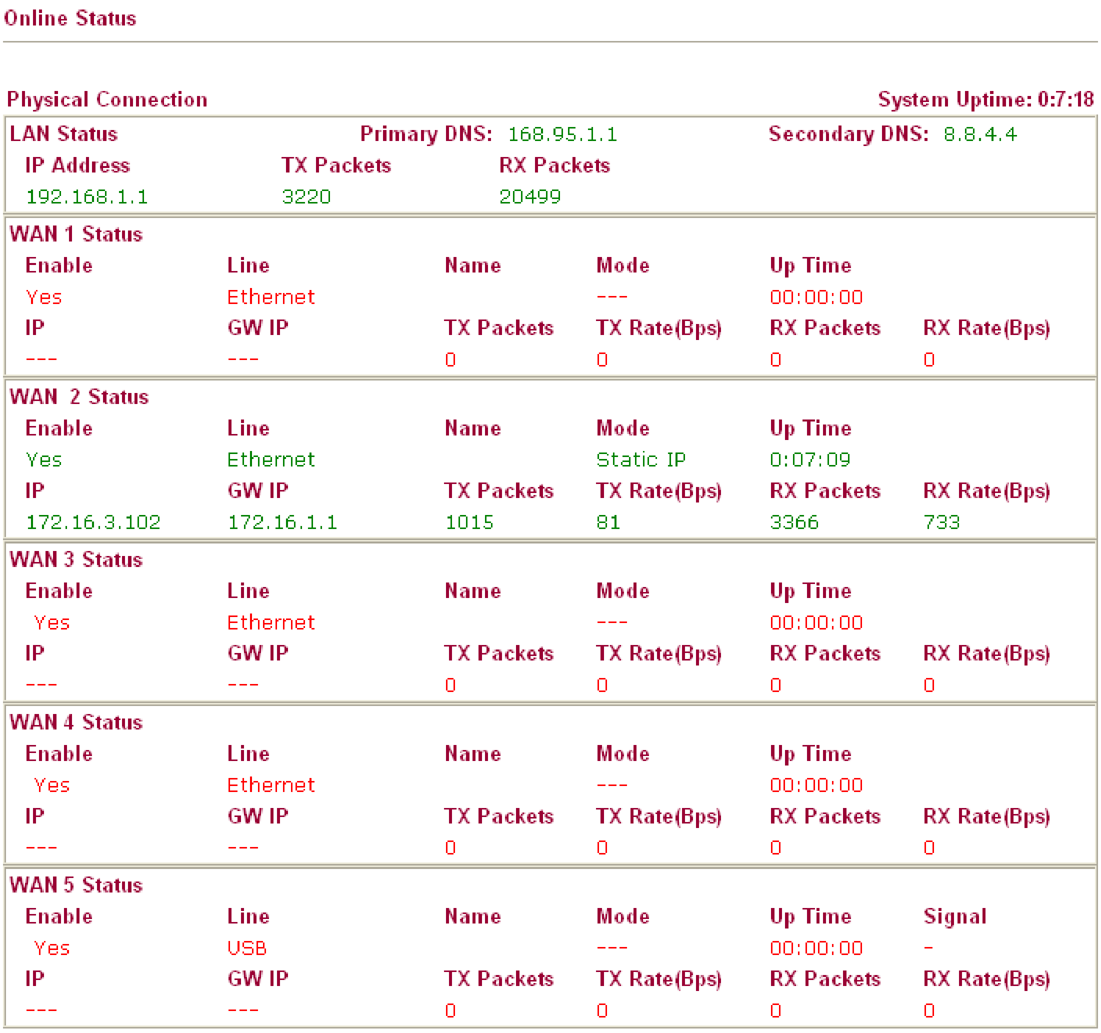
Please choose the item you want to use.
WCF service:
● Web Content Filter (Commtouch) License Agreement
Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.
Enter your License key: Activation Date : 2010-12-19 select

□ I have read and accept the above Agreement. (Please check this box).

Note: The activation date is brought out by the server automatically and cannot be changed.

2.6 Online Status

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



Online Status

Physical Connection — System Uptime: 0:7:18

LAN Status		Primary DNS: 168.95.1.1	Secondary DNS: 8.8.4.4
IP Address	TX Packets	RX Packets	
192.168.1.1	3220	20499	

WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		---	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:07:09	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
172.16.3.102	172.16.1.1	1015	81	3366	733

WAN 3 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		---	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 4 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		---	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 5 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	-
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

Detailed explanation is shown below:

Primary DNS Displays the IP address of the primary DNS.

Secondary DNS Displays the IP address of the secondary DNS.

LAN Status

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 number of received packets at the LAN interface.

WAN1~WAN5 Status

Line Displays the physical connection (Ethernet) of this interface.

Name Displays the name set in WAN web page.

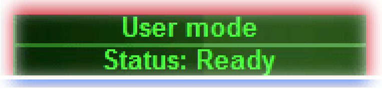
Mode Displays the type of WAN connection (e.g., PPPoE).

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.

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.

2.7 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.



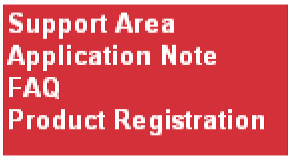
User mode
Status: Ready

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

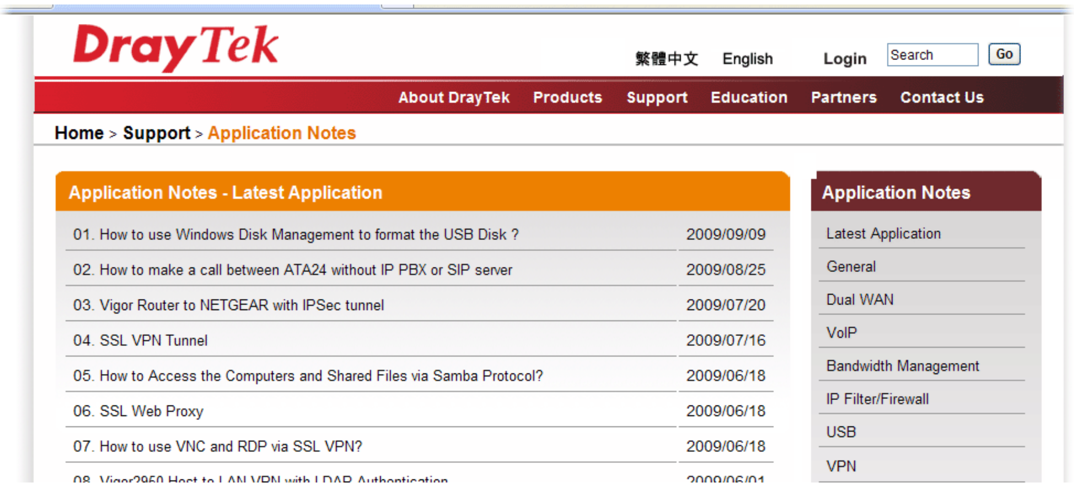
Settings Saved means your settings are saved once you click **Finish** or **OK** button.

2.8 Support Area

When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



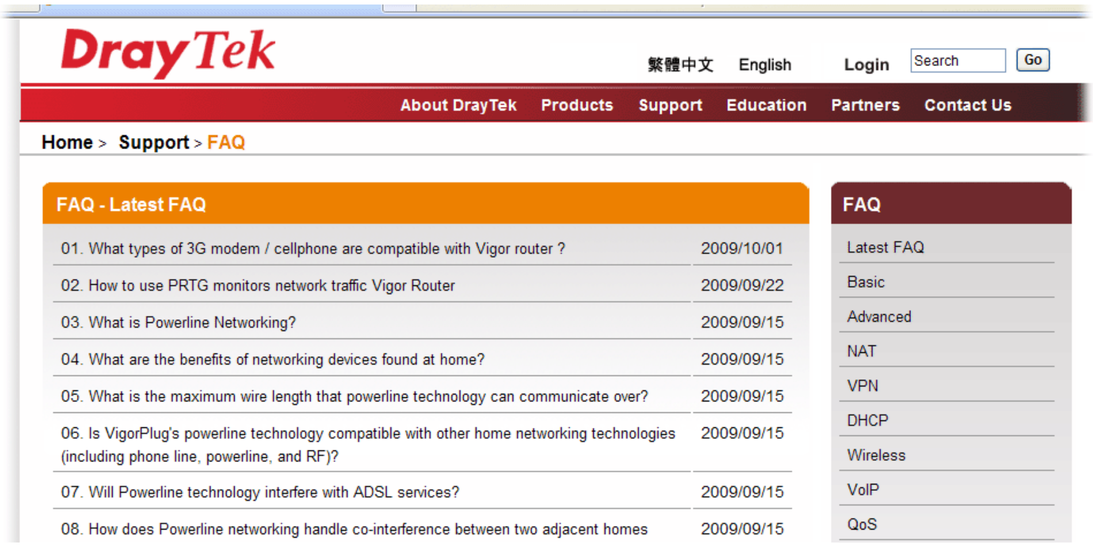
Click **Support Area>>Application Note**, the following web page will be displayed.



Application Notes - Latest Application

01. How to use Windows Disk Management to format the USB Disk ?	2009/09/09
02. How to make a call between ATA24 without IP PBX or SIP server	2009/08/25
03. Vigor Router to NETGEAR with IPSec tunnel	2009/07/20
04. SSL VPN Tunnel	2009/07/16
05. How to Access the Computers and Shared Files via Samba Protocol?	2009/06/18
06. SSL Web Proxy	2009/06/18
07. How to use VNC and RDP via SSL VPN?	2009/06/18
08. Vigor2950 Host to LAN VPN with LDAP Authentication	2009/06/01

Click **Support Area>>FAQ**, the following web page will be displayed.

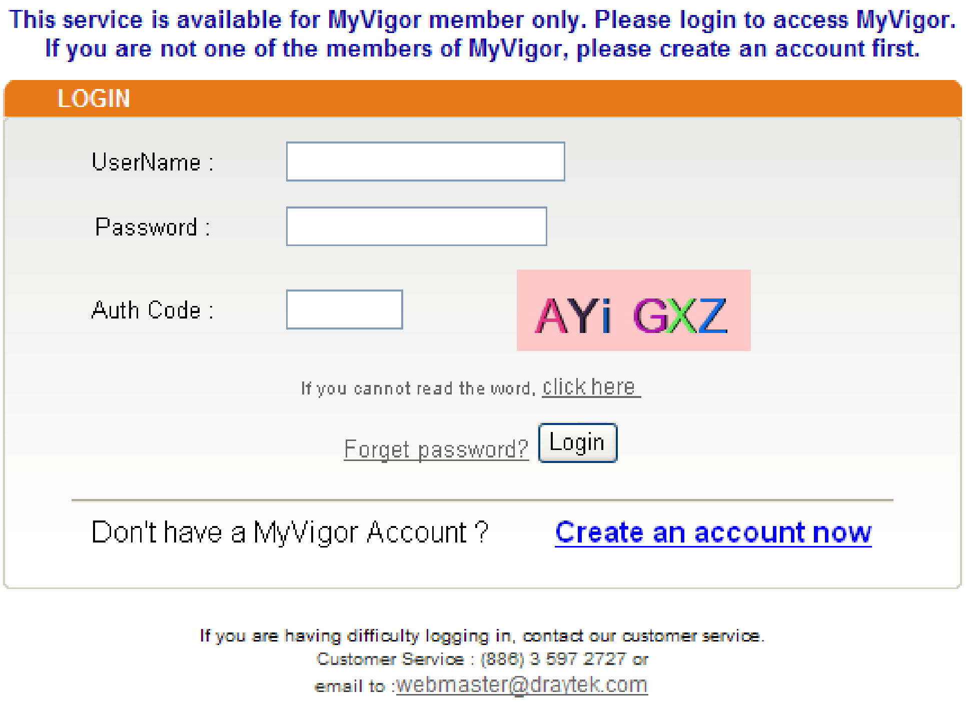


Home > Support > FAQ

FAQ - Latest FAQ

01. What types of 3G modem / cellphone are compatible with Vigor router ?	2009/10/01
02. How to use PRTG monitors network traffic Vigor Router	2009/09/22
03. What is Powerline Networking?	2009/09/15
04. What are the benefits of networking devices found at home?	2009/09/15
05. What is the maximum wire length that powerline technology can communicate over?	2009/09/15
06. Is VigorPlug's powerline technology compatible with other home networking technologies (including phone line, powerline, and RF)?	2009/09/15
07. Will Powerline technology interfere with ADSL services?	2009/09/15
08. How does Powerline networking handle co-interference between two adjacent homes	2009/09/15

Click **Support Area>>Product Registration**, the following web page will be displayed.



This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code :

If you cannot read the word, click here

Forget password? Login

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

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or
email to :webmaster@draytek.com

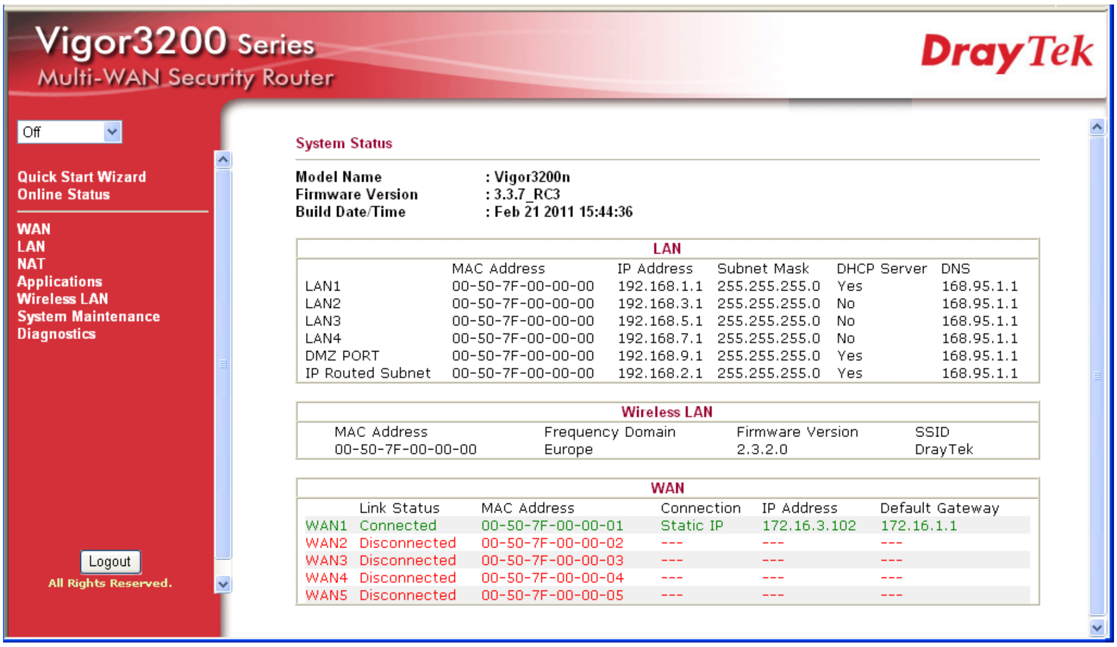
This page is left blank.

3 User Mode Operation

This chapter will guide users to execute simple configuration through user mode operation. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

Now, the **Main Screen** will appear. Be aware that “User mode” will be displayed on the bottom left side.



System Status

Model Name : Vigor3200n
Firmware Version : 3.3.7_RC3
Build Date/Time : Feb 21 2011 15:44:36

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-00-00-00	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-00-00-00	192.168.3.1	255.255.255.0	No	168.95.1.1
LAN3	00-50-7F-00-00-00	192.168.5.1	255.255.255.0	No	168.95.1.1
LAN4	00-50-7F-00-00-00	192.168.7.1	255.255.255.0	No	168.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.2.1	255.255.255.0	Yes	168.95.1.1

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-00-00-00	Europe	2.3.2.0	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-00-00-01	Static IP	172.16.3.102	172.16.1.1
WAN2	Disconnected	00-50-7F-00-00-02	---	---	---
WAN3	Disconnected	00-50-7F-00-00-03	---	---	---
WAN4	Disconnected	00-50-7F-00-00-04	---	---	---
WAN5	Disconnected	00-50-7F-00-00-05	---	---	---

3.1 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.

3.1.1 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.

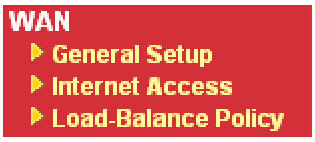
Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is more and more popular, Vigor3200 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor3200, it can support HSDPA/UMTS/EDGE/GPRS and the future 3G standard (HSUPA, etc). Vigor3200n 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 the LAN port on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor3200n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor3200n series.

Mobile Coffee shop
Internet
Web surfing, E-Mail, Instant messaging etc.
VPN
Vigor
3.5G HSDPA USB Modem

After connecting into the router, 3G USB Modem will be regarded as the fifth WAN port. However, the other Ethernet WAN ports still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN5 also can be used as backup device. Therefore, when other Ethernet WAN port is 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**.

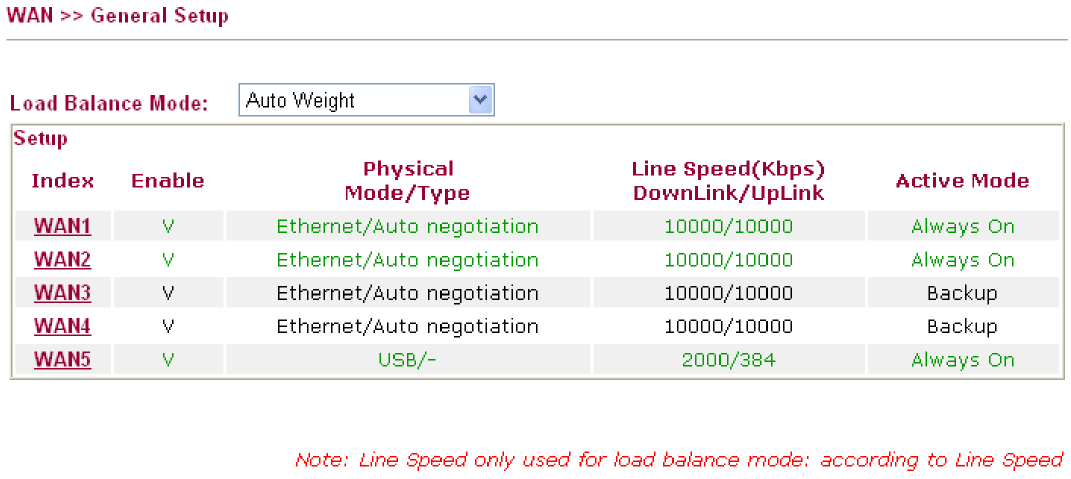


3.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 to WAN5 in details.

There are four WAN ports (represented with WAN1, WAN2, WAN3 and WAN4 in web pages) and one USB port (represented with WAN5 in web pages) offered by the router. For this router supports multiple WANs 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.

This webpage allows you to set general setup for WAN1 to WAN5 respectively.



WAN >> General Setup

Load Balance Mode: Auto Weight

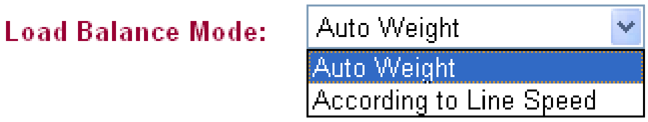
Setup

Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	V	Ethernet/Auto negotiation	10000/10000	Always On
WAN2	V	Ethernet/Auto negotiation	10000/10000	Always On
WAN3	V	Ethernet/Auto negotiation	10000/10000	Backup
WAN4	V	Ethernet/Auto negotiation	10000/10000	Backup
WAN5	V	USB/-	2000/384	Always On

Note: Line Speed only used for load balance mode: according to Line Speed

From the above figure, WAN1 ~ WAN4 connect to Internet through the interface of Ethernet; WAN5 connects to Internet via USB interface. Therefore the configuration for each WAN port will be different slightly. Please click the WAN link under Index to open the web page for detailed configuration.

Load Balance Mode This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Weigh** to let the router reach the best load balance.



Load Balance Mode: Auto Weight

Index Click the WAN interface link under Index to access into the

WAN configuration page.

Enable **V** means such WAN interface is enabled and ready to be used.

Physical Mode / Type Display the physical mode and physical type of such WAN interface.

Line Speed Display the downstream and upstream rate of such WAN interface.

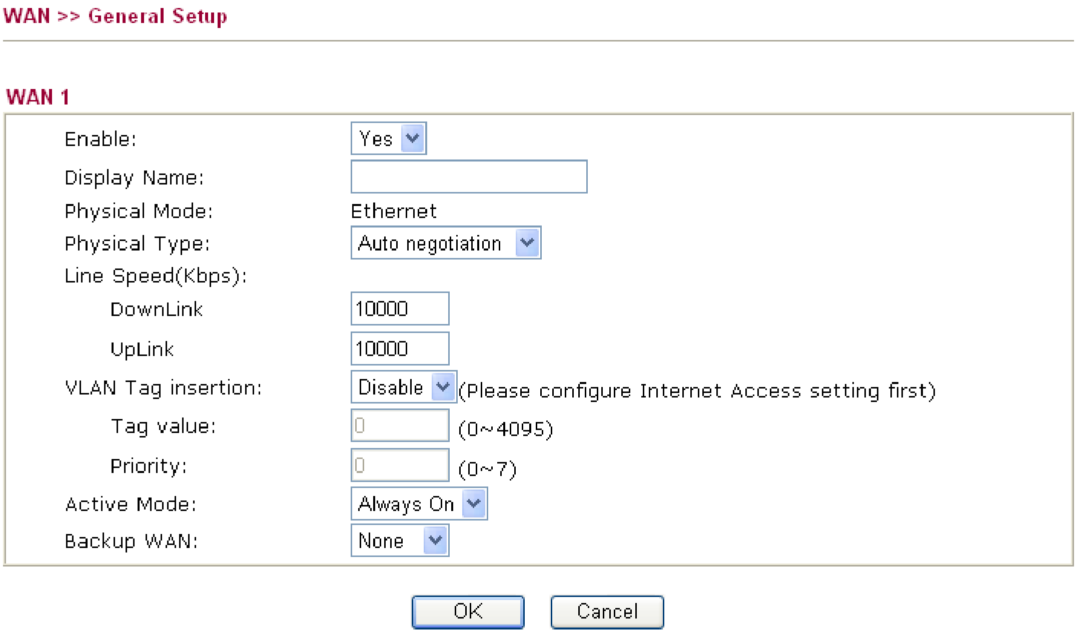
Active Mode Display whether such WAN interface is Active device or backup device.

Backup WAN Display the Backup WAN interface for such WAN when it is disabled.

> **Note:** In default, each WAN is enabled.

For WAN1 ~ WAN4

WAN1 ~ WAN4 are fixed with physical mode of Giga Ethernet. Here we take WAN1 as an example.



WAN >> General Setup

WAN 1

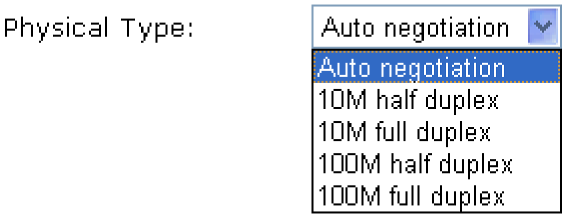
Enable:	Yes
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Line Speed(Kbps):	
DownLink	10000
UpLink	10000
VLAN Tag insertion:	Disable (Please configure Internet Access setting first)
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On
Backup WAN:	None

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.



Physical Type: Auto negotiation

- Auto negotiation
- 10M half duplex
- 10M full duplex
- 100M half duplex
- 100M full duplex

Line Speed

If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps. The default setting for down link and up link is 10000Kbps.

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.

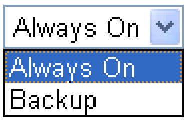
Disable – Disable the function of VLAN with tag.

Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.

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

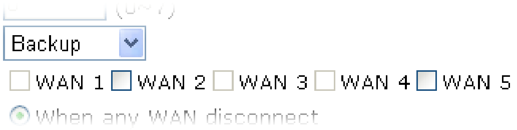
Active Mode

Determine the WAN interface will be active for always (**Always On**) or be treated as a backup WAN interface (**Backup**).



Backup Type

If you choose **Always On** as **Active Mode**, you can choose from the available WAN interfaces as a backup WAN. Later, when current WAN is disconnected for some reason, the backup WAN will be activated automatically to prevent data transmission from connection interrupted.

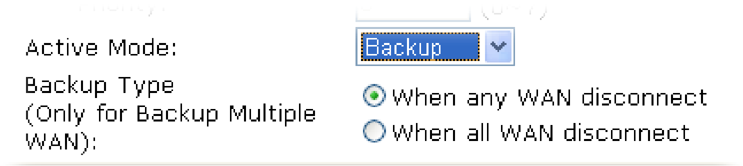


Backup

□ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5

● When any WAN disconnect

If you choose **Backup** as the **Active Mode**, The option of **Backup Type** will be displayed. You have to specify which role the WAN interface should play.



Active Mode: Backup

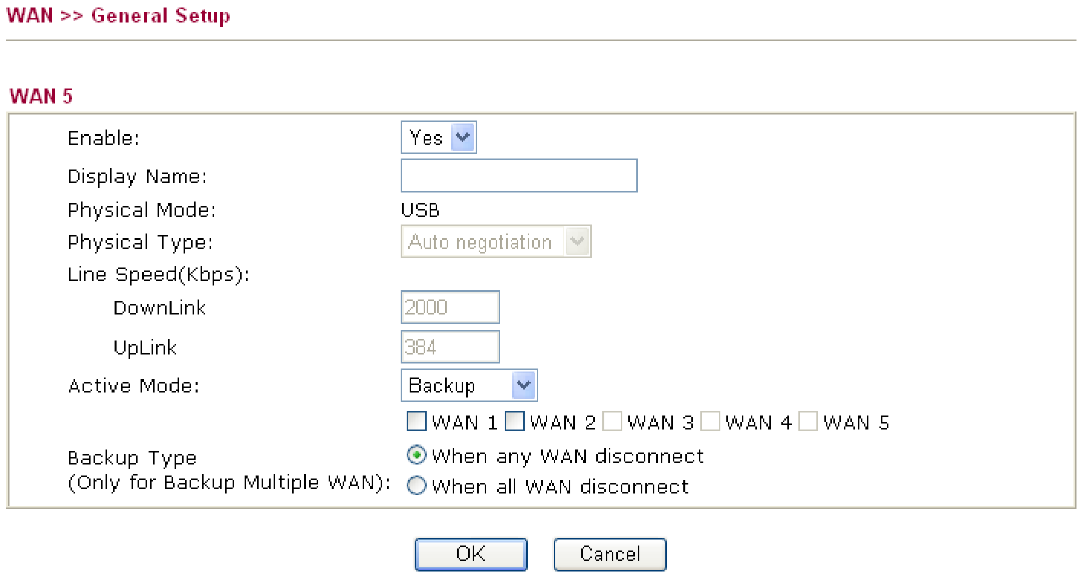
Backup Type (Only for Backup Multiple WAN): ● When any WAN disconnect ○ When all WAN disconnect

When any WAN disconnect –WAN1 will be activated when any master WAN interface disconnects.

When all WAN disconnect –WAN1 will be activated when all master WAN interfaces disconnect.

For WAN5

To use 3G network connection through 3G USB Modem, please configure **WAN5** interface.



WAN >> General Setup

WAN 5

Enable:	Yes
Display Name:	
Physical Mode:	USB
Physical Type:	Auto negotiation
Line Speed(Kbps):	
DownLink	2000
UpLink	384
Active Mode:	Backup
	□ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5
Backup Type (Only for Backup Multiple WAN):	● When any WAN disconnect ○ When all WAN disconnect

Enable Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.

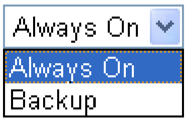
Display Name Type the description for such WAN interface.

Physical Mode Display the physical mode of such WAN interface.

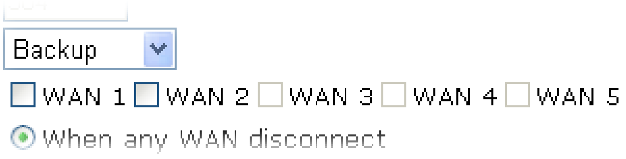
Physical type For such WAN interface is fixed to USB network connection, it is not necessary to specify physical type.

Line Speed If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.

Active Mode Determine the WAN interface will be active for always (**Always On**) or be treated as a backup WAN interface (**Backup**).



Backup Type If you choose **Always On** as **Active Mode**, you can choose from the available WAN interfaces as a backup WAN. Later, when current WAN is disconnected for some reason, the backup WAN will be activated automatically to prevent data transmission from connection interrupted.

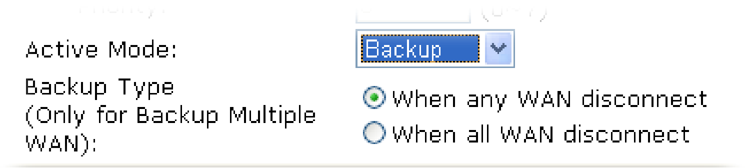


Backup

□ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5

● When any WAN disconnect

If you choose **Backup** as the **Active Mode**, Backup WAN will be changed into **Backup Type**. You have to specify which role the WAN interface should play.



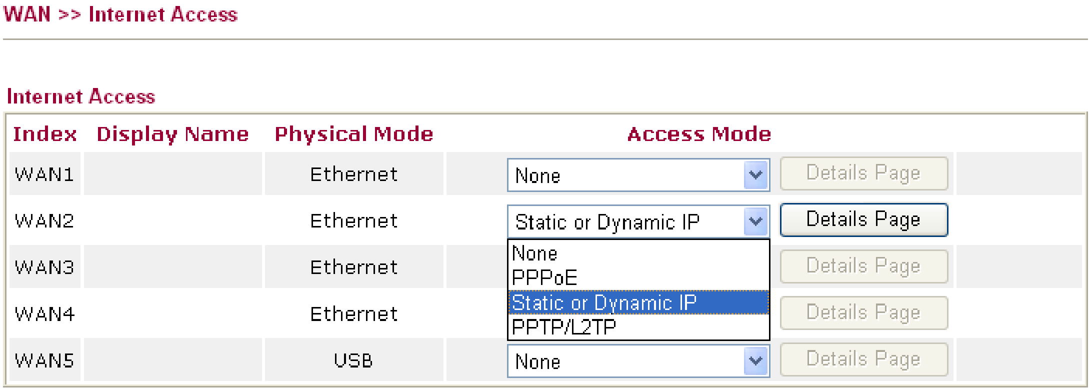
Active Mode:	Backup
Backup Type (Only for Backup Multiple WAN):	● When any WAN disconnect ○ When all WAN disconnect

When any WAN disconnect – WAN1 will be activated when any WAN interface disconnects.

When all WAN disconnect – WAN1 will be activated when all the WAN interfaces disconnect.

3.1.3 Internet Access

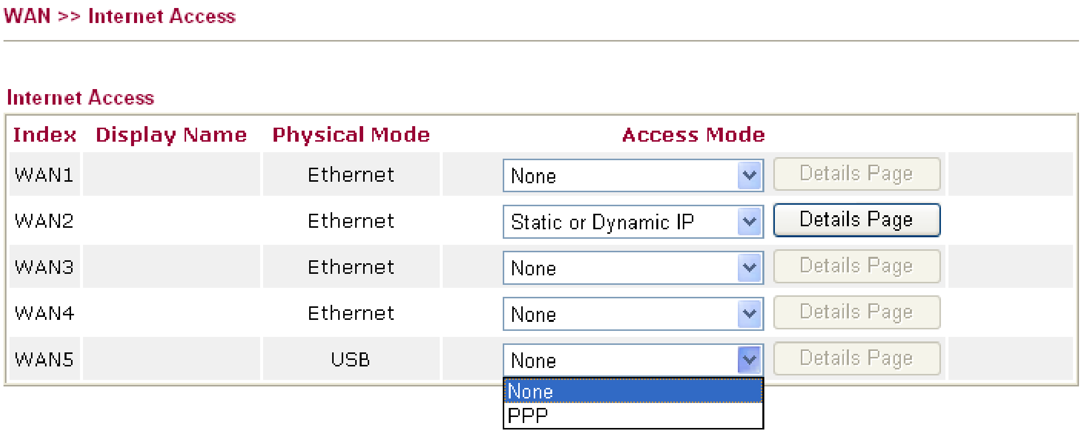
For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3/WAN4/WAN5) for Internet Access. Due to different Physical Mode of WAN interface, the Access Mode for these connections also varies. Refer to the following figures.



WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	None	Details Page
WAN2		Ethernet	Static or Dynamic IP	Details Page
WAN3		Ethernet		Details Page
WAN4		Ethernet		Details Page
WAN5		USB	None	Details Page



WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	None	Details Page
WAN2		Ethernet	Static or Dynamic IP	Details Page
WAN3		Ethernet	None	Details Page
WAN4		Ethernet	None	Details Page
WAN5		USB	None	Details Page

Index Display the WAN interface.

Display Name It shows the name of the WAN1/WAN2/WAN3/WAN4/WAN5 that entered in general setup.

Physical Mode It shows the physical connection for WAN1-WAN4 (Ethernet) /WAN5 (3G USB Modem) according to the real network connection.

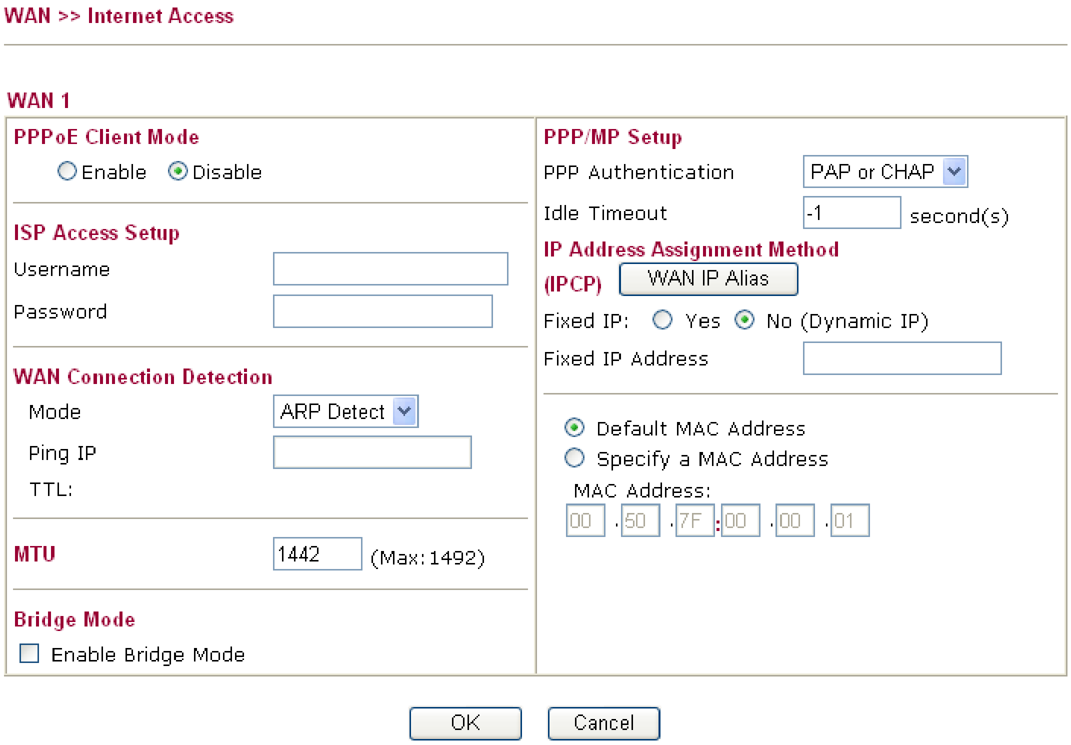
Access Mode Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click

Details Page for accessing the page to configure the settings.

Details Page
This button will open different web page according to the access mode that you choose in WAN interface

Details Page for PPPoE in WAN1 ~ WAN4

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



WAN >> Internet Access

WAN 1

PPPoE Client Mode
○ Enable ● Disable

ISP Access Setup
Username
Password

WAN Connection Detection
Mode: ARP Detect
Ping IP
TTL:

MTU: 1442 (Max:1492)

Bridge Mode
□ Enable Bridge Mode

PPP/MP Setup
PPP Authentication: PAP or CHAP
Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP) [WAN IP Alias]
Fixed IP: ○ Yes ● No (Dynamic IP)
Fixed IP Address

● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 .50 .7F :00 .00 .01

[OK] [Cancel]

PPPoE Client 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.

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.

Password – Type in the password provided by ISP in this field.

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 1442.

Bridge Mode If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.

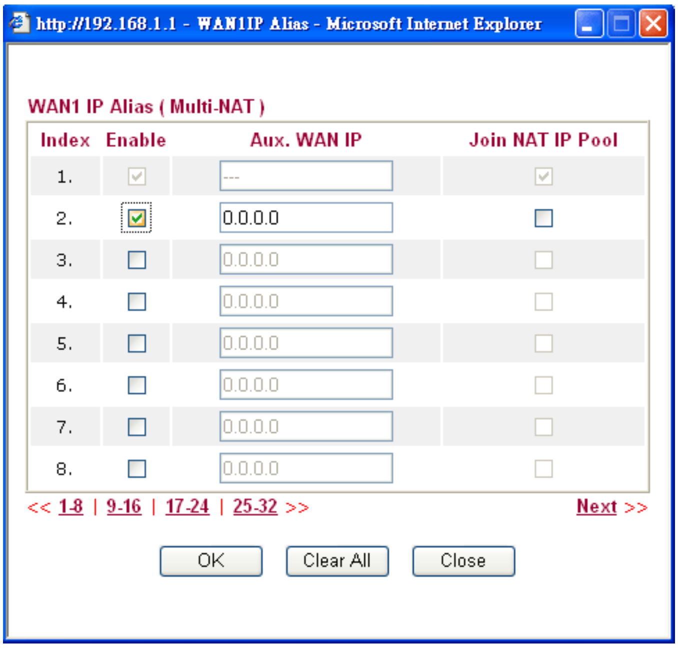
PPP/MP Setup **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. If you want to connect to Internet all the time, you can check **Always On**.

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 **32** public IP addresses other than the current one you are using.

Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	☑	---	☑
2.	☑	0.0.0.0	□
3.	□	0.0.0.0	□
4.	□	0.0.0.0	□
5.	□	0.0.0.0	□
6.	□	0.0.0.0	□
7.	□	0.0.0.0	□
8.	□	0.0.0.0	□

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.

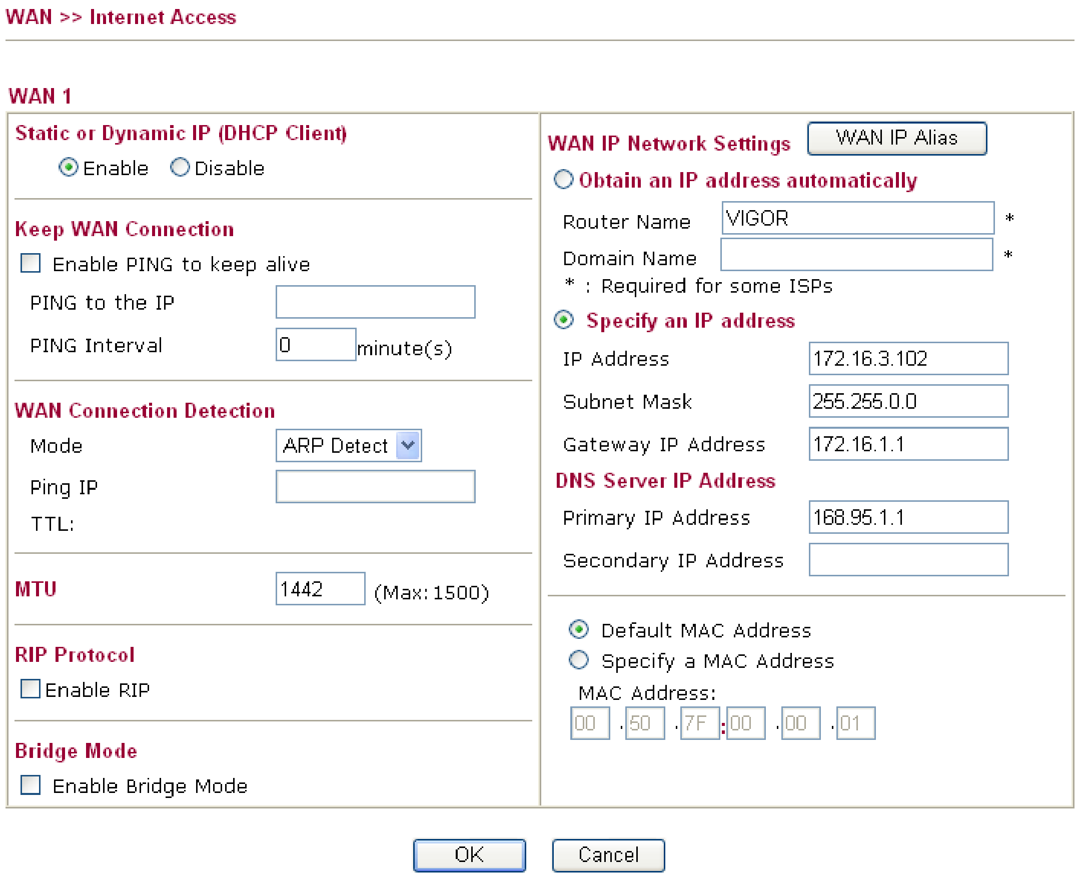
Specify a MAC Address – Type the MAC address for the router manually.

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

Details Page for Static or Dynamic IP in WAN1 ~ WAN4

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 choose **Static or Dynamic IP** mode from **Internet Access** menu. The following web page will be shown.



WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client)

● Enable ○ Disable

Keep WAN Connection

□ Enable PING to keep alive

PING to the IP:

PING Interval: 0 minute(s)

WAN Connection Detection

Mode: ARP Detect

Ping IP:

TTL:

MTU: 1442 (Max:1500)

RIP Protocol

□ Enable RIP

Bridge Mode

□ Enable Bridge Mode

WAN IP Network Settings [WAN IP Alias]

○ Obtain an IP address automatically

Router Name: VIGOR *

Domain Name: *

* : Required for some ISPs

● Specify an IP address

IP Address: 172.16.3.102

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.1.1

DNS Server IP Address

Primary IP Address: 168.95.1.1

Secondary IP Address:

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F : 00 . 00 . 01

Static or Dynamic IP — 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. The default setting is 1442.

RIP Protocol

Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.

Bridge Mode

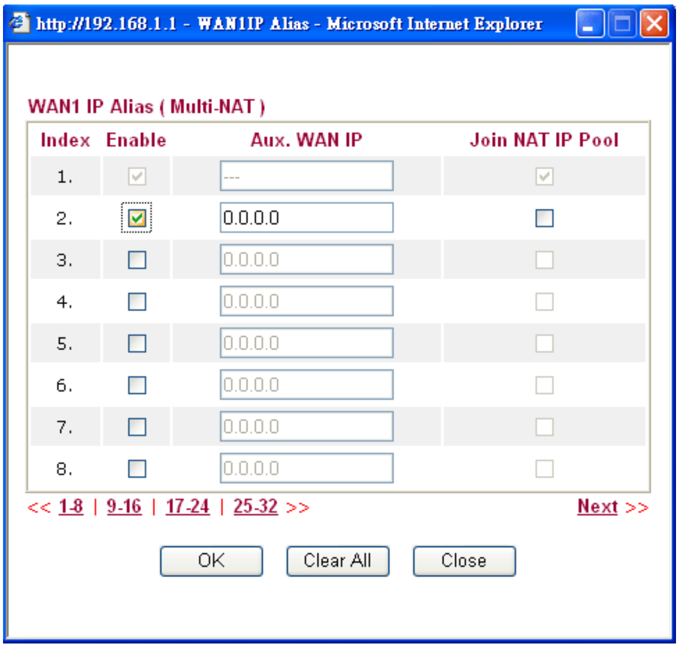
If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.

WAN IP Network Settings

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 **32** public IP addresses other than the current one you are using.

Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	☑	---	☑
2.	☑	0.0.0.0	□
3.	□	0.0.0.0	□
4.	□	0.0.0.0	□
5.	□	0.0.0.0	□
6.	□	0.0.0.0	□
7.	□	0.0.0.0	□
8.	□	0.0.0.0	□

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.

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.

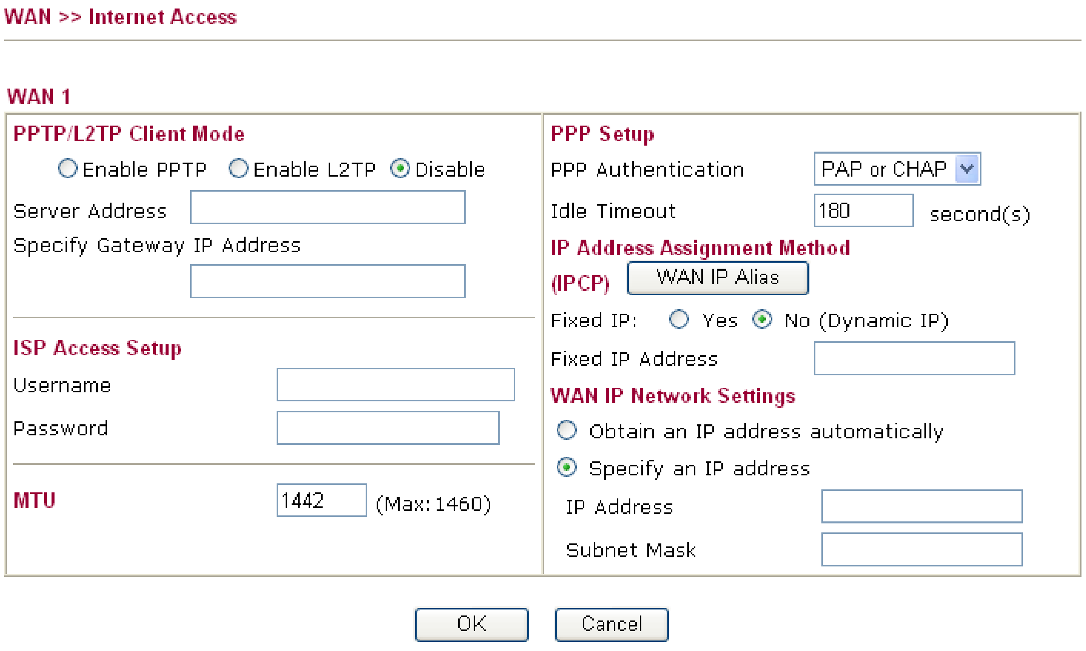
Default MAC Address : Click this radio button to use default MAC address for the router.

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.

Details Page for PPTP/L2TP in WAN1 ~ WAN4

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Internet Access** menu. The following web page will be shown.



WAN >> Internet Access

WAN 1

PPTP/L2TP Client Mode

○ Enable PPTP ○ Enable L2TP ● Disable

Server Address

Specify Gateway IP Address

ISP Access Setup

Username

Password

MTU 1442 (Max:1460)

PPP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: 180 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

Subnet Mask

PPTP/L2TP Client Mode

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.

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.

Password -Type in the password provided by ISP in this field.

MTU

It means Max Transmit Unit for packet. The default setting is 1442.

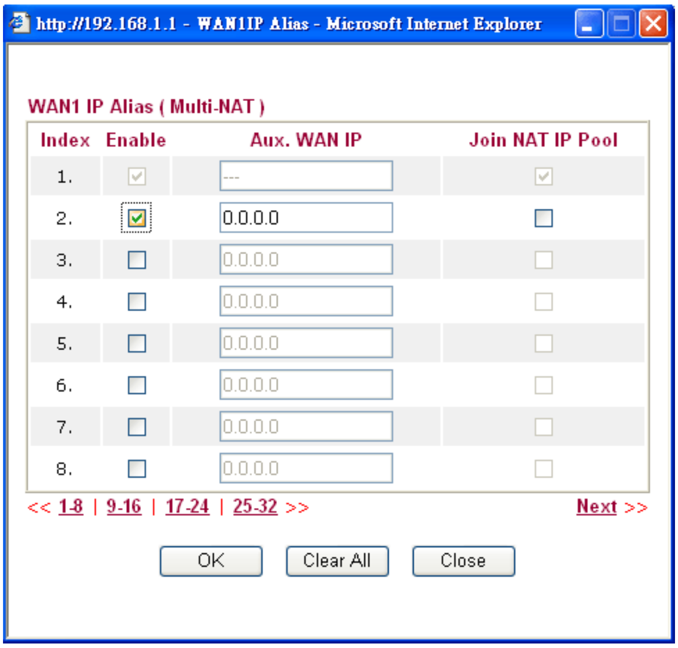
PPP Setup

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)

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.



http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	☑	---	☑
2.	☑	0.0.0.0	□
3.	□	0.0.0.0	□
4.	□	0.0.0.0	□
5.	□	0.0.0.0	□
6.	□	0.0.0.0	□
7.	□	0.0.0.0	□
8.	□	0.0.0.0	□

<< 1-8 | 9-16 | 17-24 | 25-32 >>   Next >>

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.

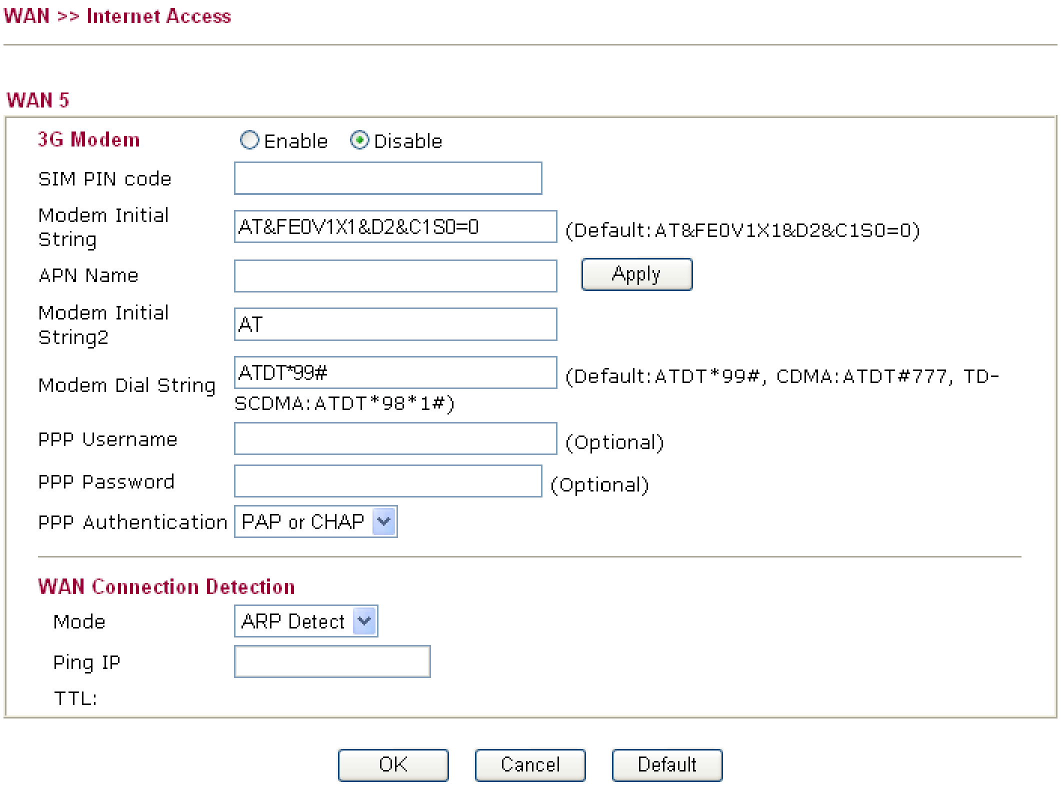
Specify an IP address – Click this radio button to specify some data.

IP Address – Type the IP address.

Subnet Mask – Type the subnet mask.

Details Page for PPP in WAN5

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN5. The following web page will be shown.



WAN >> Internet Access

WAN 5

3G Modem	○ Enable ● Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Initial String2	AT	
Modem Dial String	ATDT*99#	(Default:ATDT*99#, CDMA:ATDT#777, TD-SCDMA:ATDT*98*1#)
PPP Username		(Optional)
PPP Password		(Optional)
PPP Authentication	PAP or CHAP	

WAN Connection Detection

Mode	ARP Detect
Ping IP	
TTL:	

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

SIM PIN code Type PIN code of the SIM card that will be used to access Internet.

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.

APN Name APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.

Modem Initial String2 The initial string is shared with APN.

In some cases, users may need another initial ***AT*** command to restrict 3G band or do any special settings.

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.

PPP Username Type the PPP username (optional).

PPP Password Type the PPP password (optional).

PPP Authentication Select **PAP only** or **PAP or CHAP** for PPP.

WAN Connection Such function allows you to verify whether network connection

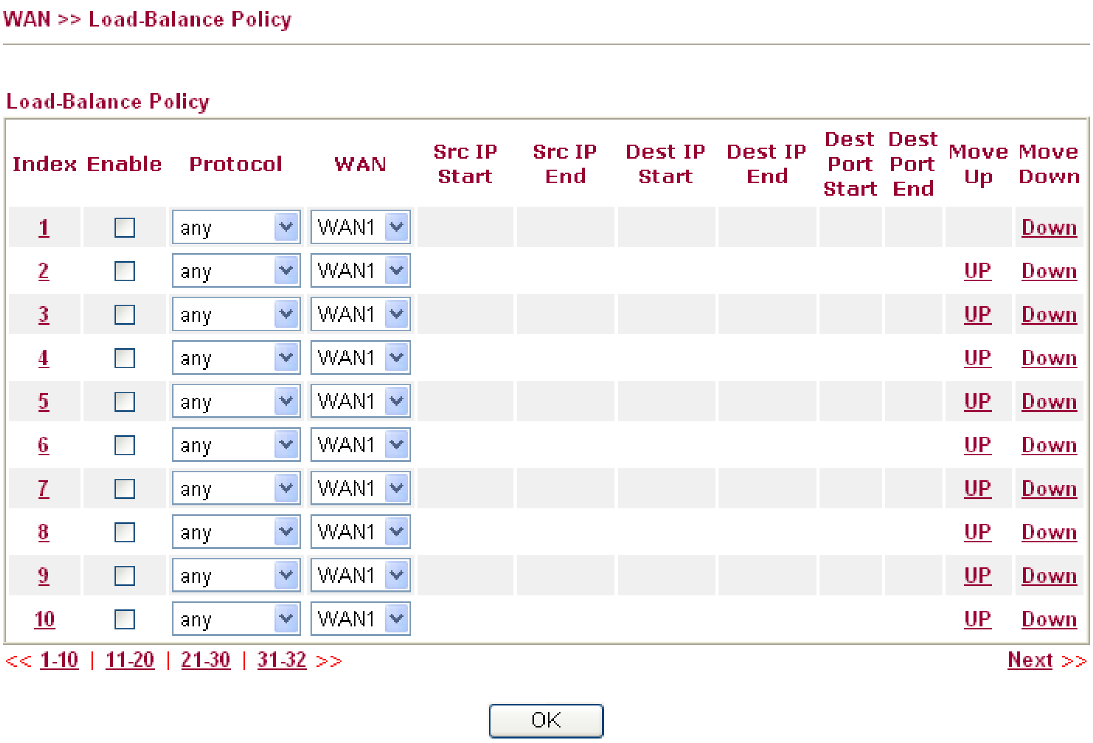
Detection	is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
Default	Click it to reset to the factory default setting for 3G connection.

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

3.1.4 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

Note: Load-Balance Policy is running only when more than two WAN interfaces are activated.



WAN >> Load-Balance Policy

Load-Balance Policy

Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	□	any	WAN1								Down
2	□	any	WAN1							UP	Down
3	□	any	WAN1							UP	Down
4	□	any	WAN1							UP	Down
5	□	any	WAN1							UP	Down
6	□	any	WAN1							UP	Down
7	□	any	WAN1							UP	Down
8	□	any	WAN1							UP	Down
9	□	any	WAN1							UP	Down
10	□	any	WAN1							UP	Down

<< 1-10 | 11-20 | 21-30 | 31-32 >> Next >>

OK

Index Click the number of index to access into the load-balance policy configuration web page.

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to change the protocol for the WAN interface.

WAN Use the drop-down menu to change the WAN interface.

Src IP Start Displays the IP address for the start of the source IP

Src IP End Displays the IP address for the end of the source IP.

Dest IP Start Displays the IP address for the start of the destination IP.

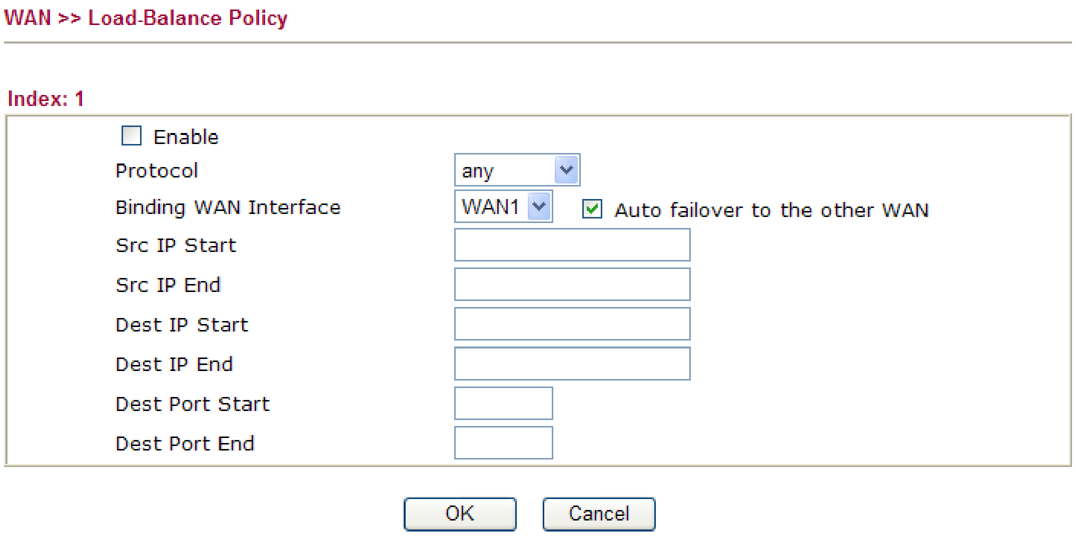
Dest IP End Displays the IP address for the end of the destination IP.

Dest Port Start Displays the IP address for the start of the destination port.

Dest Port End Displays the IP address for the end of the destination port.

Move UP/Move Down Use **Up** or **Down** link to move the order of the policy.

Click **Index 1** to access into the following page for configuring load-balance policy.



WAN >> Load-Balance Policy

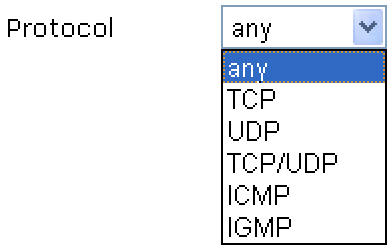
Index: 1

□ Enable

Protocol	any
Binding WAN Interface	WAN1 ☑ Auto failover to the other WAN
Src IP Start	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
Dest Port End	

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to choose a proper protocol for the WAN interface.



Binding WAN interface Choose the WAN interface (WAN1 / WAN2 / WAN3 / WAN4 /WAN5) for binding.

Auto failover to other WAN – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is failover.

Src IP Start Type the source IP start for the specified WAN interface.

Src IP End Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.

Dest IP Start Type the destination IP start for the specified WAN interface.

Dest IP End Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

Dest Port Start Type the destination port start for the destination IP.

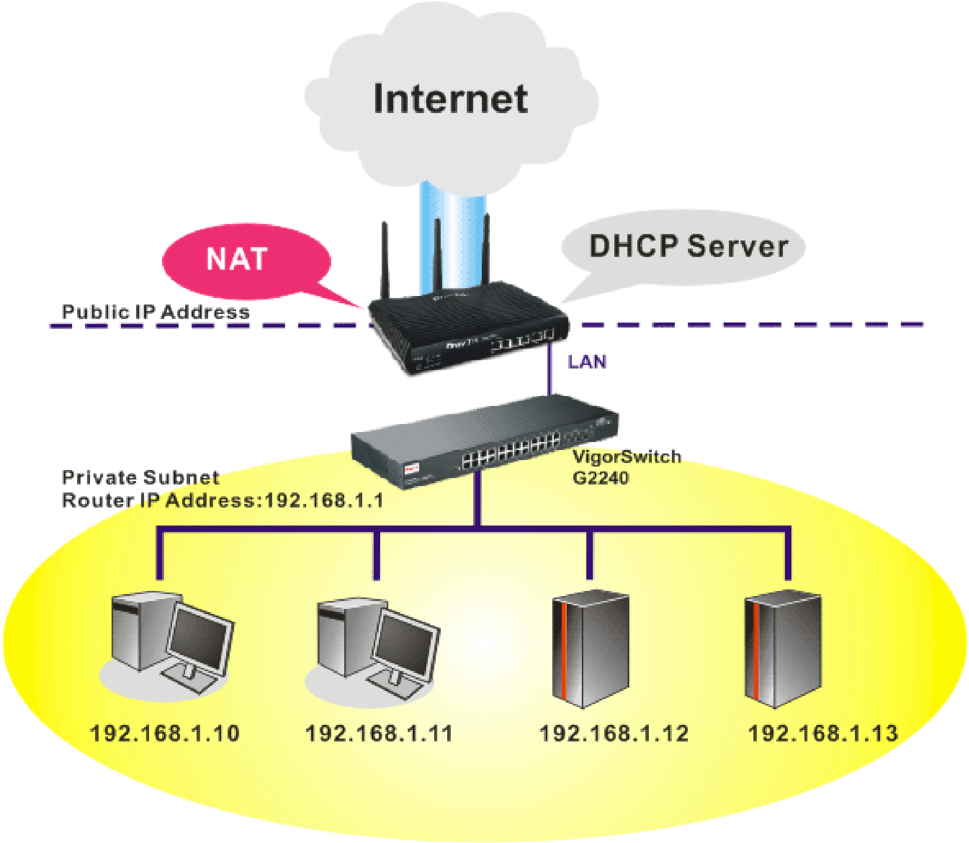
Dest Port End Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

3.2 LAN

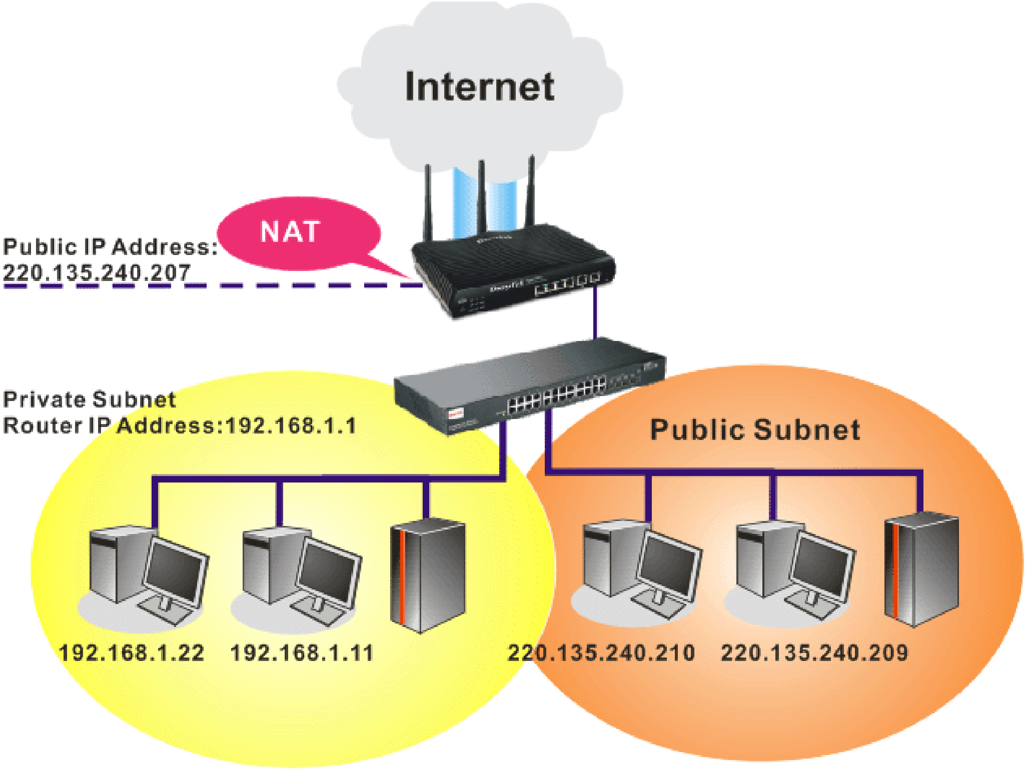
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

3.2.1 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.

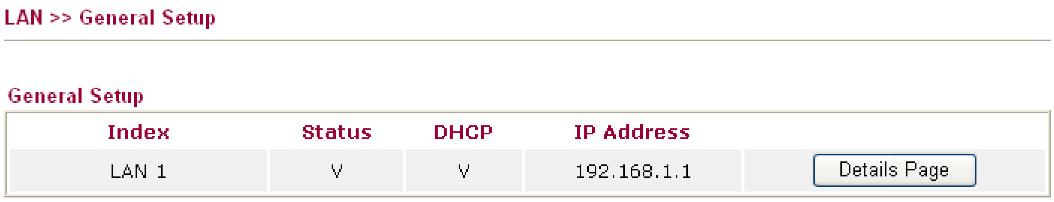


What is Routing Information Protocol (RIP)

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.

3.2.2 General Setup

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



LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page

Index Display the number of LAN interface.

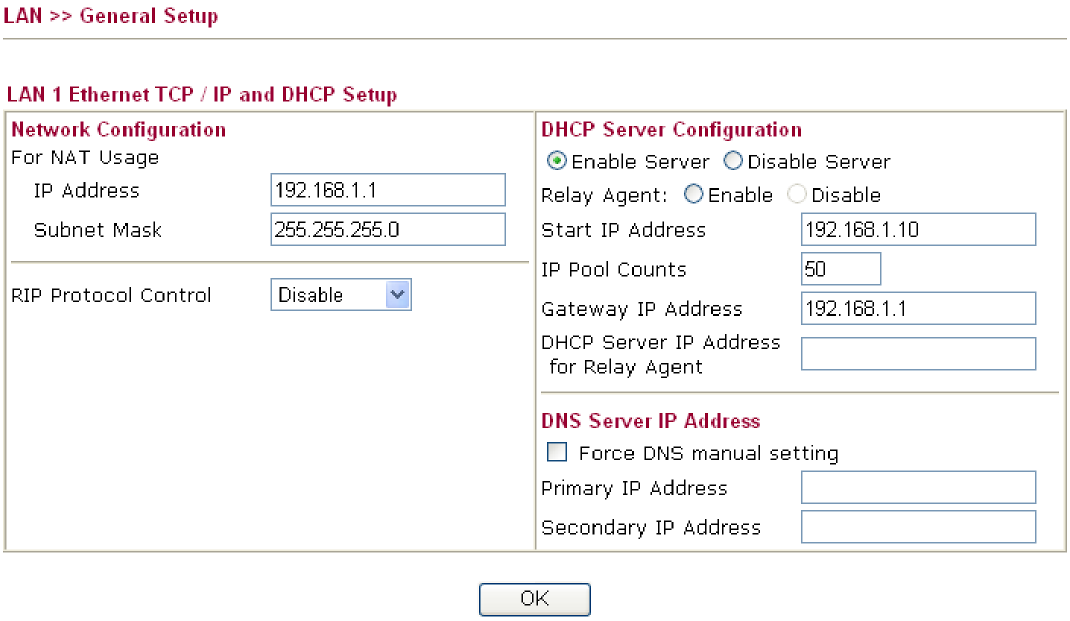
Status Basically, LAN1 status is enabled in default.

DHCP LAN1 is configured with DHCP in default.

IP Address Display the IP address for LAN1. Such information is set in default.

Details Page Click it to access into the setting page.

Details Page for LAN1



LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration

For NAT Usage

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable

DHCP Server Configuration

● Enable Server ○ Disable Server

Relay Agent: ○ Enable ○ Disable

Start IP Address: 192.168.1.10

IP Pool Counts: 50

Gateway IP Address: 192.168.1.1

DHCP Server IP Address for Relay Agent:

DNS Server IP Address

□ Force DNS manual setting

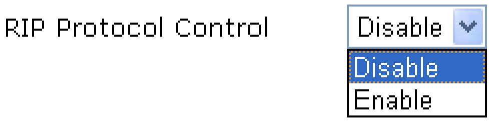
Primary IP Address:

Secondary IP Address:

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 interruption of the exchange of routing information between routers.



RIP Protocol Control: Disable

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

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

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

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

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 192.168.1.10, the starting IP address must be 192.168.1.11 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.

DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server IP Address

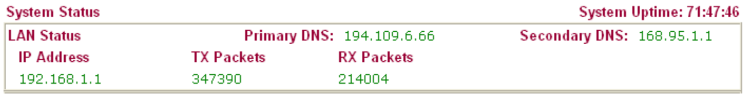
DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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:



System Status   System Uptime: 71:47:46

LAN Status   Primary DNS: 194.109.6.66   Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	347390	214004

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.

3.3 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.

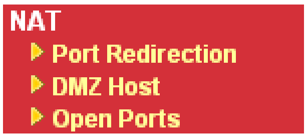
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize 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.

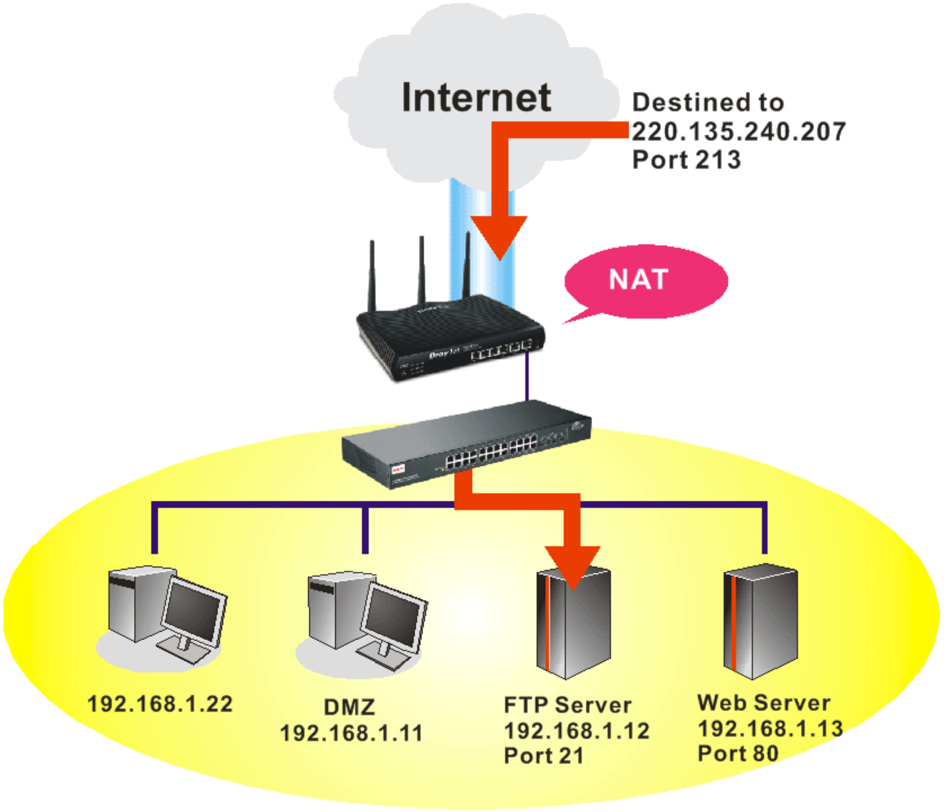
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



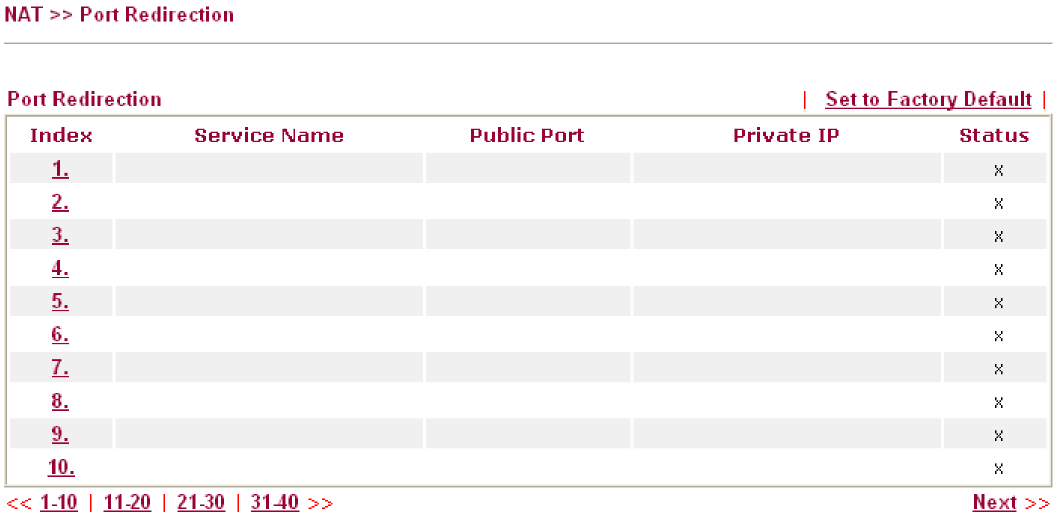
3.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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



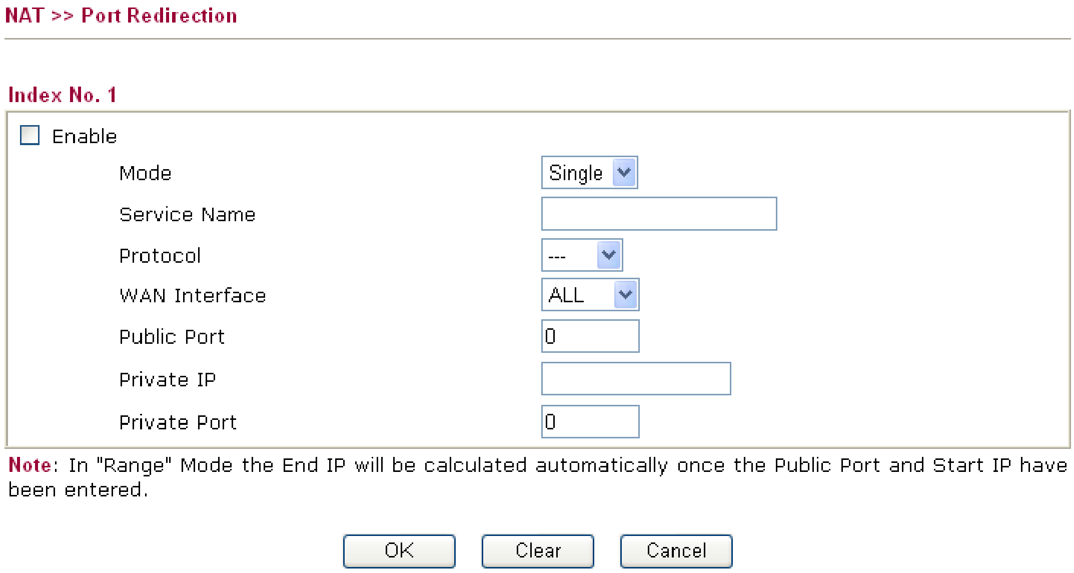
NAT >> Port Redirection

Port Redirection | Set to Factory Default |

Index	Service Name	Public Port	Private IP	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 | 21-30 | 31-40 >> Next >>

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



NAT >> Port Redirection

Index No. 1

□ Enable	
Mode	Single
Service Name	
Protocol	---
WAN Interface	ALL
Public Port	0
Private IP	
Private Port	0

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

Enable Check this box to enable such port redirection setting.

Mode Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name Enter the description of the specific network service.

Protocol Select the transport layer protocol (TCP or UDP).

WAN Interface Select the WAN interface used for port redirection.

The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port.

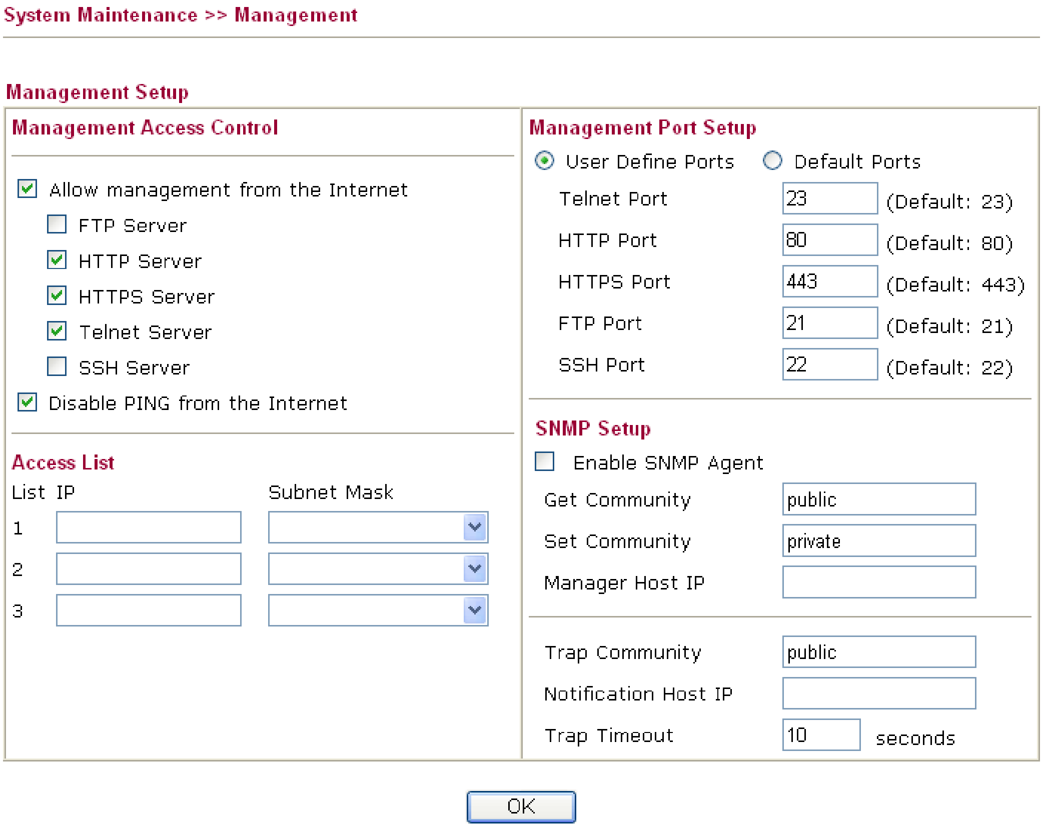
Public Port Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.

Private IP Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).

Private Port Specify the private port number of the service offered by the internal host

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



System Maintenance >> Management

Management Setup

Management Access Control	Management Port Setup
☑ Allow management from the Internet	● User Define Ports ○ Default Ports
□ FTP Server	Telnet Port: 23 (Default: 23)
☑ HTTP Server	HTTP Port: 80 (Default: 80)
☑ HTTPS Server	HTTPS Port: 443 (Default: 443)
☑ Telnet Server	FTP Port: 21 (Default: 21)
□ SSH Server	SSH Port: 22 (Default: 22)
☑ Disable PING from the Internet	

Access List

List	IP	Subnet Mask
1		
2		
3		

SNMP Setup

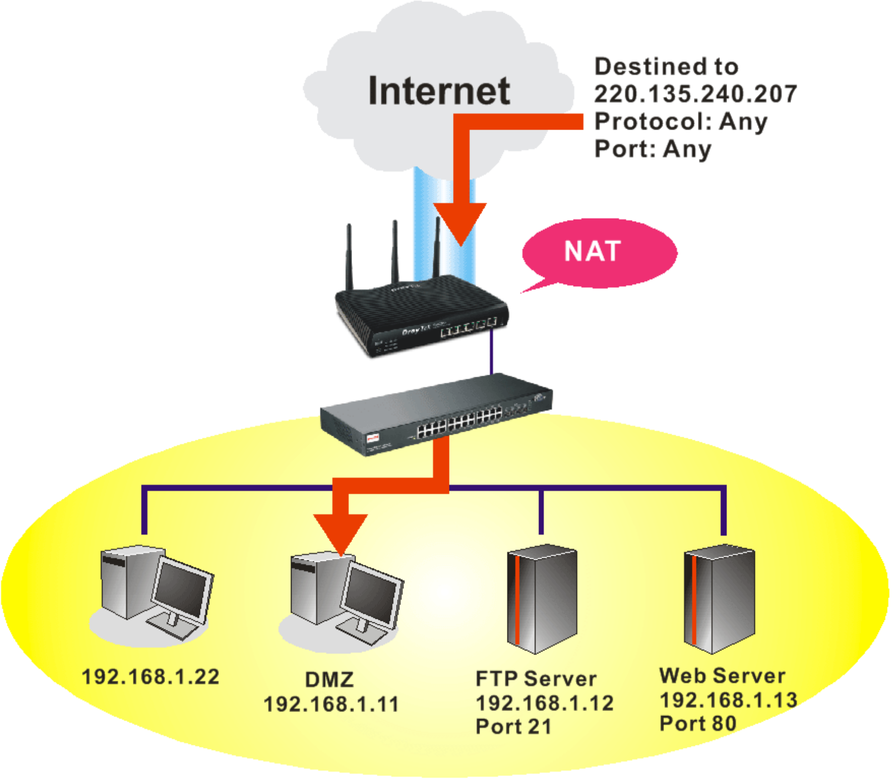
□ Enable SNMP Agent

Get Community	public
Set Community	private
Manager Host IP	
Trap Community	public
Notification Host IP	
Trap Timeout	10 seconds

OK

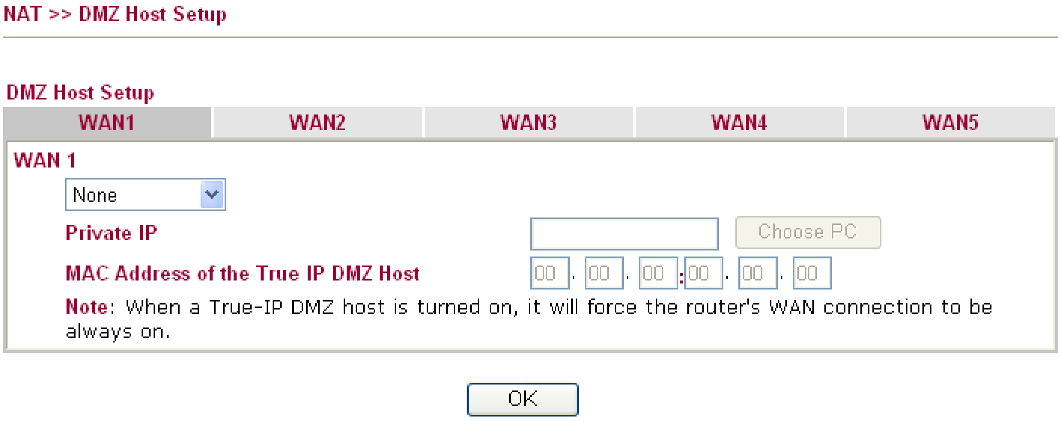
3.3.2 DMZ Host

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



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

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



NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

None

Private IP [ ] Choose PC

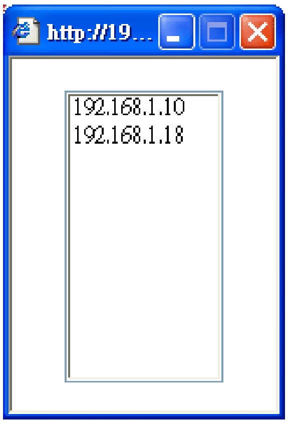
MAC Address of the True IP DMZ Host 00 . 00 . 00 : 00 . 00 . 00

Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

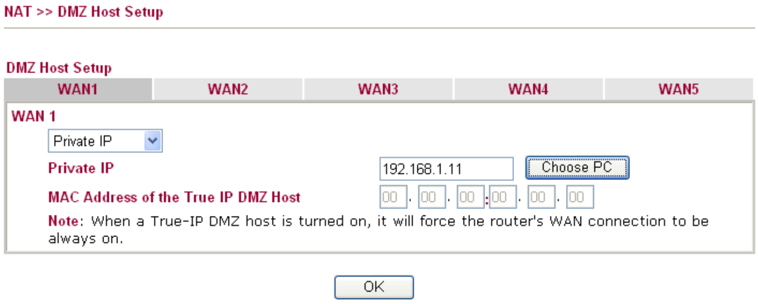
Enable Check to enable the DMZ Host function.

Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

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



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


NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

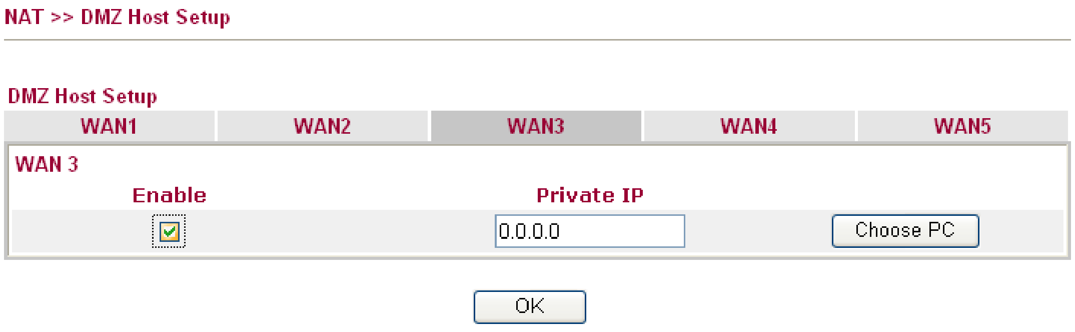
Private IP

Private IP 192.168.1.11 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.

DMZ Host for WAN2 ~ WAN5 are slightly different with WAN1. See the following figure.



NAT >> DMZ Host Setup

DMZ Host Setup

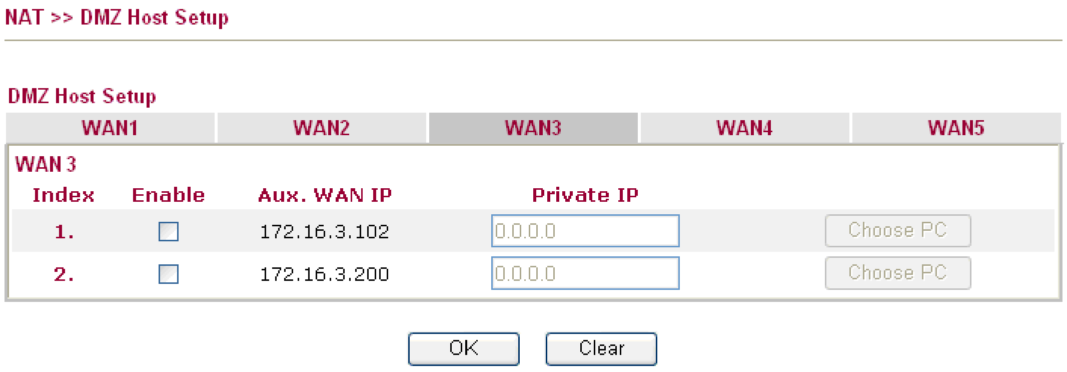
WAN1 | WAN2 | WAN3 | WAN4 | WAN5

WAN 3

Enable	Private IP	
☑	0.0.0.0	Choose PC

OK

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2/WAN3/WAN4/WAN5 interface**,** you will find them in **Aux. WAN IP** for your selection.



NAT >> DMZ Host Setup

DMZ Host Setup

WAN1 | WAN2 | WAN3 | WAN4 | WAN5

WAN 3

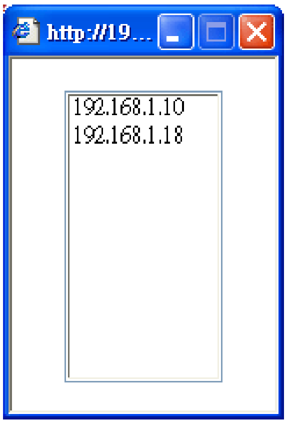
Index	Enable	Aux. WAN IP	Private IP	
1.	□	172.16.3.102	0.0.0.0	Choose PC
2.	□	172.16.3.200	0.0.0.0	Choose PC

OK | Clear

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

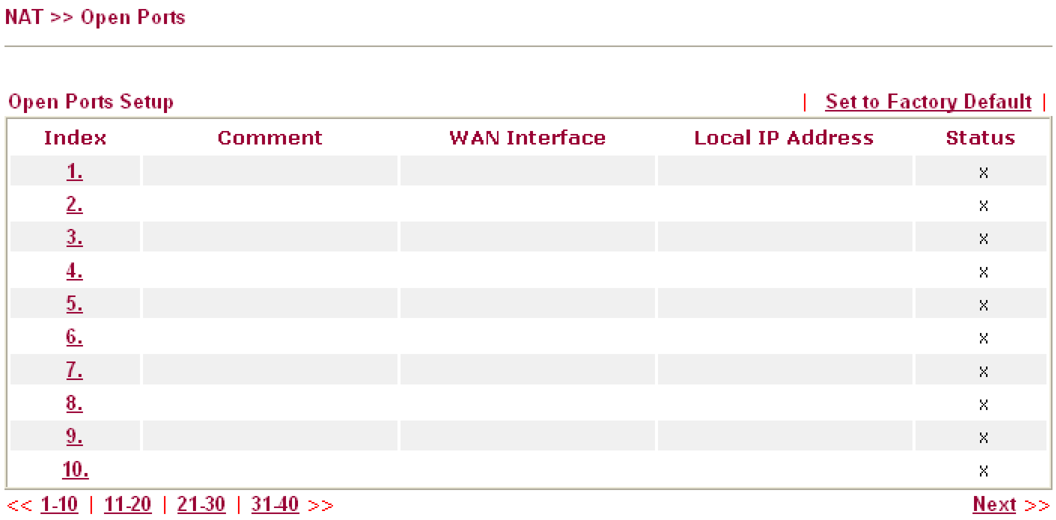
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.

3.3.3 Open Ports

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

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

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



NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Comment	WAN Interface	Local IP Address	Status
1.				×
2.				×
3.				×
4.				×
5.				×
6.				×
7.				×
8.				×
9.				×
10.				×

<< 1-10 | 11-20 | 21-30 | 31-40 >> Next >>

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.

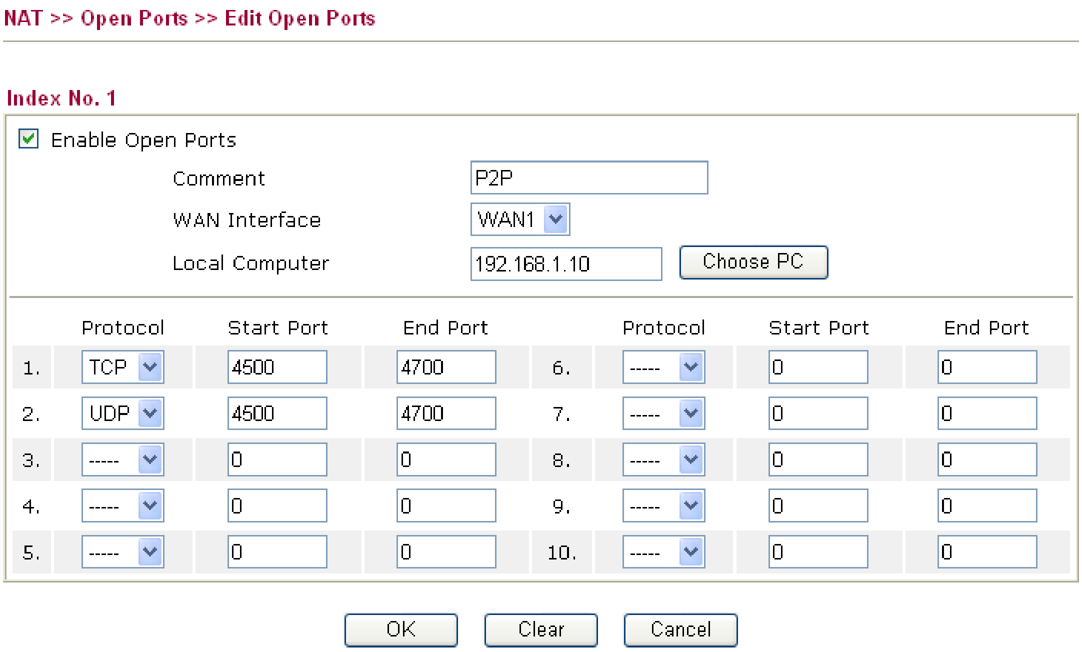
WAN Interface Display the WAN interface for such NAT profile.

Aux. WAN IP Display the WAN IP address specified in WAN IP Alias page. It will be hidden if WAN IP Alias page is not configured.

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	P2P
WAN Interface	WAN1
Local Computer	192.168.1.10 [Choose PC]

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	4500	4700	6.	-----	0	0
2.	UDP	4500	4700	7.	-----	0	0
3.	-----	0	0	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

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.

Local Computer 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.

3.4 Applications

Below shows the menu items for Applications.

3.4.1 Dynamic DNS

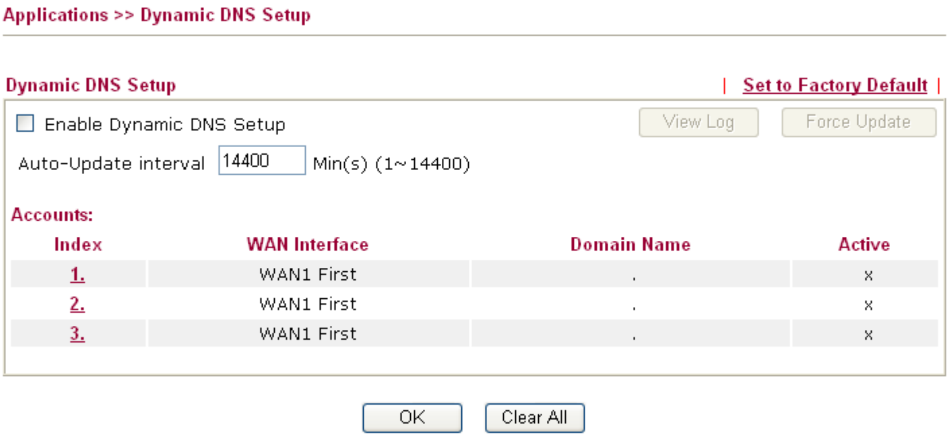
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router 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**.



Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

□ Enable Dynamic DNS Setup

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

Accounts:

Index	WAN Interface	Domain Name	Active
1.	WAN1 First	.	x
2.	WAN1 First	.	x
3.	WAN1 First	.	x

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

Set to Factory Default Clear all profiles and recover to factory settings.

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).

WAN Interface Display the WAN interface used.

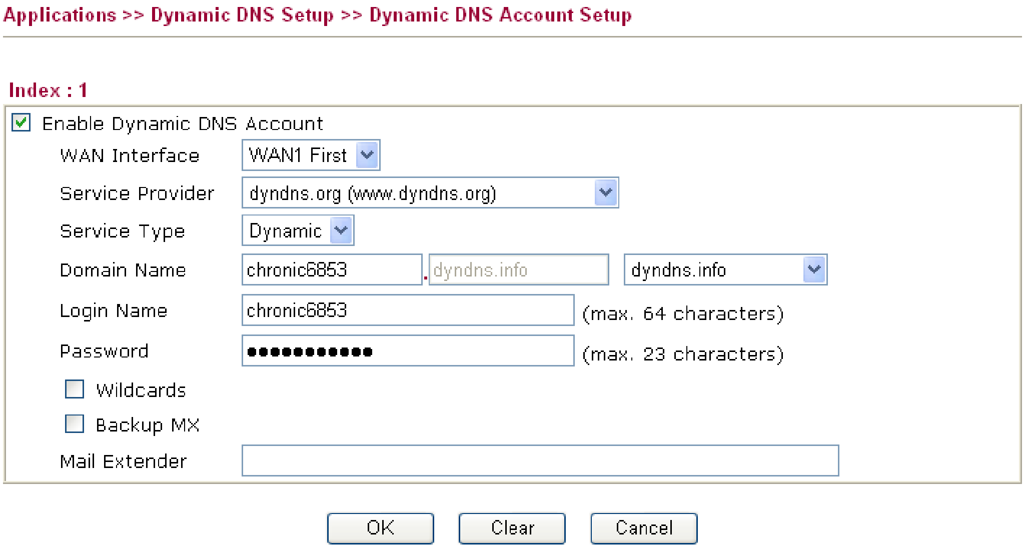
Domain Name Display the domain name that you set on the setting page of DDNS setup.

Active Display if this account is active or inactive.

View Log Display DDNS log status.

Force Update Force the router updates its information to DDNS server.

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

WAN Interface	WAN1 First
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic
Domain Name	chronic6853 . dyndns.info dyndns.info
Login Name	chronic6853 (max. 64 characters)
Password	●●●●●●●●●●● (max. 23 characters)
☐ Wildcards	
☐ Backup MX	
Mail Extender	

Enable Dynamic DNS Account Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).

WAN Interface **WAN1/WAN2/WAN3/WAN4/WAN5 First -** While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead.
WAN1/WAN2/WAN3/WAN4/WAN5 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the only channel for such account.

Service Provider Select the service provider for the DDNS account.

Service Type Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.

Domain Name Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.

Login Name Type in the login name that you set for applying domain.

Password Type in the password that you set for applying domain.

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

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

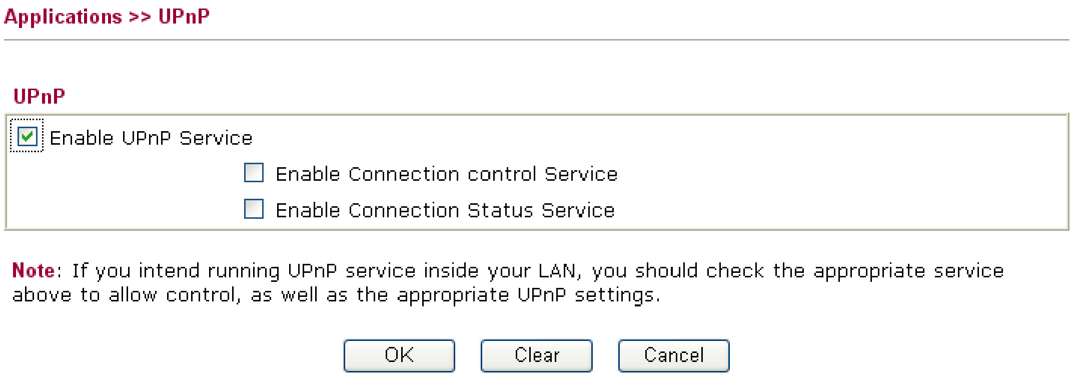
In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

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.

3.4.2 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. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.



Applications >> UPnP

UPnP

☑ Enable UPnP Service

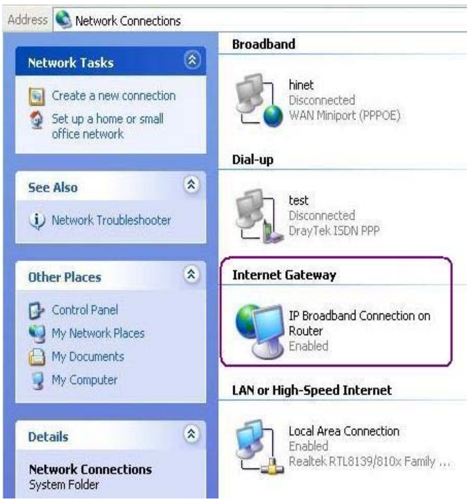
□ Enable Connection control Service

□ Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

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

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



Address: Network Connections

Network Tasks
- Create a new connection
- Set up a home or small office network

See Also
- Network Troubleshooter

Other Places
- Control Panel
- My Network Places
- My Documents
- My Computer

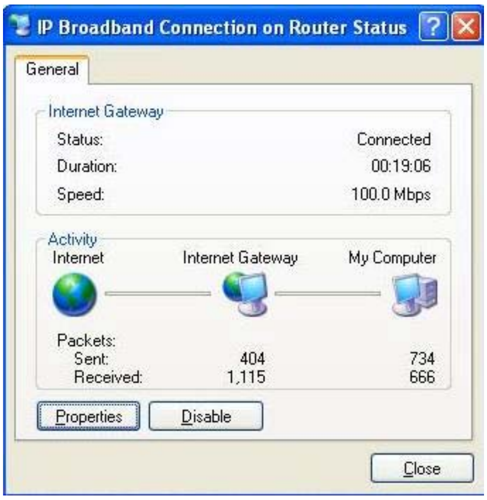
Details
Network Connections
System Folder

Broadband
hinet
Disconnected
WAN Miniport (PPPOE)

Dial-up
test
Disconnected
DrayTek ISDN PPP

Internet Gateway
IP Broadband Connection on Router
Enabled

LAN or High-Speed Internet
Local Area Connection
Enabled
Realtek RTL8139/810x Family ...



IP Broadband Connection on Router Status

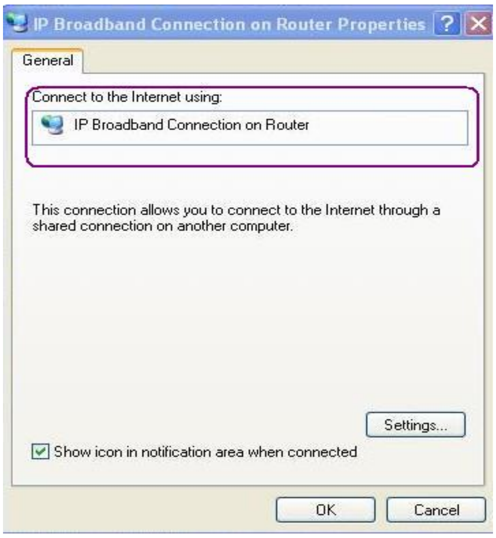
General

Internet Gateway
Status: Connected
Duration: 00:19:06
Speed: 100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		404	734
Received:		1,115	666

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.



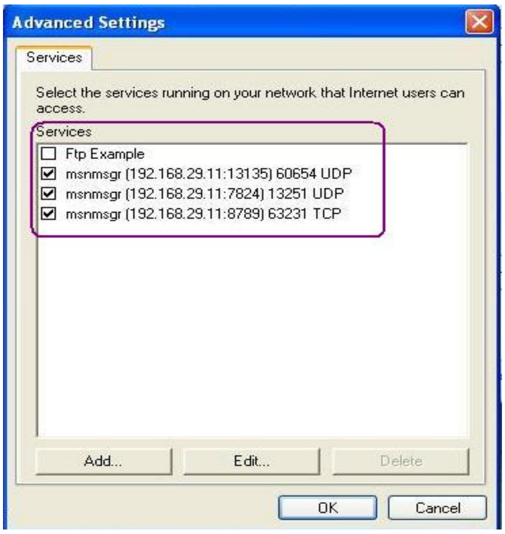
IP Broadband Connection on Router Properties

General

Connect to the Internet using:
IP Broadband Connection on Router

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected



Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services
- ☐ Ftp Example
- ☑ msnmsgr (192.168.29.11:13135) 60654 UDP
- ☑ msnmsgr (192.168.29.11:7824) 13251 UDP
- ☑ msnmsgr (192.168.29.11:8789) 63231 TCP

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.

3.5 Wireless LAN

This function is used for “n” models.

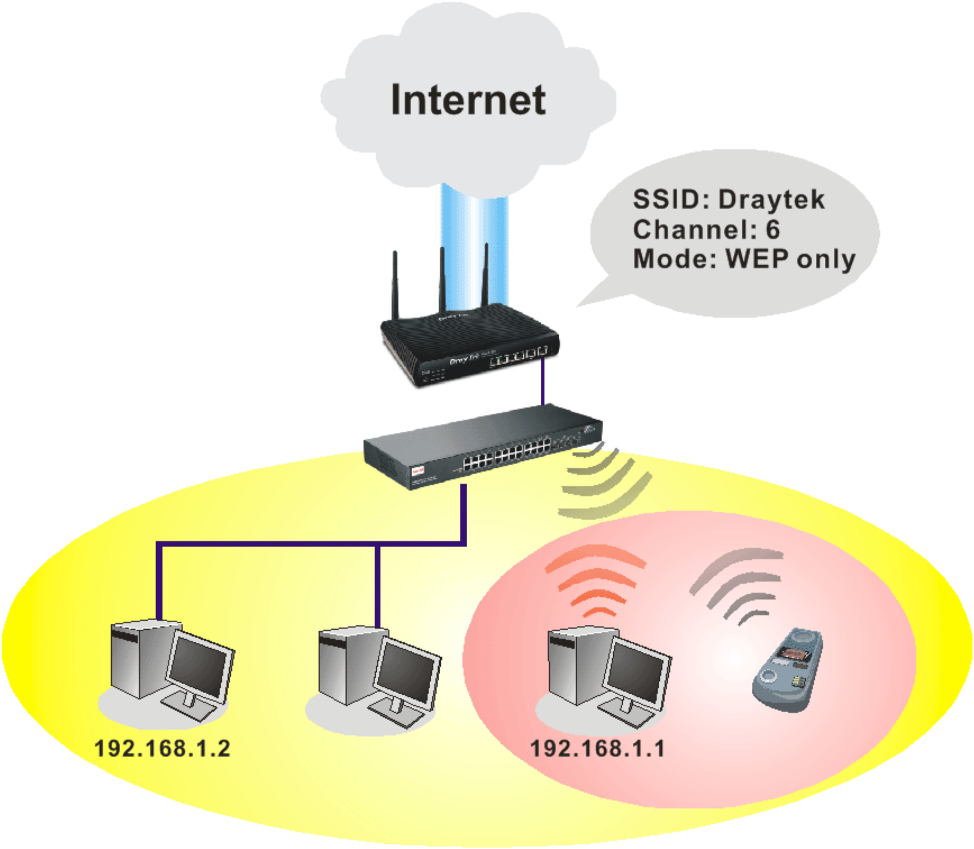
3.5.1 Basic Concepts

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.



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/802.1x.

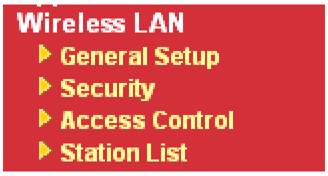
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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.

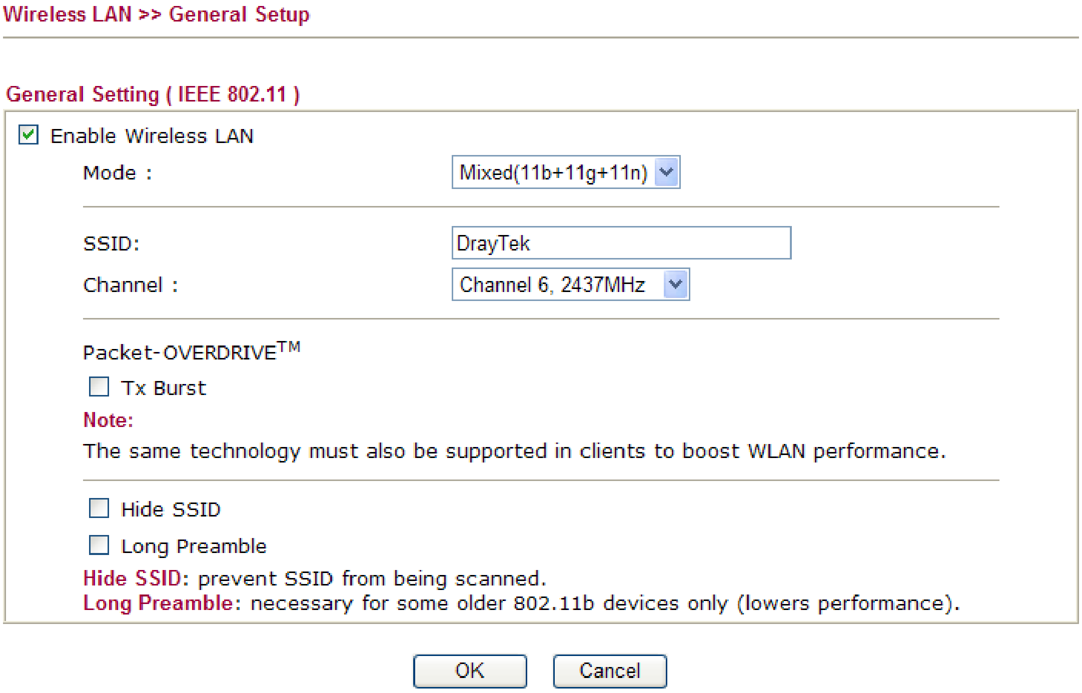
Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.



3.5.2 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.



Wireless LAN >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

Mode : Mixed(11b+11g+11n)

SSID: DrayTek

Channel : Channel 6, 2437MHz

Packet-OVERDRIVE™

□ Tx Burst

Note:
The same technology must also be supported in clients to boost WLAN performance.

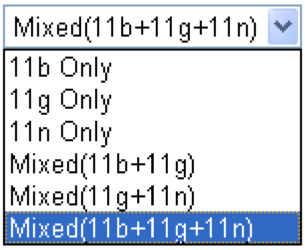
□ Hide SSID

□ Long Preamble

Hide SSID: prevent SSID from being scanned.
Long Preamble: necessary for some older 802.11b devices only (lowers performance).

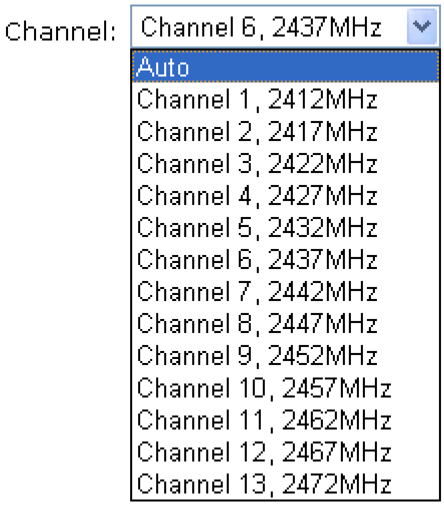
Enable Wireless LAN Check the box to enable wireless function.

Mode At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.



SSID Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.

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.

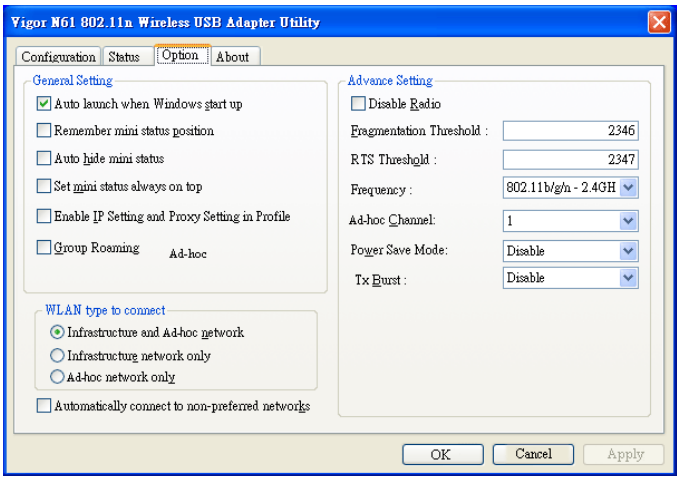


Channel: Channel 6, 2437MHz

Packet-OVERDRIVE

This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). 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**).



Vigor N61 802.11n Wireless USB Adapter Utility

General Setting

☑ Auto launch when Windows start up
□ Remember mini status position
□ Auto hide mini status
□ Set mini status always on top
□ Enable IP Setting and Proxy Setting in Profile
□ Group Roaming Ad-hoc

WLAN type to connect

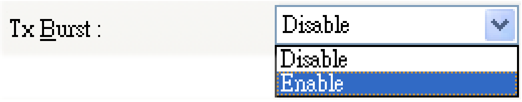
● Infrastructure and Ad-hoc network
○ Infrastructure network only
○ Ad-hoc network only

□ Automatically connect to non-preferred networks

Advance Setting

□ Disable Radio

Fragmentation Threshold : 2346
RTS Threshold : 2347
Frequency : 802.11b/g/n - 2.4GH
Ad-hoc Channel: 1
Power Save Mode: Disable
Tx Burst : Disable



Tx Burst : Disable

Hide SSID

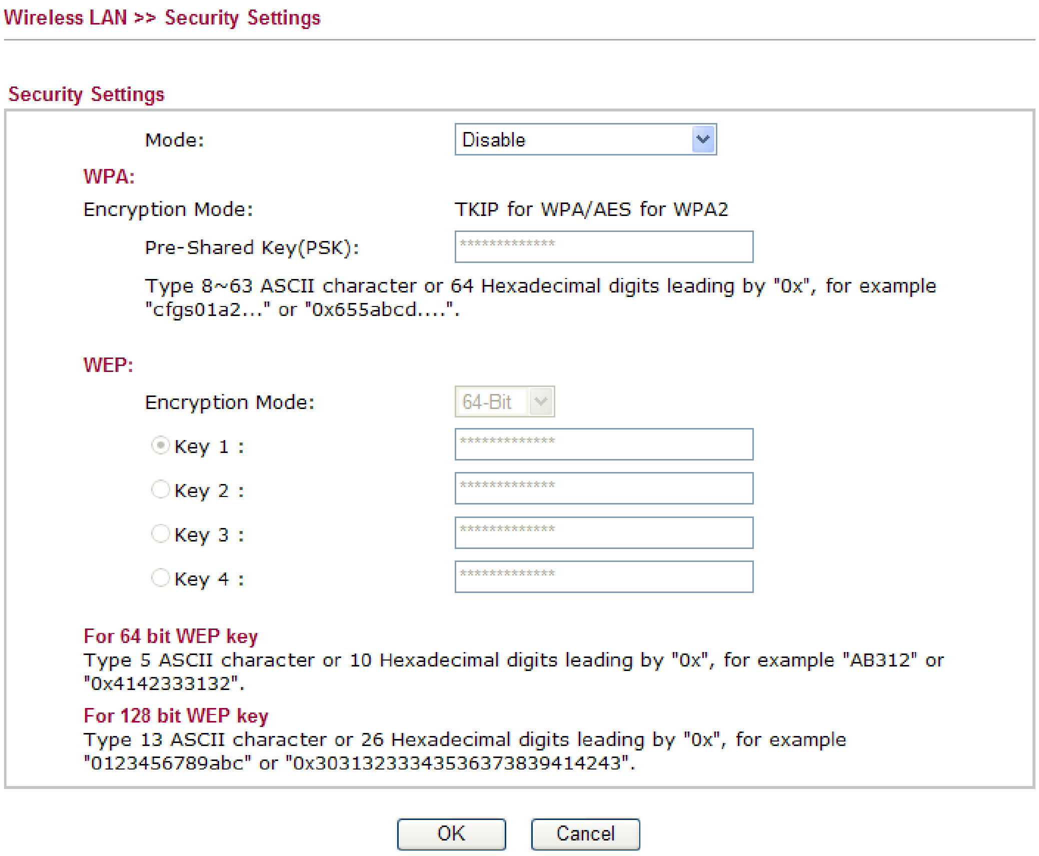
Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows 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.

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. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

3.5.3 Security

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.

Default Pre-Shared Key (PSK) 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.


Wireless LAN >> Security Settings

Security Settings

Mode: Disable

WPA:

Encryption Mode: TKIP for WPA/AES for WPA2

Pre-Shared Key(PSK): *************

Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

WEP:

Encryption Mode: 64-Bit

● Key 1 : *************

○ Key 2 : *************

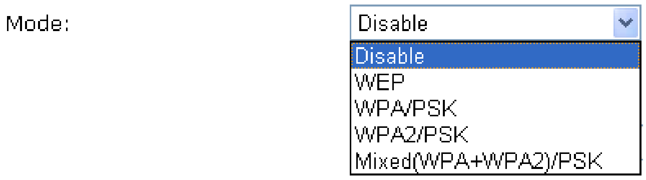
○ Key 3 : *************

○ Key 4 : *************

For 64 bit WEP key
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".

For 128 bit WEP key
Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".

Mode There are several modes provided for you to choose.


Mode: Disable

Disable - Turn off the encryption mechanism.
WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.

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 802.1x 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.

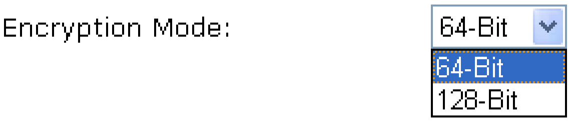
Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

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).

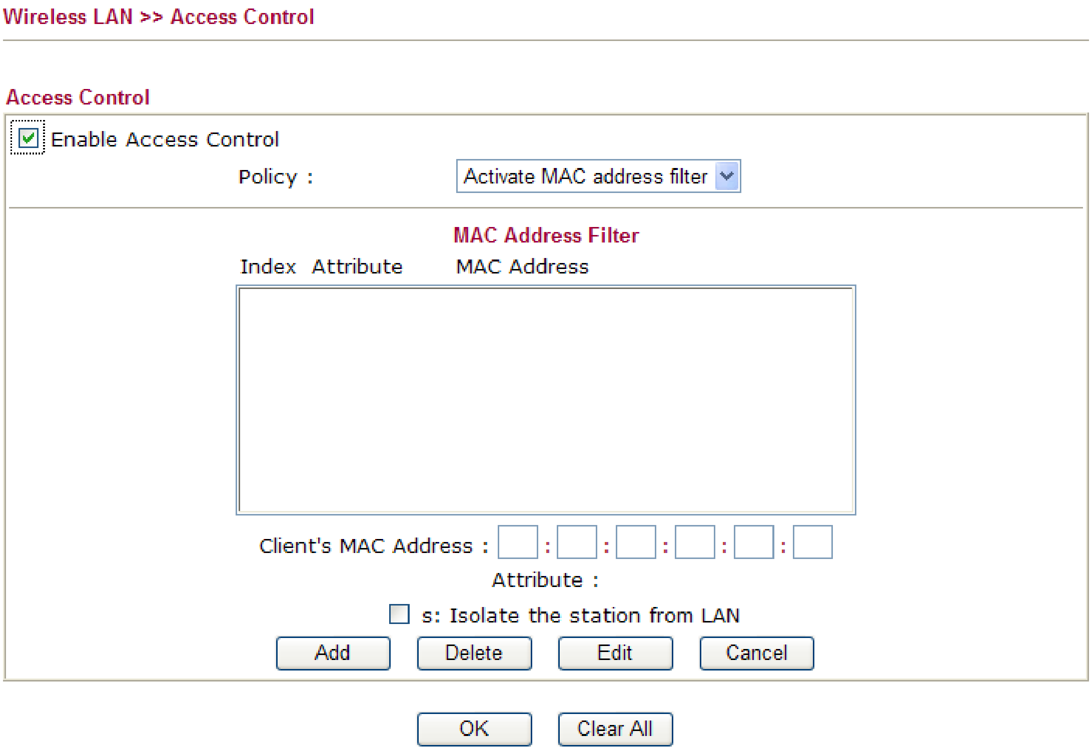
All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.



Encryption Mode: 64-Bit

3.5.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.



Wireless LAN >> Access Control

Access Control

☑ Enable Access Control

Policy : Activate MAC address filter

MAC Address Filter

Index Attribute MAC Address

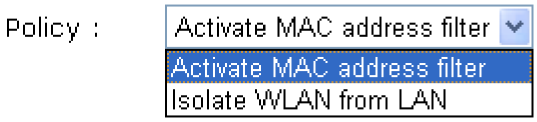
Client's MAC Address : __ : __ : __ : __ : __ : __

Attribute :

□ s: Isolate the station from LAN

Enable Access Control Select to enable the MAC Address access control feature.

Policy Select to enable any one of the following policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Isolate WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.



Policy : Activate MAC address filter

MAC Address Filter Display all MAC addresses that are edited before.

Client's MAC Address Manually enter the MAC address of wireless client.

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.

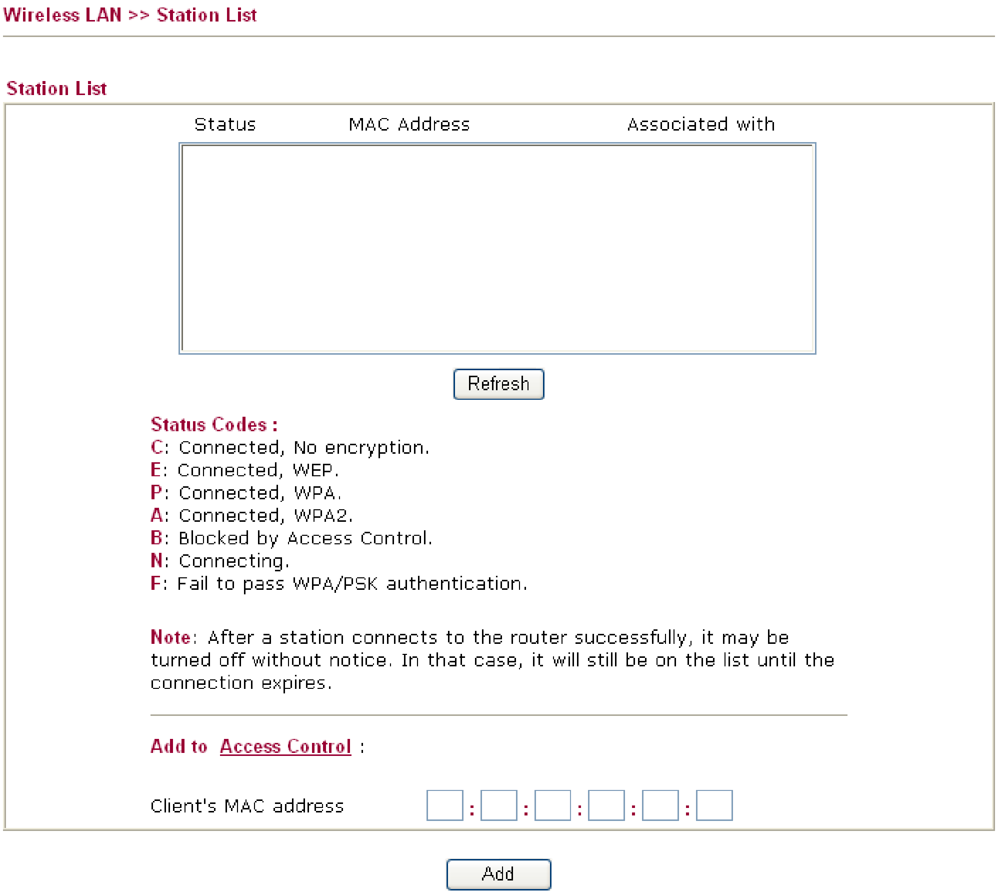
Delete Delete the selected MAC address in the list.

Edit Edit the selected MAC address in the list.

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.

3.5.5 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.



Wireless LAN >> Station List

Station List

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 :

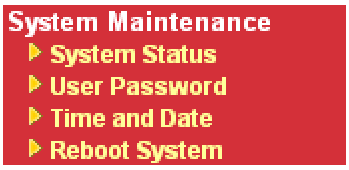
Client's MAC address □ : □ : □ : □ : □ : □

Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into **Access Control**.

3.6 System Maintenance

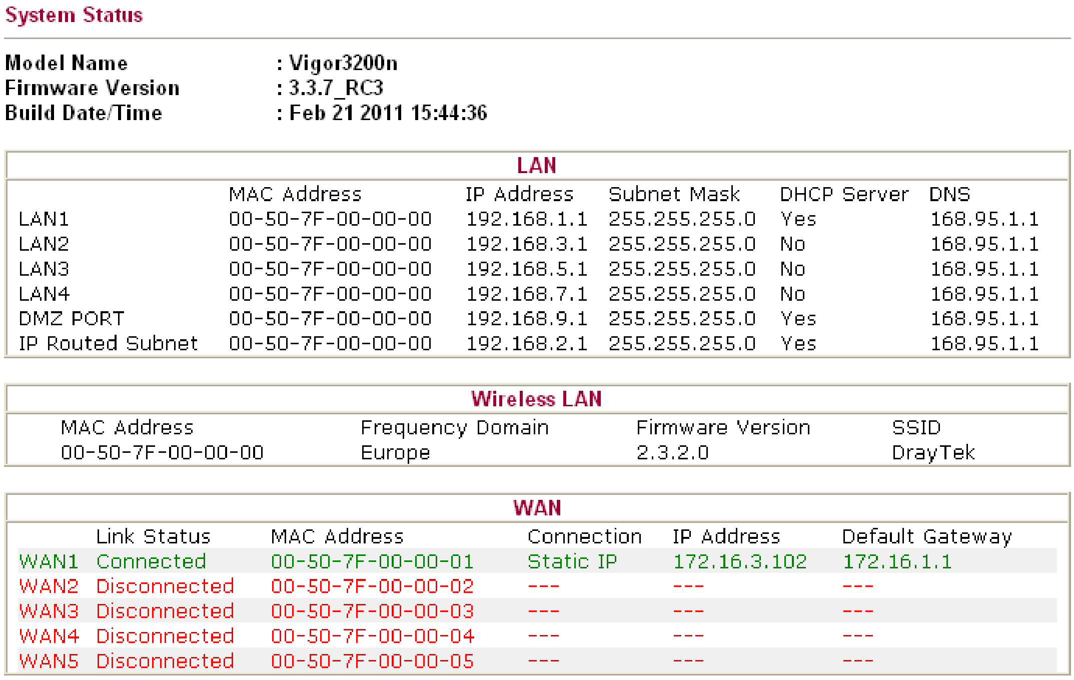
For the system setup, there are several items that you have to know the way of configuration: Status, User Password, Time setup and Reboot System.

Below shows the menu items for System Maintenance.



3.6.1 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 : Vigor3200n
Firmware Version : 3.3.7_RC3
Build Date/Time : Feb 21 2011 15:44:36

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-00-00-00	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-00-00-00	192.168.3.1	255.255.255.0	No	168.95.1.1
LAN3	00-50-7F-00-00-00	192.168.5.1	255.255.255.0	No	168.95.1.1
LAN4	00-50-7F-00-00-00	192.168.7.1	255.255.255.0	No	168.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.2.1	255.255.255.0	Yes	168.95.1.1

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-00-00-00	Europe	2.3.2.0	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-00-00-01	Static IP	172.16.3.102	172.16.1.1
WAN2	Disconnected	00-50-7F-00-00-02	---	---	---
WAN3	Disconnected	00-50-7F-00-00-03	---	---	---
WAN4	Disconnected	00-50-7F-00-00-04	---	---	---
WAN5	Disconnected	00-50-7F-00-00-05	---	---	---

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 built.

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.

Wireless LAN-------

MAC Address Display the MAC address of the wireless LAN.

Frequency Domain It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.

Firmware Version It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.

SSID Display the SSID of the router.

WAN-------

Link Status Display current connection status.

MAC Address Display the MAC address of the WAN Interface.

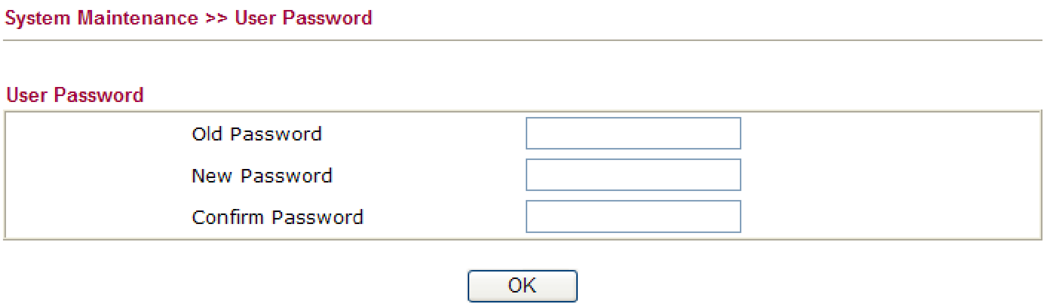
Connection Display the connection type.

IP Address Display the IP address of the WAN interface.

Default Gateway Display the assigned IP address of the default gateway.

3.6.2 User Password

This page allows you to set new password for user operation.



System Maintenance >> User Password

User Password

Old Password	
New Password	
Confirm Password	

Old Password Type in the old password. The factory default setting for password is blank.

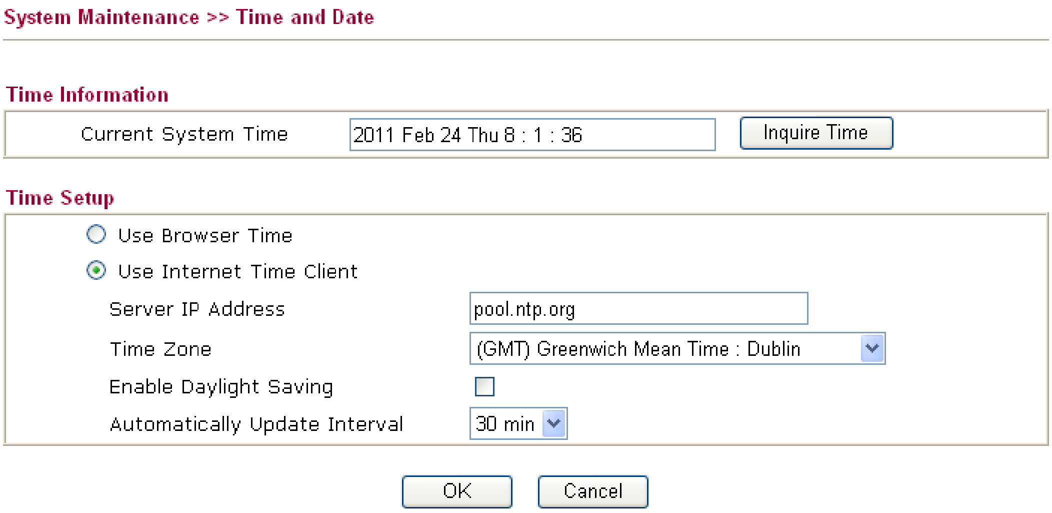
New Password Type in new password in this field.

Confirm Password Type in the new password again.

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

3.6.3 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: 2011 Feb 24 Thu 8 : 1 : 36 [Inquire Time]

Time Setup

○ Use Browser Time

● Use Internet Time Client

Server IP Address: pool.ntp.org

Time Zone: (GMT) Greenwich Mean Time : Dublin

Enable Daylight Saving: □

Automatically Update Interval: 30 min

[OK] [Cancel]

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 Protocol Select a time protocol.

Server IP Address Type the IP address of the time server.

Time Zone Select the time zone where the router is located.

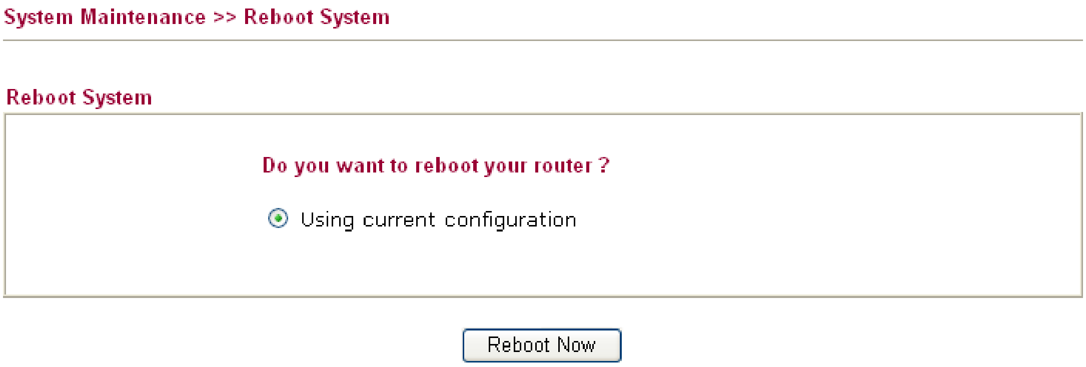
Enable Daylight Saving Check the box to activate daylight saving function. Such feature is useful for some areas.

Automatically Update Interval Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.6.4 Reboot System

The Web Configurator may be used to restart your router for using current configuration. 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

[Reboot Now]

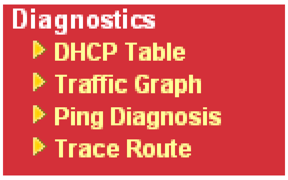
Click **OK**. The router will take 5 seconds to reboot the system.

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

3.7 Diagnostics

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

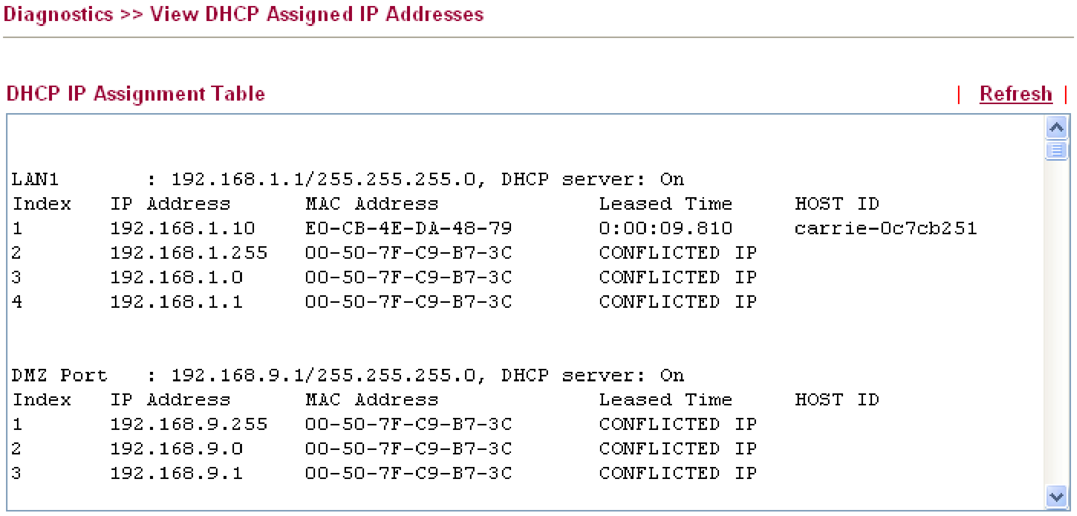
Below shows the menu items for Diagnostics.



3.7.1 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.

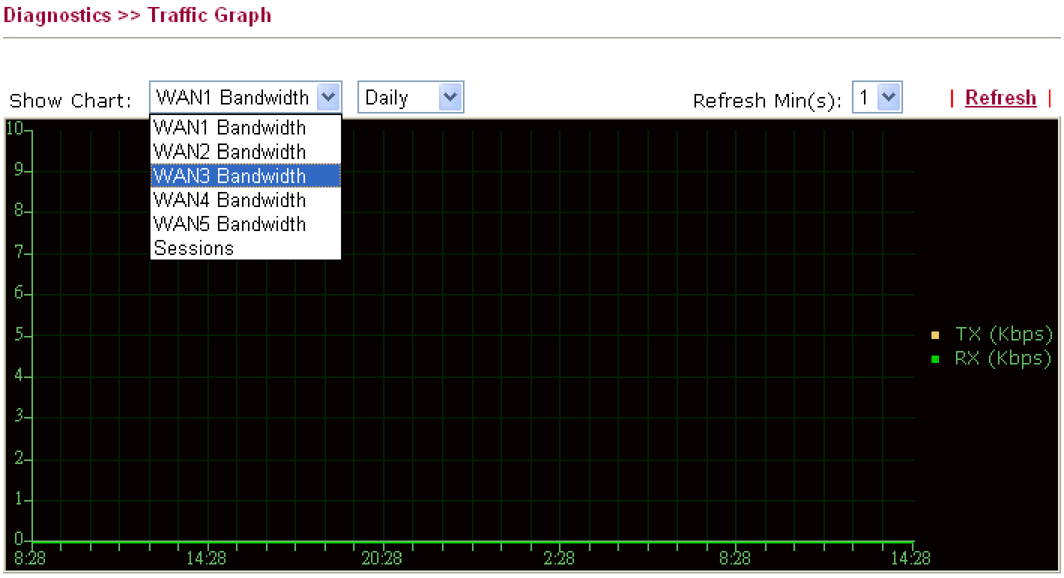


```
LAN1       : 192.168.1.1/255.255.255.0, DHCP server: On
Index   IP Address      MAC Address             Leased Time     HOST ID
1       192.168.1.10    E0-CB-4E-DA-48-79       0:00:09.810     carrie-0c7cb251
2       192.168.1.255   00-50-7F-C9-B7-3C       CONFLICTED IP
3       192.168.1.0     00-50-7F-C9-B7-3C       CONFLICTED IP
4       192.168.1.1     00-50-7F-C9-B7-3C       CONFLICTED IP


DMZ Port   : 192.168.9.1/255.255.255.0, DHCP server: On
Index   IP Address      MAC Address             Leased Time     HOST ID
1       192.168.9.255   00-50-7F-C9-B7-3C       CONFLICTED IP
2       192.168.9.0     00-50-7F-C9-B7-3C       CONFLICTED IP
3       192.168.9.1     00-50-7F-C9-B7-3C       CONFLICTED IP
```

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.

3.7.2 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WAN3/WAN4/WAN5 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time. The following two figures display different charts by daily and weekly.


Diagnostics >> Traffic Graph

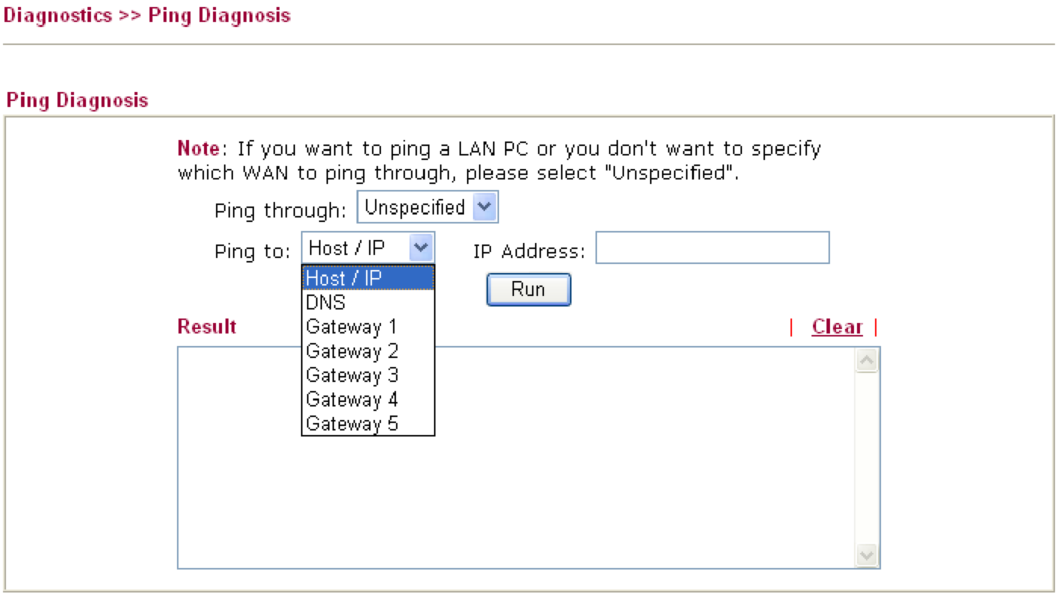
Show Chart: WAN1 Bandwidth | Daily | Refresh Min(s): 1 | Refresh |

The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/WAN4/WAN5 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.

3.7.3 Ping Diagnosis

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


Diagnostics >> Ping Diagnosis

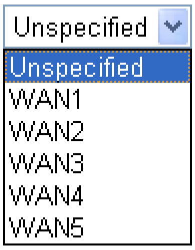
Ping Diagnosis

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

Ping through: Unspecified

Ping to: Host / IP   IP Address:

Ping through Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.



Ping to Use the drop down list to choose the destination that you want to ping.

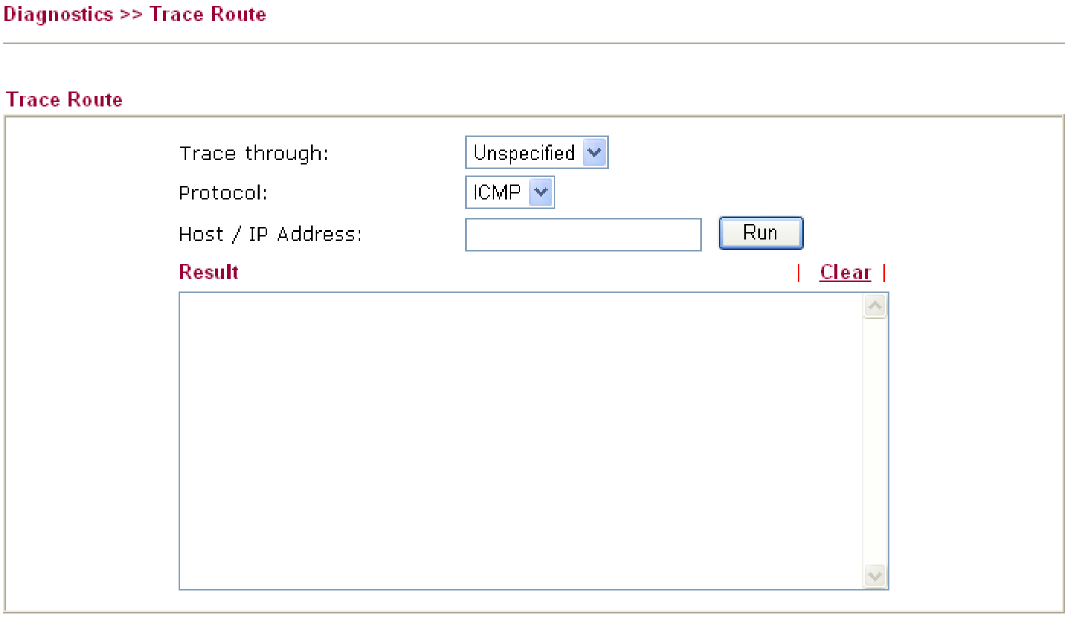
IP Address Type in the IP address of the Host/IP that you want to ping.

Run Click this button to start the ping work. The result will be displayed on the screen.

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

3.7.4 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

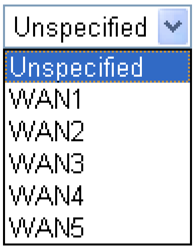
Trace Route

Trace through: Unspecified

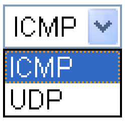
Protocol: ICMP

Host / IP Address:

Trace through Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.



Protocol Choose the protocol for using trace route.



ICMP
ICMP
UDP

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

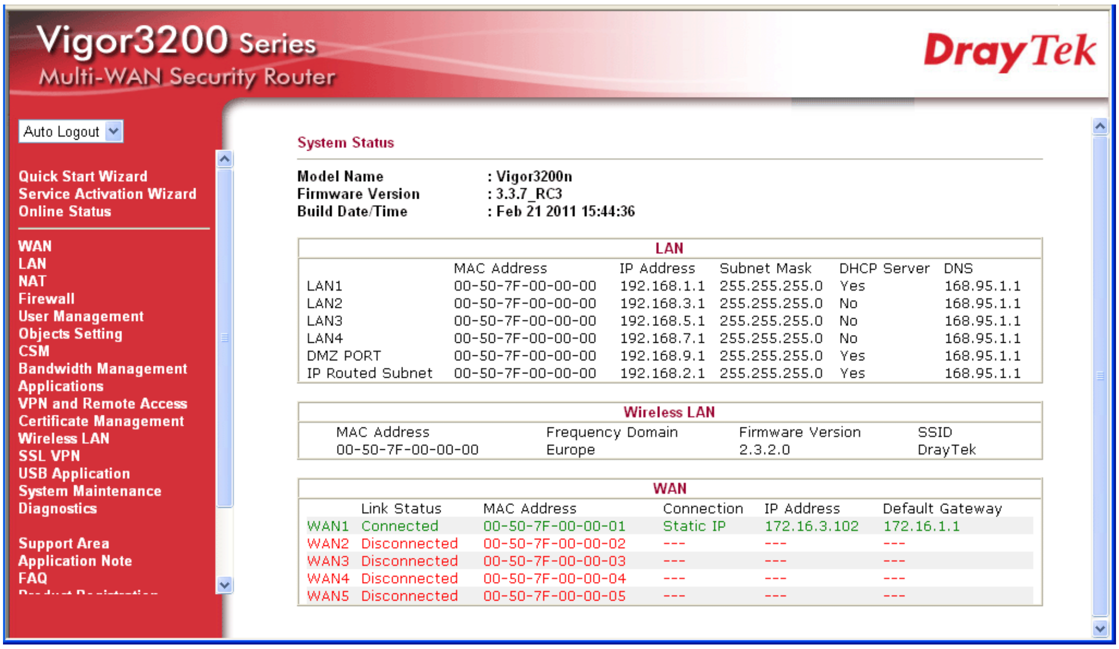
.

4 Admin Mode Operation

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

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

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



System Status

Model Name : Vigor3200n
Firmware Version : 3.3.7_RC3
Build Date/Time : Feb 21 2011 15:44:36

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-00-00-00	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-00-00-00	192.168.3.1	255.255.255.0	No	168.95.1.1
LAN3	00-50-7F-00-00-00	192.168.5.1	255.255.255.0	No	168.95.1.1
LAN4	00-50-7F-00-00-00	192.168.7.1	255.255.255.0	No	168.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.2.1	255.255.255.0	Yes	168.95.1.1

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-00-00-00	Europe	2.3.2.0	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-00-00-01	Static IP	172.16.3.102	172.16.1.1
WAN2	Disconnected	00-50-7F-00-00-02	---	---	---
WAN3	Disconnected	00-50-7F-00-00-03	---	---	---
WAN4	Disconnected	00-50-7F-00-00-04	---	---	---
WAN5	Disconnected	00-50-7F-00-00-05	---	---	---

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, Vigor3200 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor3200, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor3200n 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 the LAN port on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor3200n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor3200n series.

Mobile Coffee shop
Internet
Web surfing, E-Mail, Instant messaging etc.
VPN
3.5G HSDPA USB Modem

After connecting into the router, 3G USB Modem will be regarded as the fifth WAN port. However, the other Ethernet WAN ports still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem also can be used as backup device. Therefore, when other Ethernet WAN ports 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.

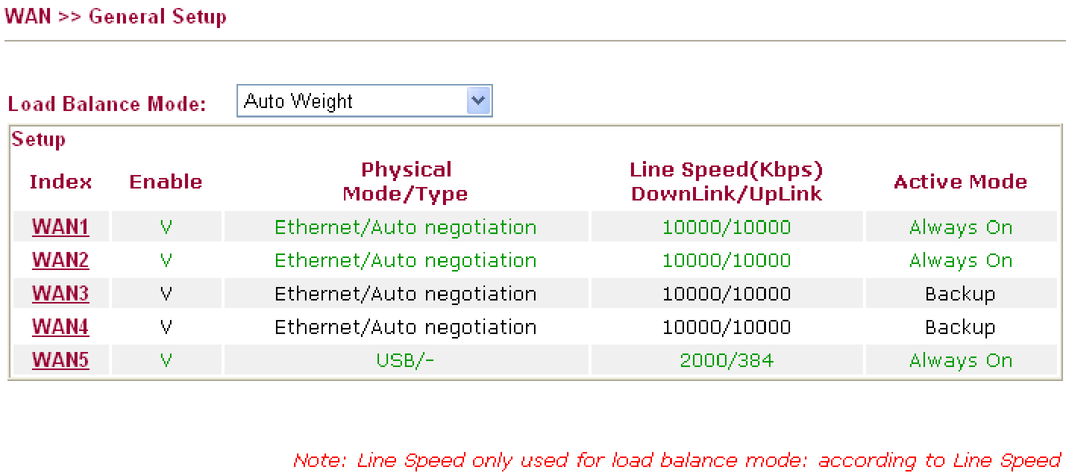
Below shows the menu items for **WAN**.

4.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 to WAN5 in details.

There are four WAN ports (represented with WAN1, WAN2, WAN3 and WAN4 in web pages) and one USB port (represented with WAN5 in web pages) offered by the router. For this router supports multiple WANs 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.

This webpage allows you to set general setup for WAN1 to WAN5 respectively.


WAN >> General Setup

Load Balance Mode: Auto Weight

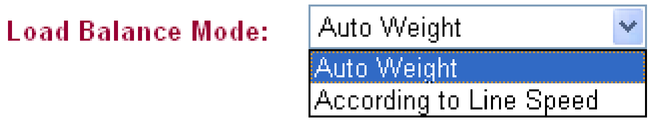
Setup

Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	V	Ethernet/Auto negotiation	10000/10000	Always On
WAN2	V	Ethernet/Auto negotiation	10000/10000	Always On
WAN3	V	Ethernet/Auto negotiation	10000/10000	Backup
WAN4	V	Ethernet/Auto negotiation	10000/10000	Backup
WAN5	V	USB/-	2000/384	Always On

Note: Line Speed only used for load balance mode: according to Line Speed

From the above figure, WAN1 ~ WAN4 connect to Internet through the interface of Ethernet; WAN5 connects to Internet via USB interface. Therefore the configuration for each WAN port will be different slightly. Please click the WAN link under Index to open the web page for detailed configuration.

Load Balance Mode This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Weigh** to let the router reach the best load balance.


Load Balance Mode: Auto Weight

Index Click the WAN interface link under Index to access into the WAN configuration page.

Enable **V** means such WAN interface is enabled and ready to be used.

Physical Mode / Type Display the physical mode and physical type of such WAN interface.

Line Speed Display the downstream and upstream rate of such WAN interface.

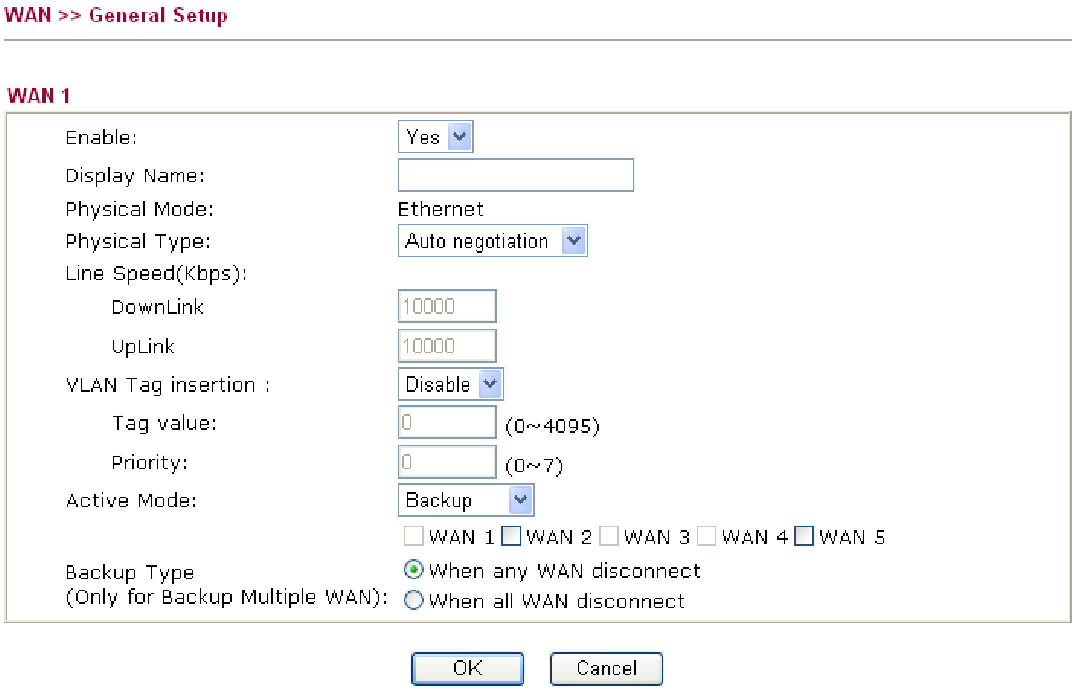
Active Mode Display whether such WAN interface is Active device or backup device.

Backup WAN Display the Backup WAN interface for such WAN when it is disabled.

Note: In default, each WAN is enabled.

For WAN1 ~ WAN4 (Ethernet)

WAN1 ~ WAN4 are fixed with physical mode of Giga Ethernet. Here we take WAN1 as an example.



WAN >> General Setup

WAN 1

Enable: Yes

Display Name:

Physical Mode: Ethernet

Physical Type: Auto negotiation

Line Speed(Kbps):

DownLink 10000

UpLink 10000

VLAN Tag insertion : Disable

Tag value: 0 (0~4095)

Priority: 0 (0~7)

Active Mode: Backup

□ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5

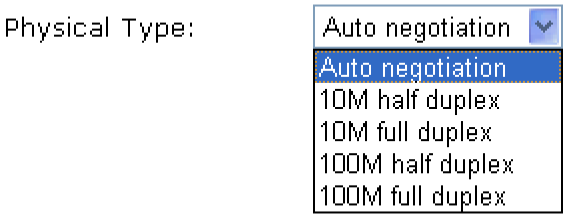
Backup Type (Only for Backup Multiple WAN): ● When any WAN disconnect ○ When all WAN disconnect

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.



Physical Type: Auto negotiation

Line Speed If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading for such

WAN interface. The unit is kbps. The default setting for down link and up link is 10000Kbps.

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.

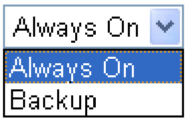
Disable – Disable the function of VLAN with tag.

Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.

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

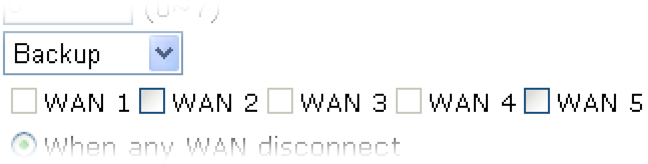
Active Mode

Determine the WAN interface will be active for always (**Always On**) or be treated as a backup WAN interface (**Backup**).



Backup Type

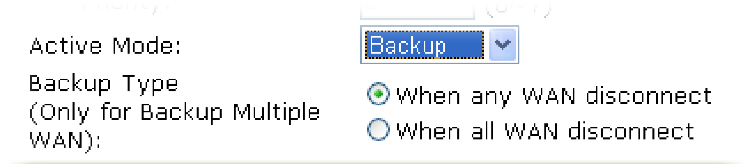
If you choose **Always On** as **Active Mode**, you can choose from the available WAN interfaces as a backup WAN. Later, when current WAN is disconnected for some reason, the backup WAN will be activated automatically to prevent data transmission from connection interrupted.



□ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5

● When any WAN disconnect

If you choose **Backup** as the **Active Mode**, The option of **Backup Type** will be displayed. You have to specify which role the WAN interface should play.



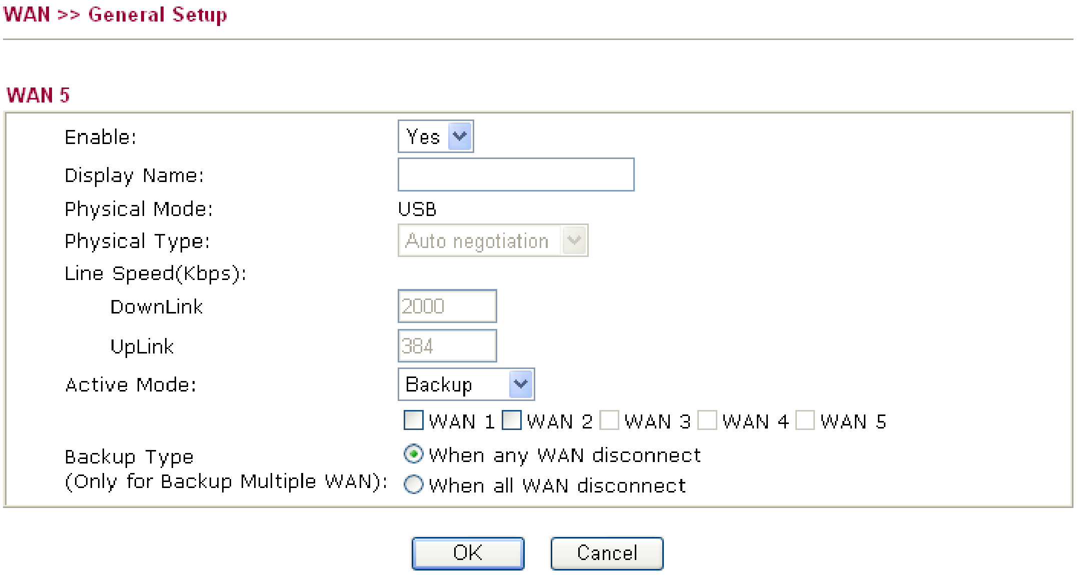
Active Mode:	Backup
Backup Type (Only for Backup Multiple WAN):	● When any WAN disconnect ○ When all WAN disconnect

When any WAN disconnect – WAN1 will be activated when any WAN interface disconnects.

When all WAN disconnect – WAN1 will be activated when all the WAN interfaces disconnect.

For WAN5 (USB)

To use 3G network connection through 3G USB Modem, please configure **WAN5** interface.



WAN >> General Setup

WAN 5

Enable:	Yes
Display Name:	
Physical Mode:	USB
Physical Type:	Auto negotiation
Line Speed(Kbps):	
DownLink	2000
UpLink	384
Active Mode:	Backup □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5
Backup Type (Only for Backup Multiple WAN):	● When any WAN disconnect ○ When all WAN disconnect

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

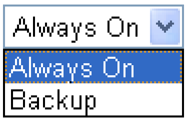
For such WAN interface is fixed to USB network connection, it is not necessary to specify physical type.

Line Speed

If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.

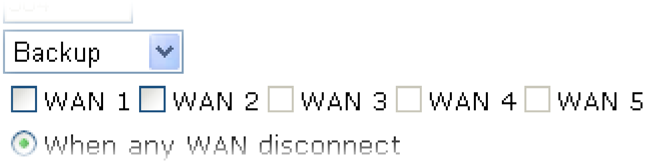
Active Mode

Determine the WAN interface will be active for always (**Always On**) or be treated as a backup WAN interface (**Backup**).



Backup Type

If you choose **Always On** as **Active Mode**, you can choose from the available WAN interfaces as a backup WAN. Later, when current WAN is disconnected for some reason, the backup WAN will be activated automatically to prevent data transmission from connection interrupted.

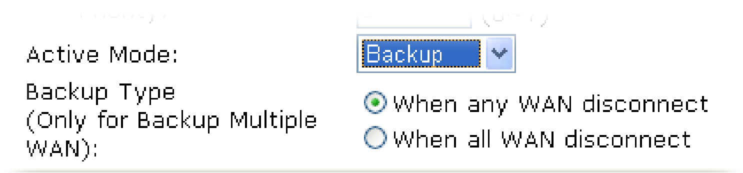


Backup

□ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5

● When any WAN disconnect

If you choose **Backup** as the **Active Mode**, The option of **Backup Type** will be displayed. You have to specify which role the WAN interface should play.



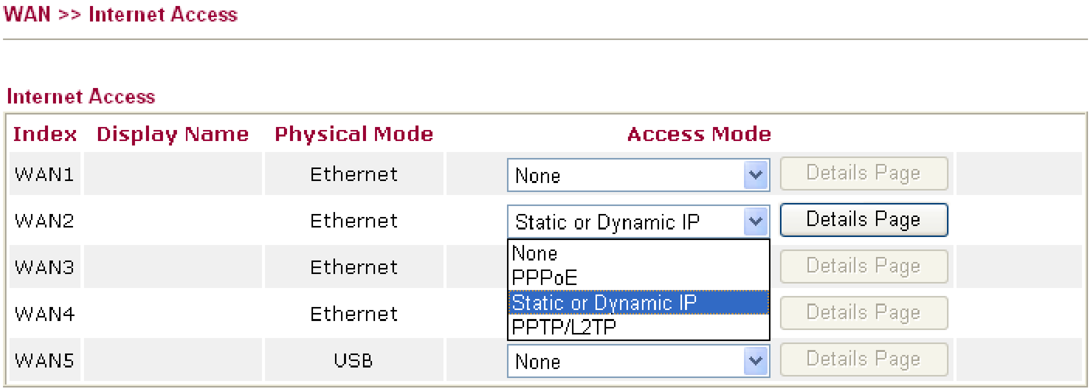
Active Mode:	Backup
Backup Type (Only for Backup Multiple WAN):	● When any WAN disconnect ○ When all WAN disconnect

When any WAN disconnect – WAN1 will be activated when any WAN interface disconnects.

When all WAN disconnect – WAN1 will be activated when all the WAN interfaces disconnect.

4.1.3 Internet Access

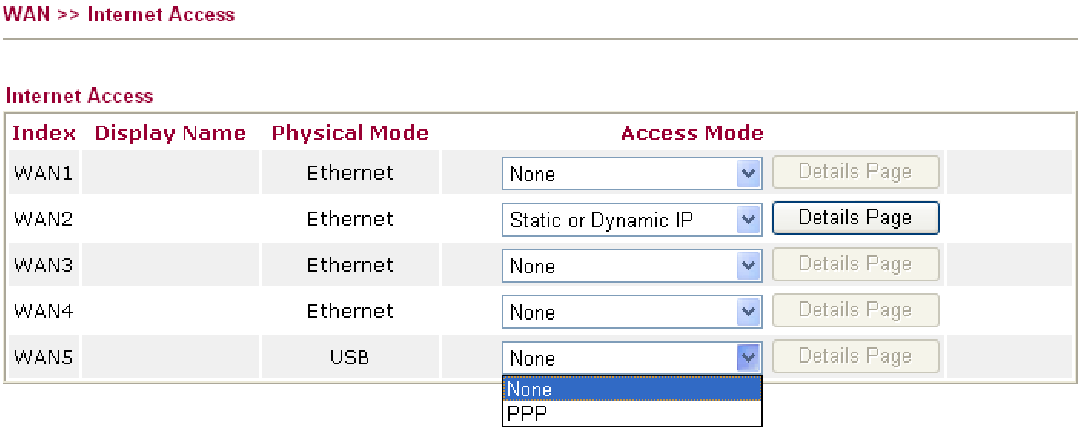
For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3/WAN4/WAN5) for Internet Access. Due to different Physical Mode of WAN interface, the Access Mode for these connections also varies. Refer to the following figures.



WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	None	Details Page
WAN2		Ethernet	Static or Dynamic IP	Details Page
WAN3		Ethernet		Details Page
WAN4		Ethernet		Details Page
WAN5		USB	None	Details Page



WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	None	Details Page
WAN2		Ethernet	Static or Dynamic IP	Details Page
WAN3		Ethernet	None	Details Page
WAN4		Ethernet	None	Details Page
WAN5		USB	None	Details Page

Index Display the WAN interface.

Display Name It shows the name of the WAN1/WAN2/WAN3/WAN4/WAN5 that entered in general setup.

Physical Mode It shows the physical connection for WAN1-WAN4 (Ethernet) /WAN5 (3G USB Modem) according to the real network connection.

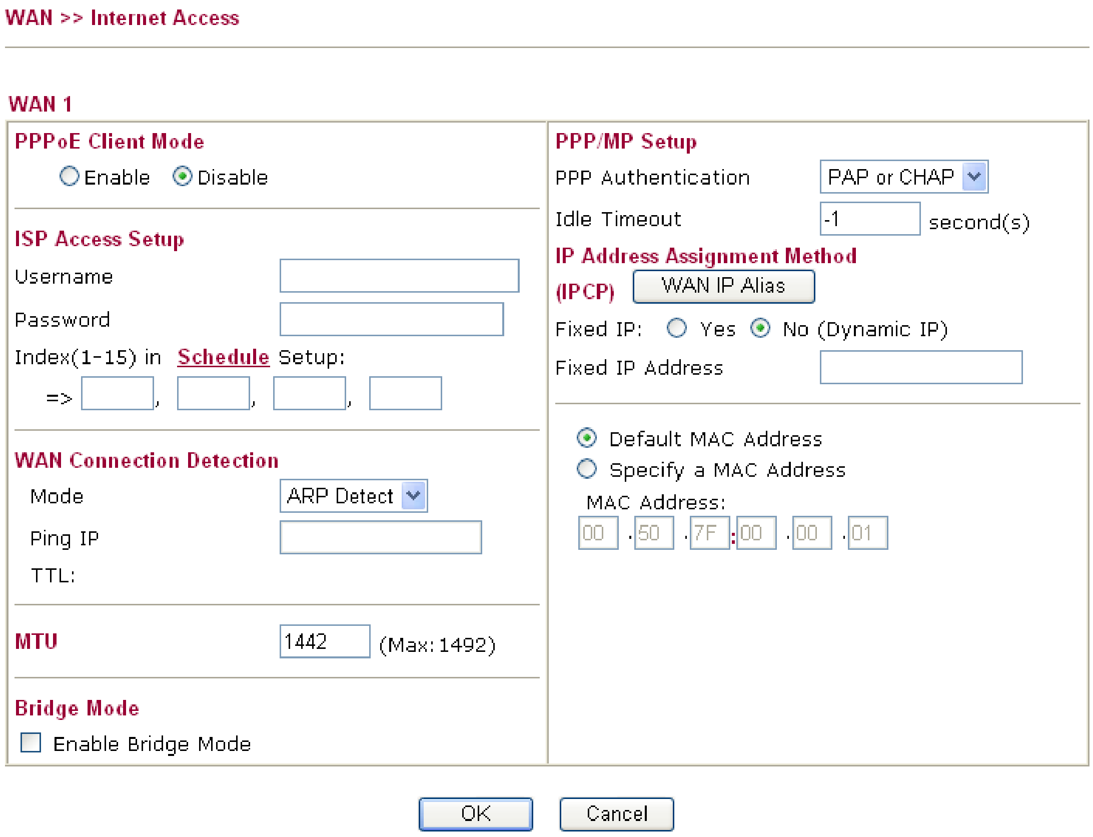
Access Mode Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click

Details Page for accessing the page to configure the settings.

Details Page This button will open different web page according to the access mode that you choose in WAN interface

Details Page for PPPoE in WAN1 ~ WAN4

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



WAN >> Internet Access

WAN 1

PPPoE Client Mode

○ Enable ● Disable

ISP Access Setup

Username

Password

Index(1-15) in Schedule Setup:

=> , , ,

WAN Connection Detection

Mode: ARP Detect

Ping IP

TTL:

MTU: 1442 (Max: 1492)

Bridge Mode

□ Enable Bridge Mode

PPP/MP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP) WAN IP Alias

Fixed IP: ○ Yes ● No (Dynamic IP)

Fixed IP Address

● Default MAC Address

○ Specify a MAC Address

MAC Address:

00 . 50 . 7F : 00 . 00 . 01

PPPoE Client 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.

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.

Password – Type in the password provided by ISP in this field.

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 1442.

Bridge Mode

If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.

PPP/MP Setup

PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP. If you want to connect to Internet all the time, you can check **Always On**.

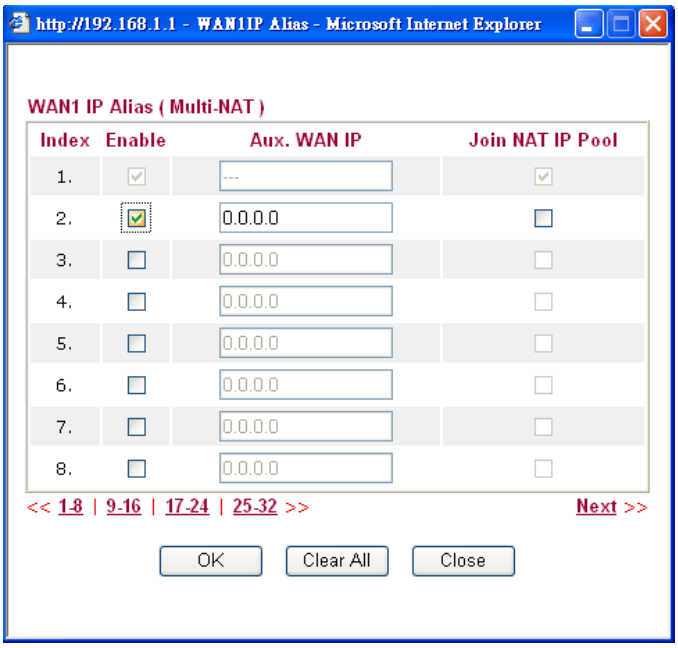
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

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 **32** public IP addresses other than the current one you are using.

Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	☑	---	☑
2.	☑	0.0.0.0	□
3.	□	0.0.0.0	□
4.	□	0.0.0.0	□
5.	□	0.0.0.0	□
6.	□	0.0.0.0	□
7.	□	0.0.0.0	□
8.	□	0.0.0.0	□

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.

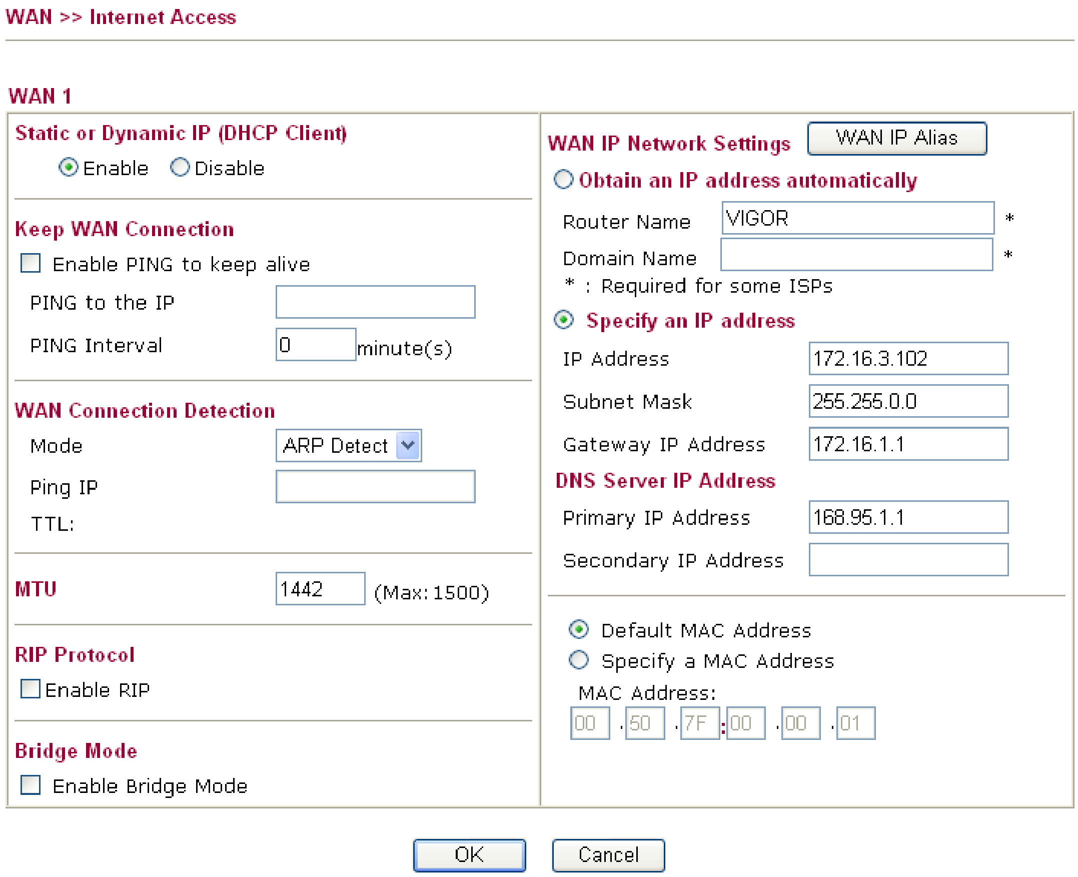
Specify a MAC Address – Type the MAC address for the router manually.

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

Details Page for Static or Dynamic IP in WAN1 ~ WAN4

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 choose **Static or Dynamic IP** mode from **Internet Access** menu. The following web page will be shown.



WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client)
● Enable ○ Disable

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

WAN Connection Detection
Mode ARP Detect
Ping IP
TTL:

MTU 1442 (Max:1500)

RIP Protocol
□ Enable RIP

Bridge Mode
□ Enable Bridge Mode

WAN IP Network Settings [WAN IP Alias]

○ Obtain an IP address automatically
Router Name VIGOR *
Domain Name *
* : Required for some ISPs

● Specify an IP address
IP Address 172.16.3.102
Subnet Mask 255.255.0.0
Gateway IP Address 172.16.1.1

DNS Server IP Address
Primary IP Address 168.95.1.1
Secondary IP Address

● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 . 50 . 7F : 00 . 00 . 01

Static or Dynamic IP

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. The default setting is 1442.

RIP Protocol

Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.

Bridge Mode

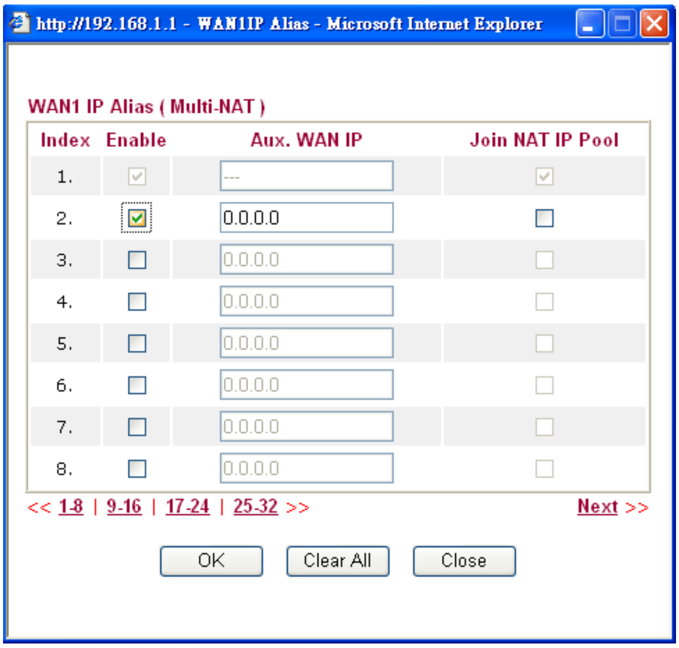
If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.

WAN IP Network Settings

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 **32** public IP addresses other than the current one you are using.

Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	☑	---	☑
2.	☑	0.0.0.0	□
3.	□	0.0.0.0	□
4.	□	0.0.0.0	□
5.	□	0.0.0.0	□
6.	□	0.0.0.0	□
7.	□	0.0.0.0	□
8.	□	0.0.0.0	□

<< 1-8 | 9-16 | 17-24 | 25-32 >>
Next >>
OK
Clear All
Close

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.

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.

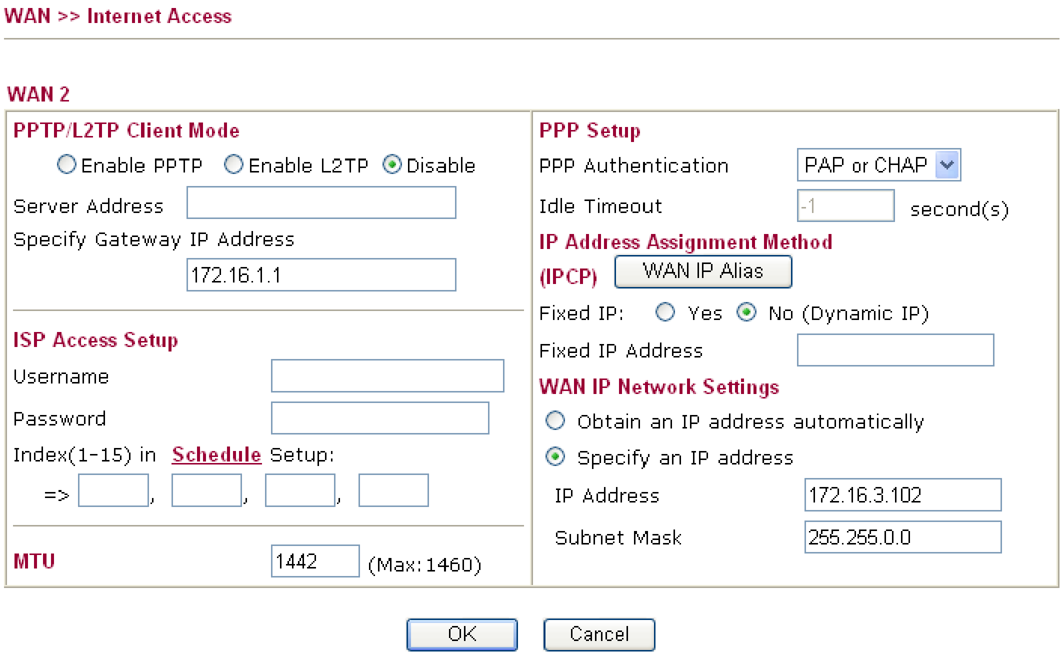
Default MAC Address : Click this radio button to use default MAC address for the router.

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.

Details Page for PPTP/L2TP in WAN1 ~ WAN4

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Internet Access** menu. The following web page will be shown.



WAN >> Internet Access

WAN 2

PPTP/L2TP Client Mode

○ Enable PPTP ○ Enable L2TP ● Disable

Server Address

Specify Gateway IP Address: 172.16.1.1

ISP Access Setup

Username

Password

Index(1-15) in Schedule Setup:

=> , , ,

MTU 1442 (Max:1460)

PPP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP) WAN IP Alias

Fixed IP: ○ Yes ● No (Dynamic IP)

Fixed IP Address

WAN IP Network Settings

○ Obtain an IP address automatically

● Specify an IP address

IP Address: 172.16.3.102

Subnet Mask: 255.255.0.0

PPTP/L2TP Client Mode

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.

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.

Password -Type in the password provided by ISP in this field.

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. The default setting is 1442.

PPP Setup

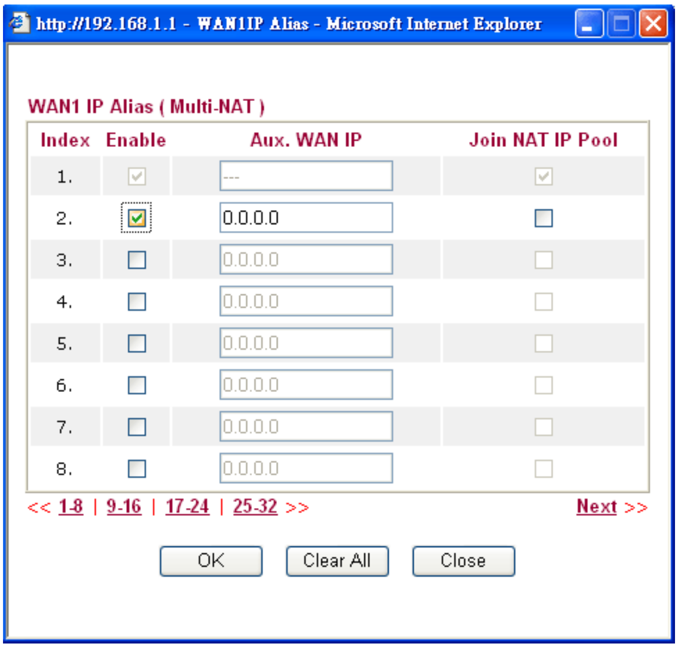
PPP Authentication - Select **PAP only** or **PAP or CHAP** for PPP.

Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address Assignment Method(IPCP)

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.



http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	☑	---	☑
2.	☑	0.0.0.0	□
3.	□	0.0.0.0	□
4.	□	0.0.0.0	□
5.	□	0.0.0.0	□
6.	□	0.0.0.0	□
7.	□	0.0.0.0	□
8.	□	0.0.0.0	□

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.

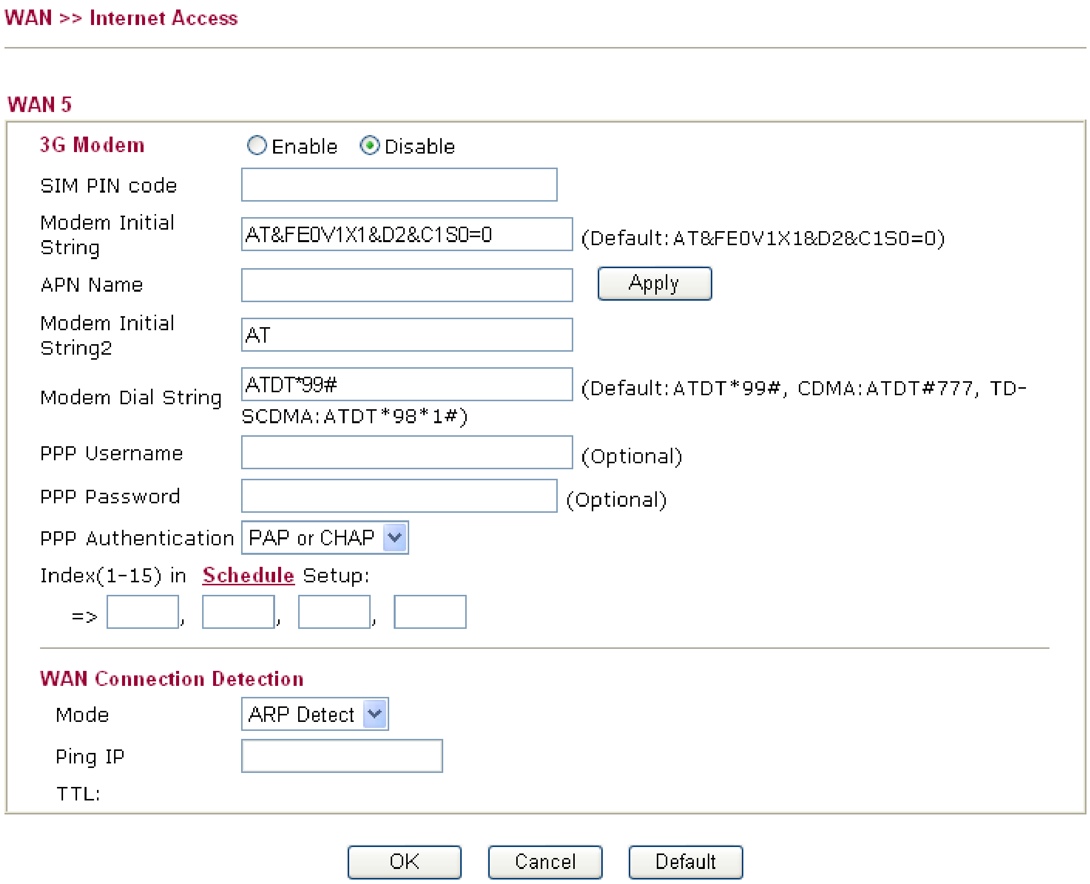
Specify an IP address – Click this radio button to specify some data.

IP Address – Type the IP address.

Subnet Mask – Type the subnet mask.

Details Page for PPP in WAN5

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN5. The following web page will be shown.



WAN >> Internet Access

WAN 5

3G Modem ○ Enable ● Disable

SIM PIN code

Modem Initial String: AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)

APN Name [Apply]

Modem Initial String2: AT

Modem Dial String: ATDT*99# (Default:ATDT*99#, CDMA:ATDT#777, TD-SCDMA:ATDT*98*1#)

PPP Username (Optional)

PPP Password (Optional)

PPP Authentication: PAP or CHAP

Index(1-15) in Schedule Setup:

=> , , ,

WAN Connection Detection

Mode: ARP Detect

Ping IP

TTL:

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

SIM PIN code Type PIN code of the SIM card that will be used to access Internet.

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.

APN Name APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.

Modem Initial String2 The initial string 1 is shared with APN.

In some cases, users may need another initial ***AT*** command to restrict 3G band or do any special settings.

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.

PPP Username Type the PPP username (optional).

PPP Password Type the PPP password (optional).

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.

Default

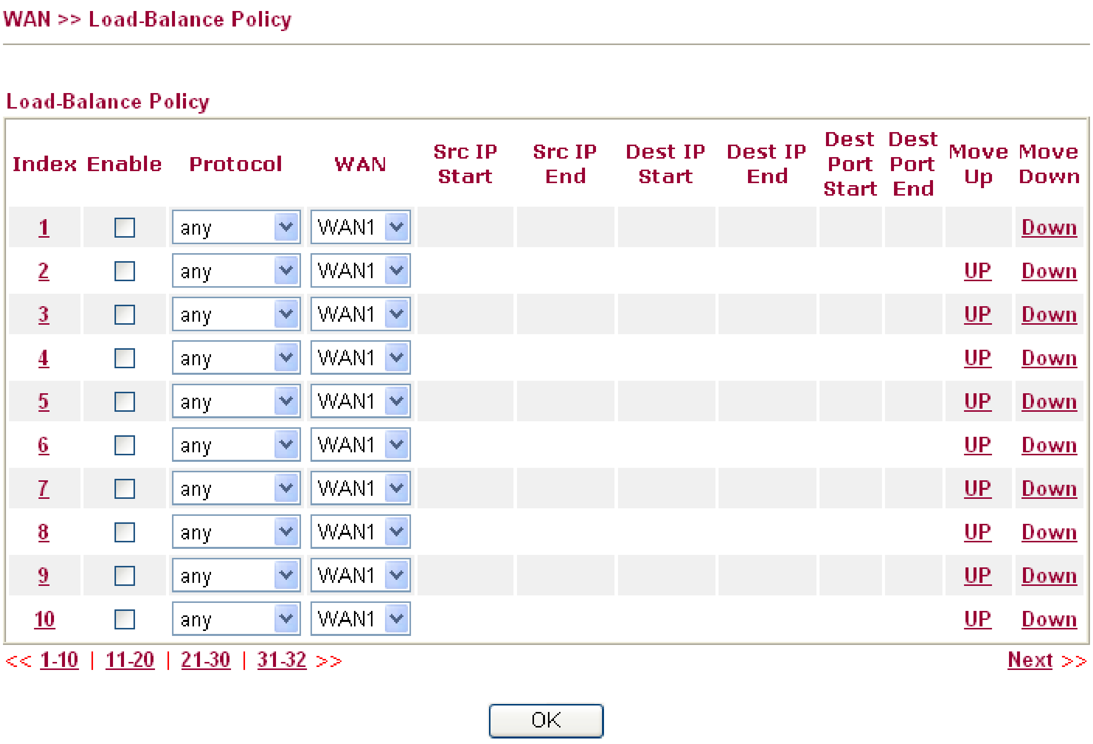
Click it to reset to the factory default setting for 3G connection.

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

4.1.4 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

> **Note:** Load-Balance Policy is running only when more than two WAN interfaces are activated.



WAN >> Load-Balance Policy

Load-Balance Policy

Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	□	any	WAN1								Down
2	□	any	WAN1							UP	Down
3	□	any	WAN1							UP	Down
4	□	any	WAN1							UP	Down
5	□	any	WAN1							UP	Down
6	□	any	WAN1							UP	Down
7	□	any	WAN1							UP	Down
8	□	any	WAN1							UP	Down
9	□	any	WAN1							UP	Down
10	□	any	WAN1							UP	Down

<< 1-10 | 11-20 | 21-30 | 31-32 >>   Next >>

Index Click the number of index to access into the load-balance policy configuration web page.

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to change the protocol for the WAN interface.

WAN Use the drop-down menu to change the WAN interface.

Src IP Start Displays the IP address for the start of the source IP

Src IP End Displays the IP address for the end of the source IP.

Dest IP Start Displays the IP address for the start of the destination IP.

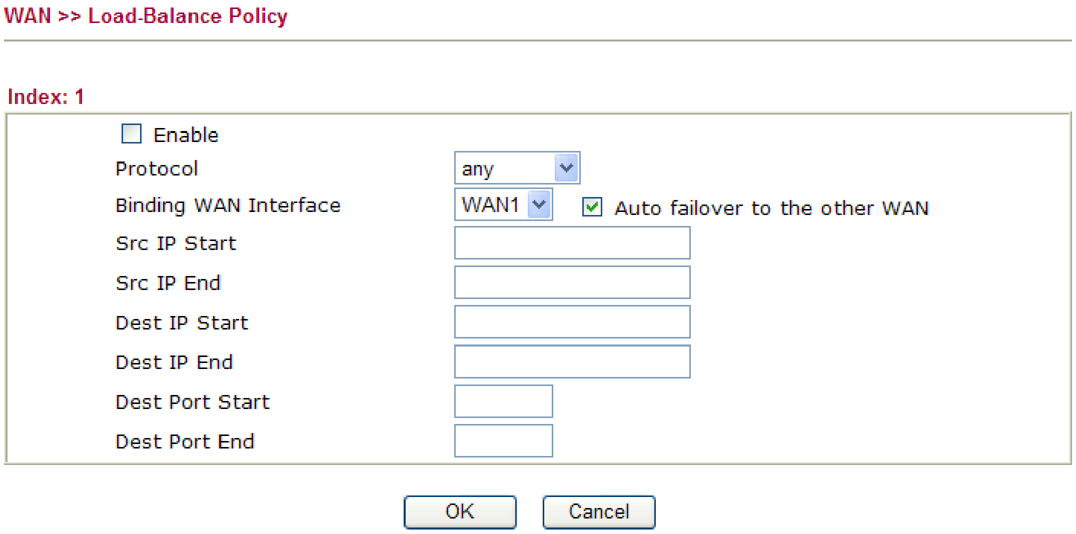
Dest IP End Displays the IP address for the end of the destination IP.

Dest Port Start Displays the IP address for the start of the destination port.

Dest Port End Displays the IP address for the end of the destination port.

Move UP/Move Down Use **Up** or **Down** link to move the order of the policy.

Click **Index 1** to access into the following page for configuring load-balance policy.



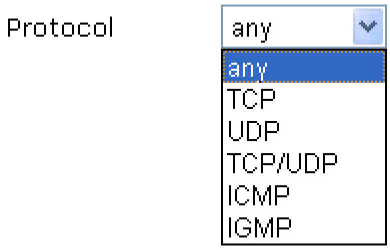
WAN >> Load-Balance Policy

Index: 1

☐ Enable	
Protocol	any
Binding WAN Interface	WAN1 ☑ Auto failover to the other WAN
Src IP Start	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
Dest Port End	

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to choose a proper protocol for the WAN interface.



Binding WAN interface Choose the WAN interface (WAN1 / WAN2 / WAN3 / WAN4 / WAN5) for binding.

Auto failover to other WAN – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is failover.

Src IP Start Type the source IP start for the specified WAN interface.

Src IP End Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.

Dest IP Start Type the destination IP start for the specified WAN interface.

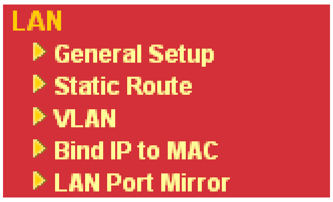
Dest IP End Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

Dest Port Start Type the destination port start for the destination IP.

Dest Port End Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

4.2 LAN

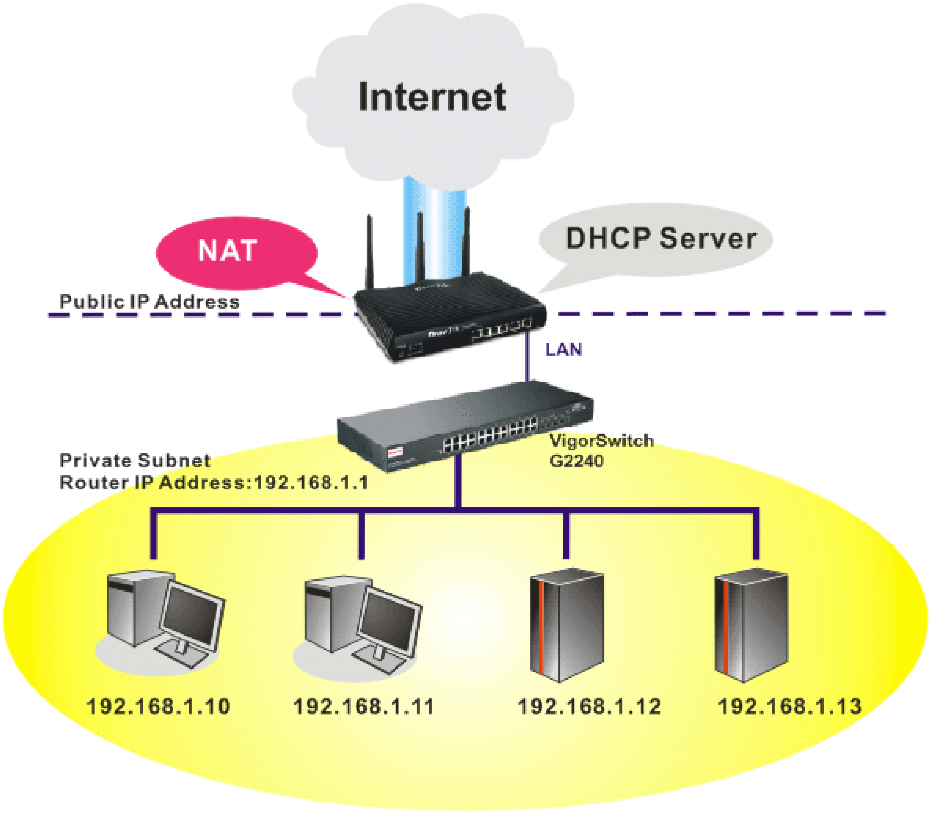
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.



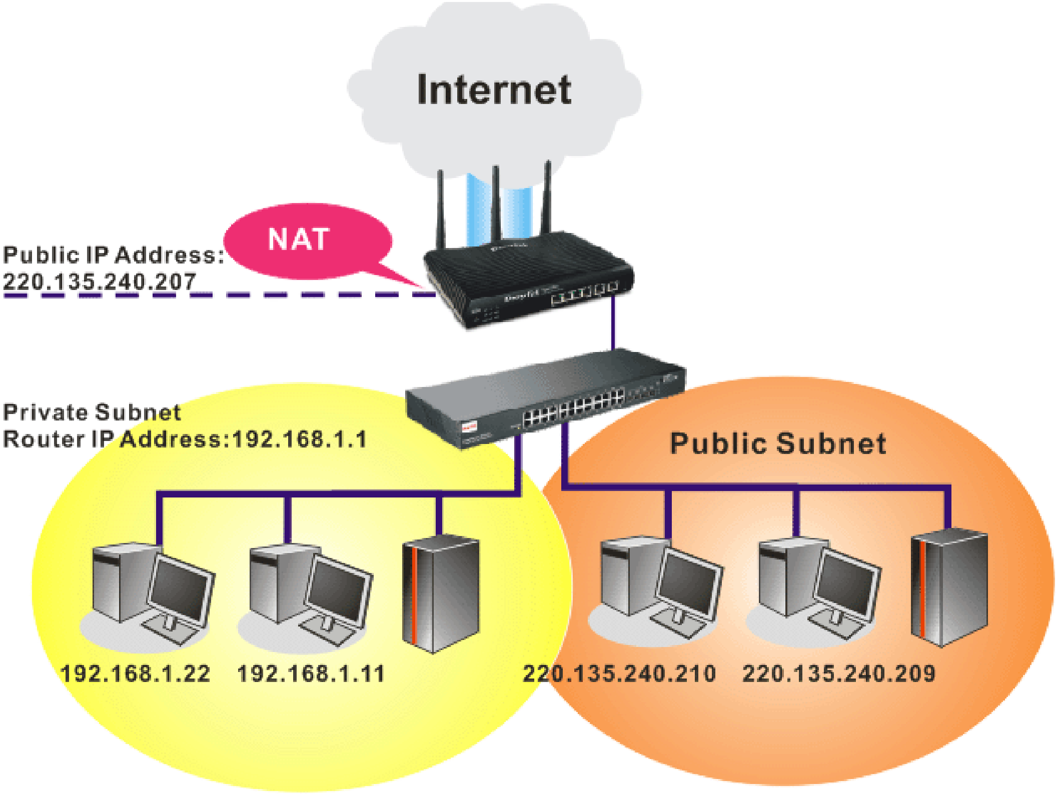
LAN
- General Setup
- Static Route
- VLAN
- Bind IP to MAC
- LAN Port Mirror

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.



What is Routing Information Protocol (RIP)

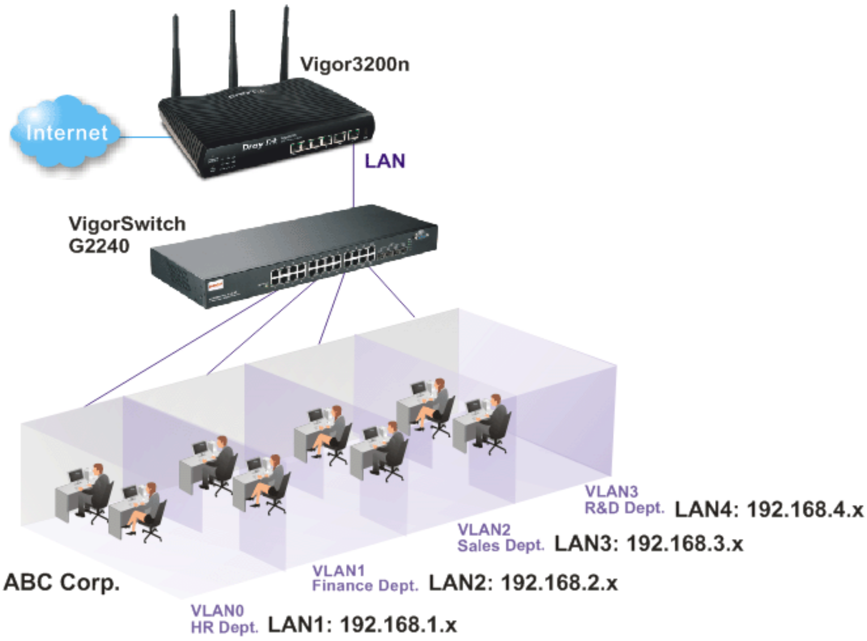
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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 port and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.

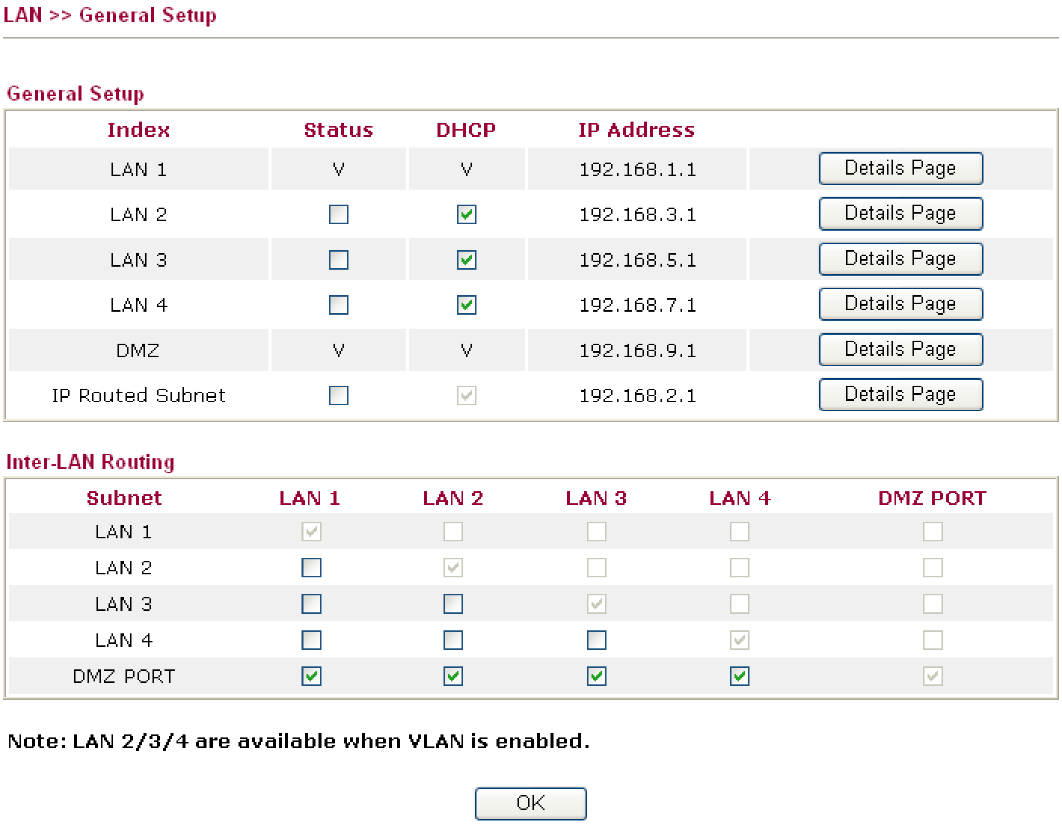

Vigor3200n
Internet
LAN
VigorSwitch G2240
VLAN3 R&D Dept. LAN4: 192.168.4.x
VLAN2 Sales Dept. LAN3: 192.168.3.x
ABC Corp.
VLAN1 Finance Dept. LAN2: 192.168.2.x
VLAN0 HR Dept. LAN1: 192.168.1.x

4.2.2 General Setup

This page provides you the general settings for LAN. Vigor3200 series provides four LANs, one DMZ and one IP Routed Subnet.

Click **LAN** to open the LAN settings page and choose **General Setup**.

There are four subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN4). In addition, different subnets can link for each other by configuring Inter-LAN Routing. At present, LAN1 setting is fixed with NAT mode only. LAN2 – LAN4 can be operated under NAT or Route mode. IP Routed Subnet can be operated under Route mode.



LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page
LAN 2	□	☑	192.168.3.1	Details Page
LAN 3	□	☑	192.168.5.1	Details Page
LAN 4	□	☑	192.168.7.1	Details Page
DMZ	V	V	192.168.9.1	Details Page
IP Routed Subnet	□	☑	192.168.2.1	Details Page

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1	☑	□	□	□	□
LAN 2	□	☑	□	□	□
LAN 3	□	□	☑	□	□
LAN 4	□	□	□	☑	□
DMZ PORT	☑	☑	☑	☑	☑

Note: LAN 2/3/4 are available when VLAN is enabled.

OK

General Setup----- Allow to configure settings for each subnet respectively.

Index Display all of the LAN items, DMZ and IP Routed Subnet.

Status Check the box to enable such LAN configuration. Basically, LAN1 status is enabled in default. LAN2, LAN3, LAN4 and IP Routed Subnet can be observed by checking the box of **Status**.

DHCP Check the box to enable DHCP server for such LAN configuration. LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.

IP Address Display the IP address of the LAN configuration. 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.**

Inter-LAN Routing --- Check the box to allow to link or route two subnets.

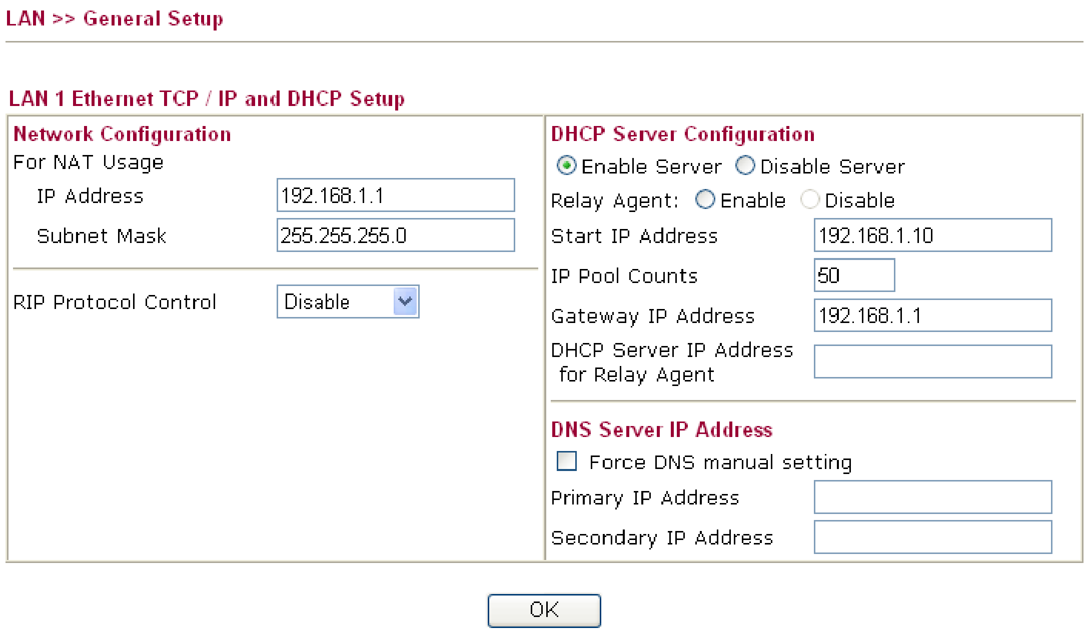
Subnet Display four LANs and one DMZ PORT available for routing.

LAN 1 ~ LAN 4, DMZ PORT Check the box to make the routing among LANs.

To configure LAN 1 ~ LAN 4, DMZ or IP Routed Subnet, simply click **Details Page** to open the settings page.

LAN 1

LAN1 is the default configuration for basic host connection.



LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration

For NAT Usage

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable

DHCP Server Configuration

● Enable Server ○ Disable Server

Relay Agent: ○ Enable ○ Disable

Start IP Address: 192.168.1.10

IP Pool Counts: 50

Gateway IP Address: 192.168.1.1

DHCP Server IP Address for Relay Agent:

DNS Server IP Address

□ Force DNS manual setting

Primary IP Address:

Secondary IP Address:

Network Configuration Set IP address and Subnet Mask for clients connected via LAN1.

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)

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

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

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

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

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

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.

DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server IP Address

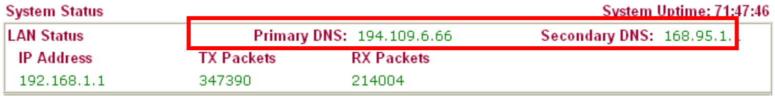
DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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:



System Status | System Uptime: 71:47:46

LAN Status | Primary DNS: 194.109.6.66 | Secondary DNS: 168.95.1.

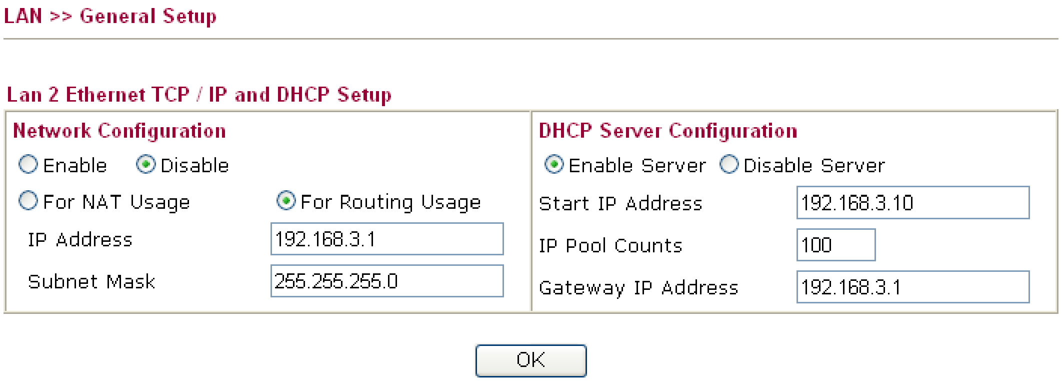
IP Address	TX Packets	RX Packets
192.168.1.1	347390	214004

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.

LAN 2, LAN 3, LAN 4

With the multi-subnet feature offered by Vigor router, LAN2 ~ LAN4 are used for different subnets.



LAN >> General Setup

Lan 2 Ethernet TCP / IP and DHCP Setup

Network Configuration

○ Enable ● Disable

○ For NAT Usage ● For Routing Usage

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

DHCP Server Configuration

● Enable Server ○ Disable Server

Start IP Address: 192.168.3.10

IP Pool Counts: 100

Gateway IP Address: 192.168.3.1

Network Configuration

Enable – enable the configuration for such LAN.

Disable – disable the configuration for such LAN.

For NAT Usage

Click this item to invoke NAT usage.

For Routing Usage

Click this item to invoke Routing 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)

DHCP Server Configuration

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

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

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.

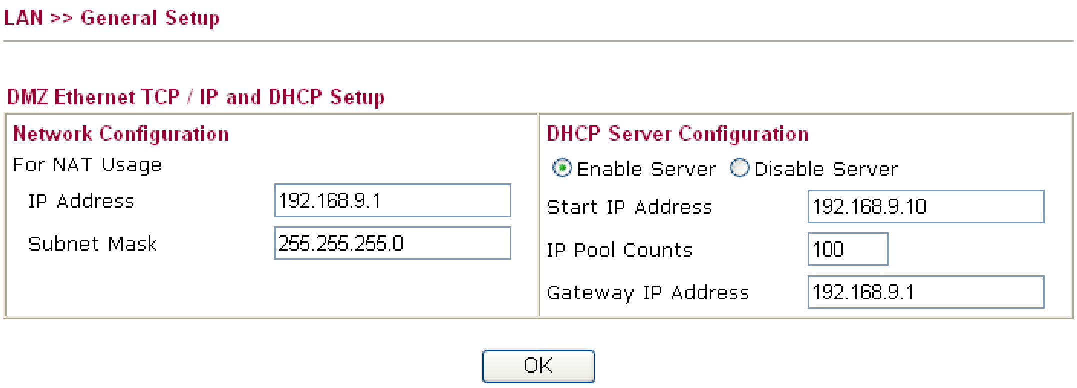
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

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.

DMZ

DMZ port setting is used for connecting host in DMZ.



LAN >> General Setup

DMZ Ethernet TCP / IP and DHCP Setup

Network Configuration		DHCP Server Configuration	
For NAT Usage		● Enable Server ○ Disable Server	
IP Address	192.168.9.1	Start IP Address	192.168.9.10
Subnet Mask	255.255.255.0	IP Pool Counts	100
		Gateway IP Address	192.168.9.1

Network Configuration Set IP address and Subnet Mask for clients connected via DMZ port.

For NAT Usage **IP Address -** Type in private IP address for connecting to a local private network (Default: 192.168.9.1).

Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

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

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

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.

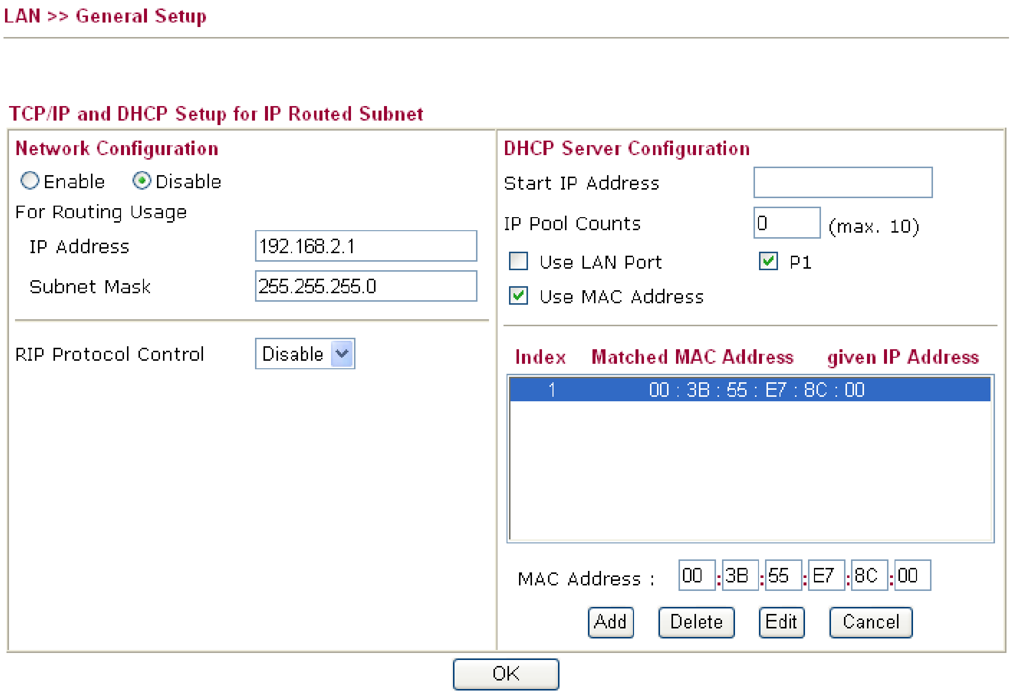
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.9.10, the starting IP address must be 192.168.9.11 or greater, but smaller than 192.168.1.254.

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.

IP Routed Subnet

Vigor router can serve as a DHCP server to route the request coming from LAN PC.



LAN >> General Setup

TCP/IP and DHCP Setup for IP Routed Subnet

Network Configuration

○ Enable ● Disable

For Routing Usage

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable

DHCP Server Configuration

Start IP Address:

IP Pool Counts: 0 (max. 10)

□ Use LAN Port ☑ P1

☑ Use MAC Address

Index	Matched MAC Address	given IP Address
1	00 : 3B : 55 : E7 : 8C : 00	

MAC Address : 00 : 3B : 55 : E7 : 8C : 00

Network Configuration

Enable – enable the configuration for such LAN.

Disable – disable the configuration for such LAN.

IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.2.1).

Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

RIP Protocol - Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers.

DHCP Server Configuration

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

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

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

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 0 and the maximum is 10.

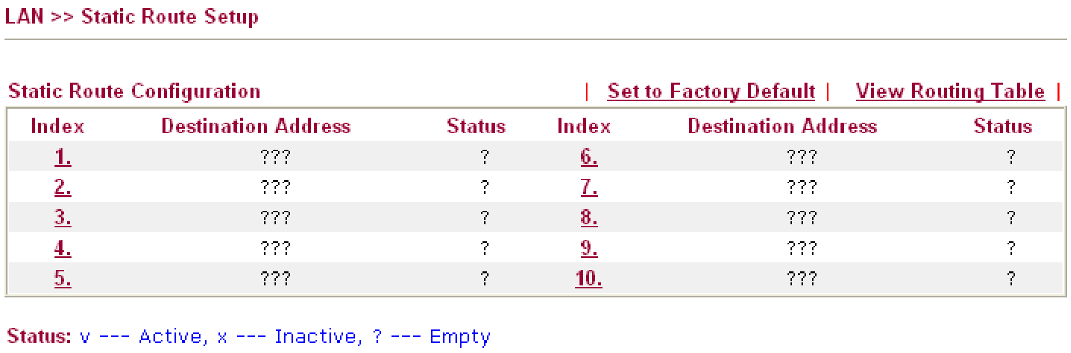
Use LAN Port – Any PC asked for LAN IP address assigned by the DHCP server will send the request through the LAN port of the router.

Use MAC Address - IP Routed Subnet will automatically assign the subnet for incoming DHCP with listed MAC address. Only the PC which matches the MAC address added can ask for LAN IP address assigned by DHCP server.

Add /Delete /Edit- Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address of the DHCP server which can help the router to assign the correct IP address of the correct subnet to the correct host.

4.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**.



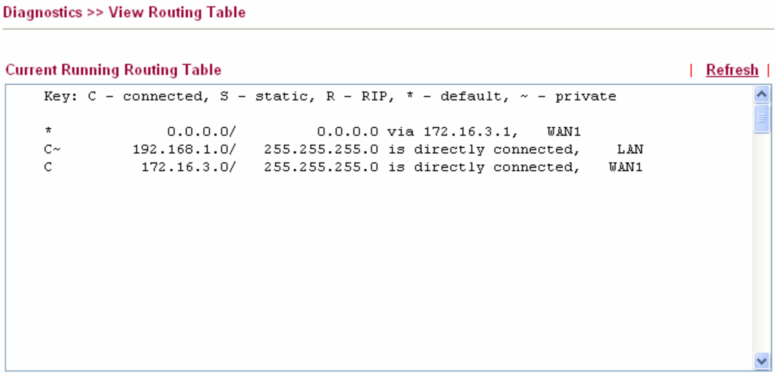
LAN >> Static Route Setup

Static Route Configuration | 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

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.
Viewing Routing Table	Displays the routing table for your reference.



Diagnostics >> View Routing Table

Current Running Routing Table | Refresh |

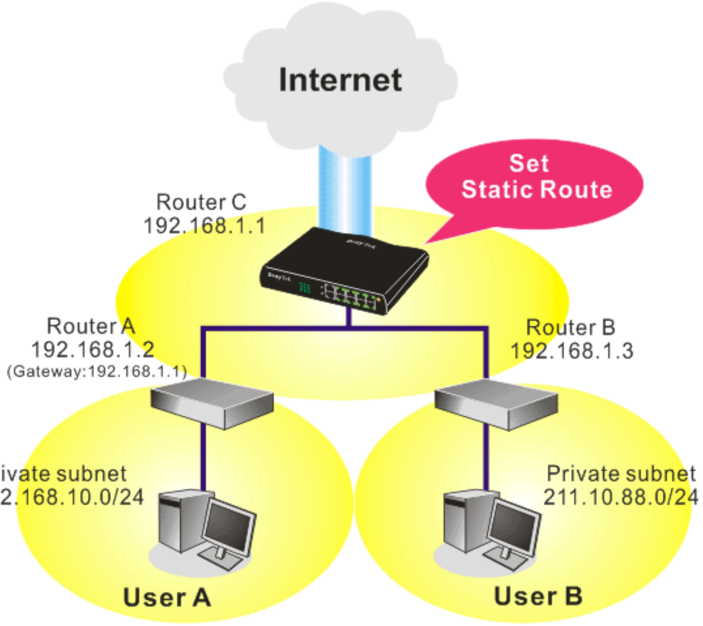
```
Key: C - connected, S - static, R - RIP, * - default, ~ - private

*            0.0.0.0/          0.0.0.0 via 172.16.3.1,   WAN1
C~         192.168.1.0/   255.255.255.0 is directly connected,    LAN
C           172.16.3.0/   255.255.255.0 is directly connected,   WAN1
```

Add Static Routes to Private and Public Networks

Here is an example 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.

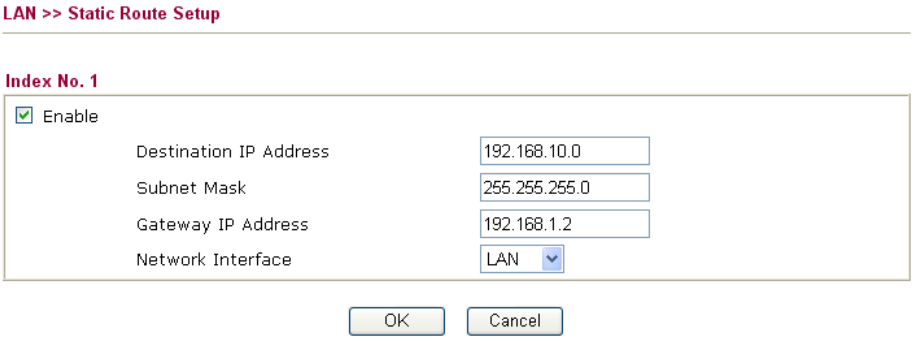
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



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**.



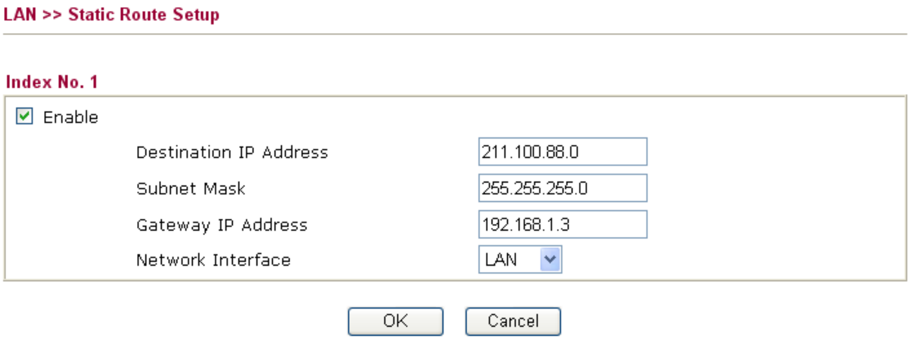
LAN >> Static Route Setup

Index No. 1

☑ Enable

Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN

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.



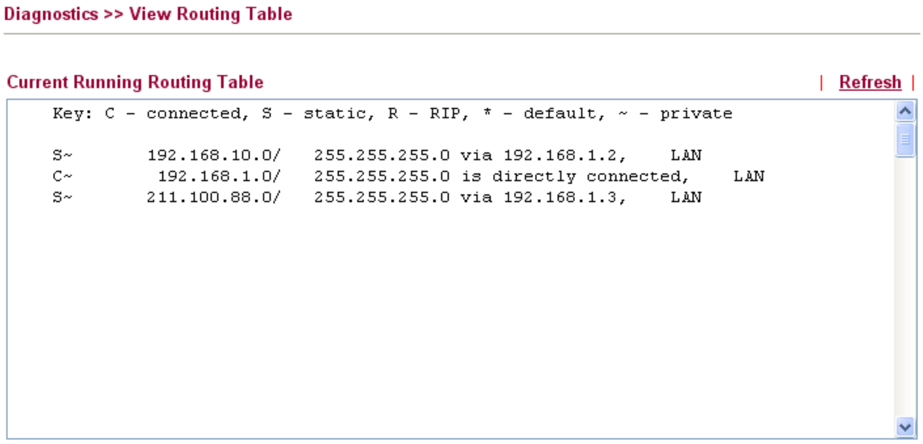
LAN >> Static Route Setup

Index No. 1

☑ Enable

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

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



Diagnostics >> View Routing Table

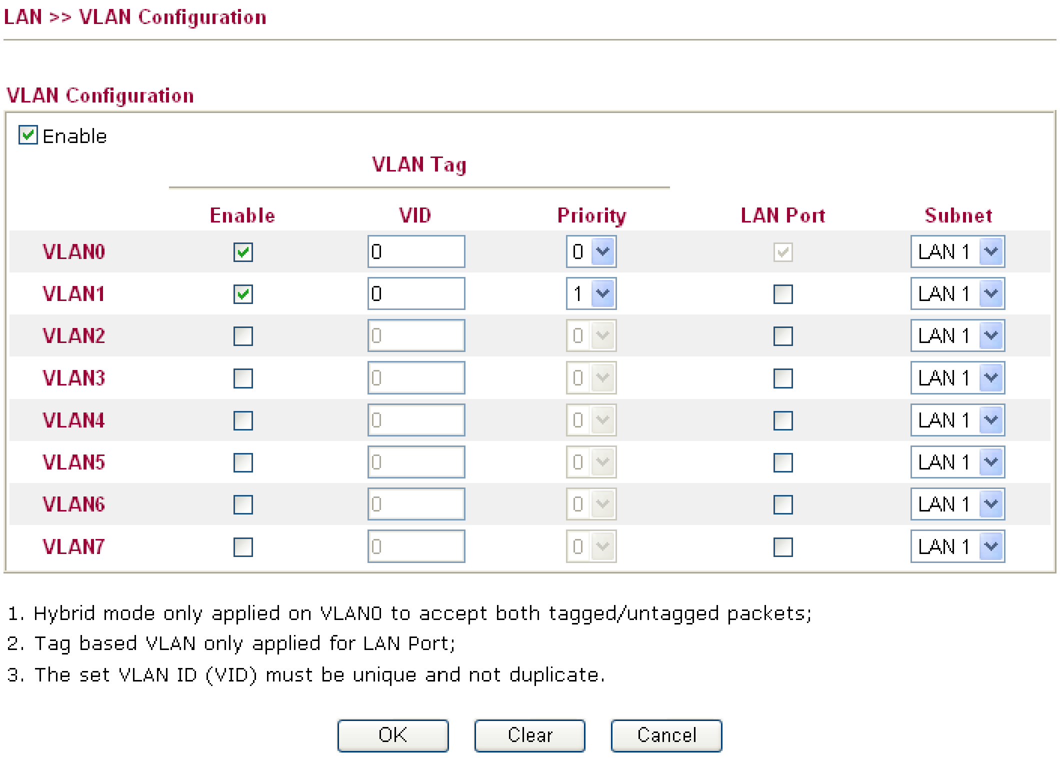
Current Running Routing Table

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private

S~       192.168.10.0/   255.255.255.0 via 192.168.1.2,    LAN
C~        192.168.1.0/   255.255.255.0 is directly connected,    LAN
S~       211.100.88.0/   255.255.255.0 via 192.168.1.3,    LAN
```

4.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage subnets by grouping them.

Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.



LAN >> VLAN Configuration

VLAN Configuration

☑ Enable

	VLAN Tag				
	Enable	VID	Priority	LAN Port	Subnet
VLAN0	☑	0	0	☑	LAN 1
VLAN1	☑	0	1	□	LAN 1
VLAN2	□	0	0	□	LAN 1
VLAN3	□	0	0	□	LAN 1
VLAN4	□	0	0	□	LAN 1
VLAN5	□	0	0	□	LAN 1
VLAN6	□	0	0	□	LAN 1
VLAN7	□	0	0	□	LAN 1

1. Hybrid mode only applied on VLAN0 to accept both tagged/untagged packets;
2. Tag based VLAN only applied for LAN Port;
3. The set VLAN ID (VID) must be unique and not duplicate.

Enable Check this box to enable VLAN configuration. The router will add specific VLAN tagging 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 LAN port.

VLAN Tag **Enable** – Check this box to enable the VID and the Priority. The router will add specific VLAN number to all packets on LAN while sending them out.

VID Type the value as the VLAN ID number. The range is form 0 to 4095.

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

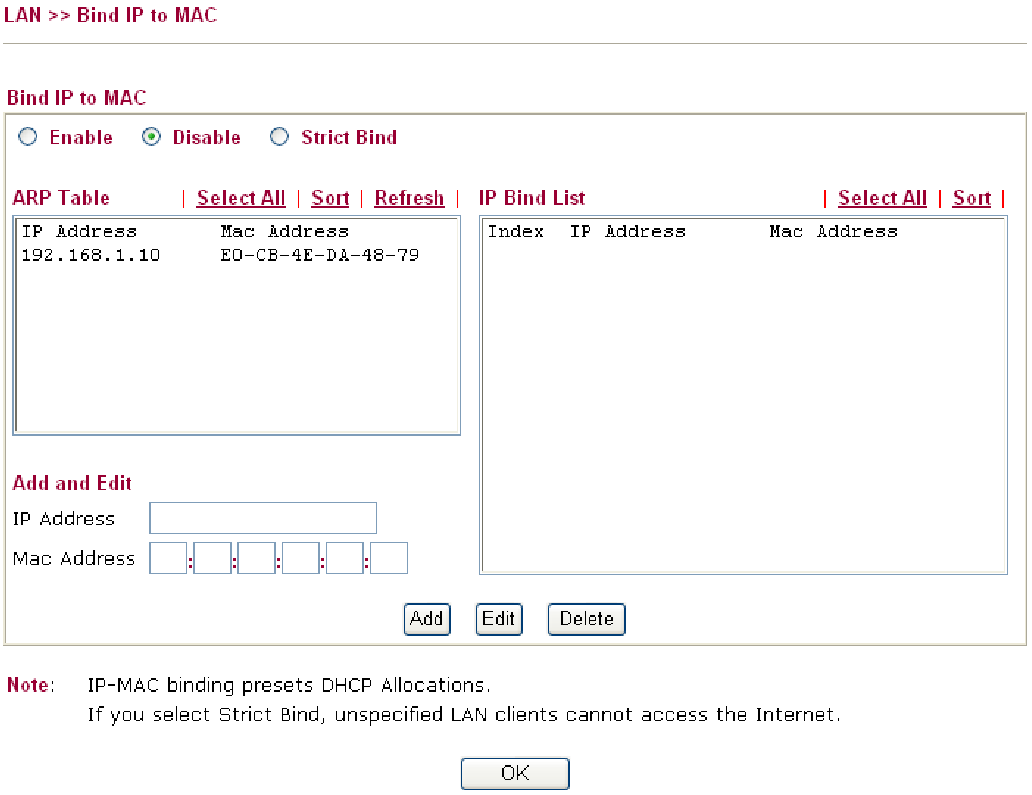
LAN Port Check this box to make the VLAN settings (such as VID, priority, subnet) applying to the LAN port.

Subnet Choose one of them to make the selected VLAN group mapping to specified subnet only. For example, LAN1 is specified for VLAN0 group. It means that PCs grouped under VLAN0 can get the IP address (es) that specified by the subnet.

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.



LAN >> Bind IP to MAC

Bind IP to MAC

○ Enable ● Disable ○ Strict Bind

ARP Table | Select All | Sort | Refresh |

```
IP Address          Mac Address
192.168.1.10        E0-CB-4E-DA-48-79
```

IP Bind List | Select All | Sort |

```
Index   IP Address          Mac Address
```

Add and Edit

IP Address

Mac Address : : : : :

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

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.

Add and Edit **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.

Refresh It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.

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**.

Edit It allows you to edit and modify the selected IP address and MAC address that you create before.

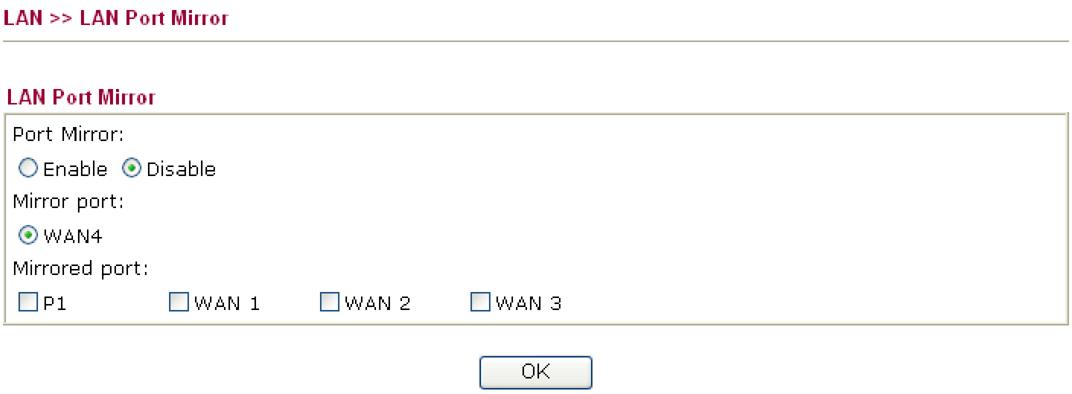
Delete You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**.

> **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 configurator of the router might not be accessed.

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 connect 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:

● WAN4

Mirrored port:

□ P1 □ WAN 1 □ WAN 2 □ WAN 3

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. At present, only WAN4 will be treated as mirror port.

Mirrored port Select which ports (LAN port or WAN port) are necessary to be mirrored. P1 represents LAN port.

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.

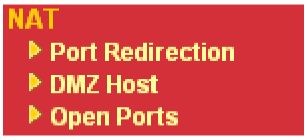
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize 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.

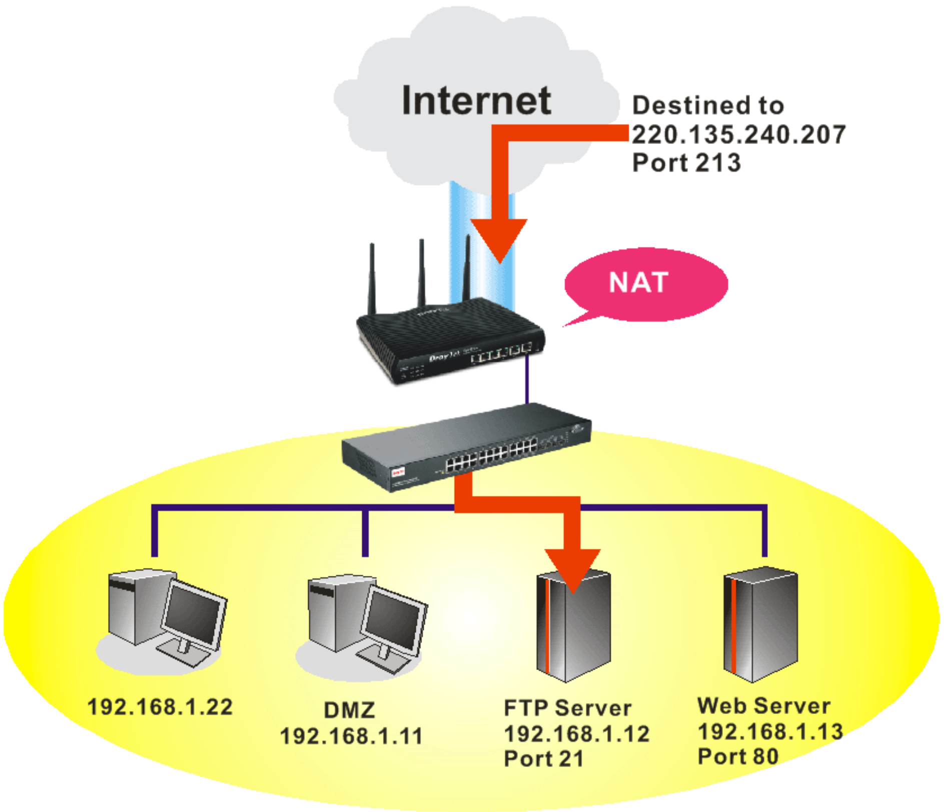
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



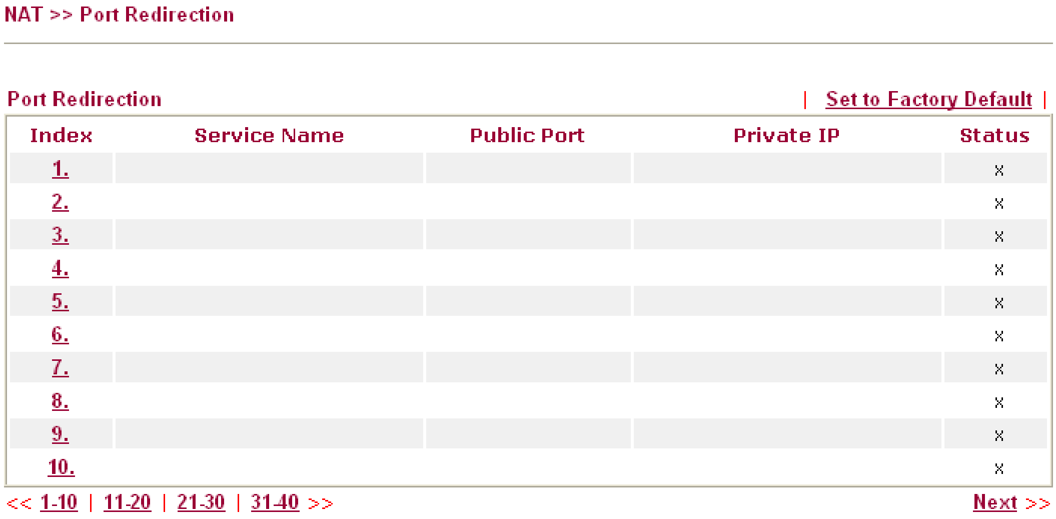
4.3.1 Port Redirection

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.

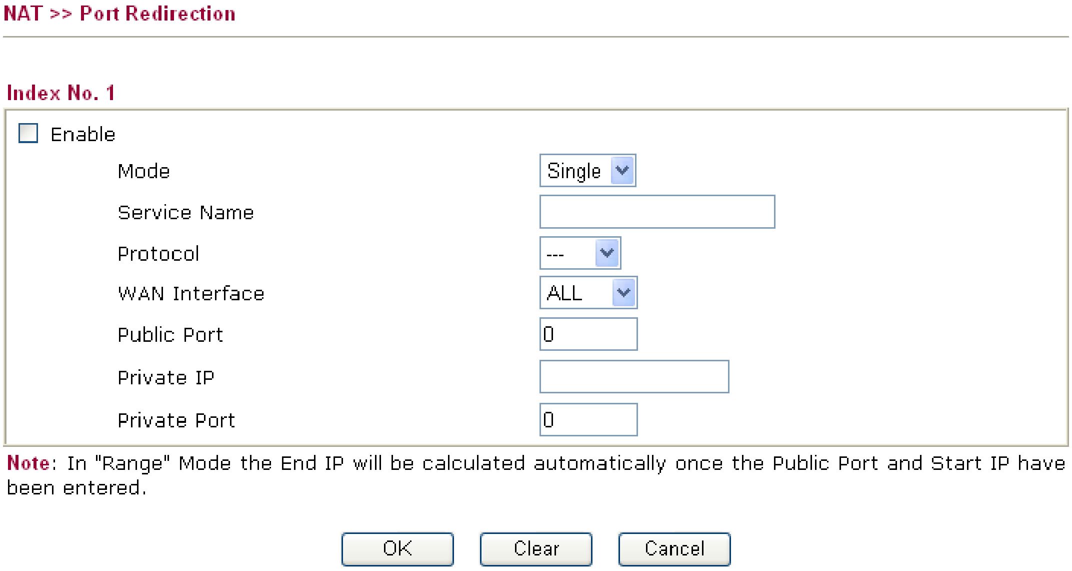

NAT >> Port Redirection

Port Redirection | Set to Factory Default |

Index	Service Name	Public Port	Private IP	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 | 21-30 | 31-40 >> Next >>

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



NAT >> Port Redirection

Index No. 1

□ Enable	
Mode	Single
Service Name	
Protocol	---
WAN Interface	ALL
Public Port	0
Private IP	
Private Port	0

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

Enable Check this box to enable such port redirection setting.

Mode Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name Enter the description of the specific network service.

Protocol Select the transport layer protocol (TCP or UDP).

WAN Interface Select the WAN interface used for port redirection.

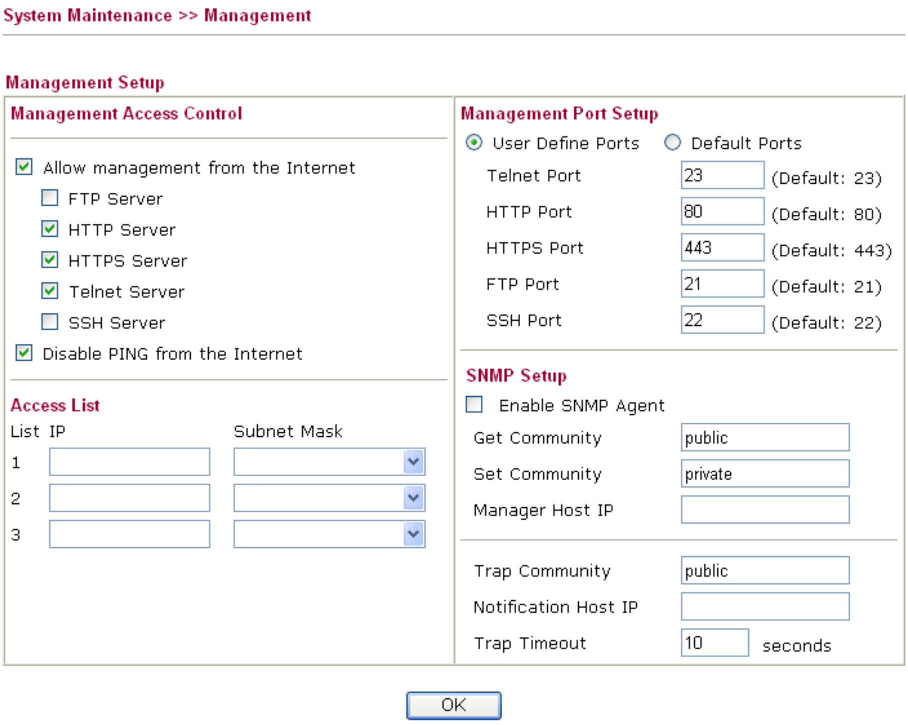
Public Port Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.

Private IP Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).

Private Port Specify the private port number of the service offered by the internal host.

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



System Maintenance >> Management

Management Setup

Management Access Control

☑ Allow management from the Internet
- □ FTP Server
- ☑ HTTP Server
- ☑ HTTPS Server
- ☑ Telnet Server
- □ SSH Server

☑ Disable PING from the Internet

Access List

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)
SSH Port	22	(Default: 22)

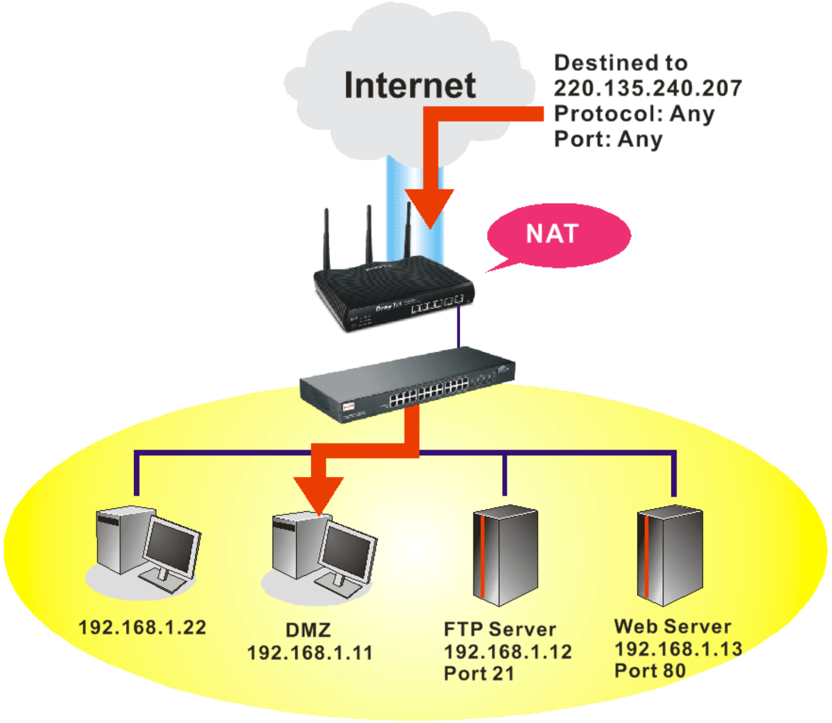
SNMP Setup

□ Enable SNMP Agent

Get Community	public
Set Community	private
Manager Host IP	
Trap Community	public
Notification Host IP	
Trap Timeout	10 seconds

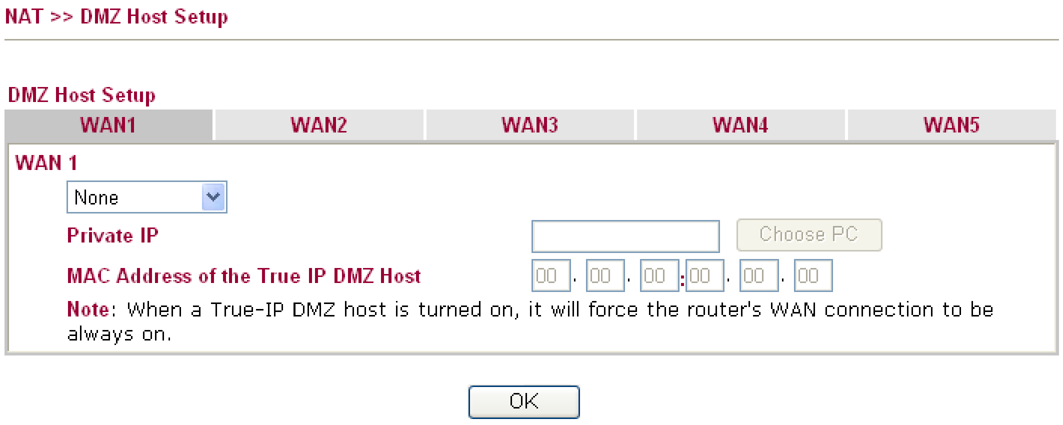
4.3.2 DMZ Host

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.



NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

None

Private IP: Choose PC

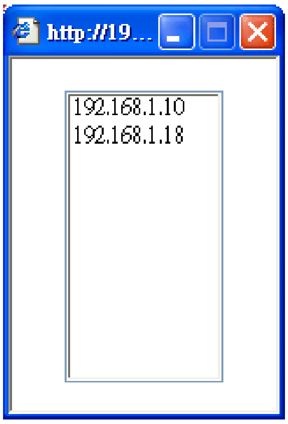
MAC Address of the True IP DMZ Host: 00 . 00 . 00 : 00 . 00 . 00

Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

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

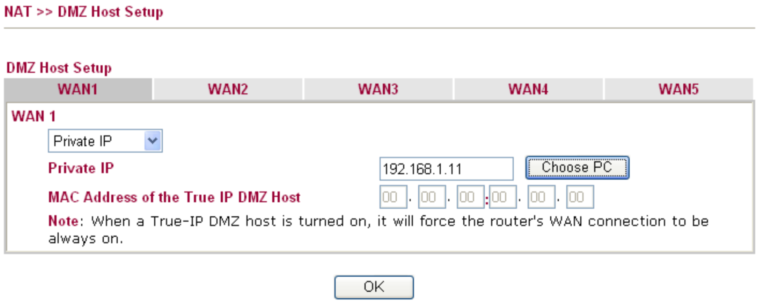
to select one.

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.



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

WAN 1

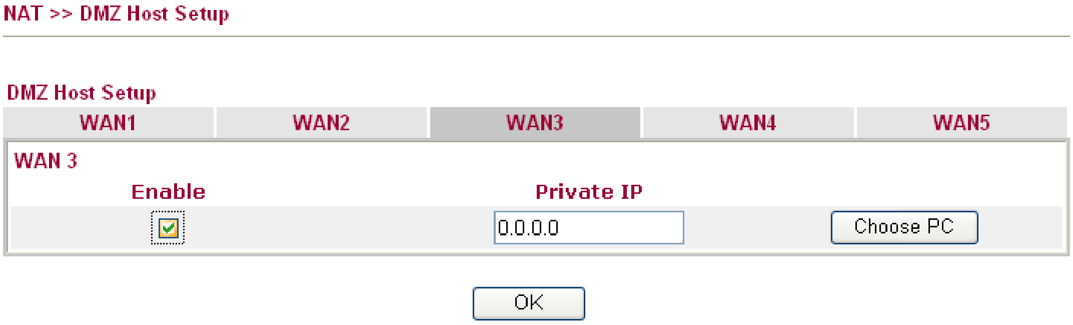
Private IP

Private IP: 192.168.1.11

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.

DMZ Host for WAN2 ~ WAN5 are slightly different with WAN1. See the following figure.



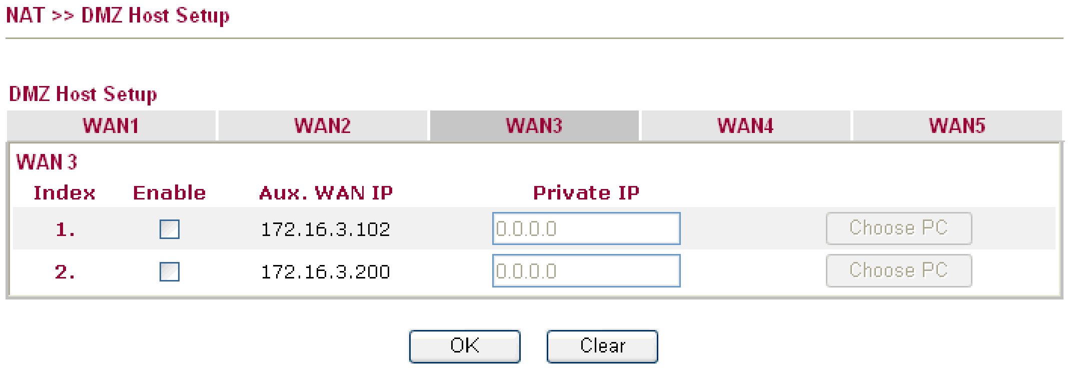
NAT >> DMZ Host Setup

DMZ Host Setup

WAN 3

Enable	Private IP	
☑	0.0.0.0	Choose PC

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2/WAN3/WAN4/WAN5 interface**,** you will find them in **Aux. WAN IP** for your selection.



NAT >> DMZ Host Setup

DMZ Host Setup

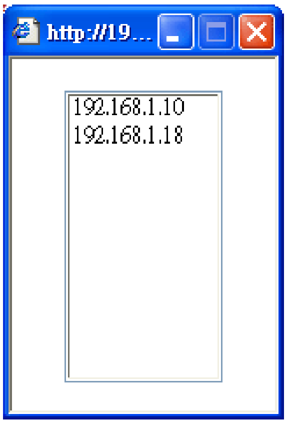
WAN 3

Index	Enable	Aux. WAN IP	Private IP	
1.	□	172.16.3.102	0.0.0.0	Choose PC
2.	□	172.16.3.200	0.0.0.0	Choose PC

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

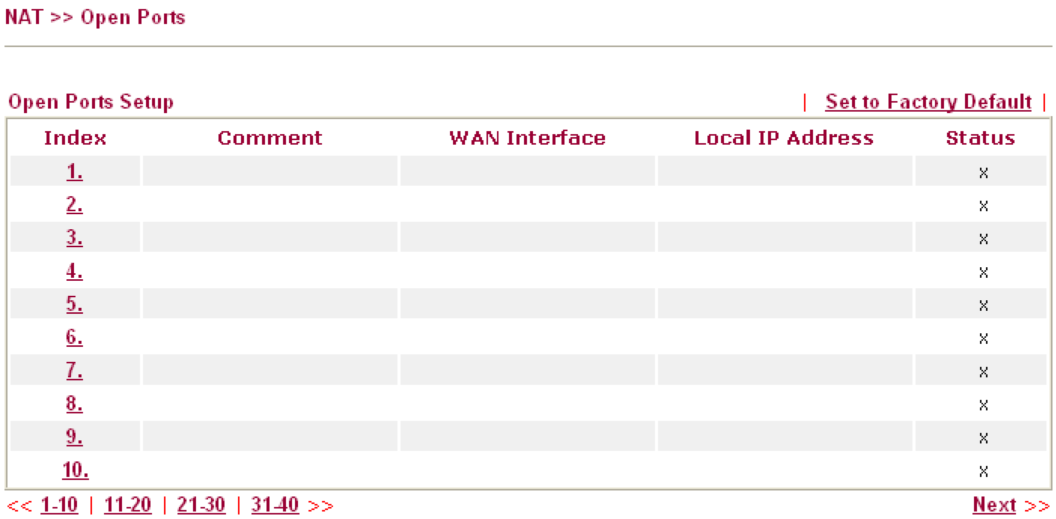
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.

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:



NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Comment	WAN Interface	Local IP Address	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 | 21-30 | 31-40 >> Next >>

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.

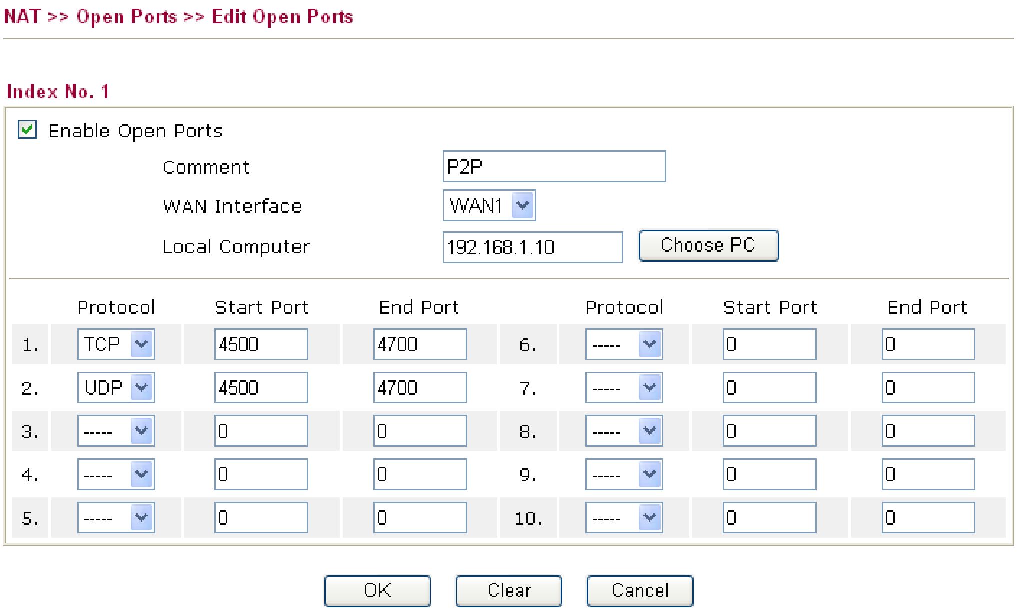
Comment Specify the name for the defined network service.

WAN Interface Display the WAN interface used by such index.

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	P2P
WAN Interface	WAN1
Local Computer	192.168.1.10 [Choose PC]

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	4500	4700	6.	-----	0	0
2.	UDP	4500	4700	7.	-----	0	0
3.	-----	0	0	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

Enable Open Ports Check to enable this entry.

Comment Make a name for the defined network application/service.

WAN IP Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.

Local Computer 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.

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:

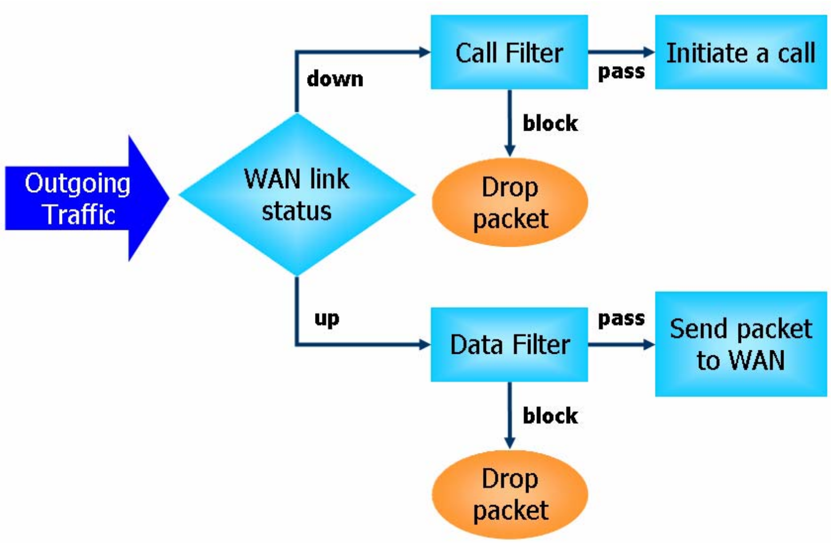
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

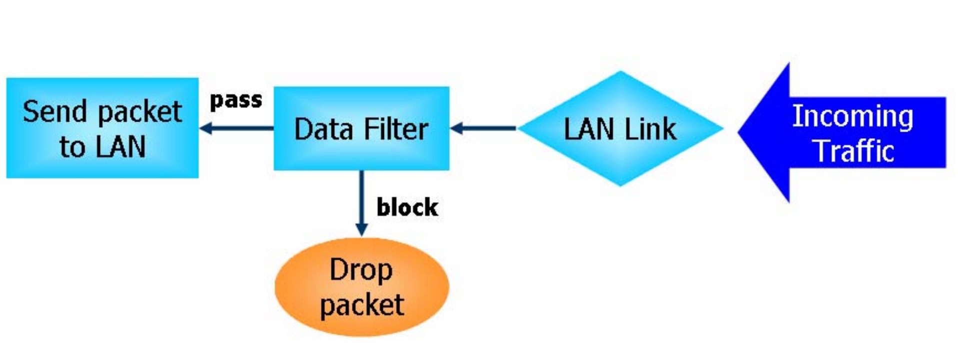
IP Filters

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 examine the header information also monitor the state of the connection.

Denial of Service (DoS) Defense

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

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

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

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

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

Below shows the menu items for Firewall.

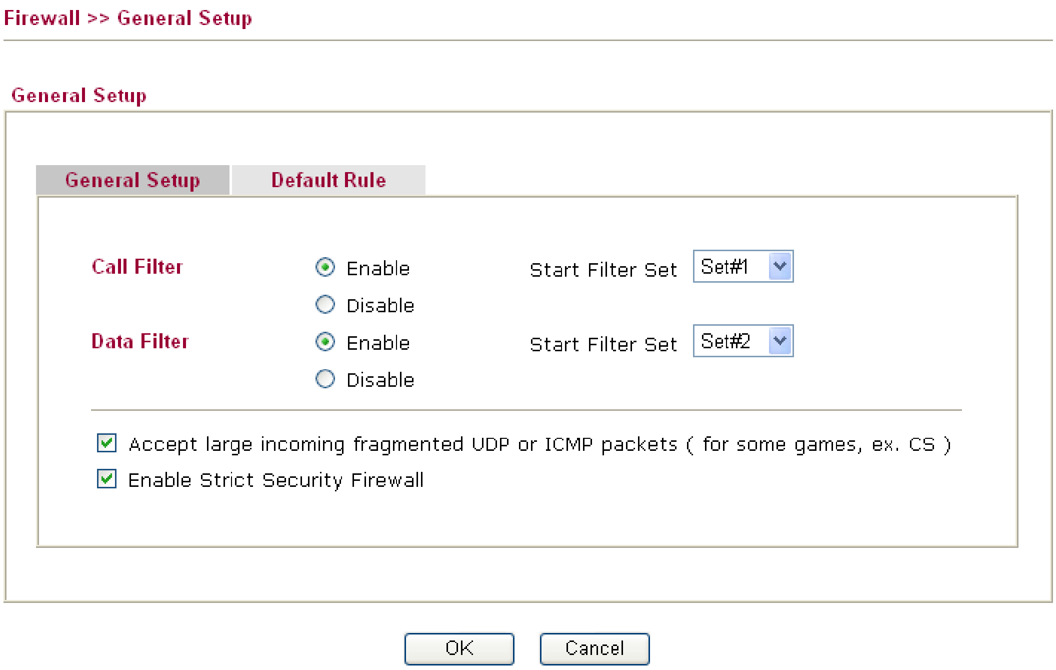
4.4.2 General Setup

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.

General Setup Page

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



Firewall >> General Setup

General Setup

General Setup | Default Rule

Call Filter ● Enable ○ Disable Start Filter Set Set#1

Data Filter ● Enable ○ Disable Start Filter Set Set#2

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

☑ Enable Strict Security Firewall

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.

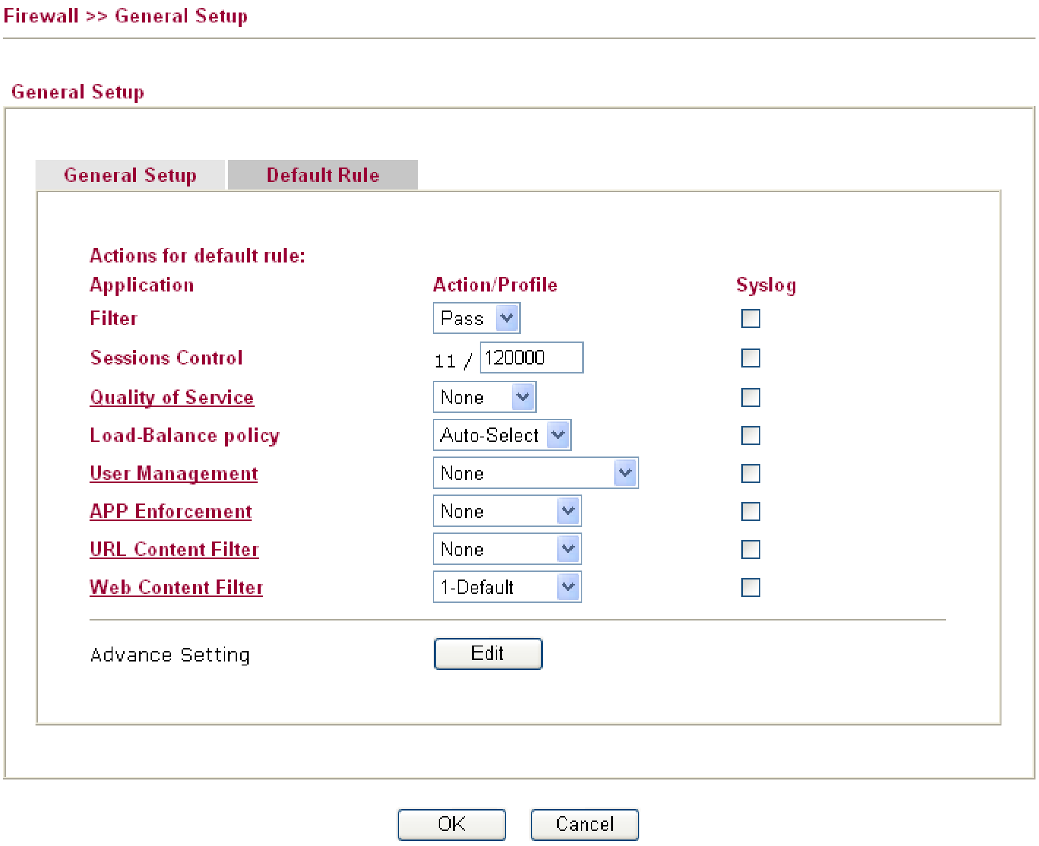
Accept large incoming… Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming fragmented UDP or ICMP Packets**". 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 will be inspected by the web content filter server while transmitting through Vigor router. If the web content filter server does not make any response (pass or block) for the packets, Vigor router's firewall will block the packets directly for security.

Default Rule Page

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



Firewall >> General Setup

General Setup

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	□
Sessions Control	11 / 120000	□
Quality of Service	None	□
Load-Balance policy	Auto-Select	□
User Management	None	□
APP Enforcement	None	□
URL Content Filter	None	□
Web Content Filter	1-Default	□

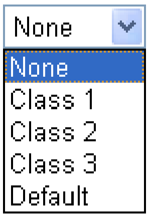
Advance Setting Edit

Filter Select **Pass** or **Block** for the packets that do not match with the filter rules.

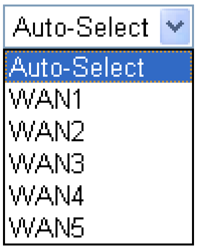
Filter Pass

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.

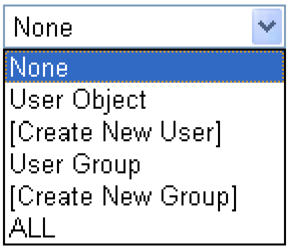
Quality of Service Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.



Load-Balance Policy Choose the WAN interface for applying Load-Balance Policy.



User Management Such item is available only when **Rule-Based** is selected in User **Management>>General Setup**. The general firewall rule will be applied to the user/user group/all users specified here.



> **Note:** When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.

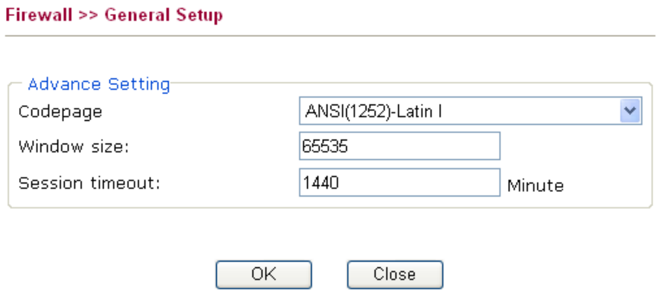
APP Enforcement Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to selelct, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** 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.



Firewall >> General Setup

Advance Setting

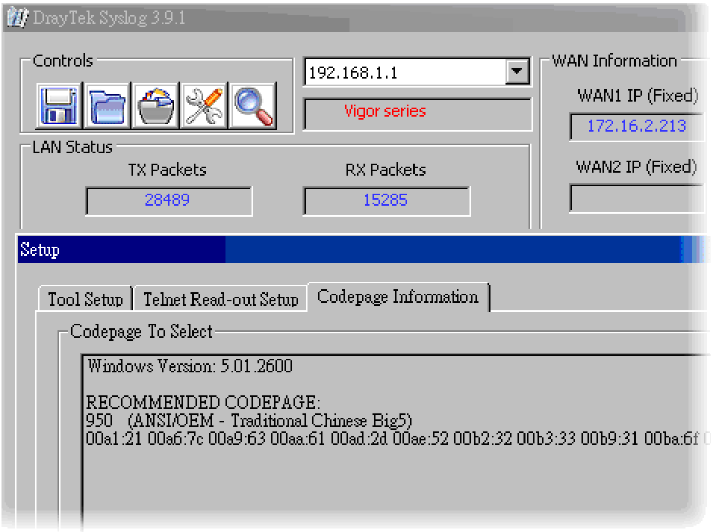
Codepage: ANSI(1252)-Latin I

Window size: 65535

Session timeout: 1440 Minute

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system 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.



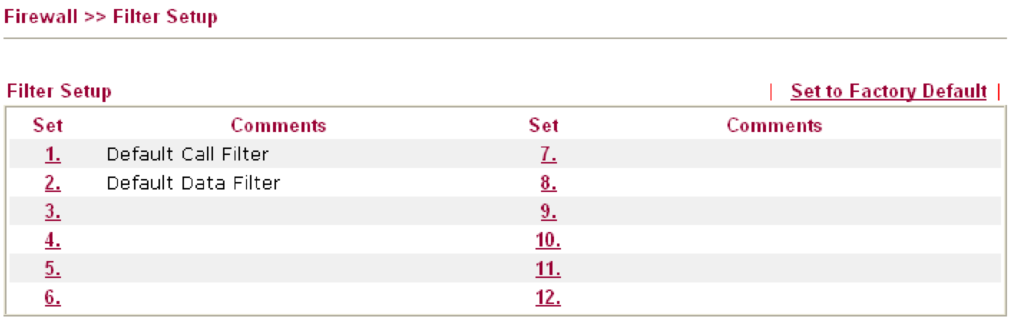
```
Windows Version: 5.01.2600

RECOMMENDED CODEPAGE:
950   (ANSI/OEM - Traditional Chinese Big5)
00a1:21 00a6:7c 00a9:63 00aa:61 00ad:2d 00ae:52 00b2:32 00b3:33 00b9:31 00ba:6f
```

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.

4.4.3 Filter Setup

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

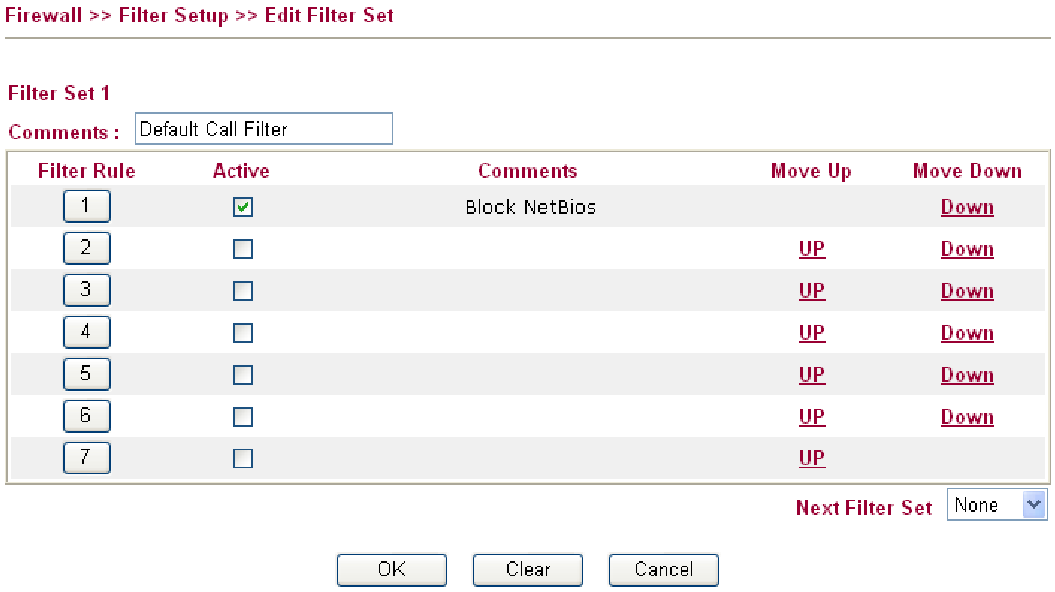


Firewall >> Filter Setup

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

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.

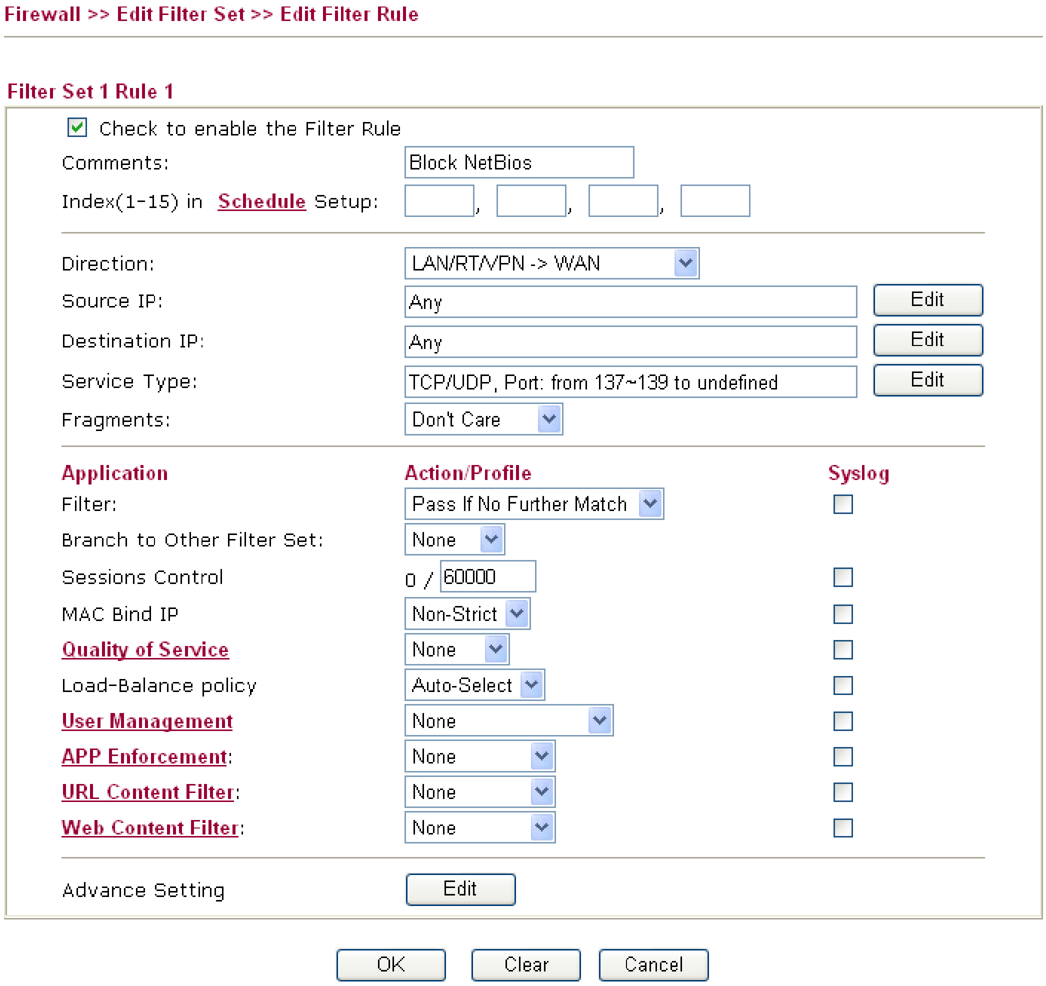
Active Enable or disable the filter rule.

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 1 Rule 1

☑ Check to enable the Filter Rule

Comments:	Block NetBios	
Index(1-15) in Schedule Setup:	, , ,	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to undefined	Edit
Fragments:	Don't Care	

Application	Action/Profile	Syslog
Filter:	Pass If No Further Match	□
Branch to Other Filter Set:	None	
Sessions Control	0 / 60000	□
MAC Bind IP	Non-Strict	□
Quality of Service	None	□
Load-Balance policy	Auto-Select	□
User Management	None	□
APP Enforcement:	None	□
URL Content Filter:	None	□
Web Content Filter:	None	□

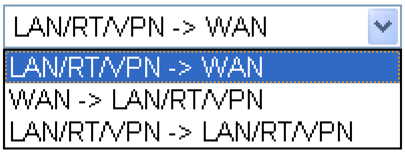
Advance Setting Edit

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.

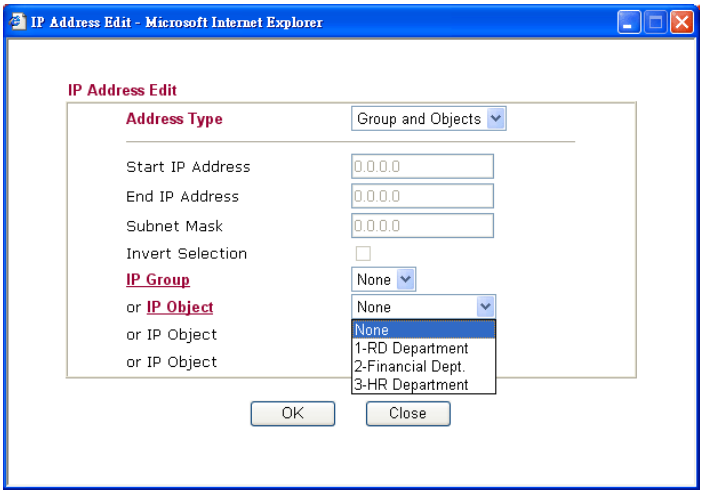
Index(1-15) Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this field is blank and the function will always work.

Direction Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.



Note: RT means routing domain for 2nd subnet or other LAN.

Source/Destination IP Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.



IP Address Edit - Microsoft Internet Explorer

IP Address Edit

Address Type: Group and Objects

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Invert Selection: □

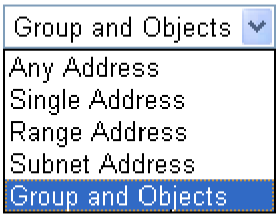
IP Group: None

or IP Object: None

or IP Object

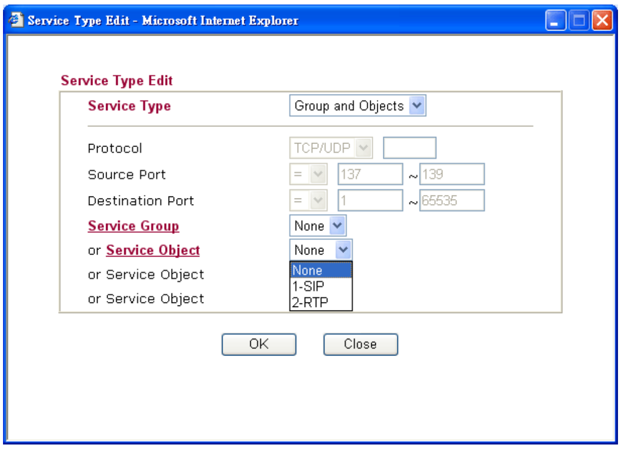
or IP Object

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.



Service Type Edit - Microsoft Internet Explorer

Service Type Edit

Service Type: Group and Objects

Protocol: TCP/UDP

Source Port: = 137 ~ 139

Destination Port: = 1 ~ 65535

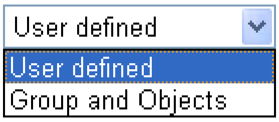
Service Group: None

or Service Object: None

or Service Object

or Service Object

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



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

Source/Destination Port –

(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.

(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

(<) – the port number less than this value is available for this profile.

Service Group/Object - Use the drop down list to choose the one that you want.

Fragments

Specify the action for fragmented packets. And it is used for **Data Filter** only.

Don't care -No action will be taken towards fragmented packets.

Unfragmented -Apply the rule to unfragmented packets.

Fragmented - Apply the rule to fragmented packets.

Too Short - Apply the rule only to packets that are too short to contain a complete header.

Filter

Specifies the action to be taken when packets match the rule.

Block Immediately - Packets matching the rule will be dropped immediately.

Pass Immediately - Packets matching the rule will be passed immediately.

Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.

Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter Set

If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.

Sessions Control

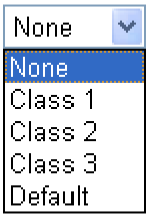
The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.

MAC Bind IP

Strict – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP** be bound for applying such filter rule.

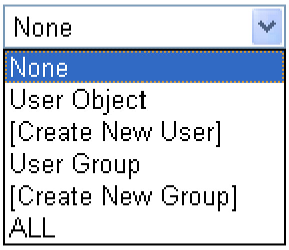
No-Strict - no limitation.

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.



Load-Balance policy Choose the WAN interface for applying Load-Balance Policy.

User Management Such item is available only when **Rule-Based** is selected in User **Management>>General Setup**. The general firewall rule will be applied to the user/user group/all users specified here.



> **Note:** When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.

APP Enforcement Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

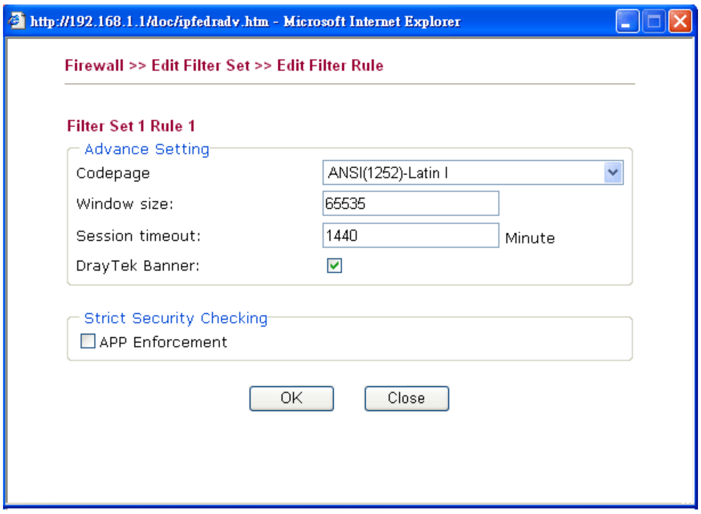
URL Content Filter Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web**

Content Filter web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

Advance Setting

Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.



http://192.168.1.1/doc/ipfedradv.htm - Microsoft Internet Explorer

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Advance Setting

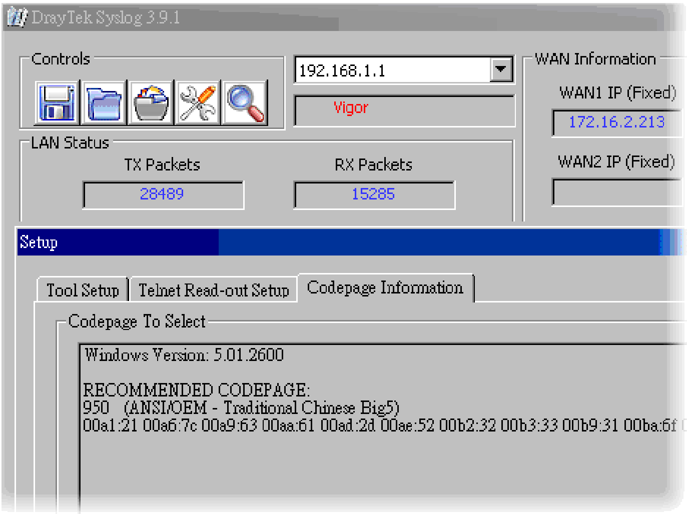
Codepage	ANSI(1252)-Latin I
Window size:	65535
Session timeout:	1440 Minute
DrayTek Banner:	☑

Strict Security Checking

☐ APP Enforcement

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.



DrayTek Syslog 3.9.1

Controls: 192.168.1.1 — Vigor

WAN Information: WAN1 IP (Fixed) 172.16.2.213; WAN2 IP (Fixed)

LAN Status: TX Packets 28489; RX Packets 15285

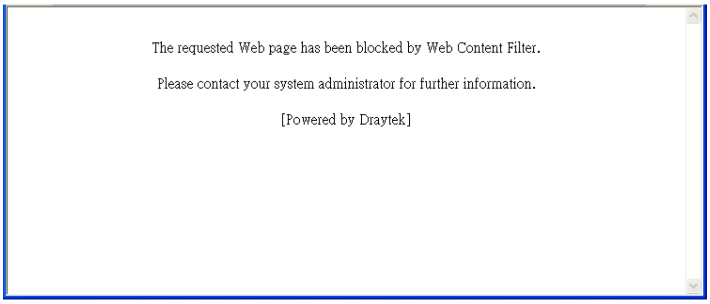
Setup

```
Windows Version: 5.01.2600

RECOMMENDED CODEPAGE:
950   (ANSI/OEM - Traditional Chinese Big5)
00a1:21 00a6:7c 00a9:63 00aa:61 00ad:2d 00ae:52 00b2:32 00b3:33 00b9:31 00ba:6f
```

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.

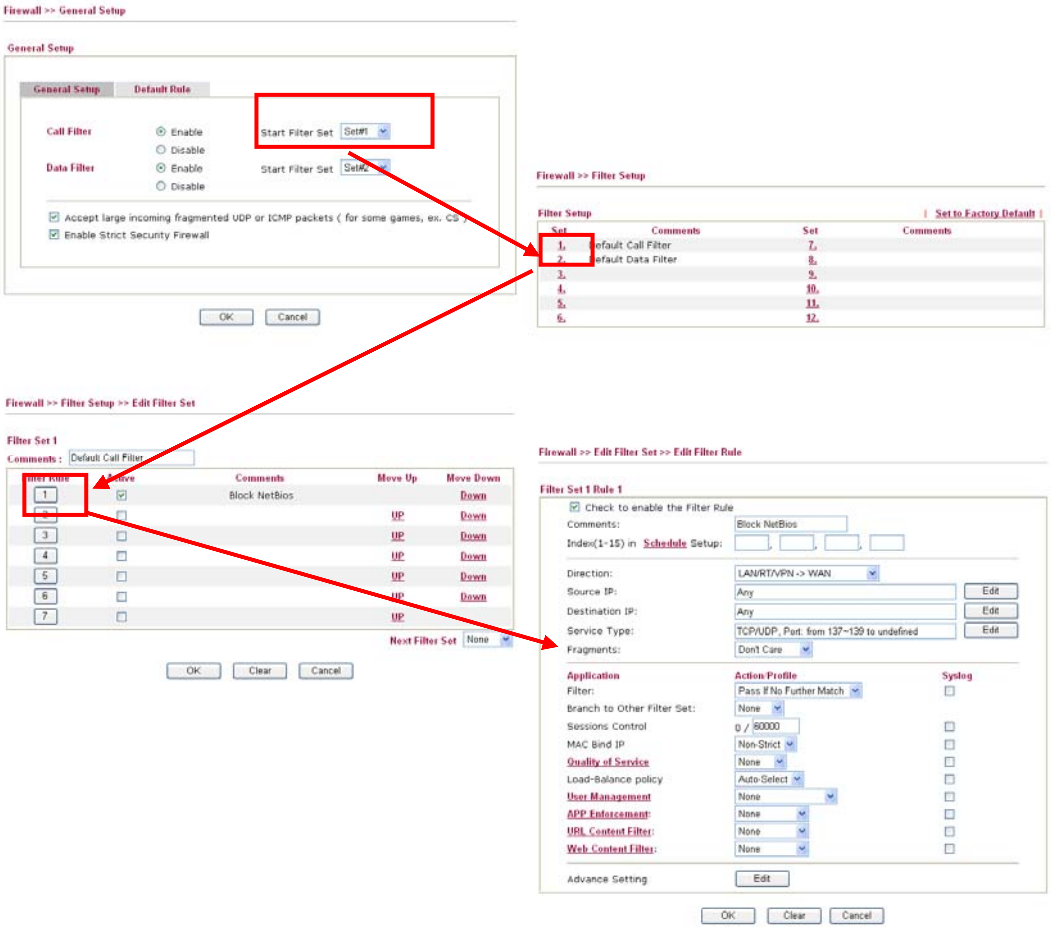
Please contact your system administrator for further information.

[Powered by Draytek]

Strict Security Checking - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.

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.



Firewall >> General Setup

General Setup

Call Filter ● Enable ○ Disable — Start Filter Set: Set#1

Data Filter ● Enable ○ Disable — Start Filter Set: Set#2

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

☑ Enable Strict Security Firewall

Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☑ Check to enable the Filter Rule

Comments: Block NetBios

Index(1-15) in Schedule Setup:

Direction: LAN/RT/VPN -> WAN

Source IP: Any

Destination IP: Any

Service Type: TCP/UDP, Port: from 137~139 to undefined

Fragments: Don't Care

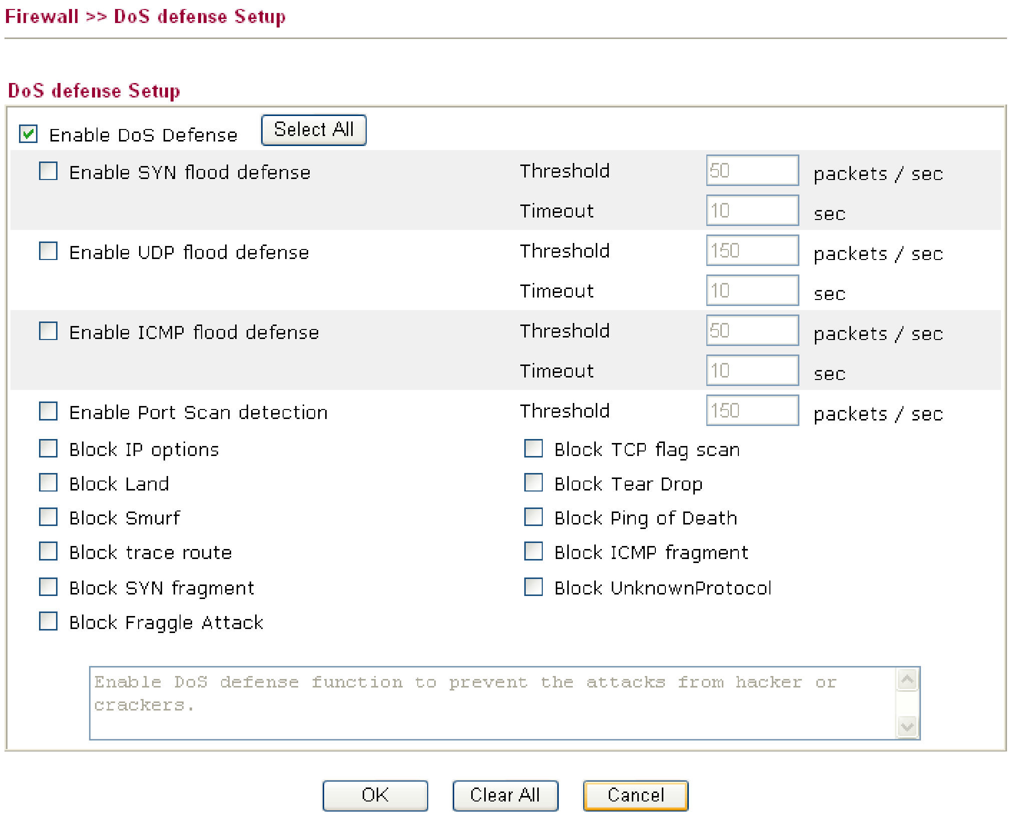
Application	Action/Profile	Syslog
Filter:	Pass If No Further Match	□
Branch to Other Filter Set:	None	
Sessions Control	0 / 60000	□
MAC Bind IP	Non-Strict	□
Quality of Service	None	□
Load-Balance policy	Auto-Select	□
User Management	None	□
APP Enforcement:	None	□
URL Content Filter:	None	□
Web Content Filter:	None	□

Advance Setting

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.



Firewall >> DoS defense Setup

DoS defense Setup

☑ Enable DoS Defense [Select All]

□ Enable SYN flood defense	Threshold	50	packets / sec
	Timeout	10	sec
□ Enable UDP flood defense	Threshold	150	packets / sec
	Timeout	10	sec
□ Enable ICMP flood defense	Threshold	50	packets / sec
	Timeout	10	sec
□ Enable Port Scan detection	Threshold	150	packets / sec

□ Block IP options	□ Block TCP flag scan
□ Block Land	□ Block Tear Drop
□ Block Smurf	□ Block Ping of Death
□ Block trace route	□ Block ICMP fragment
□ Block SYN fragment	□ Block UnknownProtocol
□ Block Fraggle Attack	

Enable DoS defense function to prevent the attacks from hacker or crackers.

[OK] [Clear All] [Cancel]

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 50 packets per second and 10 seconds, respectively.

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 150 packets per second and 10 seconds, respectively.

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 50 packets per second and 10 seconds, respectively.

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 150 packets per second.

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 router
Check the box to enforce the Vigor router not to forward any trace route packets.

Block SYN fragment
Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.

Block Fraggle Attack
Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.

Block TCP flag scan
Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.

Block Tear Drop
Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.

Block Ping of Death
Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang

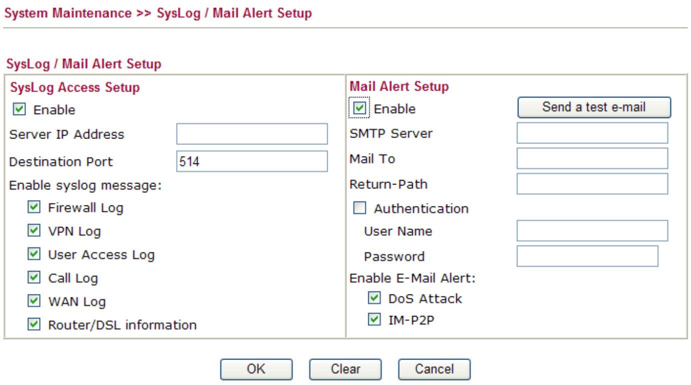
once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.

Block ICMP Fragment Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

Block Unknown Protocol Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.

Warning Messages We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.

All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.



System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup

☑ Enable

Server IP Address

Destination Port: 514

Enable syslog message:

- ☑ Firewall Log
- ☑ VPN Log
- ☑ User Access Log
- ☑ Call Log
- ☑ WAN Log
- ☑ Router/DSL information

Mail Alert Setup

☑ Enable

SMTP Server

Mail To

Return-Path

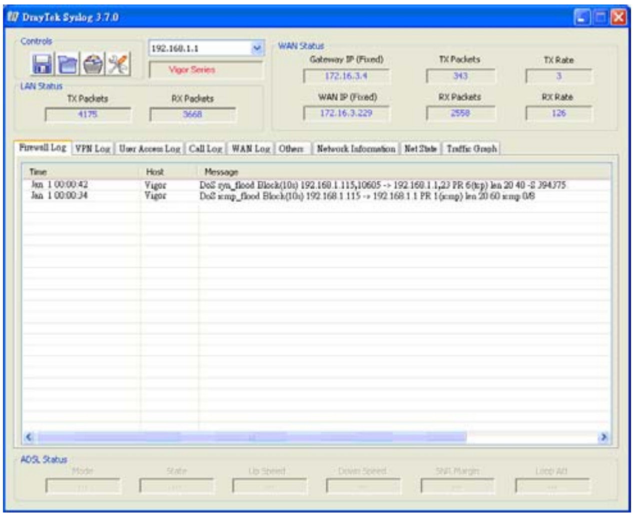
☐ Authentication

User Name

Password

Enable E-Mail Alert:

- ☑ DoS Attack
- ☑ IM-P2P



DrayTek Syslog 3.7.0

Controls: 192.168.1.1 — Vigor Series

LAN Status: TX Packets 4175, RX Packets 3668

WAN Status: Gateway IP (Fixed) 172.16.3.4, TX Packets 343, TX Rate 3, WAN IP (Fixed) 172.16.3.229, RX Packets 2558, RX Rate 126

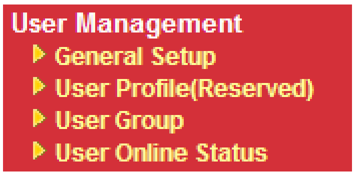
```
Time              Host    Message
Jan 1 00:00:42    Vigor   DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 394375
Jan 1 00:00:34    Vigor   DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8
```

4.5 User Management

User Management is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password. Instead of managing with IP address/MAC address, User Management function manages hosts with user account. Network administrator can give different firewall policies or rules for different hosts with different User Management accounts. This is more flexible and convenient for network management. Not only offering the basic checking for Internet access, User Management also provides additional firewall rules, e.g. CSM checking for protecting hosts.

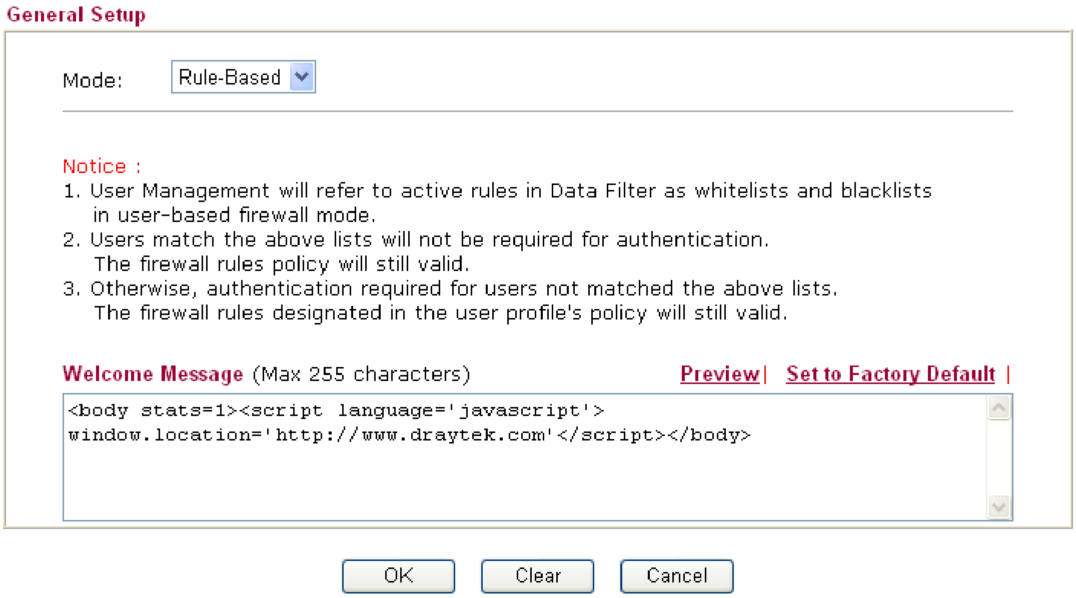
Note: Filter rules configured under Firewall usually are applied to the host (the one that the router installed) only. With user management, the rules can be applied to every user connected to the router with customized profiles.

Note: If **Transparency Mode** is selected in **Firewall>>General Setup**, User Management cannot be used any more. Please uncheck Transparency Mode first if you want to utilize user management to handle users in LAN, WAN or WLAN.



4.5.1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.



General Setup

Mode: Rule-Based

Notice :
1. User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode.
2. Users match the above lists will not be required for authentication. The firewall rules policy will still valid.
3. Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid.

Welcome Message (Max 255 characters)

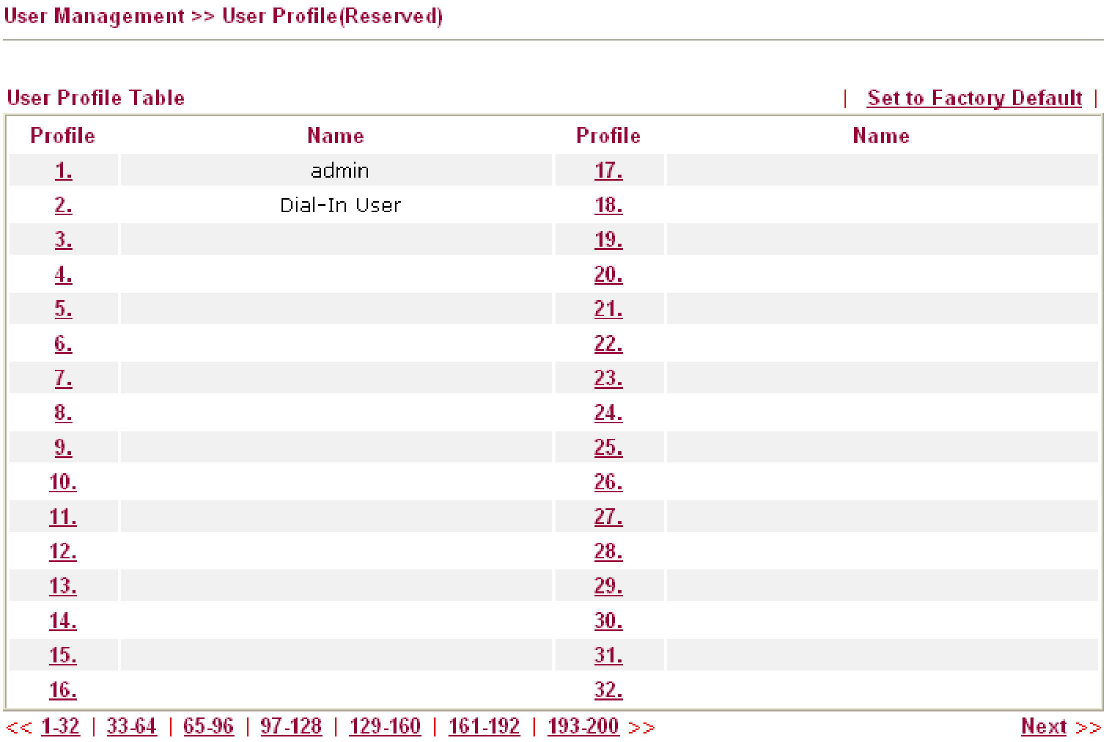
```
<body stats=1><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

Mode	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved. **User-Based -** If you choose such mode, the router will apply the filter rules configured in **User Management>>User Profile** to the users. **Rule-Based** –If you choose such mode, the router will apply

the filter rules configured in **Firewall>>General Setup** and **Filter Rule** to the users.

4.5.2 User Profile (Reserved)

This page allows you to set customized profiles (up to 200) which will be applied for users controlled under **User Management**. Simply open **User Management>>User Profile (Reserved)**.



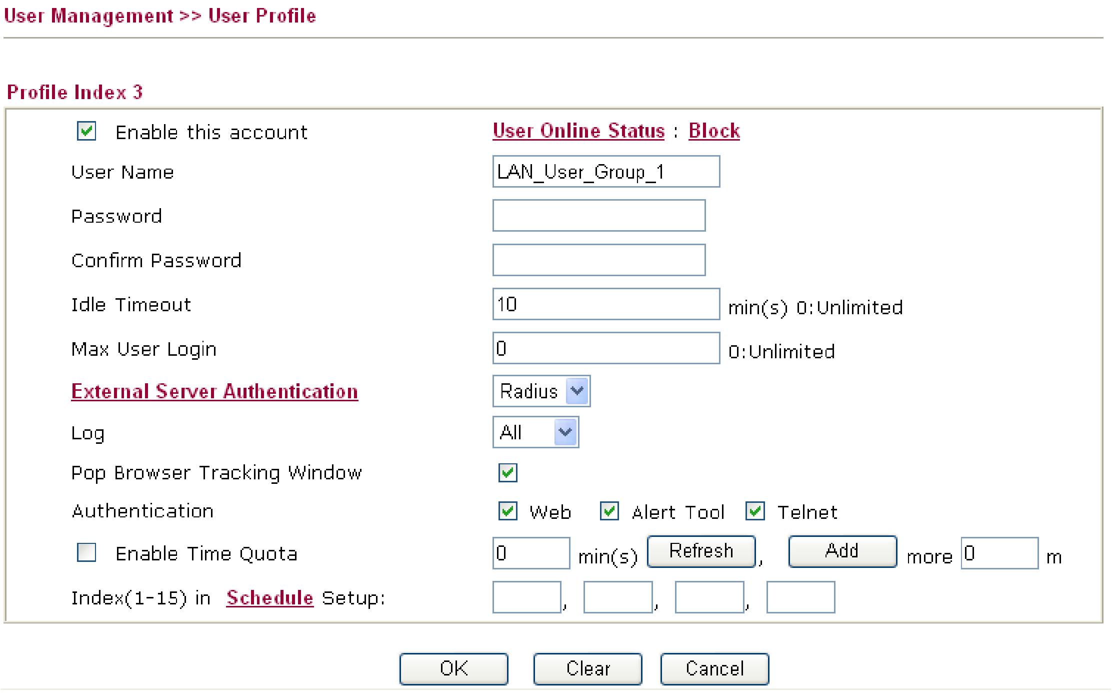
User Management >> User Profile(Reserved)

User Profile Table | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> Next >>

To set the user profile, please click any index number link to open the following page. Notice that profile 1 (Admin) and profile 2 (Dial-In User) are factory default settings and only few settings for them can be modified.



User Management >> User Profile

Profile Index 3

☑ Enable this account	User Online Status : Block
User Name	LAN_User_Group_1
Password	
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	Radius
Log	All
Pop Browser Tracking Window	☑
Authentication	☑ Web ☑ Alert Tool ☑ Telnet
☐ Enable Time Quota	0 min(s) Refresh , Add more 0 m
Index(1-15) in Schedule Setup:	, , ,

OK Clear Cancel

Enable this account Check this box to enable such user profile.

User Name Type a name for such user profile (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the User Name specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.

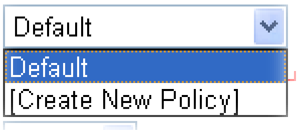
Password Type a password for such profile (e.g., *lug123*, *wug123*,*wug456*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.

Confirm Password Type the password again for confirmation.

Idle Timeout If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 10 minutes.

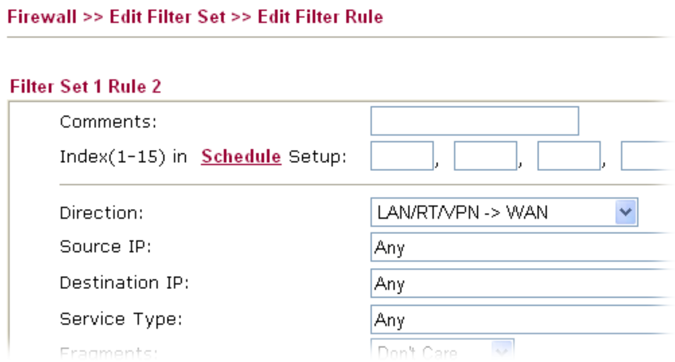
Max User Login Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.

Policy It is available only when **User-Based** mode selected in **User Management>>General Setup**.



Default – If you choose such item, the filter rules pre-configured in **Firewall** can be adopted for such user profile.

Create New Policy – If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.



Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 2

Comments:

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

Direction: LAN/RT/VPN -> WAN

Source IP: Any

Destination IP: Any

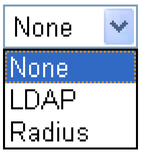
Service Type: Any

Fragments: Don't Care

For the detailed configuration, simply refer to **Firewall>>Filter Rule**. The firewall filter rules that are not selected in **Firewall>>General>>Default rule** can be available for use in **User Management>>User Profile**.

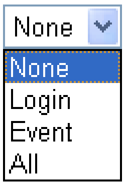
External Service Authentication

The router will authenticate the dial-in user by itself or by external service such as LDAP server or Radius server. If LDAP or Radius is selected here, it is not necessary to configure the password setting above.



Log

Time of login/log out, block/unblock for the user(s) can be sent to and displayed in Syslog. Please choose any one of the log items to take down relational records for the user(s).



Pop Browser Tracking Window

If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.

Authentication

Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.

Web – If it is selected, the use can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a **Welcome Message** (configured in **User Management** >> **General Setup)** will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.

Alert Tool – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site.

Telnet – If it is selected, the user can use Telnet command to perform the authentication job.

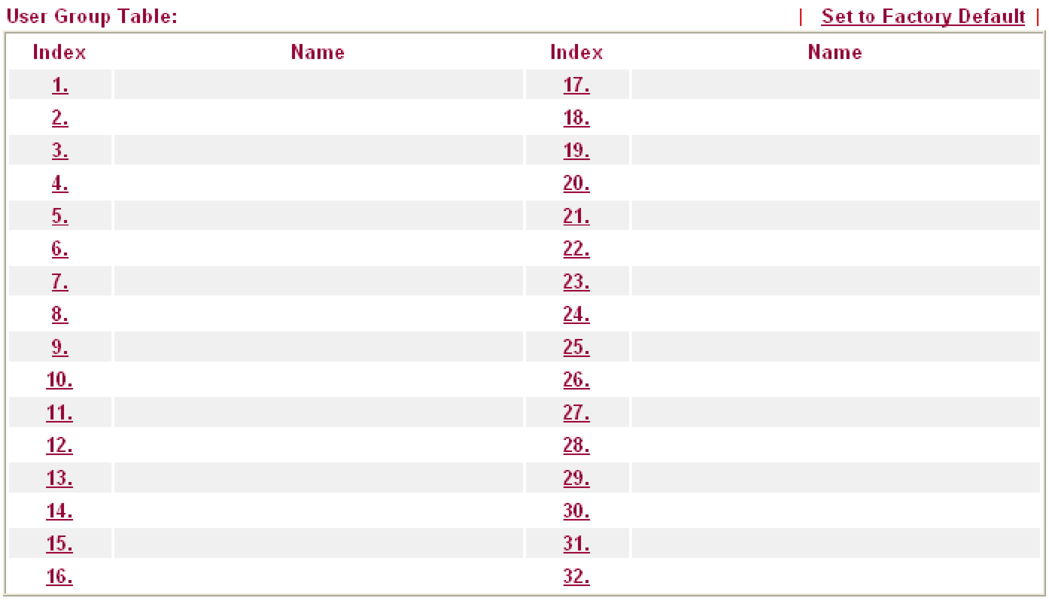
Enable Time Quota

Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet.

	Refresh – Click this button to recalculate the time quota.
	Add – Click this box to set the time quota for such profile.
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.

4.5.3 User Group

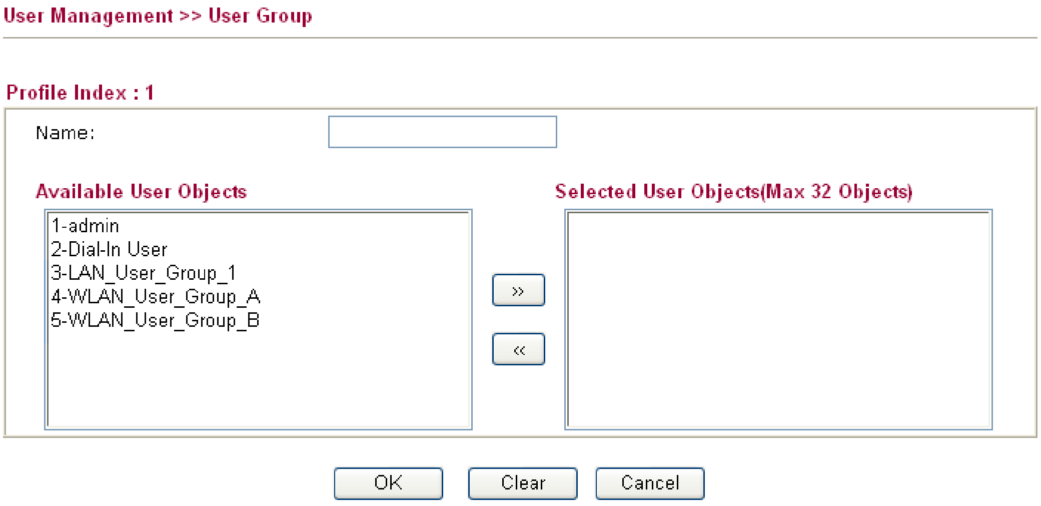
This page allows you to bind several user profiles into one group. These groups will be used in **Firewall>>General Setup** as part of filter rules.



User 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.	

Please click any index number link to open the following page.



User Management >> User Group

Profile Index : 1

Name:

Available User Objects

1-admin
2-Dial-In User
3-LAN_User_Group_1
4-WLAN_User_Group_A
5-WLAN_User_Group_B

Selected User Objects(Max 32 Objects)

Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from **User Profile** page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined

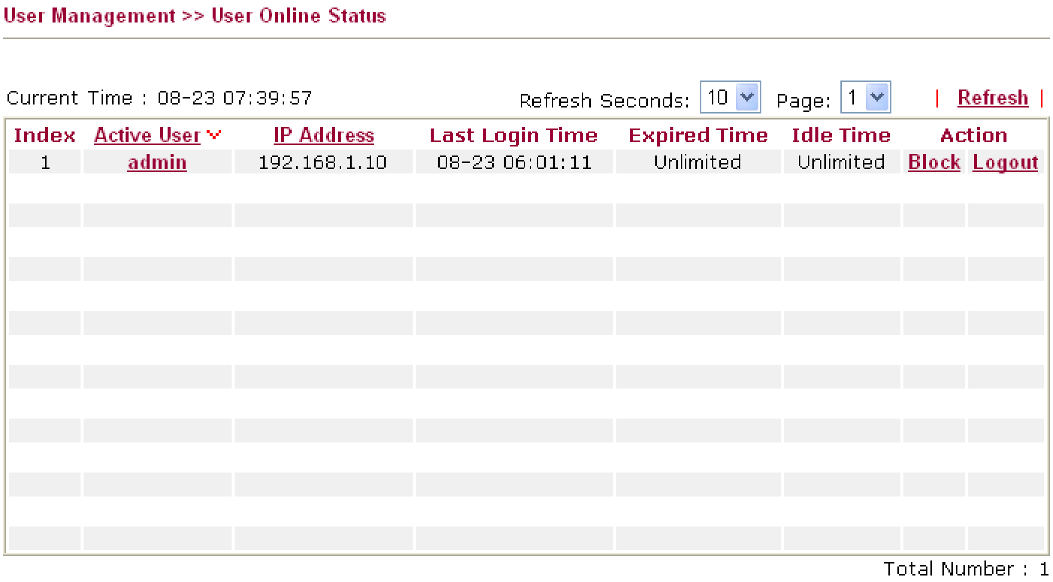
profiles will be numbered with 3, 4, 5 and so on.

Selected Keyword Objects

Click » button to add the selected user objects in this box.

3.5.4 User Online Status

This page displays the user(s) connected to the router and refreshes the connection status in an interval of several seconds.



User Management >> User Online Status

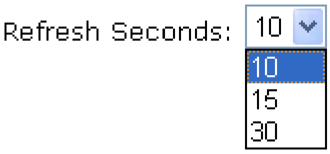
Current Time : 08-23 07:39:57

Refresh Seconds: 10 Page: 1 | Refresh |

Index	Active User	IP Address	Last Login Time	Expired Time	Idle Time	Action
1	admin	192.168.1.10	08-23 06:01:11	Unlimited	Unlimited	Block Logout

Total Number : 1

Refresh Seconds Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.



Refresh Click this link to refresh this page manually.

Index Display the number of the data flow.

Active User Display the users which connect to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.

IP Address Display the IP address of the device.

Last Login Time Display the login time that such user connects to the router last time.

Expired Time Display the expired time of the network connection for the user.

Idle Time Display the idle timeout setting for such profile.

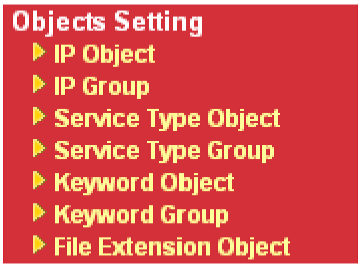
Action **Block -** can prevent specified user accessing into Internet.

Unblock – the user will be blocked.

Logout – the user will be logged out forcefully.

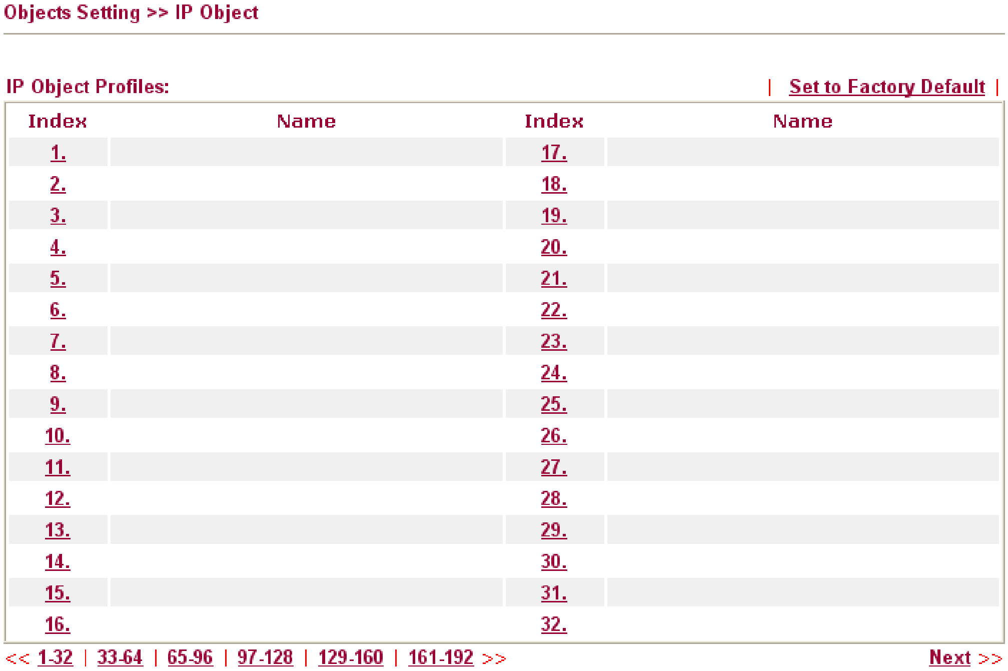
4.6 Objects Settings

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).



4.6.1 IP Object

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



Objects Setting >> IP Object

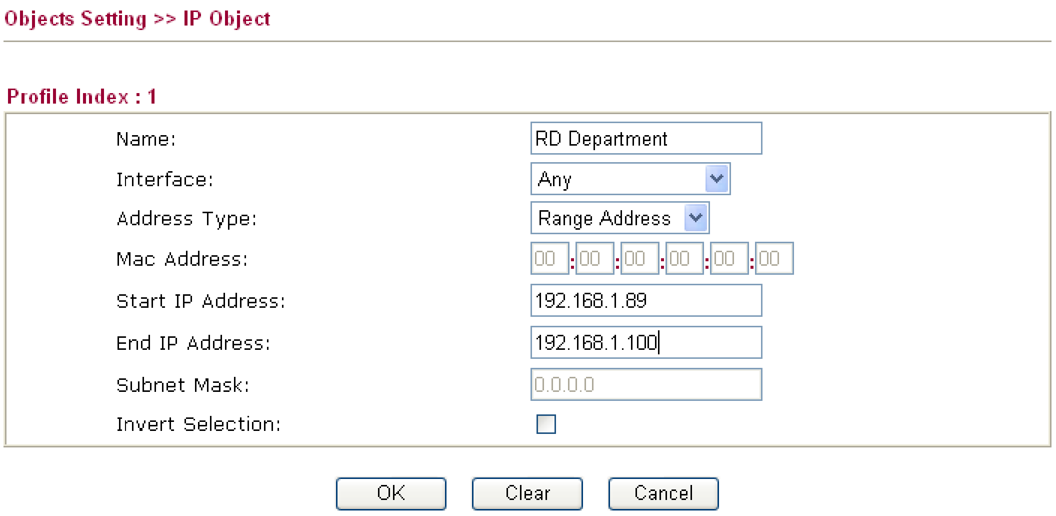
IP Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >> Next >>

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



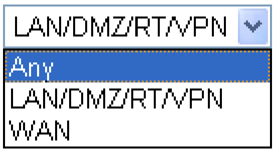
Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.89
End IP Address:	192.168.1.100
Subnet Mask:	0.0.0.0
Invert Selection:	□

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

Interface Choose a proper interface.



For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in **Edit Filter Rule** page.

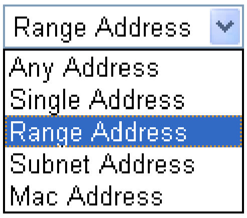
Address Type Determine the address type for the IP address.
Select **Single Address** if this object contains one IP address only.

Select **Range Address** if this object contains several IPs within a range.

Select **Subnet Address** if this object contains one subnet for IP address.

Select **Any Address** if this object contains any IP address.

Select **Mac Address** if this object contains Mac address.



MAC Address Type the MAC address for Mac Address type.

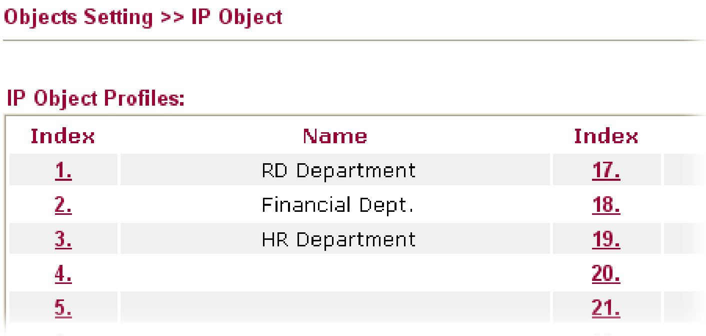
Start IP Address Type the start IP address for Single Address type.

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.

Below is an example of IP objects settings.



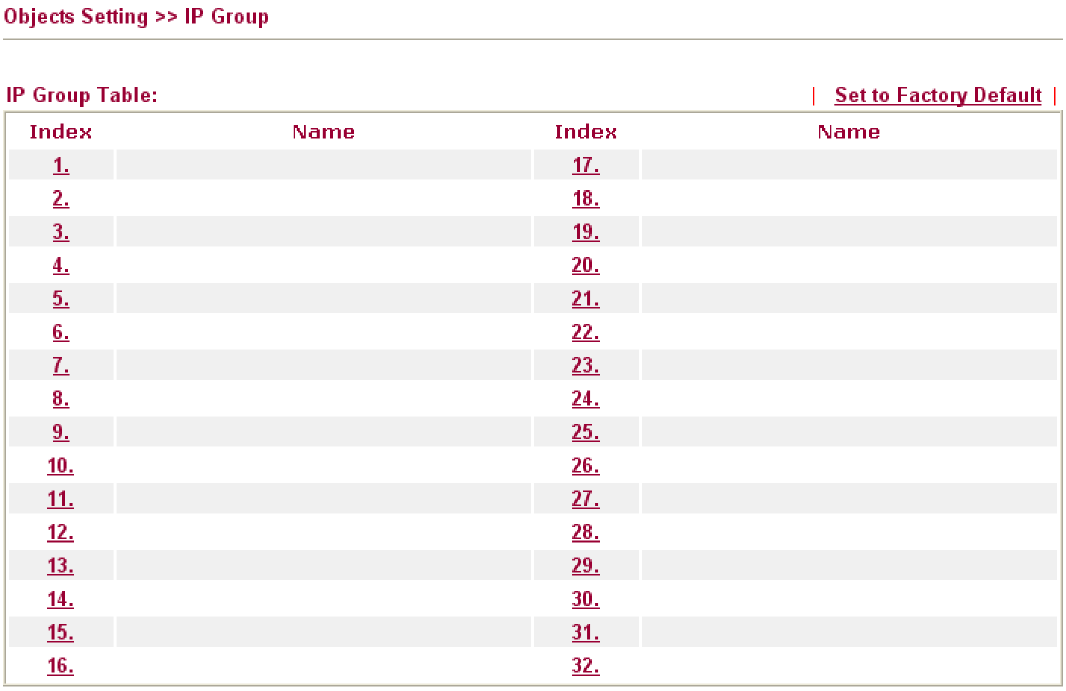
Objects Setting >> IP Object

IP Object Profiles:

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

4.6.2 IP Group

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



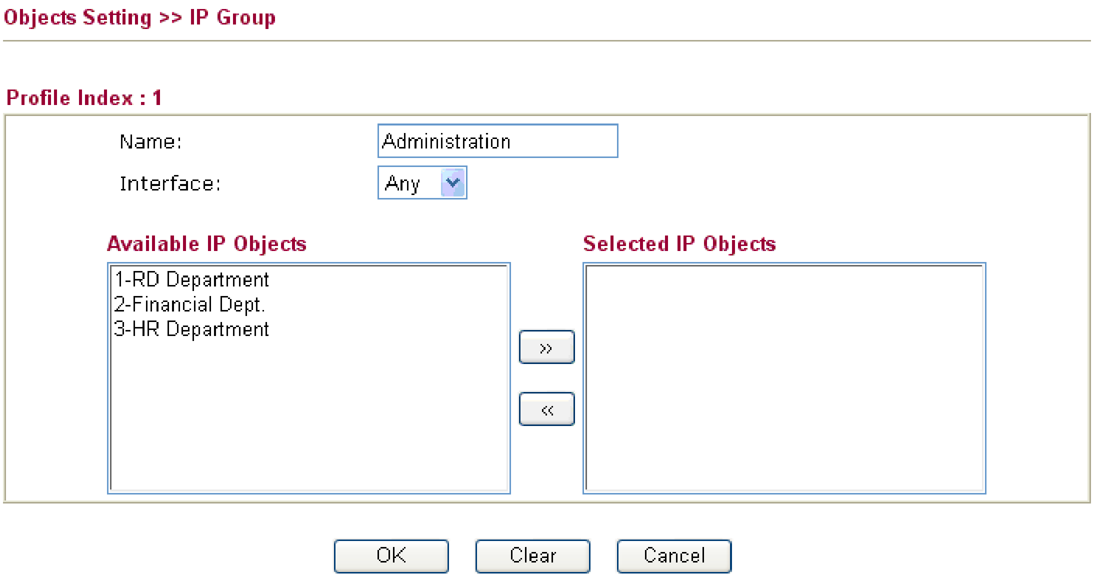
Objects Setting >> IP Group

IP Group Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.


Objects Setting >> IP Group

Profile Index : 1

Name: Administration

Interface: Any

Available IP Objects

1-RD Department
2-Financial Dept.
3-HR Department

Selected IP Objects

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

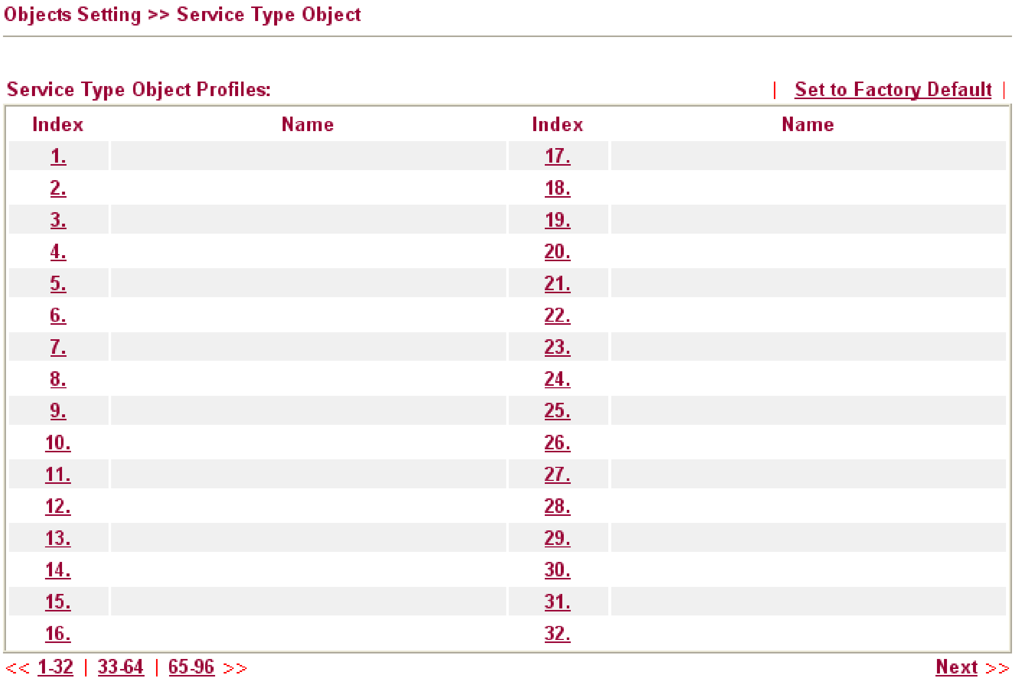
Interface Choose WAN, LAN or Any to display all the available IP objects with the specified interface.

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.

4.6.3 Service Type Object

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



Objects Setting >> Service Type Object

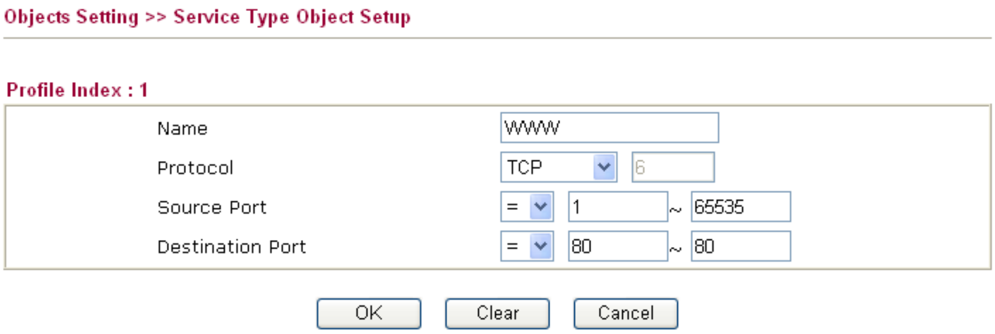
Service Type Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 >> Next >>

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



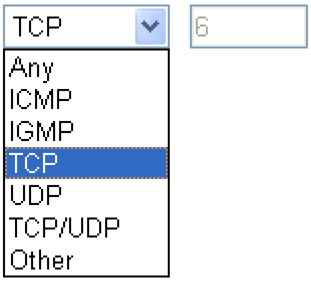
Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	WWW
Protocol	TCP 6
Source Port	= 1 ~ 65535
Destination Port	= 80 ~ 80

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** column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.

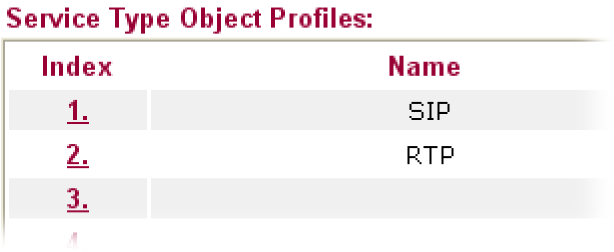
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.

(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

(<) – the port number less than this value is available for this profile.

Below is an example of service type objects settings.

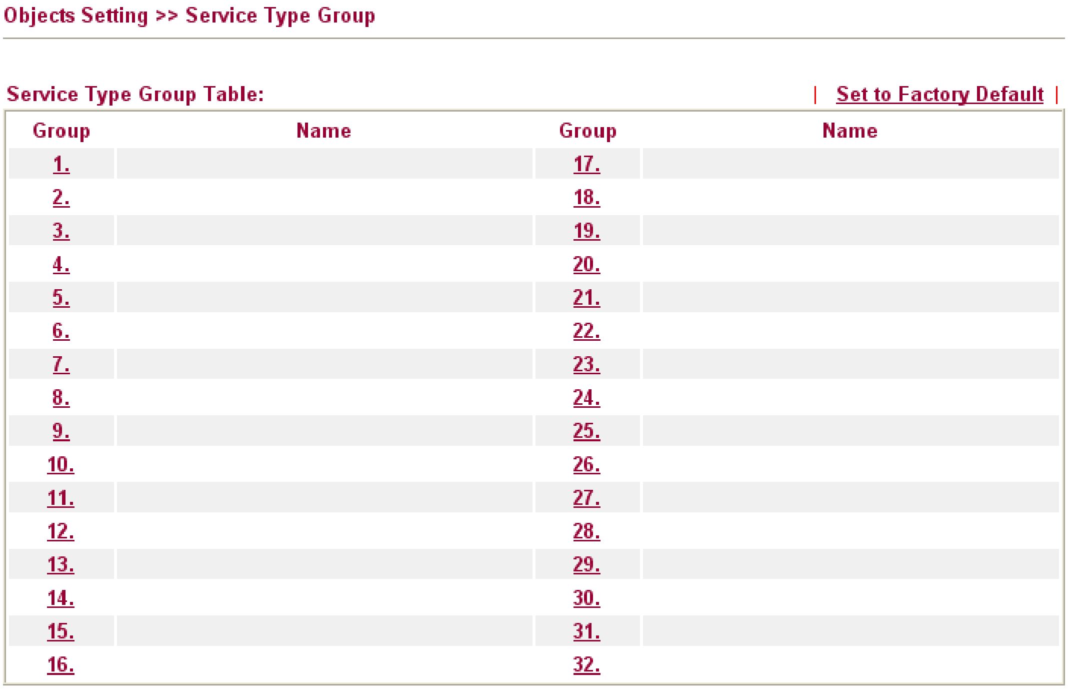


Service Type Object Profiles:

Index	Name
1.	SIP
2.	RTP
3.	
4	

4.6.4 Service Type Group

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



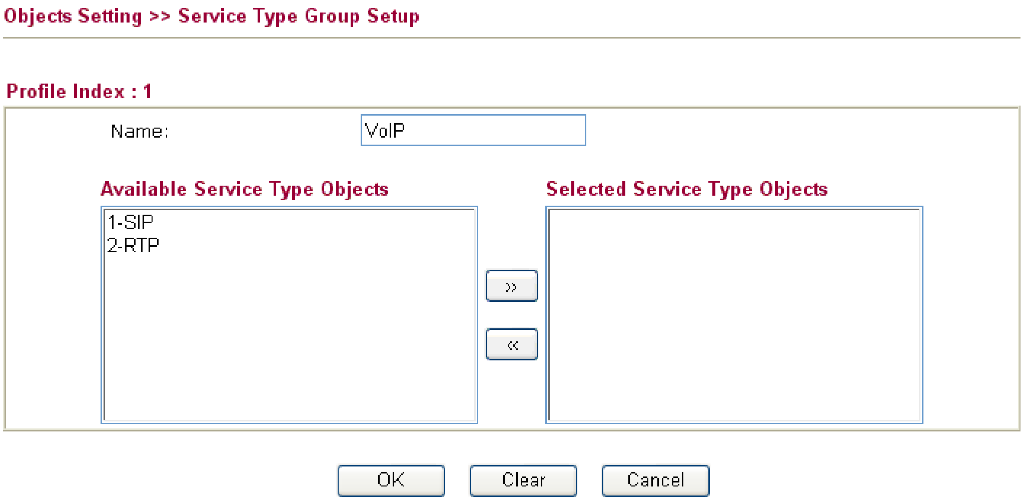
Objects Setting >> Service Type Group

Service Type Group Table:

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.	

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Objects Setting >> Service Type Group Setup

Profile Index : 1

Name: VoIP

Available Service Type Objects: 1-SIP, 2-RTP

Selected Service Type Objects

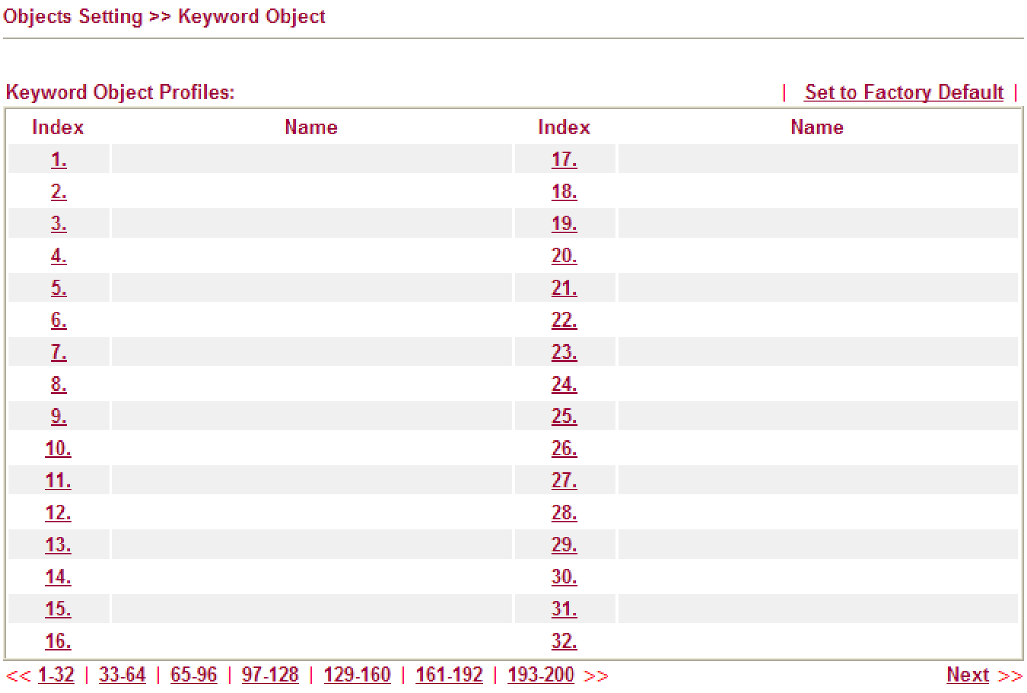
Name Type a name for this profile.

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.

4.6.5 Keyword Object

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



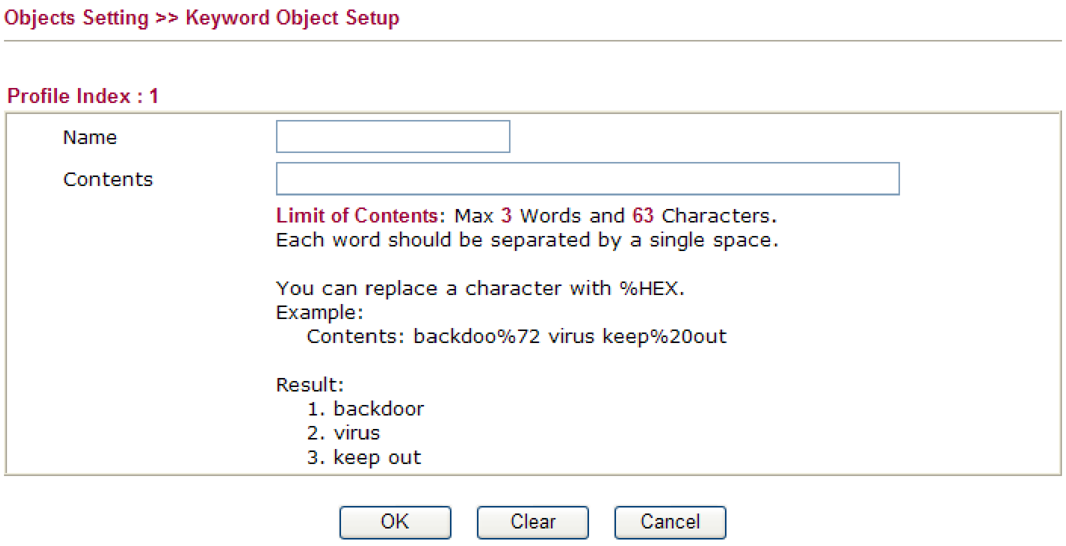
Objects Setting >> Keyword Object

Keyword Object Profiles: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



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

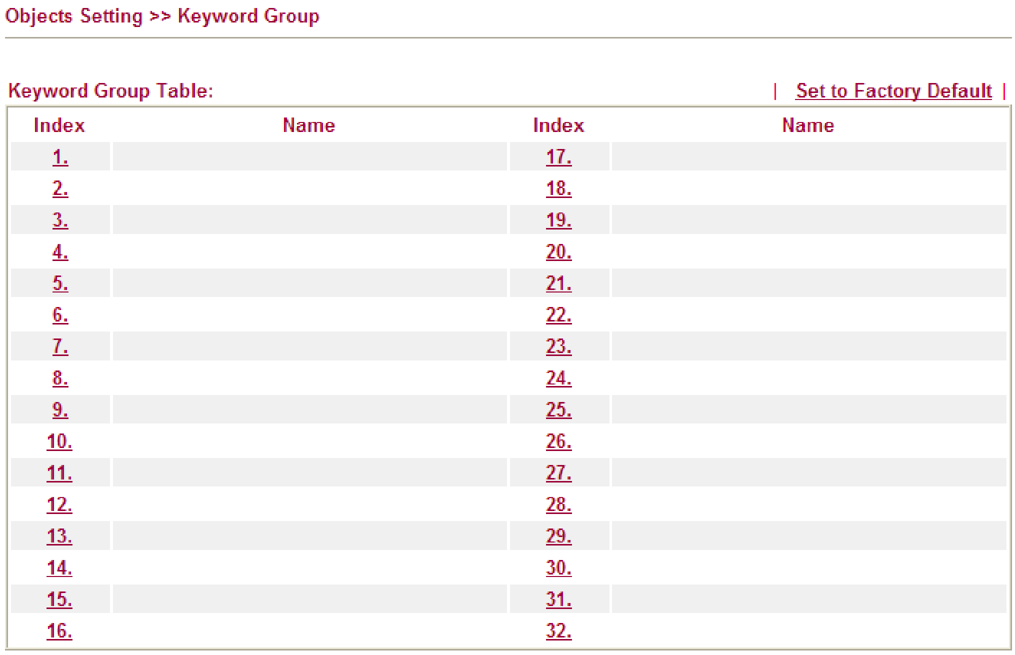
Result:
    1. backdoor
    2. virus
    3. keep out

Name 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.

4.6.6 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**.



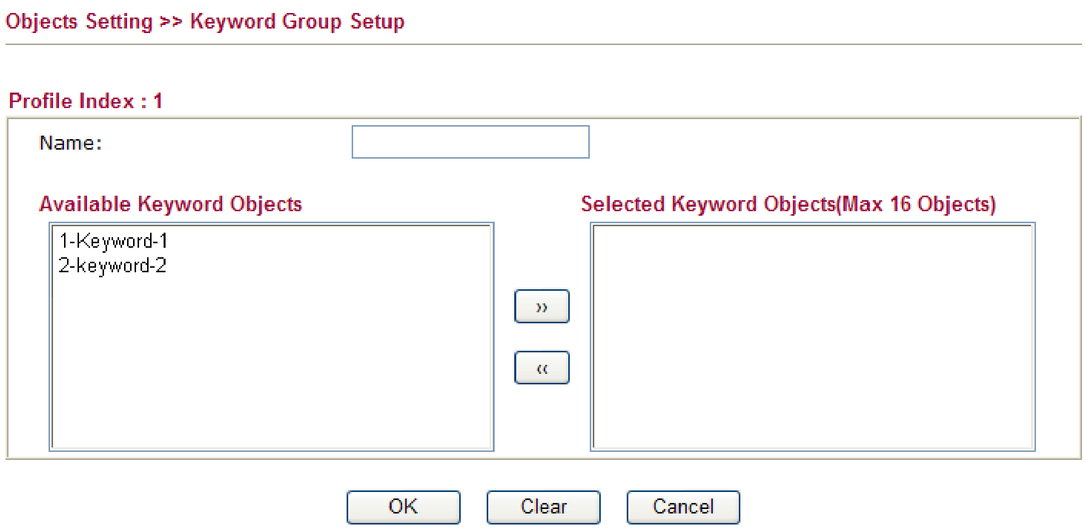
Objects Setting >> Keyword Group

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.	

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects

1-Keyword-1
2-keyword-2

Selected Keyword Objects(Max 16 Objects)

Name Type a name for this group.

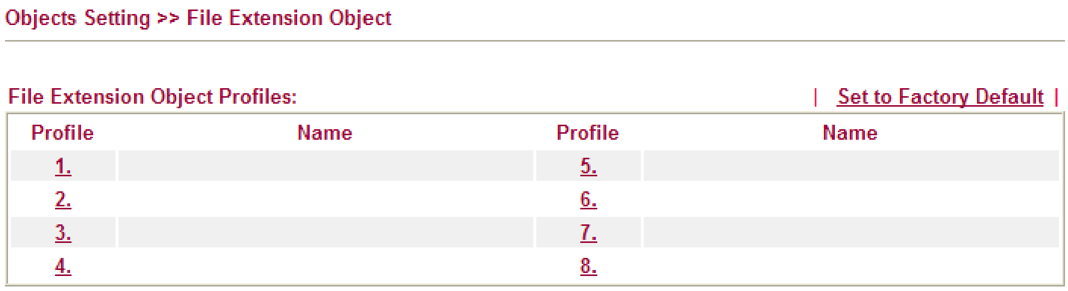
Available Keyword Objects You can gather keyword objects from **Keyword Object** page within one keyword group. All the available Keyword objects that you have created will be shown in this box.

Selected Keyword Objects Click >> button to add the selected Keyword objects in this box.

4.6.7 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.

Profile 1 with name of “default” is the default profile, some files with the file extensions specified in this profile will be ignored and not be scanned by Vigor router.



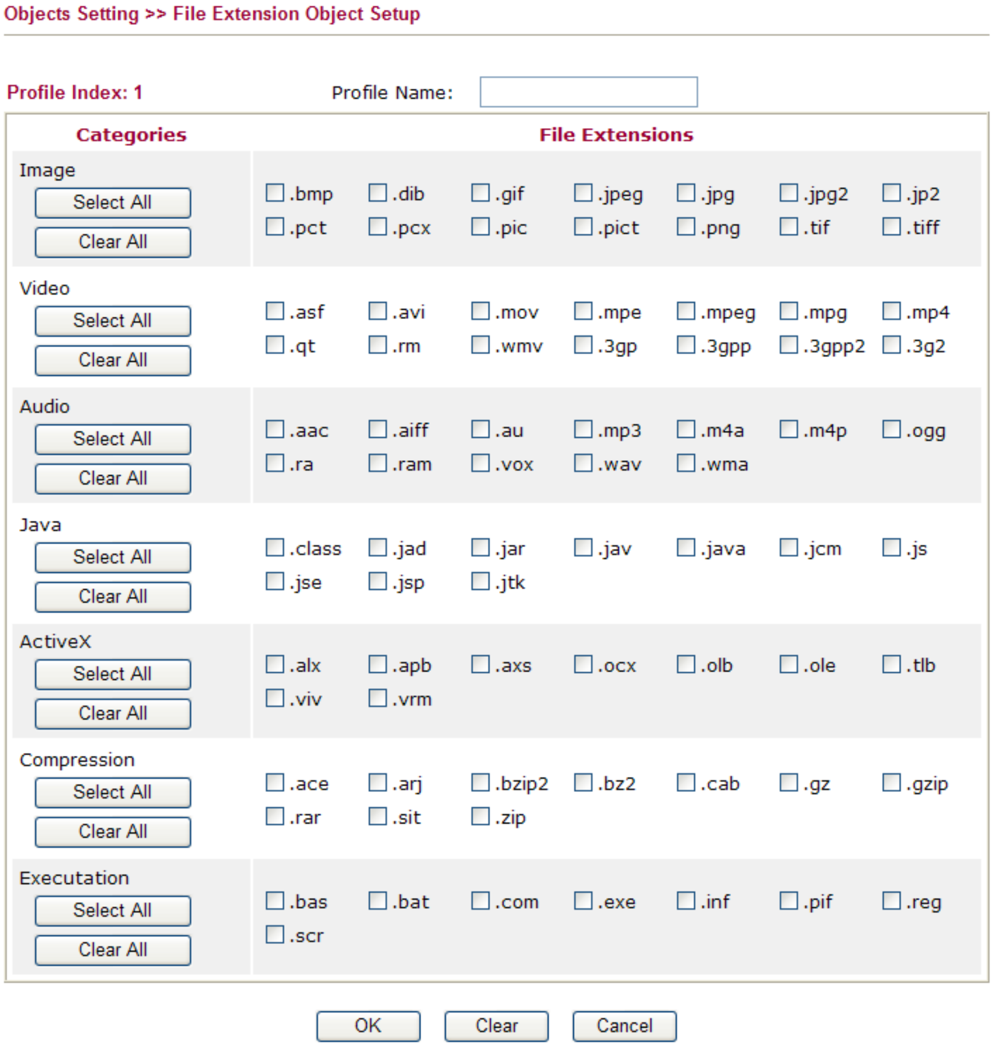
Objects Setting >> File Extension Object

File Extension Object Profiles: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details.



Objects Setting >> File Extension Object Setup

Profile Index: 1

Profile Name:

Categories	File Extensions						
Image Select All Clear All	□ .bmp □ .pct	□ .dib □ .pcx	□ .gif □ .pic	□ .jpeg □ .pict	□ .jpg □ .png	□ .jpg2 □ .tif	□ .jp2 □ .tiff
Video Select All Clear All	□ .asf □ .qt	□ .avi □ .rm	□ .mov □ .wmv	□ .mpe □ .3gp	□ .mpeg □ .3gpp	□ .mpg □ .3gpp2	□ .mp4 □ .3g2
Audio Select All Clear All	□ .aac □ .ra	□ .aiff □ .ram	□ .au □ .vox	□ .mp3 □ .wav	□ .m4a □ .wma	□ .m4p	□ .ogg
Java Select All Clear All	□ .class □ .jse	□ .jad □ .jsp	□ .jar □ .jtk	□ .jav	□ .java	□ .jcm	□ .js
ActiveX Select All Clear All	□ .alx □ .viv	□ .apb □ .vrm	□ .axs	□ .ocx	□ .olb	□ .ole	□ .tlb
Compression Select All Clear All	□ .ace □ .rar	□ .arj □ .sit	□ .bzip2 □ .zip	□ .bz2	□ .cab	□ .gz	□ .gzip
Executation Select All Clear All	□ .bas □ .scr	□ .bat	□ .com	□ .exe	□ .inf	□ .pif	□ .reg

Profile Name Type a name for this profile.

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.

4.7 CSM Profile

Content Security Management (CSM)

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

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 reserve 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.

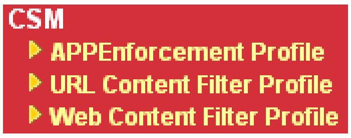
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It’s very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from 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.

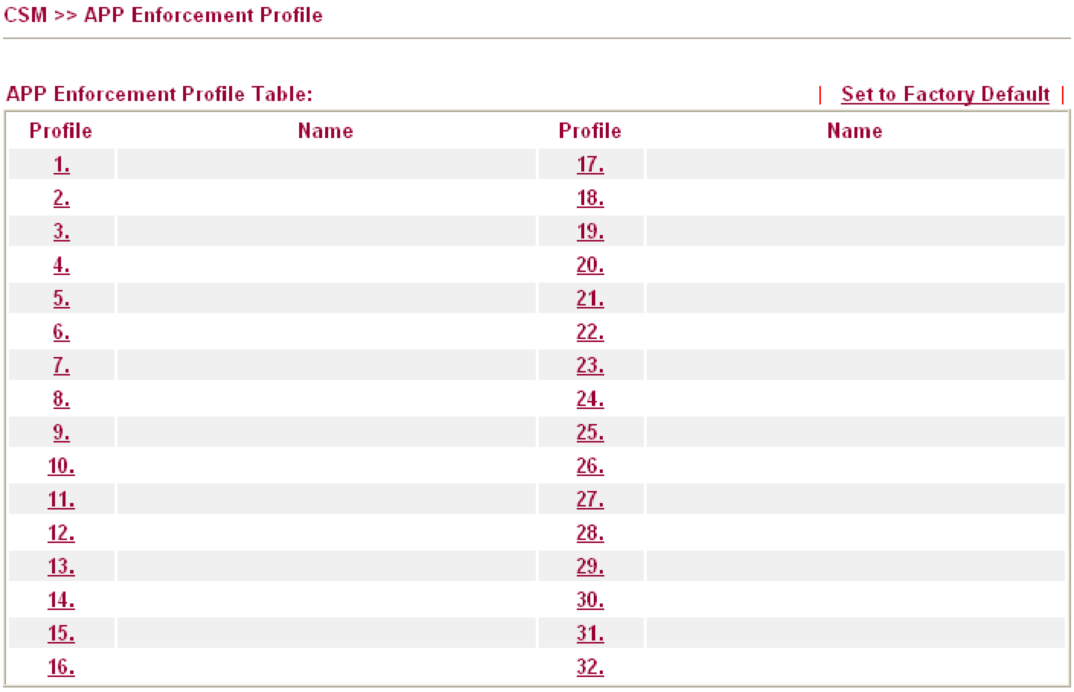
Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. 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.



4.7.1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.



CSM >> APP Enforcement Profile

APP Enforcement Profile Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

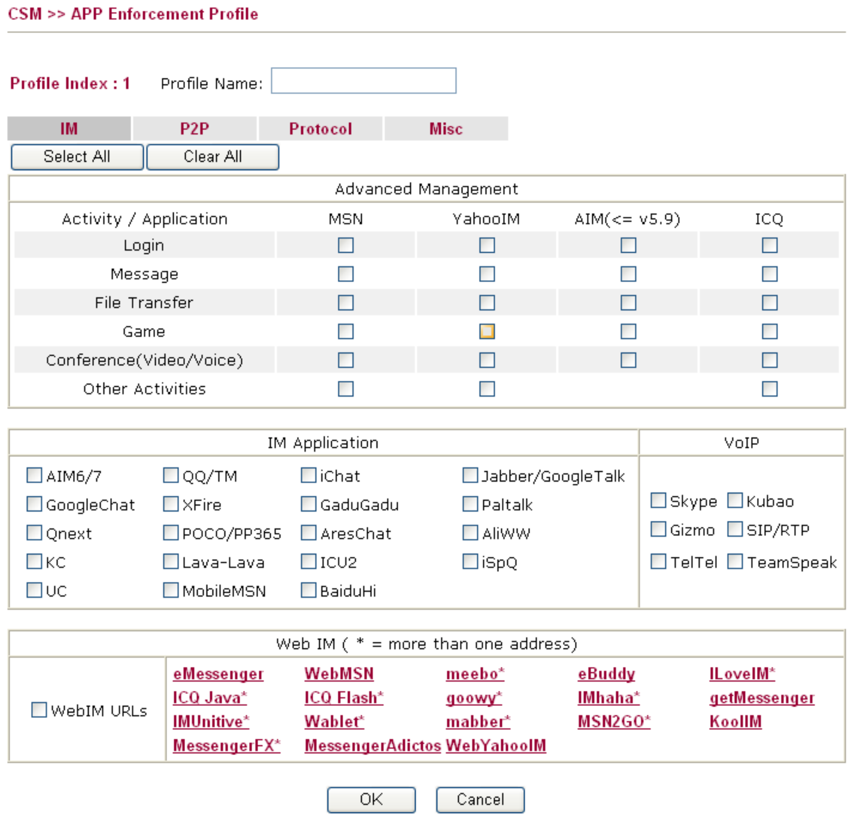
Profile Display the number of the profile which allows you to click to set different policy.

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 Misc 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 **IM**.



CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM | P2P | Protocol | Misc

Select All | Clear All

Advanced Management				
Activity / Application	MSN	YahooIM	AIM(<= v5.9)	ICQ
Login	□	□	□	□
Message	□	□	□	□
File Transfer	□	□	□	□
Game	□	□	□	□
Conference(Video/Voice)	□	□	□	□
Other Activities	□	□		□

IM Application				VoIP	
□ AIM6/7	□ QQ/TM	□ iChat	□ Jabber/GoogleTalk	□ Skype	□ Kubao
□ GoogleChat	□ XFire	□ GaduGadu	□ Paltalk	□ Gizmo	□ SIP/RTP
□ Qnext	□ POCO/PP365	□ AresChat	□ AliWW	□ TelTel	□ TeamSpeak
□ KC	□ Lava-Lava	□ ICU2	□ iSpQ		
□ UC	□ MobileMSN	□ BaiduHi			

Web IM (* = more than one address)					
□ WebIM URLs	eMessenger	WebMSN	meebo*	eBuddy	ILoveIM*
	ICQ Java*	ICQ Flash*	goowy*	IMhaha*	getMessenger
	IMUnitive*	Wablet*	mabber*	MSN2GO*	KoolIM
	MessengerFX*	MessengerAdictos	WebYahooIM		

OK | Cancel

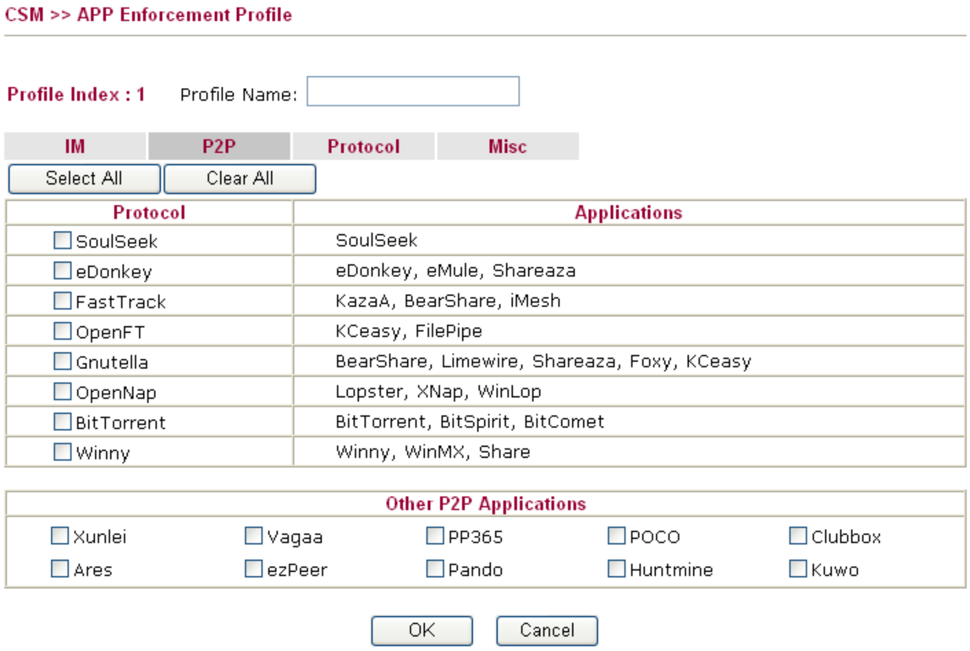
Profile Name Type a name for the CSM profile.

Select All Click it to choose all of the items in this page.

Clear All Uncheck all the selected boxes.

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.

Below shows the items which are categorized under **P2P**.



CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM | P2P | Protocol | Misc

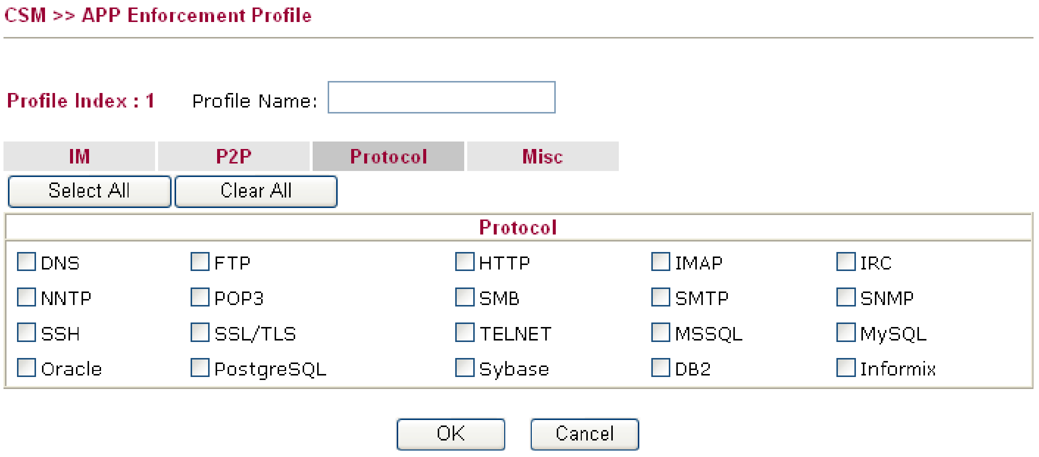
Select All | Clear All

Protocol	Applications
□ SoulSeek	SoulSeek
□ eDonkey	eDonkey, eMule, Shareaza
□ FastTrack	KazaA, BearShare, iMesh
□ OpenFT	KCeasy, FilePipe
□ Gnutella	BearShare, Limewire, Shareaza, Foxy, KCeasy
□ OpenNap	Lopster, XNap, WinLop
□ BitTorrent	BitTorrent, BitSpirit, BitComet
□ Winny	Winny, WinMX, Share

Other P2P Applications				
□ Xunlei	□ Vagaa	□ PP365	□ POCO	□ Clubbox
□ Ares	□ ezPeer	□ Pando	□ Huntmine	□ Kuwo

OK | Cancel

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



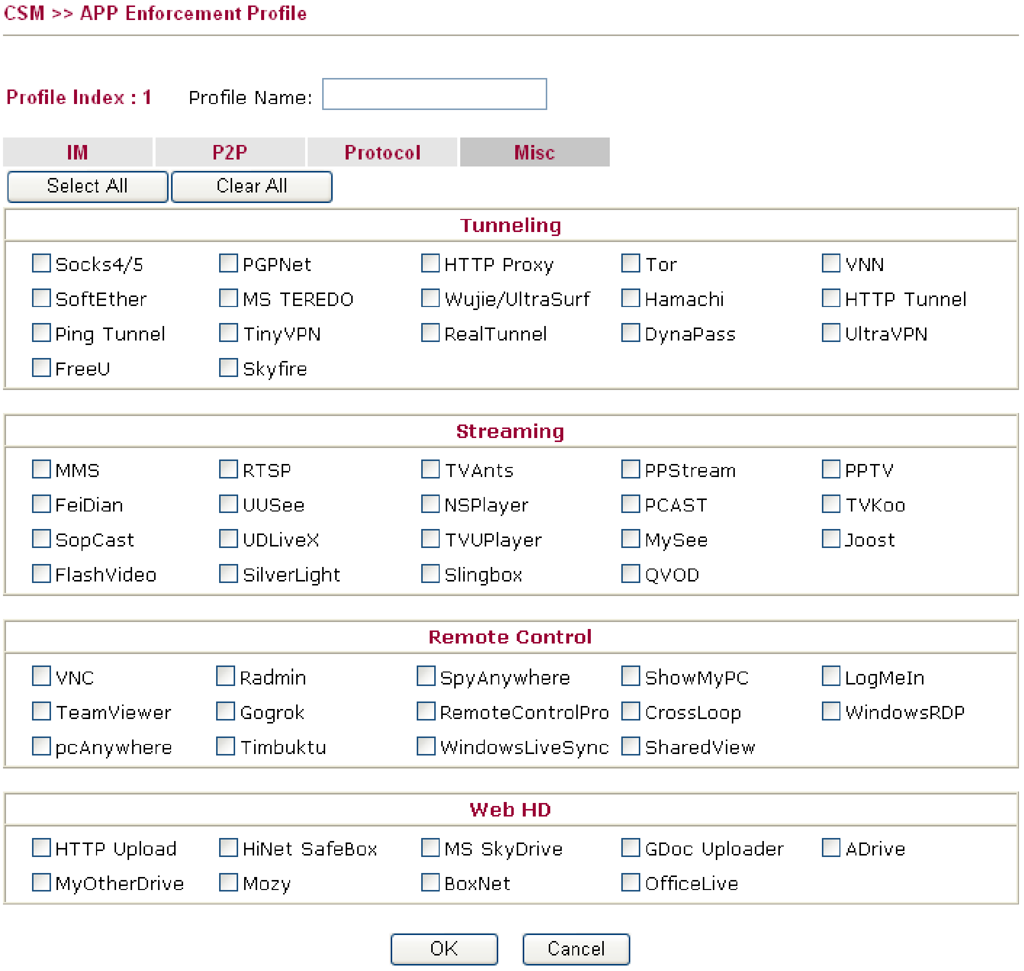
CSM >> APP Enforcement Profile

Profile Index : 1   Profile Name:

Protocol

□ DNS	□ FTP	□ HTTP	□ IMAP	□ IRC
□ NNTP	□ POP3	□ SMB	□ SMTP	□ SNMP
□ SSH	□ SSL/TLS	□ TELNET	□ MSSQL	□ MySQL
□ Oracle	□ PostgreSQL	□ Sybase	□ DB2	□ Informix

The items categorized under **Misc.**



CSM >> APP Enforcement Profile

Profile Index : 1   Profile Name:

Tunneling

□ Socks4/5	□ PGPNet	□ HTTP Proxy	□ Tor	□ VNN
□ SoftEther	□ MS TEREDO	□ Wujie/UltraSurf	□ Hamachi	□ HTTP Tunnel
□ Ping Tunnel	□ TinyVPN	□ RealTunnel	□ DynaPass	□ UltraVPN
□ FreeU	□ Skyfire			

Streaming

□ MMS	□ RTSP	□ TVAnts	□ PPStream	□ PPTV
□ FeiDian	□ UUSee	□ NSPlayer	□ PCAST	□ TVKoo
□ SopCast	□ UDLiveX	□ TVUPlayer	□ MySee	□ Joost
□ FlashVideo	□ SilverLight	□ Slingbox	□ QVOD	

Remote Control

□ VNC	□ Radmin	□ SpyAnywhere	□ ShowMyPC	□ LogMeIn
□ TeamViewer	□ Gogrok	□ RemoteControlPro	□ CrossLoop	□ WindowsRDP
□ pcAnywhere	□ Timbuktu	□ WindowsLiveSync	□ SharedView	

Web HD

□ HTTP Upload	□ HiNet SafeBox	□ MS SkyDrive	□ GDoc Uploader	□ ADrive
□ MyOtherDrive	□ Mozy	□ BoxNet	□ OfficeLive	

4.7.2 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.

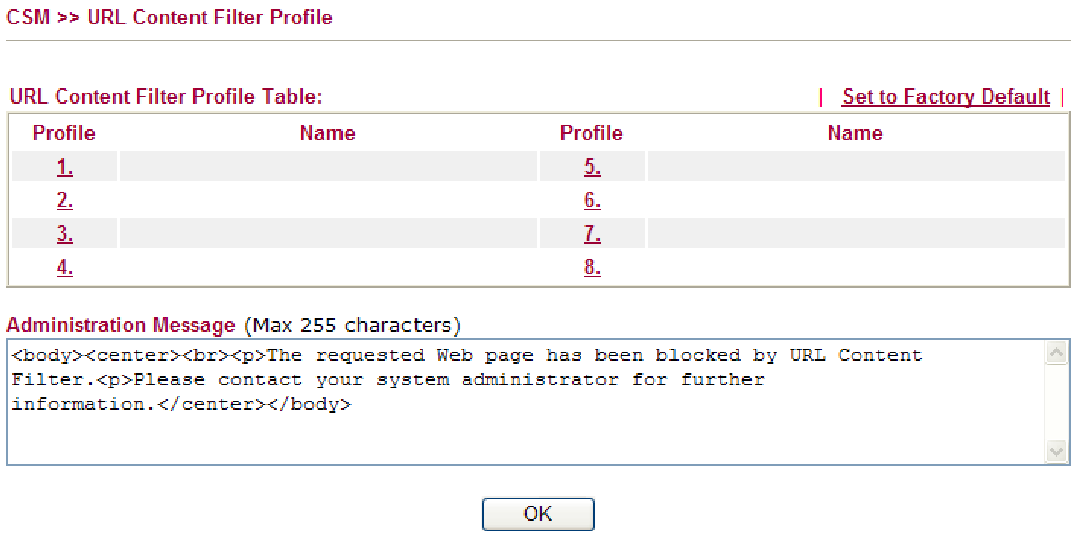
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines 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

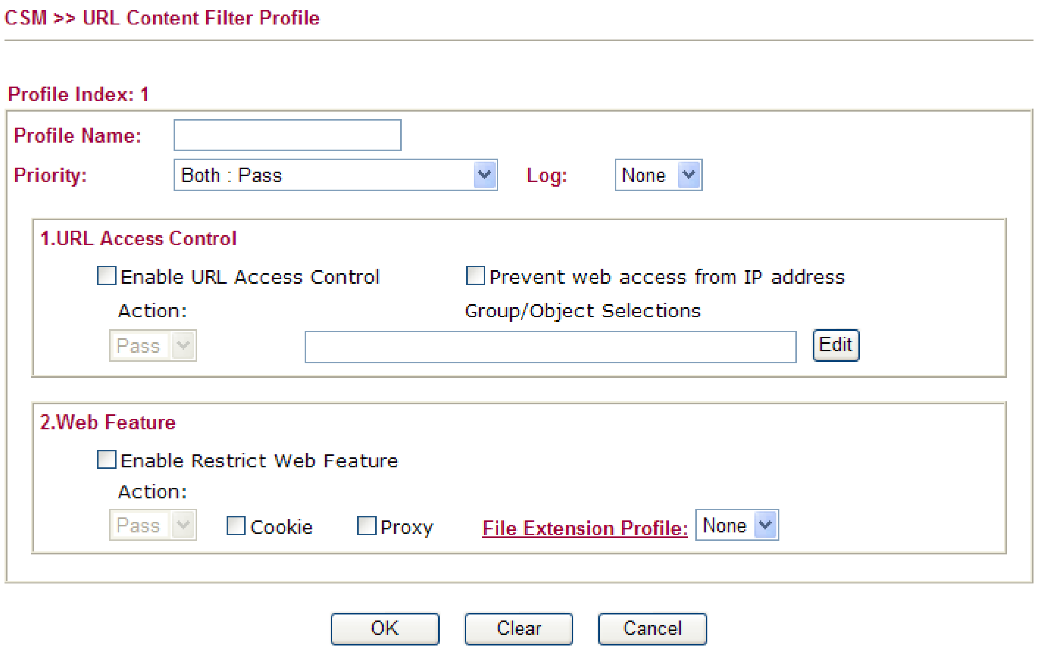
URL Content Filter Profile Table: | Set to Factory Default |

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

Administration Message (Max 255 characters)

```
<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>
```

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



CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: Both : Pass

Log: None

1.URL Access Control

□ Enable URL Access Control

Action: Pass

□ Prevent web access from IP address

Group/Object Selections

2.Web Feature

□ Enable Restrict Web Feature

Action: Pass

□ Cookie

□ Proxy

File Extension Profile: None

Profile Name Type a name for the CSM profile.

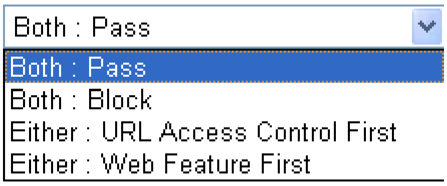
Priority It determines the action that this router will apply.

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.

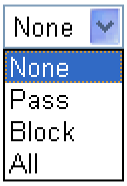


Log **None** – There is no log file will be recorded for this profile.

Pass – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

All – All the actions (Pass and Block) will be recorded in Syslog.



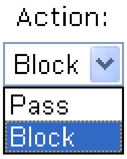
URL Access Control

Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.

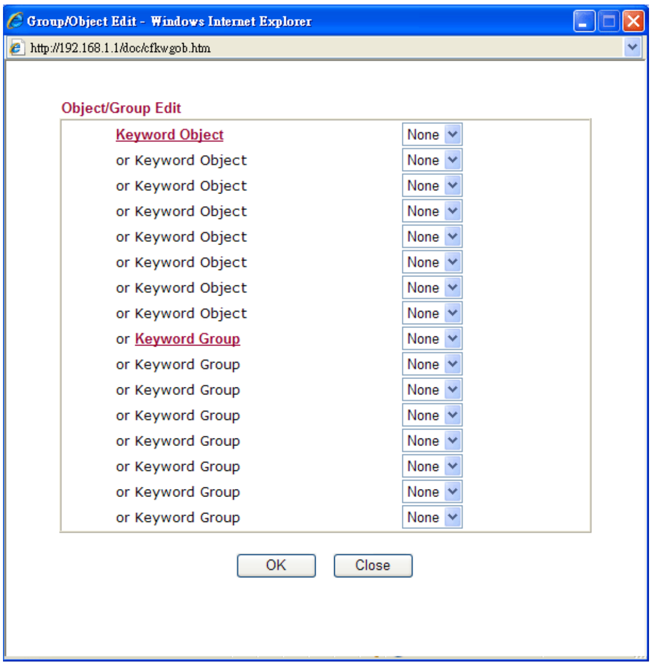
Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly 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.



Group/Object Selections – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.

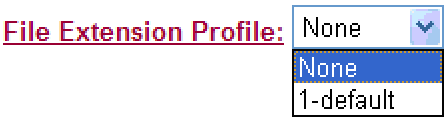


Group/Object Edit - Windows Internet Explorer
http://192.168.1.1/doc/cfkwgob.htm

Object/Group Edit

Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None

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



File Extension Profile: None

4.7.3 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**.

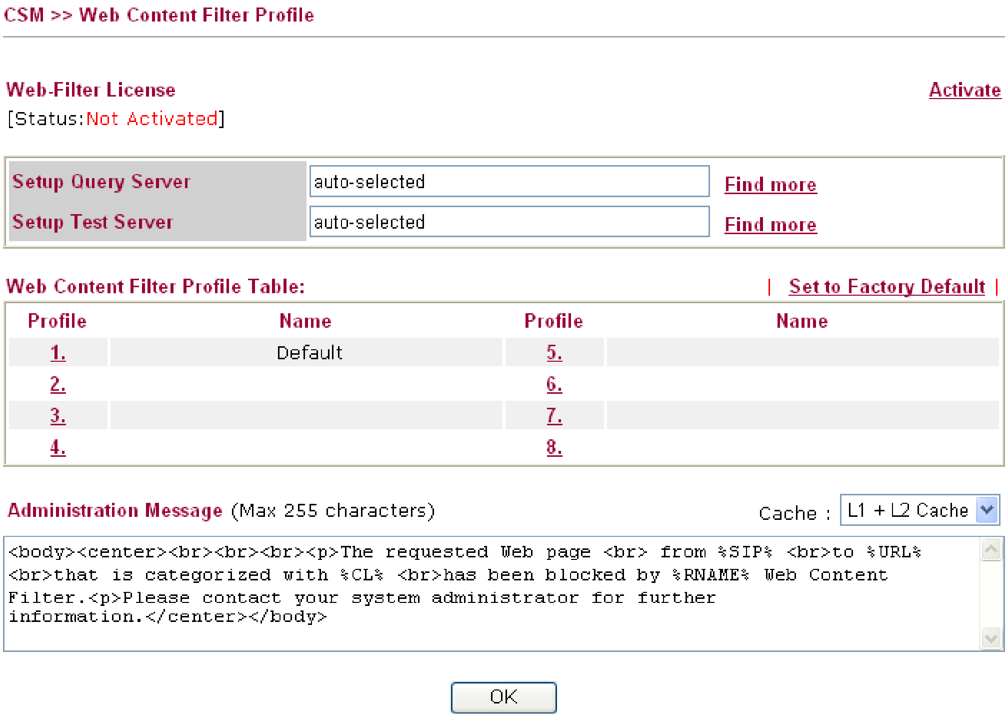
Service Activation Wizard allows you to use trial version or update the license of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com.

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. Next, click the link of **Test a site to verify whether it is categorized** to do the verification.



CSM >> Web Content Filter Profile

Web-Filter License [Status:Not Activated] Activate

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) 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>
```

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.

Set to Factory Default Click this link to retrieve the factory settings.

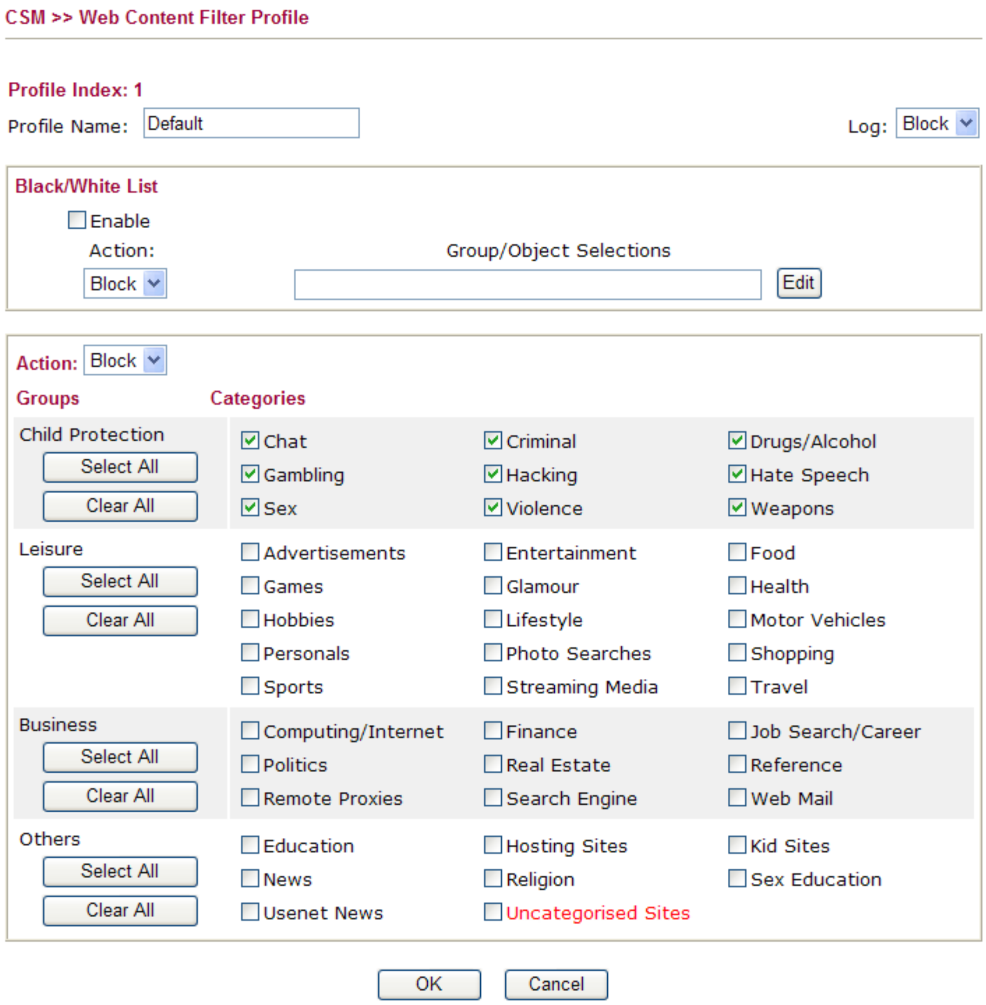
Cache **None** – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.

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.



CSM >> Web Content Filter Profile

Profile Index: 1

Profile Name: Default

Log: Block

Black/White List

□ Enable

Action: Block

Group/Object Selections

Edit

Action: Block

Groups	Categories		
Child Protection Select All Clear All	☑ Chat ☑ Gambling ☑ Sex	☑ Criminal ☑ Hacking ☑ Violence	☑ Drugs/Alcohol ☑ Hate Speech ☑ Weapons
Leisure Select All Clear All	□ Advertisements □ Games □ Hobbies □ Personals □ Sports	□ Entertainment □ Glamour □ Lifestyle □ Photo Searches □ Streaming Media	□ Food □ Health □ Motor Vehicles □ Shopping □ Travel
Business Select All Clear All	□ Computing/Internet □ Politics □ Remote Proxies	□ Finance □ Real Estate □ Search Engine	□ Job Search/Career □ Reference □ Web Mail
Others Select All Clear All	□ Education □ News □ Usenet News	□ Hosting Sites □ Religion □ Uncategorised Sites	□ Kid Sites □ Sex Education

OK Cancel

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.

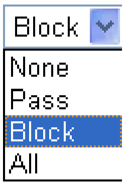
Log

None – There is no log file will be recorded for this profile.

Pass – Only the log about Pass will be recorded in Syslog.

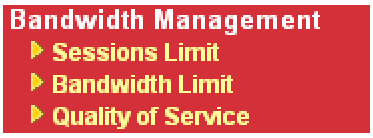
Block – Only the log about Block will be recorded in Syslog.

All – All the actions (Pass and Block) will be recorded in Syslog.



4.8 Bandwidth Management

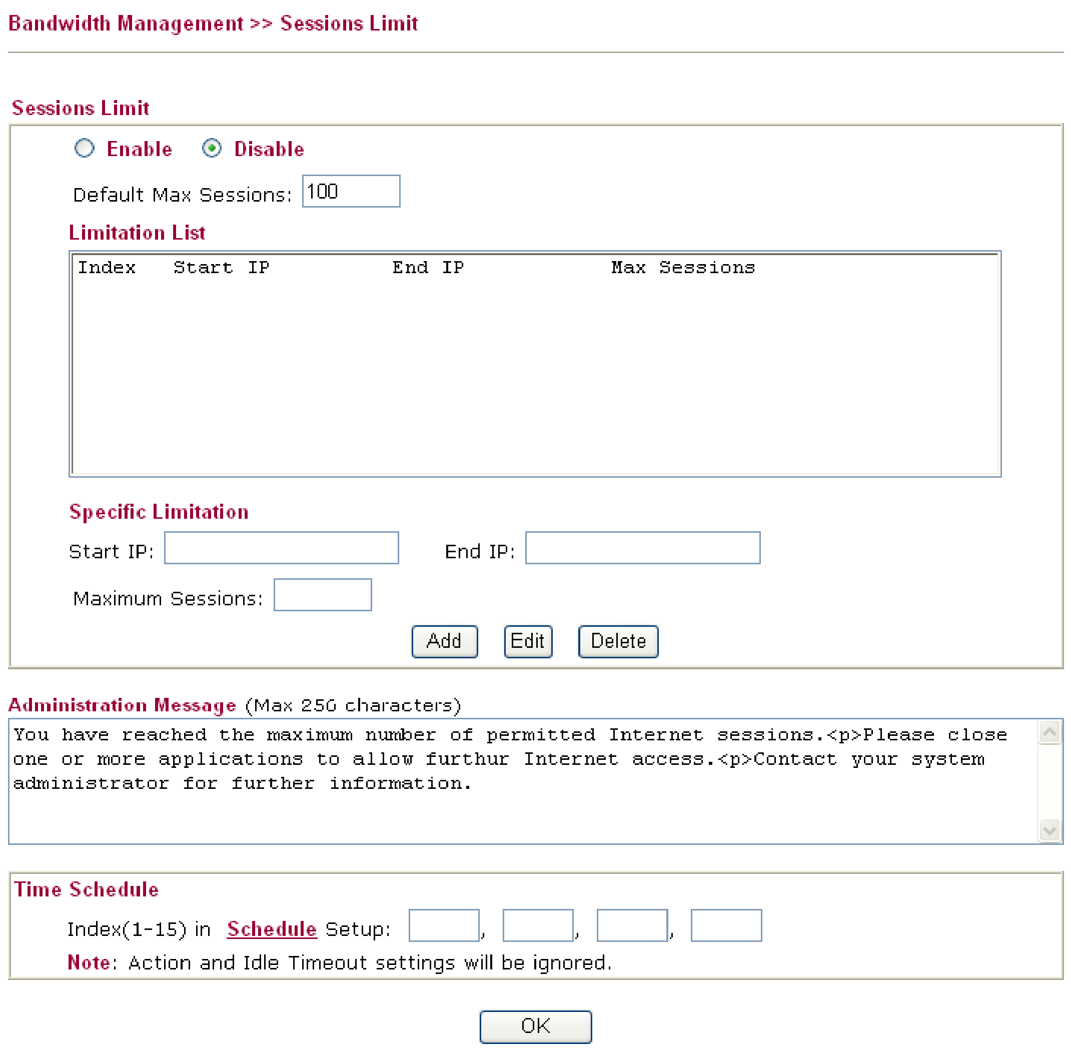
Below shows the menu items for Bandwidth Management.



4.8.1 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.



Bandwidth Management >> Sessions Limit

Sessions Limit

○ Enable ● Disable

Default Max Sessions: 100

Limitation List

```
Index   Start IP          End IP             Max Sessions
```

Specific Limitation

Start IP: ______ End IP: ______

Maximum Sessions: ______

Administration Message (Max 256 characters)

```
You have reached the maximum number of permitted Internet sessions.<p>Please close
one or more applications to allow furthur Internet access.<p>Contact your system
administrator for further information.
```

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

To activate the function of limit session, simply click **Enable** and set the default 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.

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.

Remove Remove the selected settings existing on the limitation list.

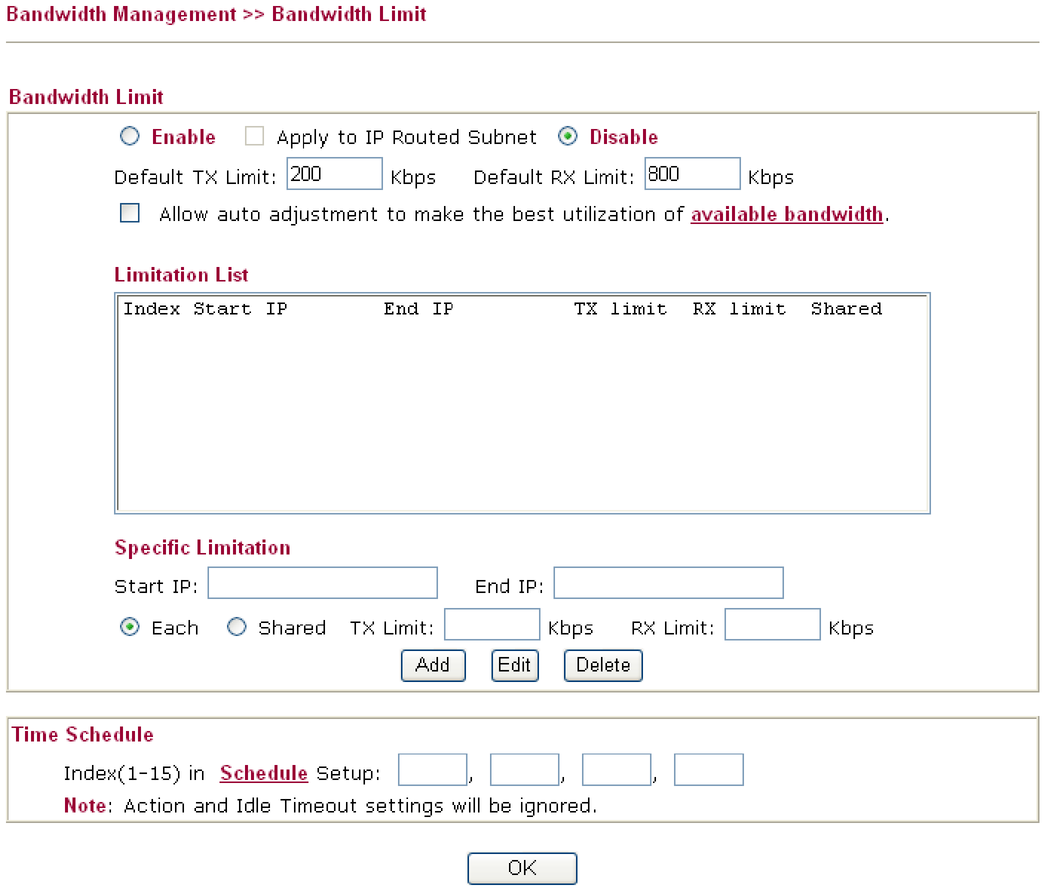
Administration Message Type the words which will be displayed when reaches the

	maximum number of Internet sessions permitted.
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.

4.8.2 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 □ Apply to IP Routed Subnet ● Disable

Default TX Limit: 200 Kbps Default RX Limit: 800 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

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Enable	Click this button to activate the function of limit bandwidth. **Apply to IP Routed Subnet** – Check this box to apply the bandwidth limit to the 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.

Limitation List Display a list of specific limitations that you set on this web page.

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.

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.

4.8.3 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?

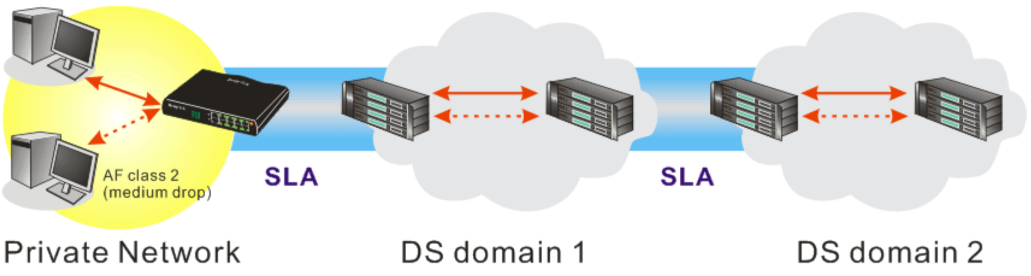
There are two components within Primary configuration of QoS deployment:

- 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.

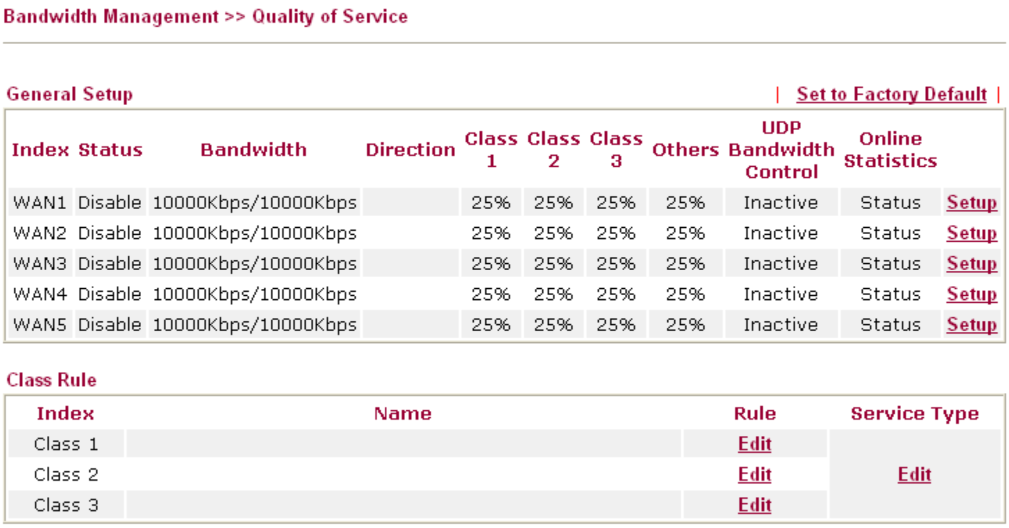
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes 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.



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	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

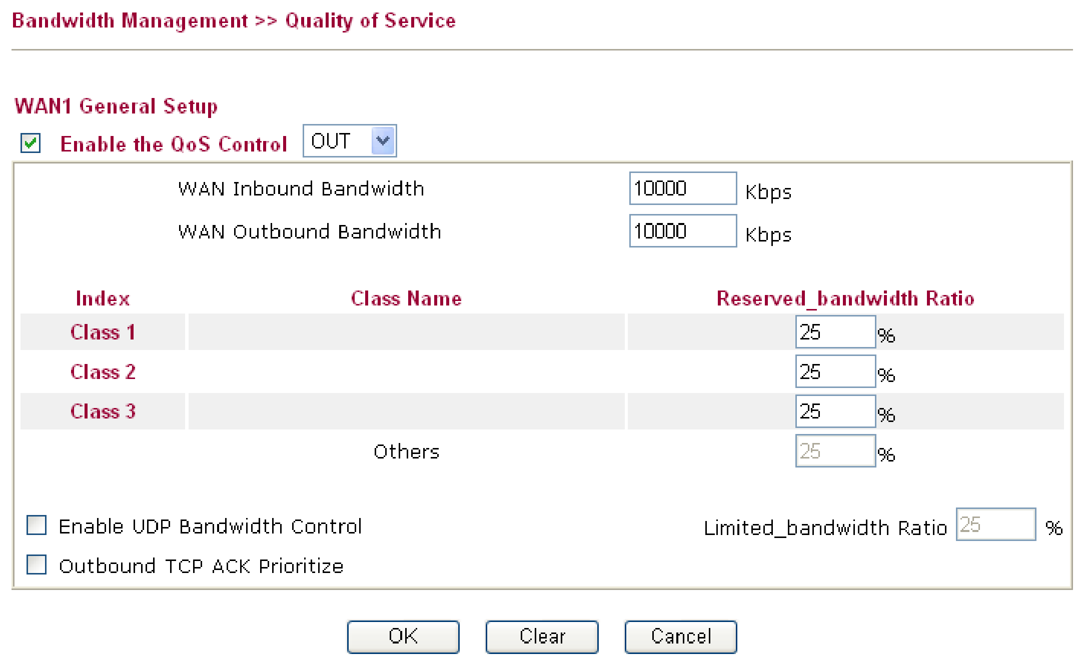
Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

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.

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.



Bandwidth Management >> Quality of Service

WAN1 General Setup

☑ Enable the QoS Control OUT

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %

□ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

□ Outbound TCP ACK Prioritize

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. 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. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.

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.

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

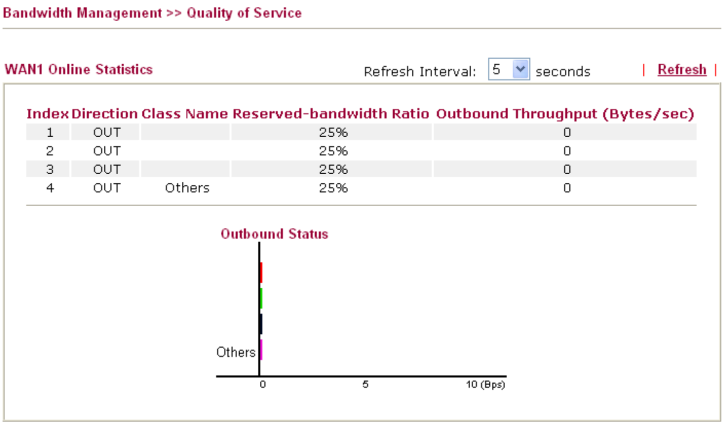
The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

Limited_bandwidth Ratio

The ratio typed here is reserved for limited bandwidth of UDP application.

Online Statistics

Display an online statistics for quality of service for your reference.



Bandwidth Management >> Quality of Service

WAN1 Online Statistics

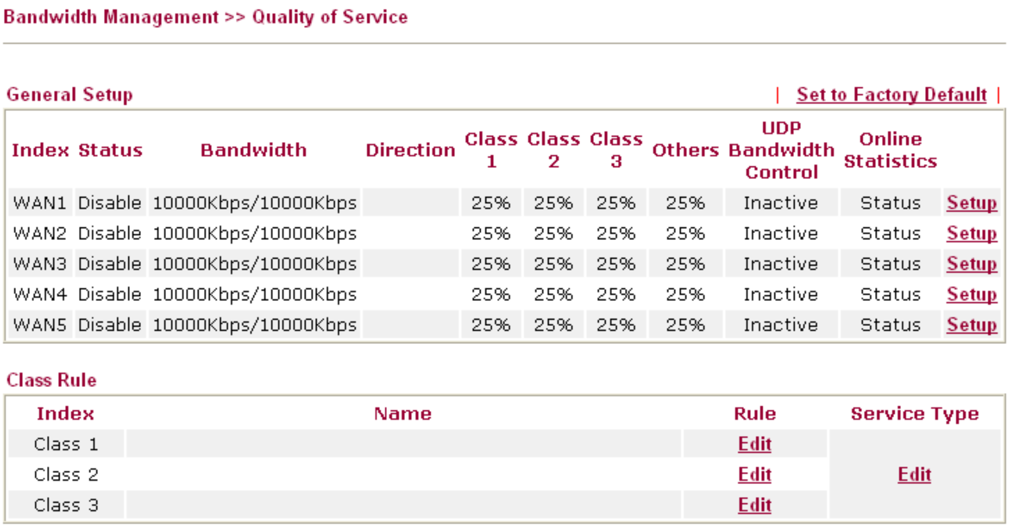
Refresh Interval: 5 seconds | Refresh |

Index	Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)
1	OUT		25%	0
2	OUT		25%	0
3	OUT		25%	0
4	OUT	Others	25%	0

Outbound Status

Edit the Class Rule for QoS

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

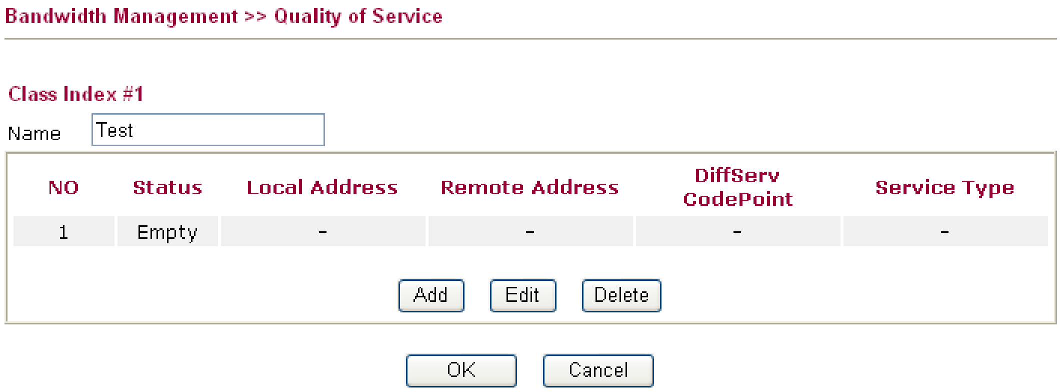
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

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

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.



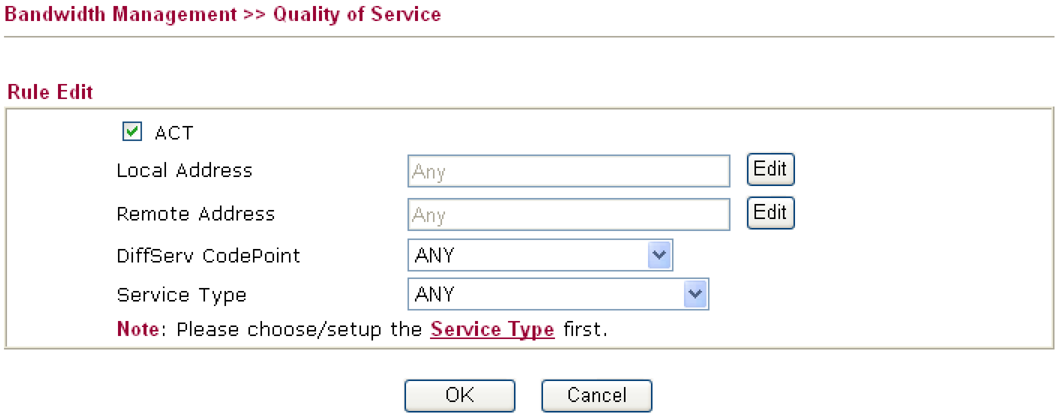
Bandwidth Management >> Quality of Service

Class Index #1

Name: Test

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

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



Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT

Local Address: Any

Remote Address: Any

DiffServ CodePoint: ANY

Service Type: ANY

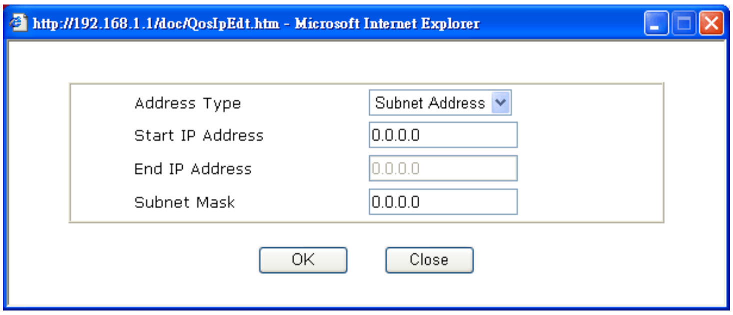
Note: Please choose/setup the Service Type first.

ACT Check this box to invoke these settings.

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.

Edit It allows you to edit source address information.



http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer

Address Type: Subnet Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Address Type – Determine the address type for the source address.

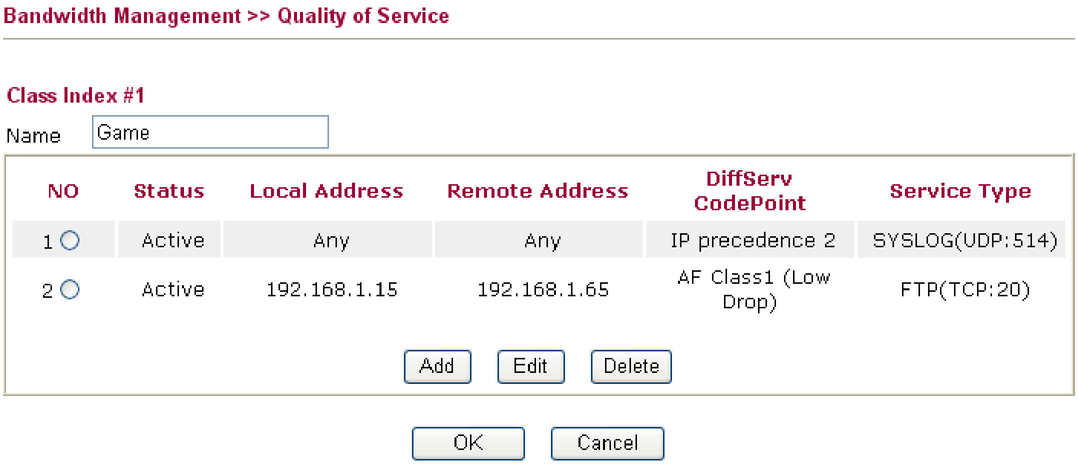
For **Single Address**, you have to fill in Start IP address.

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.

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.



Bandwidth Management >> Quality of Service

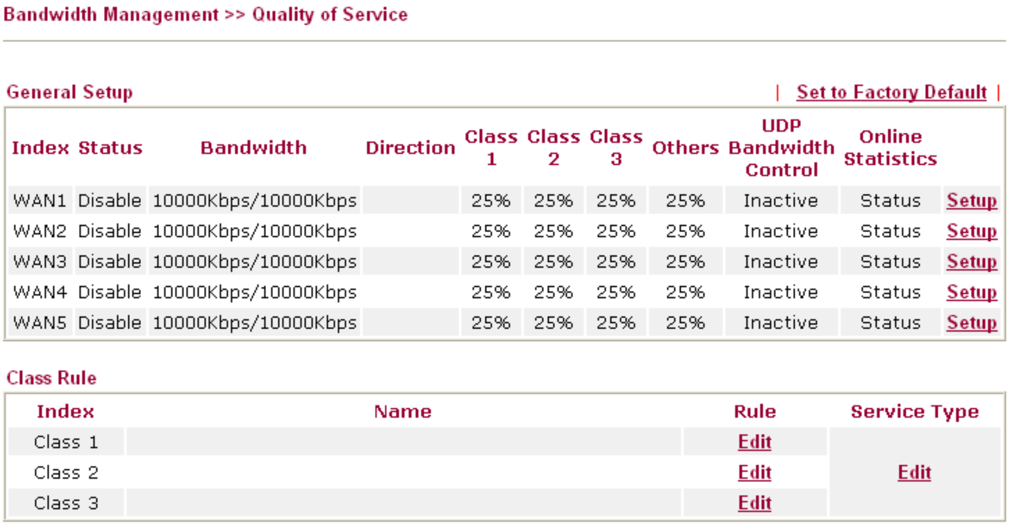
Class Index #1

Name: Game

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Active	Any	Any	IP precedence 2	SYSLOG(UDP:514)
2 ○	Active	192.168.1.15	192.168.1.65	AF Class1 (Low Drop)	FTP(TCP:20)

Edit the Service Type for Class Rule

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



Bandwidth Management >> Quality of Service

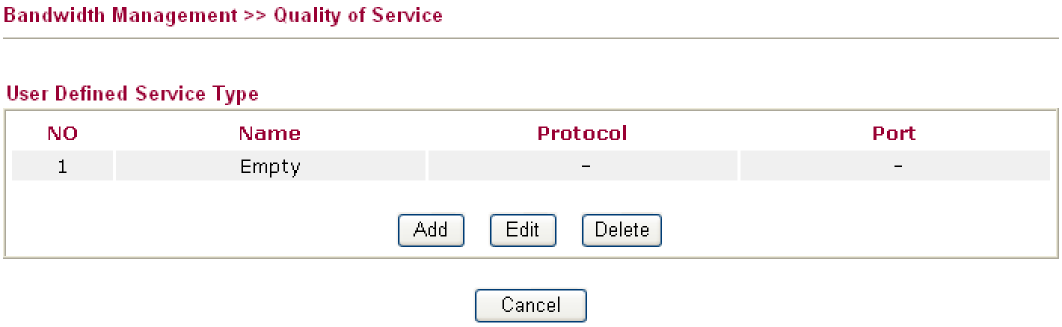
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

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

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

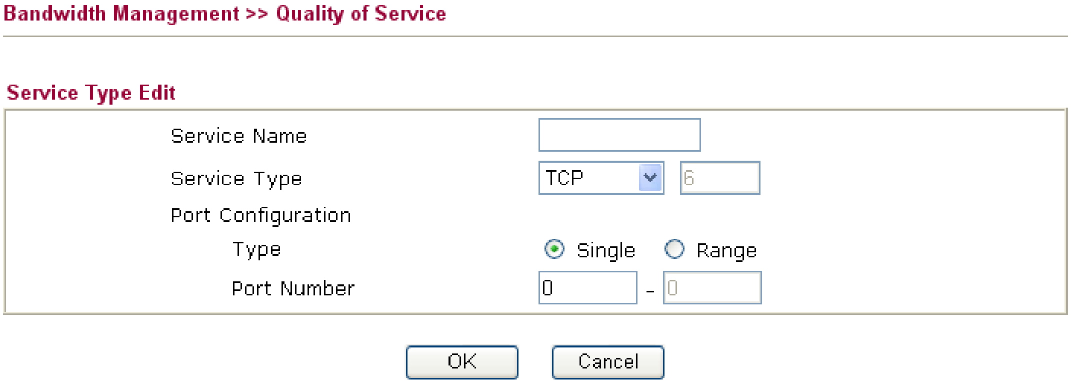


Bandwidth Management >> Quality of Service

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

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

Service Name Type in a new service for your request.

Service Type Choose the type (TCP, UDP or TCP/UDP) for the new service.

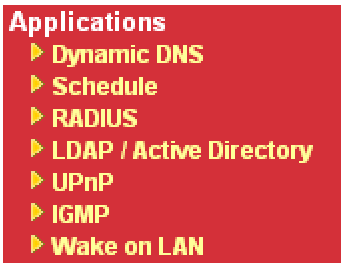
Port Configuration Click **Single** or **Range** as the **Type**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.

Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

4.9 Applications

Below shows the menu items for Applications.



4.9.1 Dynamic DNS

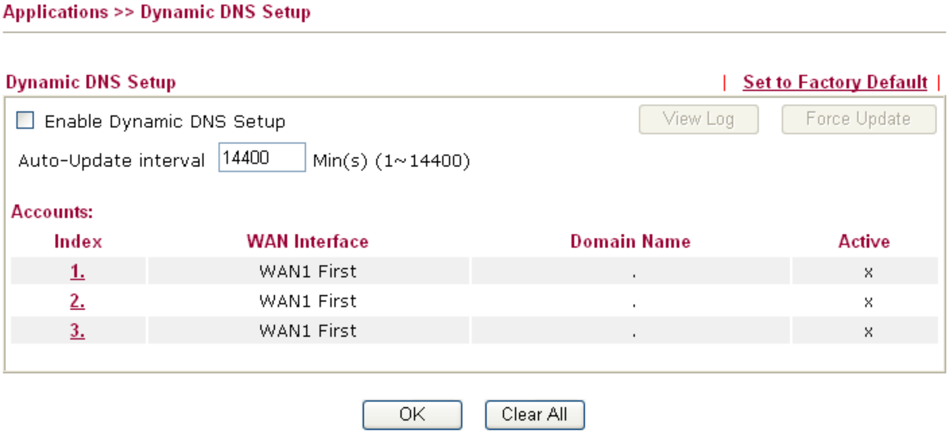
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router 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**.



Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

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

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

Accounts:

Index	WAN Interface	Domain Name	Active
1.	WAN1 First	.	x
2.	WAN1 First	.	x
3.	WAN1 First	.	x

[OK] [Clear All]

Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
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).

WAN Interface Display the WAN interface used.

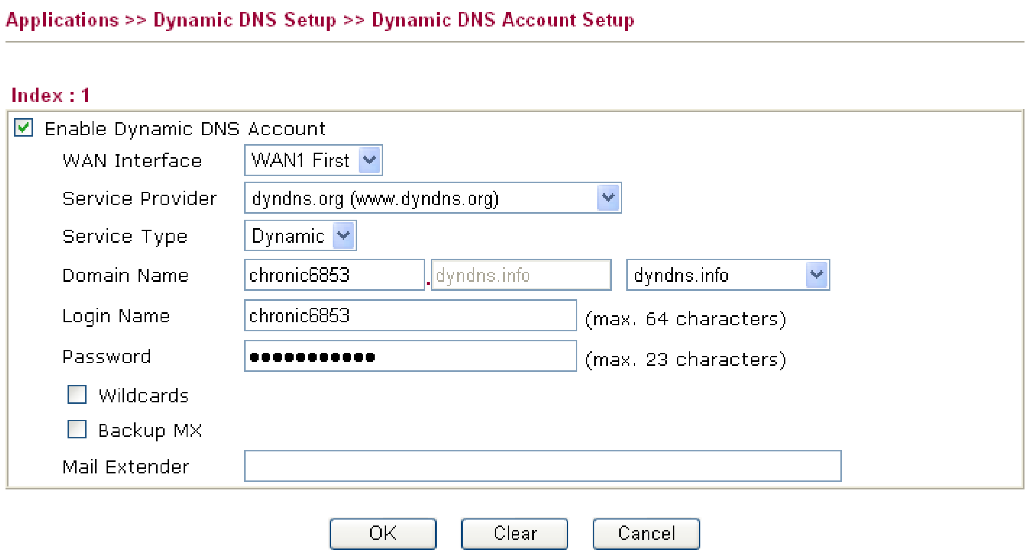
Domain Name Display the domain name that you set on the setting page of DDNS setup.

Active Display if this account is active or inactive.

View Log Display DDNS log status.

Force Update Force the router updates its information to DDNS server.

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

WAN Interface: WAN1 First

Service Provider: dyndns.org (www.dyndns.org)

Service Type: Dynamic

Domain Name: chronic6853 . dyndns.info dyndns.info

Login Name: chronic6853 (max. 64 characters)

Password: ●●●●●●●●●●●● (max. 23 characters)

□ Wildcards

□ Backup MX

Mail Extender:

Enable Dynamic DNS Account Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).

WAN Interface **WAN1/WAN2/WAN3/WAN4/WAN5 First -** While connecting, the router will use WAN1/WAN2/WAN3 /WAN4 /WAN5 as the first channel for such account. If WAN1/WAN2/WAN3/WAN4/WAN5 fails, the router will use another WAN interface instead.
WAN1/WAN2/WAN3/WAN4/WAN5 Only - While connecting, the router will use WAN1/WAN2/WAN3 /WAN4/WAN5 as the only channel for such account.

Service Provider Select the service provider for the DDNS account.

Service Type Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.

Domain Name Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.

Login Name Type in the login name that you set for applying domain.

Password Type in the password that you set for applying domain.

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

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.

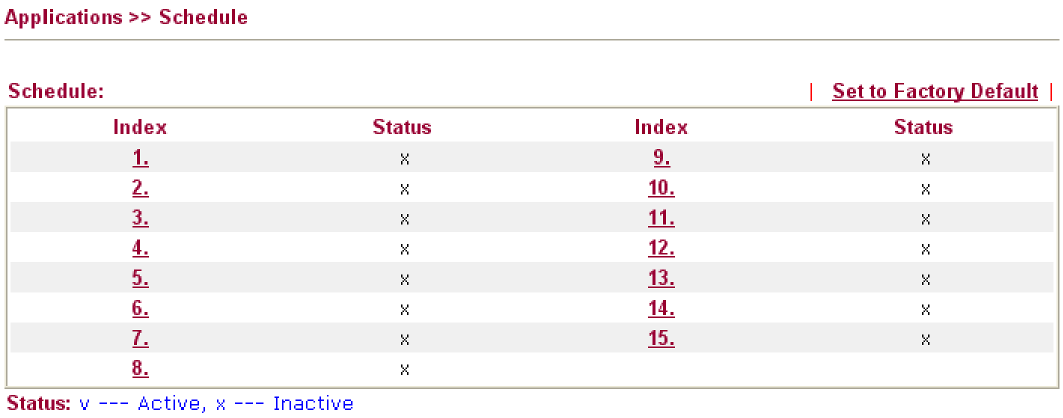
Delete a Dynamic DNS Account

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

4.9.2 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the 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.



Applications >> Schedule

Schedule: | Set to Factory Default |

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

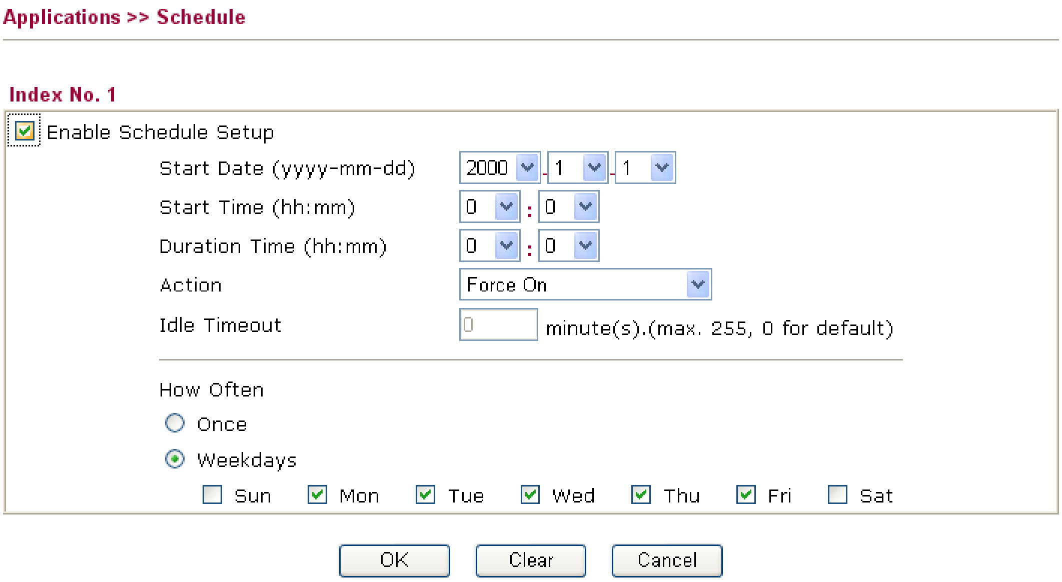
Set to Factory Default Clear all profiles and recover to factory settings.

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



Applications >> Schedule

Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd)	2000 - 1 - 1
Start Time (hh:mm)	0 : 0
Duration Time (hh:mm)	0 : 0
Action	Force On
Idle Timeout	0 minute(s).(max. 255, 0 for default)

How Often

○ Once

● Weekdays

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Enable Schedule Setup Check to enable the schedule.

Start Date (yyyy-mm-dd) Specify the starting date of the schedule.

Start Time (hh:mm) Specify the starting time of the schedule.

Duration Time (hh:mm) Specify the duration (or period) for the schedule.

Action Specify which action Call Schedule should apply during the period of the schedule.

Force On -Force the connection to be always on.

Force Down -Force the connection to be always down.

Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field.

Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

Idle Timeout Specify the duration (or period) for the schedule.

How often -Specify how often the schedule will be applied
Once -The schedule will be applied just once

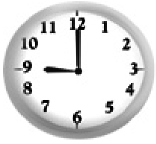
Weekdays -Specify which days in one week should perform the schedule.

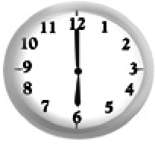
Example

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)





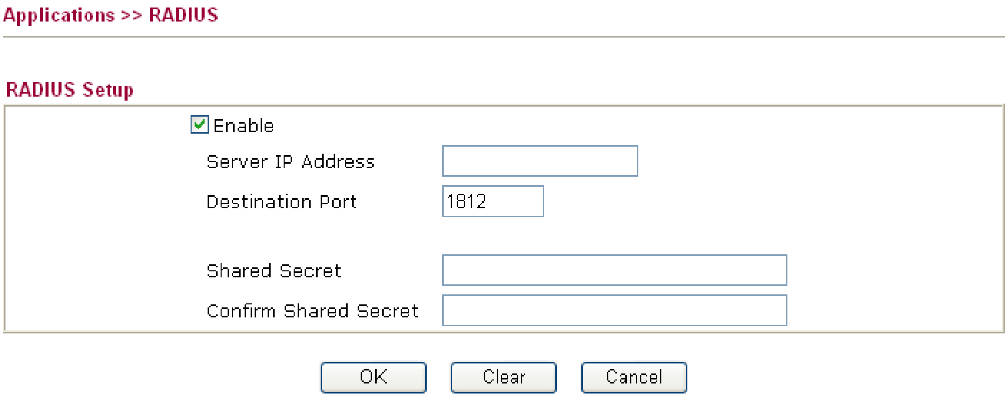
Mon - Sun	**9:00 am**	**to**	**6:00 pm**

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.

4.9.3 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.



Applications >> RADIUS

RADIUS Setup

☑ Enable

Server IP Address

Destination Port: 1812

Shared Secret

Confirm Shared Secret

Enable Check to enable RADIUS client feature.

Server IP Address Enter 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.

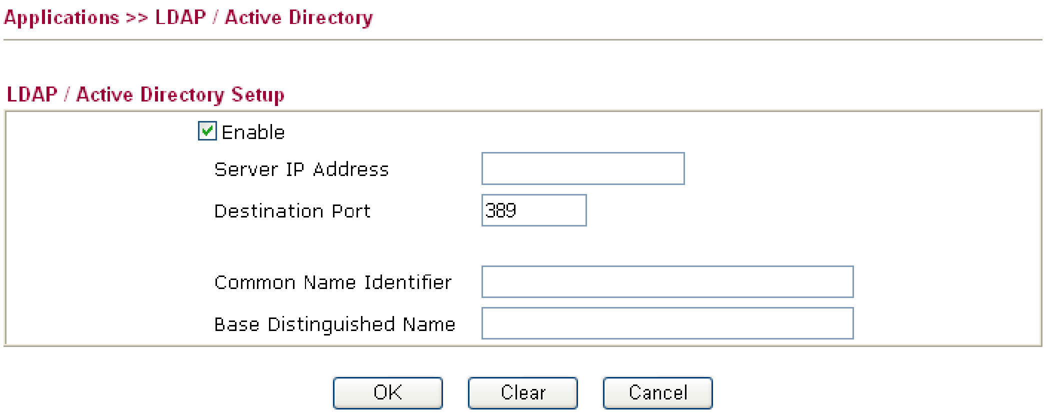
Shared Secret The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Confirm Shared Secret Re-type the Shared Secret for confirmation.

4.9.4 LDAP / Active Directory

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

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



Applications >> LDAP / Active Directory

LDAP / Active Directory Setup

☑ Enable

Server IP Address

Destination Port 389

Common Name Identifier

Base Distinguished Name

Enable Check to enable such function.

Server IP Address Enter the IP address of LDAP server.

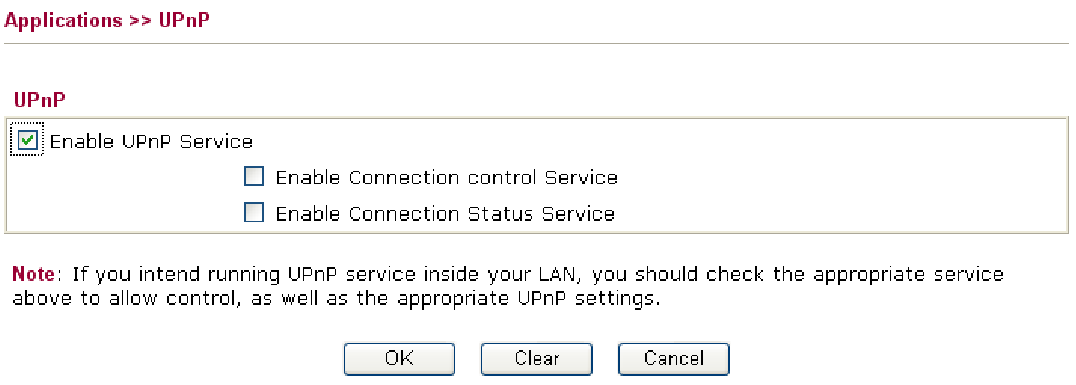
Destination Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

Common Name Identifier Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is “cn”.

Base Distinguished Name Type or edit the distinguished name used to look up entries on the LDAP server.

4.9.5 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. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.



Applications >> UPnP

UPnP

☑ Enable UPnP Service

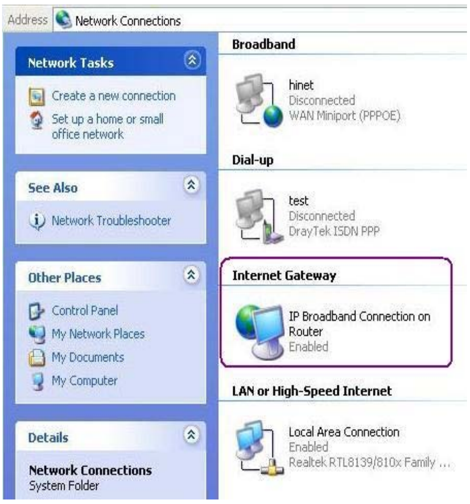
□ Enable Connection control Service

□ Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

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

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



Address Network Connections

Network Tasks

- Create a new connection
- Set up a home or small office network

See Also

- Network Troubleshooter

Other Places

- Control Panel
- My Network Places
- My Documents
- My Computer

Details

Network Connections
System Folder

Broadband

hinet
Disconnected
WAN Miniport (PPPOE)

Dial-up

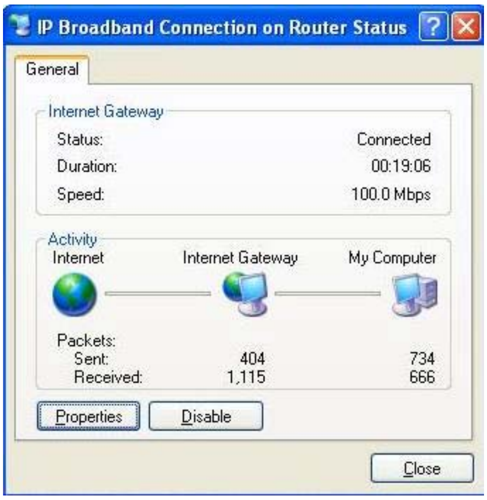
test
Disconnected
DrayTek ISDN PPP

Internet Gateway

IP Broadband Connection on Router
Enabled

LAN or High-Speed Internet

Local Area Connection
Enabled
Realtek RTL8139/810x Family ...



IP Broadband Connection on Router Status

General

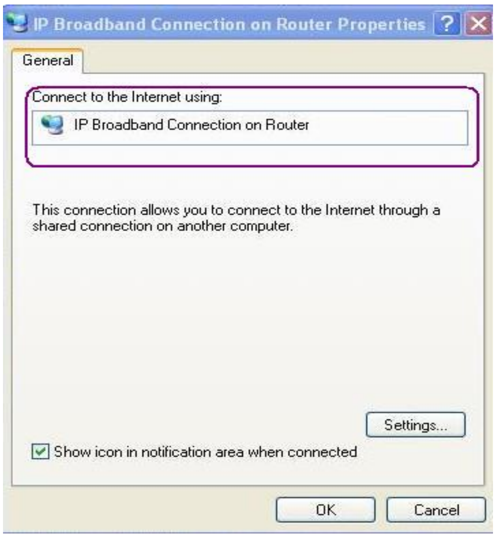
Internet Gateway

Status:	Connected
Duration:	00:19:06
Speed:	100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		404	734
Received:		1,115	666

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.

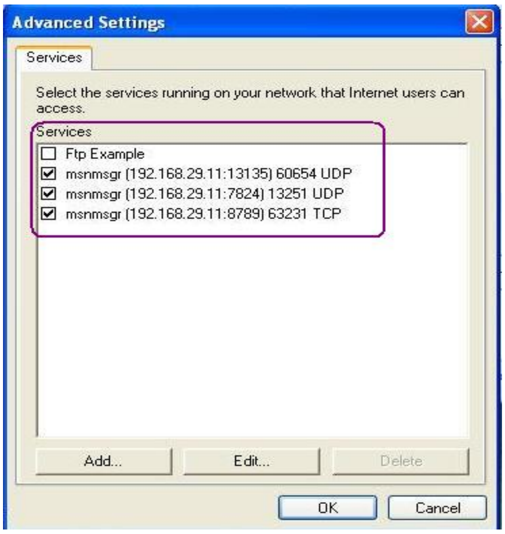


Connect to the Internet using:

IP Broadband Connection on Router

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected



Select the services running on your network that Internet users can access.

Services

☐ Ftp Example
☑ msnmsgr (192.168.29.11:13135) 60654 UDP
☑ msnmsgr (192.168.29.11:7824) 13251 UDP
☑ msnmsgr (192.168.29.11:8789) 63231 TCP

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

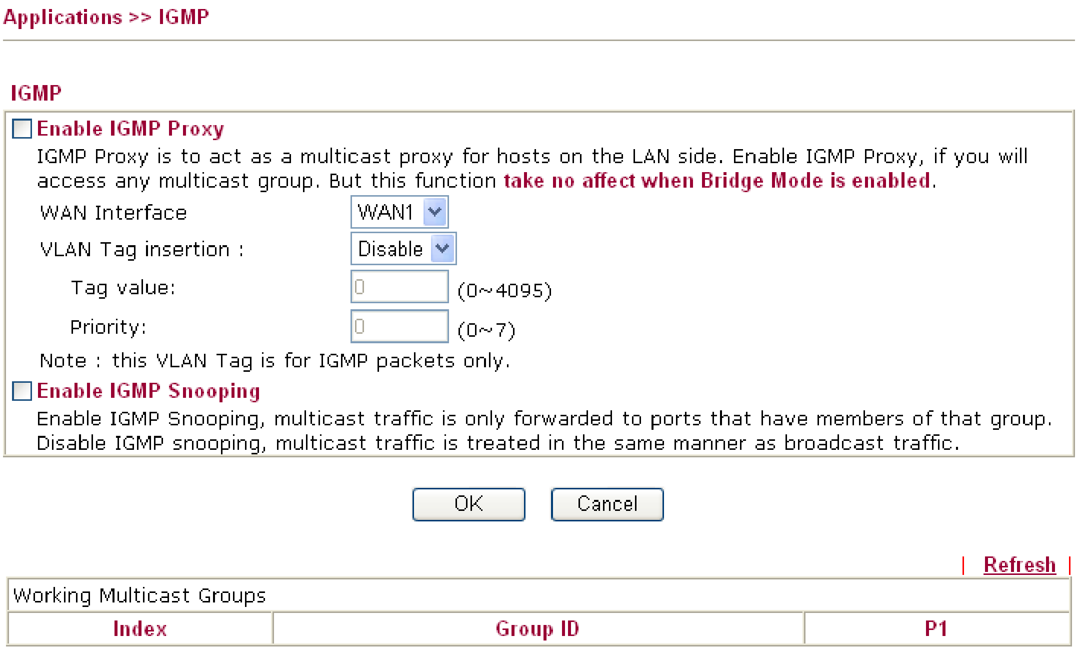
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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.

4.9.6 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.



Applications >> IGMP

IGMP

□ Enable IGMP Proxy

IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function **take no affect when Bridge Mode is enabled.**

WAN Interface	WAN1
VLAN Tag insertion :	Disable
Tag value:	0 (0~4095)
Priority:	0 (0~7)

Note : this VLAN Tag is for IGMP packets only.

□ Enable IGMP Snooping

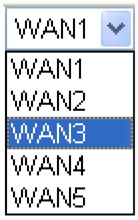
Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.

Working Multicast Groups

Index	Group ID	P1

Enable IGMP Proxy Check this box to enable this function.

WAN Interface - The application of multicast will be executed through WAN port selected. In addition, such function is available in NAT mode.



VLAN Tag insertion – It allows to enable / disable VLAN tag feature for IGMP packet.

Tag value – Give a tag value for outgoing IGMP packets. The range is form 0 to 4095.

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

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.

Group ID This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.

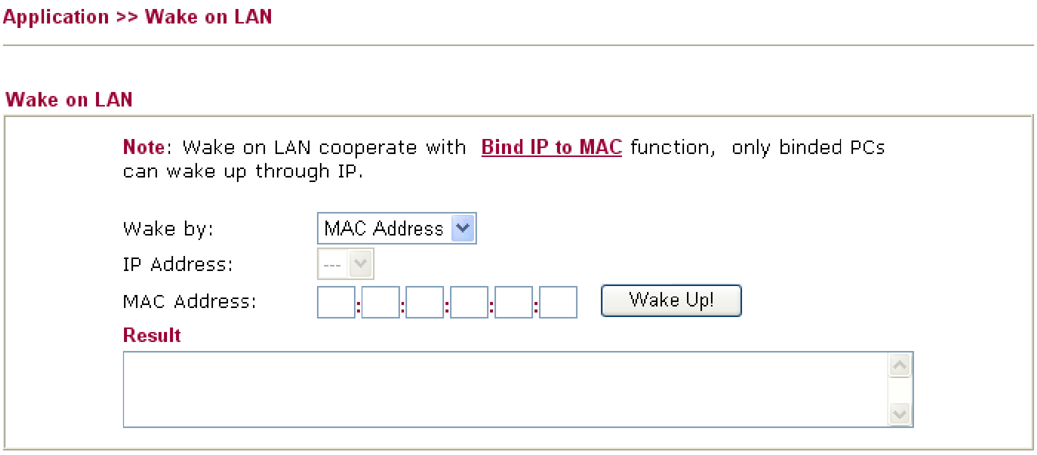
P1 It indicates the LAN port used for the multicast group.

Refresh Click this link to renew the working multicast group status.

4.9.7 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** 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.



Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN cooperate with Bind IP to MAC function, only binded PCs can wake up through IP.

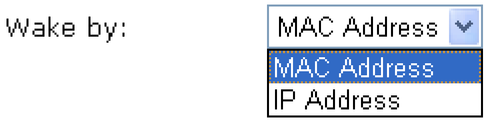
Wake by: MAC Address

IP Address: ---

MAC Address: __ : __ : __ : __ : __ : __

Result

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.

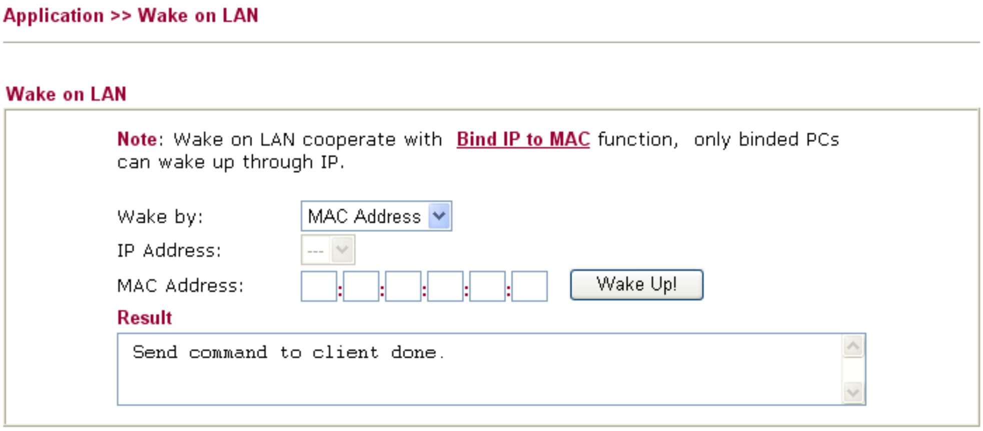


Wake by: MAC Address

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 cooperate with **Bind IP to MAC** function, only binded PCs can wake up through IP.

Wake by:	MAC Address
IP Address:	---
MAC Address:	__ : __ : __ : __ : __ : __

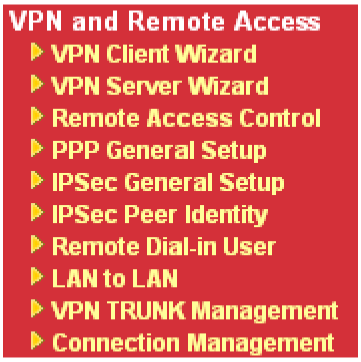
Result

```
Send command to client done.
```

4.10 VPN and Remote Access

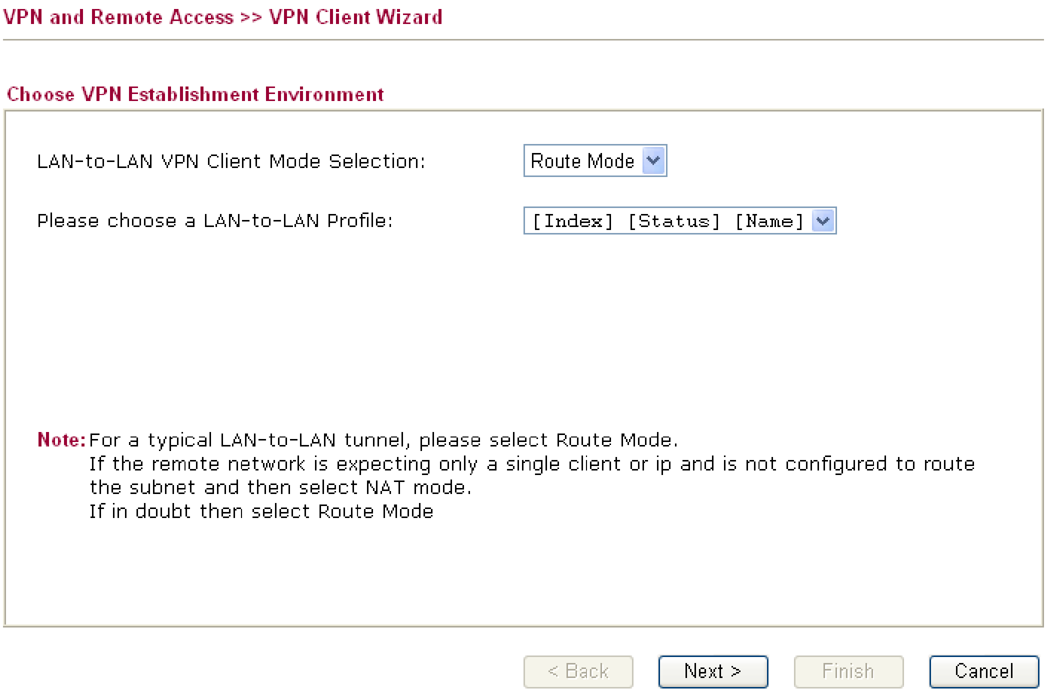
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



4.10.1 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.



VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Environment

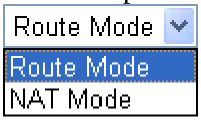
LAN-to-LAN VPN Client Mode Selection: Route Mode

Please choose a LAN-to-LAN Profile: [Index] [Status] [Name]

Note: For a typical LAN-to-LAN tunnel, please select Route Mode.
If the remote network is expecting only a single client or ip and is not configured to route the subnet and then select NAT mode.
If in doubt then select Route Mode

LAN-to-LAN Client Mode Selection

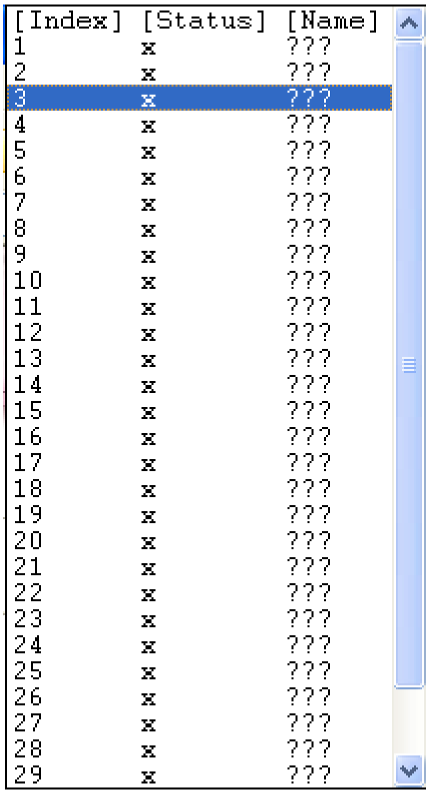
Choose the client mode.
Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode.



Please choose a

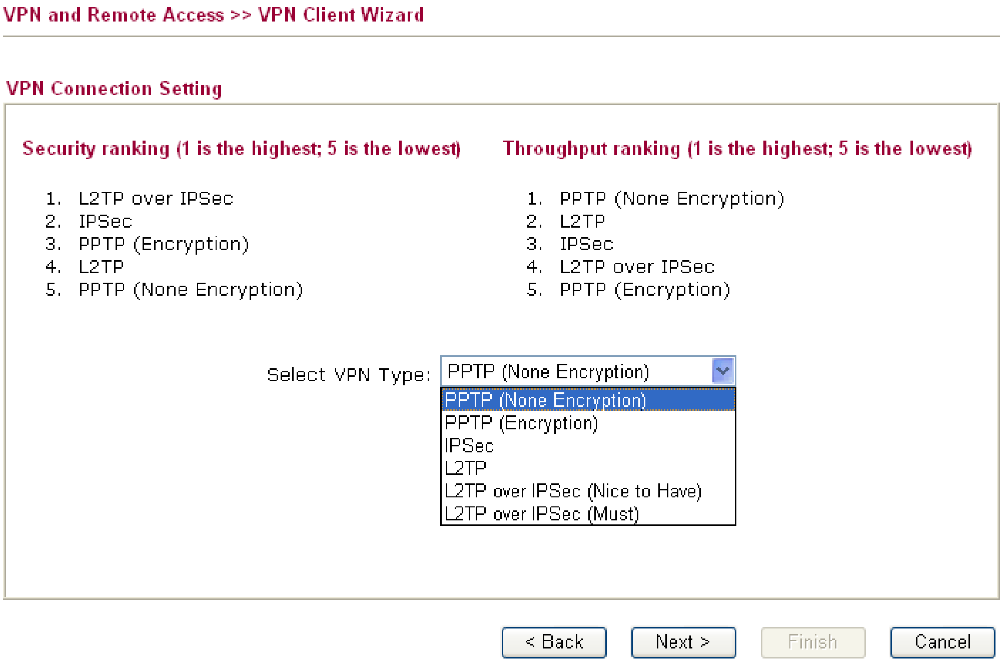
There are 32 VPN profiles for users to set.

LAN-to-LAN Profile



```
[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        ???
```

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)

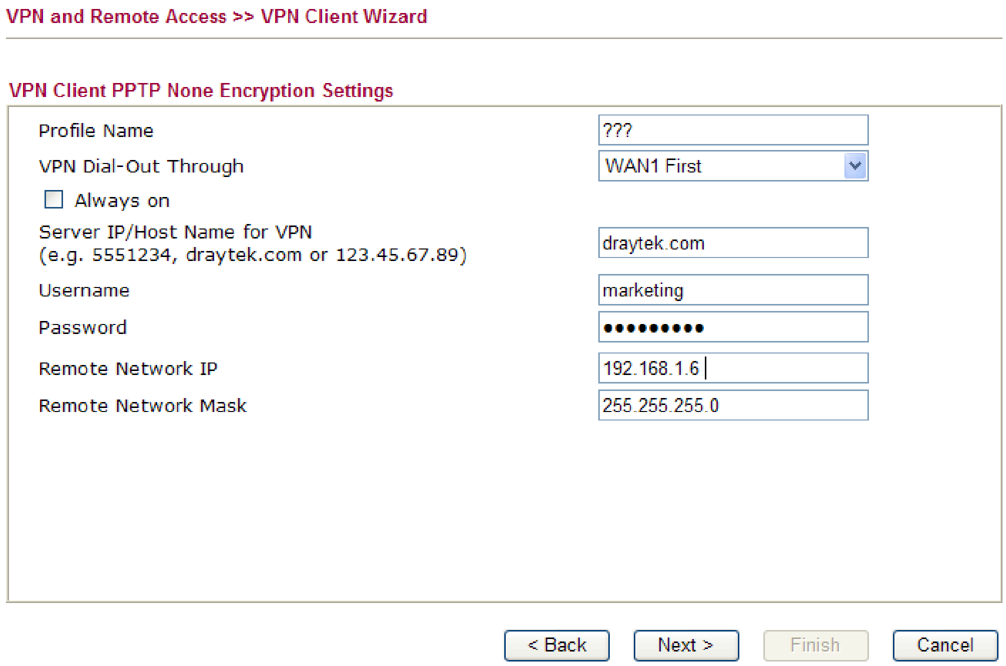
Throughput ranking (1 is the highest; 5 is the lowest)

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

Select VPN Type: PPTP (None Encryption)

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.

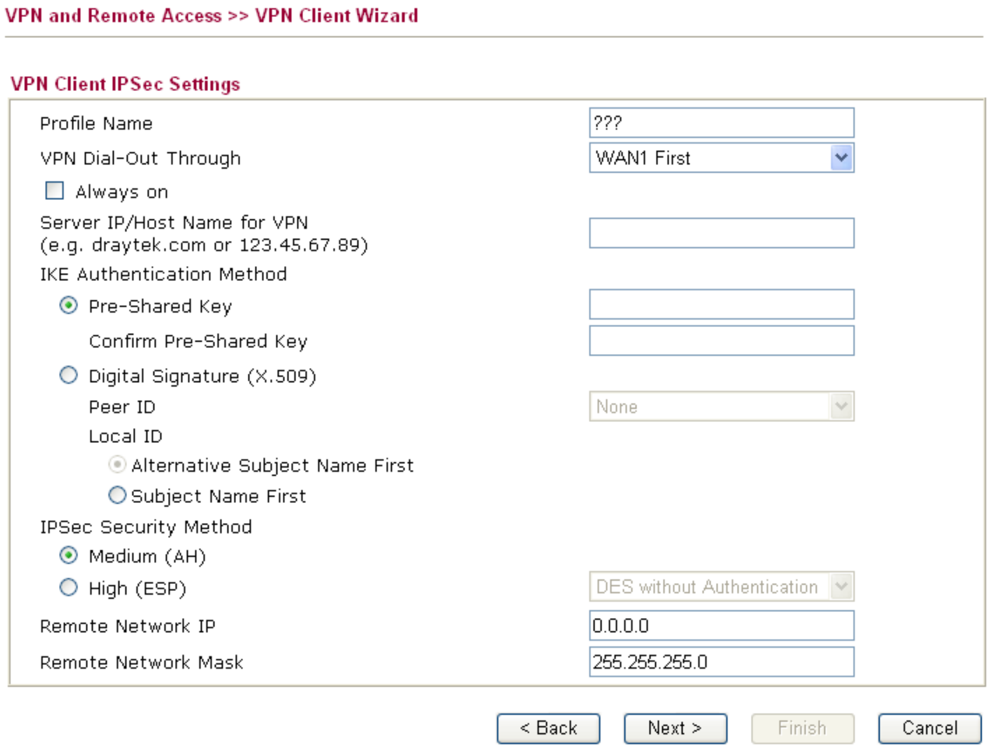
- When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:


VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP None Encryption Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
□ Always on	
Server IP/Host Name for VPN (e.g. 5551234, 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

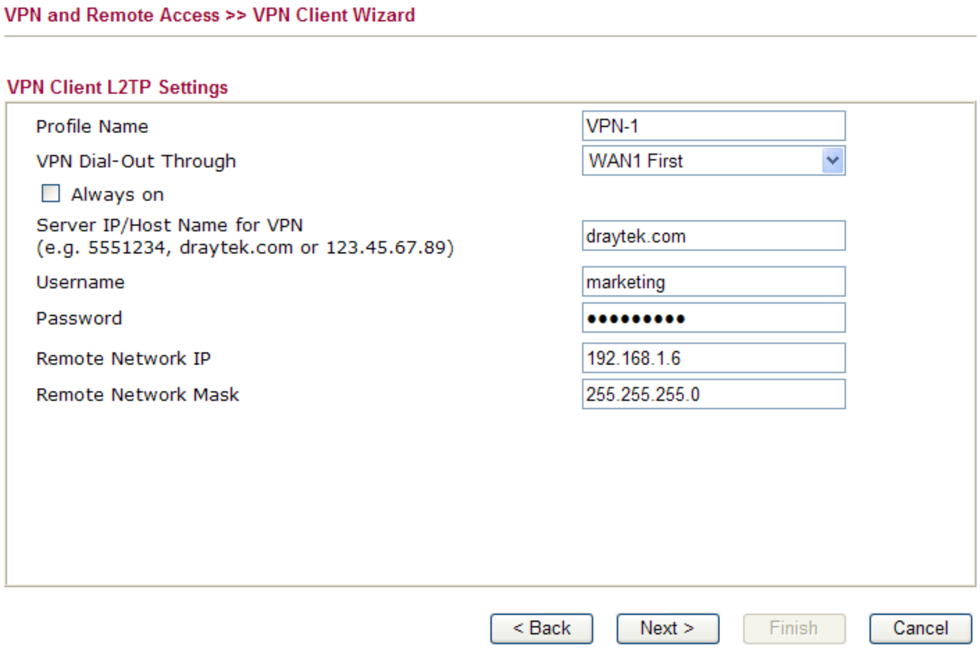
- When you choose **IPSec**, you will see the following graphic:


VPN and Remote Access >> VPN Client Wizard

VPN Client IPSec Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
□ 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	
IPSec Security Method	
● Medium (AH)	
○ High (ESP)	DES without Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

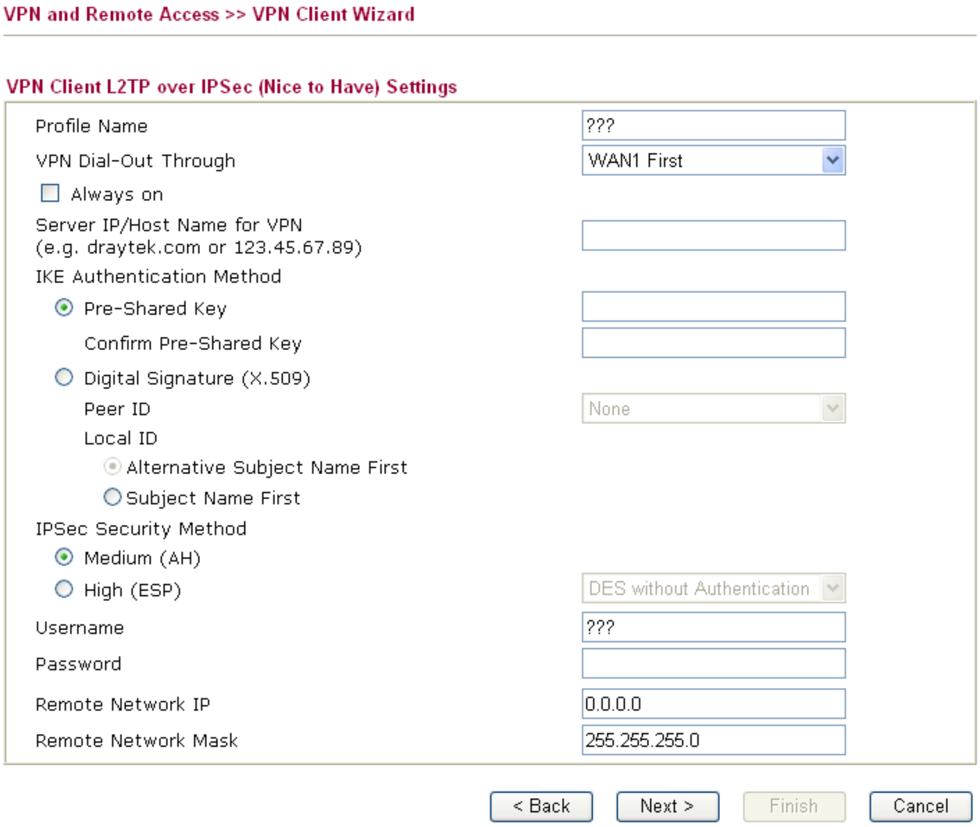


VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP Settings

Profile Name	VPN-1
VPN Dial-Out Through	WAN1 First
□ Always on	
Server IP/Host Name for VPN (e.g. 5551234, 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

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

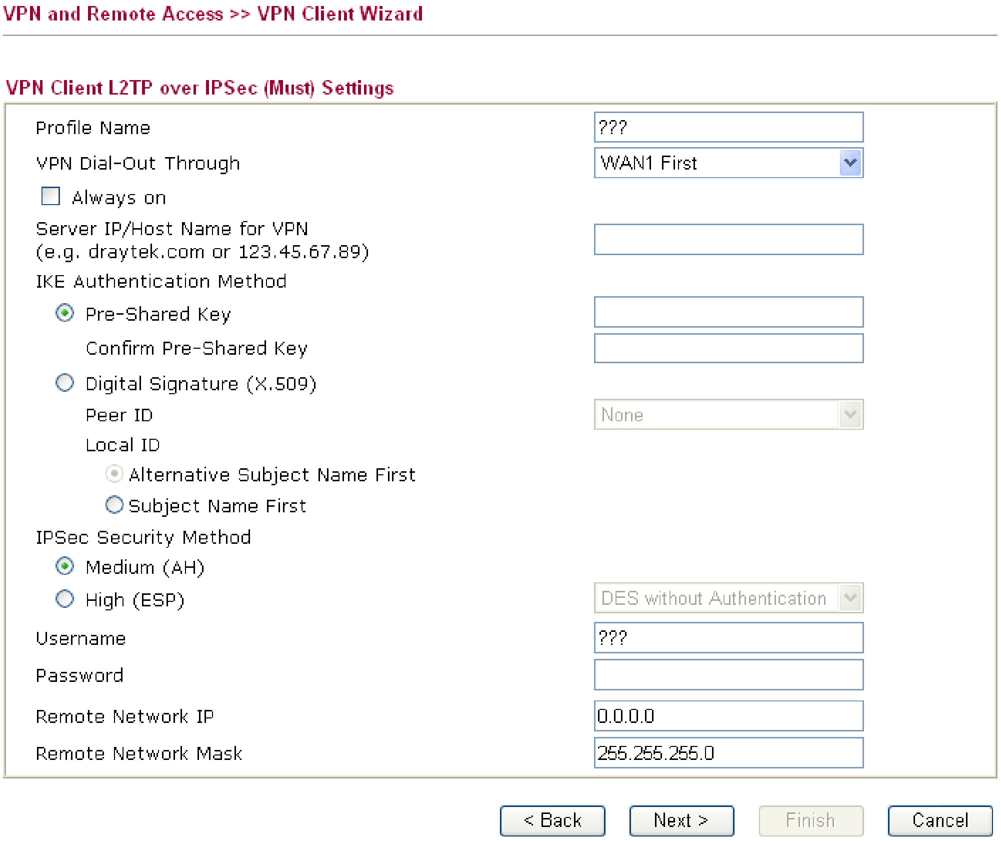


VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPSec (Nice to Have) Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
□ 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	
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

- When you choose **L2TP over IPSec (Must),** you will see the following graphic:



VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPSec (Must) Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
□ 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	
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

Profile Name Type a name for such profile. The length of the file is limited to 10 characters.

VPN Dial-Out Through Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.

WAN1 First / WAN2 First / WAN3 First / WAN4 First / WAN5 First - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the first channel for VPN connection. If WAN1/WAN2/WAN3 /WAN4/WAN5 fails, the router will use another WAN interface instead.

WAN1 Only / WAN2 Only / WAN3 Only / WAN4 Only/ WAN5 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the only channel for VPN connection.

Always On Check to enable router always keep VPN connection.

Pre-Shared Key **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. 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.

Peer ID – Choose one of the ID from the drop down list.

Local ID – Choose **Alternative Subject Name First** or **Subject Name First**.

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.

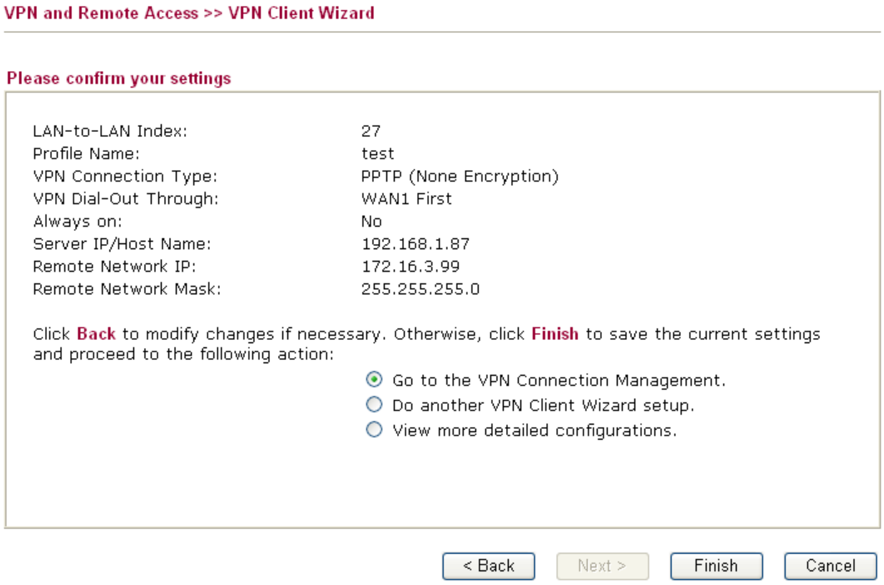
User Name This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.

Password This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.

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.

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 and Remote Access >> VPN Client Wizard

Please confirm your settings

LAN-to-LAN Index:	27
Profile Name:	test
VPN Connection Type:	PPTP (None Encryption)
VPN Dial-Out Through:	WAN1 First
Always on:	No
Server IP/Host Name:	192.168.1.87
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.

Go to the VPN Connection Click this radio button to access **VPN and Remote**

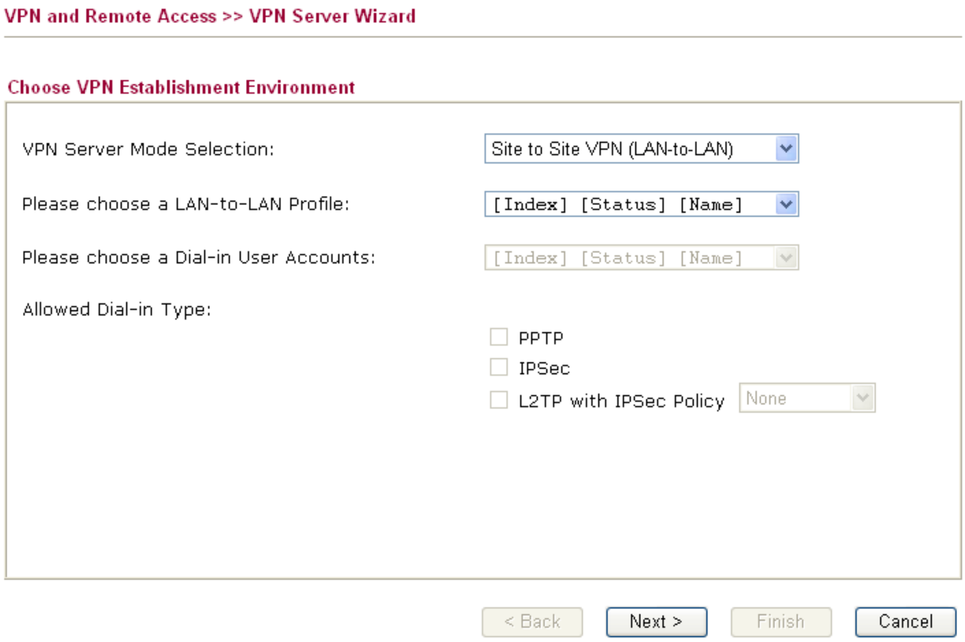
Management — **Access>>Connection Management** for viewing VPN Connection status.

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.

4.10.2 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.



VPN and Remote Access >> VPN Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection: Site to Site VPN (LAN-to-LAN)

Please choose a LAN-to-LAN Profile: [Index] [Status] [Name]

Please choose a Dial-in User Accounts: [Index] [Status] [Name]

Allowed Dial-in Type:

□ PPTP

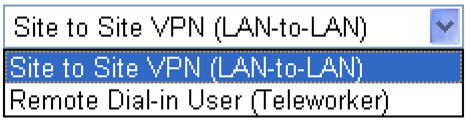
□ IPSec

□ L2TP with IPSec Policy None

VPN Server Mode Selection — Choose the direction for the VPN server.

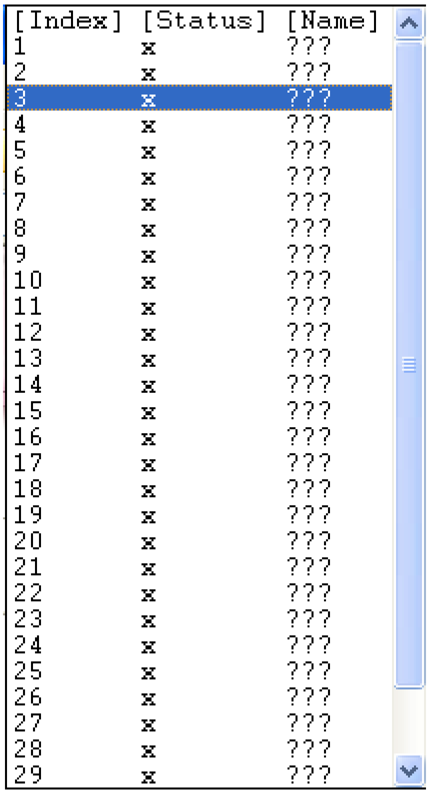
Site to Site VPN/Remote Dial-in User – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.

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.



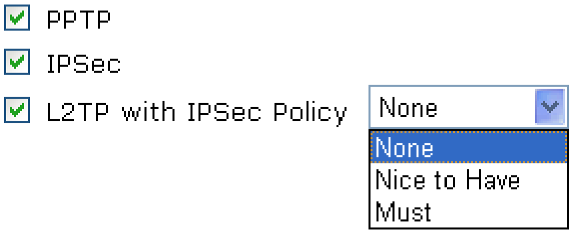
```
[Index] [Status] [Name]
1        x        ???
2        x        ???
3        x        ???
4        x        ???
5        x        ???
6        x        ???
7        x        ???
8        x        ???
9        x        ???
10       x        ???
11       x        ???
12       x        ???
13       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

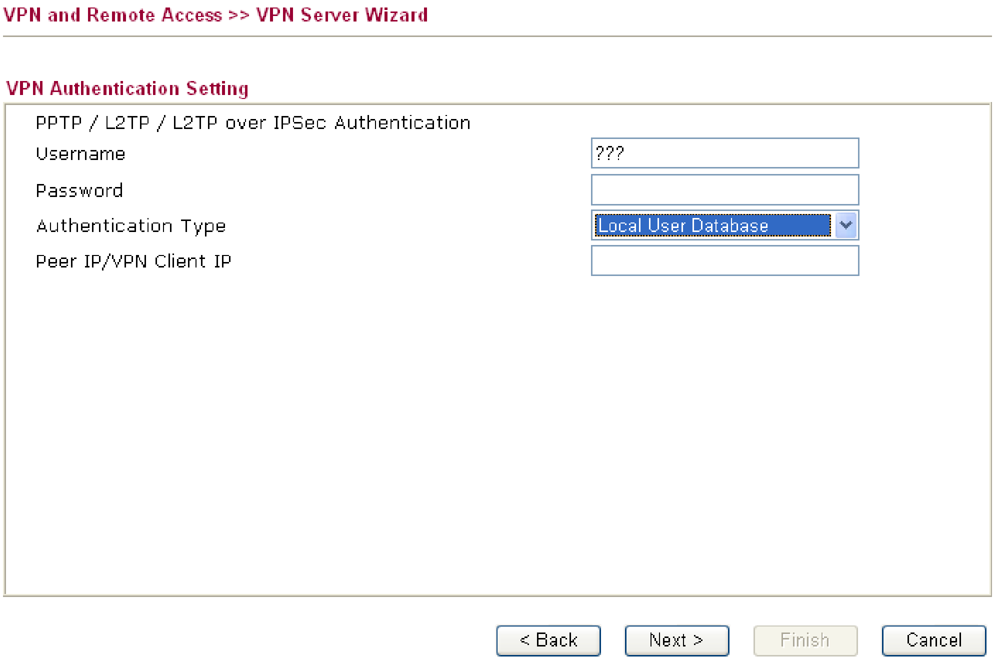
☑ IPSec

☑ L2TP with IPSec Policy [None ▾]

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.

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 example of choosing **Remote-Dial-in User** as the **VPN Server Mode**.

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



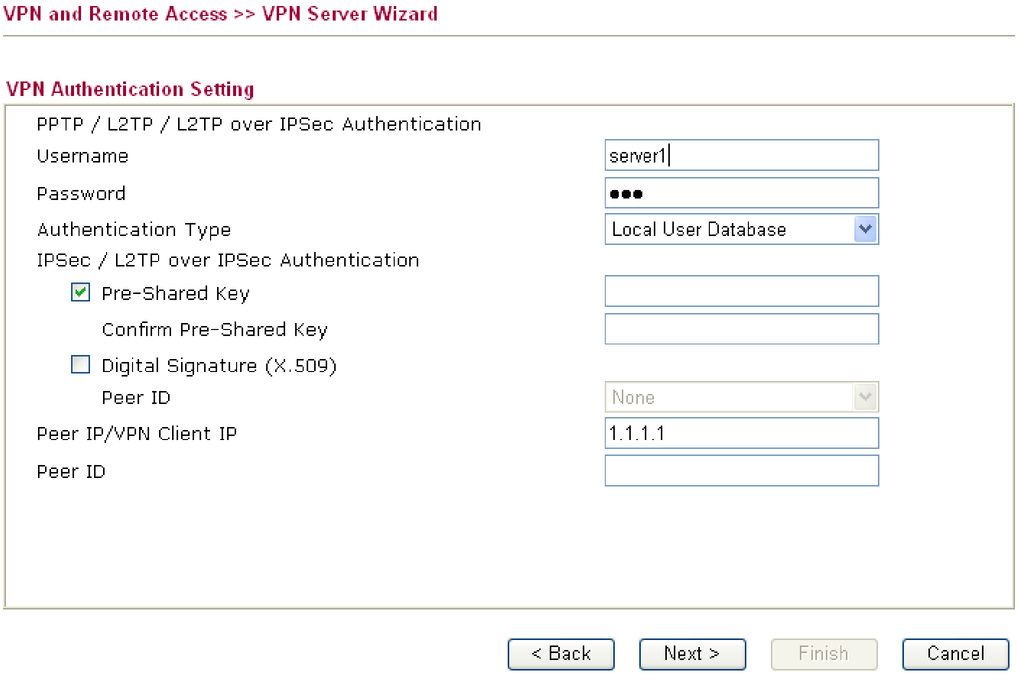
VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

PPTP / L2TP / L2TP over IPSec Authentication

Username	???
Password	
Authentication Type	Local User Database
Peer IP/VPN Client IP	

- 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:



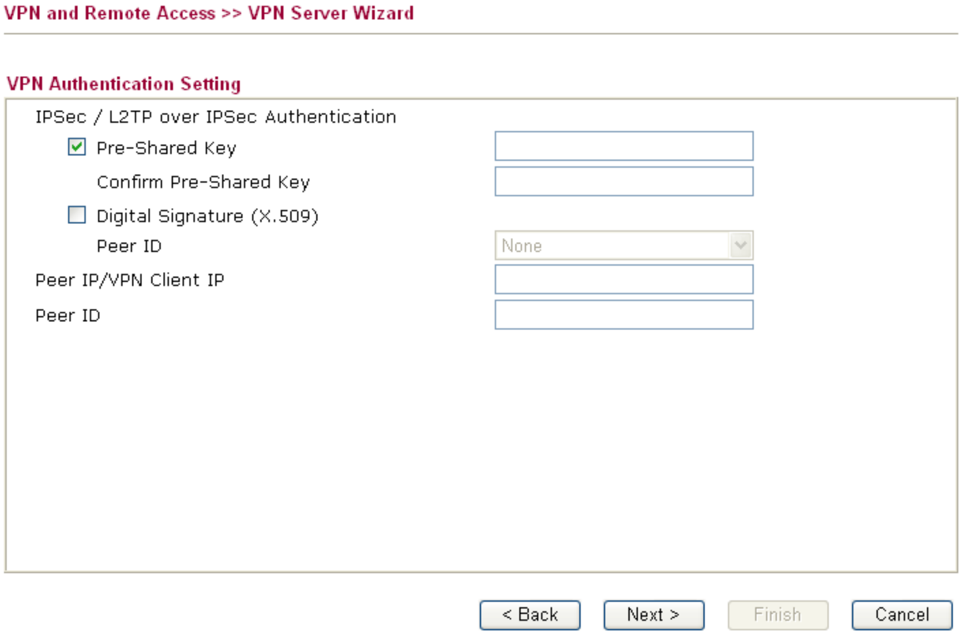
VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

PPTP / L2TP / L2TP over IPSec Authentication

Username	server1
Password	●●●
Authentication Type	Local User Database
IPSec / L2TP over IPSec Authentication	
☑ Pre-Shared Key	
Confirm Pre-Shared Key	
□ Digital Signature (X.509)	
Peer ID	None
Peer IP/VPN Client IP	1.1.1.1
Peer ID	

- When you check **IPSec**, you will see the following graphic:



VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

IPSec / L2TP over IPSec Authentication

☑ Pre-Shared Key

Confirm Pre-Shared Key

□ Digital Signature (X.509)

Peer ID: None

Peer IP/VPN Client IP

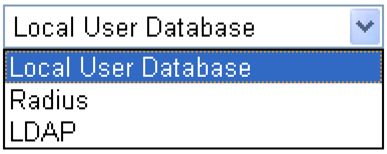
Peer ID

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.

Password This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.

Authentication Type Choose a proper authentication type for VPN connection.



Pre-Shared Key For IPSec/L2TP IPSec authentication, you have to type a pre-shared key.

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.

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.

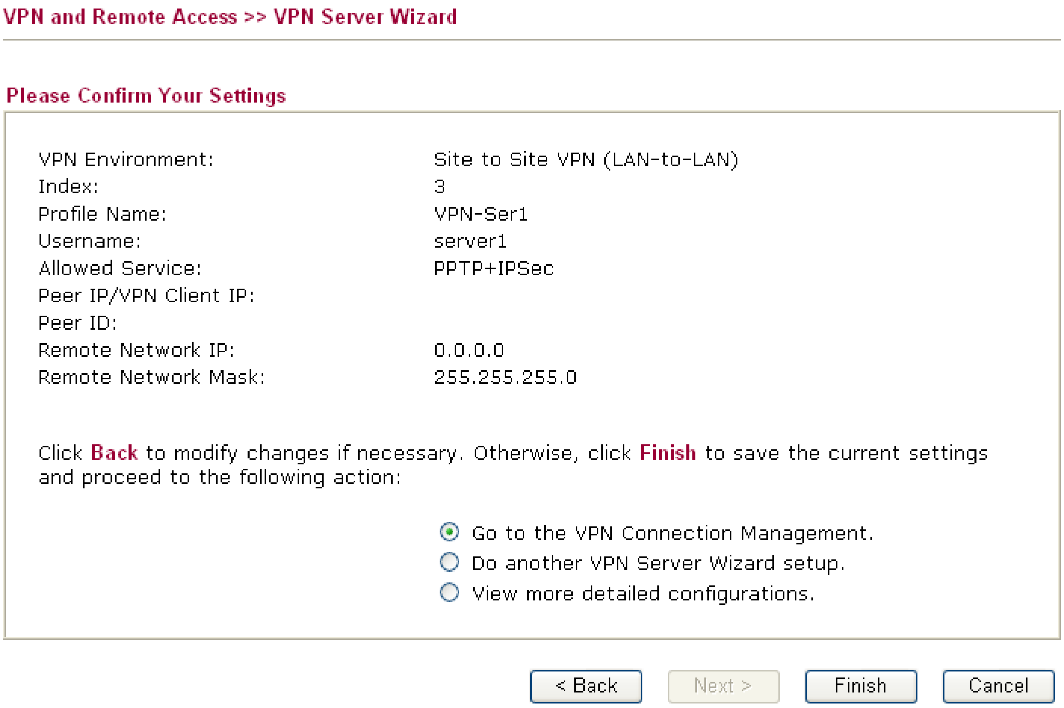
Peer IP/VPN Client IP Type the WAN IP address or VPN client IP address for the remote client.

Peer ID Type the ID name for the remote client.

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

	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.

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 and Remote Access >> VPN Server Wizard

Please Confirm Your Settings

VPN Environment:	Site to Site VPN (LAN-to-LAN)
Index:	3
Profile Name:	VPN-Ser1
Username:	server1
Allowed Service:	PPTP+IPSec
Peer IP/VPN Client IP:	
Peer ID:	
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0

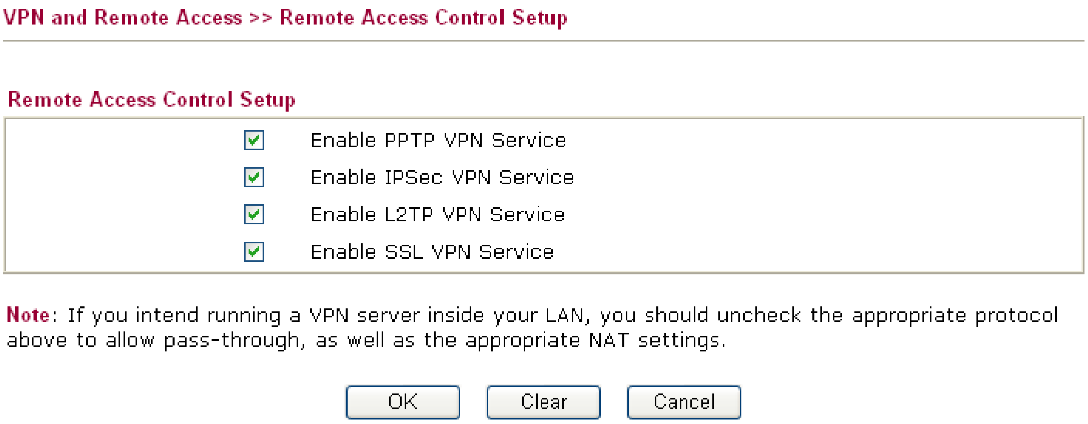
Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and proceed to the following action:

● Go to the VPN Connection Management.
○ Do another VPN Server Wizard setup.
○ View more detailed configurations.

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.

4.10.3 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 (e.g., PPTP VPN, IPSec VPN, L2TP VPN, SSL VPN, etc.) of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.



VPN and Remote Access >> Remote Access Control Setup

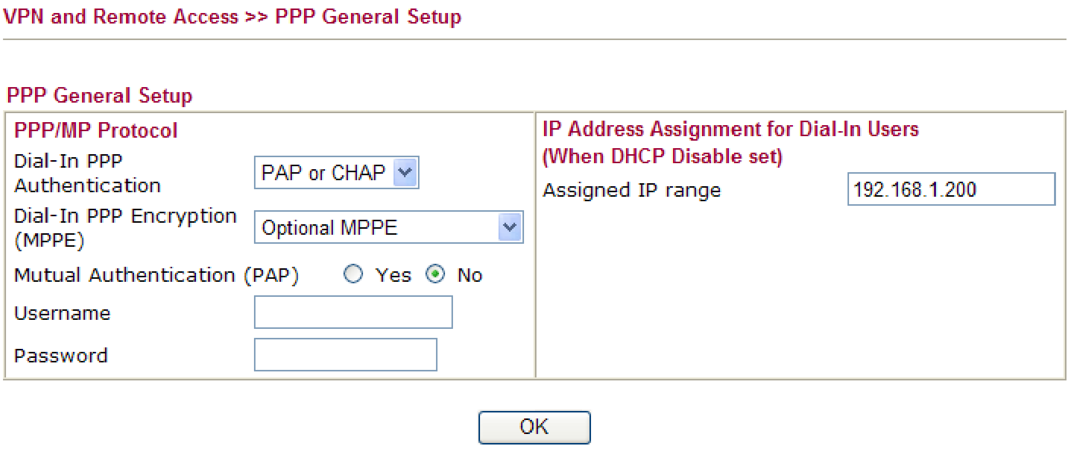
Remote Access Control Setup

☑ Enable PPTP VPN Service
☑ Enable IPSec VPN Service
☑ Enable L2TP VPN Service
☑ Enable SSL VPN Service

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

4.10.4 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 or CHAP

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 range: 192.168.1.200

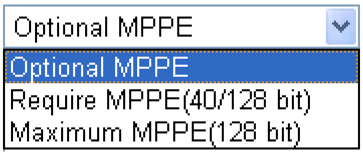
Dial-In PPP Authentication

PAP Only - elect this option to force the router to authenticate dial-in users with the PAP protocol.

PAP or CHAP - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

Dial-In PPP Encryption (MPPE)

Optional MPPE - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit “no MPPE encrypted packets”. Otherwise, the MPPE encryption scheme will be used to encrypt the data.



Optional MPPE

Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.

Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.

Mutual Authentication (PAP)

The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer.

Assigned IP Range

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.

4.10.5 IPSec General Setup

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

There are two phases of IPSec.

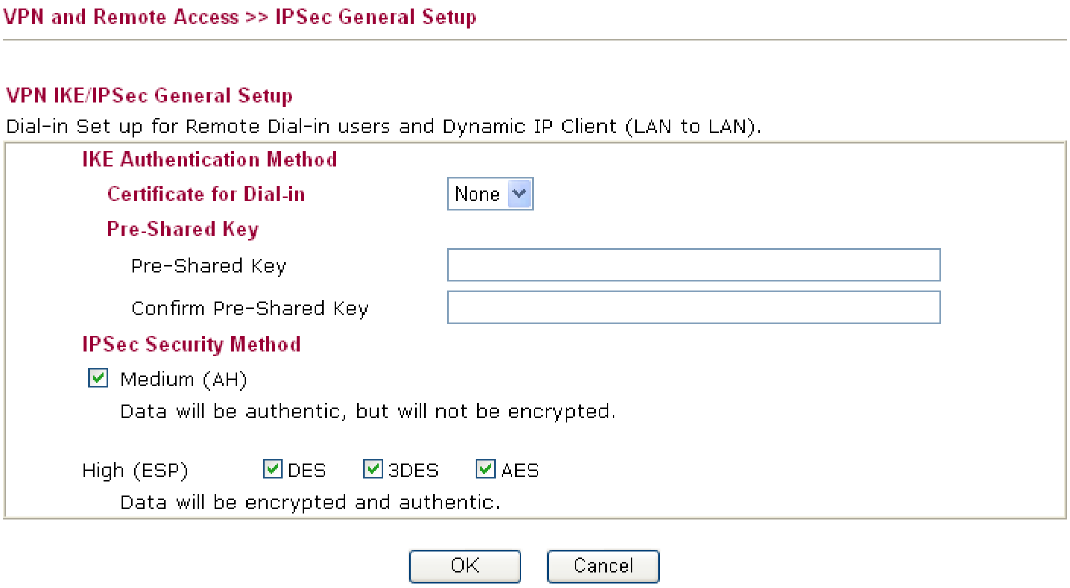
- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies 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.

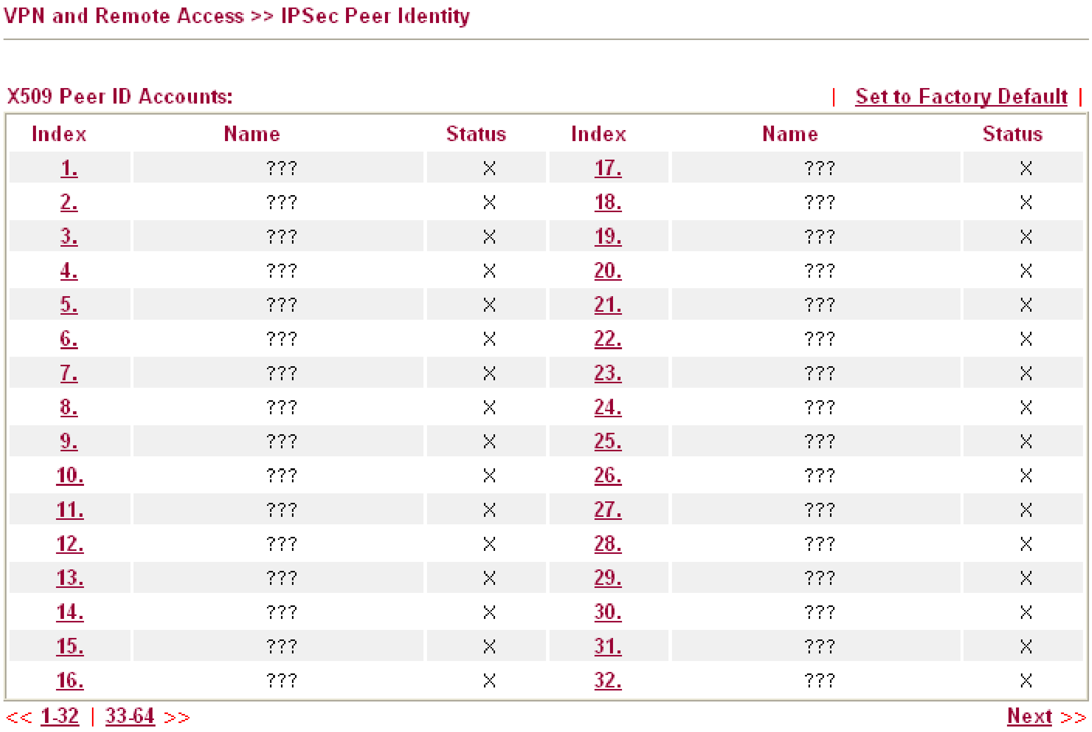
High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

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. **Pre-Shared Key** -Currently only support Pre-Shared Key authentication. **Pre-Shared Key-** Specify a key for IKE authentication **Confirm Pre-Shared Key-** Retype the characters to confirm the pre-shared key.
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.

4.10.6 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

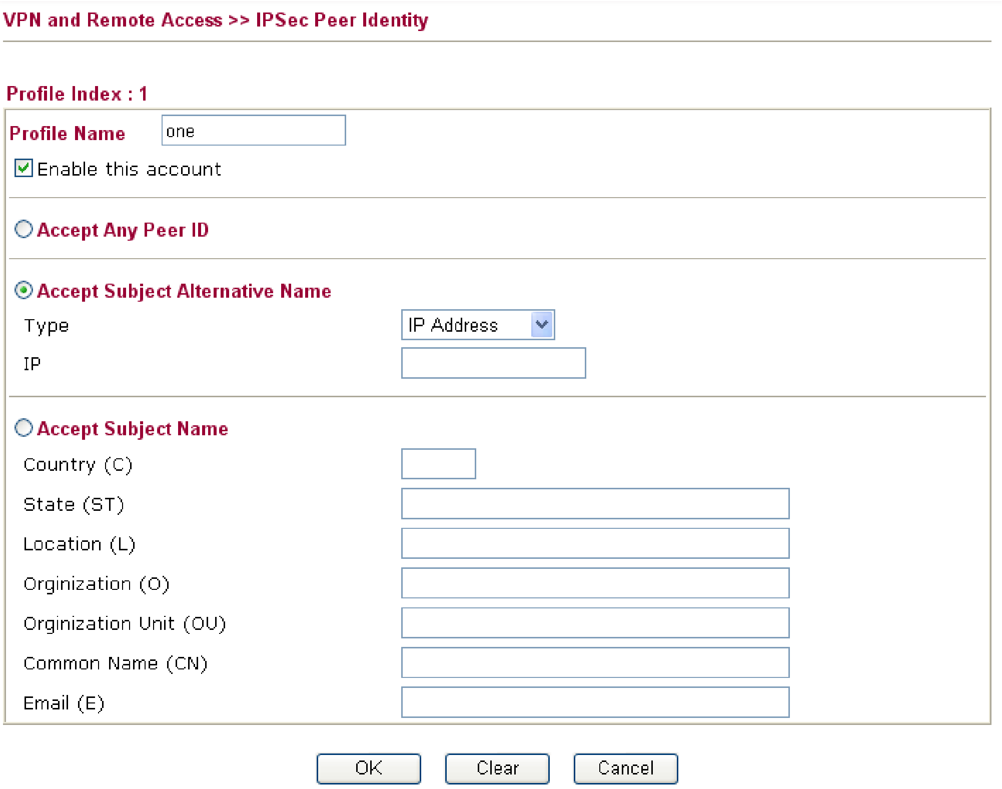
X509 Peer ID Accounts: | Set to Factory Default |

Index	Name	Status	Index	Name	Status
1.	???	×	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 >>

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.



VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1

Profile Name: one

☑ Enable this account

○ Accept Any Peer ID

● Accept Subject Alternative Name

Type	IP Address
IP	

○ Accept Subject Name

Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	

Profile Name Type the name of the profile.

Accept Any Peer ID Click to accept any peer regardless of its identity.

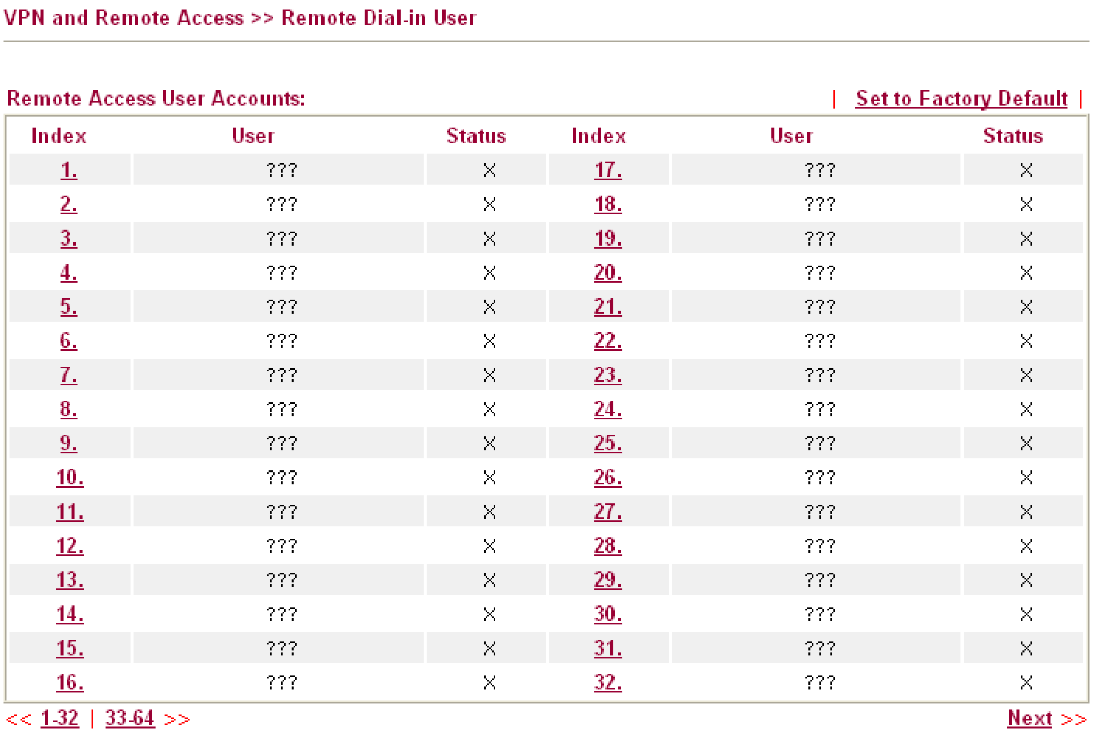
Accept Subject Alternative Name Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail Address**. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.

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)**.

4.10.7 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 **64** 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	Status	Index	User	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

<< 1-32 | 33-64 >> Next >>

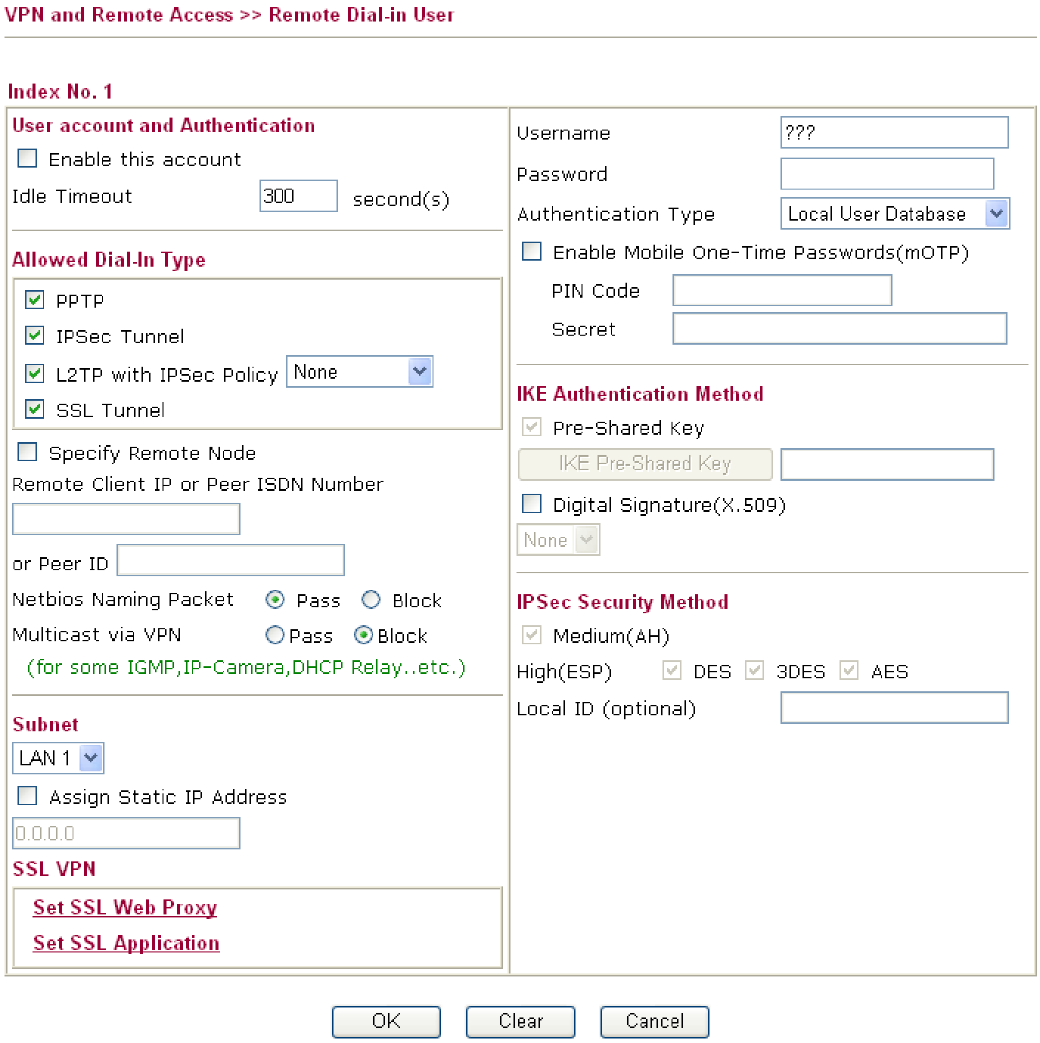
Set to Factory Default Click to clear all indexes.

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.

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. 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 ISDN Number

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 Web Proxy

Set SSL Application

Username ???

Password

Authentication Type Local User Database

□ 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)

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 - 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-You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).

Uncheck the checkbox-This 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.

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.

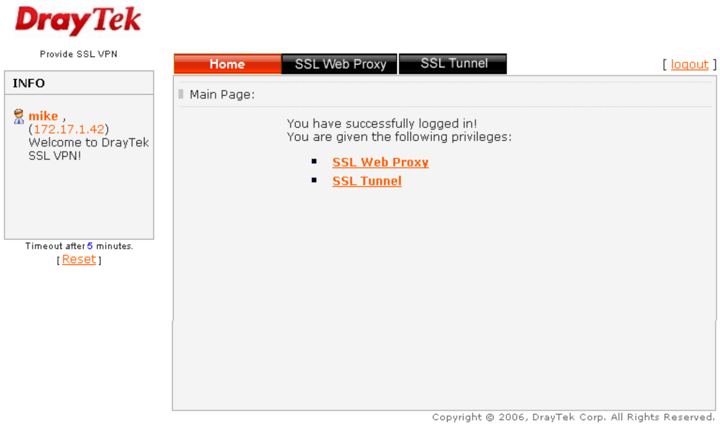
Assign Static IP Address – Please type a static IP address for the subnet you specified.

SSL VPN

Set SSL Web Proxy - It allows the remote dial-in user to access internal web over SSL VPN, suitable for the application through web only (e.g., HTTP). Click **SSL VPN>> SSL Web Proxy** to set profiles.

If you have set several profiles beforehand, you can check SSL Web Proxy and choose the one(s) you need as SSL VPN.

To check if SSL Web Proxy is activated or not, please open Draytek SSL VPN portal interface. From the web page, you will see the message to indicate that you have the privilege for the SSL Web Proxy.



mike ,
(172.17.1.42)
Welcome to DrayTek SSL VPN!

Main Page:

You have successfully logged in!
You are given the following privileges:

- SSL Web Proxy
- SSL Tunnel

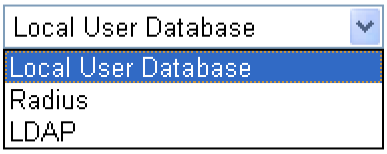
If you haven't set any SSL VPN web proxy profiles, you will a link here. Click this link to access into the configuration page of SSL VPN.

Note: SSL VPN can be applied in browser (e.g., IE) which supports ActivateX only.

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.

Authentication Type Choose an authentication type for VPN connection.



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 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 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.

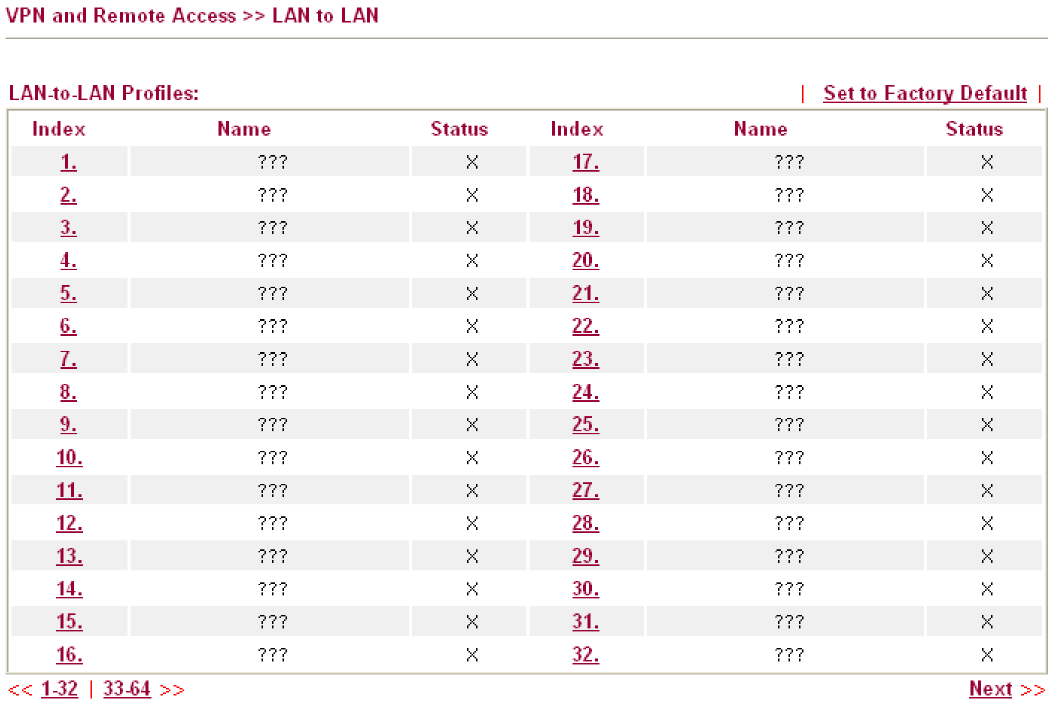
High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

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.

4.10.8 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 **64** VPN tunnels simultaneously. The following figure shows the summary table.



VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | Set to Factory Default |

Index	Name	Status	Index	Name	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.	???	×

<< 1-32 | 33-64 >> Next >>

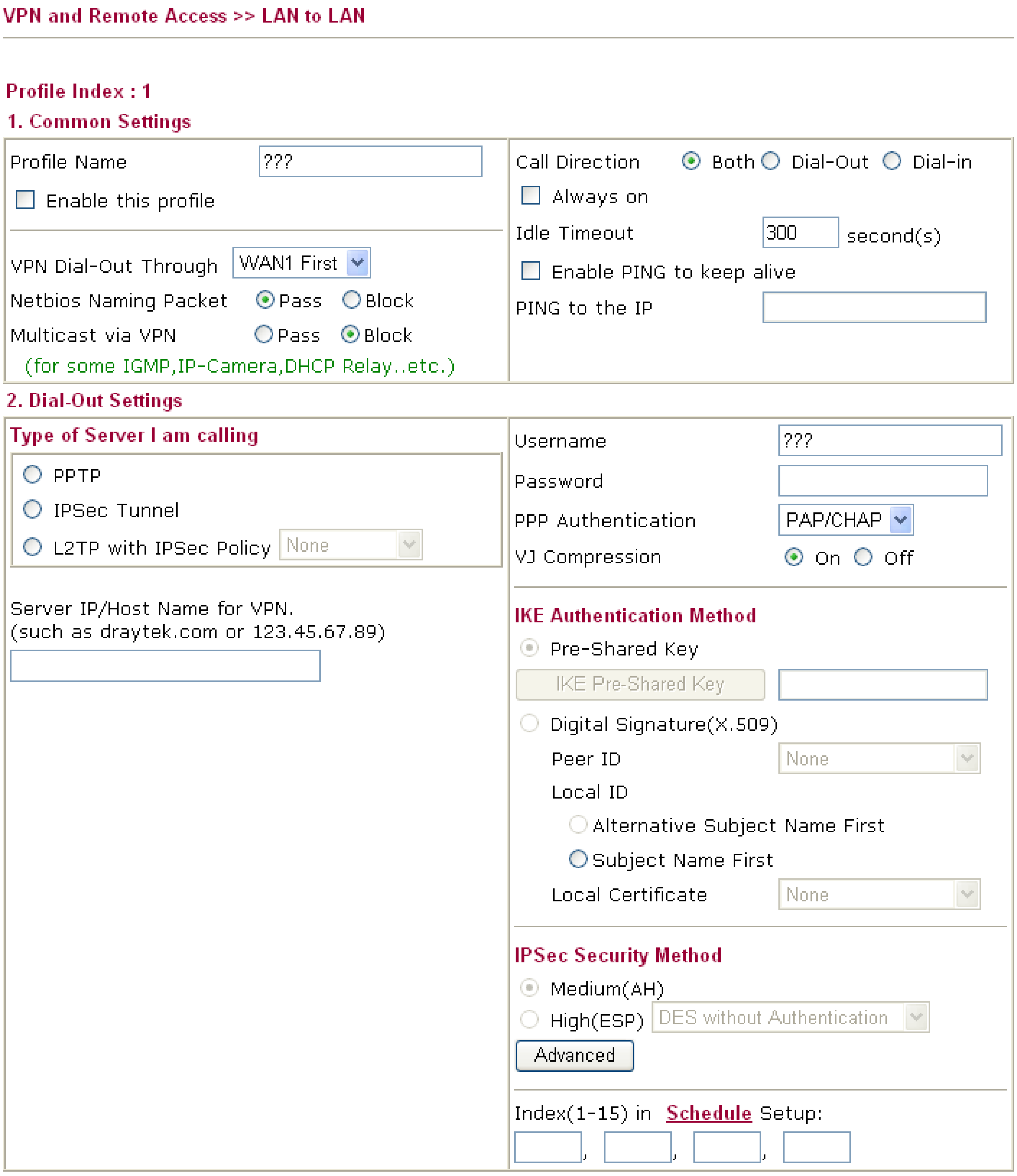
Set to Factory Default Click to clear all indexes.

Name Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.

Status Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

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.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: ???

□ Enable this profile

VPN Dial-Out Through: WAN1 First

Netbios Naming Packet ● Pass ○ Block

Multicast via VPN ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction ● Both ○ Dial-Out ○ Dial-in

□ Always on

Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

○ IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE 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

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

Profile Name Specify a name for the profile of the LAN-to-LAN connection.

Enable this profile Check here to activate this profile.

VPN Dial-Out Through Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.

WAN1 /WAN2 /WAN3 /WAN4 /WAN5 First - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.
WAN1 /WAN2 /WAN3 /WAN4 /WAN5 Only - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the only channel for VPN connection.

Netbios Naming Packet **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

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

Multicast via VPN

Some programs might send multicast packets via VPN connection.

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

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

Call Direction

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

Both:-initiator/responder

Dial-Out- initiator only

Dial-In- responder only.

Always On or Idle Timeout

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.

PING to the IP

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

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).

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.

Password

This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

PPP Authentication

This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP 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) – Check the box of Digital Signature to invoke this function. Then, specify the following items for authentication with digital signature.

- **Peer ID -** Select one of the predefined Profiles set in **VPN and Remote Access >>IPSec Peer Identity.**
- **Local ID –** Specify a local ID **(Alternative Subject Name First** or **Subject Name First)** to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

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

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.

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

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

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

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

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

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

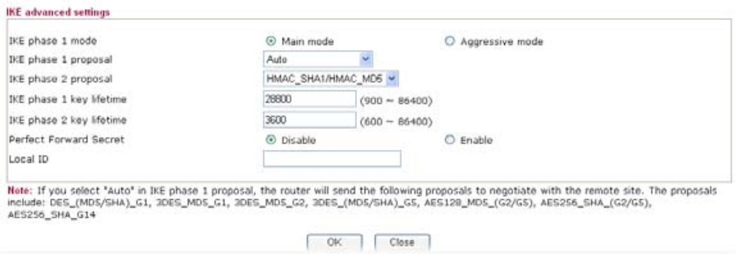
AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.

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

Advanced

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

The window of advance setup is shown as below:



IKE advanced settings

IKE phase 1 mode	● Main mode	○ Aggressive mode
IKE phase 1 proposal	Auto	
IKE phase 2 proposal	HMAC_SHA1/HMAC_MD5	
IKE phase 1 key lifetime	28800 (900 ~ 86400)	
IKE phase 2 key lifetime	3600 (600 ~ 86400)	
Perfect Forward Secret	● Disable	○ Enable
Local ID		

Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MD5/SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5/SHA)_G5, AES128_MD5_(G2/G5), AES256_SHA_(G2/G5), AES256_SHA_G14

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.

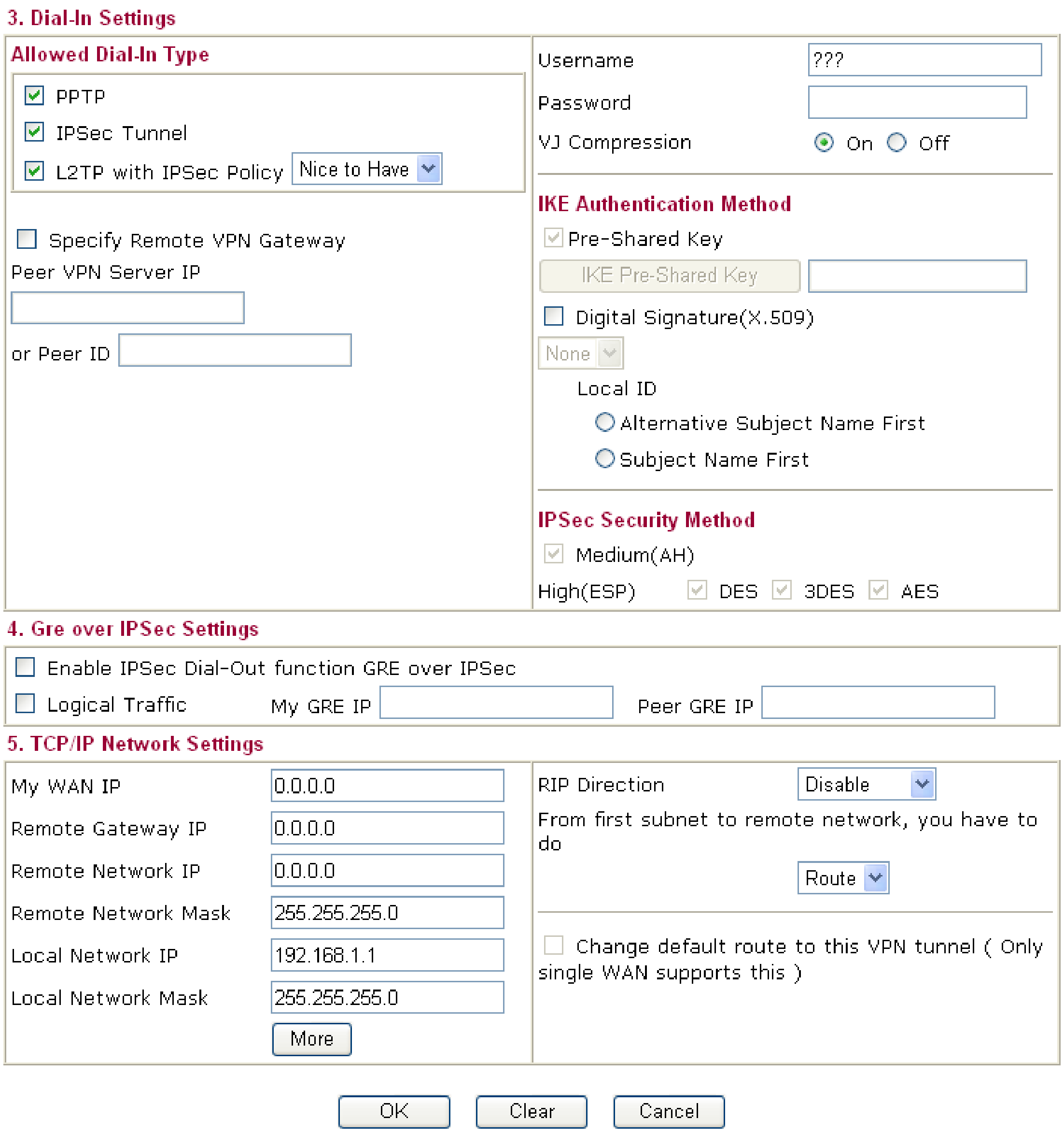
IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

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.



3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy [Nice to Have]

□ Specify Remote VPN Gateway

Peer VPN Server IP

or Peer ID

Username	???
Password	
VJ Compression	● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

None

Local ID

○ Alternative Subject Name First

○ Subject Name First

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

4. Gre over IPSec Settings

□ Enable IPSec Dial-Out function GRE over IPSec

□ Logical Traffic My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0

RIP Direction [Disable]

From first subnet to remote network, you have to do [Route]

□ Change default route to this VPN tunnel (Only single WAN supports this)

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.

Password - This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

VJ Compression – VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.

Pre-Shared Key – Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.

Digital Signature (X.509) –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.

- **Local ID –** Specify 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.

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.
Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.

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

Gre Over IPSec Settings

Enable IPSec Dial-Out function GRE over IPSec - Check this box to verify data and transmit data in encryption with GRE over IPSec packet after configuring IPSec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.

Logical Traffic - Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPSec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.

TCP/IP Network Settings

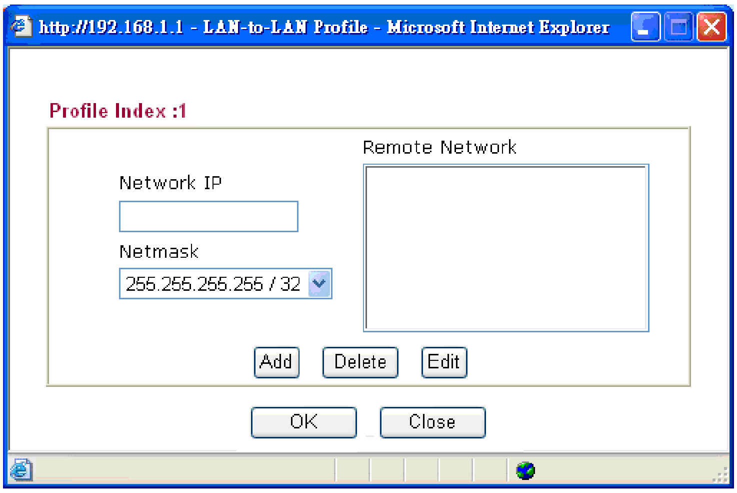
My WAN IP - This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify 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.



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.

4.10.9 VPN TRUNK Management

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

Features of VPN TRUNK – VPN Backup Mechanism

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

- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and ISDN (depends on hardware specification)
- The web page is simple to understand and easy to configure
- Filly compliant with VPN Server LAN Sit Single/Multi Network
- Mail Alert support, please refer to **System Maintenance** >> **SysLog / Mail Alert** for detailed configuration
- Syslog support, please refer to **System Maintenance** >> **SysLog / Mail Alert** for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

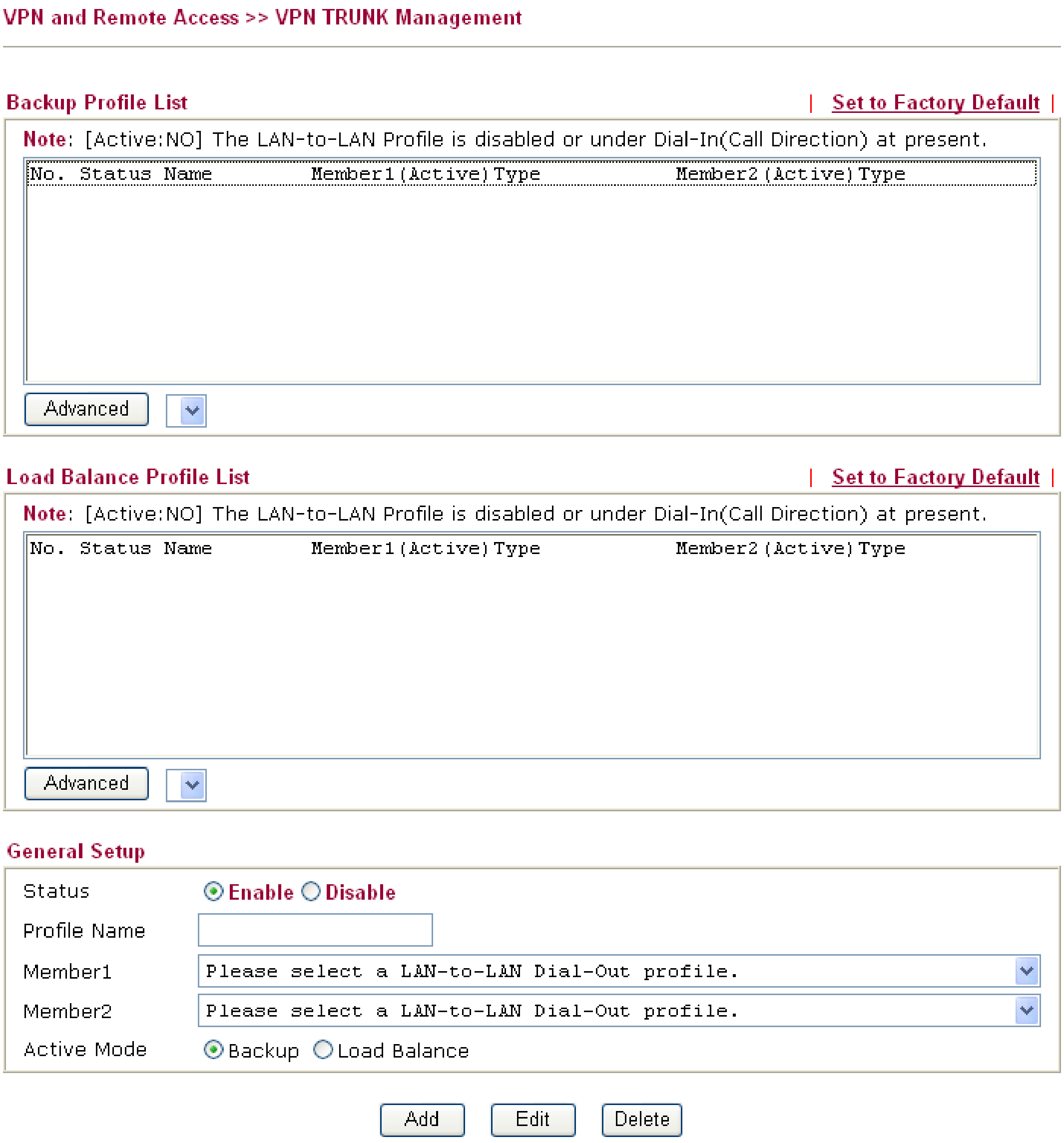
VPN TRUNK-VPN Backup mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will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

Features of VPN TRUNK – VPN Load Balance Mechanism

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

- Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest
- Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and GRE over IPSec

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



VPN and Remote Access >> VPN TRUNK Management

Backup Profile List | Set to Factory Default |

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

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

Load Balance Profile List | Set to Factory Default |

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

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

General Setup

Status	● Enable ○ Disable
Profile Name	
Member1	Please select a LAN-to-LAN Dial-Out profile.
Member2	Please select a LAN-to-LAN Dial-Out profile.
Active Mode	● Backup ○ Load Balance

Backup Profile List

Set to Factory Default - Click to clear all VPN TRUNK-VPN Backup mechanism profile.

No – The order of VPN TRUNK-VPN Backup mechanism profile.

Status (on Backup Profile field) - "v" means such profile is enabled; "x" means such profile is disabled.

Name (on Backup Profile field) - Display the name of VPN TRUNK-VPN Backup mechanism profile.

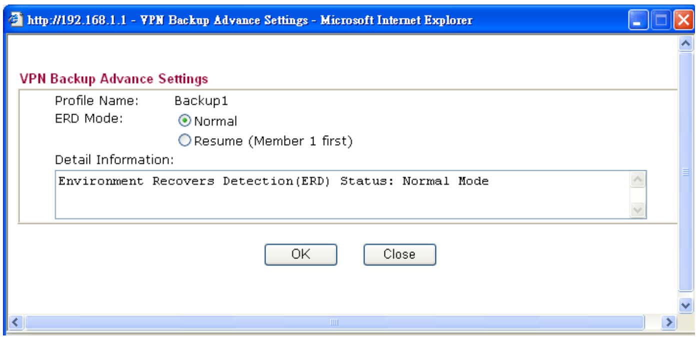
Member1 (on Backup Profile field) - Display the dial-out profile selected from the Member1 drop down list below.

Active (on Backup Profile field) - "Yes" means normal condition. ”No” means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.

Type (on Backup Profile field) - Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.

Member2 (on Backup Profile field) - Display the dial-out profile selected from the Member2 drop down list below.

Advanced – This button is available only when LAN to LAN profile (or more) is created.


http://192.168.1.1 - VPN Backup Advance Settings - Microsoft Internet Explorer
OK
Close

VPN Backup Advance Settings

Profile Name: Backup1

ERD Mode: ● Normal ○ Resume (Member 1 first)

Detail Information:

```
Environment Recovers Detection(ERD) Status: Normal Mode
```

Detailed information for this dialog, see later section - **Advanced Load Balance and Backup**.

Load Balance Profile List

Set to Factory Default - Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.
No - The order of VPN TRUNK-VPN Load Balance mechanism profile.

Status - “v” means such profile is enabled; ”x” means such profile is disabled.

Name - Display the name of VPN TRUNK-VPN Load Balance mechanism profile.

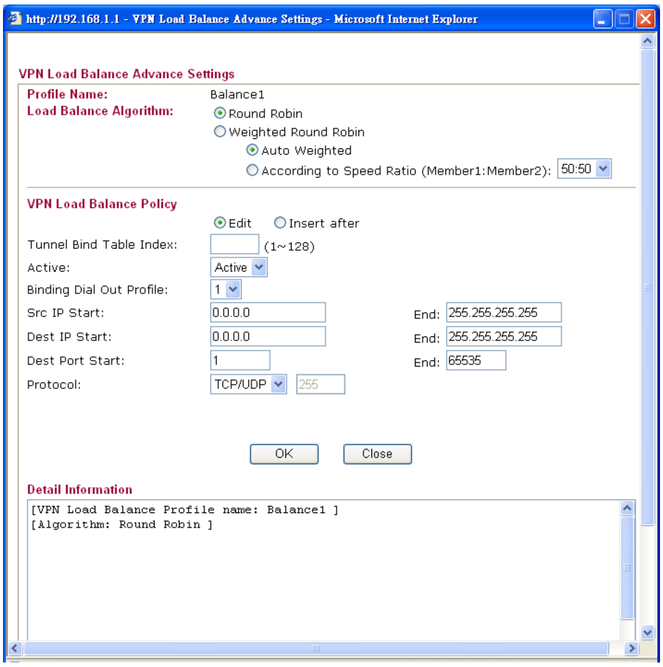
Member1 - Display the dial-out profile selected from the Member1 drop down list below.

Active - “Yes” means normal condition. ”No” means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.

Type - Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.

Member2 - Display the dial-out profile selected from the Member2 drop down list below.

Advanced – This button is only available when there is one or more profiles created in this page.



http://192.168.1.1 - VPN Load Balance Advance Settings - Microsoft Internet Explorer

VPN Load Balance Advance Settings

Profile Name: Balance1

Load Balance Algorithm: ● Round Robin

○ Weighted Round Robin

● Auto Weighted

○ According to Speed Ratio (Member1:Member2): 50:50

VPN Load Balance Policy

● Edit ○ Insert after

Tunnel Bind Table Index:	(1~128)		
Active:	Active		
Binding Dial Out Profile:	1		
Src IP Start:	0.0.0.0	End:	255.255.255.255
Dest IP Start:	0.0.0.0	End:	255.255.255.255
Dest Port Start:	1	End:	65535
Protocol:	TCP/UDP 255		

Detail Information

```
[VPN Load Balance Profile name: Balance1 ]
[Algorithm: Round Robin ]
```

Detailed information for this dialog, see later section - **Advanced Load Balance and Backup**.

General Setup

Status- After choosing one of the profile listed above, please click **Enable** to activate this profile. If you click **Disable**, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.

Profile Name- Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields.

Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in **VPN and Remote Access >> LAN-to-LAN**) for you to choose for grouping under certain VPN TRUNK-VPN Backup/Load Balance mechanism profile.

No - Index number of LAN-to-LAN dial-out profile.

Name - Profile name of LAN-to-LAN dial-out profile.

Connection Type - Connection type of LAN-to-LAN dial-out profile.

VPN ServerIP (Private Network) - VPN Server IP of LAN-to-LAN dial-out profiles.

Aactive Mode - Display available mode for you to choose. Choose **Backup** or **Load Balance** for your router.

Add

Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK – VPN Backup mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in red. VPN TRUNK – VPN Load Balance mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in blue.

Edit Click this button to save the changes to the **Status** (Enable or Disable), profile name, member1 or member2.

Delete Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

Time for activating VPN TRUNK – VPN Backup mechanism profile

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

Time for activating VPN TRUNK – VPN Load Balance mechanism profile

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

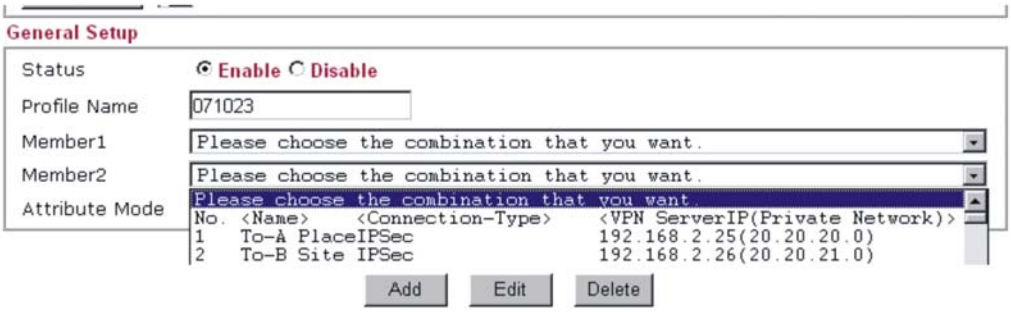
Time for activating VPN TRUNK –Dial-out when VPN Load Balance Disconnected

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

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

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

1. First of all, go to **VPN and Remote Access>>LAN-to-LAN**. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup /Load Balance mechanism profile management well.
2. Access into **VPN and Remote Access>>VPN TRUNK Management**.
3. Set one group of VPN TRUNK – VPN Backup/Load Balance mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.



General Setup

Status ● Enable ○ Disable

Profile Name 071023

Member1 Please choose the combination that you want.

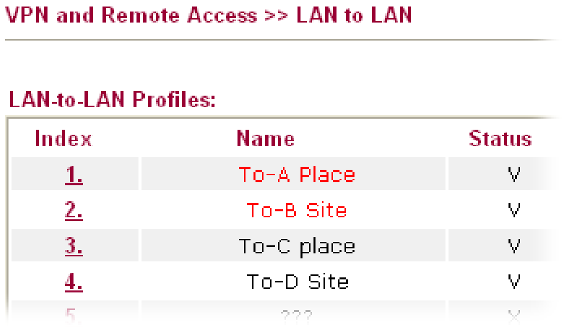
Member2 Please choose the combination that you want.

Attribute Mode

```
Please choose the combination that you want.
No. <Name>      <Connection-Type>    <VPN ServerIP(Private Network)>
1   To-A PlaceIPSec                  192.168.2.25(20.20.20.0)
2   To-B Site IPSec                  192.168.2.26(20.20.21.0)
```

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

Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.



VPN and Remote Access >> LAN to LAN

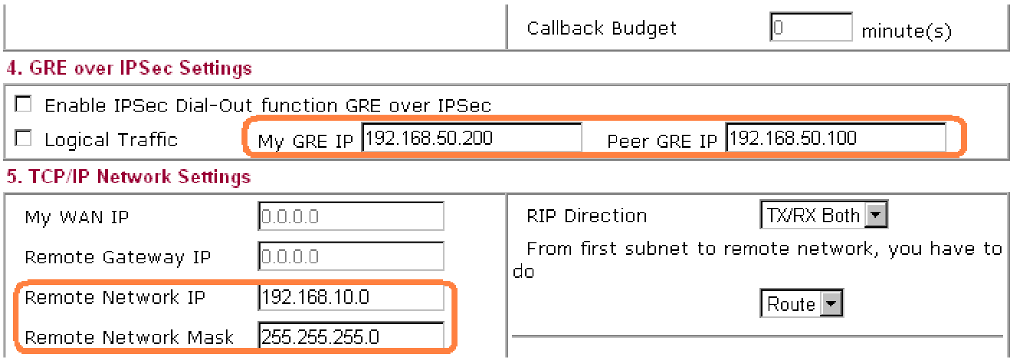
LAN-to-LAN Profiles:

Index	Name	Status
1.	To-A Place	V
2.	To-B Site	V
3.	To-C place	V
4.	To-D Site	V
5.	???	X

How can you set a GRE over IPSec profile?

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

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



Callback Budget 0 minute(s)

4. GRE over IPSec Settings

☐ Enable IPSec Dial-Out function GRE over IPSec

☐ Logical Traffic My GRE IP 192.168.50.200 Peer GRE IP 192.168.50.100

5. TCP/IP Network Settings

My WAN IP 0.0.0.0

Remote Gateway IP 0.0.0.0

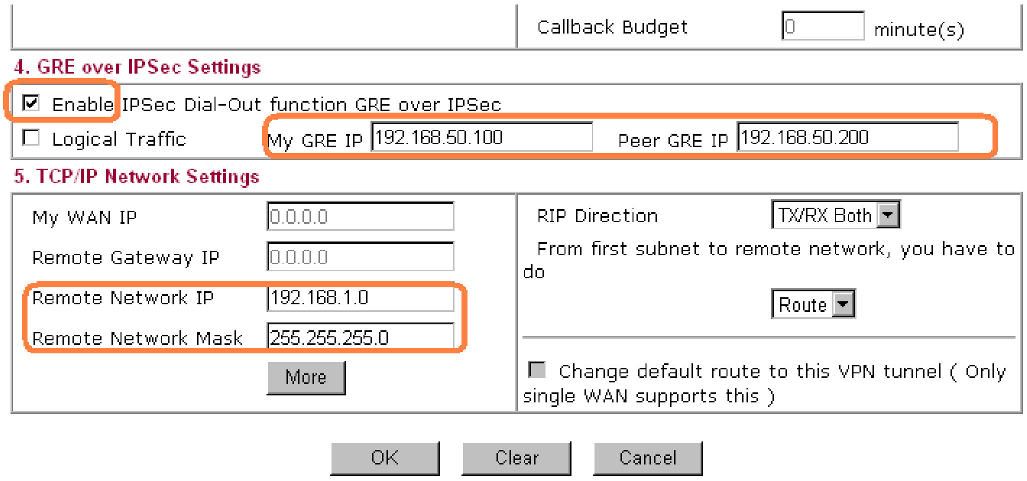
Remote Network IP 192.168.10.0

Remote Network Mask 255.255.255.0

RIP Direction TX/RX Both

From first subnet to remote network, you have to do Route

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



Callback Budget 0 minute(s)

4. GRE over IPSec Settings

☑ Enable IPSec Dial-Out function GRE over IPSec

☐ Logical Traffic My GRE IP 192.168.50.100 Peer GRE IP 192.168.50.200

5. TCP/IP Network Settings

My WAN IP 0.0.0.0

Remote Gateway IP 0.0.0.0

Remote Network IP 192.168.1.0

Remote Network Mask 255.255.255.0

RIP Direction TX/RX Both

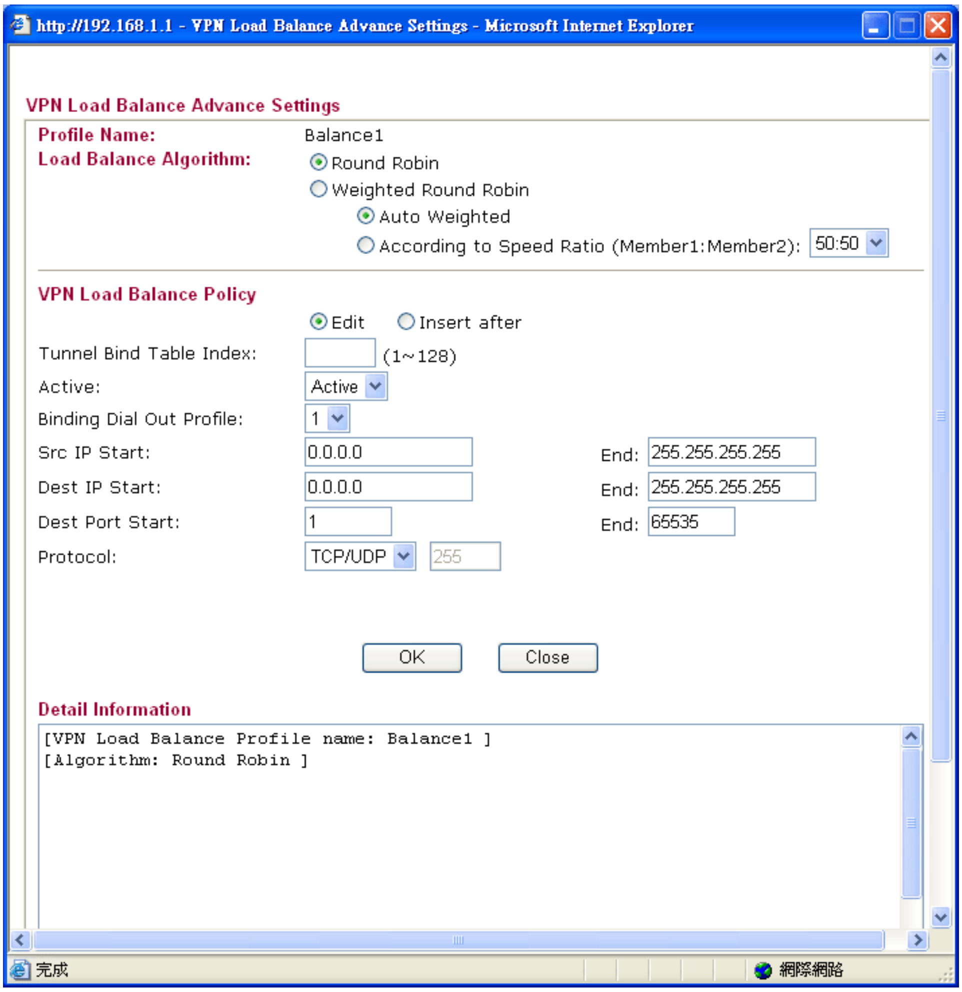
From first subnet to remote network, you have to do Route

☐ Change default route to this VPN tunnel (Only single WAN supports this)

Advanced Load Balance and Backup

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

Advanced Load Balance



http://192.168.1.1 - VPN Load Balance Advance Settings - Microsoft Internet Explorer

VPN Load Balance Advance Settings

Profile Name: Balance1

Load Balance Algorithm:
● Round Robin
○ Weighted Round Robin
● Auto Weighted
○ According to Speed Ratio (Member1:Member2): 50:50

VPN Load Balance Policy

● Edit ○ Insert after

Tunnel Bind Table Index: (1~128)

Active: Active

Binding Dial Out Profile: 1

Src IP Start: 0.0.0.0 End: 255.255.255.255

Dest IP Start: 0.0.0.0 End: 255.255.255.255

Dest Port Start: 1 End: 65535

Protocol: TCP/UDP 255

Detail Information

```
[VPN Load Balance Profile name: Balance1 ]
[Algorithm: Round Robin ]
```

Profile Name List the load balance profile name.

Load Balance Algorithm **Round Robin** – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.

Weighted Round Robin –Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. **Auto Weighted** can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. **According to Speed Ratio** allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).

VPN Load Balance Policy Below shows the algorithm for Load Balance.

Edit – Click this radio button for assign a blank table for configuring Binding Tunnel.

After insert – Click this radio button to adding a new binding tunnel table.

Tunnel Bind Table Index- 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile.

Active – In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.

Binding Dial Out Index – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.

Scr IP Start /End– Specify source IP addresses as starting point and ending point.

Dest IP Start/End – Specify destination IP addresses as starting point and ending point.

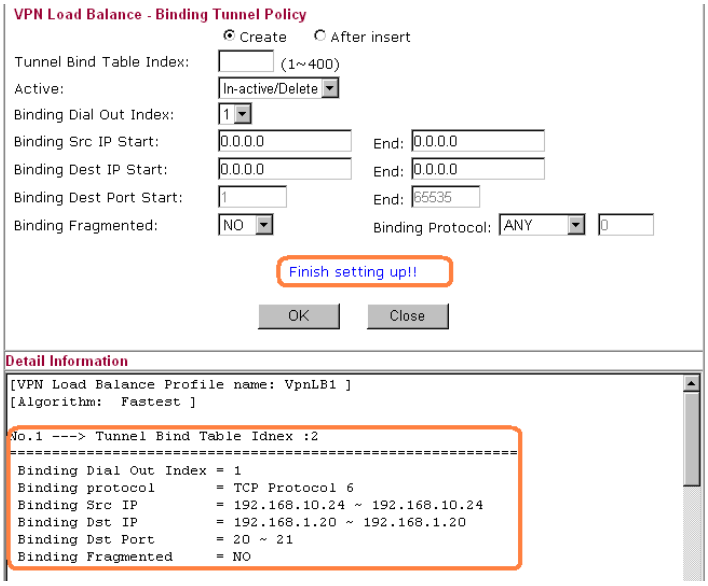
Dest Port Start /End– Specify destination service port as starting point and ending point.

Protocol – **Any** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/UDP Service Port/ICMP/IGMP specified here.

TCP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. **UDP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. **TCP/UPD** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. **ICMP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. IGMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. **Other** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.

Detail Information

This field will display detailed information for Binding Tunnel Policy. Below shows a successful binding tunnel policy for load balance:



VPN Load Balance - Binding Tunnel Policy

● Create ○ After insert

Tunnel Bind Table Index: (1~400)

Active: In-active/Delete

Binding Dial Out Index: 1

Binding Src IP Start: 0.0.0.0 End: 0.0.0.0

Binding Dest IP Start: 0.0.0.0 End: 0.0.0.0

Binding Dest Port Start: 1 End: 65535

Binding Fragmented: NO Binding Protocol: ANY 0

Finish setting up!!

Detail Information

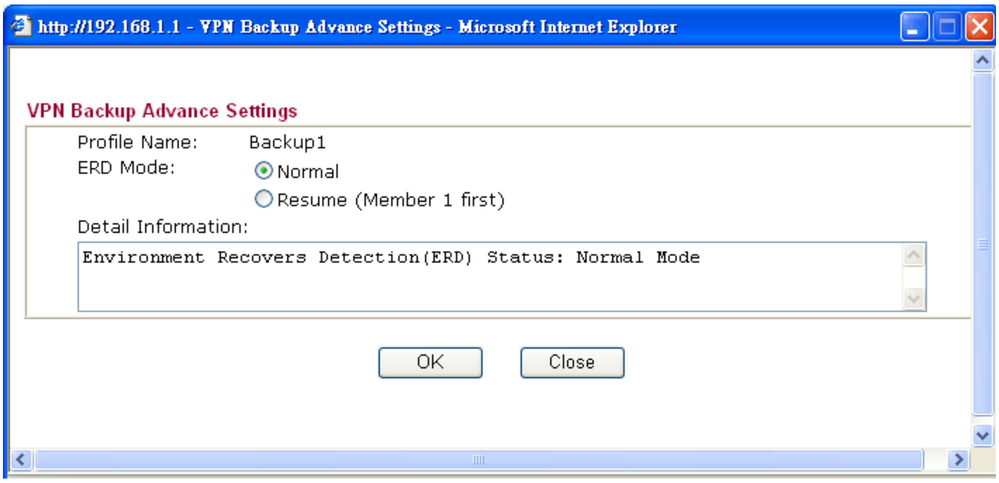
```
[VPN Load Balance Profile name: VpnLB1 ]
[Algorithm:  Fastest ]

No.1 ---> Tunnel Bind Table Idnex :2
=========================================================
 Binding Dial Out Index = 1
 Binding protocol       = TCP Protocol 6
 Binding Src IP         = 192.168.10.24 ~ 192.168.10.24
 Binding Dst IP         = 192.168.1.20 ~ 192.168.1.20
 Binding Dst Port       = 20 ~ 21
 Binding Fragmented     = NO
```

以上的範例，這邊做不成功，請協助提供一張，TKS!

Note : To configure a successful binding tunnel, you have to:

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

Advanced Backup



http://192.168.1.1 - VPN Backup Advance Settings - Microsoft Internet Explorer

VPN Backup Advance Settings

Profile Name: Backup1

ERD Mode: ● Normal ○ Resume (Member 1 first)

Detail Information:

```
Environment Recovers Detection(ERD) Status: Normal Mode
```

Profile Name List the backup profile name.

ERD Mode ERD means “Environment Recovers Detection”.

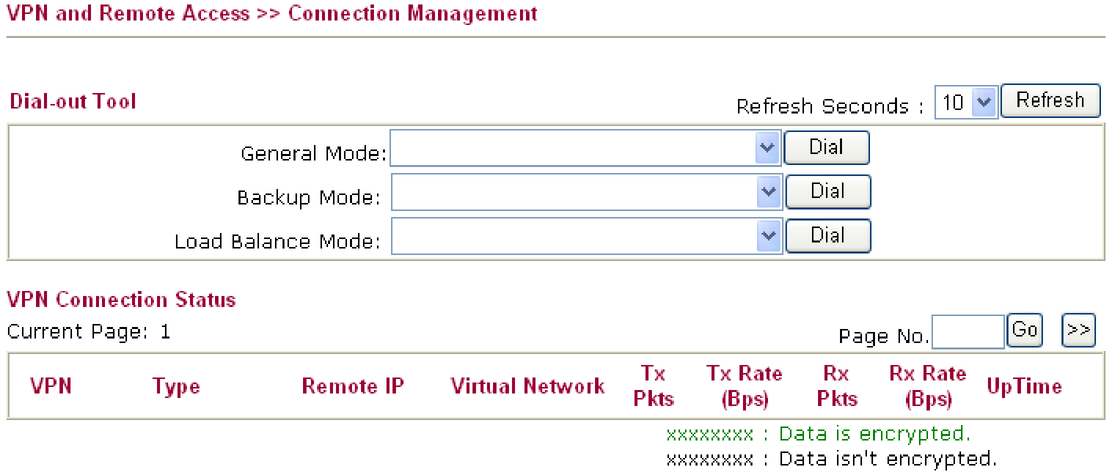
Normal – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively.

Resume – when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.

Detail Information This field will display detailed information for Environment Recovers Detection.

4.10.10 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

General Mode:

Backup Mode:

Load Balance Mode:

VPN Connection Status

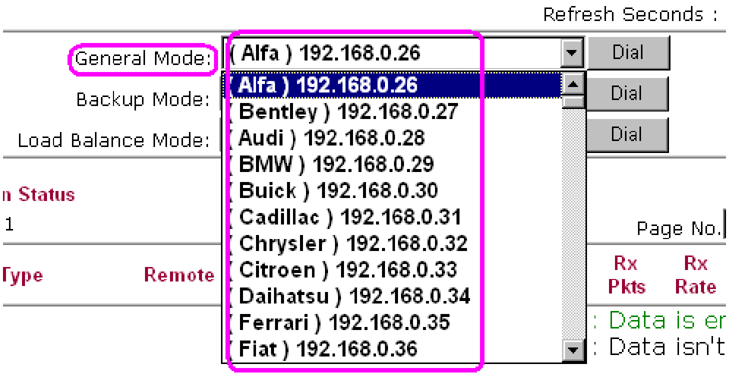
Current Page: 1

Page No.

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.

General Mode This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.


Refresh Seconds :

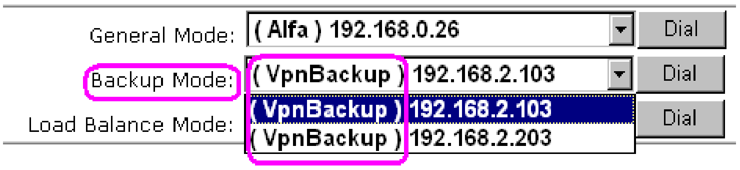
General Mode: (Alfa) 192.168.0.26

(Alfa) 192.168.0.26
(Bentley) 192.168.0.27
(Audi) 192.168.0.28
(BMW) 192.168.0.29
(Buick) 192.168.0.30
(Cadillac) 192.168.0.31
(Chrysler) 192.168.0.32
(Citroen) 192.168.0.33
(Daihatsu) 192.168.0.34
(Ferrari) 192.168.0.35
(Fiat) 192.168.0.36

Backup Mode:

Load Balance Mode:

Backup Mode This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.


General Mode: (Alfa) 192.168.0.26

Backup Mode: (VpnBackup) 192.168.2.103

(VpnBackup) 192.168.2.103
(VpnBackup) 192.168.2.203

Load Balance Mode:

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.

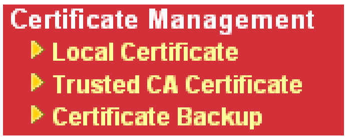
4.11 Certificate Management

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.

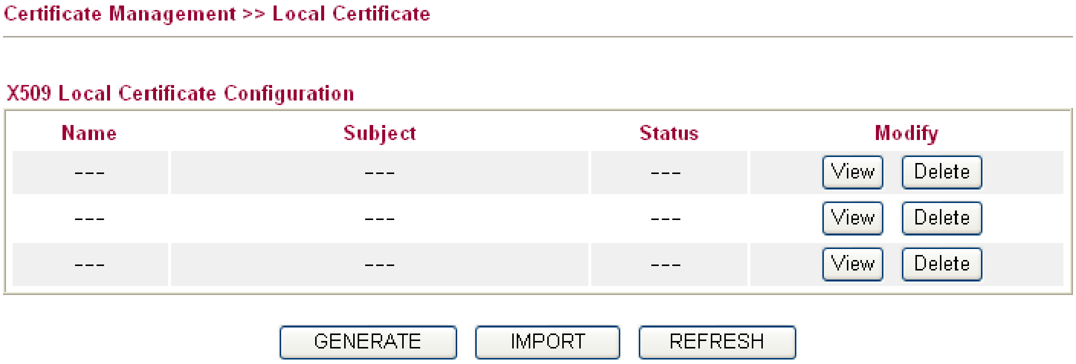
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

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.



4.11.1 Local Certificate



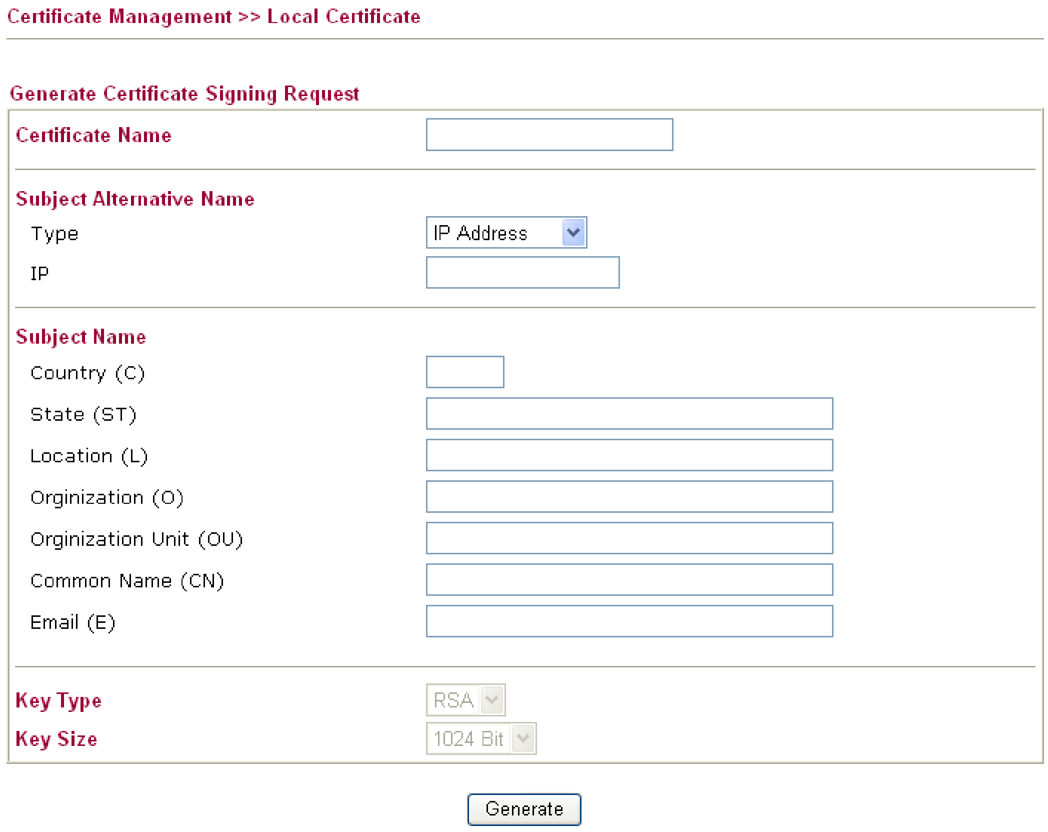
Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
---	---	---	View Delete
---	---	---	View Delete
---	---	---	View Delete

GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.



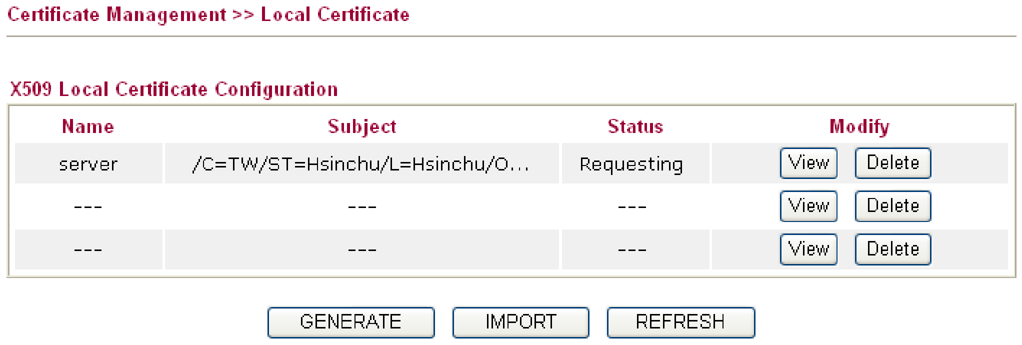
Certificate Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name	
Subject Alternative Name	
Type	IP Address
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
Key Type	RSA
Key Size	1024 Bit

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

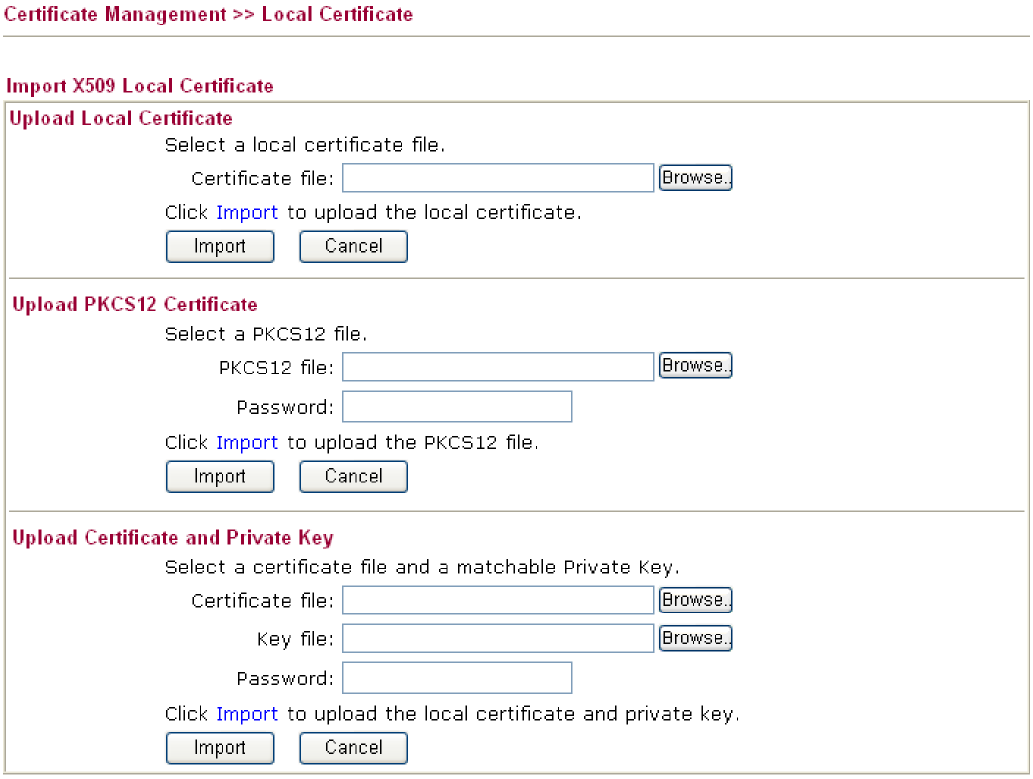
X509 Local Certificate Configuration

Name	Subject	Status	Modify
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	View Delete
---	---	---	View Delete
---	---	---	View Delete

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.



Certificate Management >> Local Certificate

Import X509 Local Certificate

Upload Local Certificate

Select a local certificate file.

Certificate file: Browse...

Click Import to upload the local certificate.

Upload PKCS12 Certificate

Select a PKCS12 file.

PKCS12 file: Browse...

Password:

Click Import to upload the PKCS12 file.

Upload Certificate and Private Key

Select a certificate file and a matchable Private Key.

Certificate file: Browse...

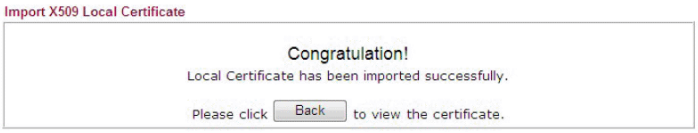
Key file: Browse...

Password:

Click Import to upload the local certificate and private key.

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**".

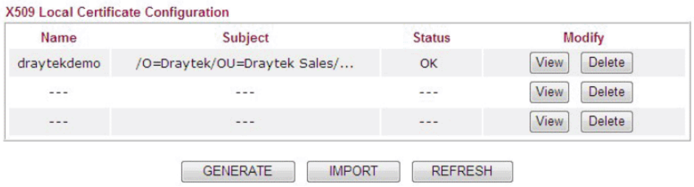


Import X509 Local Certificate

Congratulation!

Local Certificate has been imported successfully.

Please click Back to view the certificate.



X509 Local Certificate Configuration

Name	Subject	Status	Modify
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	View Delete
---	---	---	View Delete
---	---	---	View Delete

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.

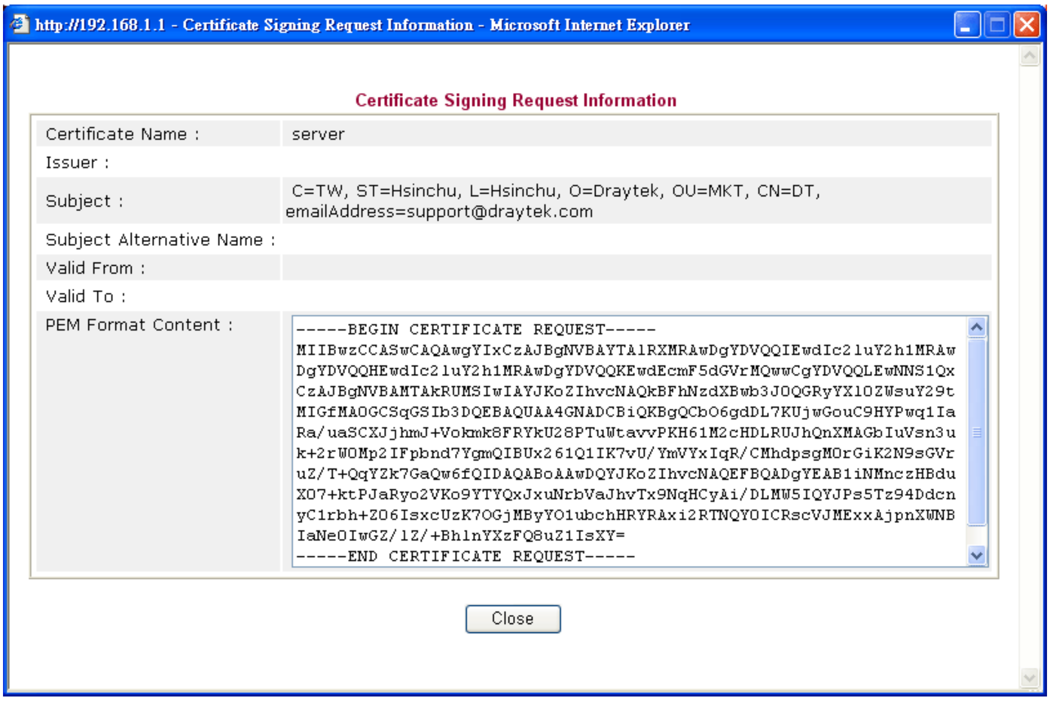
Upload Certificate and Private Key It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.


http://192.168.1.1 - Certificate Signing Request Information - Microsoft Internet Explorer

Certificate Signing Request Information

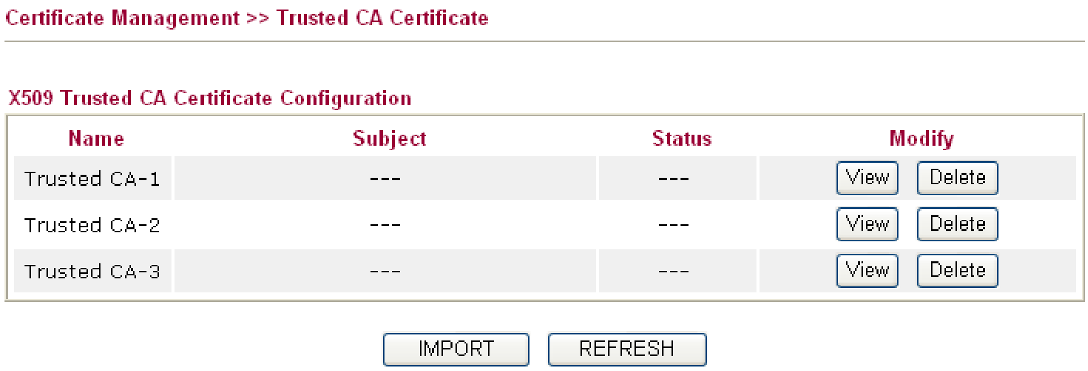
Certificate Name :	server
Issuer :	
Subject :	C=TW, ST=Hsinchu, L=Hsinchu, O=Draytek, OU=MKT, CN=DT, emailAddress=support@draytek.com
Subject Alternative Name :	
Valid From :	
Valid To :	
PEM Format Content :	see below

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBwzCCASwCAQAwgYIxCzAJBgNVBAYTAlRXMRAwDgYDVQQIEwdIc2luY2h1MRAw
DgYDVQQHEwdIc2luY2h1MRAwDgYDVQQKEwdEcmF5dGVrMQwwCgYDVQQLEwNNS1Qx
CzAJBgNVBAMTAkRUMSIwIAYJKoZIhvcNAQkBFhNzdXBwb3J0QGRyYXl0ZWsuY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbO6gdDL7KUjwGouC9HYPwq1Ia
Ra/uaSCXJjhmJ+Vokmk8FRYkU28PTuWtavvPKH61M2cHDLRUJhQnXMAGbIuVsn3u
k+2rW0Mp2IFpbnd7YgmQIBUx261Q1IK7vU/YmVYxIqR/CMhdpsgM0rGiK2N9sGVr
uZ/T+QqYZk7GaQw6fQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAB1iNMnczHBdu
X07+ktPJaRyo2VKo9YTYQxJxuNrbVaJhvTx9NqHCyAi/DLMW5IQYJPs5Tz94Ddcn
yC1rbh+Z06IsxcUzK7OGjMByYO1ubchHRYRAxi2RTNQYOICRscVJMExxAjpnXWNB
IaNe0IwGZ/lZ/+BhlnYXzFQ8uZ1IsXY=
-----END 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.

4.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

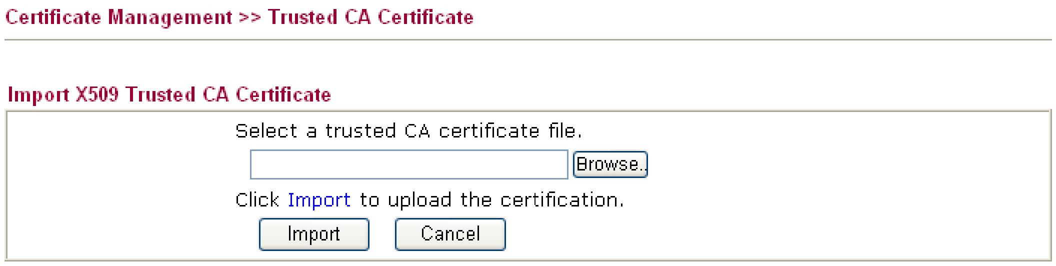


Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

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.



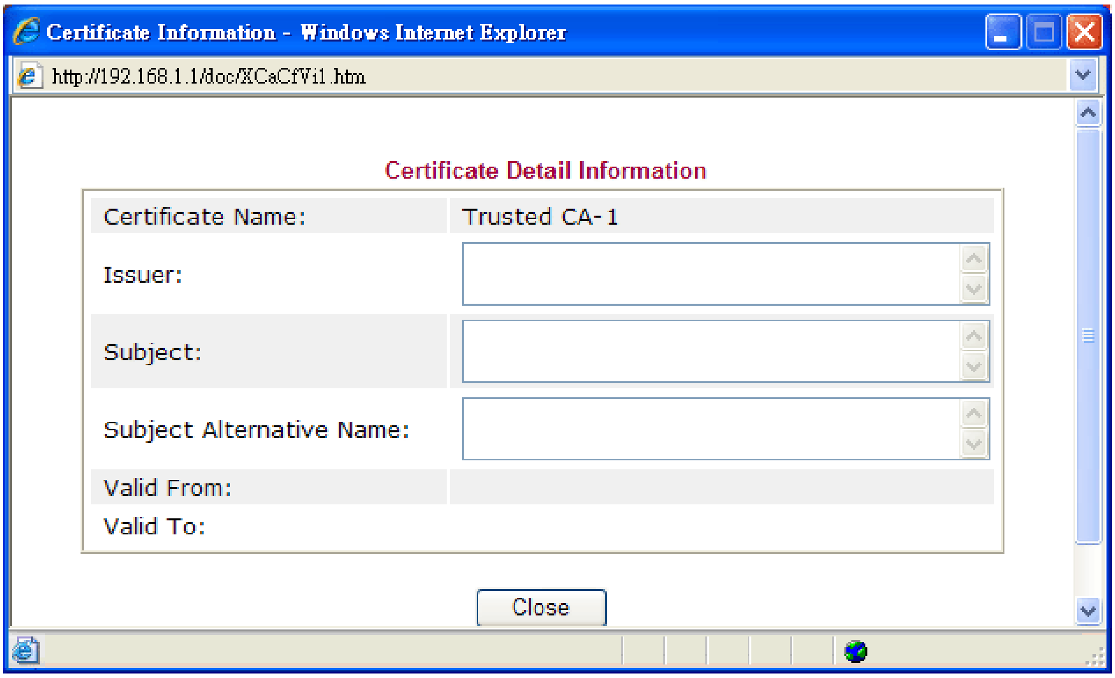
Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click Import to upload the certification.

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.



Certificate Information - Windows Internet Explorer

http://192.168.1.1/doc/XCaCfVi1.htm

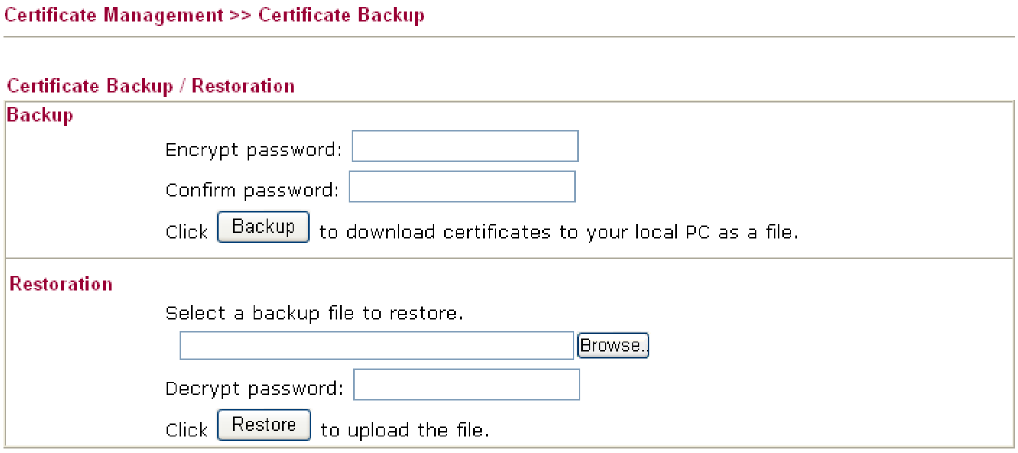
Certificate Detail Information

Certificate Name:	Trusted CA-1
Issuer:	
Subject:	
Subject Alternative Name:	
Valid From:	
Valid To:	

4.11.3 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.

Decrypt password:

Click Restore to upload the file.

4.12 Wireless LAN

This function is used for “n” models only.

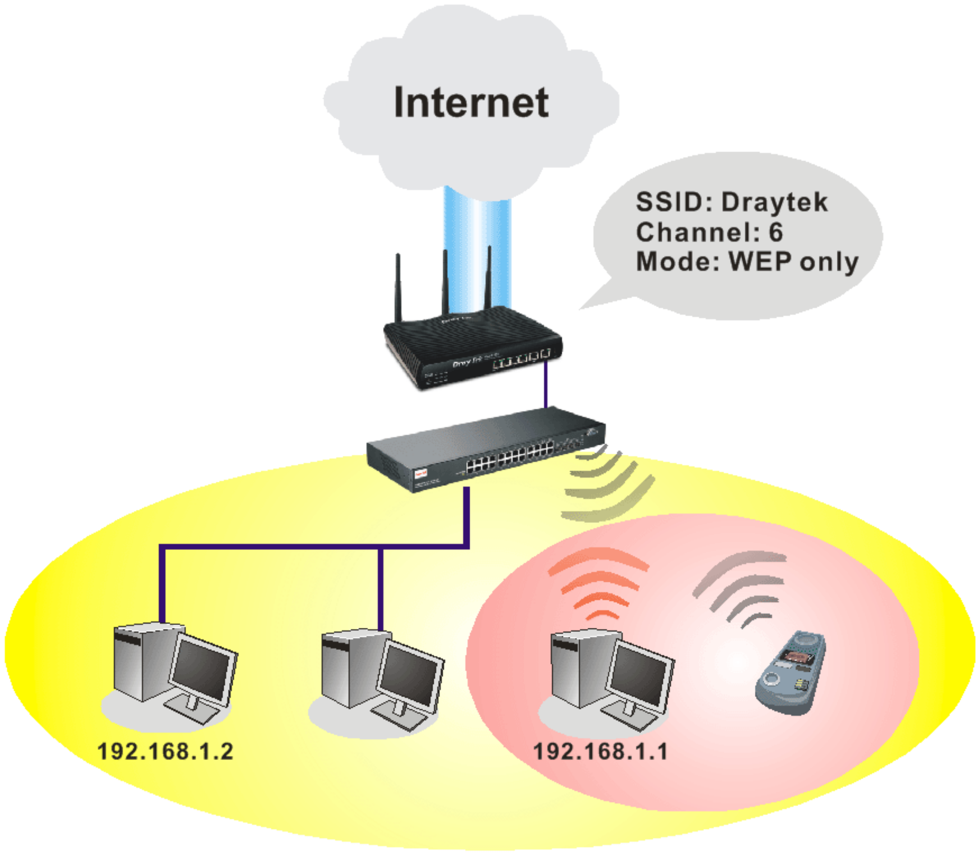
4.12.1 Basic Concepts

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/802.1x.

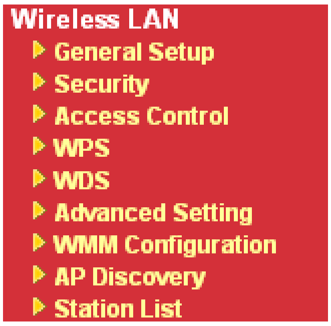
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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.

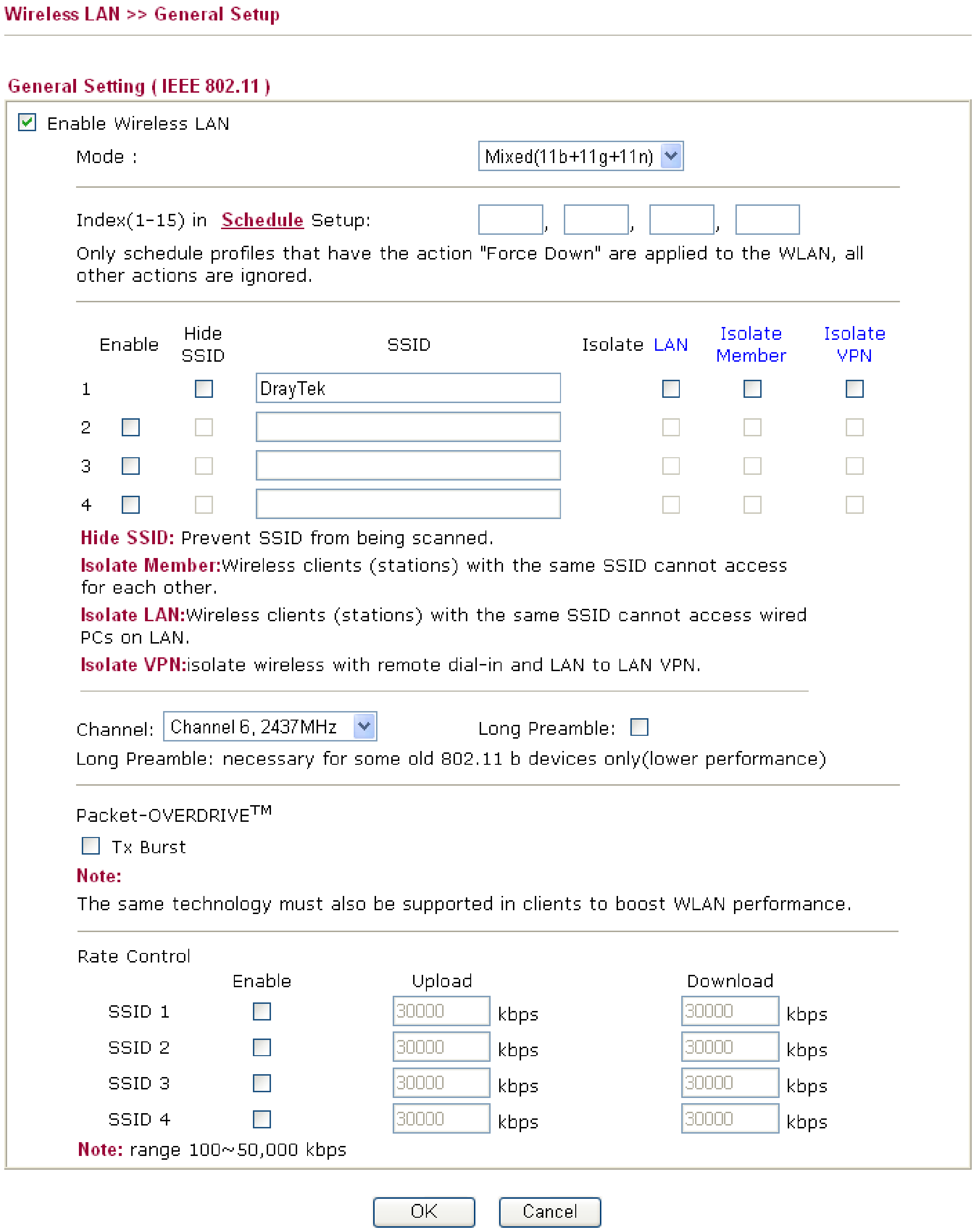
Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.



4.12.2 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.



Wireless LAN >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

Mode : Mixed(11b+11g+11n)

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

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	Isolate VPN
1		□	DrayTek	□	□	□
2	□	□		□	□	□
3	□	□		□	□	□
4	□	□		□	□	□

Hide SSID: Prevent SSID from being scanned.

Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.

Isolate VPN:isolate wireless with remote dial-in and LAN to LAN VPN.

Channel: Channel 6, 2437MHz   Long Preamble: □

Long Preamble: necessary for some old 802.11 b devices only(lower performance)

Packet-OVERDRIVE^TM

□ Tx Burst

Note:

The same technology must also be supported in clients to boost WLAN performance.

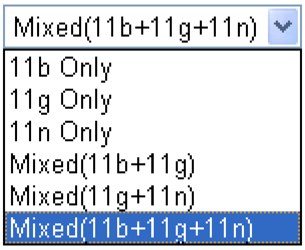
Rate Control

	Enable	Upload		Download	
SSID 1	□	30000	kbps	30000	kbps
SSID 2	□	30000	kbps	30000	kbps
SSID 3	□	30000	kbps	30000	kbps
SSID 4	□	30000	kbps	30000	kbps

Note: range 100~50,000 kbps

Enable Wireless LAN Check the box to enable wireless function.

Mode At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.



Mixed(11b+11g+11n)

11b Only
11g Only
11n Only
Mixed(11b+11g)
Mixed(11g+11n)
Mixed(11b+11g+11n)

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.

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.

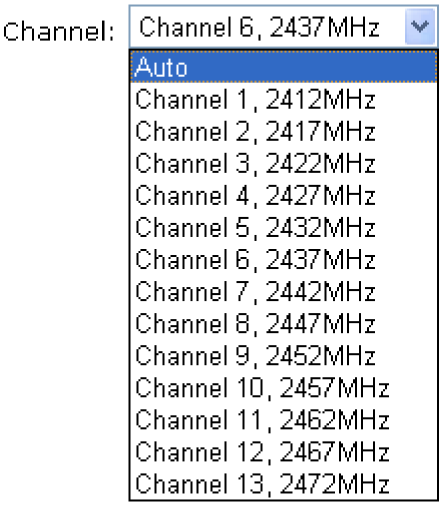
SSID Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek. We suggest you to change it.

Isolate **LAN** – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.

Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

VPN - Check this box to make the wireless clients (stations) with different VPN not accessing for each other.

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.



Channel: Channel 6, 2437MHz

Auto
Channel 1, 2412MHz
Channel 2, 2417MHz
Channel 3, 2422MHz
Channel 4, 2427MHz
Channel 5, 2432MHz
Channel 6, 2437MHz
Channel 7, 2442MHz
Channel 8, 2447MHz
Channel 9, 2452MHz
Channel 10, 2457MHz
Channel 11, 2462MHz
Channel 12, 2467MHz
Channel 13, 2472MHz

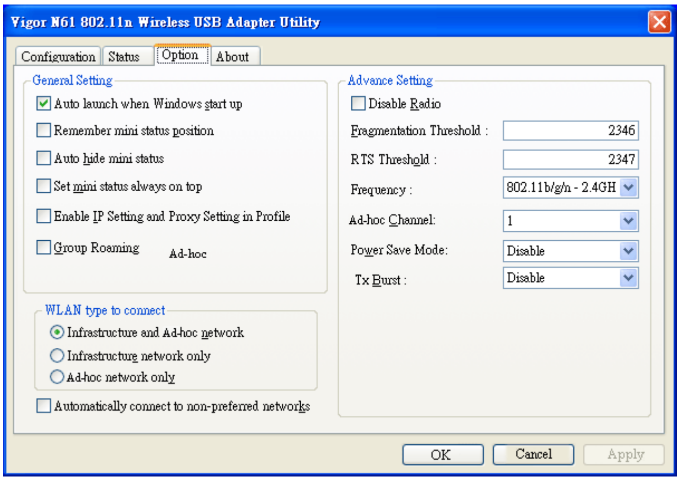
Long Preamble

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. Check it 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 Burs**t). 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**).



General Setting

- ☑ Auto launch when Windows start up
- □ Remember mini status position
- □ Auto hide mini status
- □ Set mini status always on top
- □ Enable IP Setting and Proxy Setting in Profile
- □ Group Roaming   Ad-hoc

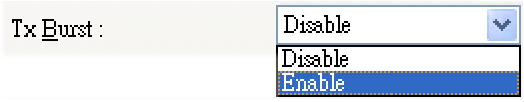
WLAN type to connect

- ● Infrastructure and Ad-hoc network
- ○ Infrastructure network only
- ○ Ad-hoc network only

□ Automatically connect to non-preferred networks

Advance Setting

- □ Disable Radio
- Fragmentation Threshold : 2346
- RTS Threshold : 2347
- Frequency : 802.11b/g/n - 2.4GH
- Ad-hoc Channel: 1
- Power Save Mode: Disable
- Tx Burst : Disable



Tx Burst : Disable

Note: * means the real transmission rate depends on the environment of the 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.

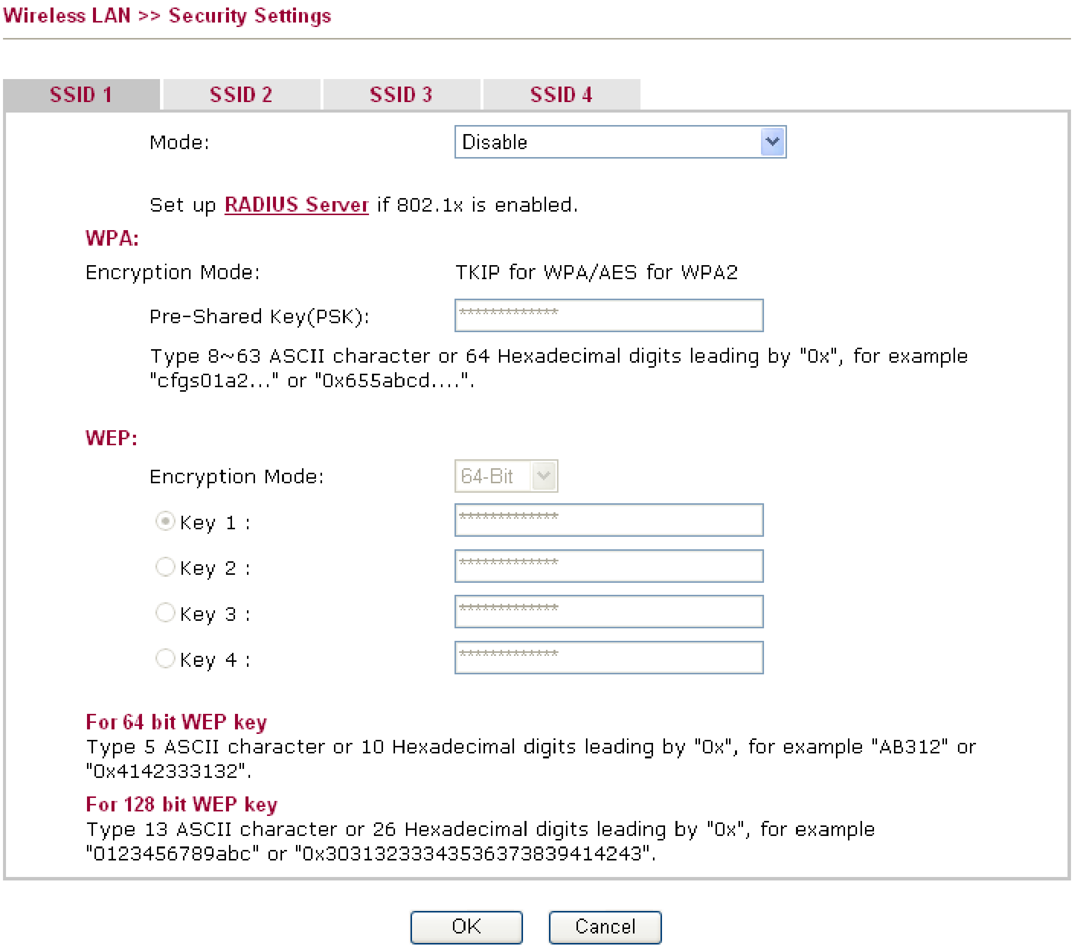
Download – Type the transmitting rate for data download. Default value is 30,000 kbps.

4.12.3 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.

Default Pre-Shared Key (PSK) 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 WEP and WPA.



Wireless LAN >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode: Disable

Set up RADIUS Server if 802.1x is enabled.

WPA:

Encryption Mode: TKIP for WPA/AES for WPA2

Pre-Shared Key(PSK): **************

Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

WEP:

Encryption Mode: 64-Bit

● Key 1 : **************

○ Key 2 : **************

○ Key 3 : **************

○ Key 4 : **************

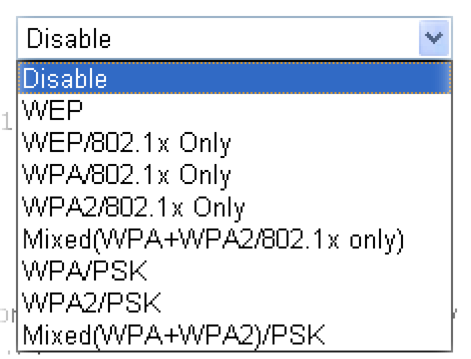
For 64 bit WEP key

Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".

For 128 bit WEP key

Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".

Mode There are several modes provided for you to choose.



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

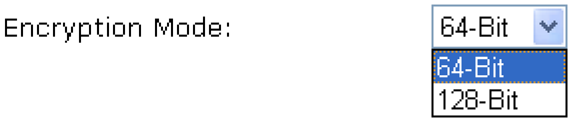
The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

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).

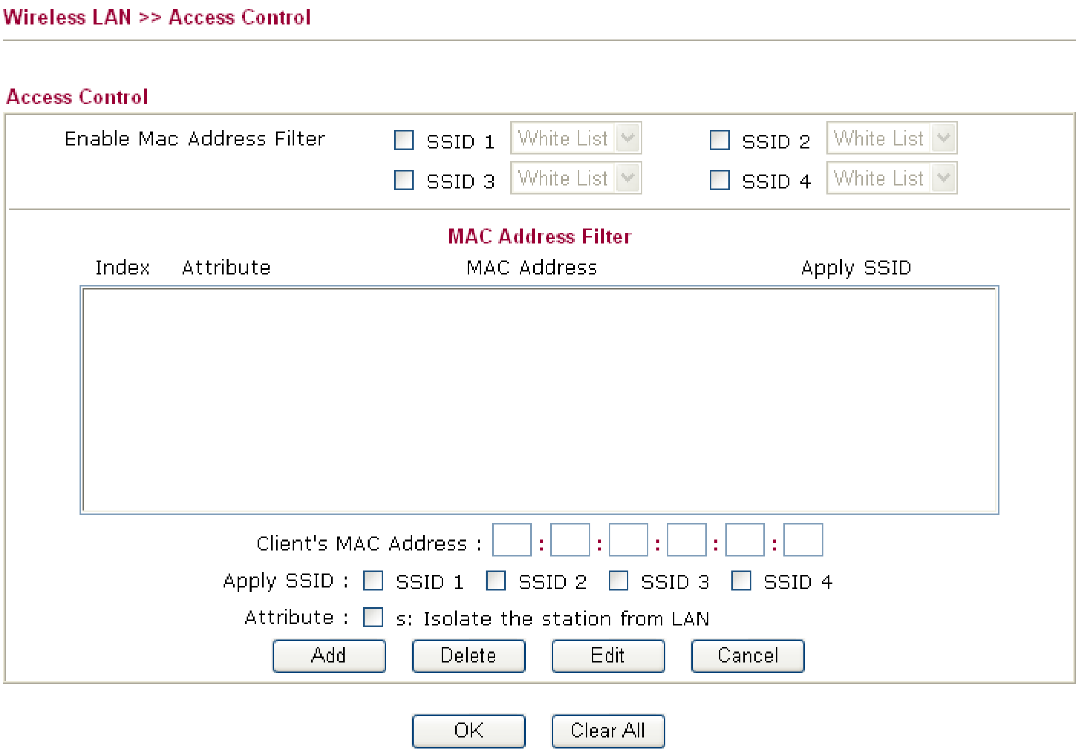

Encryption Mode: 64-Bit

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.

4.12.4 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.



Wireless LAN >> Access Control

Access Control

Enable Mac Address Filter □ SSID 1 White List □ SSID 2 White List
□ SSID 3 White List □ SSID 4 White List

MAC Address Filter

Index Attribute MAC Address Apply SSID

Client's MAC Address : __ : __ : __ : __ : __ : __

Apply SSID : □ SSID 1 □ SSID 2 □ SSID 3 □ SSID 4

Attribute : □ s: Isolate the station from LAN

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.

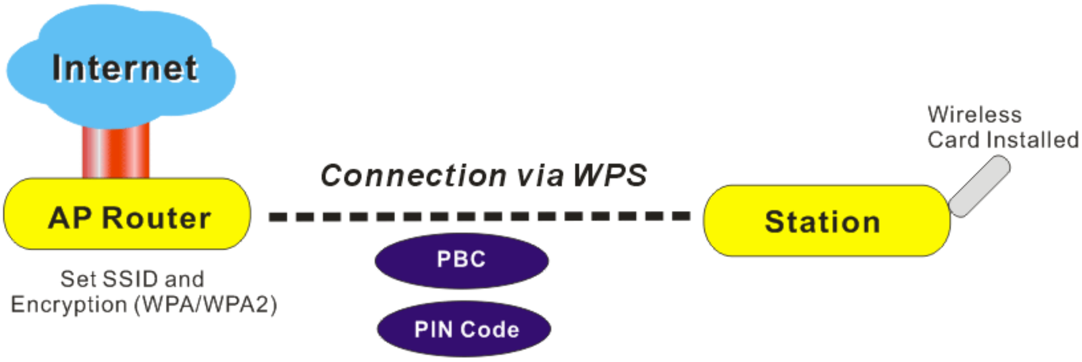
Edit Edit the selected MAC address in the list.

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.

4.12.5 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.

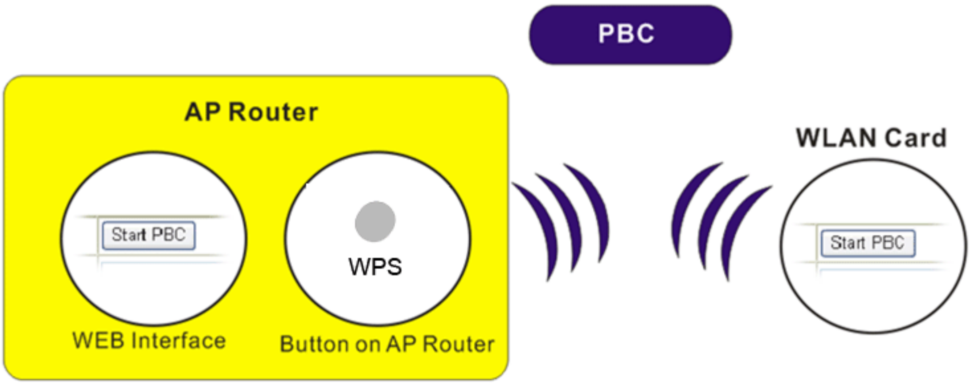


Note: Such function is available for the wireless station with WPS supported.

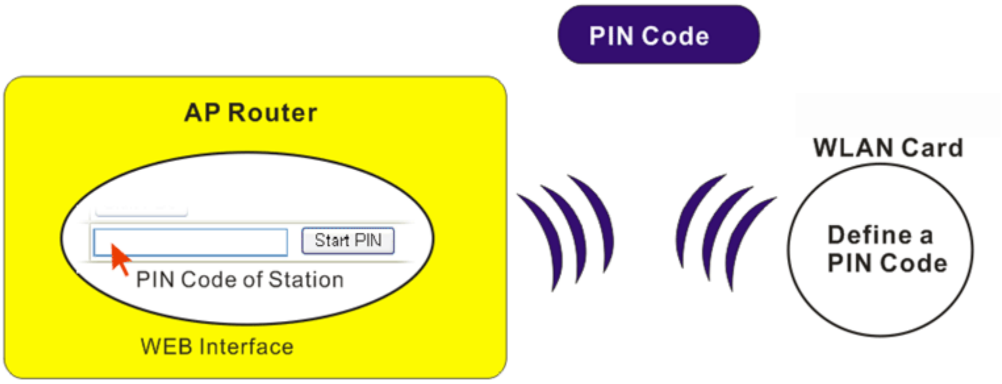
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for 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***.

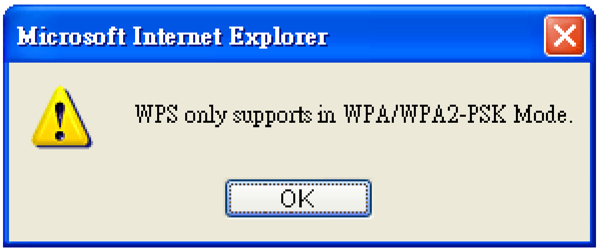
- On the side of Vigor 3200 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



- 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.



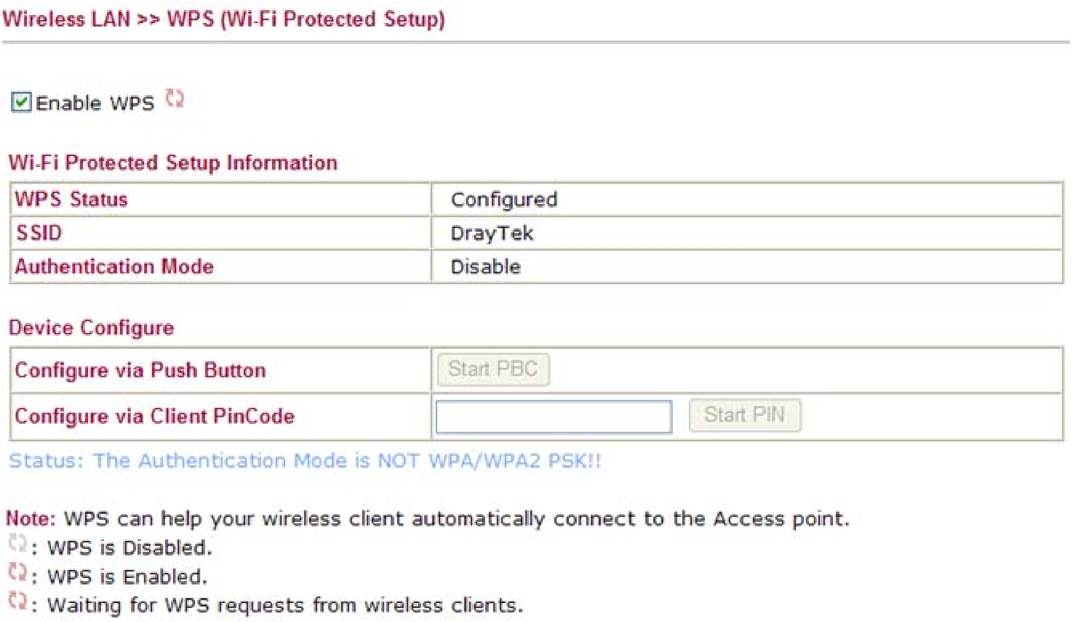
For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



WPS only supports in WPA/WPA2-PSK Mode.

Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Below shows **Wireless LAN>>WPS** web page.



Wireless LAN >> WPS (Wi-Fi Protected Setup)

☑ Enable WPS

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Disable

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

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.

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)

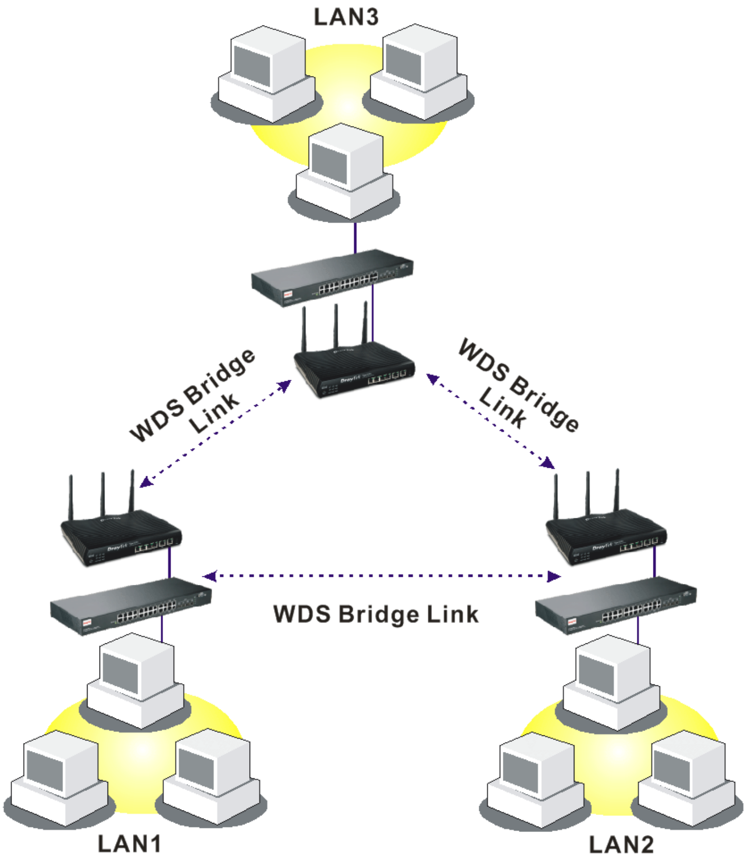
Configure via Client PinCode Please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

4.12.6 WDS

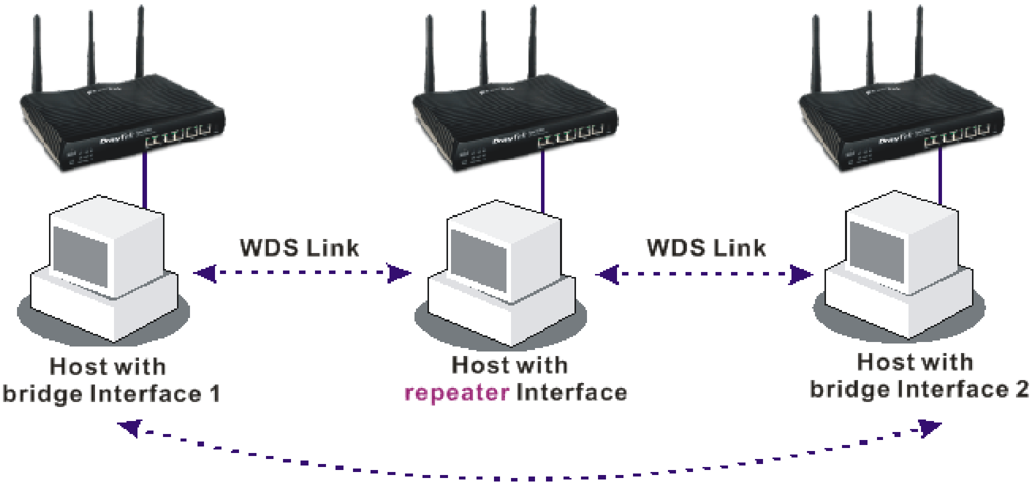
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:

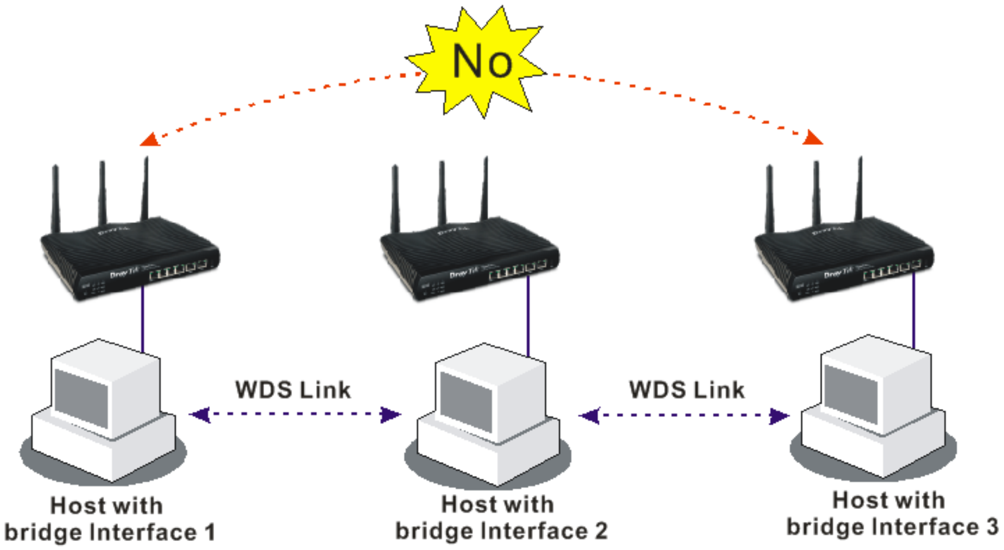


The application for the WDS-Repeater mode is depicted as below:

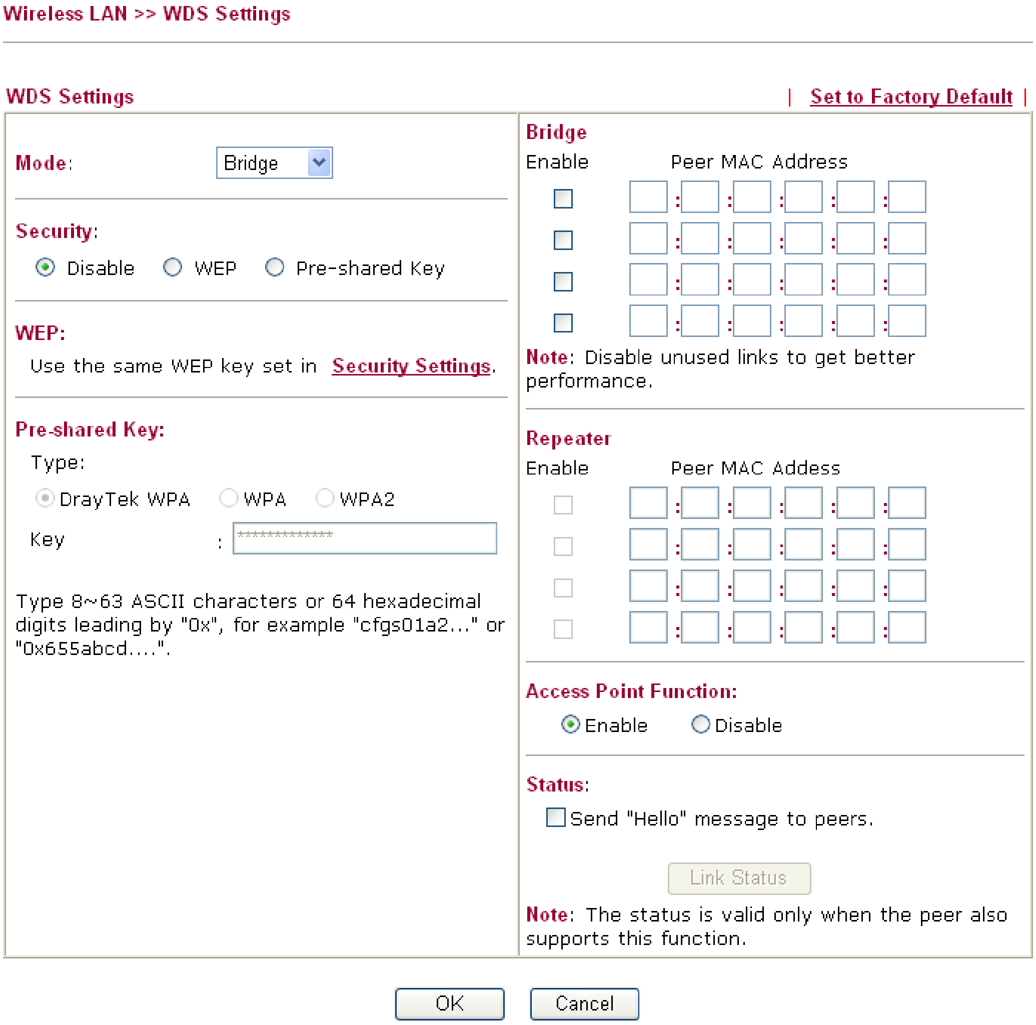


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, 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.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.



Wireless LAN >> WDS Settings

WDS Settings | Set to Factory Default |

Mode: Bridge

Security:
● Disable ○ WEP ○ Pre-shared Key

WEP:
Use the same WEP key set in Security Settings.

Pre-shared Key:
Type:
● DrayTek WPA ○ WPA ○ WPA2
Key : **************

Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

Bridge
Enable Peer MAC Address
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
Note: Disable unused links to get better performance.

Repeater
Enable Peer MAC Addess
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□ [ ]:[ ]:[ ]:[ ]:[ ]:[ ]

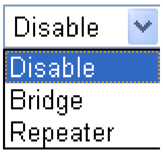
Access Point Function:
● Enable ○ Disable

Status:
□ Send "Hello" message to peers.
Link Status
Note: The status is valid only when the peer also supports this function.

OK Cancel

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 three types for you to choose. **DrayTek WPA** can be used for all DrayTek wireless routers like Vigor2700, Vigor2800, Vigor2820, and etc., except for other brand's wireless routers. **WPA** and **WPA2** are used for WDS devices (e.g., AP700). For example, if you have a wireless AP and a Vigor2820n 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

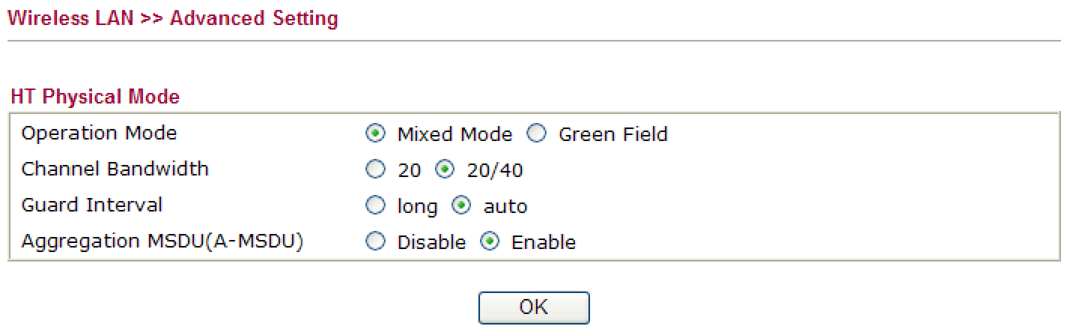
Click **Enable** to make this router serving as an access point; click **Disable** to cancel this function.

Status

It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.

4.12.7 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.



Wireless LAN >> Advanced Setting

HT Physical Mode

Operation Mode	● Mixed Mode ○ Green Field
Channel Bandwidth	○ 20 ● 20/40
Guard Interval	○ long ● auto
Aggregation MSDU(A-MSDU)	○ Disable ● Enable

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 happening 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 transit.

Guard Interval

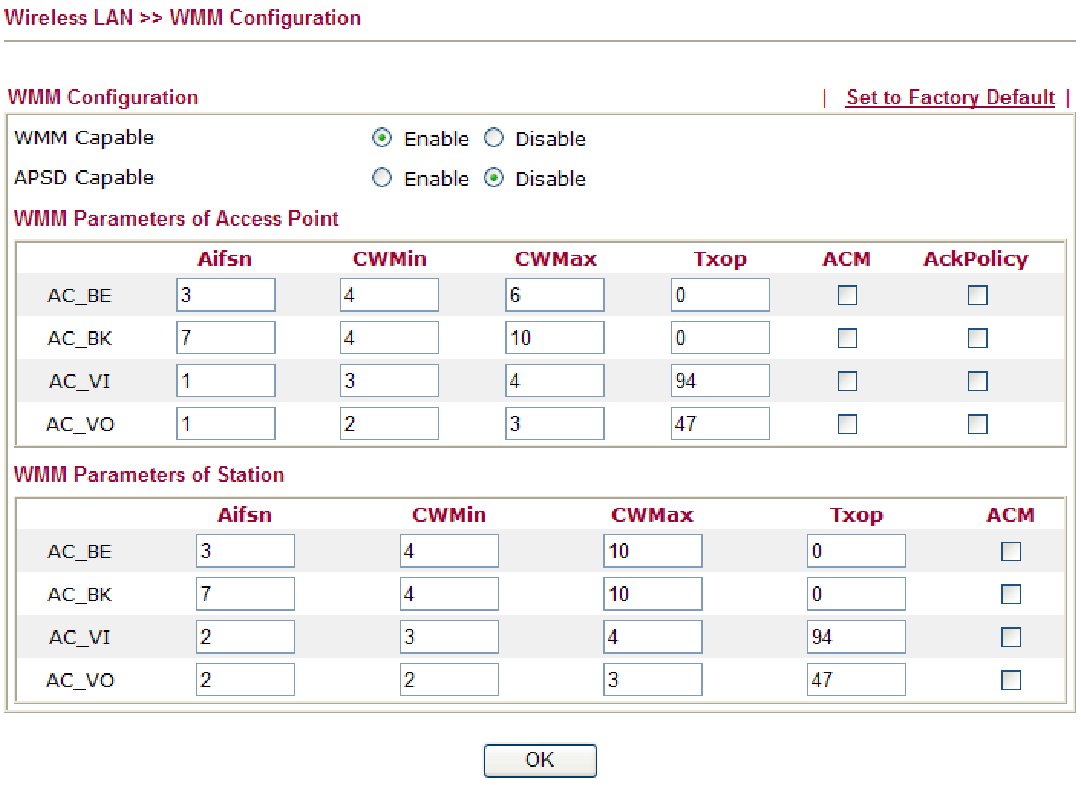
It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose **auto** as guard interval,

	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.**

4.12.8 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.



Wireless LAN >> WMM Configuration

WMM Configuration | Set to Factory Default |

WMM Capable ● Enable ○ Disable

APSD Capable ○ Enable ● Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	4	6	0	□	□
AC_BK	7	4	10	0	□	□
AC_VI	1	3	4	94	□	□
AC_VO	1	2	3	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	4	10	0	□
AC_BK	7	4	10	0	□
AC_VI	2	3	4	94	□
AC_VO	2	2	3	47	□

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: Vigor2830 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.

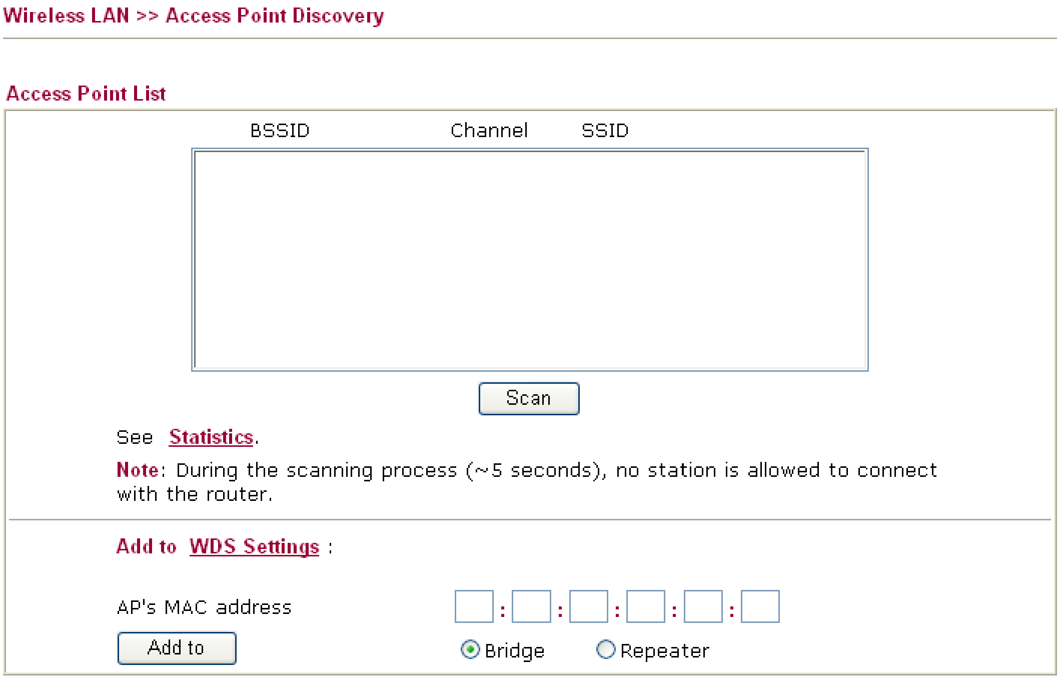
AckPolicy **“**Uncheck” (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.

“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.

4.12.9 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 all the connected APs.


Wireless LAN >> Access Point Discovery

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.

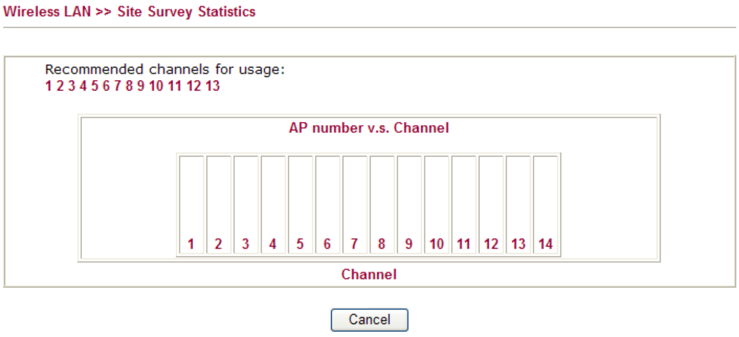
Add to WDS Settings :

AP's MAC address □ : □ : □ : □ : □ : □

Add to ● Bridge ○ Repeater

Scan It is used to discover all the connected AP. 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

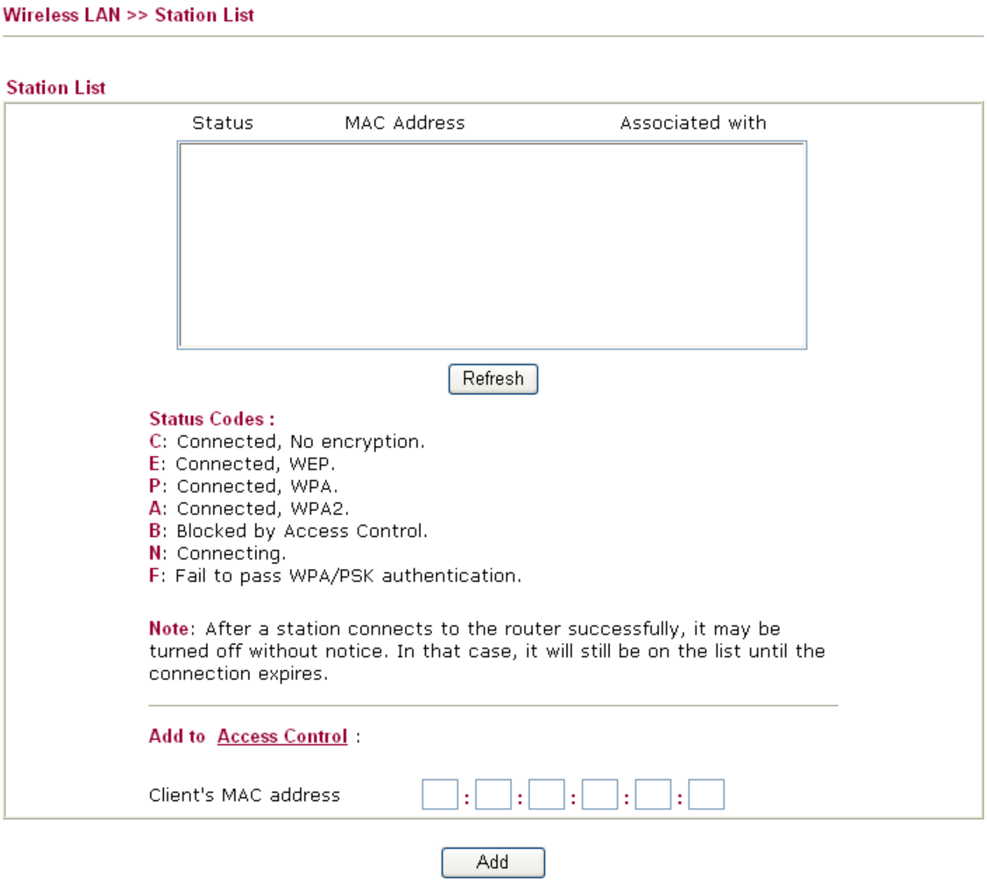
Recommended channels for usage:
1 2 3 4 5 6 7 8 9 10 11 12 13

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.

4.12.10 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.



Wireless LAN >> Station List

Station List

Status MAC Address Associated with

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 □ : □ : □ : □ : □ : □

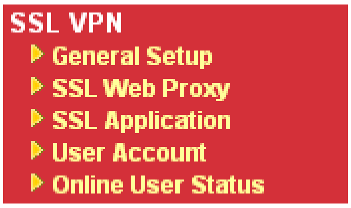
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into **Access Control.**

4.13 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

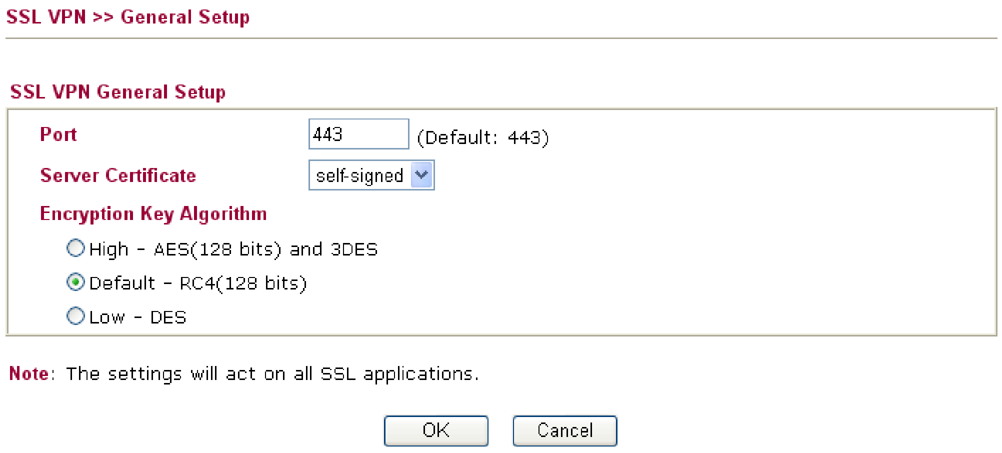
There are two benefits that SSL VPN provides:

- 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.



4.13.1 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

Encryption Key Algorithm

○ High - AES(128 bits) and 3DES

● Default - RC4(128 bits)

○ Low - DES

Note: The settings will act on all SSL applications.

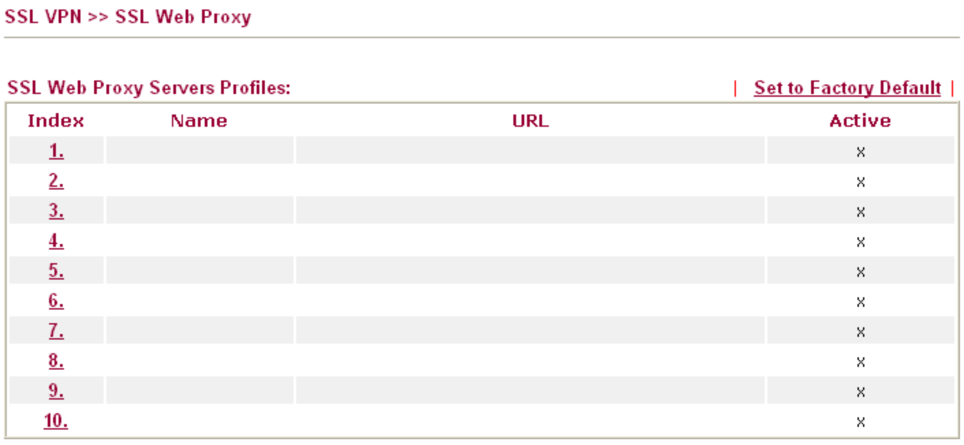
Port Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in **System Maintenance>>Management**. In general, the default setting is 443.

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.

Encryption Key Algorithm Choose the encryption level for the data connection in SSL VPN server.

4.13.2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.



SSL VPN >> SSL Web Proxy

SSL Web Proxy Servers Profiles: | Set to Factory Default |

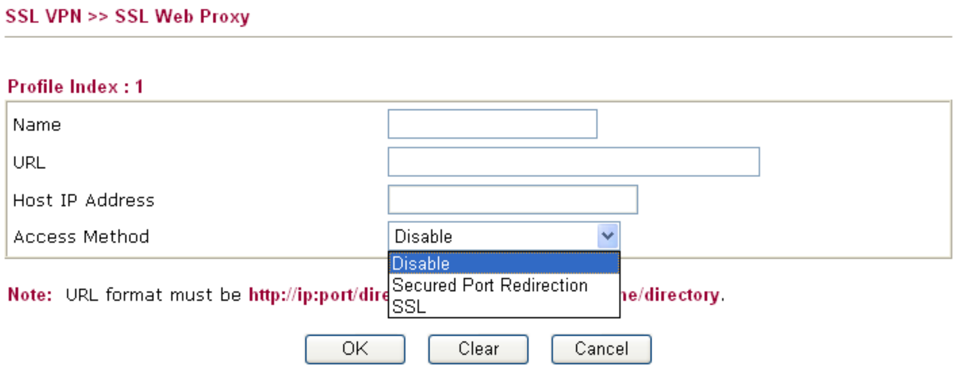
Index	Name	URL	Active
1.			x
2.			x
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x

Name Display the name of the profile that you create.

URL Display the URL.

Active Display current status (active or inactive) of such profile.

Click number link under Index filed to set detailed configuration.



SSL VPN >> SSL Web Proxy

Profile Index : 1

Name	
URL	
Host IP Address	
Access Method	Disable

Note: URL format must be **http://ip:port/dire** **ne/directory**.

Name Type name of the profile.

URL Type the address (function variation or IP address) or path of the proxy server.

Host IP Address If you type function variation as URL, you have to type corresponding IP address in this filed. Such field must match with URL setting.

Access Method There are three modes for you to choose

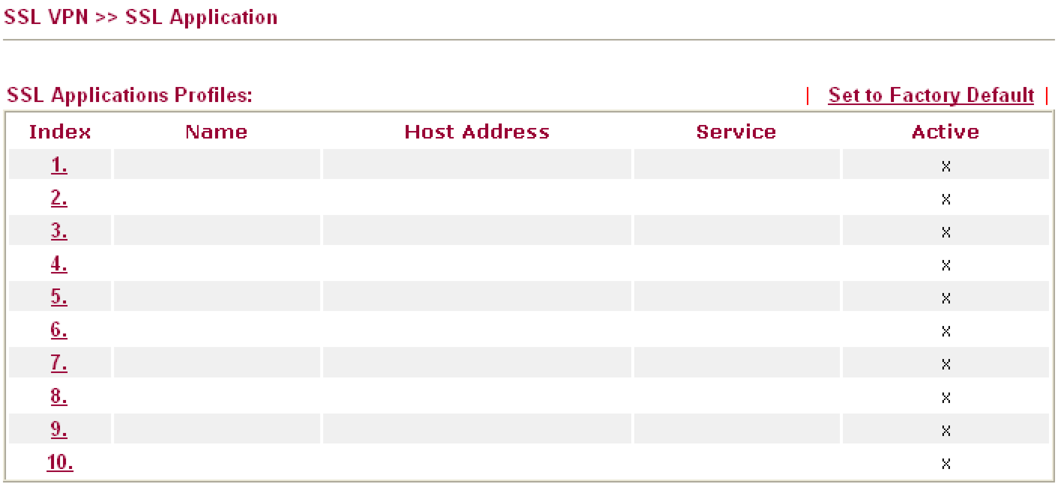
Disable – the profile will be inactive. If you choose **Disable**, all the web proxy profile appeared under VPN remote dial-in web page will disappear.

Secured Port Redirection – such technique applies private port mapping to random WAN port. There are two restrictions for proxy web server for such selection: 1) it is only used for WAN to LAN access, the web server must be configured behind vigor router; 2) web server gateway must be indicated to vigor router. In addition, users must execute "Connect" manually in SSL Client Portal page.

SSL – if you choose such selection, web proxy over SSL will be applied for VPN.

4.13.3 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol) /SAMBA, 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

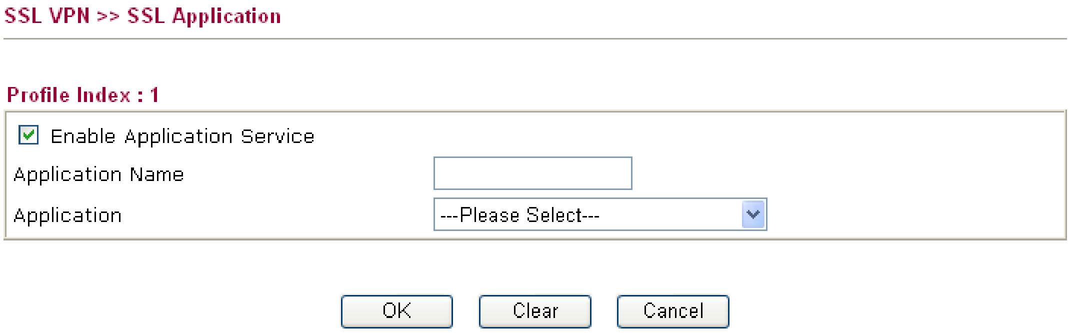
Name Display the application name of the profile that you create.

Host Address Display the IP address for VNC/RDP or SAMBA path.

Service Display the type of the service selected, e.g., VNC/RDP/SAMBA.

Active Display current status (active or inactive) of the selected profile.

Click number link under Index filed to make detailed configuration.



SSL VPN >> SSL Application

Profile Index : 1

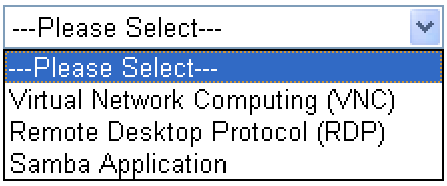
☑ Enable Application Service

Application Name	
Application	---Please Select---

Enable Application Service Check this box to enable this application.

Application Name Type the profile name for the application.

Application Use the drop down list to choose an application applied to this profile.

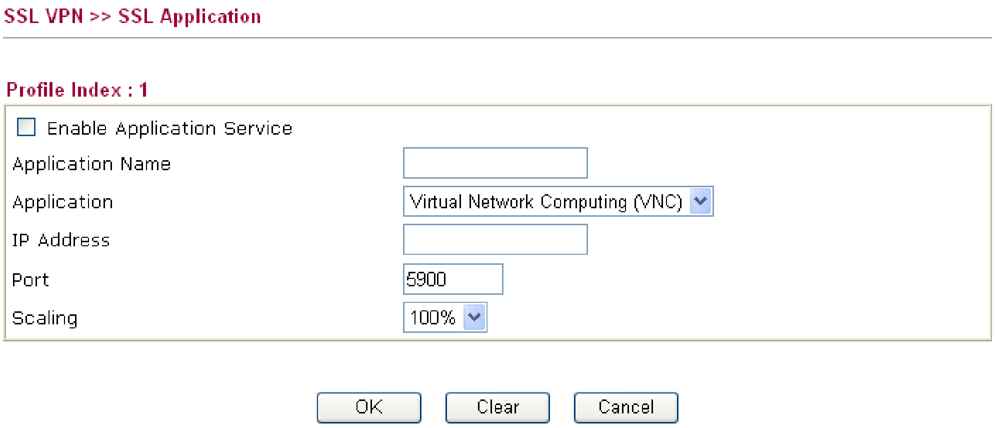


---Please Select---

---Please Select---
Virtual Network Computing (VNC)
Remote Desktop Protocol (RDP)
Samba Application

Different application type will lead different web pages. Refer to the following:

- **Virtual Network Computing** – Choose this item for accessing and controlling a remote PC through VNC protocol.



SSL VPN >> SSL Application

Profile Index : 1

☐ Enable Application Service

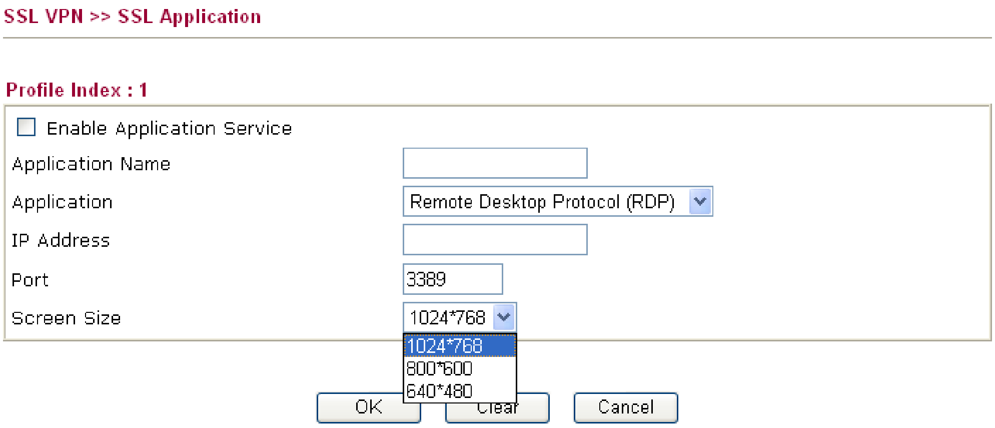
Application Name	
Application	Virtual Network Computing (VNC)
IP Address	
Port	5900
Scaling	100%

IP Address Type the IP address for this protocol.

Port Specify the port used for this protocol. The default setting is 5900.

Scaling Chose the percentage (100%, 80%, 60) for such application.

- **Remote Desktop Protocol** - Choose this item for accessing and controlling a remote PC through RDP protocol.



SSL VPN >> SSL Application

Profile Index : 1

☐ Enable Application Service

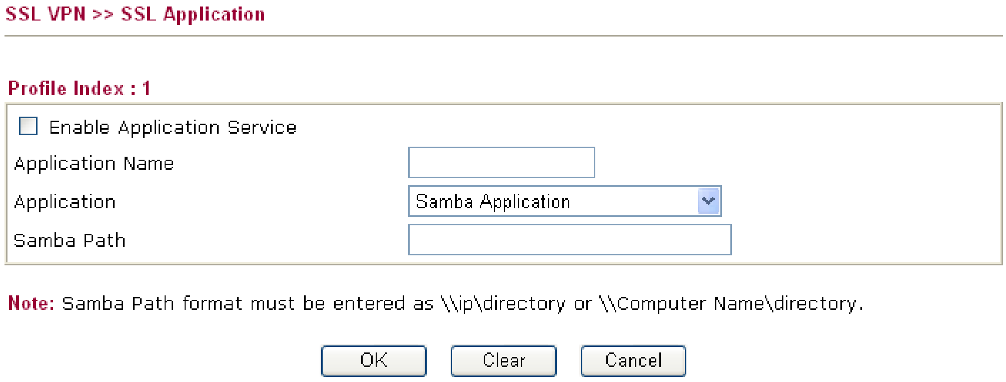
Application Name	
Application	Remote Desktop Protocol (RDP)
IP Address	
Port	3389
Screen Size	1024*768

IP Address Type the IP address for this protocol.

Port Specify the port used for this protocol.

Screen Size Chose the screen size for such application.

- **Samba Application -** Any remote user can upload/download/delete certain files on a local samba server through web browser with this application



SSL VPN >> SSL Application

Profile Index : 1

☐ Enable Application Service

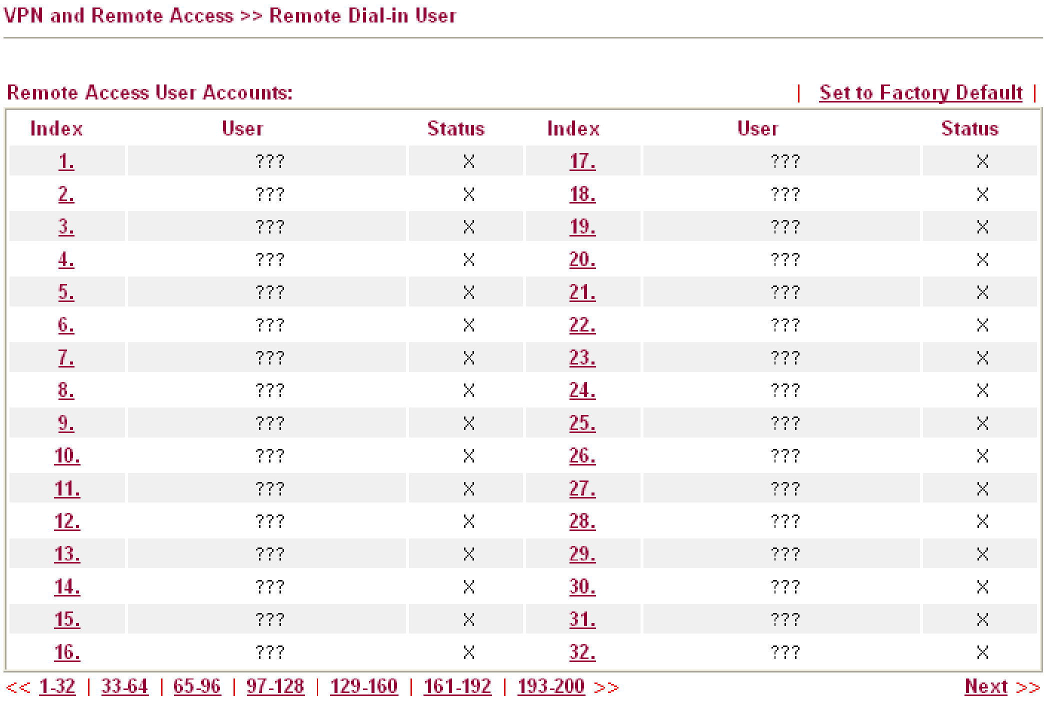
Application Name	
Application	Samba Application
Samba Path	

Note: Samba Path format must be entered as \\ip\directory or \\Computer Name\directory.

Samba Path Specify the path for this application.

4.13.4 User Account

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**.



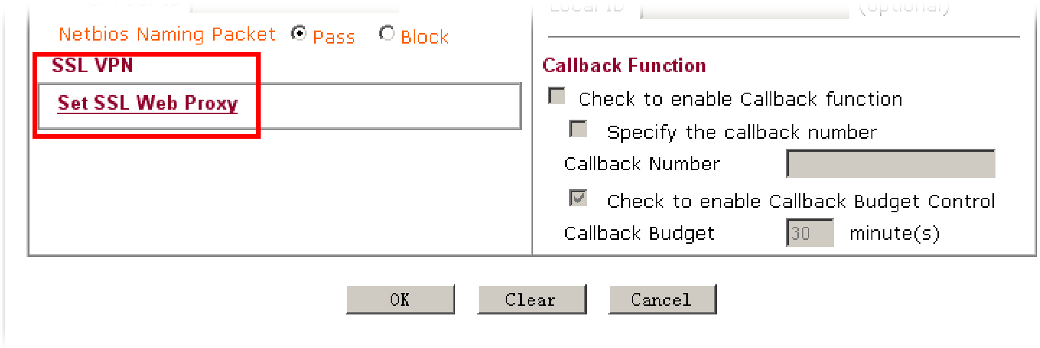
VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: | Set to Factory Default |

Index	User	Status	Index	User	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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> Next >>

You can find out the link of Set SSL Web Proxy on the profile setting page. If you haven't set any SSL Web Proxy Profile in **SSL VPN>> SSL Web Proxy** web page, there is no check box but a link appeared below.



Netbios Naming Packet ● Pass ○ Block

SSL VPN

Set SSL Web Proxy

Callback Function

□ Check to enable Callback function

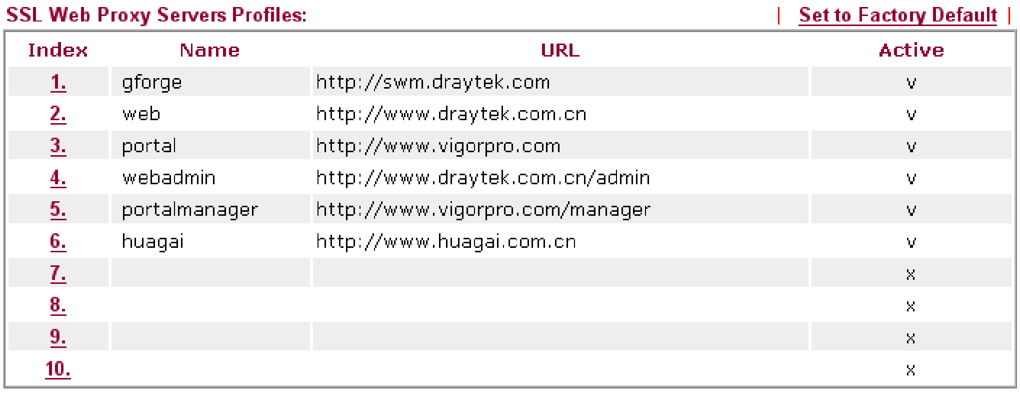
□ Specify the callback number

Callback Number

☑ Check to enable Callback Budget Control

Callback Budget 30 minute(s)

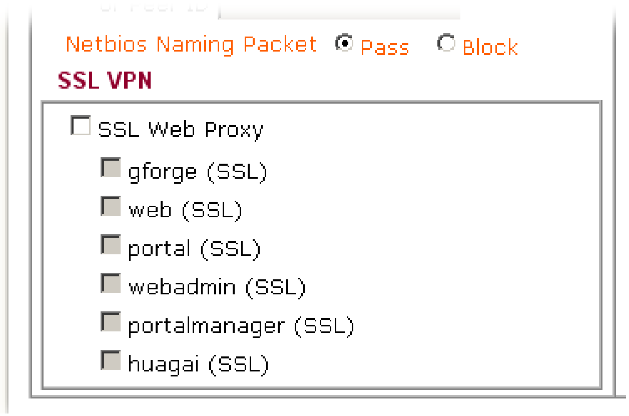
However, if you have set several SSL Web Proxy Profiles in **SSL VPN>> SSL Web Proxy** web page:



SSL Web Proxy Servers Profiles: | Set to Factory Default |

Index	Name	URL	Active
1.	gforge	http://swm.draytek.com	v
2.	web	http://www.draytek.com.cn	v
3.	portal	http://www.vigorpro.com	v
4.	webadmin	http://www.draytek.com.cn/admin	v
5.	portalmanager	http://www.vigorpro.com/manager	v
6.	huagai	http://www.huagai.com.cn	v
7.			x
8.			x
9.			x
10.			x

The SSL Web Proxy profile names will be displayed (together with check box) as shown below.



Netbios Naming Packet ● Pass ○ Block

SSL VPN

□ SSL Web Proxy

□ gforge (SSL)

□ web (SSL)

□ portal (SSL)

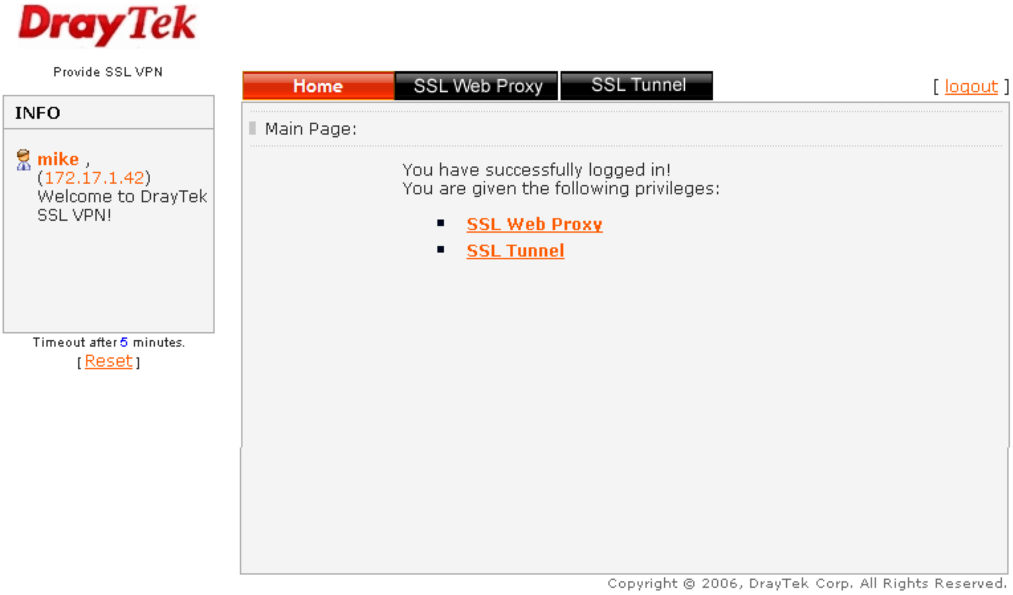
□ webadmin (SSL)

□ portalmanager (SSL)

□ huagai (SSL)

4.13.5 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.



mike , (172.17.1.42) Welcome to DrayTek SSL VPN!

Timeout after 5 minutes. [Reset]

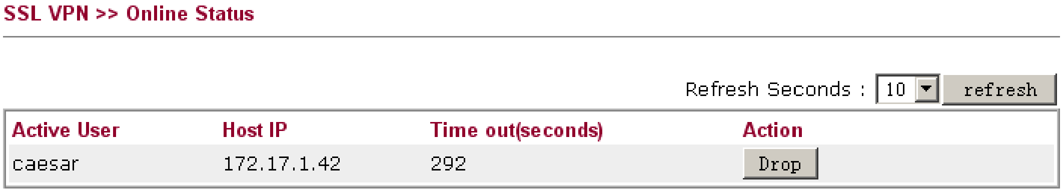
Main Page:

You have successfully logged in!
You are given the following privileges:

- SSL Web Proxy
- SSL Tunnel

Copyright © 2006, DrayTek Corp. All Rights Reserved.

Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.



SSL VPN >> Online Status

Refresh Seconds : 10 ▾ refresh

Active User	Host IP	Time out(seconds)	Action
caesar	172.17.1.42	292	Drop

Active User Display current user who visit SSL VPN server.

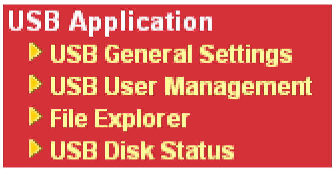
Host IP Display the IP address for the host.

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.

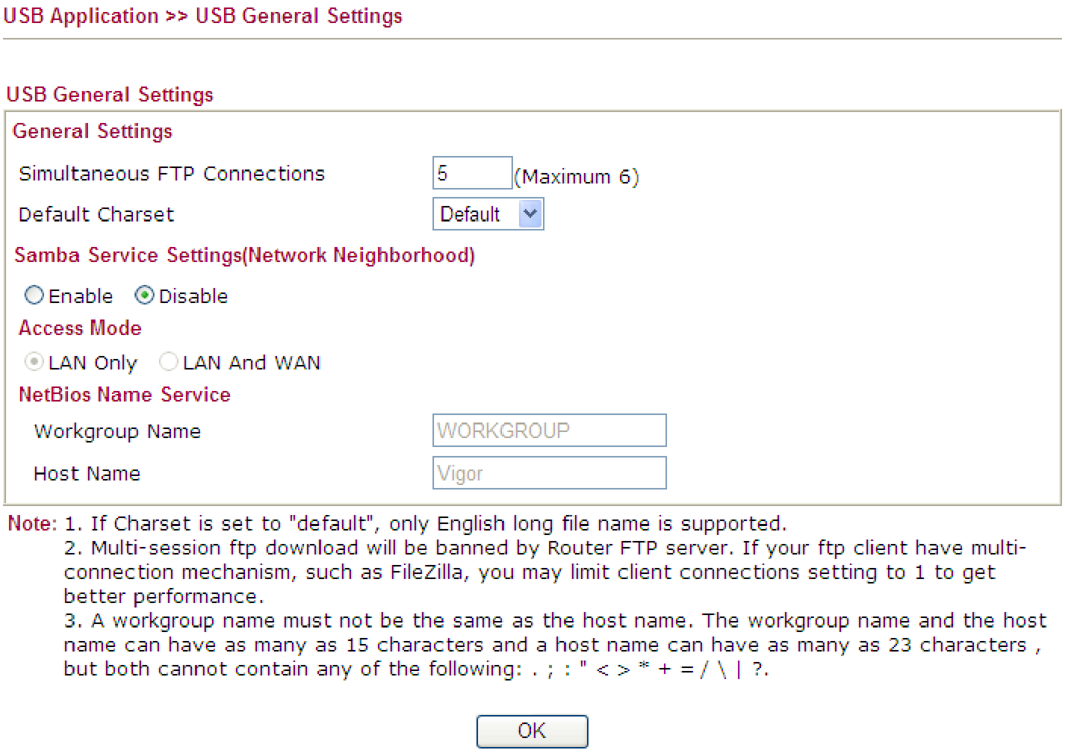
4.14 USB Application

USB diskette connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN/WAN can access, write and read data stored in USB diskette 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 diskette) or share the Samba service through Vigor router.



4.14.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB diskette with formats of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure the memory format for the USB diskette 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	Default

Samba Service Settings(Network Neighborhood)

○ Enable ● Disable

Access Mode

● LAN Only ○ LAN And WAN

NetBios Name Service

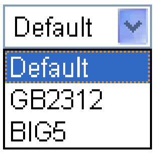
Workgroup Name	WORKGROUP
Host Name	Vigor

Note: 1. If Charset is set to "default", 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.
3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . ; : " < > * + = / \ | ?.

General Settings

Simultaneous FTP Connection - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage diskette at one time.

Default Charset - At present, Vigor router supports three types of character sets: default, GB2312 and BIG5.



Default Charset is for English based file name. For Simplified Chinese file/directory names, please choose GB2312; for Traditional Chinese file/directory names, choose BIG5.

Samba Service Settings Click **Enable** to invoke samba service via the router.

Access Mode

LAN Only – Users coming from internet cannot connect to the samba server of the router.

LAN And WAN - Both LAN and WAN users can access samba server of the router.

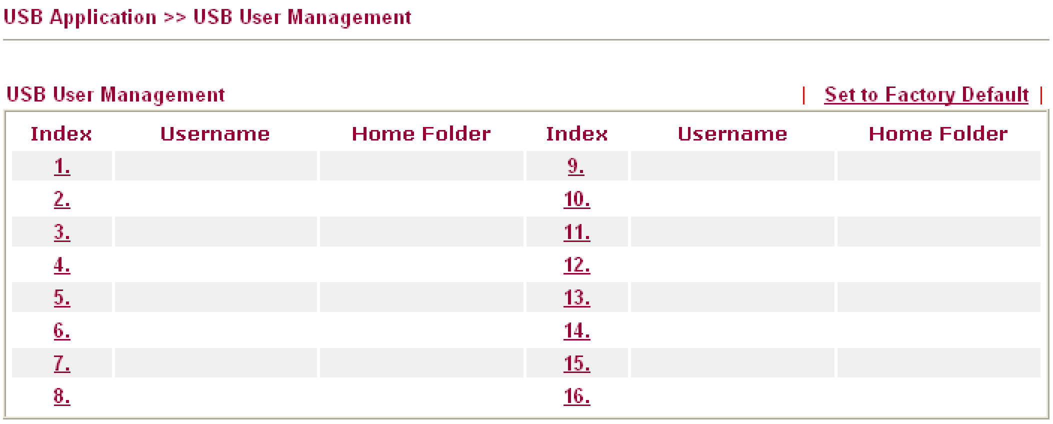
NetBios Name Service For the NetBios service of USB diskette, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following--- ; : " < > * + = \ | ?.

Workgroup Name – Type a name for the workgroup.

Host Name – Type the host name for the router.

4.14.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB diskette must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB diskette first. Otherwise, an error message will appear to warn you.

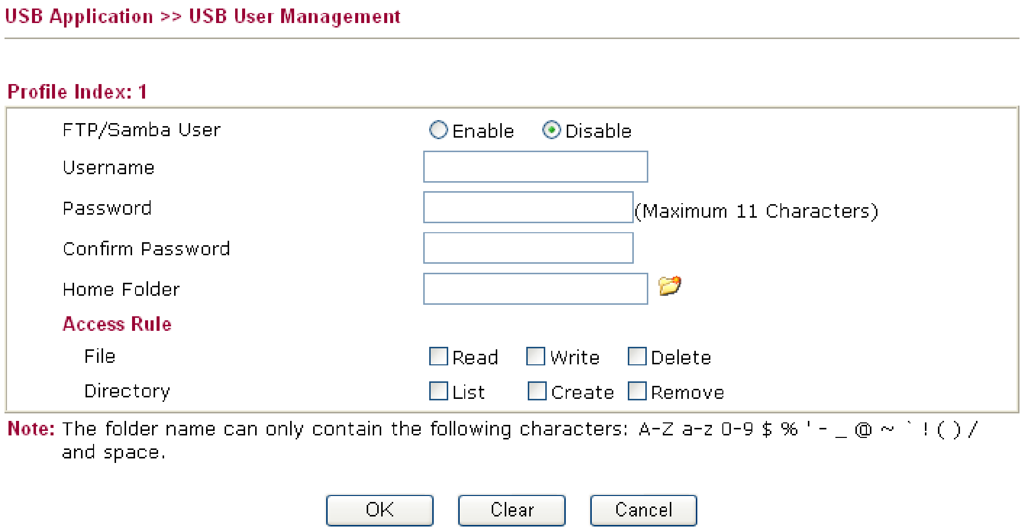


USB Application >> USB User Management

USB User Management | Set to Factory Default |

Index	Username	Home Folder	Index	Username	Home Folder
1.			9.		
2.			10.		
3.			11.		
4.			12.		
5.			13.		
6.			14.		
7.			15.		
8.			16.		

Click index number to access into configuration page.



USB Application >> USB User Management

Profile Index: 1

FTP/Samba User	○ Enable ● Disable
Username	
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	
Access Rule	
File	□ Read □ Write □ Delete
Directory	□ List □ Create □ Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 $ % ' - _ @ ~ ` ! ( ) / and space.

FTP/Samba User **Enable** – Click this button to activate this profile (account) for FTP service or Samba User 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/Samba users for accessing into FTP server (USB diskette). Be aware that users cannot access into USB diskette in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage diskette.

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/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage diskette.

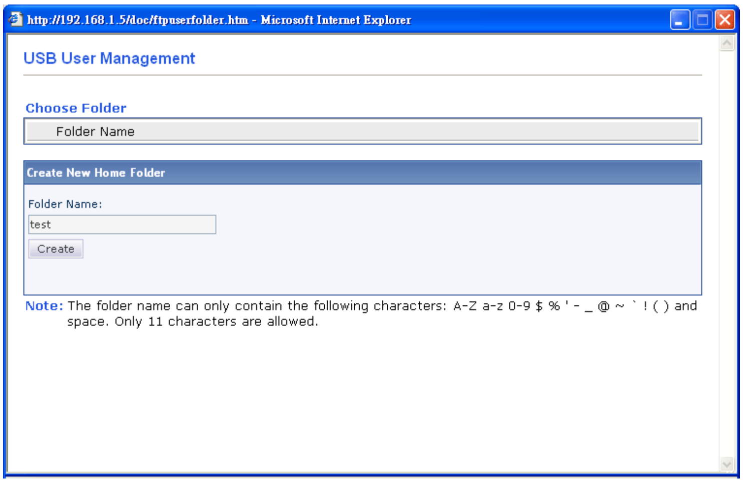
Confirm Password

Type the password again to make confirmation.

Home Folder

It determines the range 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 diskette. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB diskette.
Note: When write protect status for the USB diskette 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.



http://192.168.1.5/doc/ftpuserfolder.htm - Microsoft Internet Explorer

USB User Management

Choose Folder

Folder Name

Create New Home Folder

Folder Name:

test

Create

Note: The folder name can only contain the following characters: A-Z a-z 0-9 $ % ' - _ @ ~ ` ! ( ) and space. Only 11 characters are allowed.

Access Rule

It determines the authority for such profile. Any user, who uses such profile for accessing into USB diskette, must follow the rule specified here.

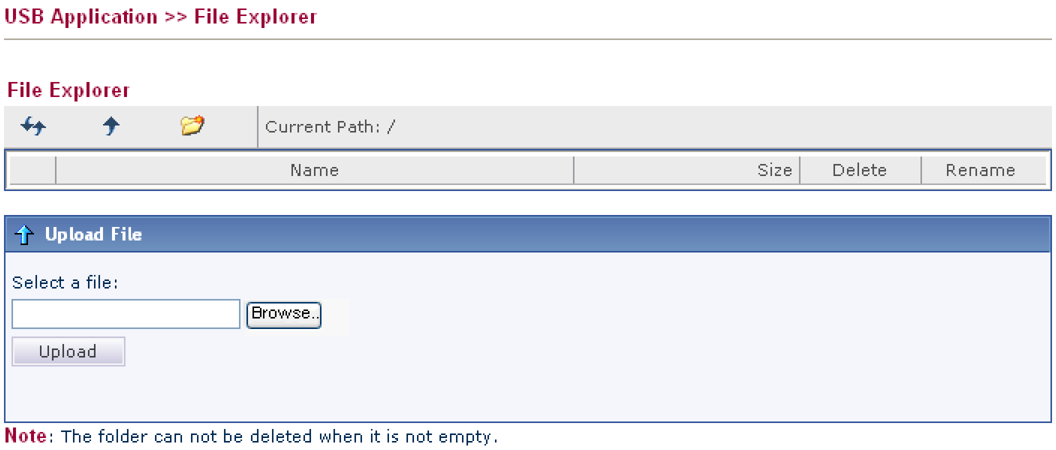
File – Check the items (Read, Write and Delete) for such profile.

Directory –Check the items (List, Create and Remove) for such profile.

Before you click **OK**, you have to insert a USB diskette into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

4.14.3 File Explorer

File Explorer offers an easy way for users to review and manage the content of USB diskette connected on Vigor router.



USB Application >> File Explorer

File Explorer

Current Path: /

	Name	Size	Delete	Rename

Upload File

Select a file:

Note: The folder can not be deleted when it is not empty.

Refresh Click this icon to refresh files list.

Back Click this icon to return to the upper directory.

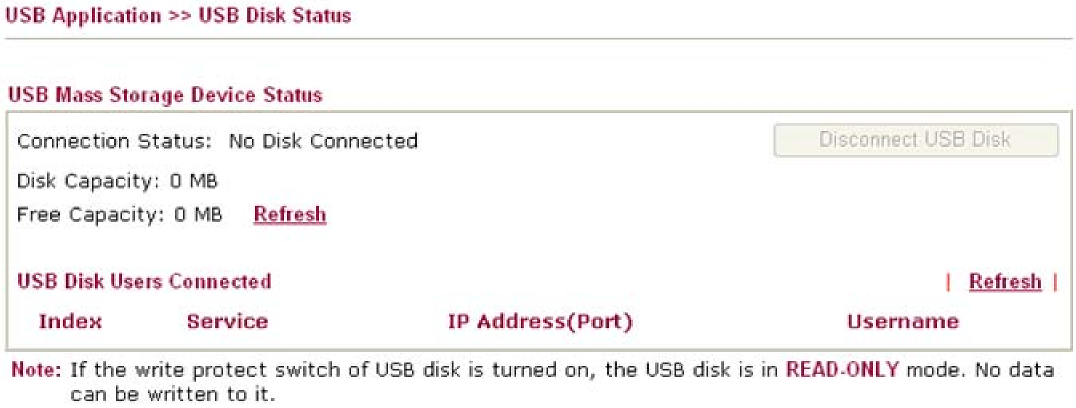
Create Click this icon to add a new folder.

Current Path Display current folder.

Upload Click this button to upload the selected file to the USB diskette. The uploaded file in the USB diskette can be shared for other user through FTP.

4.14.4 USB Disk Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB diskette) via the Vigor router. If you want to remove the diskette from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB diskette later.



USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: No Disk Connected

Disk Capacity: 0 MB

Free Capacity: 0 MB Refresh

USB Disk Users Connected | Refresh |

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.

Connection Status If there is no USB diskette connected to Vigor router, "**No Disk Connected**" will be shown here.

Disk Capacity It displays the total capacity of the USB diskette.

Free Capacity It displays the free space of the USB diskette. Click **Refresh** at any time to get new status for free capacity.

Index It displays the number of the client which connecting to FTP server.

IP Address It displays the IP address of the user's host which connecting to the FTP server.

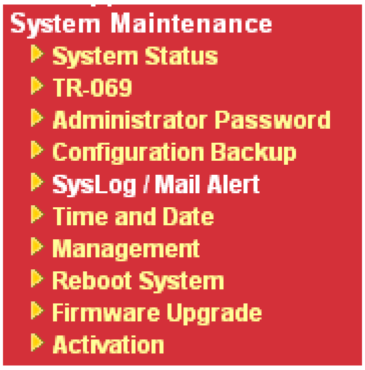
Username It displays the username that user uses to login to the FTP server.

When you insert USB diskette into the Vigor router, the system will start to find out such device within several seconds.

4.15 System Maintenance

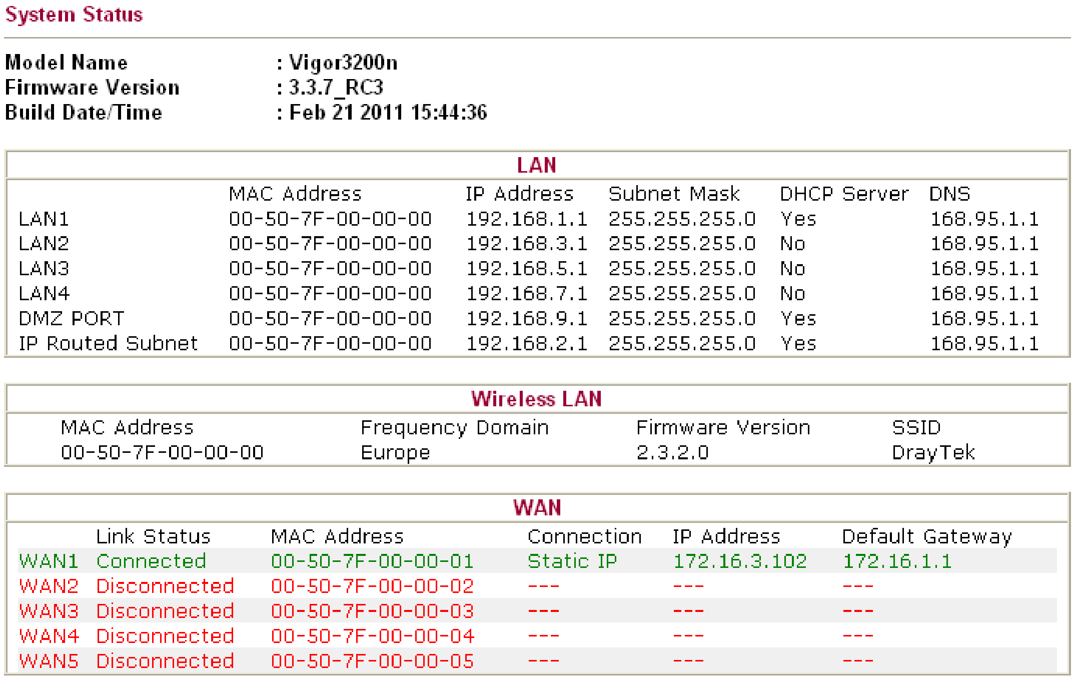
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.15.1 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 : Vigor3200n
Firmware Version : 3.3.7_RC3
Build Date/Time : Feb 21 2011 15:44:36

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-00-00-00	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-00-00-00	192.168.3.1	255.255.255.0	No	168.95.1.1
LAN3	00-50-7F-00-00-00	192.168.5.1	255.255.255.0	No	168.95.1.1
LAN4	00-50-7F-00-00-00	192.168.7.1	255.255.255.0	No	168.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.2.1	255.255.255.0	Yes	168.95.1.1

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-00-00-00	Europe	2.3.2.0	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-00-00-01	Static IP	172.16.3.102	172.16.1.1
WAN2	Disconnected	00-50-7F-00-00-02	---	---	---
WAN3	Disconnected	00-50-7F-00-00-03	---	---	---
WAN4	Disconnected	00-50-7F-00-00-04	---	---	---
WAN5	Disconnected	00-50-7F-00-00-05	---	---	---

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 built.

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.

Wireless LAN-------

MAC Address Display the MAC address of the wireless LAN.

Frequency Domain It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.

Firmware Version It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.

SSID Display the SSID of the router.

WAN-------

Link Status Display current connection status.

MAC Address Display the MAC address of the WAN Interface.

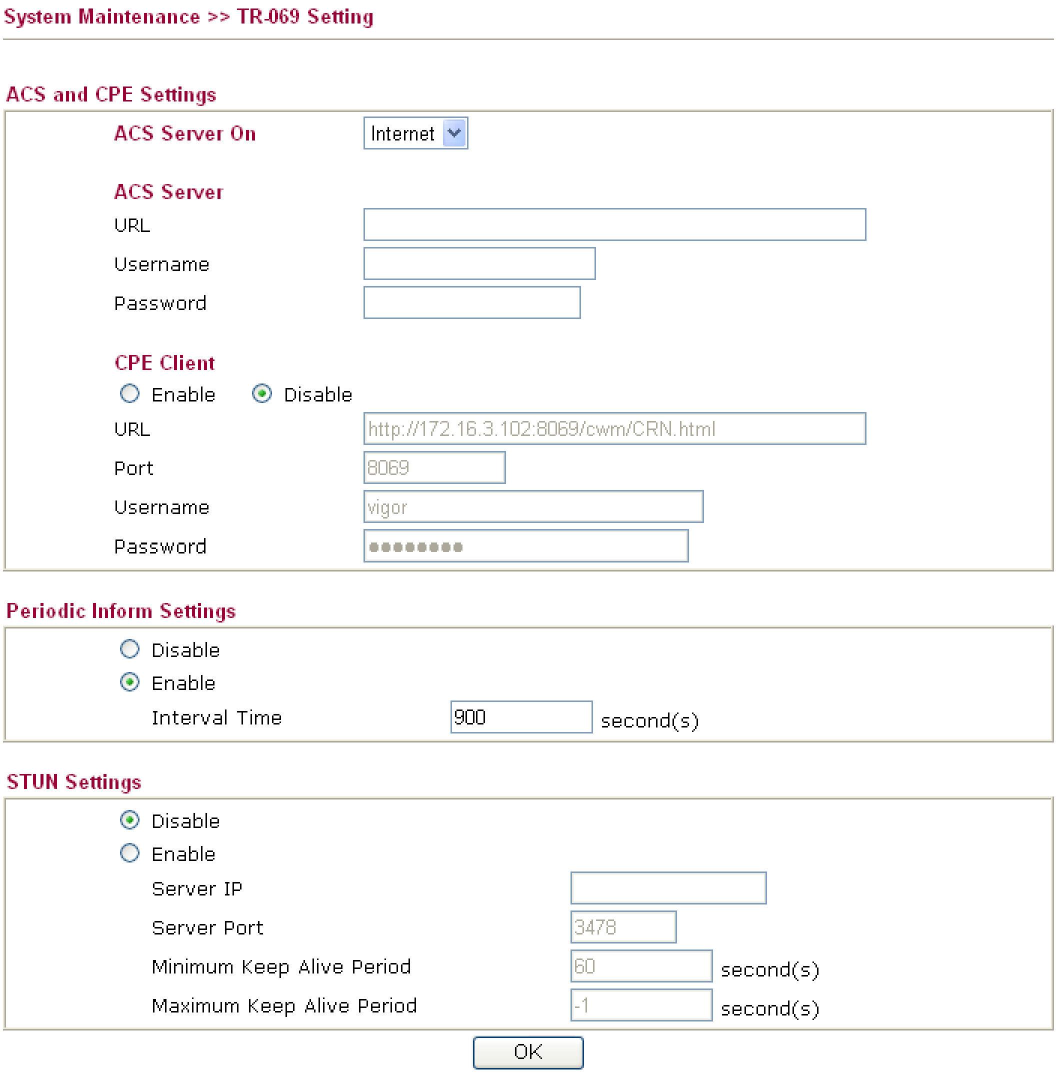
Connection Display the connection type.

IP Address Display the IP address of the WAN interface.

Default Gateway Display the assigned IP address of the default gateway.

4.15.2 TR-069

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



System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server On: Internet

ACS Server

URL:

Username:

Password:

CPE Client

○ Enable ● Disable

URL: http://172.16.3.102:8069/cwm/CRN.html

Port: 8069

Username: vigor

Password: ●●●●●●●●

Periodic Inform Settings

○ Disable

● Enable

Interval Time: 900 second(s)

STUN Settings

● Disable

○ Enable

Server IP:

Server Port: 3478

Minimum Keep Alive Period: 60 second(s)

Maximum Keep Alive Period: -1 second(s)

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.

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.

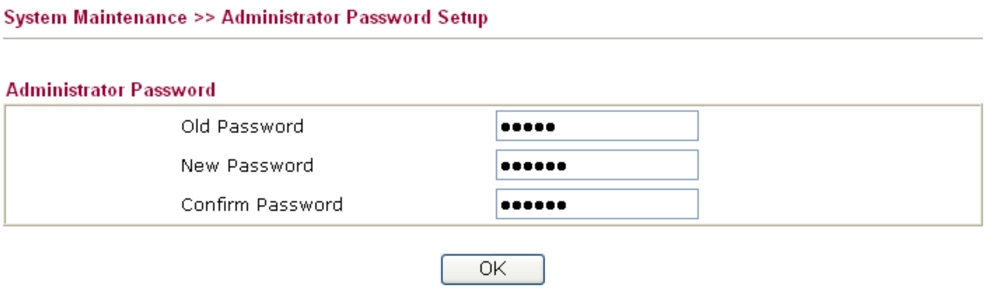
Server Port – Type the port number of the STUN server.

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.

4.15.3 Administrator Password

This page allows you to set new password.



System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	●●●●●
New Password	●●●●●●
Confirm Password	●●●●●●

Old Password Type in the old password. The factory default setting for password is **"admin"**.

New Password Type in new password in this field.

Confirm Password Type in the new password again.

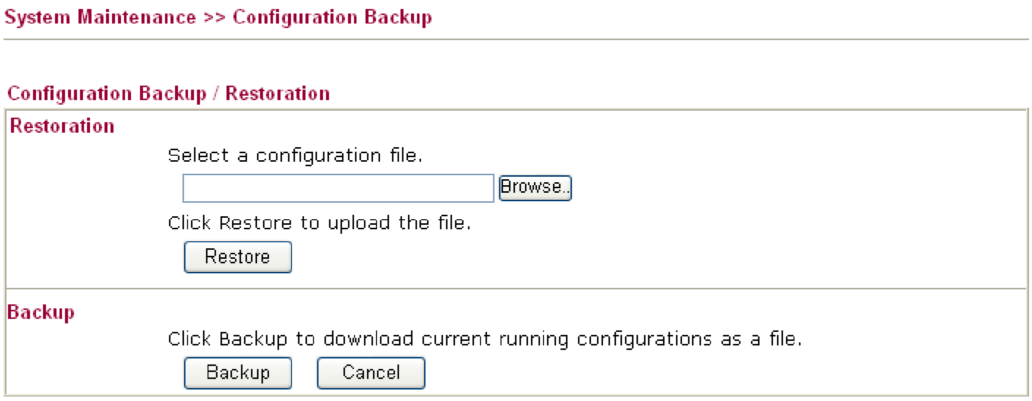
When you click **OK**, the login window will appear. Please use the new password to access into the web configurator again.

4.15.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

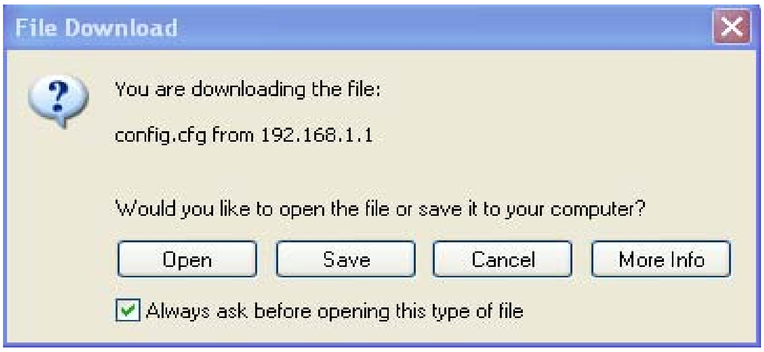
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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



File Download

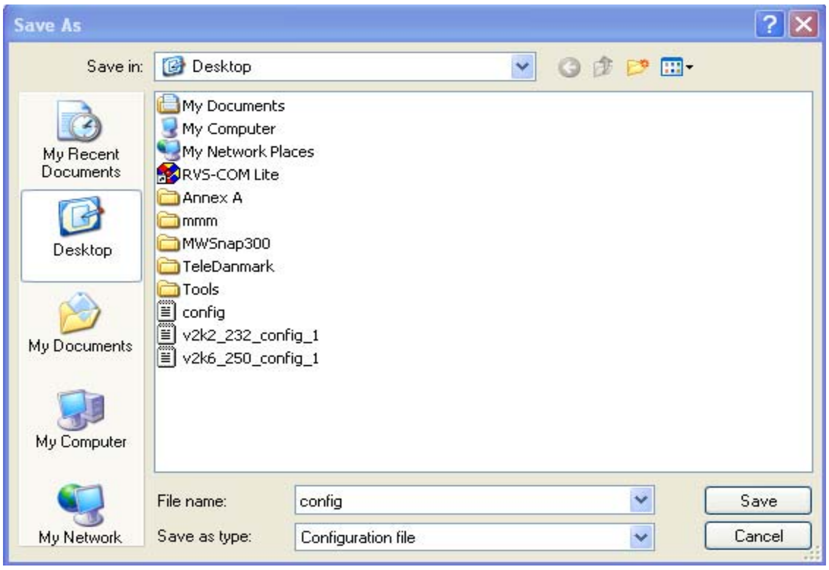
You are downloading the file:

config.cfg from 192.168.1.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

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



Save As

Save in: Desktop

File name: config

Save as type: Configuration file

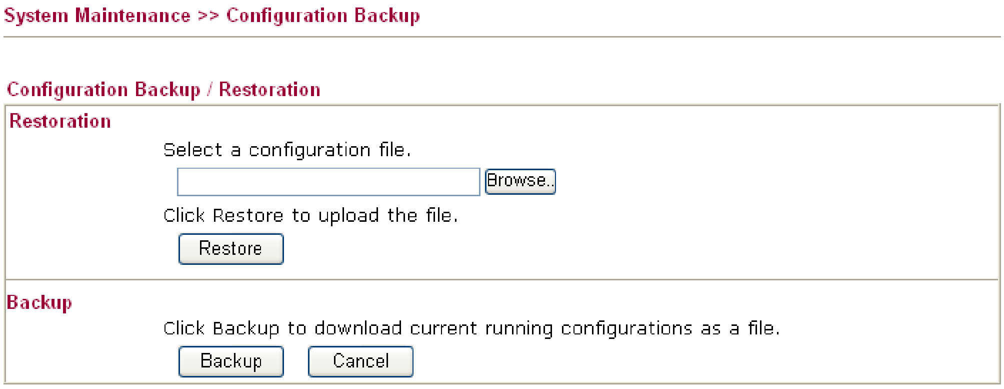
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.

Click Restore to upload the file.

Backup

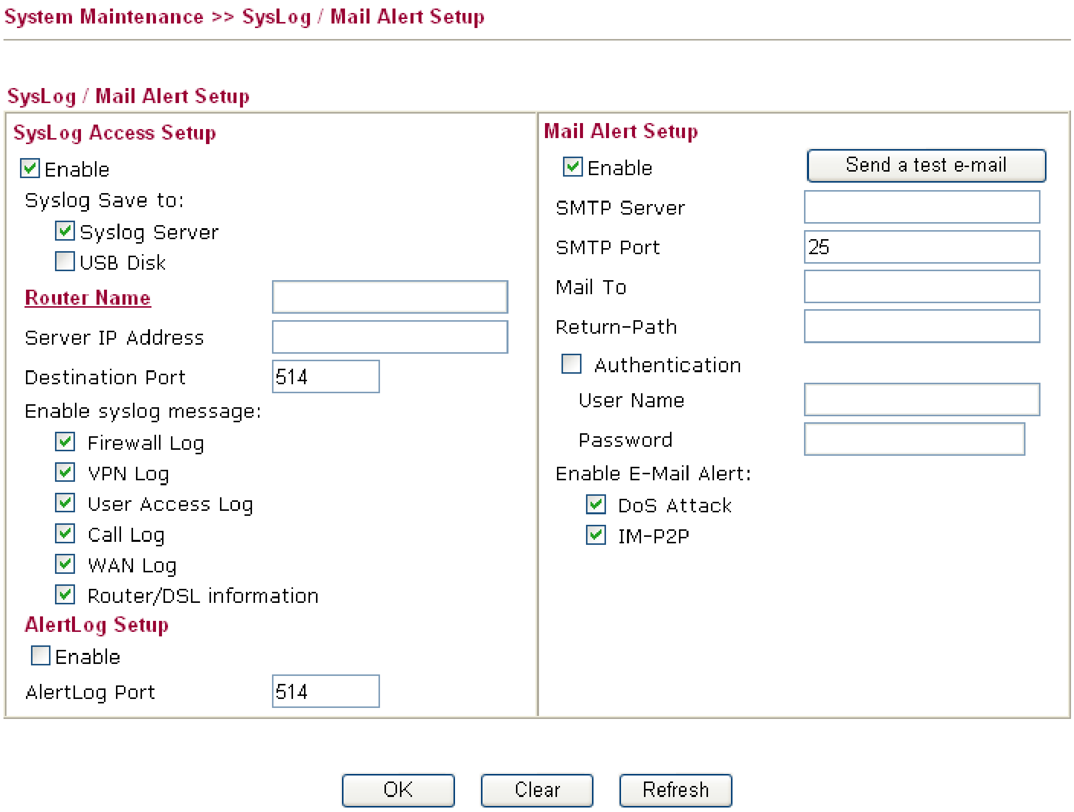
Click Backup to download current running configurations as a file.

2. Click **Browse** button to choose the correct configuration file for uploading to the router.

3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

4.15.5 Syslog/Mail Alert

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



System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup

☑ Enable

Syslog Save to:

☑ Syslog Server

□ USB Disk

Router Name

Server IP Address

Destination Port: 514

Enable syslog message:

☑ Firewall Log

☑ VPN Log

☑ User Access Log

☑ Call Log

☑ WAN Log

☑ Router/DSL information

AlertLog Setup

□ Enable

AlertLog Port: 514

Mail Alert Setup

☑ Enable

SMTP Server

SMTP Port: 25

Mail To

Return-Path

□ Authentication

User Name

Password

Enable E-Mail Alert:

☑ DoS Attack

☑ IM-P2P

Enable Check **Enable** to activate function of syslog.

Syslog Save to Check **Syslog Server** to save the log to Syslog directly.

Check **USB Disk** to save the log to the attached USB diskette.

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.

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.

AlertLog Setup Check "**Enable**" to activate function of alert log.

Type the port number for alert log. The default setting is 514.

Mail Alert Setup Check "**Enable**" to activate function of mail alert.

Send a test e-mail Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.

SMTP Server The IP address of the SMTP server.

Mail To Assign a mail address for sending mails out.

Return-Path Assign a path for receiving the mail from outside.

Authentication Check this box to activate this function while using e-mail application.

User Name Type the user name for authentication.

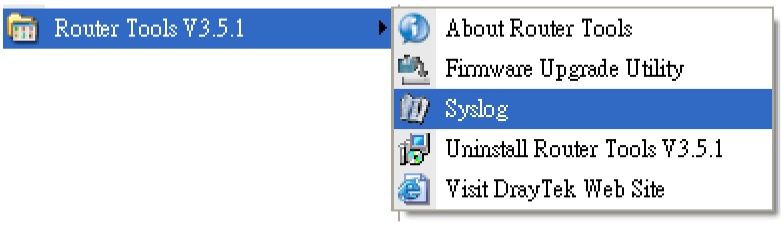
Password Type the password for authentication.

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.

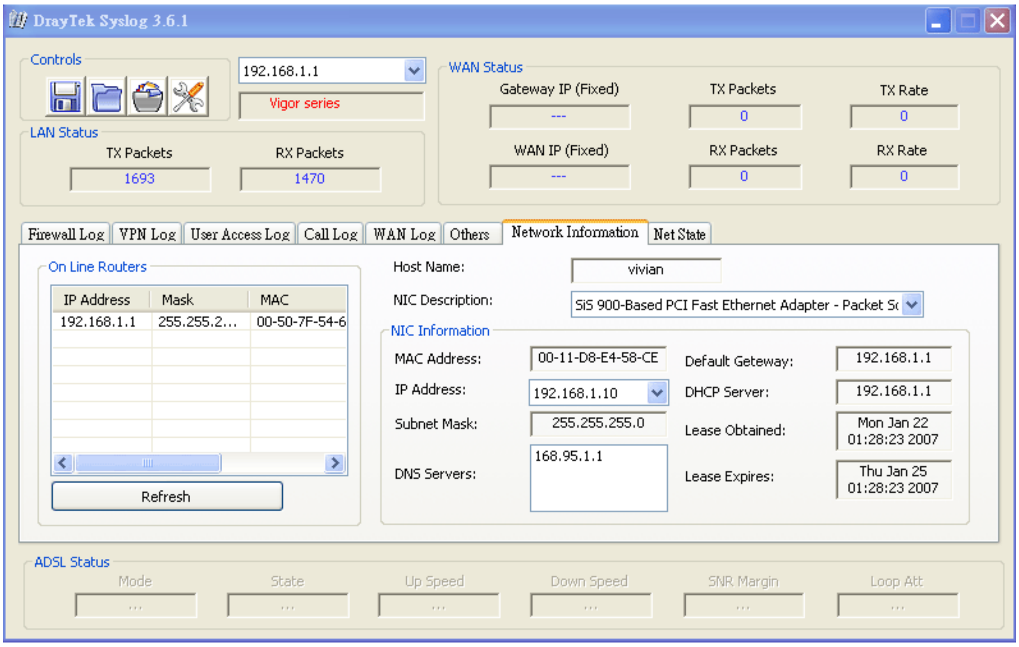
Click **OK** to save these settings.

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.



Controls: 192.168.1.1 — Vigor series

LAN Status: TX Packets 1693, RX Packets 1470

WAN Status: Gateway IP (Fixed) ---, TX Packets 0, TX Rate 0; WAN IP (Fixed) ---, RX Packets 0, RX Rate 0

IP Address	Mask	MAC
192.168.1.1	255.255.2...	00-50-7F-54-6

Host Name: vivian

NIC Description: SiS 900-Based PCI Fast Ethernet Adapter - Packet Sc

MAC Address: 00-11-D8-E4-58-CE

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DNS Servers: 168.95.1.1

Default Geteway: 192.168.1.1

DHCP Server: 192.168.1.1

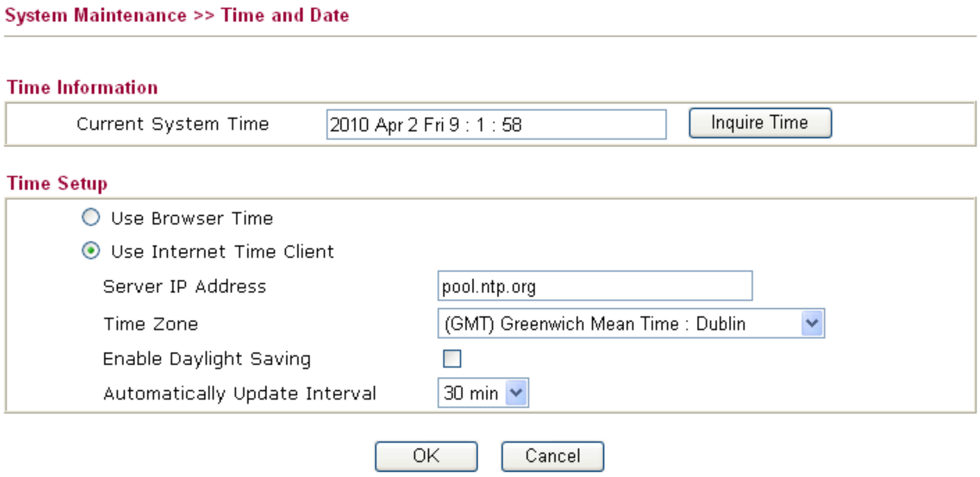
Lease Obtained: Mon Jan 22 01:28:23 2007

Lease Expires: Thu Jan 25 01:28:23 2007

ADSL Status: Mode ..., State ..., Up Speed ..., Down Speed ..., SNR Margin ..., Loop Att ...

4.15.6 Time and Date

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



System Maintenance >> Time and Date

Time Information

Current System Time: 2010 Apr 2 Fri 9 : 1 : 58

Time Setup

○ Use Browser Time

● Use Internet Time Client

Server IP Address: pool.ntp.org

Time Zone: (GMT) Greenwich Mean Time : Dublin

Enable Daylight Saving: □

Automatically Update Interval: 30 min

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 Protocol Select a time protocol.

Server IP Address Type the IP address of the time server.

Time Zone Select the time zone where the router is located.

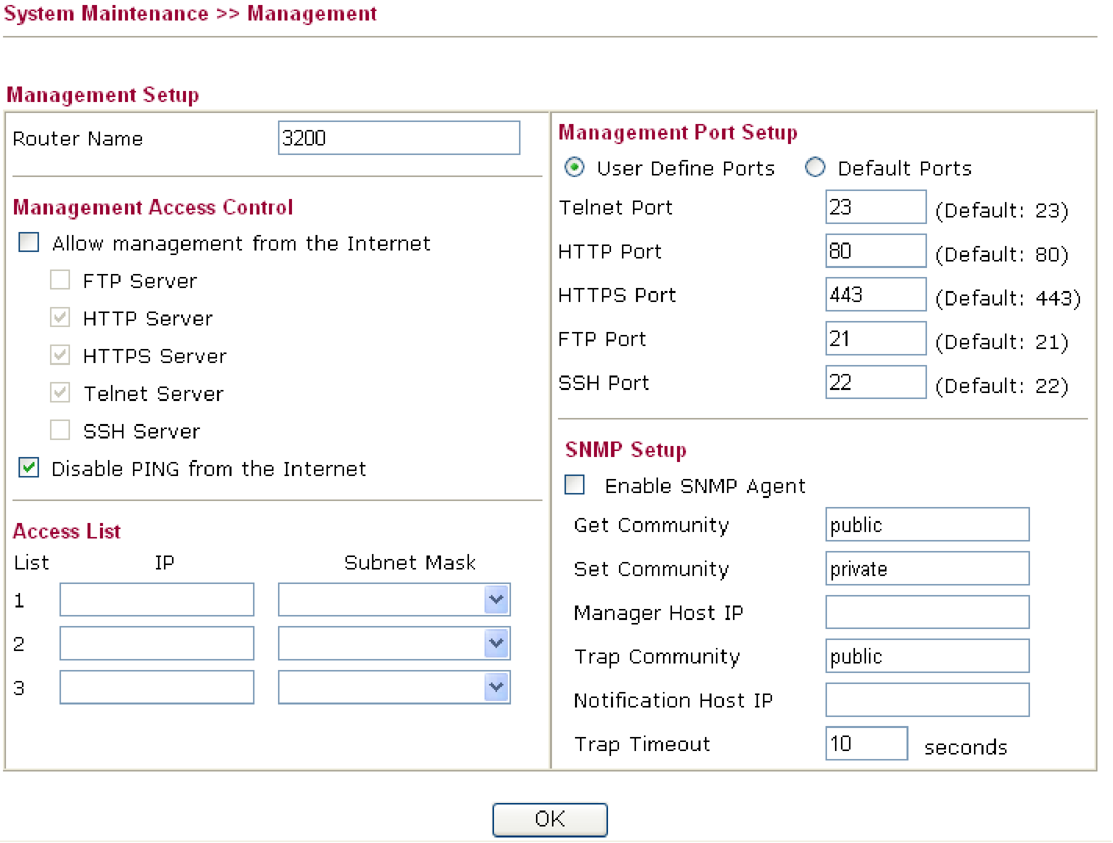
Enable Daylight Saving Check this box to enable daylight saving function.

Automatically Update Interval Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

4.15.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.



System Maintenance >> Management

Management Setup

Router Name: 3200

Management Access Control

☐ Allow management from the Internet

☐ FTP Server

☑ HTTP Server

☑ HTTPS Server

☑ Telnet Server

☐ SSH Server

☑ Disable PING from the Internet

Access List

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)
SSH Port	22	(Default: 22)

SNMP Setup

☐ Enable SNMP Agent

Get Community	public
Set Community	private
Manager Host IP	
Trap Community	public
Notification Host IP	
Trap Timeout	10 seconds

OK

Router Name Type a name as a identification for such router.

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 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.

Default Ports Check to use standard port numbers for the Telnet and HTTP servers.

User Defined Ports Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.

Enable SNMP Agent Check it to enable this function.

Get Community Set the name for getting community by typing a proper character. The default setting is **public.**

Set Community Set community by typing a proper name. The default setting is **private.**

Manager Host IP Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.

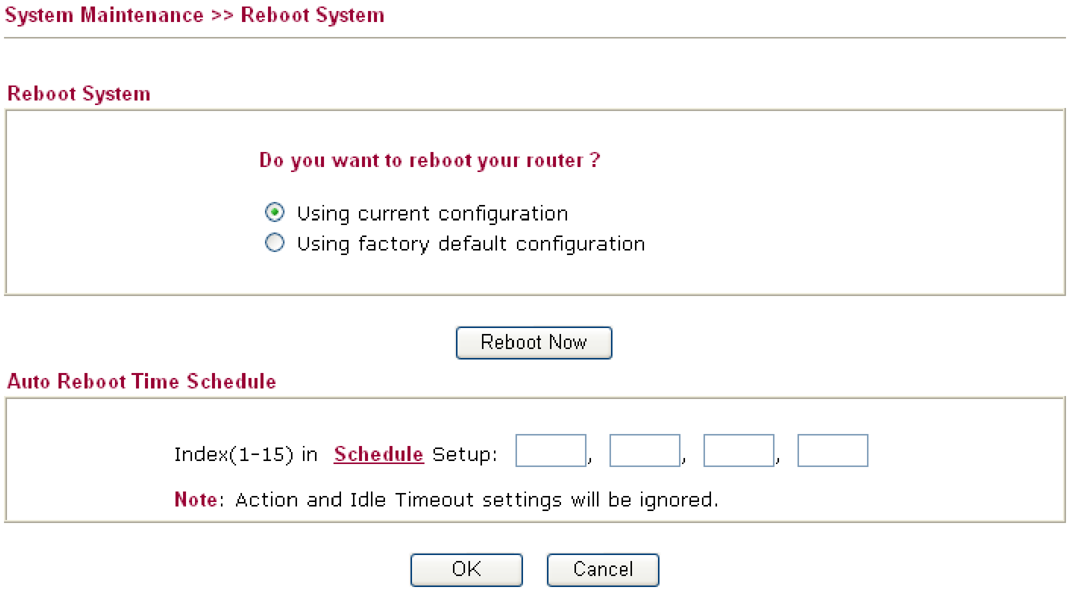
Trap Community Set trap community by typing a proper name. The default setting is **public.**

Notification Host IP Set the IP address of the host that will receive the trap community.

Trap Timeout The default setting is 10 seconds.

4.15.8 Reboot System

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



System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

● Using current configuration
○ Using factory default configuration

Auto Reboot Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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

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

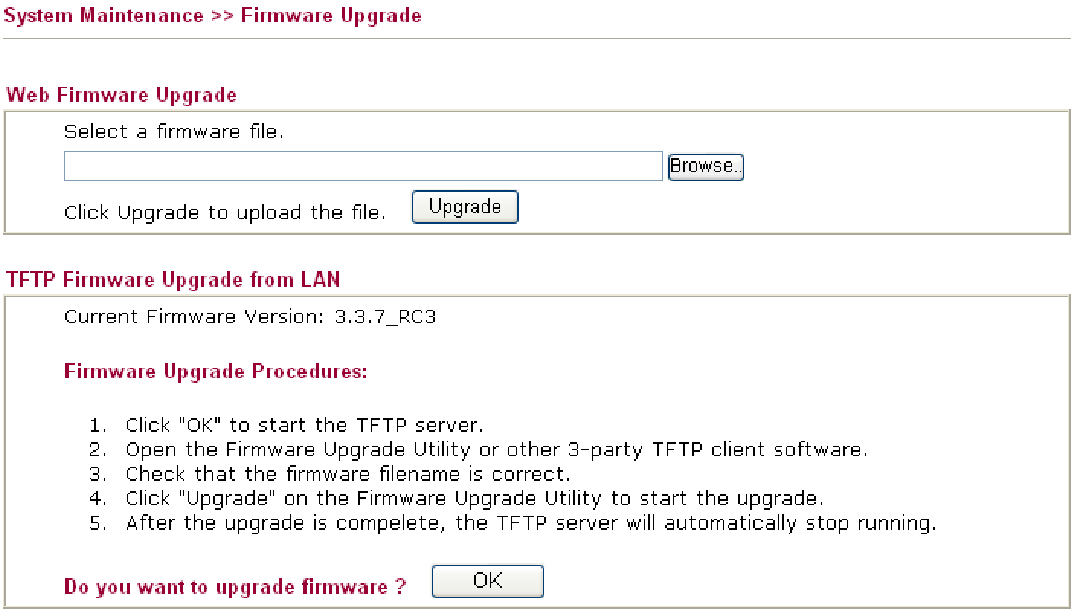
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

4.15.9 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.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

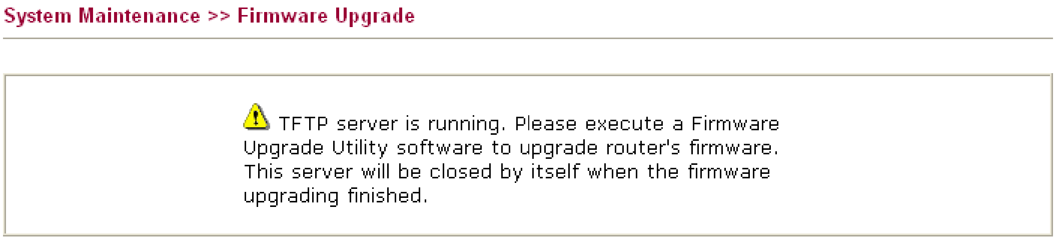
Current Firmware Version: 3.3.7_RC3

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 ?

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



System Maintenance >> Firmware Upgrade

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

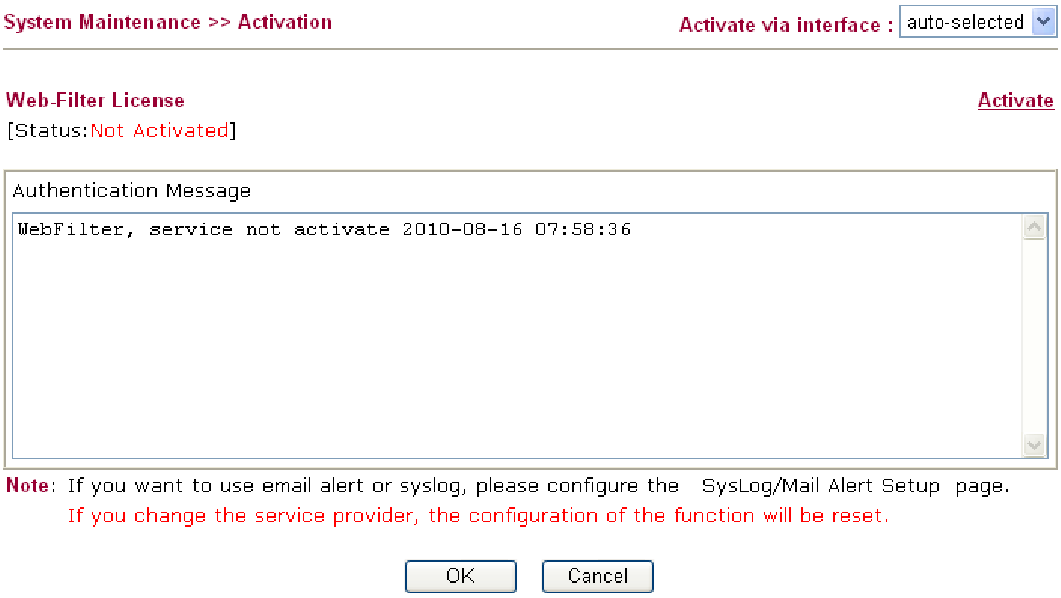
For the detailed information about firmware update, please go to Chapter 5.

4.15.10 Activation

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.


System Maintenance >> Activation
Activate via interface : auto-selected
Web-Filter License
Activate
OK
Cancel

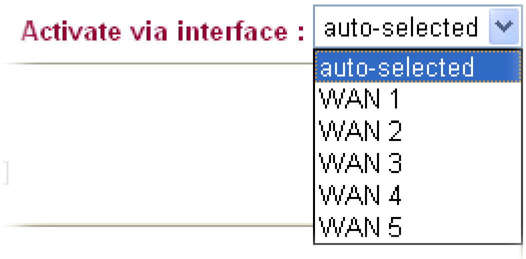
[Status:Not Activated]

Authentication Message

```
WebFilter, service not activate 2010-08-16 07:58:36
```

Note: If you want to use email alert or syslog, please configure the SysLog/Mail Alert Setup page.
If you change the service provider, the configuration of the function will be reset.

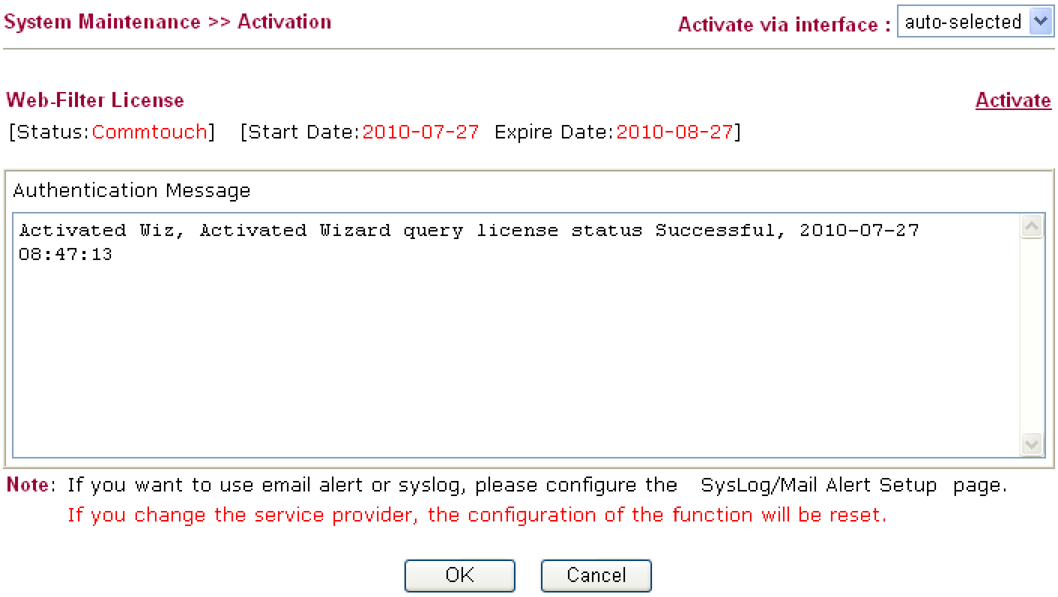
Activate via Interface Choose WAN interface used by such device for activating Web Content Filter.



Activate The **Activate** link brings you accessing into http://myvigor.draytek.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:



System Maintenance >> Activation

Activate via interface : auto-selected

Web-Filter License

Activate

[Status:Commtouch] [Start Date:2010-07-27 Expire Date:2010-08-27]

Authentication Message

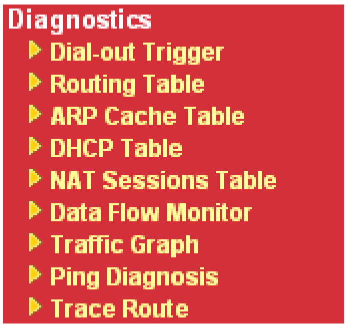
```
Activated Wiz, Activated Wizard query license status Successful, 2010-07-27
08:47:13
```

Note: If you want to use email alert or syslog, please configure the SysLog/Mail Alert Setup page.
If you change the service provider, the configuration of the function will be reset.

4.16 Diagnostics

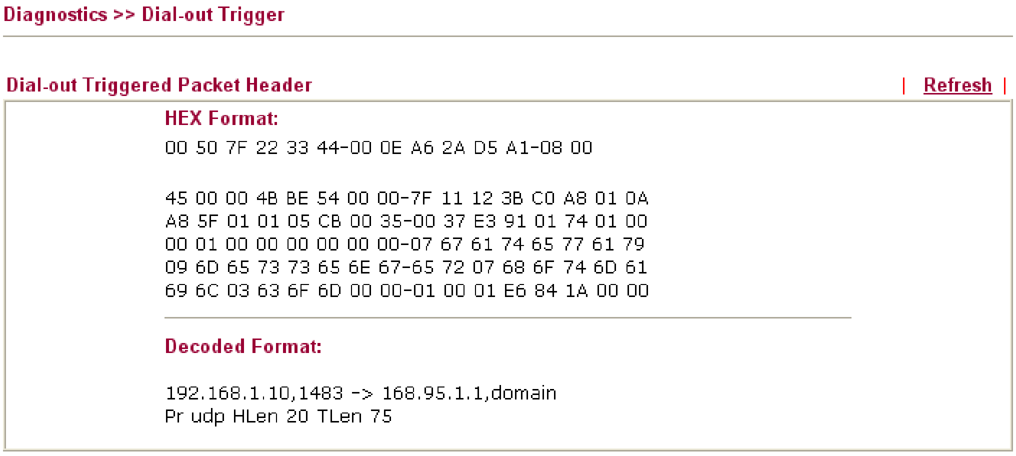
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



4.16.1 Dial-out Trigger

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



Diagnostics >> Dial-out Trigger

Dial-out Triggered Packet Header | Refresh |

HEX Format:

```
00 50 7F 22 33 44-00 0E A6 2A D5 A1-08 00

45 00 00 4B BE 54 00 00-7F 11 12 3B C0 A8 01 0A
A8 5F 01 01 05 CB 00 35-00 37 E3 91 01 74 01 00
00 01 00 00 00 00 00 00-07 67 61 74 65 77 61 79
09 6D 65 73 73 65 6E 67-65 72 07 68 6F 74 6D 61
69 6C 03 63 6F 6D 00 00-01 00 01 E6 84 1A 00 00
```

Decoded Format:

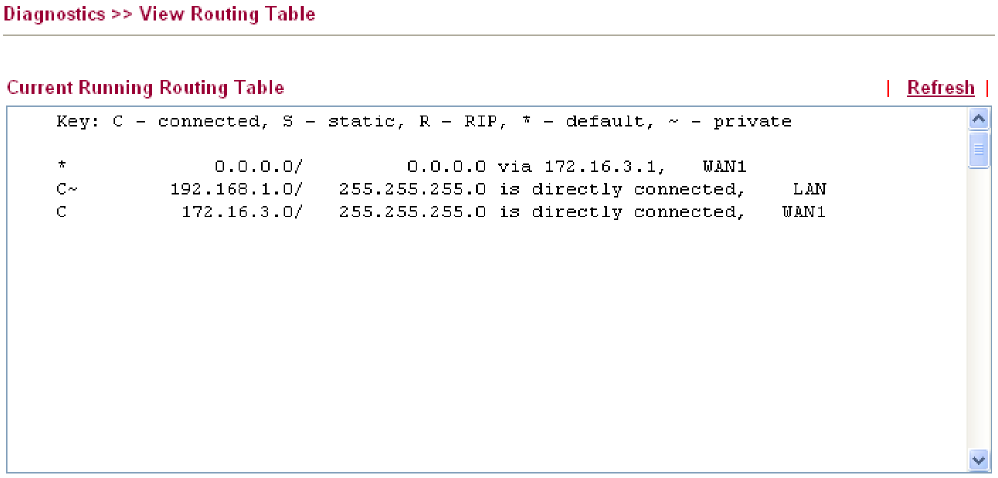
```
192.168.1.10,1483 -> 168.95.1.1,domain
Pr udp HLen 20 TLen 75
```

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.

4.16.2 Routing Table

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



Diagnostics >> View Routing Table

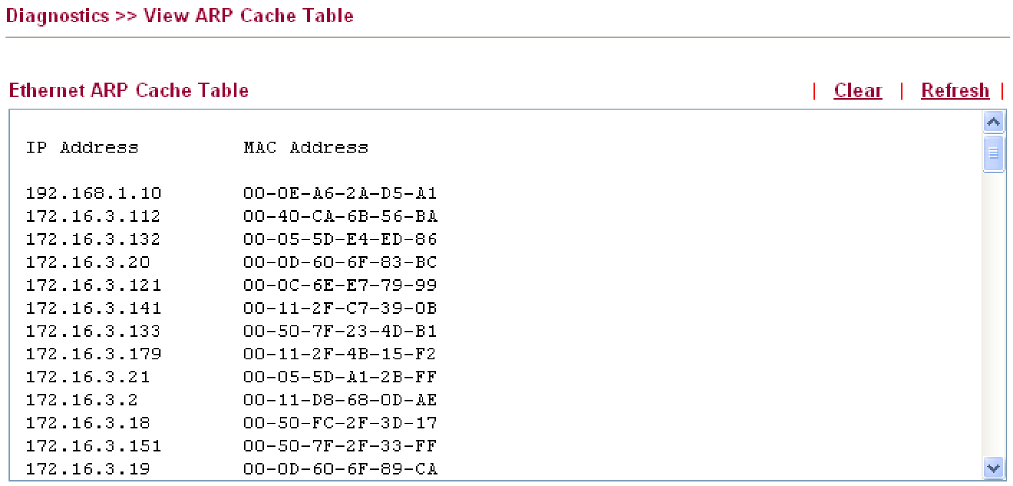
Current Running Routing Table | Refresh |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private

*            0.0.0.0/        0.0.0.0 via 172.16.3.1,   WAN1
C~        192.168.1.0/   255.255.255.0 is directly connected,    LAN
C          172.16.3.0/   255.255.255.0 is directly connected,   WAN1
```

Refresh Click it to reload the page.

4.16.3 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

192.168.1.10        00-0E-A6-2A-D5-A1
172.16.3.112        00-40-CA-6B-56-BA
172.16.3.132        00-05-5D-E4-ED-86
172.16.3.20         00-0D-60-6F-83-BC
172.16.3.121        00-0C-6E-E7-79-99
172.16.3.141        00-11-2F-C7-39-0B
172.16.3.133        00-50-7F-23-4D-B1
172.16.3.179        00-11-2F-4B-15-F2
172.16.3.21         00-05-5D-A1-2B-FF
172.16.3.2          00-11-D8-68-0D-AE
172.16.3.18         00-50-FC-2F-3D-17
172.16.3.151        00-50-7F-2F-33-FF
172.16.3.19         00-0D-60-6F-89-CA
```

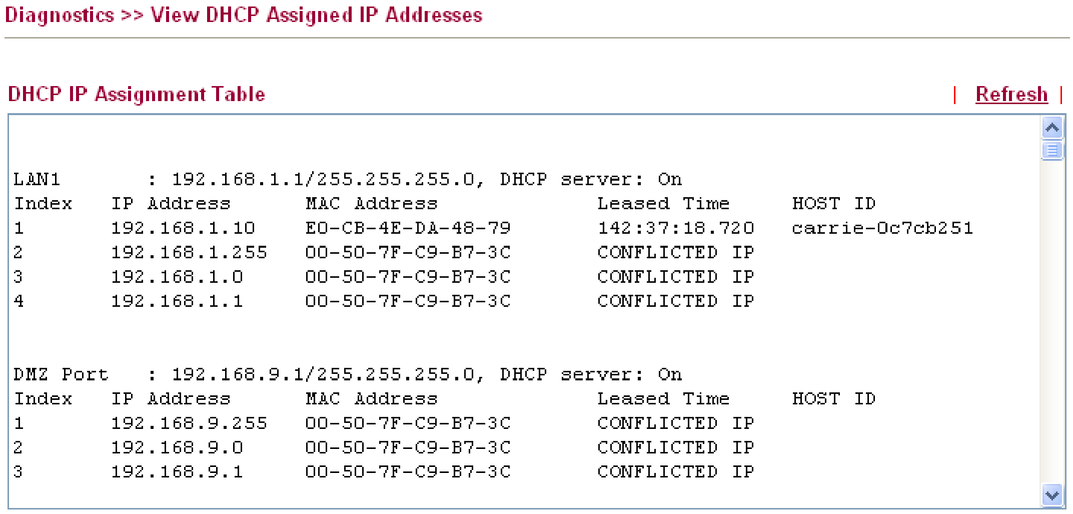
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

4.16.4 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

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



Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table | Refresh |

```
LAN1       : 192.168.1.1/255.255.255.0, DHCP server: On
Index   IP Address       MAC Address              Leased Time     HOST ID
1       192.168.1.10     E0-CB-4E-DA-48-79        142:37:18.720   carrie-0c7cb251
2       192.168.1.255    00-50-7F-C9-B7-3C        CONFLICTED IP
3       192.168.1.0      00-50-7F-C9-B7-3C        CONFLICTED IP
4       192.168.1.1      00-50-7F-C9-B7-3C        CONFLICTED IP


DMZ Port   : 192.168.9.1/255.255.255.0, DHCP server: On
Index   IP Address       MAC Address              Leased Time     HOST ID
1       192.168.9.255    00-50-7F-C9-B7-3C        CONFLICTED IP
2       192.168.9.0      00-50-7F-C9-B7-3C        CONFLICTED IP
3       192.168.9.1      00-50-7F-C9-B7-3C        CONFLICTED IP
```

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.

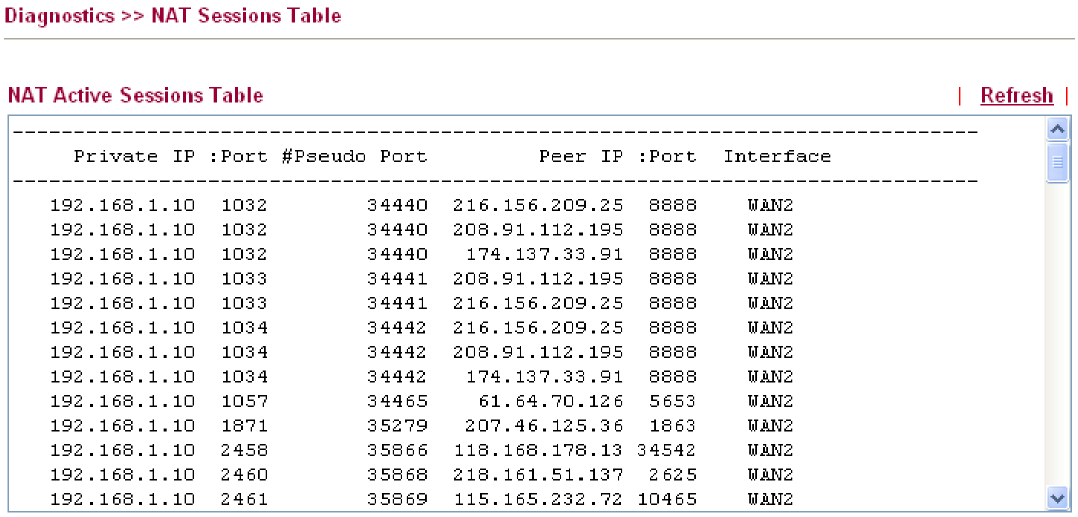
Leased Time It displays the leased time of the specified PC.

HOST ID It displays the host ID name of the specified PC.

Refresh Click it to reload the page.

4.16.5 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
--------------------------------------------------------------------------------
   192.168.1.10  1032        34440  216.156.209.25  8888    WAN2
   192.168.1.10  1032        34440  208.91.112.195  8888    WAN2
   192.168.1.10  1032        34440   174.137.33.91  8888    WAN2
   192.168.1.10  1033        34441  208.91.112.195  8888    WAN2
   192.168.1.10  1033        34441  216.156.209.25  8888    WAN2
   192.168.1.10  1034        34442  216.156.209.25  8888    WAN2
   192.168.1.10  1034        34442  208.91.112.195  8888    WAN2
   192.168.1.10  1034        34442   174.137.33.91  8888    WAN2
   192.168.1.10  1057        34465    61.64.70.126  5653    WAN2
   192.168.1.10  1871        35279   207.46.125.36  1863    WAN2
   192.168.1.10  2458        35866  118.168.178.13 34542    WAN2
   192.168.1.10  2460        35868  218.161.51.137  2625    WAN2
   192.168.1.10  2461        35869  115.165.232.72 10465    WAN2
```

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.

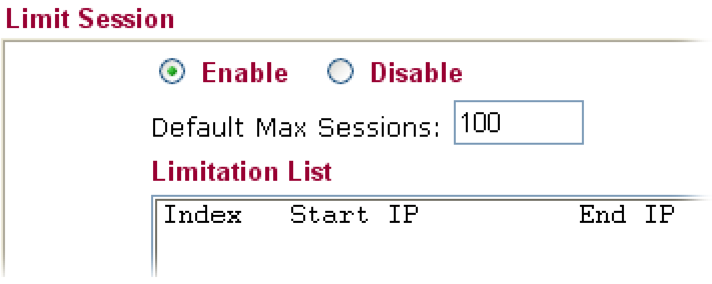
Peer IP:Port It indicates the destination IP address and port of remote host.

Interface It displays the representing number for different interface.

Refresh Click it to reload the page.

4.16.6 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 invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.



Limit Session

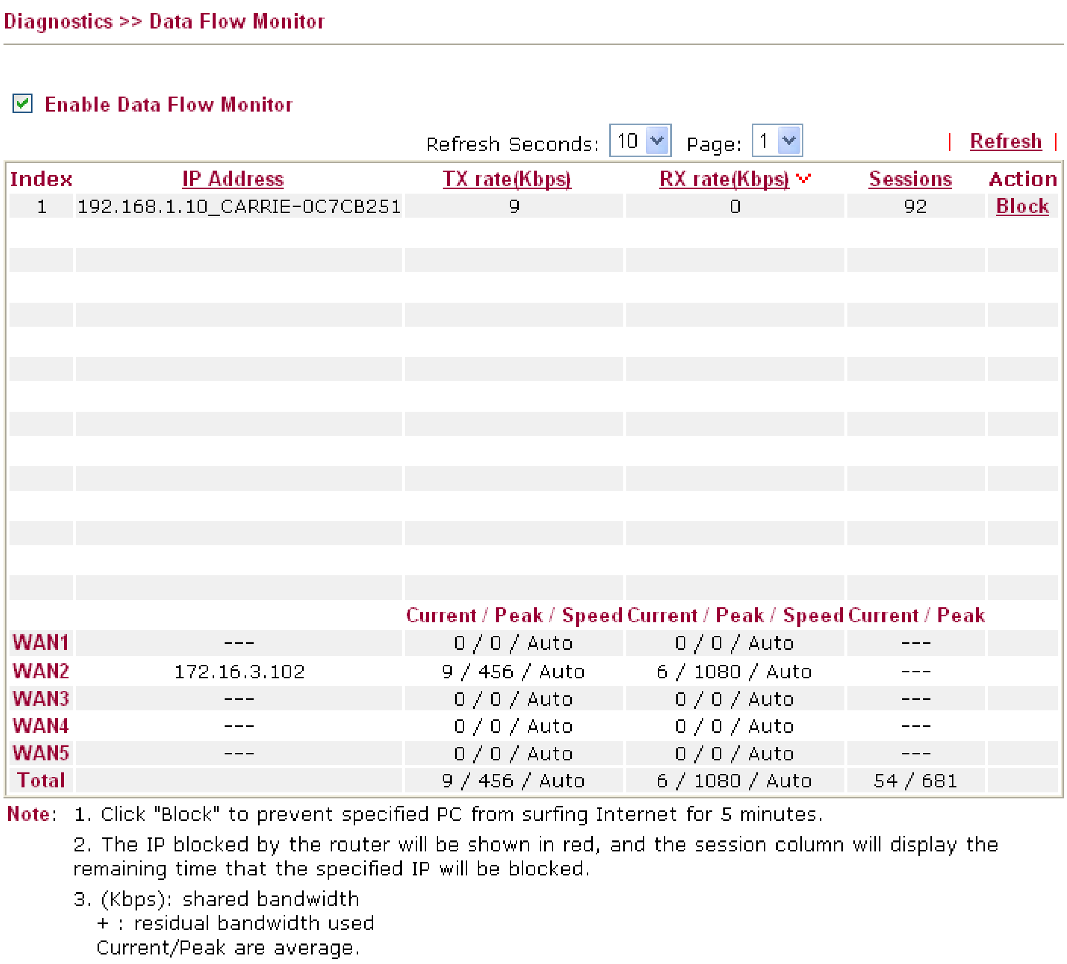
● Enable ○ Disable

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

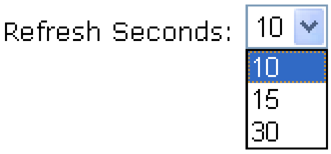
Refresh Seconds: 10 | Page: 1 | Refresh |

Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Sessions	Action
1	192.168.1.10_CARRIE-0C7CB251	9	0	92	Block
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak	
WAN1	---	0 / 0 / Auto	0 / 0 / Auto	---	
WAN2	172.16.3.102	9 / 456 / Auto	6 / 1080 / Auto	---	
WAN3	---	0 / 0 / Auto	0 / 0 / Auto	---	
WAN4	---	0 / 0 / Auto	0 / 0 / Auto	---	
WAN5	---	0 / 0 / Auto	0 / 0 / Auto	---	
Total		9 / 456 / Auto	6 / 1080 / Auto	54 / 681	

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
Current/Peak are average.

Enable Data Flow Monitor Check this box to enable this function.

Refresh Seconds Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.



Refresh Seconds: 10

Refresh Click this link to refresh this page manually.

Index Display the number of the data flow.

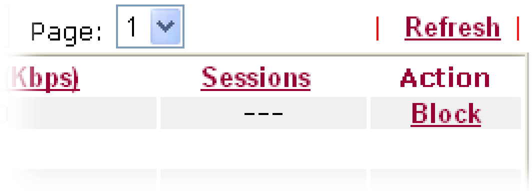
IP Address Display the IP address of the monitored device.

TX rate (kbps) Display the transmission speed of the monitored device.

RX rate (kbps) Display the receiving speed of the monitored device.

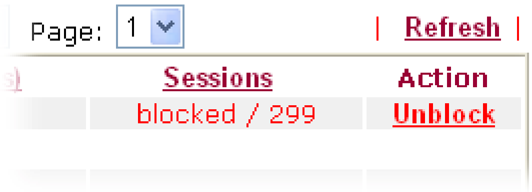
Sessions Display the session number that you specified in Limit Session web page.

Action **Block -** can prevent specified PC accessing into Internet within 5 minutes.



Kbps)	Sessions	Action
	---	Block

Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.



s)	Sessions	Action
	blocked / 299	Unblock

Current /Peak/Speed

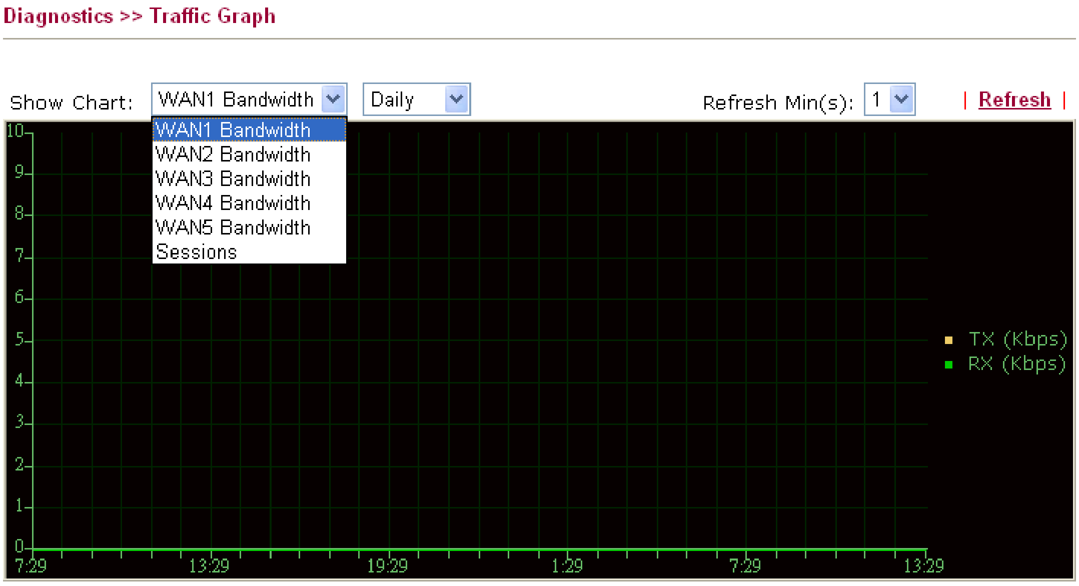
Current means current transmission rate and receiving rate for WAN interface.

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.

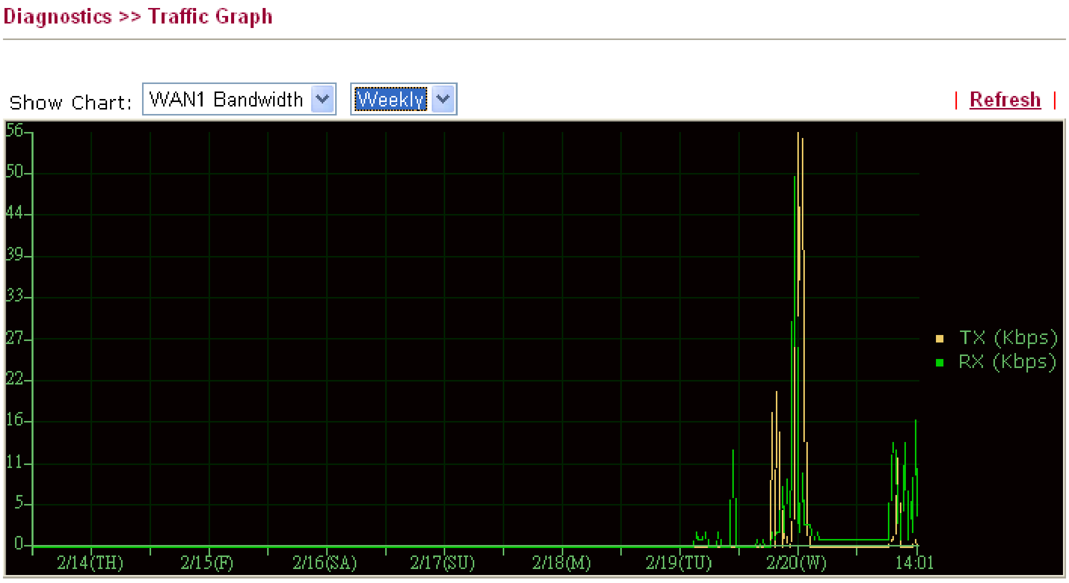
4.16.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WN3/WAN4/WAN5 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



Diagnostics >> Traffic Graph

Show Chart: WAN1 Bandwidth | Daily | Refresh Min(s): 1 | Refresh |



Diagnostics >> Traffic Graph

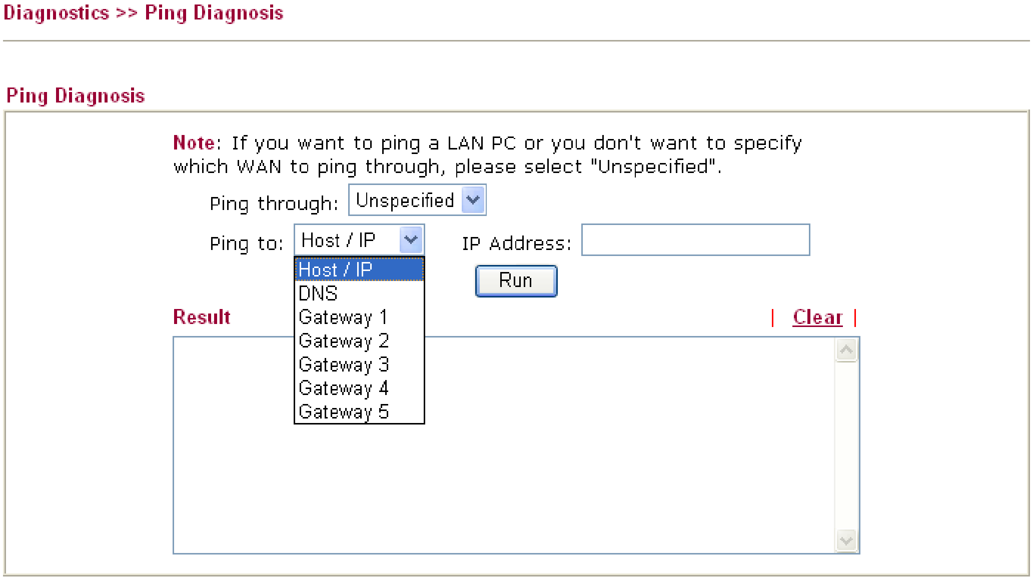
Show Chart: WAN1 Bandwidth | Weekly | Refresh |

The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/WAN4/WAN5 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.

4.16.8 Ping Diagnosis

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



Diagnostics >> Ping Diagnosis

Ping Diagnosis

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

Ping through: Unspecified

Ping to: Host / IP   IP Address:

Result | Clear |

Ping through Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Ping to Use the drop down list to choose the destination that you want to ping.

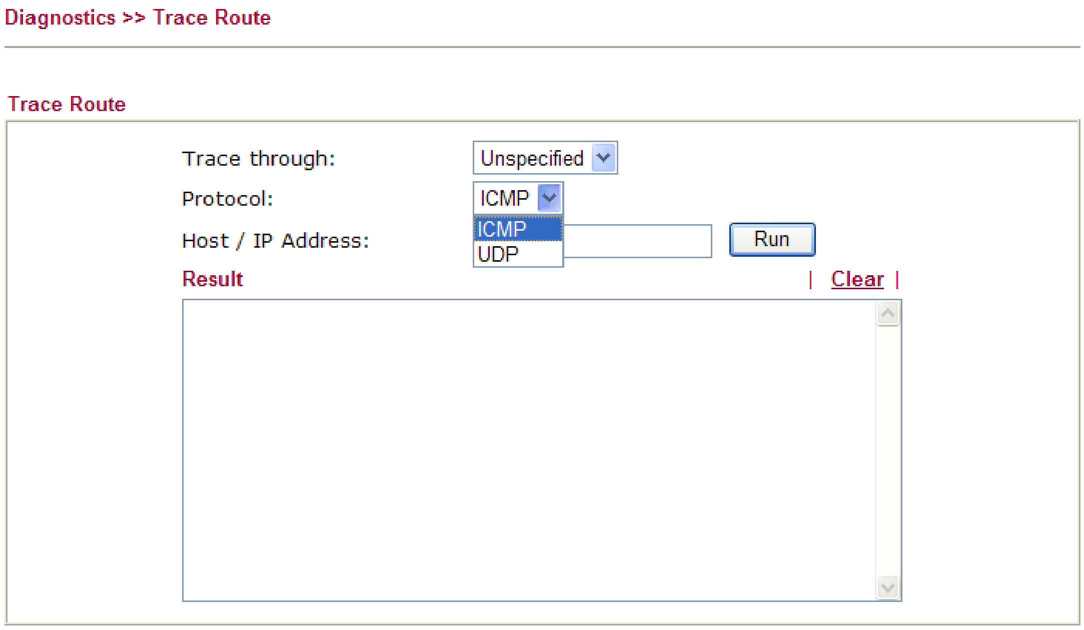
IP Address Type in the IP address of the Host/IP that you want to ping.

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.

4.16.9 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

Trace through: Unspecified

Protocol: ICMP

Host / IP Address:

Trace through Use the drop down list to choose the WAN interface that you want to ping through.

Protocol Use the drop down list to choose the protocol that you want to ping through.

Host/IP Address It indicates the IP address of the host.

Run Click this button to start route tracing work.

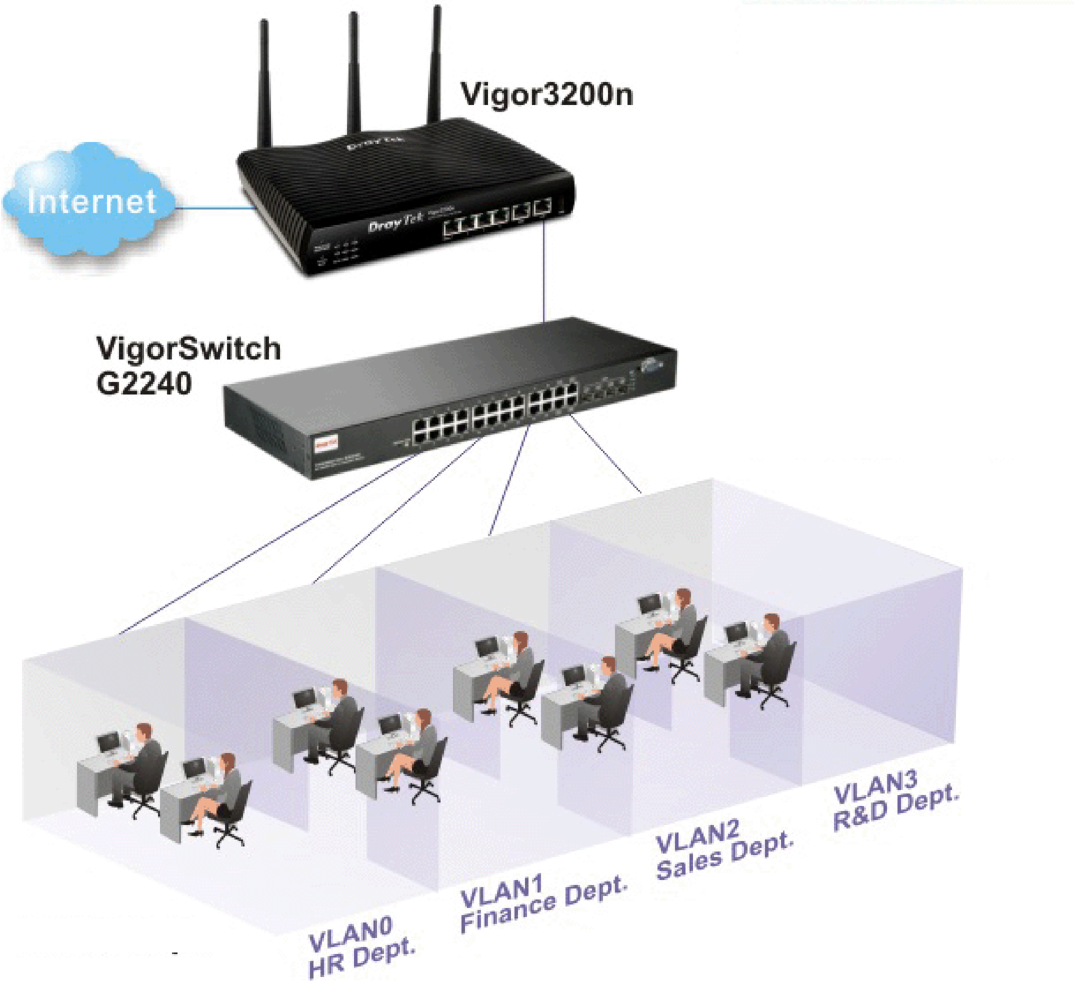
Clear Click this link to remove the result on the window.

5 Application and Examples

5.1 How to Configure Multi-Subnet

By identifying the tagged message, Vigor3200 can divide the LAN Port into several VLAN groups. Such LAN port with tagged information will accept the packets only with VLAN ID number.

For example, Vigor3200 can divide the internal departments of a company into four different groups by using VigorSwitch G2240. Each group uses different network segment and does not connect for each other. VigorSwitch G2240 Trunk Port 23 and Vigor3200 LAN Port are connected with network cable. See the following graphic for an example.



VLAN0 (Human Resource): LAN Port 4 IP: 192.168.1.0/24

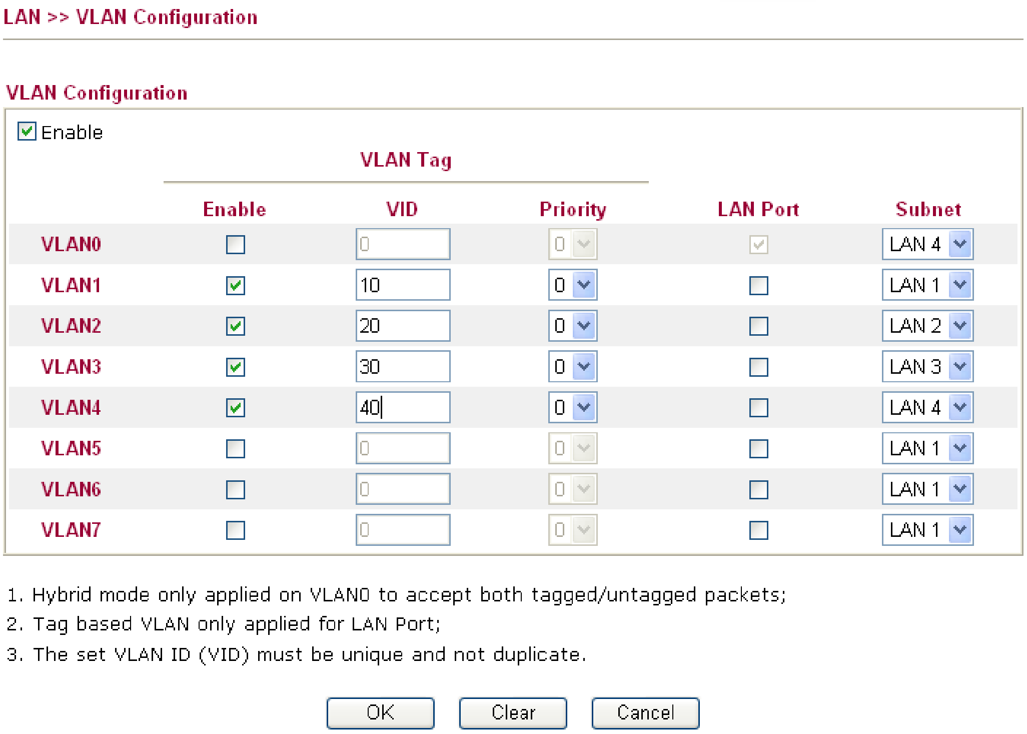
VLAN1 (Finance Dept): LAN Port 4 IP: 192.168.3.0/24

VLAN2 (Sales Dept.): LAN Port 4 IP: 192.168.5.0/24

VLAN3 (R&D): LAN Port 4 IP: 192.168.7.0/24

Configuration for Vigor3200

1. In the page of **LAN** >> **VLAN Configuration**, check the box of **Enable** to enable the function of VLAN Configuration.
2. Untag VLAN0 and set **LAN4** as the **Subnet**.
3. To activate the function of VLAN Tag for VLAN1 setting, check the box of **Enable** and type the value (10) for VID setting. Then check **LAN Port** and set **LAN1** as the **Subnet**.
4. To activate the function of VLAN Tag for VLAN2 setting, check the box of **Enable** and type the value (20) for VID setting. Then check **LAN Port** and set **LAN2** as the **Subnet**.
5. To activate the function of VLAN Tag for VLAN3 setting, check the box of **Enable** and type the value (30) for VID setting. Then check **LAN Port** and set **LAN3** as the **Subnet**.
6. To activate the function of VLAN Tag for VLAN4 setting, check the box of **Enable** and type the value (40) for VID setting. Then check **LAN Port** and set **LAN4** as the **Subnet**.



LAN >> VLAN Configuration

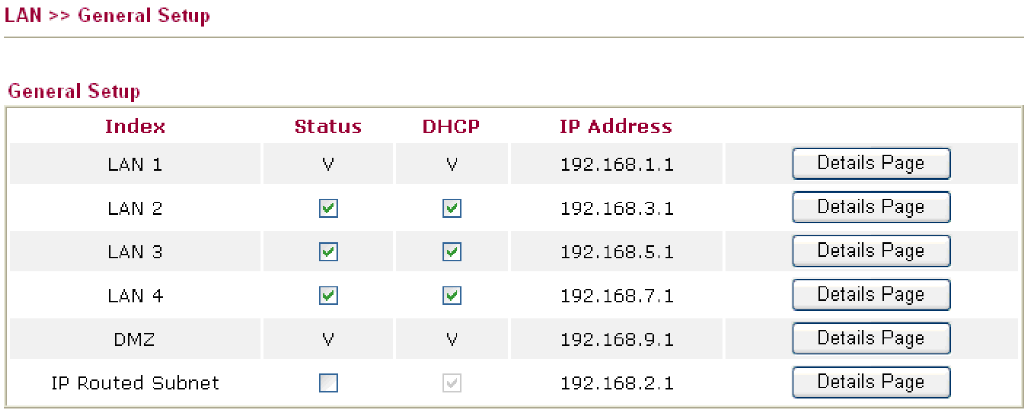
VLAN Configuration

☑ Enable

	VLAN Tag				
	Enable	VID	Priority	LAN Port	Subnet
VLAN0	□	0	0	☑	LAN 4
VLAN1	☑	10	0	□	LAN 1
VLAN2	☑	20	0	□	LAN 2
VLAN3	☑	30	0	□	LAN 3
VLAN4	☑	40	0	□	LAN 4
VLAN5	□	0	0	□	LAN 1
VLAN6	□	0	0	□	LAN 1
VLAN7	□	0	0	□	LAN 1

1. Hybrid mode only applied on VLAN0 to accept both tagged/untagged packets;
2. Tag based VLAN only applied for LAN Port;
3. The set VLAN ID (VID) must be unique and not duplicate.

In the page of **LAN** >> **General Setup**, check the **Status** box of LAN2, LAN3, LAN4 and enable the function of DHCP.



LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page
LAN 2	☑	☑	192.168.3.1	Details Page
LAN 3	☑	☑	192.168.5.1	Details Page
LAN 4	☑	☑	192.168.7.1	Details Page
DMZ	V	V	192.168.9.1	Details Page
IP Routed Subnet	□	☑	192.168.2.1	Details Page

After finishing the above configuration, the equipment connecting to Vigor3200 LAN Port can get the corresponding IP address of the network segment.

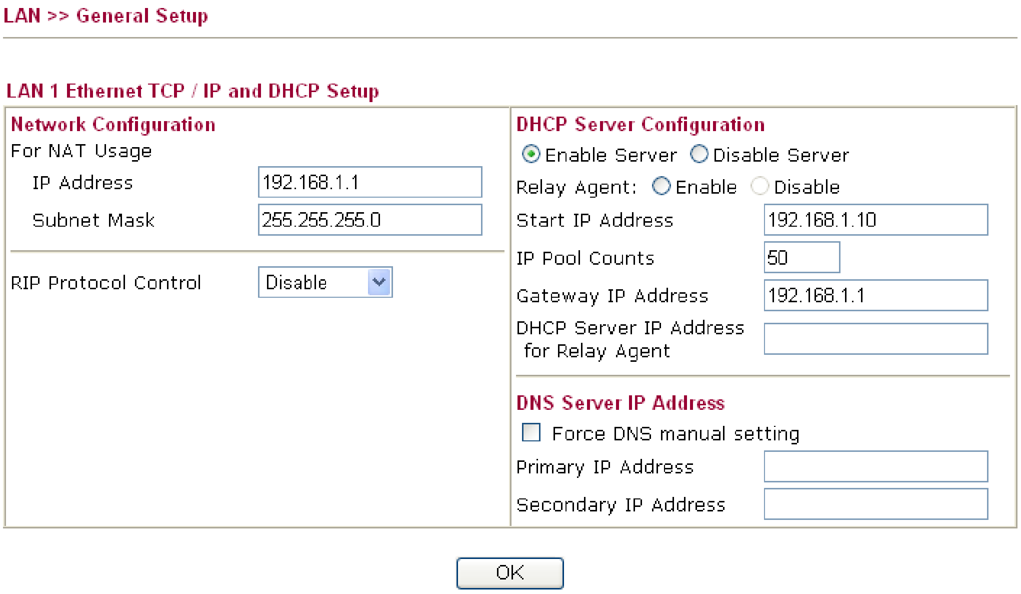
The equipment connecting to Vigor3200 LAN Port 1 (LAN1) can get the IP address of 192.168.1.0/24.

The equipment connecting to Vigor3200 LAN Port 2 (LAN2) can get the IP address of 192.168.3.0/24.

The equipment connecting to Vigor3200 LAN Port 3 (LAN3) can get the IP address of 192.168.5.0/24.

The equipment connecting to Vigor3200 LAN Port 4 (LAN4) can get the IP address of 192.168.7.0/24.

For the detailed settings of the network segment, open **LAN>>General Setup** and click **Details Page.** Adjust the settings for your request. Refer to the following figure.



LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration

For NAT Usage

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
RIP Protocol Control	Disable

DHCP Server Configuration

● Enable Server ○ Disable Server

Relay Agent: ○ Enable ○ Disable

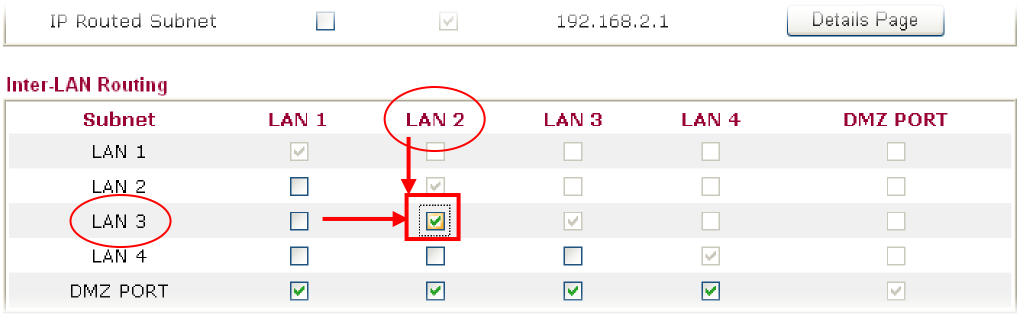
Start IP Address	192.168.1.10
IP Pool Counts	50
Gateway IP Address	192.168.1.1
DHCP Server IP Address for Relay Agent	

DNS Server IP Address

□ Force DNS manual setting

Primary IP Address	
Secondary IP Address	

7. To make any two of VLAN groups linked with each other, just check the boxes of the ones in the field of Inter-LAN Routing in the page of **LAN** >> **General Setup**. Refer to the following figure. LAN2 and LAN3 are linked.



IP Routed Subnet	□	☑	192.168.2.1	Details Page

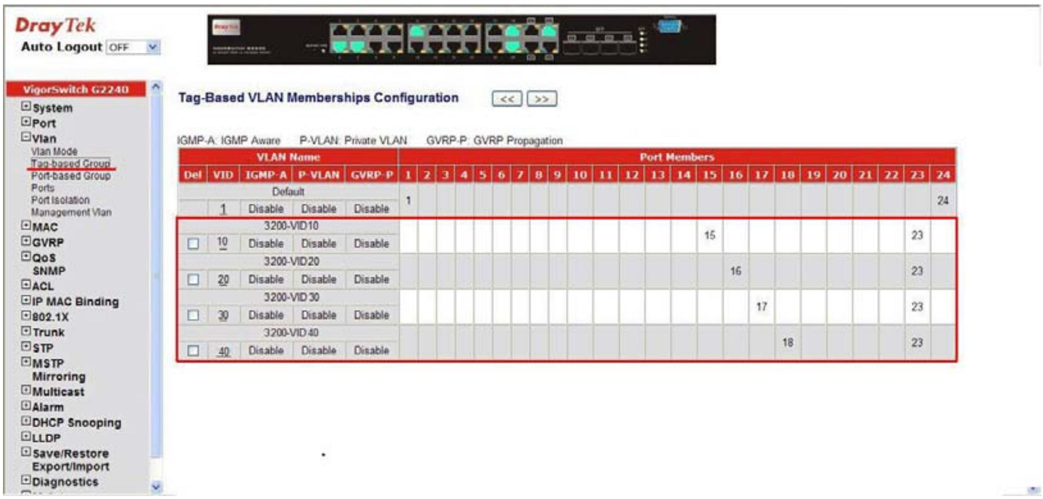
Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1	☑	□	□	□	□
LAN 2	□	☑	□	□	□
LAN 3	□	☑	☑	□	□
LAN 4	□	□	□	☑	□
DMZ PORT	☑	☑	☑	☑	☑

Configuration for VigorSwitch G2240

1. Open **Vlan>>Tag-based Group**.

2. Add four VID groups. In this case, we can explanation it with Port 15, 16, 17, 18 and Trunk Port 23.



Tag-Based VLAN Memberships Configuration

IGMP-A: IGMP Aware P-VLAN: Private VLAN GVRP-P: GVRP Propagation

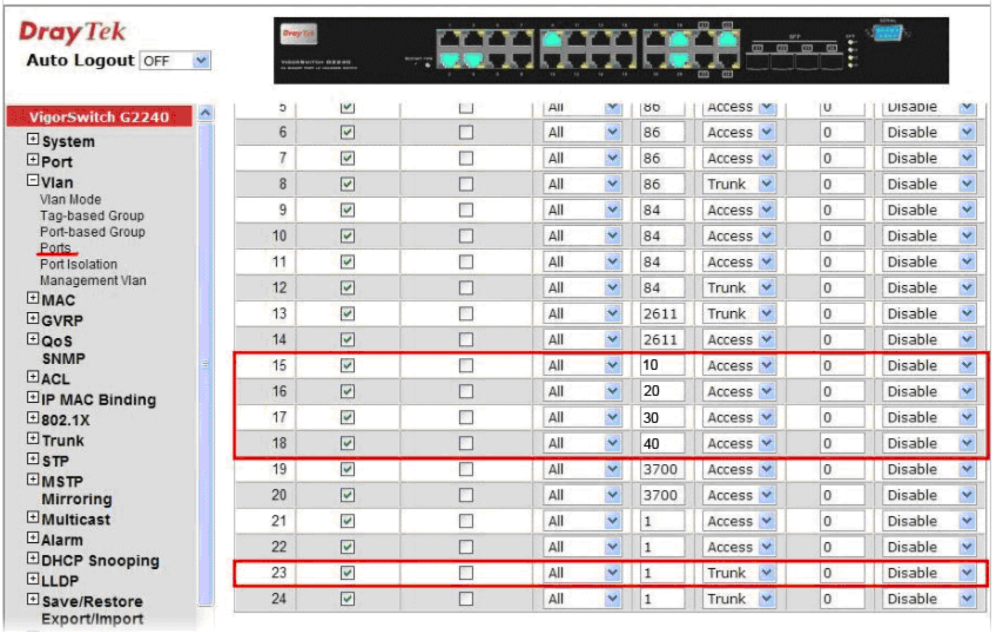
VLAN Name						Port Members																							
Name	Del	VID	IGMP-A	P-VLAN	GVRP-P	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Default		1	Disable	Disable	Disable	1																							24
3200-VID10	□	10	Disable	Disable	Disable															15								23	
3200-VID20	□	20	Disable	Disable	Disable																16							23	
3200-VID 30	□	30	Disable	Disable	Disable																	17						23	
3200-VID 40	□	40	Disable	Disable	Disable																		18					23	

VLAN Name 3200-VID10, Port Members = 15、23
VLAN Name 3200-VID20, Port Members = 16、23
VLAN Name 3200-VID30, Port Members = 17、23
VLAN Name 3200-VID40, Port Members = 18、23

3. Open **Vlan>> Ports** and set the VID value with role for each Port:

Port 15 VID = 10 Role = Access
Port 16 VID = 20 Role = Access
Port 17 VID = 30 Role = Access
Port 18 VID = 40 Role = Access
Port 23 VID = 1 Role = Trunk

Port 23 is set with Trunk in this example and will transfer the packets with VLAN Tag information. That is, packets with VID 10, 20, 30 and 40 will be transferred to Vigor3200 by Port 23 and VID information will be retained.

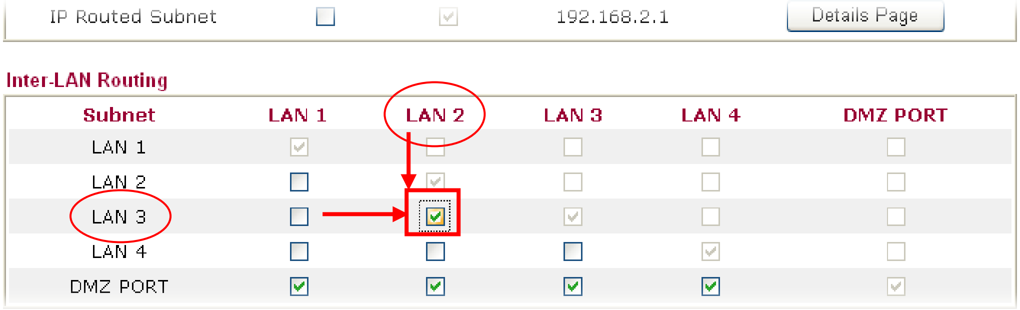


5	☑	□	All	86	Access	0	Disable
6	☑	□	All	86	Access	0	Disable
7	☑	□	All	86	Access	0	Disable
8	☑	□	All	86	Trunk	0	Disable
9	☑	□	All	84	Access	0	Disable
10	☑	□	All	84	Access	0	Disable
11	☑	□	All	84	Access	0	Disable
12	☑	□	All	84	Trunk	0	Disable
13	☑	□	All	2611	Trunk	0	Disable
14	☑	□	All	2611	Access	0	Disable
15	☑	□	All	10	Access	0	Disable
16	☑	□	All	20	Access	0	Disable
17	☑	□	All	30	Access	0	Disable
18	☑	□	All	40	Access	0	Disable
19	☑	□	All	3700	Access	0	Disable
20	☑	□	All	3700	Access	0	Disable
21	☑	□	All	1	Access	0	Disable
22	☑	□	All	1	Access	0	Disable
23	☑	□	All	1	Trunk	0	Disable
24	☑	□	All	1	Trunk	0	Disable

4. After finishing the above configuration, the equipment connecting to VigorSwitch Port 15, 16, 17 and 18 can get the corresponding IP address(es) of the network segment.

The equipment connecting to VigorSwitch Port 15 can get the IP address of 192.168.1.0/24
The equipment connecting to VigorSwitch Port 16 can get the IP address of 192.168.3.0/24
The equipment connecting to VigorSwitch Port 17 can get the IP address of 192.168.5.0/24
The equipment connecting to VigorSwitch Port 18 can get the IP address of 192.168.7.0/24

5. To make any two of VLAN groups of Tag Based VLAN linked with each other, just check the boxes of the ones in the field of **Inter-LAN Routing** in the page of **LAN** >> **General Setup**. Refer to the following figure. LAN2 and LAN3 are linked.



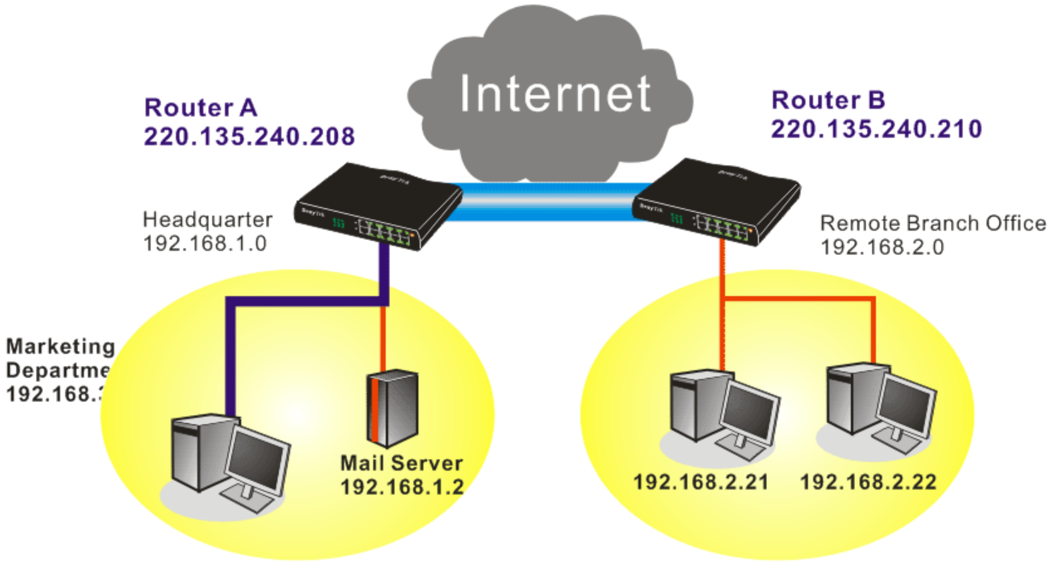
IP Routed Subnet	□	☑	192.168.2.1	Details Page

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1	☑	□	□	□	□
LAN 2	□	☑	□	□	□
LAN 3	□	☑	☑	□	□
LAN 4	□	□	□	☑	□
DMZ PORT	☑	☑	☑	☑	☑

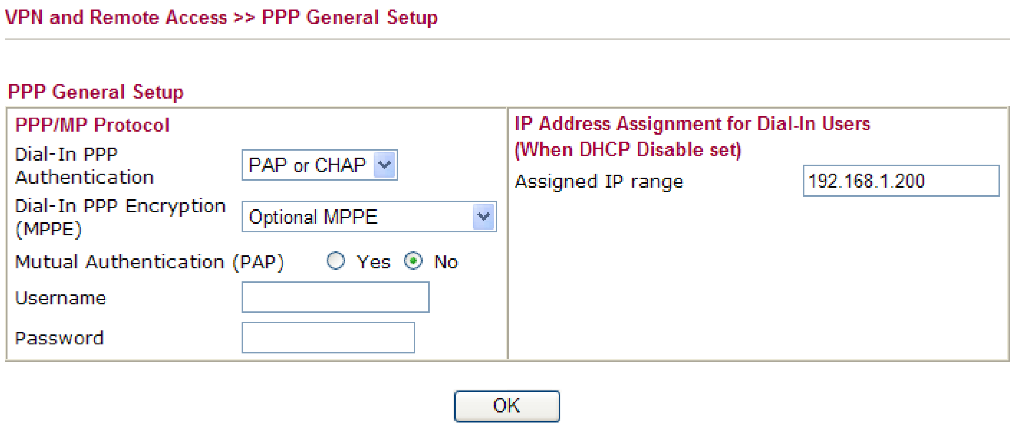
5.2 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



Settings in Router A in headquarter:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then,
   For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Dial-In PPP Encryption (MPPE): Optional MPPE

Mutual Authentication (PAP): ○ Yes ● No

Username:

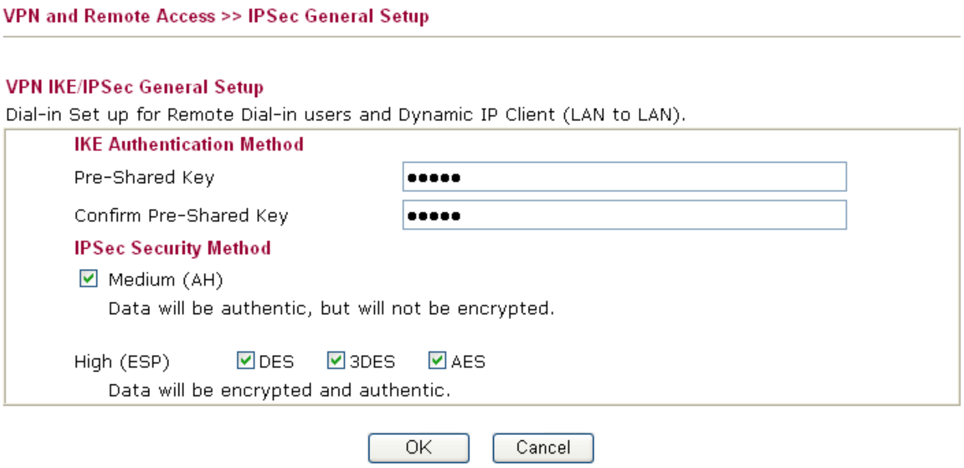
Password:

IP Address Assignment for Dial-In Users (When DHCP Disable set)

Assigned IP range: 192.168.1.200

OK

For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.


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

Pre-Shared Key: ●●●●●

Confirm Pre-Shared Key: ●●●●●

IPSec Security Method

☑ Medium (AH)

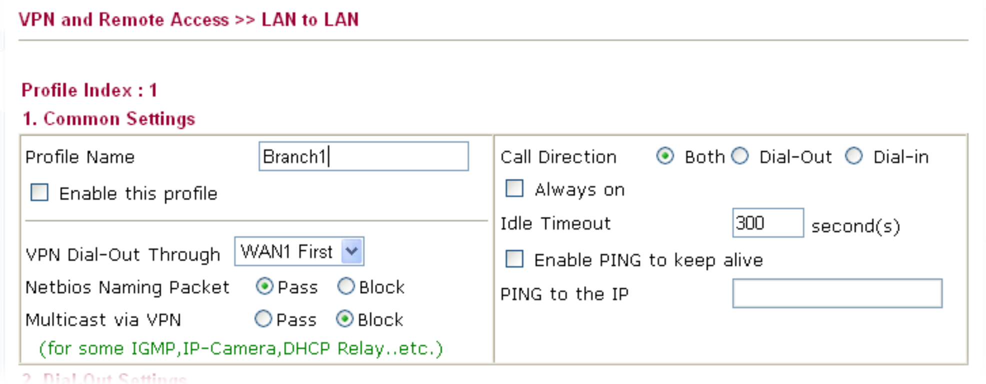
Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.

4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.


VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: Branch1

□ Enable this profile

VPN Dial-Out Through: WAN1 First

Netbios Naming Packet ● Pass ○ Block

Multicast via VPN ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction ● Both ○ Dial-Out ○ Dial-in

□ Always on

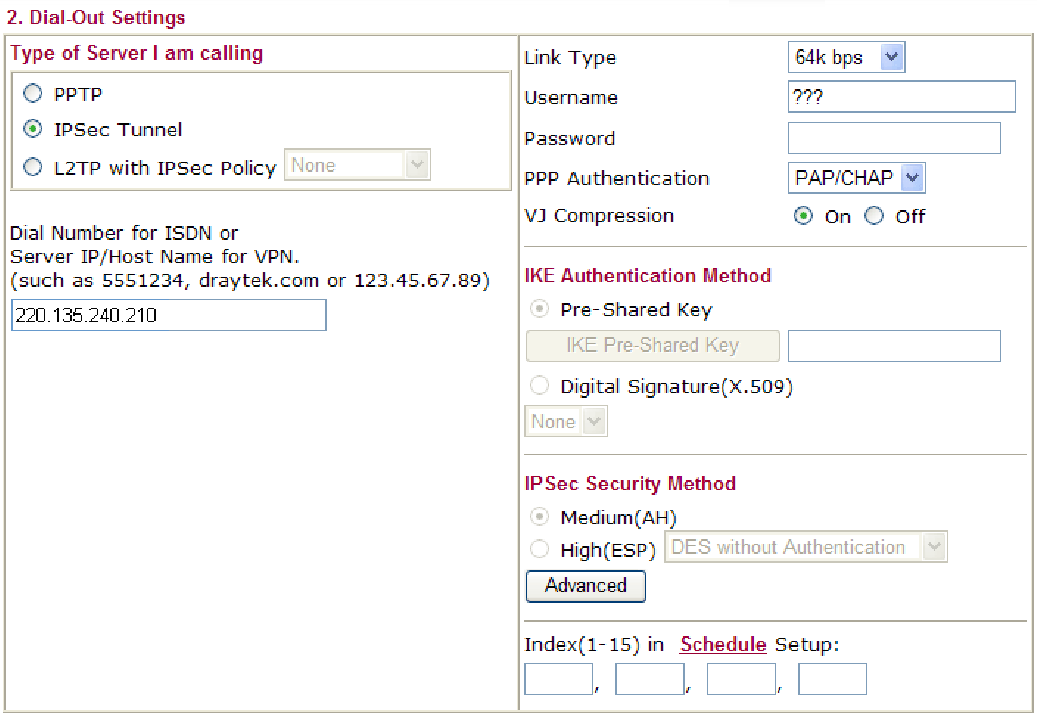
Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.



2. Dial-Out Settings

Type of Server I am calling

○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy None

Dial Number for ISDN or
Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)
220.135.240.210

Link Type	64k bps
Username	???
Password	
PPP Authentication	PAP/CHAP
VJ Compression	● On ○ Off

IKE Authentication Method

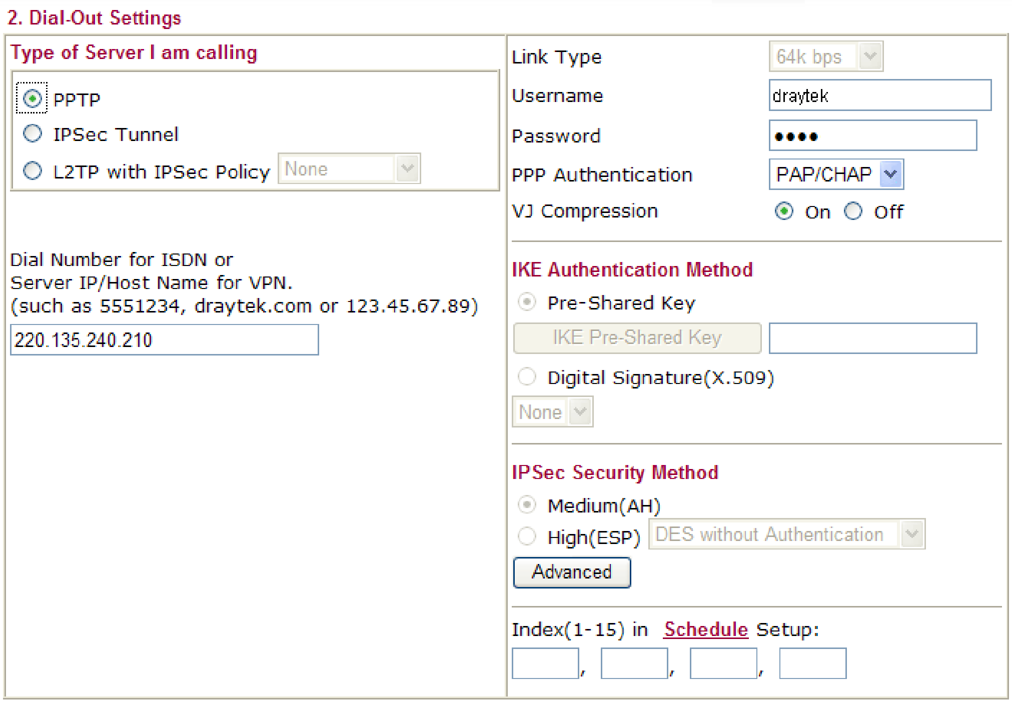
● Pre-Shared Key
IKE Pre-Shared Key
○ Digital Signature(X.509)
None

IPSec Security Method

● Medium(AH)
○ High(ESP) DES without Authentication
Advanced

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

If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.



2. Dial-Out Settings

Type of Server I am calling

● PPTP
○ IPSec Tunnel
○ L2TP with IPSec Policy None

Dial Number for ISDN or
Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)
220.135.240.210

Link Type	64k bps
Username	draytek
Password	••••
PPP Authentication	PAP/CHAP
VJ Compression	● On ○ Off

IKE Authentication Method

● Pre-Shared Key
IKE Pre-Shared Key
○ Digital Signature(X.509)
None

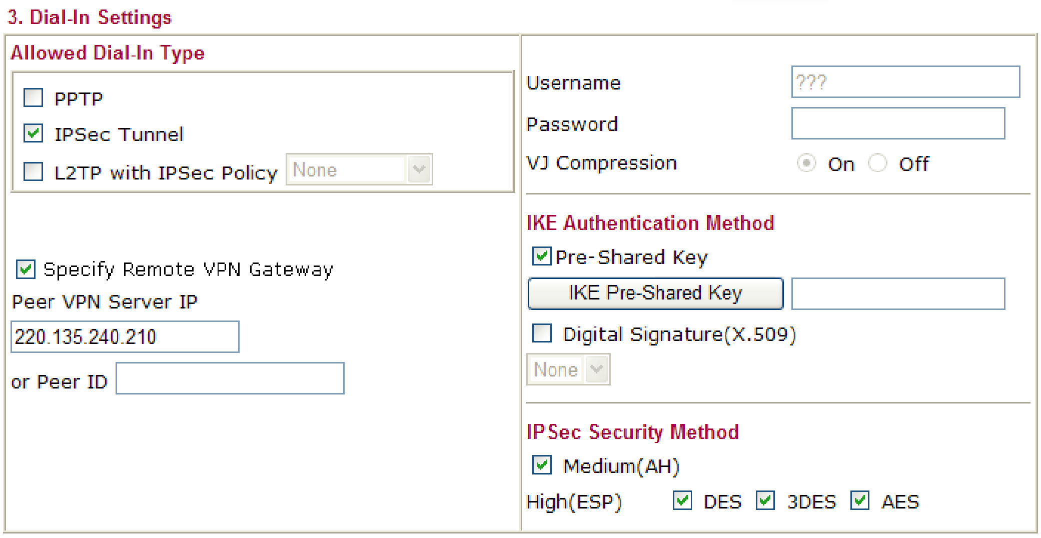
IPSec Security Method

● Medium(AH)
○ High(ESP) DES without Authentication
Advanced

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

6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



3. Dial-In Settings

Allowed Dial-In Type

□ PPTP

☑ IPSec Tunnel

□ L2TP with IPSec Policy None

☑ Specify Remote VPN Gateway

Peer VPN Server IP 220.135.240.210

or Peer ID

Username ???

Password

VJ Compression ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

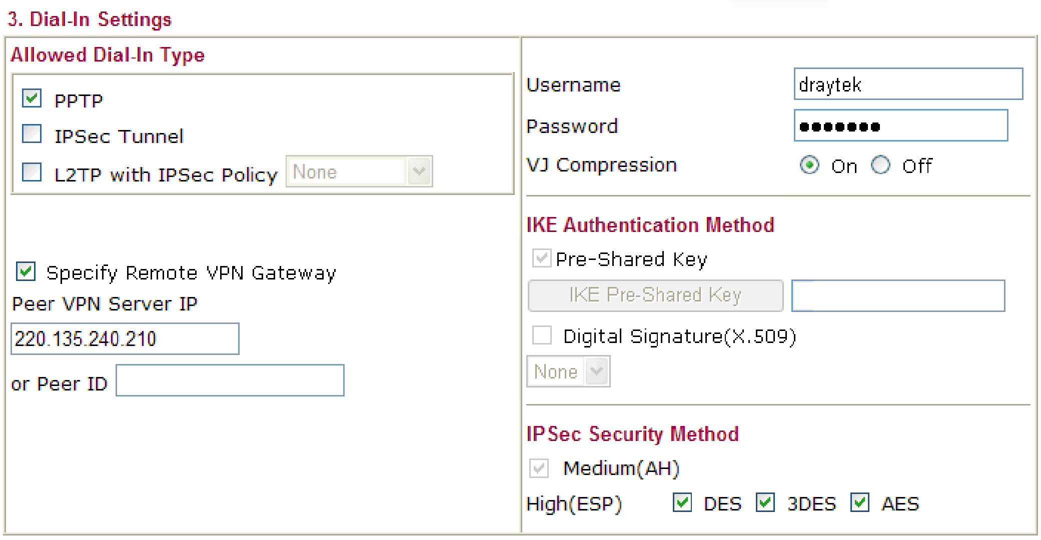
None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

□ IPSec Tunnel

□ L2TP with IPSec Policy None

☑ Specify Remote VPN Gateway

Peer VPN Server IP 220.135.240.210

or Peer ID

Username draytek

Password •••••••

VJ Compression ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

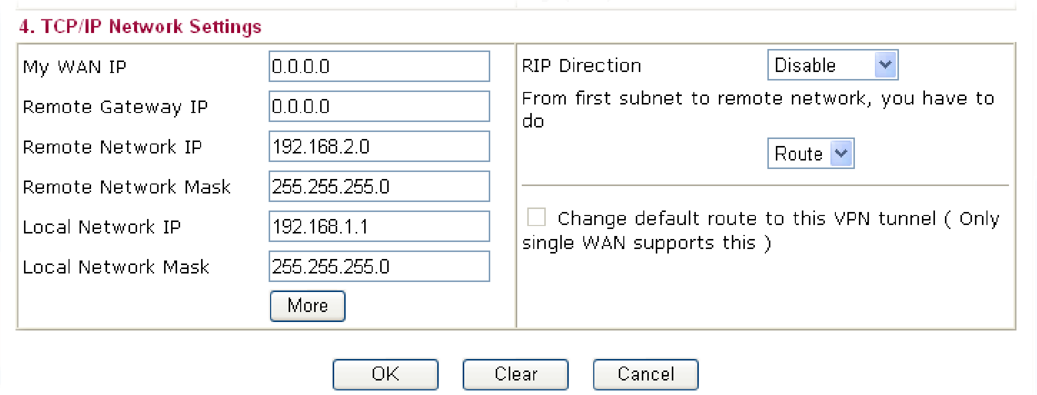
None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.



4. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.2.0
Remote Network Mask	255.255.255.0
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0

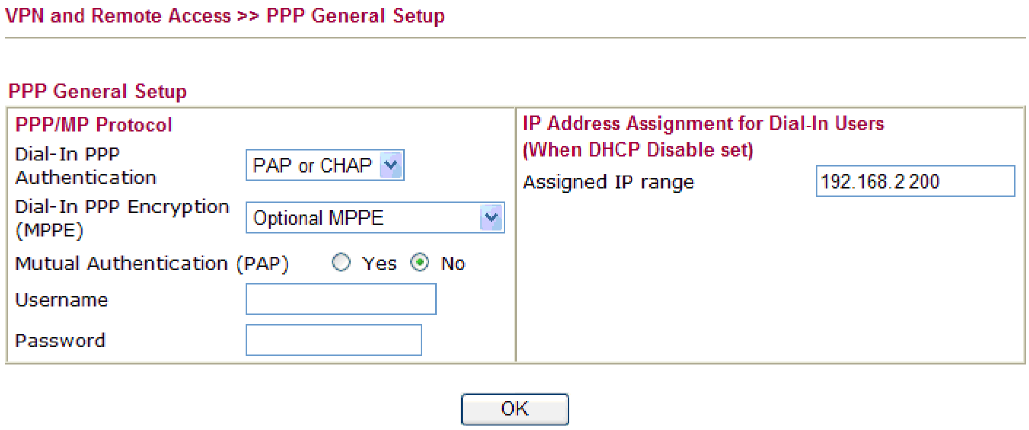
RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

Settings in Router B in the remote office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



VPN and Remote Access >> PPP General Setup

PPP General Setup

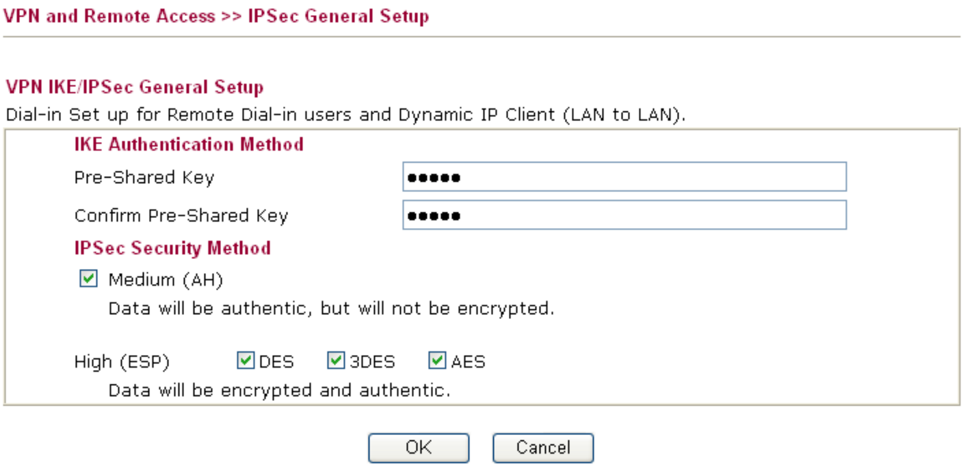
PPP/MP Protocol

Dial-In PPP Authentication	PAP or CHAP
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 range: 192.168.2.200

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



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

Pre-Shared Key ●●●●●

Confirm Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

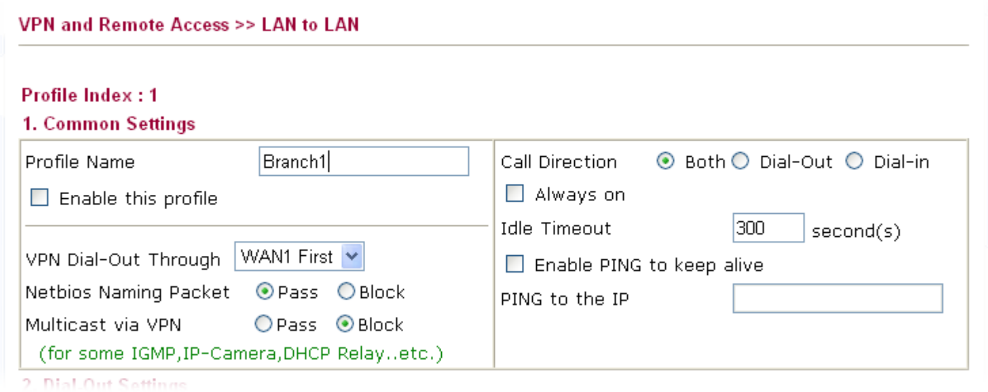
Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

OK Cancel

3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

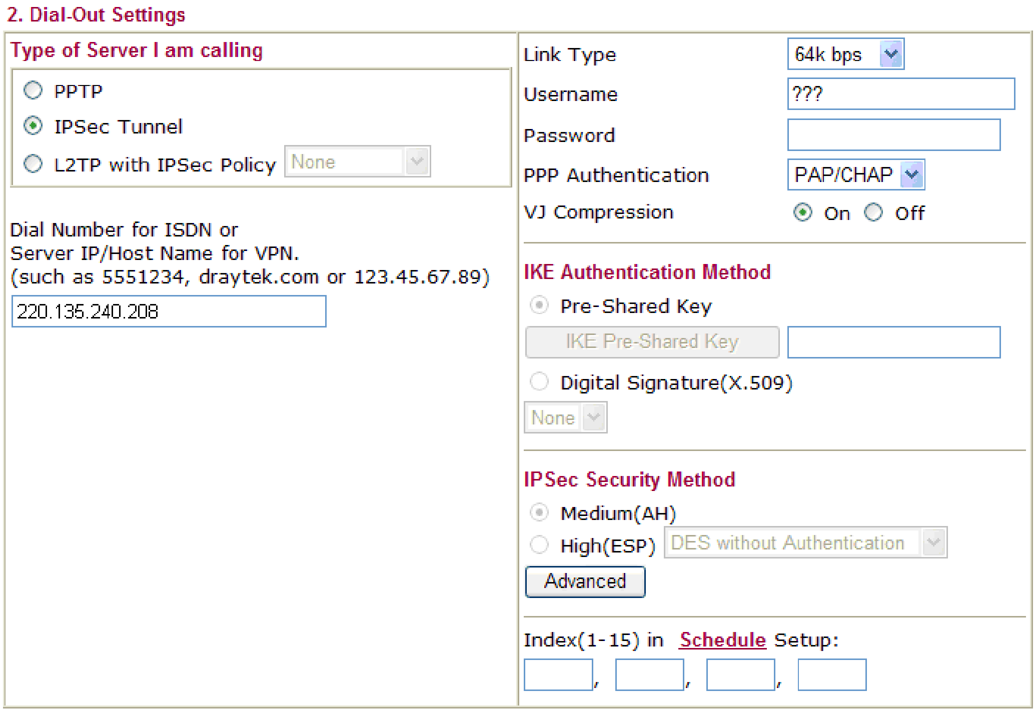
1. Common Settings

Profile Name Branch1 □ Enable this profile	Call Direction ● Both ○ Dial-Out ○ Dial-in □ Always on Idle Timeout 300 second(s) □ Enable PING to keep alive PING to the IP
VPN Dial-Out Through WAN1 First Netbios Naming Packet ● Pass ○ Block Multicast via VPN ○ Pass ● Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

2. Dial-Out Settings

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

   If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.



2. Dial-Out Settings

Type of Server I am calling

○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy [None]

Dial Number for ISDN or
Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)
220.135.240.208

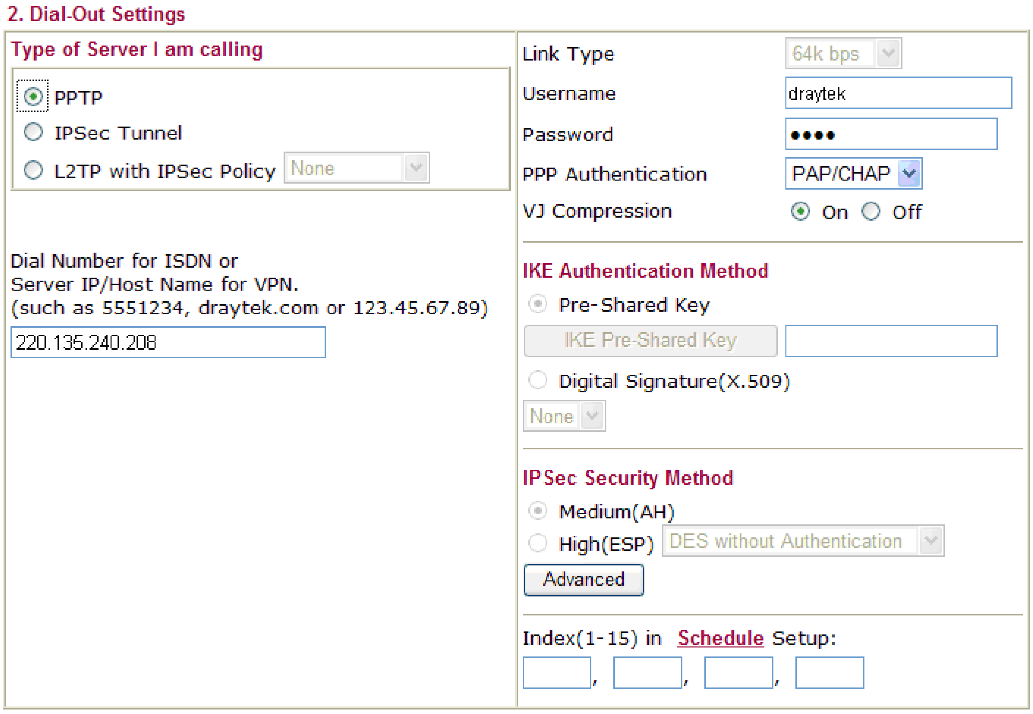
Link Type: 64k bps
Username: ???
Password:
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key:
○ Digital Signature(X.509)
None

IPSec Security Method
● Medium(AH)
○ High(ESP) DES without Authentication

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

If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.



2. Dial-Out Settings

Type of Server I am calling

● PPTP
○ IPSec Tunnel
○ L2TP with IPSec Policy [None]

Dial Number for ISDN or
Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)
220.135.240.208

Link Type: 64k bps
Username: draytek
Password: ••••
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

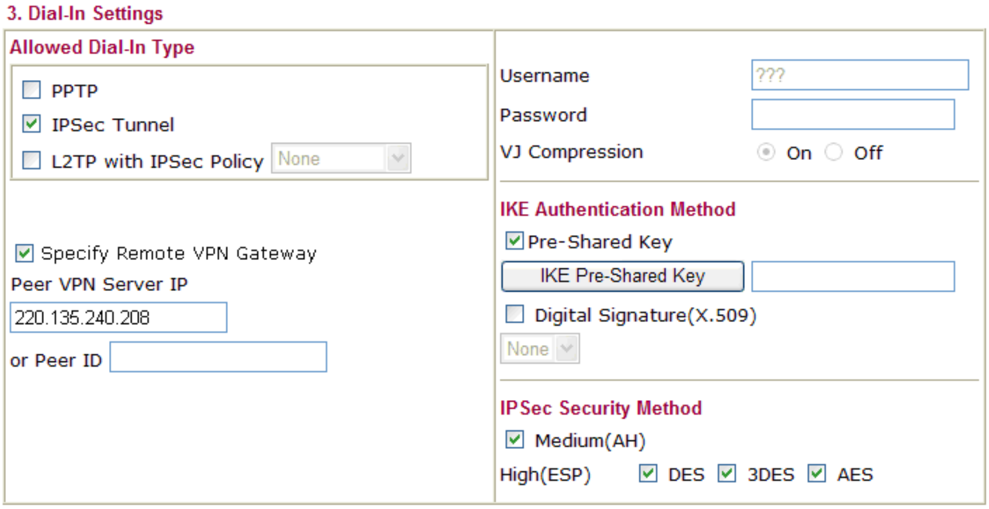
IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key:
○ Digital Signature(X.509)
None

IPSec Security Method
● Medium(AH)
○ High(ESP) DES without Authentication

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

6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



3. Dial-In Settings

Allowed Dial-In Type

☐ PPTP
☑ IPSec Tunnel
☐ L2TP with IPSec Policy: None

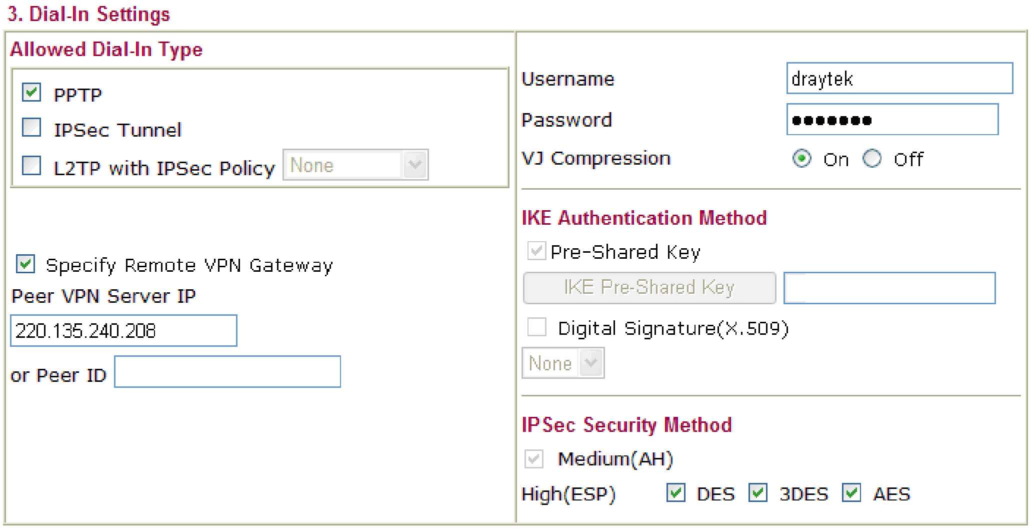
☑ Specify Remote VPN Gateway
Peer VPN Server IP: 220.135.240.208
or Peer ID:

Username: ???
Password:
VJ Compression: ● On ○ Off

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

If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP
☐ IPSec Tunnel
☐ L2TP with IPSec Policy: None

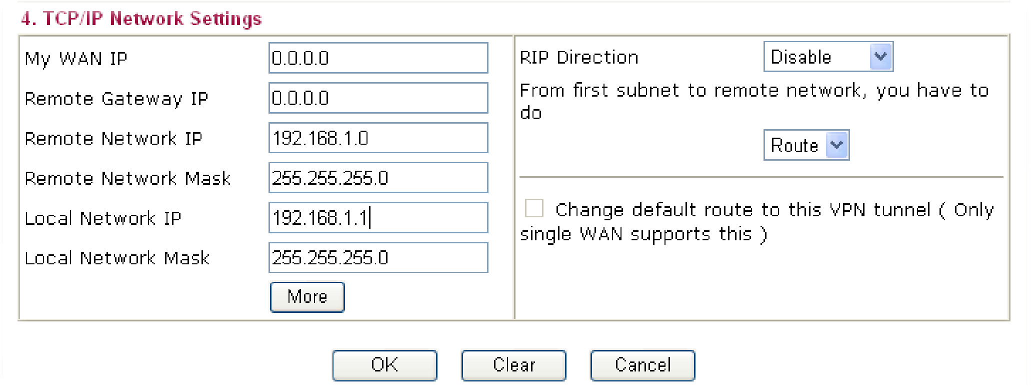
☑ Specify Remote VPN Gateway
Peer VPN Server IP: 220.135.240.208
or Peer ID:

Username: draytek
Password: ●●●●●●●
VJ Compression: ● On ○ Off

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

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.



4. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.1.0
Remote Network Mask	255.255.255.0
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0

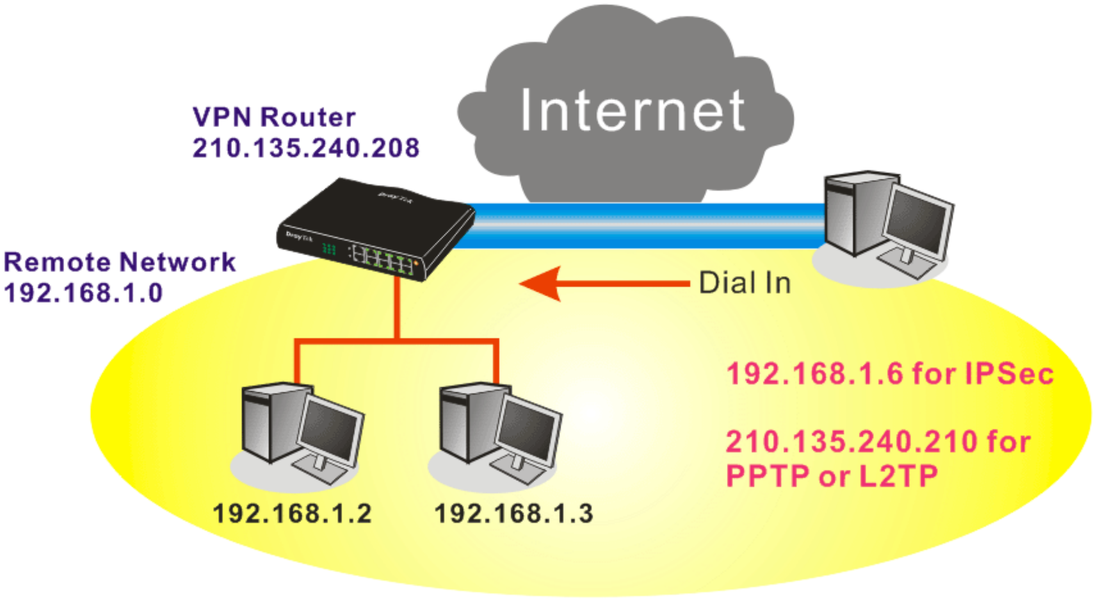
RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

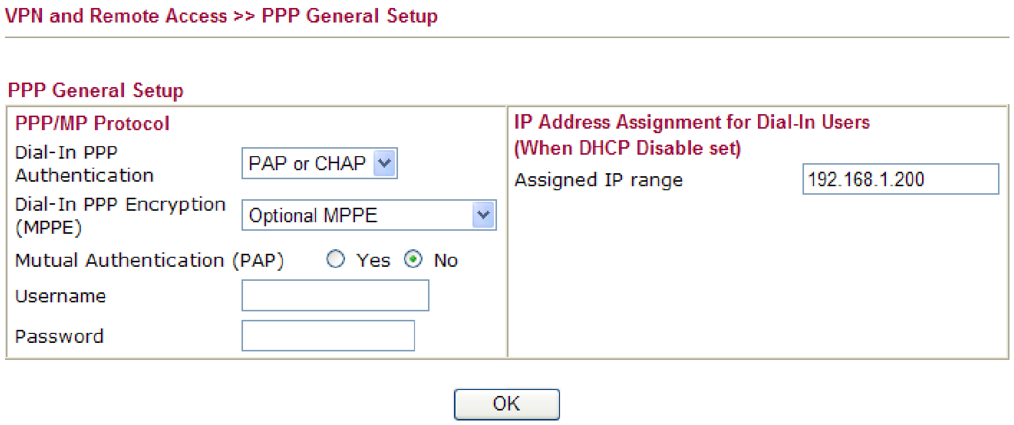
5.3 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

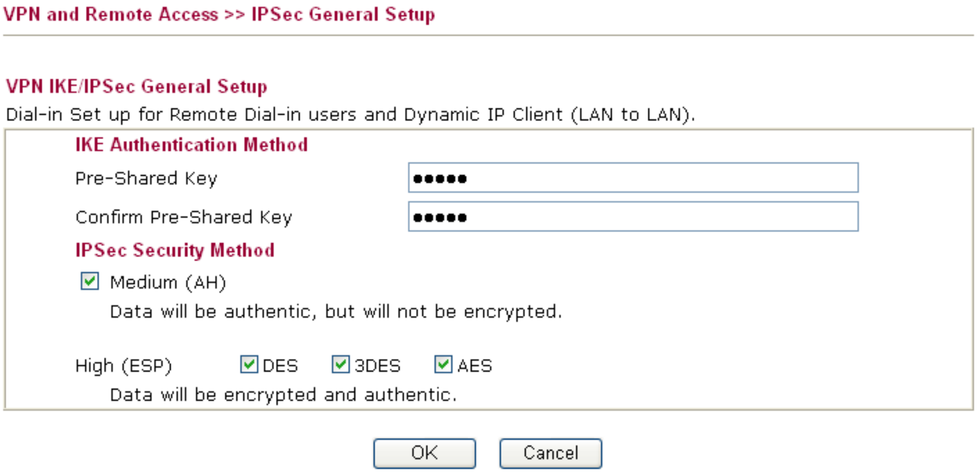


VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Dial-In PPP Authentication	PAP or CHAP	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	○ Yes ● No		
Username			
Password			

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.



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

Pre-Shared Key ●●●●●

Confirm Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

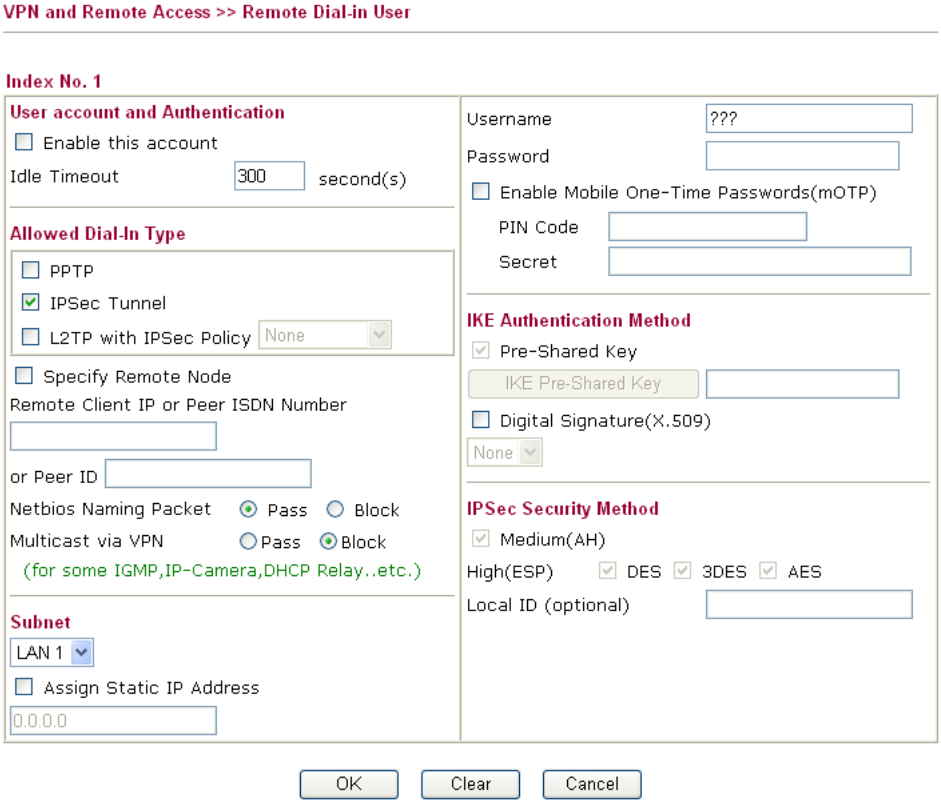
High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.

4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



VPN and Remote Access >> 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

□ Specify Remote Node

Remote Client IP or Peer ISDN Number

or Peer ID

Netbios Naming Packet ● Pass ○ Block

Multicast via VPN ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Subnet

LAN 1

□ Assign Static IP Address

0.0.0.0

Username ???

Password

□ Enable Mobile One-Time Passwords(mOTP)

PIN Code

Secret

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

None

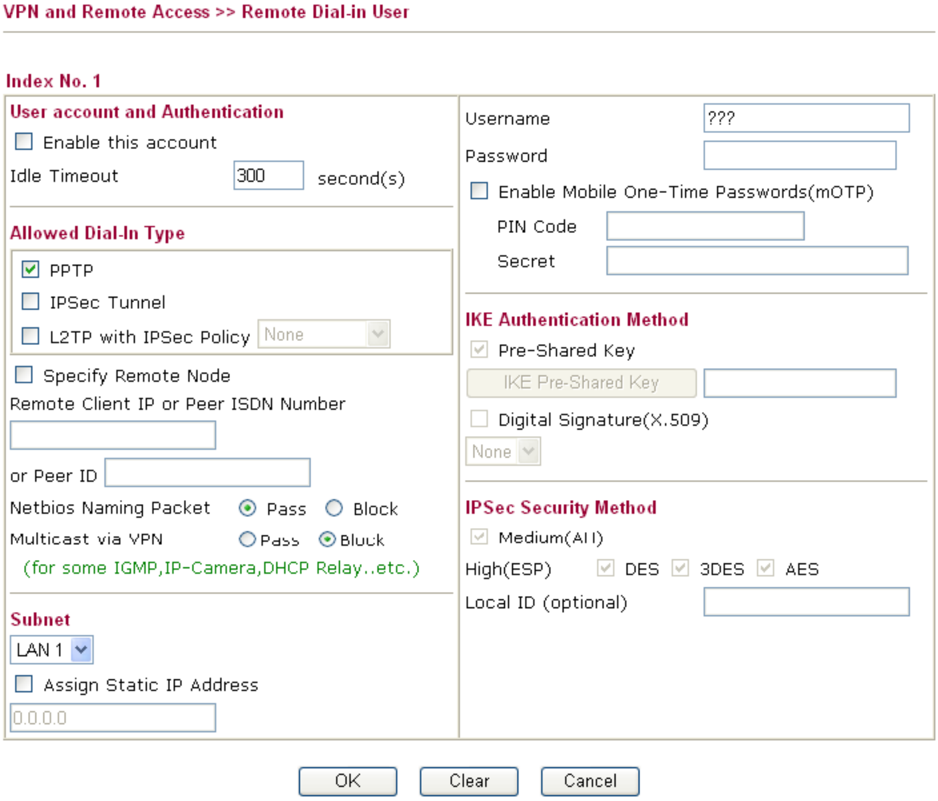
IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



VPN and Remote Access >> 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

□ Specify Remote Node

Remote Client IP or Peer ISDN Number

or Peer ID

Netbios Naming Packet ● Pass ○ Block

Multicast via VPN ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Subnet

LAN 1

□ Assign Static IP Address

0.0.0.0

Username ???

Password

□ 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)

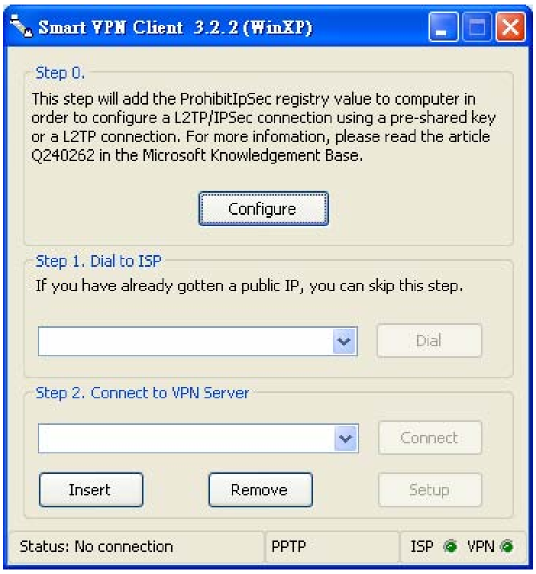
High(ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

Settings in the remote host:

1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or “Smart VPN Client”, complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.DrayTek.com download center. Install as instructed.

2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.



Smart VPN Client 3.2.2 (WinXP)

Step 0.

This step will add the ProhibitIpSec registry value to computer in order to configure a L2TP/IPSec connection using a pre-shared key or a L2TP connection. For more infomation, please read the article Q240262 in the Microsoft Knowledgement Base.

Step 1. Dial to ISP

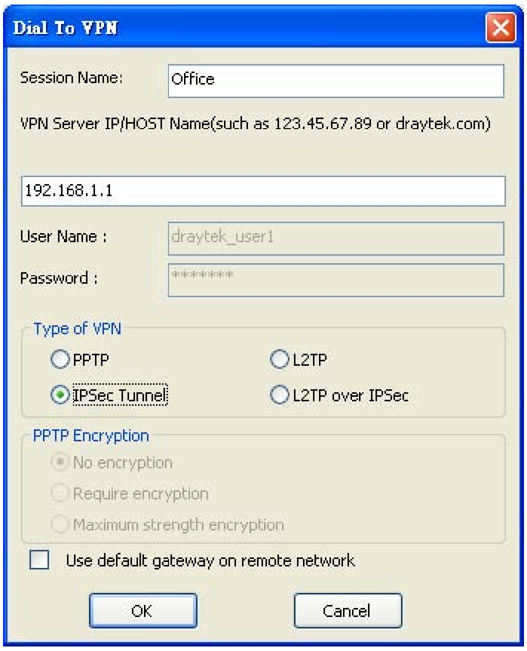
If you have already gotten a public IP, you can skip this step.

Step 2. Connect to VPN Server

Status: No connection | PPTP | ISP ● VPN ●

3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

If an IPSec-based service is selected as shown below,



Dial To VPN

Session Name: Office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : *******

Type of VPN

○ PPTP ○ L2TP

● IPSec Tunnel ○ L2TP over IPSec

PPTP Encryption

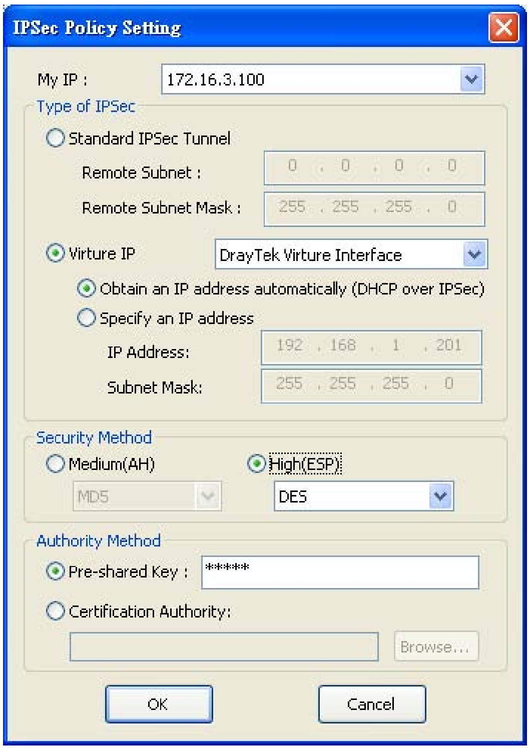
● No encryption

○ Require encryption

○ Maximum strength encryption

□ Use default gateway on remote network

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.



IPSec Policy Setting

My IP : 172.16.3.100

Type of IPSec

○ Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

● Virture IP: DrayTek Virture Interface

● Obtain an IP address automatically (DHCP over IPSec)

○ Specify an IP address

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

○ Medium(AH): MD5

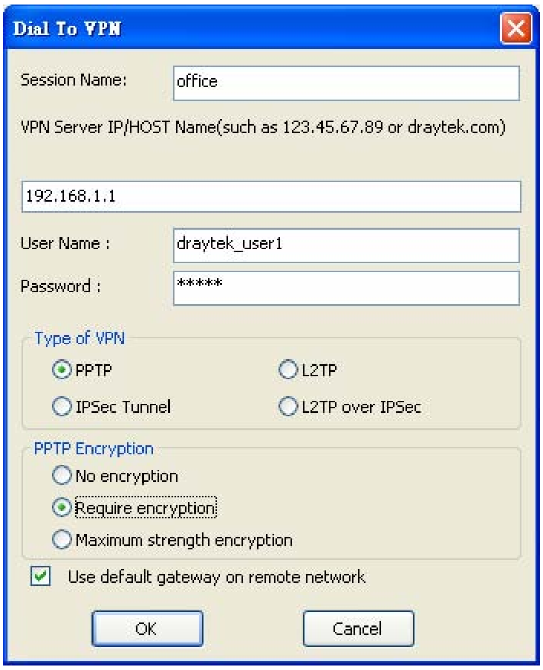
● High(ESP): DES

Authority Method

● Pre-shared Key : ******

○ Certification Authority:

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.



Dial To VPN

Session Name: office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : *****

Type of VPN

● PPTP ○ L2TP

○ IPSec Tunnel ○ L2TP over IPSec

PPTP Encryption

○ No encryption

● Require encryption

○ Maximum strength encryption

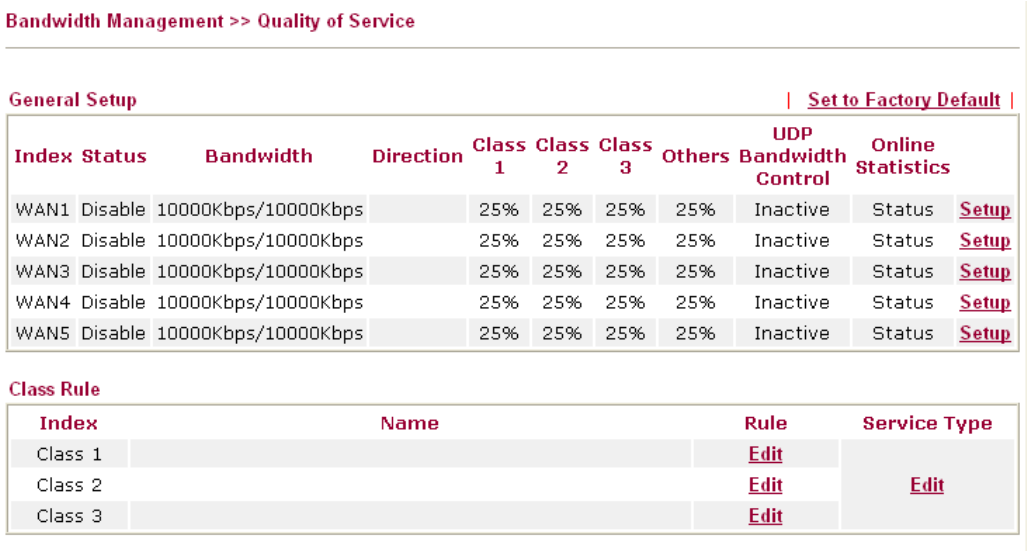
☑ Use default gateway on remote network

4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

5.4 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in other room.

1. Go to **Bandwidth Management>>Quality of Service.**



Bandwidth Management >> Quality of Service

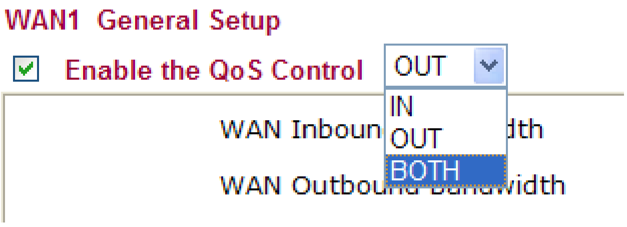
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

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

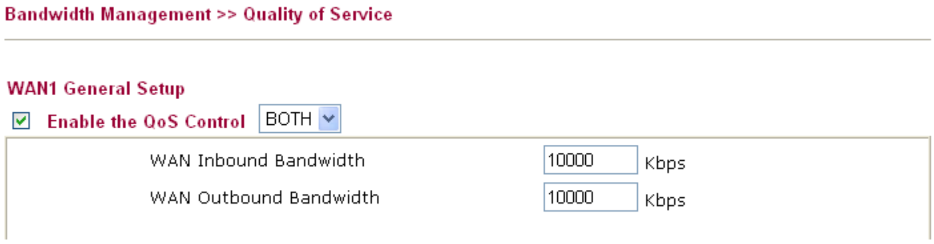
2. Click **Setup** link of WAN. Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.



WAN1 General Setup

☑ Enable the QoS Control OUT

3. Set Inbound/Outbound bandwidth.



Bandwidth Management >> Quality of Service

WAN1 General Setup

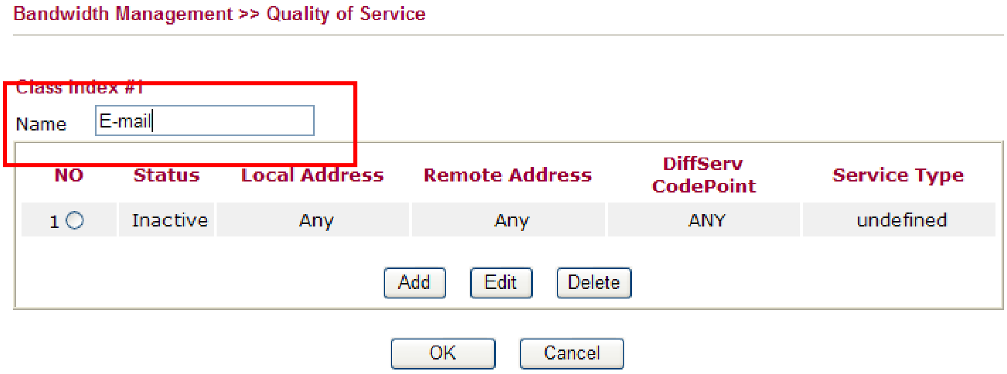
☑ Enable the QoS Control BOTH

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

> **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.

4. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1.



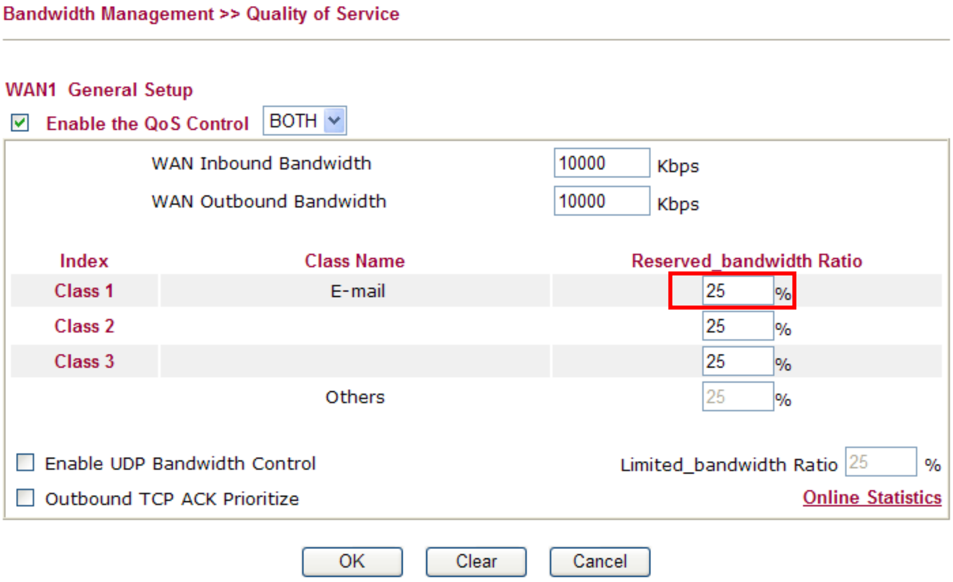
Bandwidth Management >> Quality of Service

Class Index #1

Name: E-mail

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Inactive	Any	Any	ANY	undefined

5. For this index, the user will set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP.



Bandwidth Management >> Quality of Service

WAN1 General Setup

☑ Enable the QoS Control: BOTH

WAN Inbound Bandwidth: 10000 Kbps

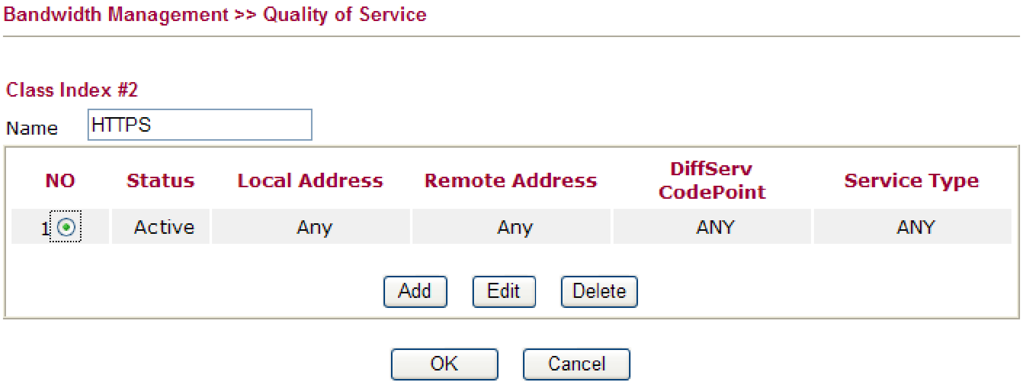
WAN Outbound Bandwidth: 10000 Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %

□ Enable UDP Bandwidth Control — Limited_bandwidth Ratio: 25 %

□ Outbound TCP ACK Prioritize

6. Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth for **HTTPS**. And click **OK**.



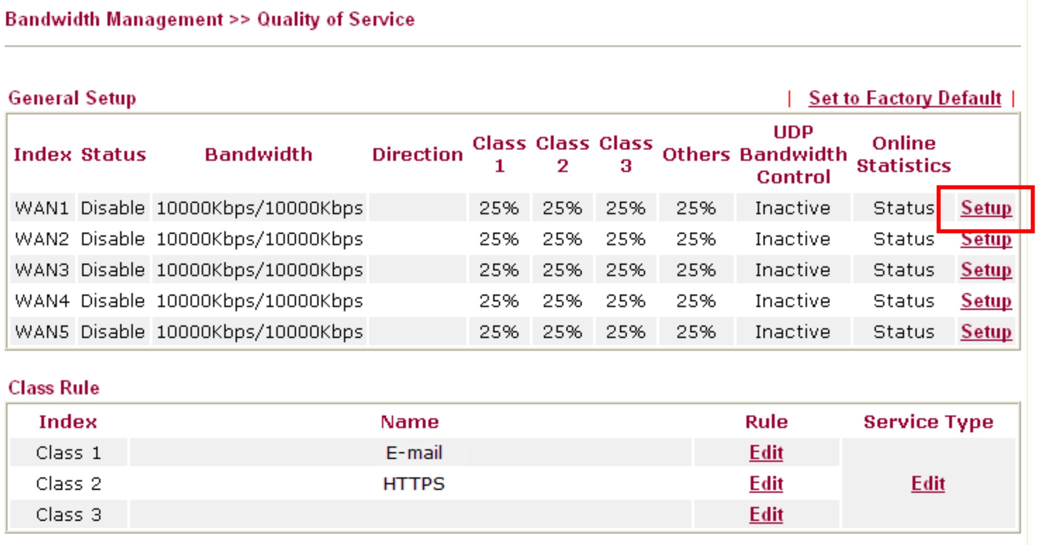
Bandwidth Management >> Quality of Service

Class Index #2

Name: HTTPS

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ●	Active	Any	Any	ANY	ANY

7. Click **Setup** link for one of the WAN interface.



Bandwidth Management >> Quality of Service

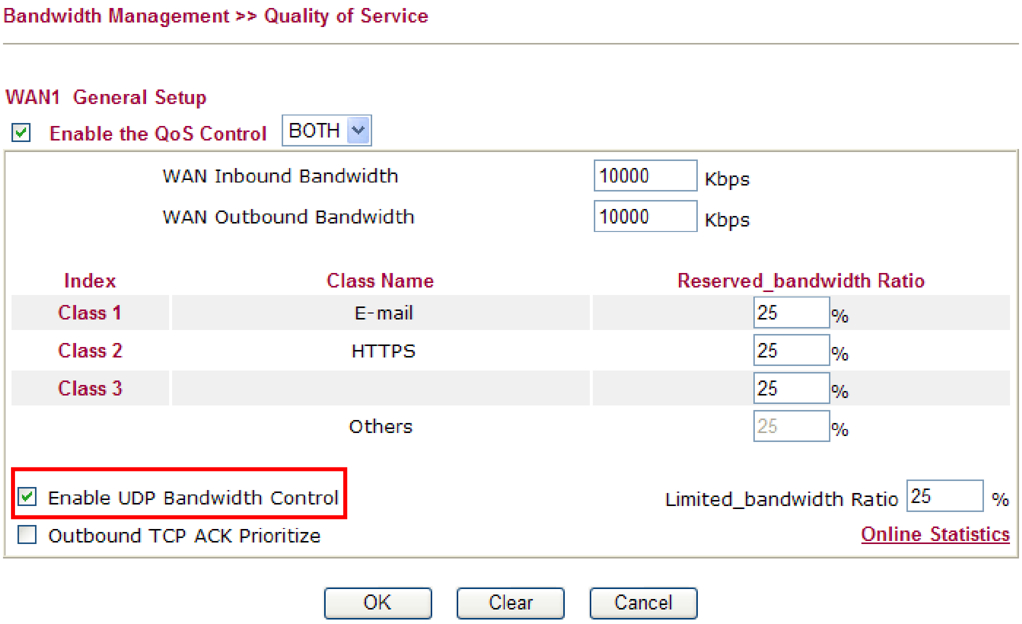
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	E-mail	Edit	Edit
Class 2	HTTPS	Edit	
Class 3		Edit	

8. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of influent other application. Click **OK**.



Bandwidth Management >> Quality of Service

WAN1 General Setup

☑ Enable the QoS Control BOTH

WAN Inbound Bandwidth 10000 Kbps

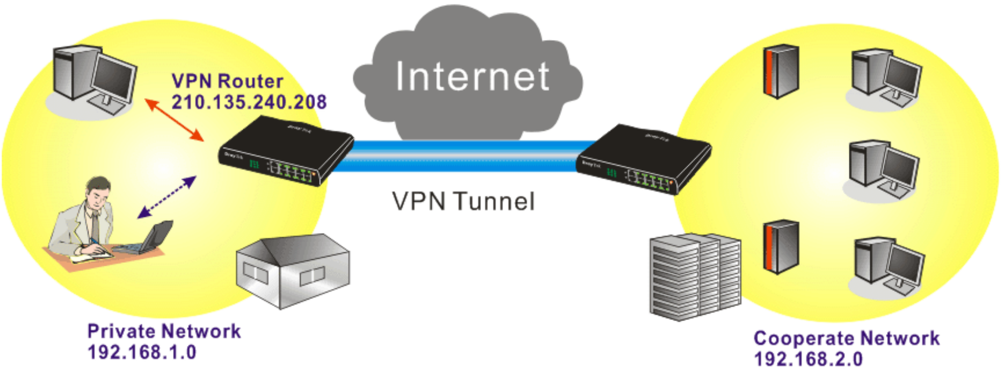
WAN Outbound Bandwidth 10000 Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %

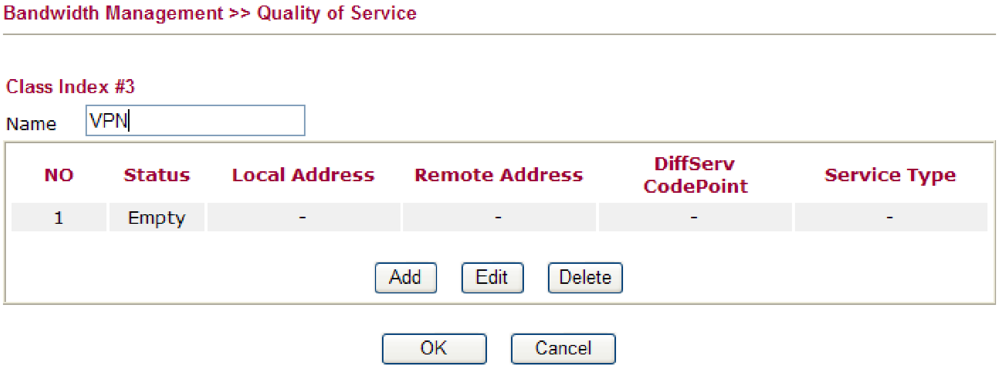
☑ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

□ Outbound TCP ACK Prioritize Online Statistics

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



10. Click **Edit** to open a new window.



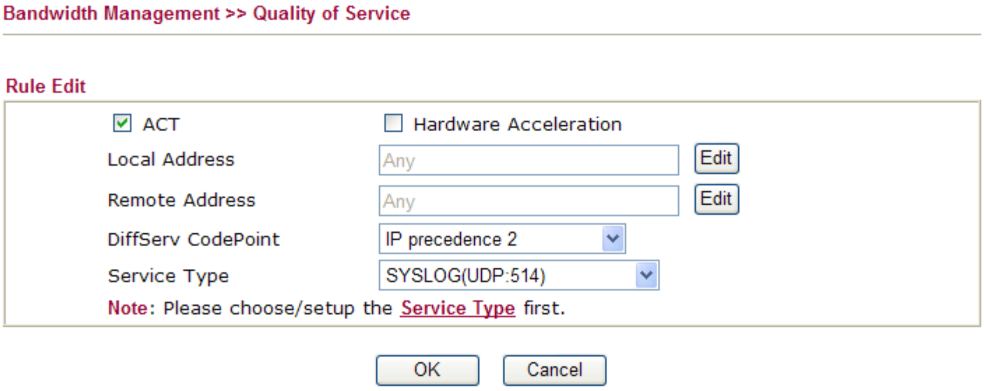
Bandwidth Management >> Quality of Service

Class Index #3

Name VPN

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

11. Click **Edit** to open the following window. Check the **ACT** box, first.



Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT ☐ Hardware Acceleration

Local Address: Any

Remote Address: Any

DiffServ CodePoint: IP precedence 2

Service Type: SYSLOG(UDP:514)

Note: Please choose/setup the Service Type first.

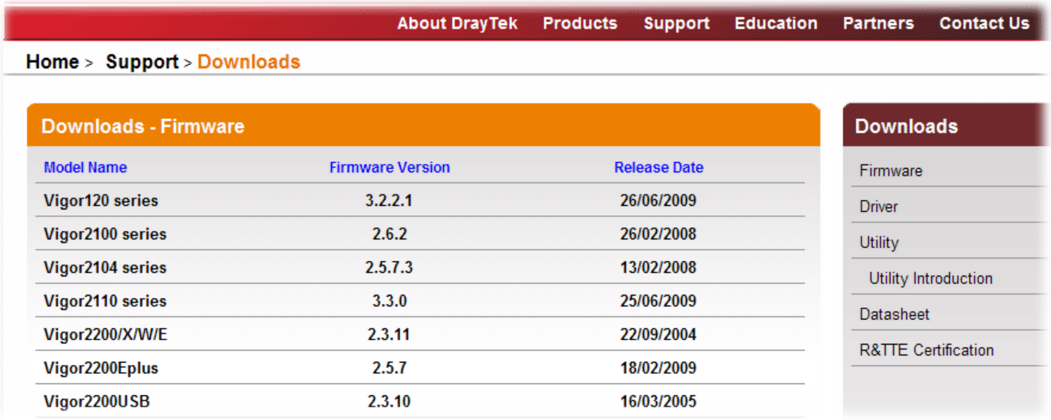
12. Then click **Edit** of **Local Address** to set a worker’s subnet address. Click **Edit** of **Remote Address** to set headquarter’s IP address. Leave other fields and click **OK**.

5.5 Upgrade Firmware for Your Router

Using Firmware Upgrade Utility

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

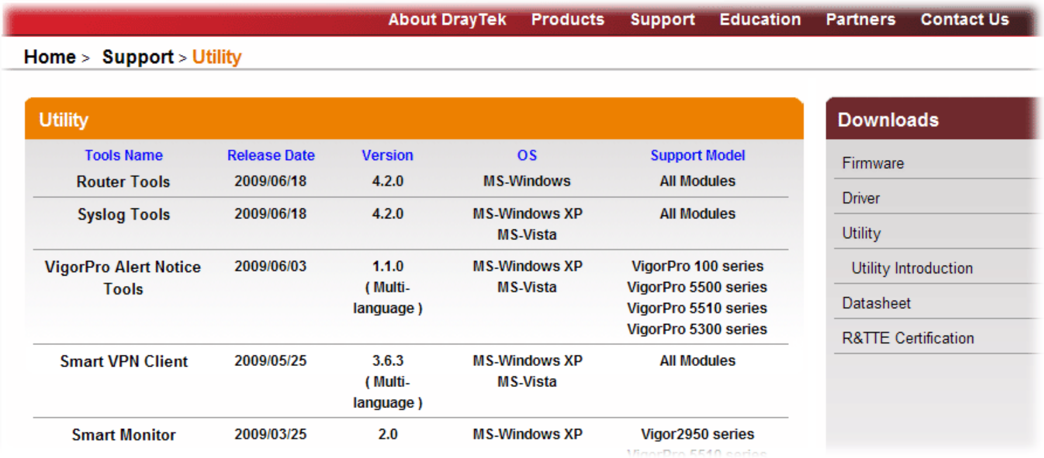
1. Go to **www.DrayTek.com**.
2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.



Downloads - Firmware

Model Name	Firmware Version	Release Date
Vigor120 series	3.2.2.1	26/06/2009
Vigor2100 series	2.6.2	26/02/2008
Vigor2104 series	2.5.7.3	13/02/2008
Vigor2110 series	3.3.0	25/06/2009
Vigor2200/X/W/E	2.3.11	22/09/2004
Vigor2200Eplus	2.5.7	18/02/2009
Vigor2200USB	2.3.10	16/03/2005

3. Access into **Support** >> **Downloads**. Please find out **Utility** menu and click it.



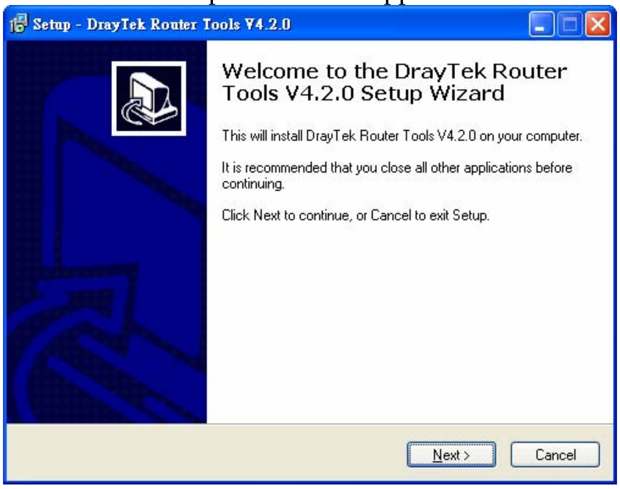
Utility

Tools Name	Release Date	Version	OS	Support Model
Router Tools	2009/06/18	4.2.0	MS-Windows	All Modules
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP MS-Vista	All Modules
VigorPro Alert Notice Tools	2009/06/03	1.1.0 (Multi-language)	MS-Windows XP MS-Vista	VigorPro 100 series VigorPro 5500 series VigorPro 5510 series VigorPro 5300 series
Smart VPN Client	2009/05/25	3.6.3 (Multi-language)	MS-Windows XP MS-Vista	All Modules
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 series

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the icon of router tool. The setup wizard will appear.

RTSv420
DrayTek Router Tools V4.2.0 Setup
DrayTek corp.



Setup - DrayTek Router Tools V4.2.0

Welcome to the DrayTek Router Tools V4.2.0 Setup Wizard

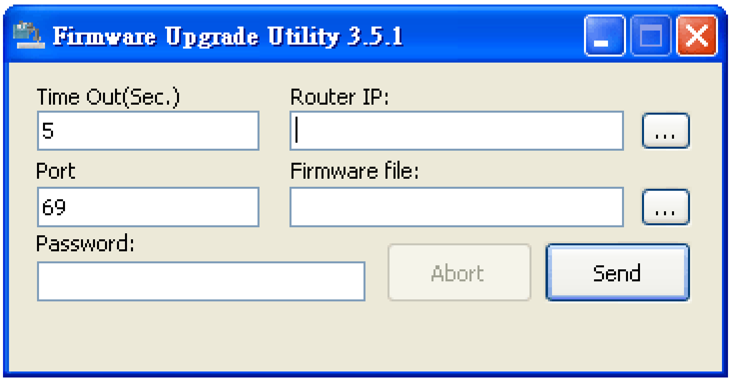
This will install DrayTek Router Tools V4.2.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.

7. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.



Firmware Upgrade Utility 3.5.1

Time Out(Sec.): 5

Router IP:

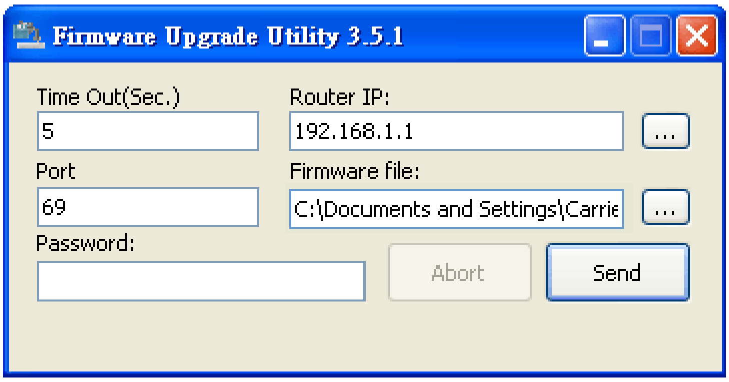
Port: 69

Firmware file:

Password:

8. Type in your router IP, usually **192.168.1.1**.

9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.



Firmware Upgrade Utility 3.5.1

Time Out(Sec.): 5

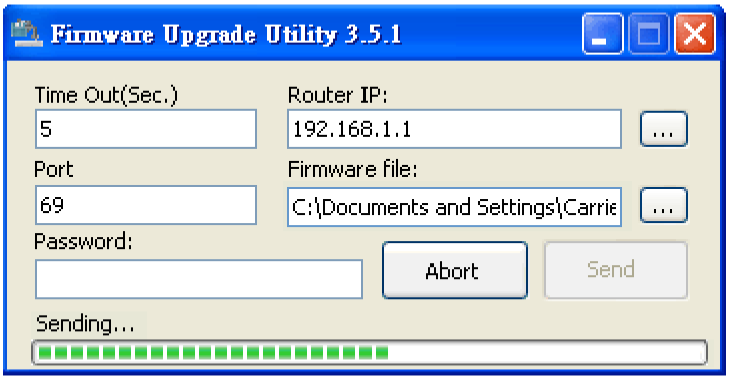
Router IP: 192.168.1.1

Port: 69

Firmware file: C:\Documents and Settings\Carrie

Password:

10. Click **Send**.


Firmware Upgrade Utility 3.5.1

Time Out(Sec.): 5

Port: 69

Password:

Router IP: 192.168.1.1

Firmware file: C:\Documents and Settings\Carrie

Sending...

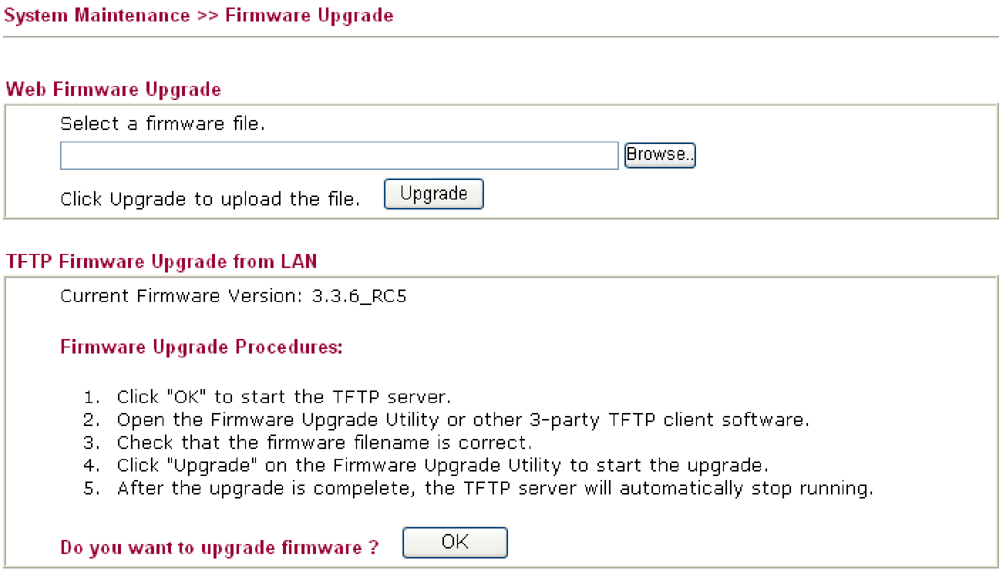
11. Now the firmware update is finished.

Using Web Page

The web page also can guide you to upgrade firmware. Note that this example is running over Windows OS (Operating System).

1. 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.

2. Click **System Maintenance>> Firmware Upgrade**.


System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.3.6_RC5

Firmware Upgrade Procedures:

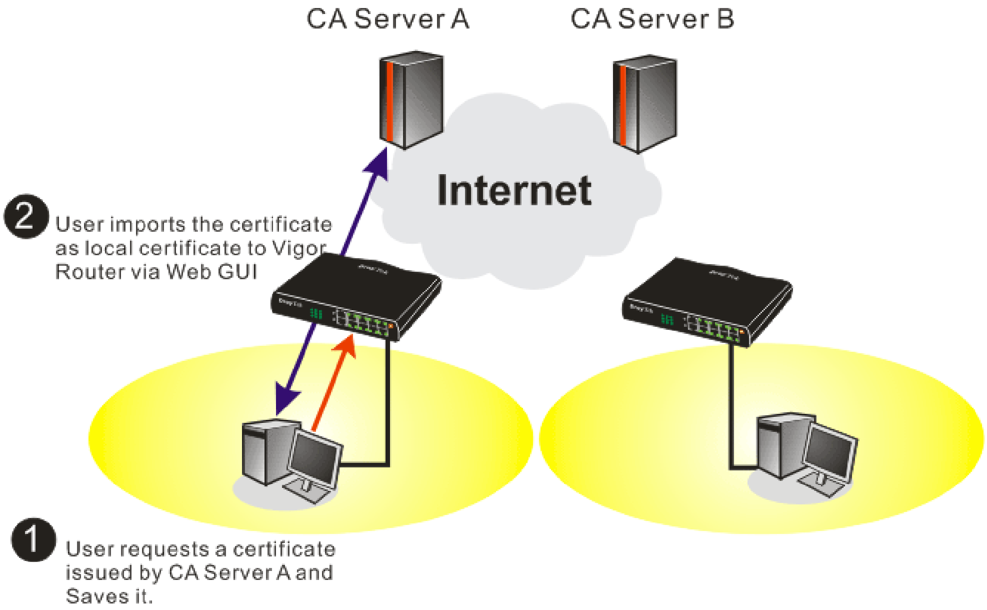
1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is compelete, the TFTP server will automatically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

Do you want to upgrade firmware ?

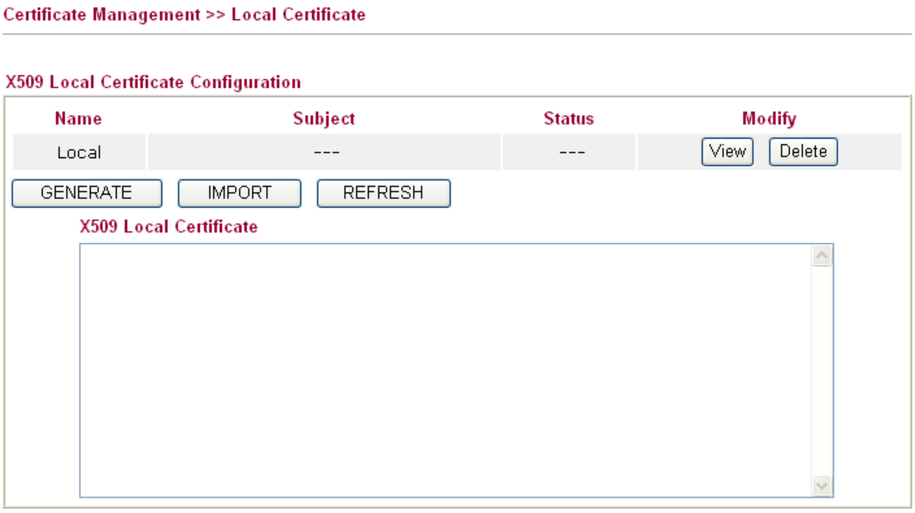
3. Select a firmware file by clicking **Browse**.

Click **Upgrade** to perform the firmware upgrade.

5.6 Request a certificate from a CA server on Windows CA Server


CA Server A
CA Server B
Internet
2 User imports the certificate as local certificate to Vigor Router via Web GUI
1 User requests a certificate issued by CA Server A and Saves it.

1. Go to **Certificate Management** and choose **Local Certificate**.

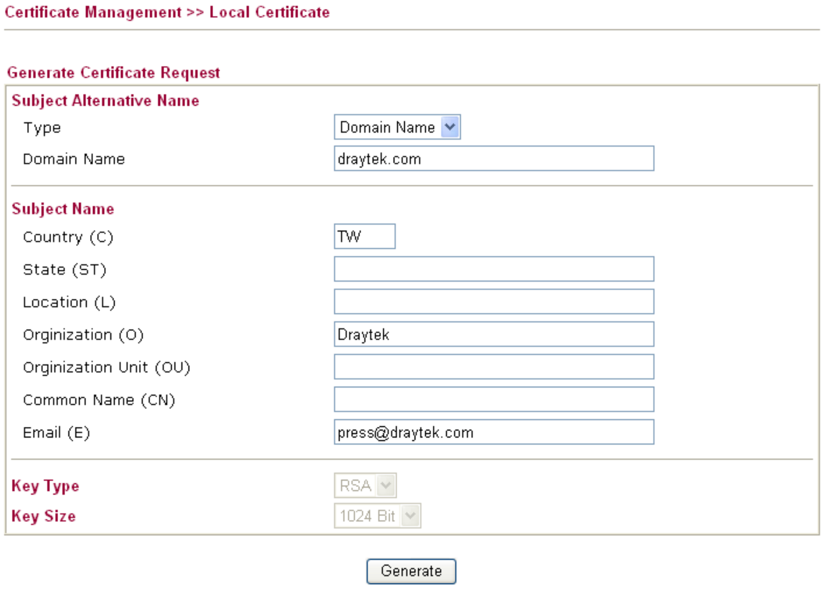


Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	---	---	View Delete

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



Certificate Management >> Local Certificate

Generate Certificate Request

Subject Alternative Name

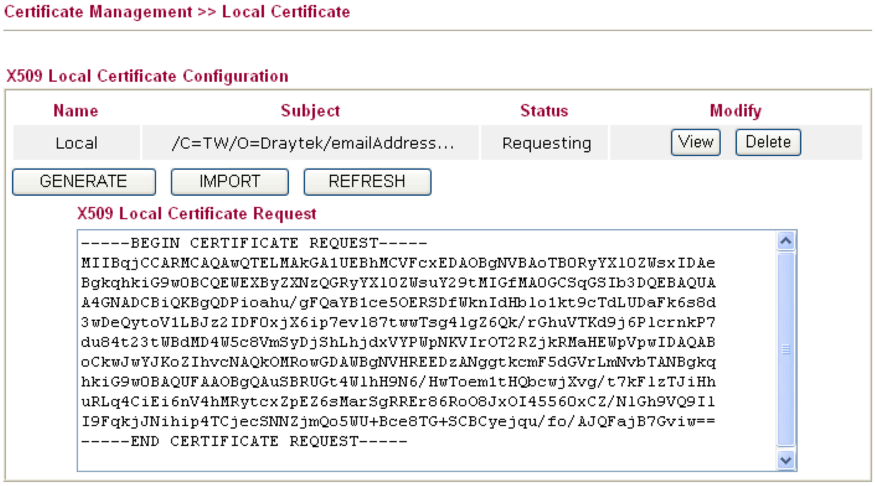
Type	Domain Name
Domain Name	draytek.com

Subject Name

Country (C)	TW
State (ST)	
Location (L)	
Orginization (O)	Draytek
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	press@draytek.com

Key Type	RSA
Key Size	1024 Bit

3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



Certificate Management >> Local Certificate

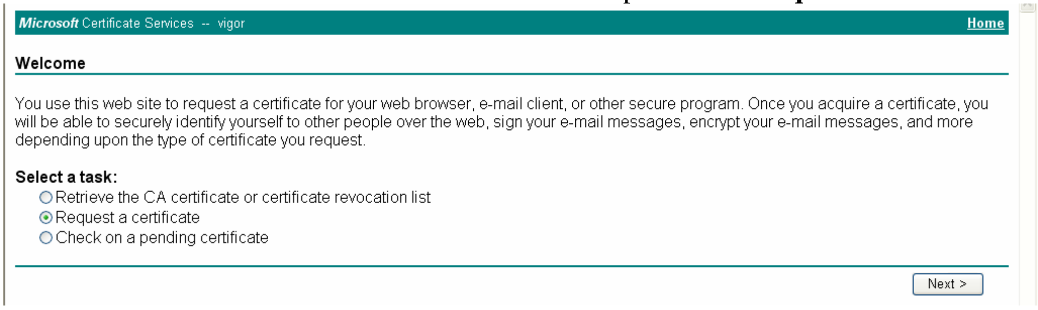
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress...	Requesting	View Delete

X509 Local Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYXl0ZWsxIDAe
BgkqhkiG9w0BCQEWEXByZXNzQGRyYXl0ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSDfWknIdHblo1kt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg41gZ6Qk/rGhuVTKd9j6P1crnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86RoO8JxOI4556OxCZ/N1Gh9VQ9Il
I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
```

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



Microsoft Certificate Services -- vigor

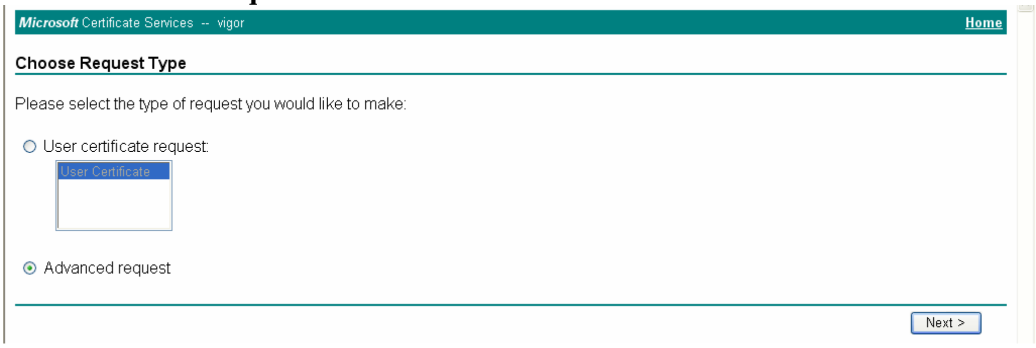
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Select **Advanced request**.



Microsoft Certificate Services -- vigor

Home

Choose Request Type

Please select the type of request you would like to make:

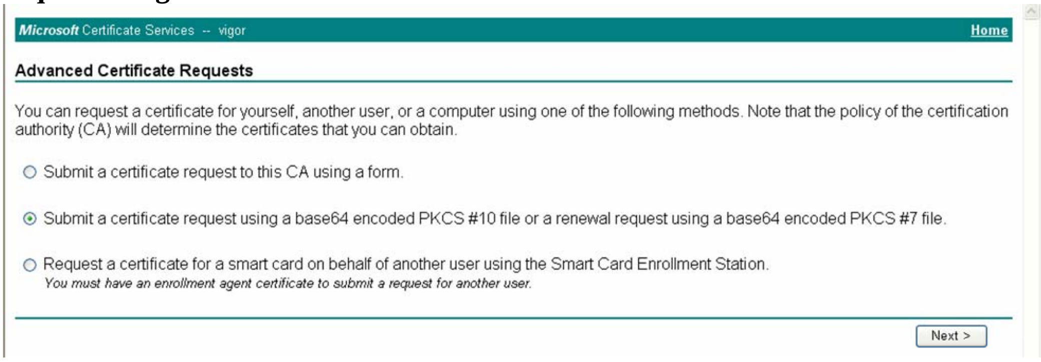
○ User certificate request:

User Certificate

● Advanced request

Next >

Select **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**



Microsoft Certificate Services -- vigor

Home

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

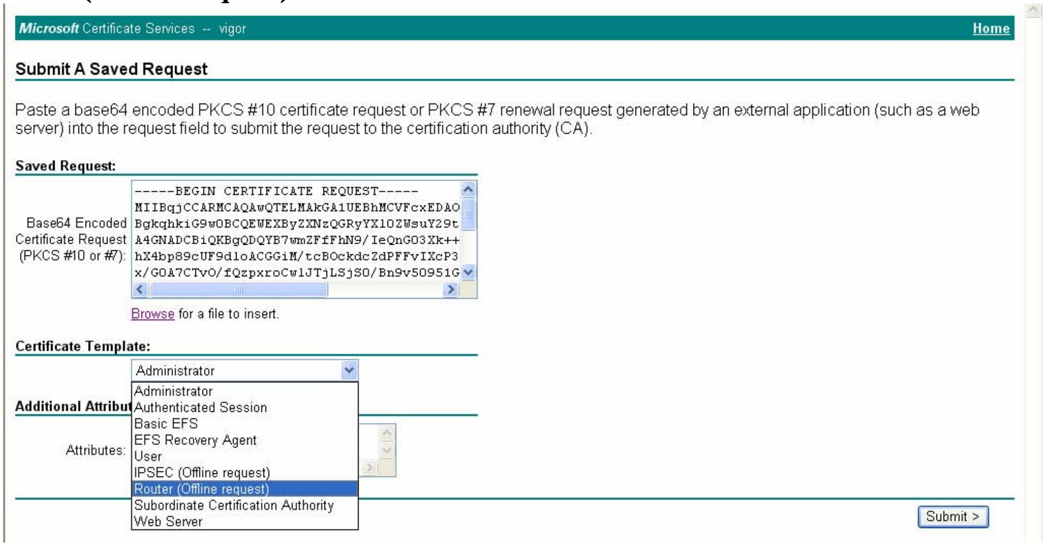
○ Submit a certificate request to this CA using a form.

● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

Import the X509 Local Certificate Requet text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



Microsoft Certificate Services -- vigor

Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO
BgkqhkiG9w0BCQEWEXByZXNzQGRyYXl0ZWsuY29t
A4GNADCBiQKBgQDQYB7wmZFfFhN9/IeQnG03Xk++
hX4bp89cUF9dloACGGiM/tcBOckdcZdPFFvIXcP3
x/G0A7CTvO/fQzpxroCwlJTjLSjS0/Bn9v50951G
```

Browse for a file to insert.

Certificate Template:

Administrator

Additional Attribut

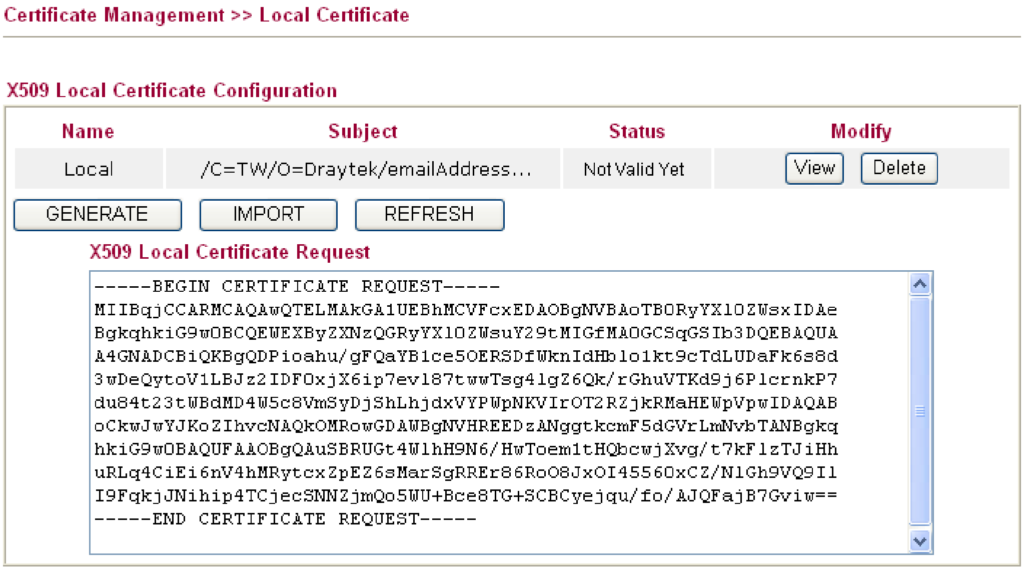
Attributes:

Submit >

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and

you will find the below window showing “------BEGINE CERTIFICATE------.....”



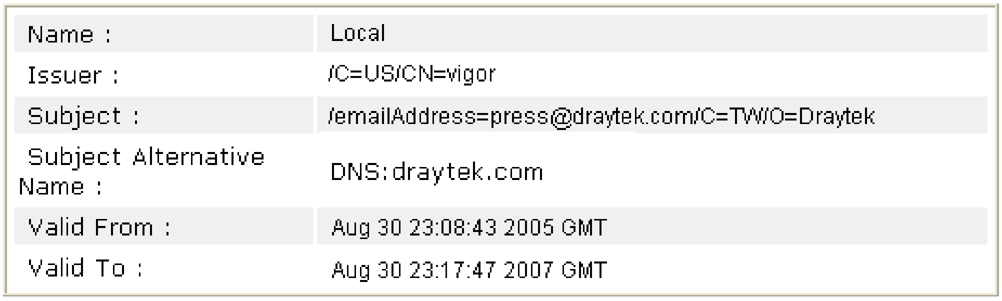
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress...	Not Valid Yet	View Delete

X509 Local Certificate Request

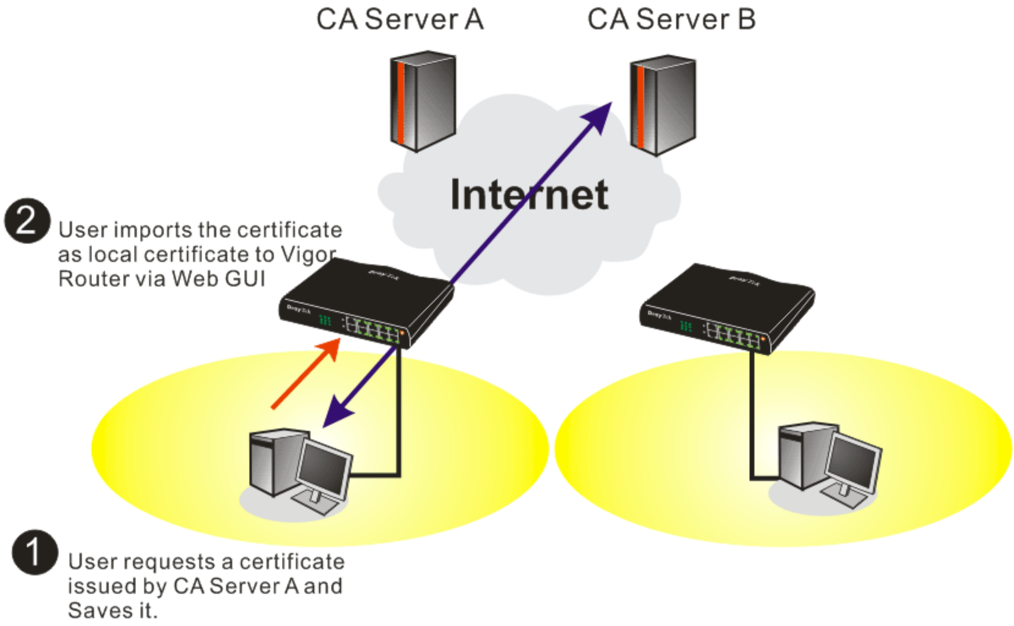
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYXl0ZWsxIDAe
BgkqhkiG9w0BCQEWEXByZXNzQGRyYXl0ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSDfWknIdHblo1kt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDFOxjX6ip7ev187twwTsg41gZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86RoO8JxOI4556OxCZ/N1Gh9VQ9Il
I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
```

6. You may review the detail information of the certificate by clicking **View** button.

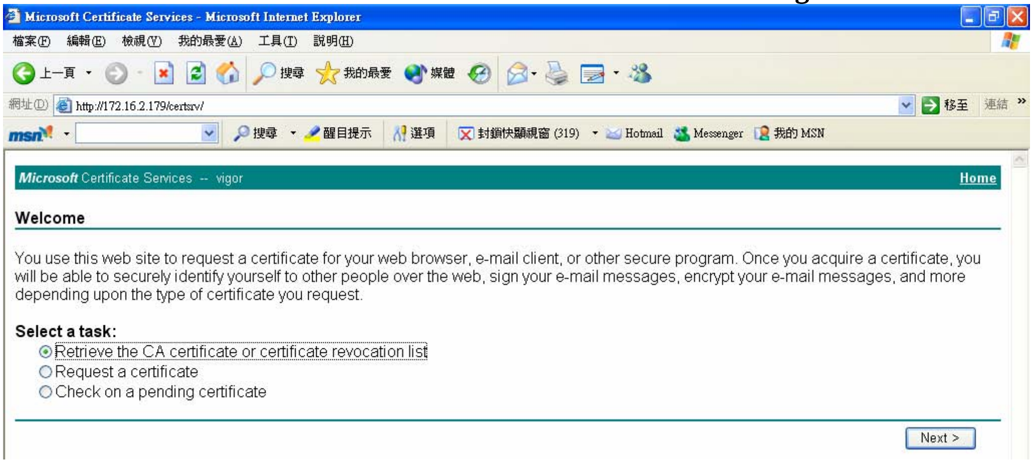


Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

5.7 Request a CA Certificate and Set as Trusted on Windows CA Server


CA Server A
CA Server B
Internet
2 User imports the certificate as local certificate to Vigor Router via Web GUI
1 User requests a certificate issued by CA Server A and Saves it.

1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.


Microsoft Certificate Services - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D) http://172.16.2.179/certsrv/
移至
連結
msn
搜尋
醒目提示
選項
封鎖快顯視窗 (319)
Hotmail
Messenger
我的 MSN

Microsoft Certificate Services -- vigor **Home**

Welcome

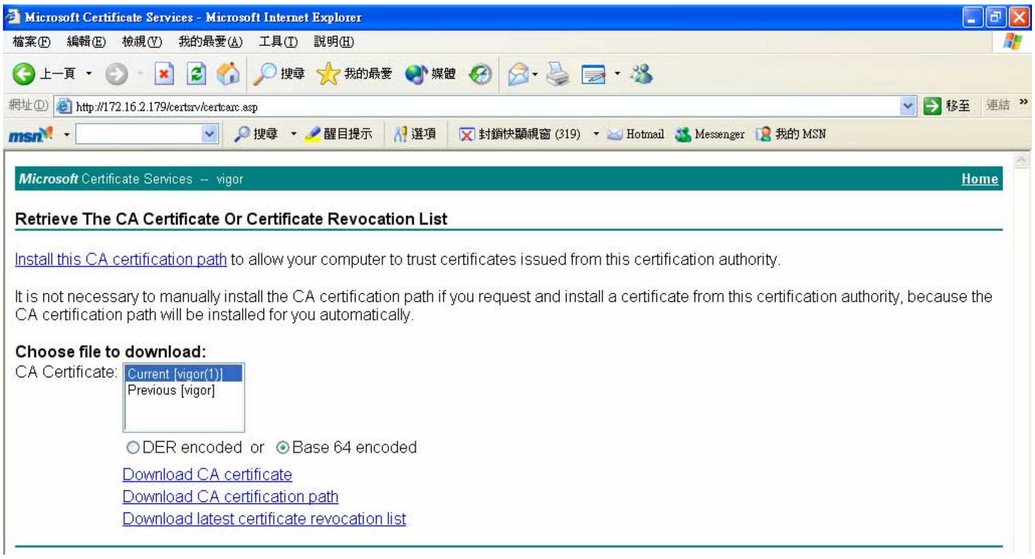
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

● Retrieve the CA certificate or certificate revocation list
○ Request a certificate
○ Check on a pending certificate

Next >

2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.


Microsoft Certificate Services - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D) http://172.16.2.179/certsrv/certcarc.asp
移至
連結
搜尋
醒目提示
選項
封鎖快顯視窗 (319)
Hotmail
Messenger
我的 MSN
Microsoft Certificate Services -- vigor
Home

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

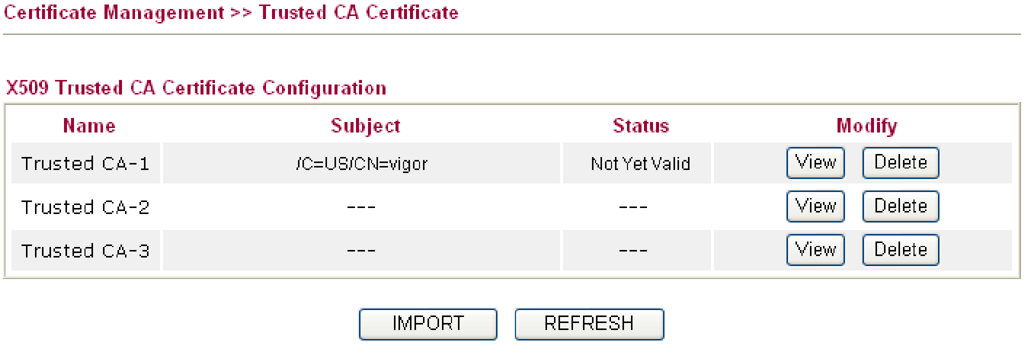
Choose file to download:

CA Certificate: Current [vigor(1)]
Previous [vigor]

○ DER encoded or ● Base 64 encoded

Download CA certificate
Download CA certification path
Download latest certificate revocation list

3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.



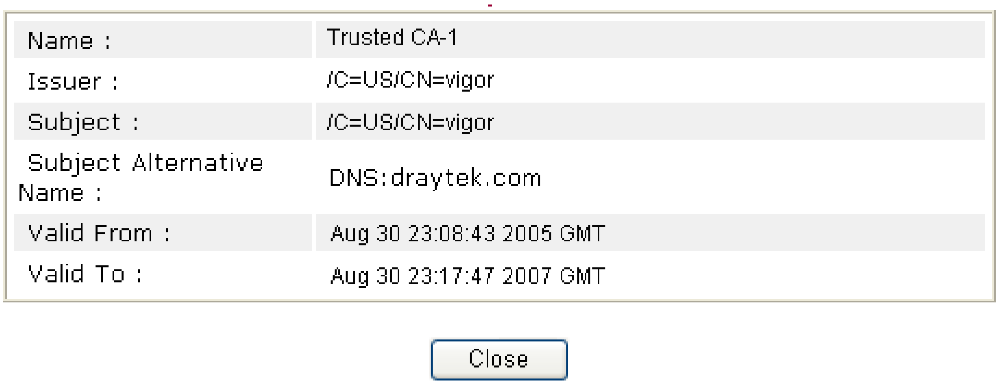
Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1	/C=US/CN=vigor	Not Yet Valid	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

IMPORT REFRESH

4. You may review the detail information of the certificate by clicking **View** button.



Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Close

Note: Before setting certificate configuration, please go to **System Maintenance >> Time and Date** to reset current time of the router first.

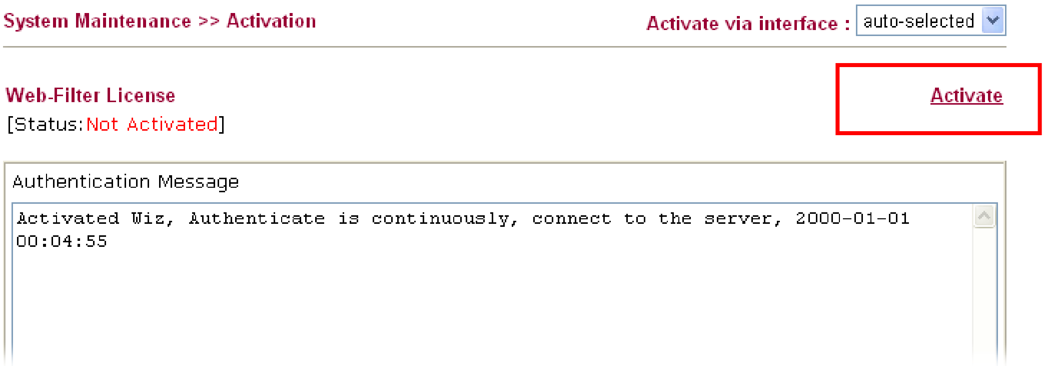
5.8 Creating an Account for MyVigor

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 filter the web pages for protecting your system.

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

5.8.1 Creating an Account via Vigor Router

1. Click **System Maintenance>>Activation** to open the following page.



System Maintenance >> Activation

Activate via interface : auto-selected

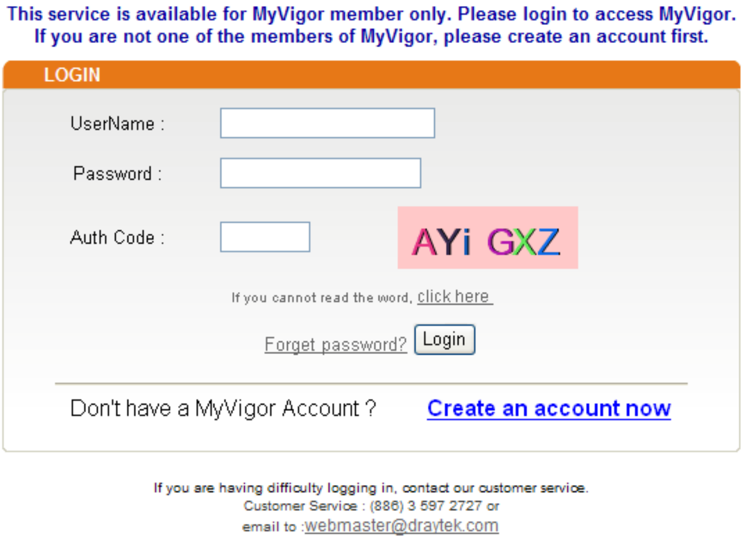
Web-Filter License
[Status:Not Activated]

Activate

Authentication Message

```
Activated Wiz, Authenticate is continuously, connect to the server, 2000-01-01
00:04:55
```

2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code :

If you cannot read the word, click here

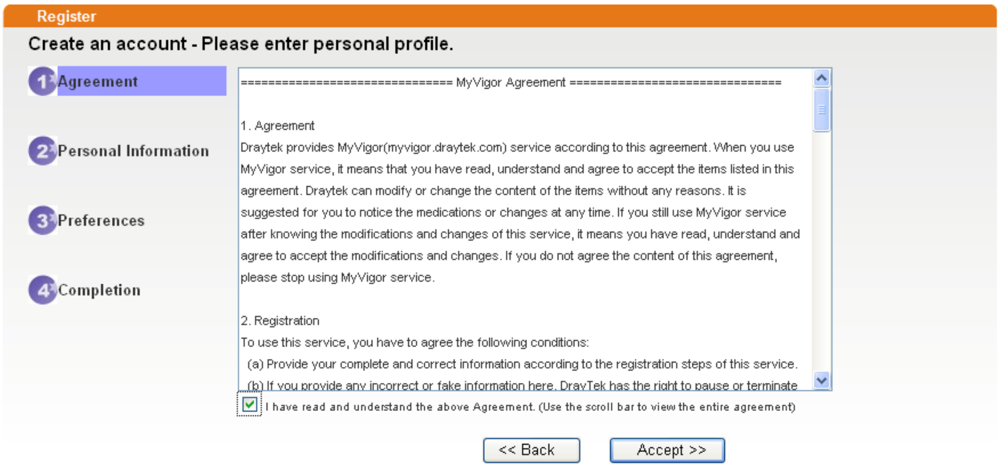
Forget password? Login

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

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or
email to :webmaster@draytek.com

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.

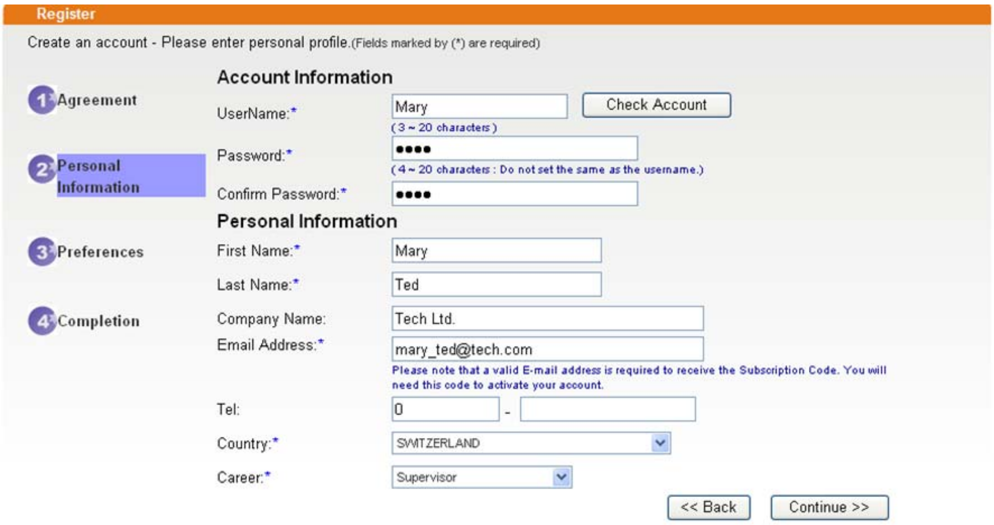
============================== MyVigor Agreement ==============================

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)

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



Register

Create an account - Please enter personal profile.(Fields marked by (*) are required)

Account Information

UserName:* Mary (3 ~ 20 characters)

Password:* ●●●● (4 ~ 20 characters : Do not set the same as the username.)

Confirm Password:* ●●●●

Personal Information

First Name:* Mary

Last Name:* Ted

Company Name: Tech Ltd.

Email Address:* mary_ted@tech.com

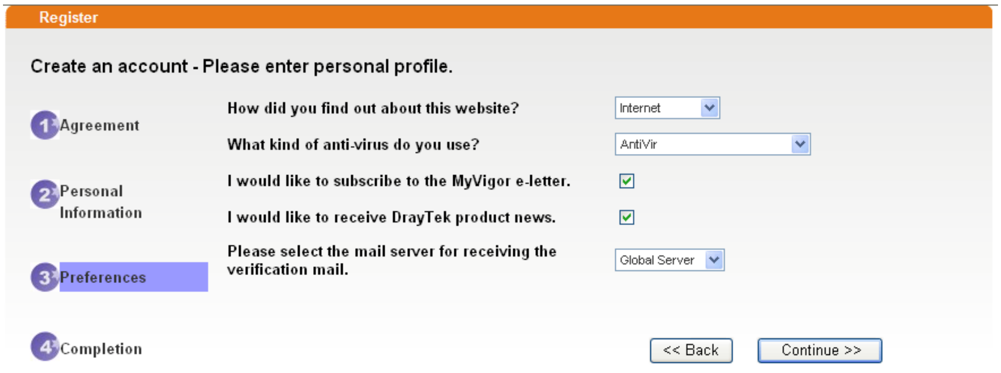
Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country:* SWITZERLAND

Career:* Supervisor

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



Register

Create an account - Please enter personal profile.

How did you find out about this website? Internet

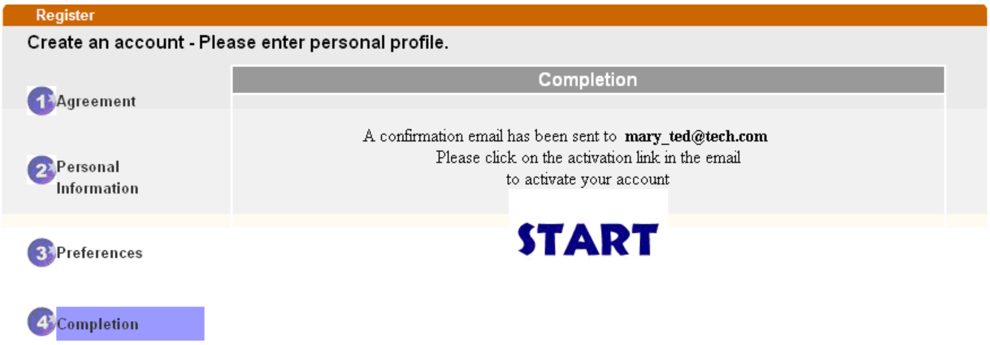
What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter. ☑

I would like to receive DrayTek product news. ☑

Please select the mail server for receiving the verification mail. Global Server

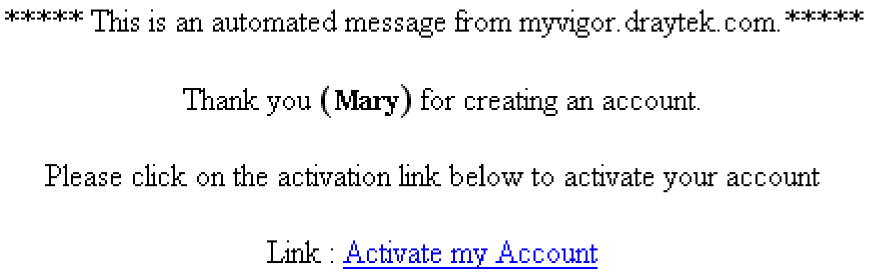
7. Now you have created an account successfully. Click START.



Create an account - Please enter personal profile.

A confirmation email has been sent to **mary_ted@tech.com**
Please click on the activation link in the email
to activate your account

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



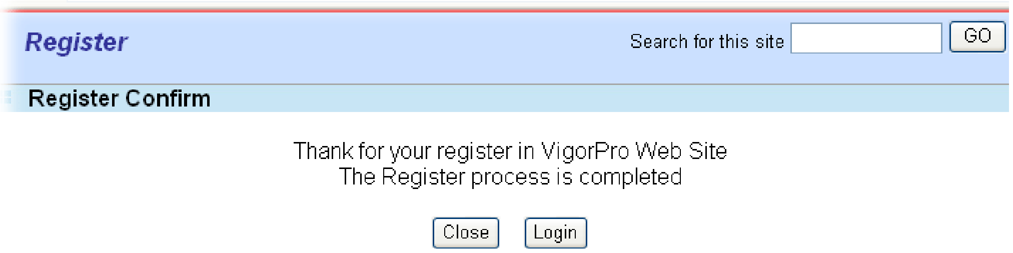
****** This is an automated message from myvigor.draytek.com.******

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

Please click on the activation link below to activate your account

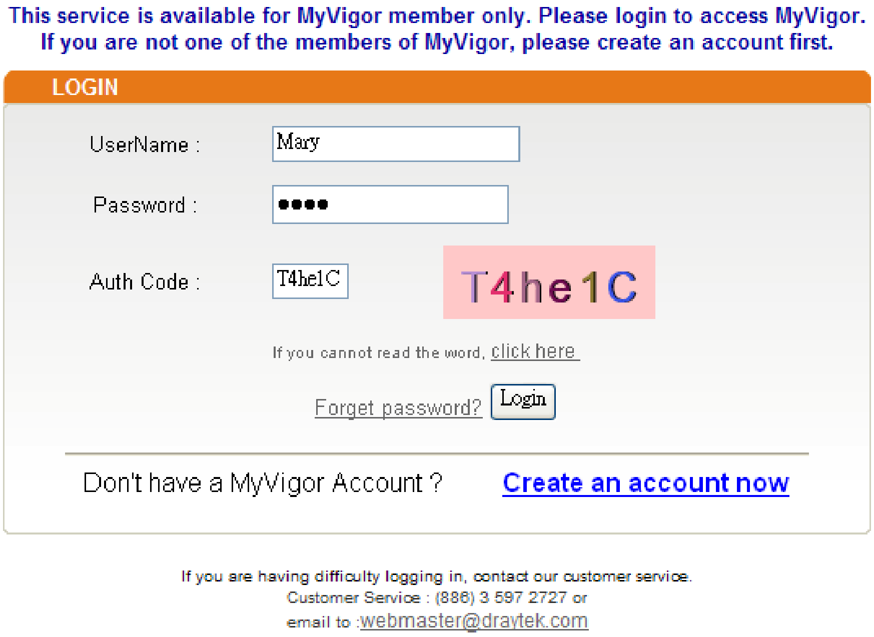
Link : Activate my Account

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**.



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

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**.



This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName : Mary

Password : ●●●●

Auth Code : T4he1C

T4he1C

If you cannot read the word, click here

Forget password? Login

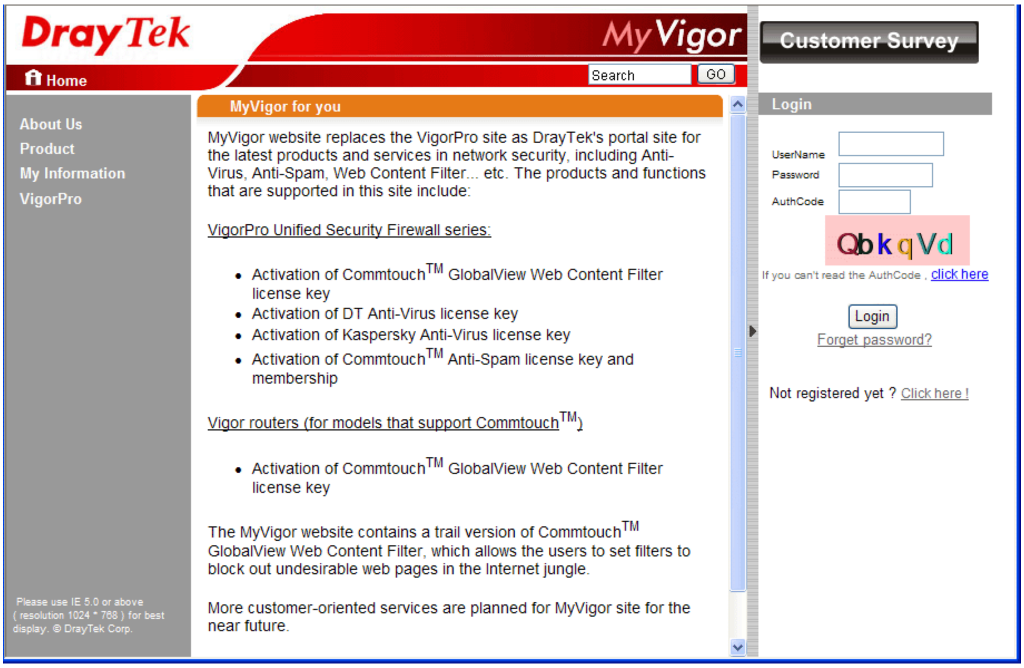
Don't have a MyVigor Account ? Create an account now

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or
email to :webmaster@draytek.com

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.

5.8.2 Creating 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.



MyVigor for you

MyVigor website replaces the VigorPro site as DrayTek's portal site for the latest products and services in network security, including Anti-Virus, Anti-Spam, Web Content Filter... etc. The products and functions that are supported in this site include:

VigorPro Unified Security Firewall series:

- Activation of Commtouch^{TM} GlobalView Web Content Filter license key
- Activation of DT Anti-Virus license key
- Activation of Kaspersky Anti-Virus license key
- Activation of Commtouch^{TM} Anti-Spam license key and membership

Vigor routers (for models that support Commtouch^{TM})

- Activation of Commtouch^{TM} GlobalView Web Content Filter license key

The MyVigor website contains a trail version of Commtouch^{TM} GlobalView Web Content Filter, which allows the users to set filters to block out undesirable web pages in the Internet jungle.

More customer-oriented services are planned for MyVigor site for the near future.

Login

UserName

Password

AuthCode

QbkqVd

If you can't read the AuthCode , click here

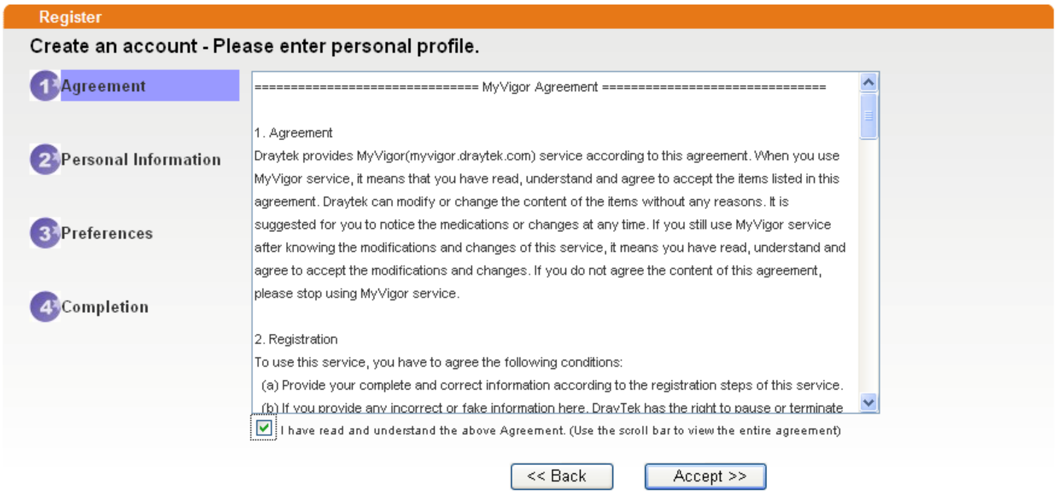
Login

Forget password?

Not registered yet ? Click here !

Please use IE 5.0 or above (resolution 1024 * 768) for best display. © DrayTek Corp.

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



Create an account - Please enter personal profile.

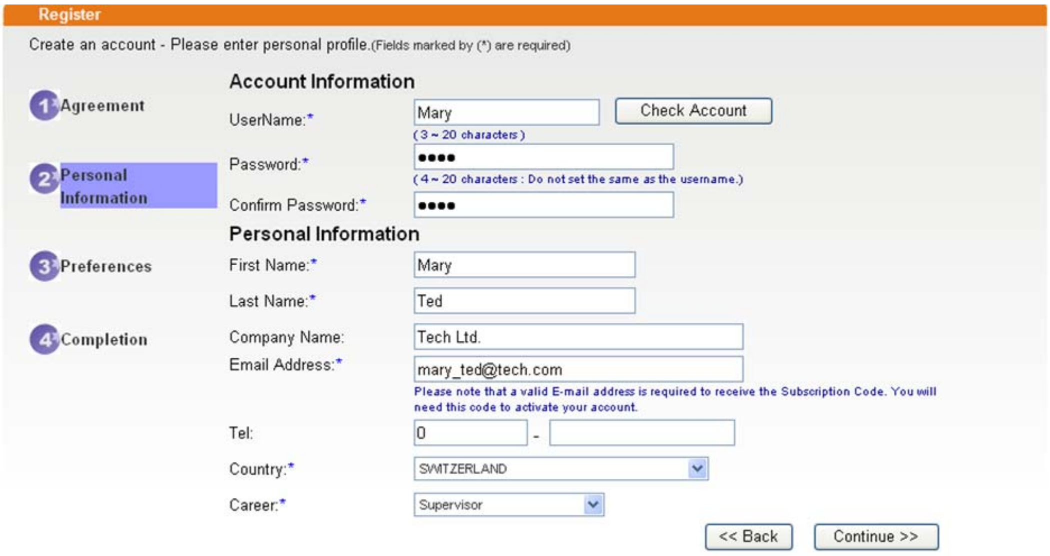
============================= MyVigor Agreement =============================

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)

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



Create an account - Please enter personal profile.(Fields marked by (*) are required)

Account Information

UserName:* Mary
(3 ~ 20 characters)

Password:* ●●●●
(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password:* ●●●●

Personal Information

First Name:* Mary

Last Name:* Ted

Company Name: Tech Ltd.

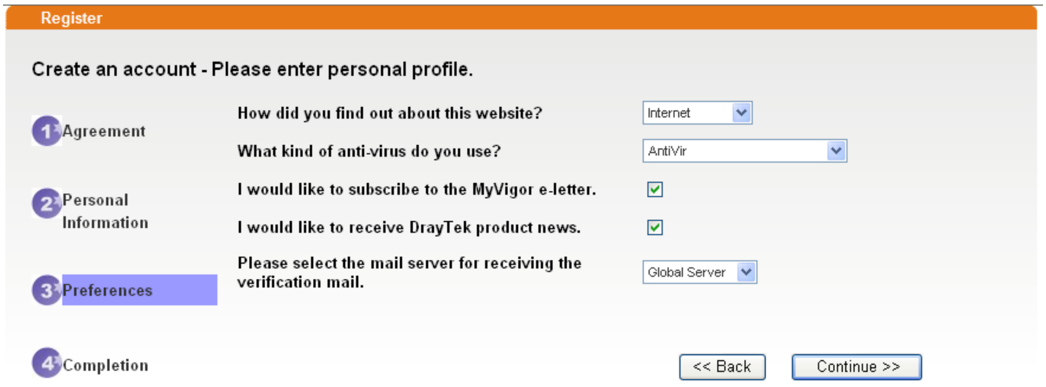
Email Address:* mary_ted@tech.com
Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country:* SWITZERLAND

Career:* Supervisor

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



Create an account - Please enter personal profile.

How did you find out about this website? Internet

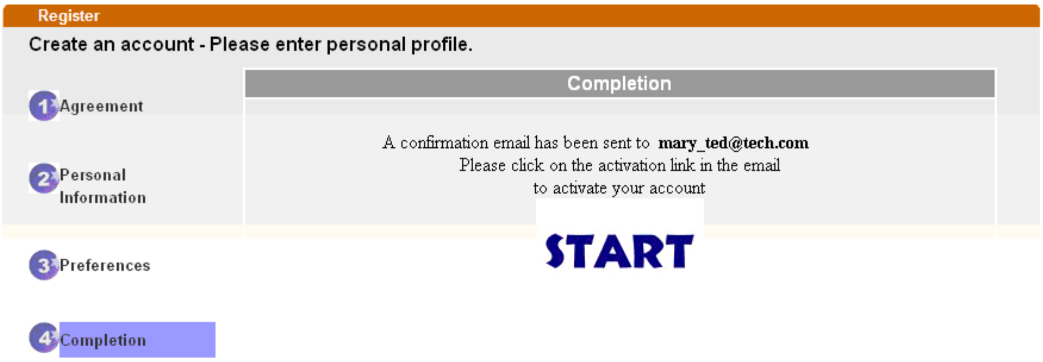
What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter. ☑

I would like to receive DrayTek product news. ☑

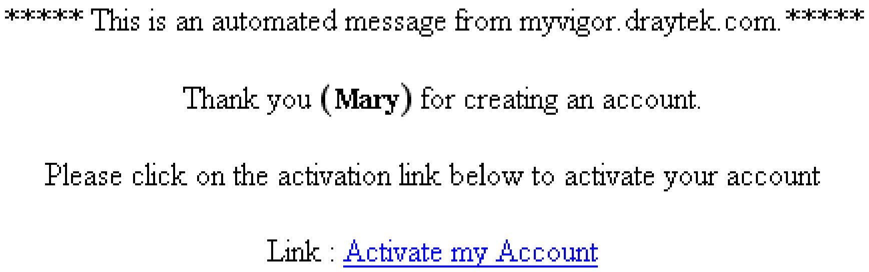
Please select the mail server for receiving the verification mail. Global Server

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



A confirmation email has been sent to **mary_ted@tech.com**
Please click on the activation link in the email
to activate your account

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



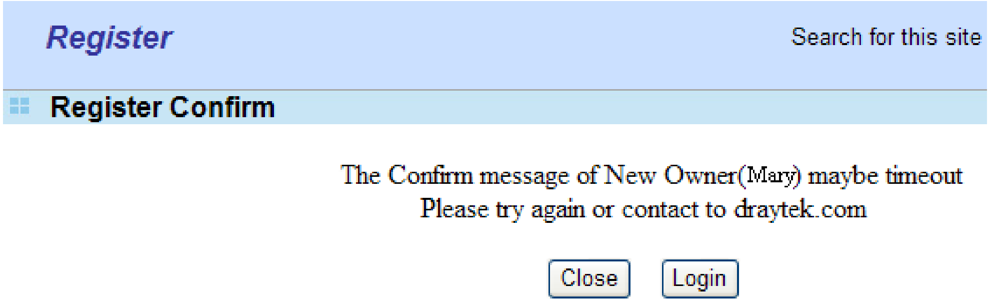
***** This is an automated message from myvigor.draytek.com.*****

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

Please click on the activation link below to activate your account

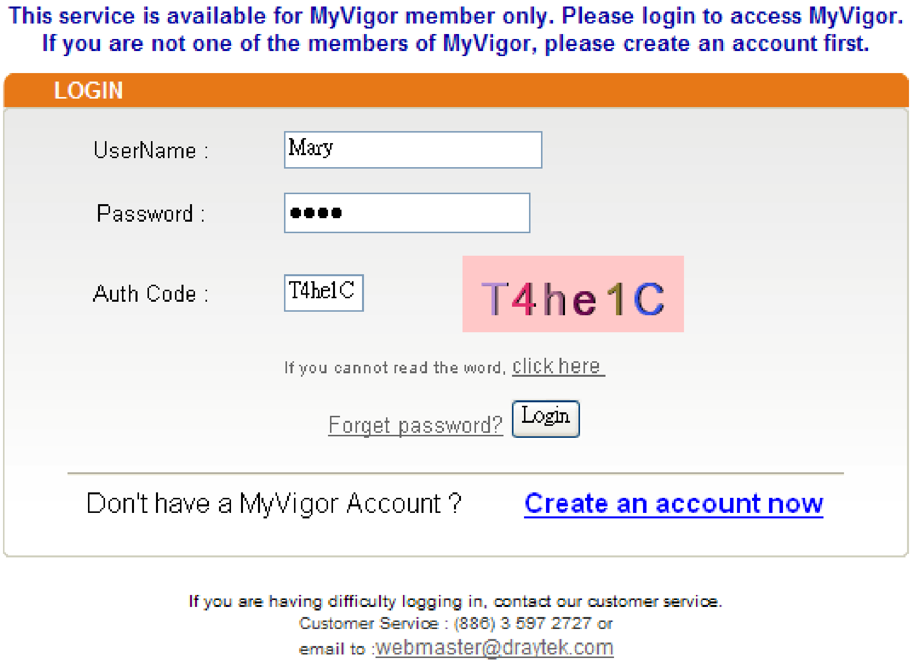
Link : Activate my Account

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



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

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.



This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName : Mary

Password : ●●●●

Auth Code : T4he1C

If you cannot read the word, click here

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

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or
email to :webmaster@draytek.com

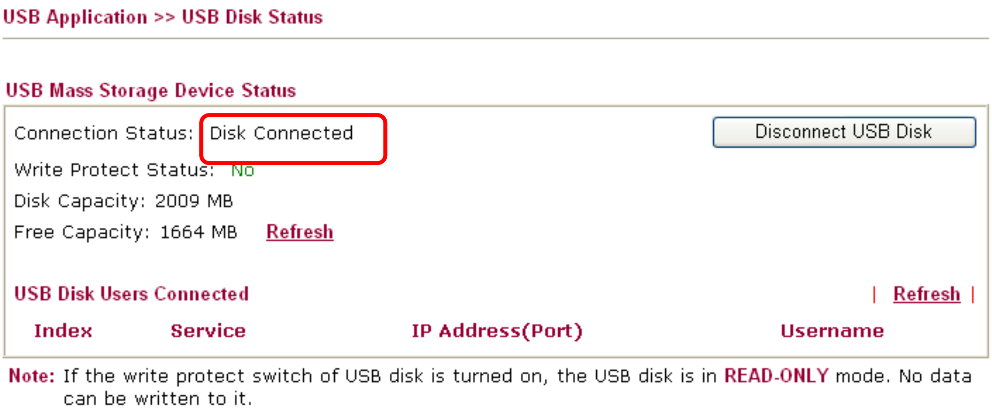
Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

5.9 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 SAMBA server or FTP server.

Samba service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

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:



USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: Disk Connected

Write Protect Status: No

Disk Capacity: 2009 MB

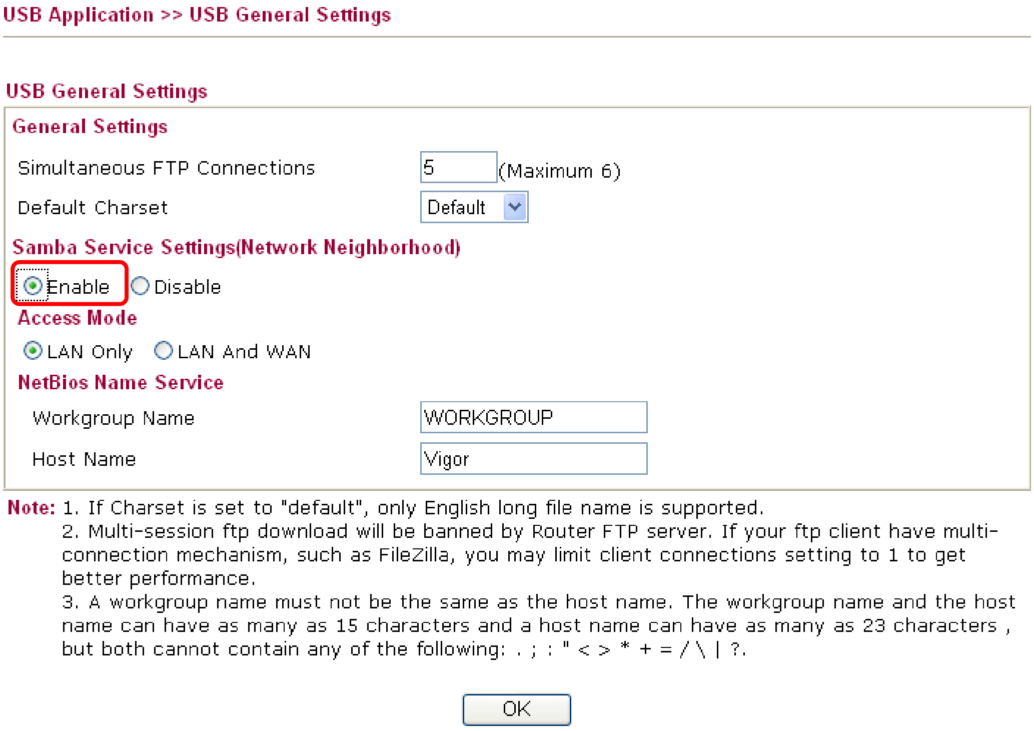
Free Capacity: 1664 MB Refresh

USB Disk Users Connected | Refresh |

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.

2. Then, please open **USB Application** >> **USB General Settings** to enable Samba service.



USB Application >> USB General Settings

USB General Settings

General Settings

Simultaneous FTP Connections: 5 (Maximum 6)

Default Charset: Default

Samba Service Settings(Network Neighborhood)

● Enable ○ Disable

Access Mode

● LAN Only ○ LAN And WAN

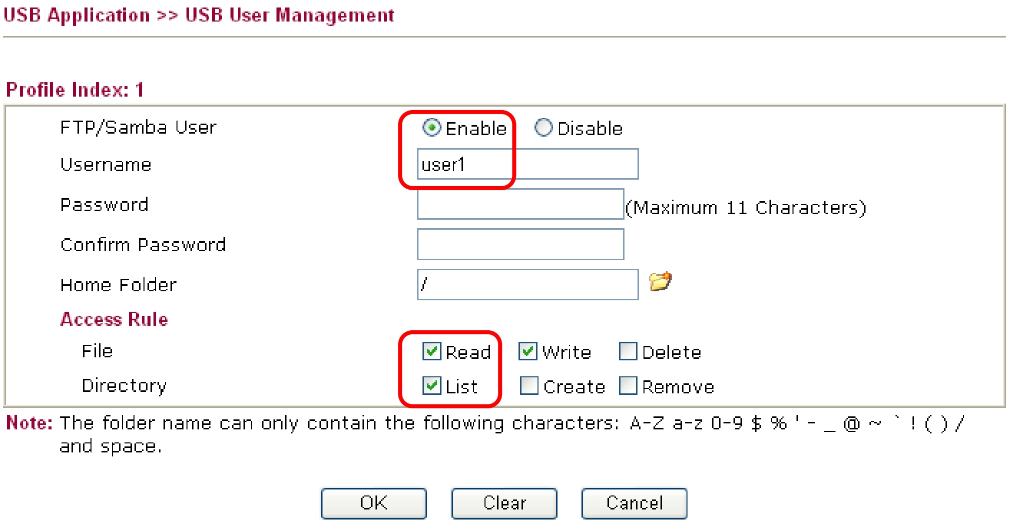
NetBios Name Service

Workgroup Name: WORKGROUP

Host Name: Vigor

Note: 1. If Charset is set to "default", 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.
3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . ; : " < > * + = / \ | ?.

3. 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.



USB Application >> USB User Management

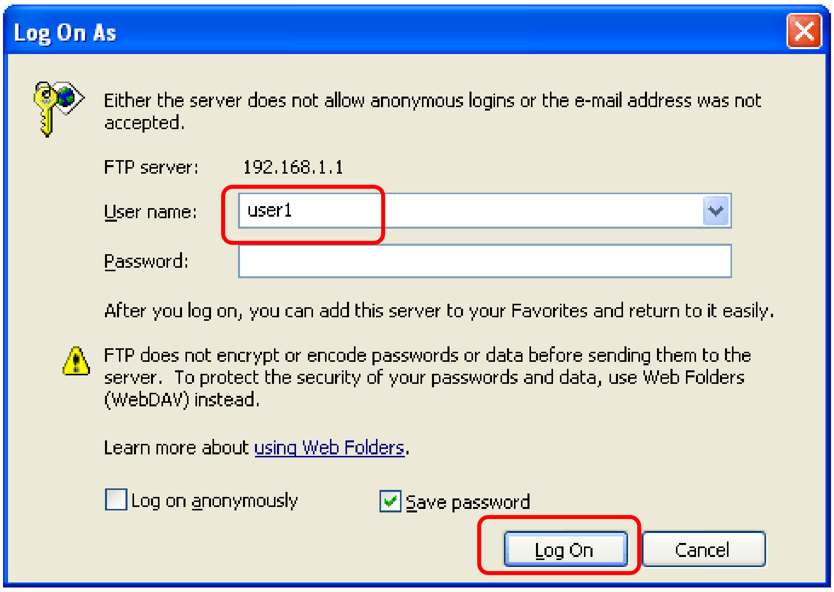
Profile Index: 1

FTP/Samba User	● Enable ○ Disable
Username	user1
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	/
Access Rule	
File	☑ Read ☑ Write □ Delete
Directory	☑ List □ Create □ Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 $ % ' - _ @ ~ ` ! ( ) / and space.

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.



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 192.168.1.1

User name: user1

Password:

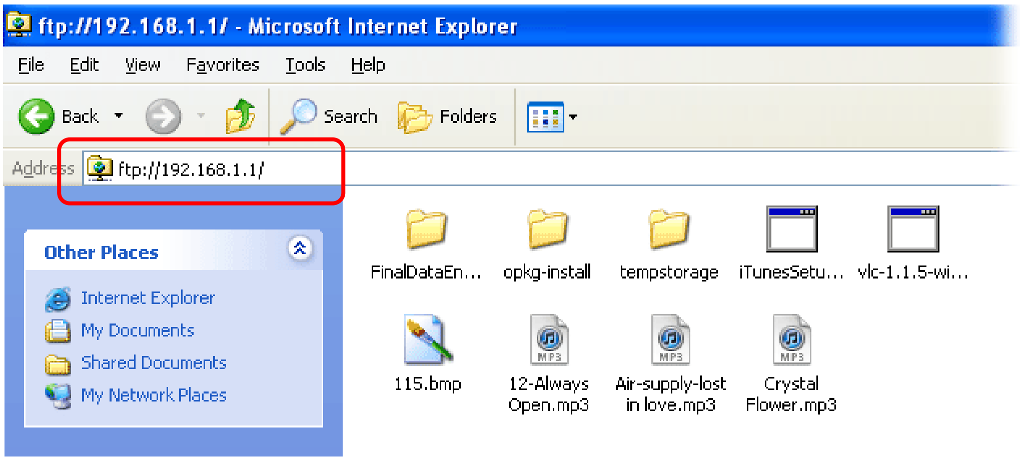
After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.

Learn more about using Web Folders.

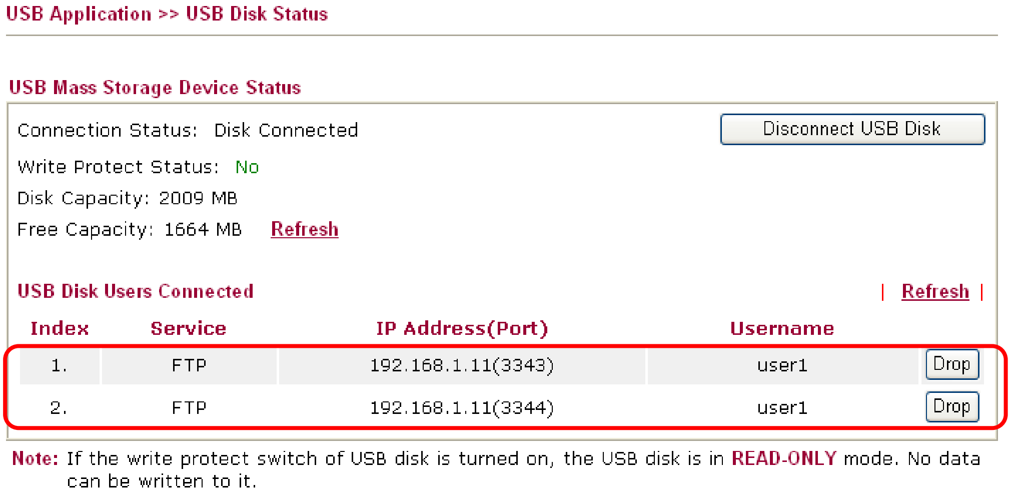
□ Log on anonymously ☑ Save password

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



Address: ftp://192.168.1.1/

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



USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: Disk Connected [Disconnect USB Disk]

Write Protect Status: No

Disk Capacity: 2009 MB

Free Capacity: 1664 MB Refresh

USB Disk Users Connected | Refresh |

Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.11(3343)	user1	Drop
2.	FTP	192.168.1.11(3344)	user1	Drop

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.

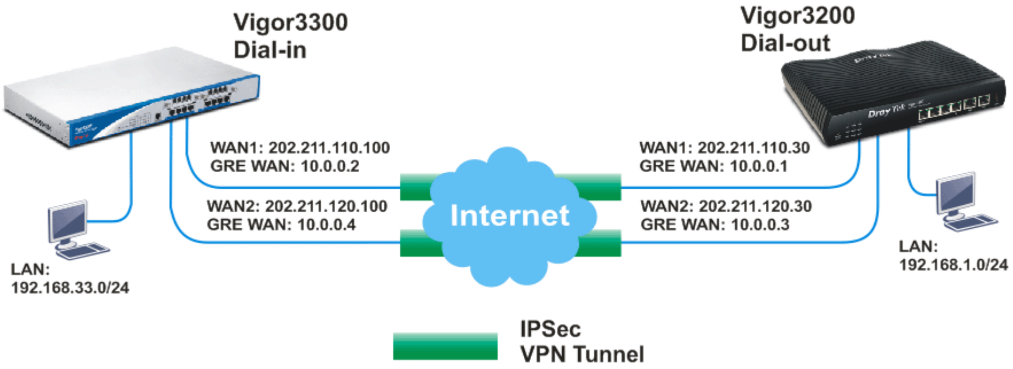
7. Now, users in LAN of Vigor3200 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management.**

5.10 VPN Trunk Load-Balance between Vigor 3200 and Other Vigor Router

This section will discuss how to build VPN Trunk with load-balance between Vigor3200 and other router (e.g., Vigor3300).

Scenario 1: One-pair VPN Trunk

The purpose is to setup a VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24).



At present, Vigor3200 just supports one VPN trunk group with two members for the same VPN network pair. In this case, the VPN trunk is built for 192.168.1.0/24 <-> 192.168.33.0/24. In other word, although Vigor3200 supports 4 WAN connections, it just allows you to use 2 VPN connections over two WAN ports for one VPN trunk group between the networks 192.168.1.0/24 and 192.168.33.0/24.

Note:

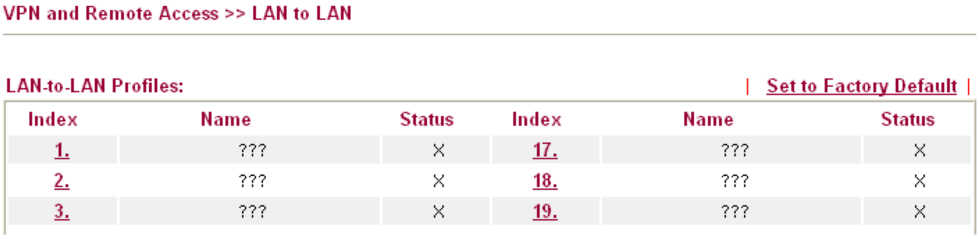
- You can still setup two VPN trunk groups over 4 WAN connections between the networks 192.168.1.0/24 and 192.168.33.0/24. But the VPN traffic can just pass through one VPN trunk group.
- You can create arbitrary number of VPN trunk groups between Vigor3200 and Vigor3300 for different VPN network pairs. For example, suppose there is another network (192.168.10.0/24) behind Vigor3300. You may create a VPN trunk group over WAN1 and WAN2 connections for 192.168.1.0/24 <-> 192.168.33.0/24, and the other VPN trunk group over WAN3 and WAN4 for 192.168.1.0/24 <-> 192.168.10.0/24. Please refer to the Scenario 2 described in this document later.

Vigor3200 as a VPN client (dial out site),
LAN: 192.168.1.0/24
WAN 1 IP: 202.211.110.30 (My GRE IP, 10.0.0.1, Peer GRE IP, 10.0.0.2)
WAN 2 IP: 202.211.120.30 (My GRE IP, 10.0.0.3, Peer GRE IP, 10.0.0.4)

Vigor3300 as a VPN server (dial in site),
LAN: 192.168.33.0/24
WAN 1 IP: 202.211.110.100 (Local GRE IP, 10.0.0.2, Remote GRE IP, 10.0.0.1)
WAN 2 IP: 202.211.120.100 (Local GRE IP, 10.0.0.4, Remote GRE IP, 10.0.0.3)

Settings for Vigor 3200:

1. Open **VPN and Remote Access>>>LAN to LAN**. Choose Index number **1** for configuring a VPN LAN to LAN profile.

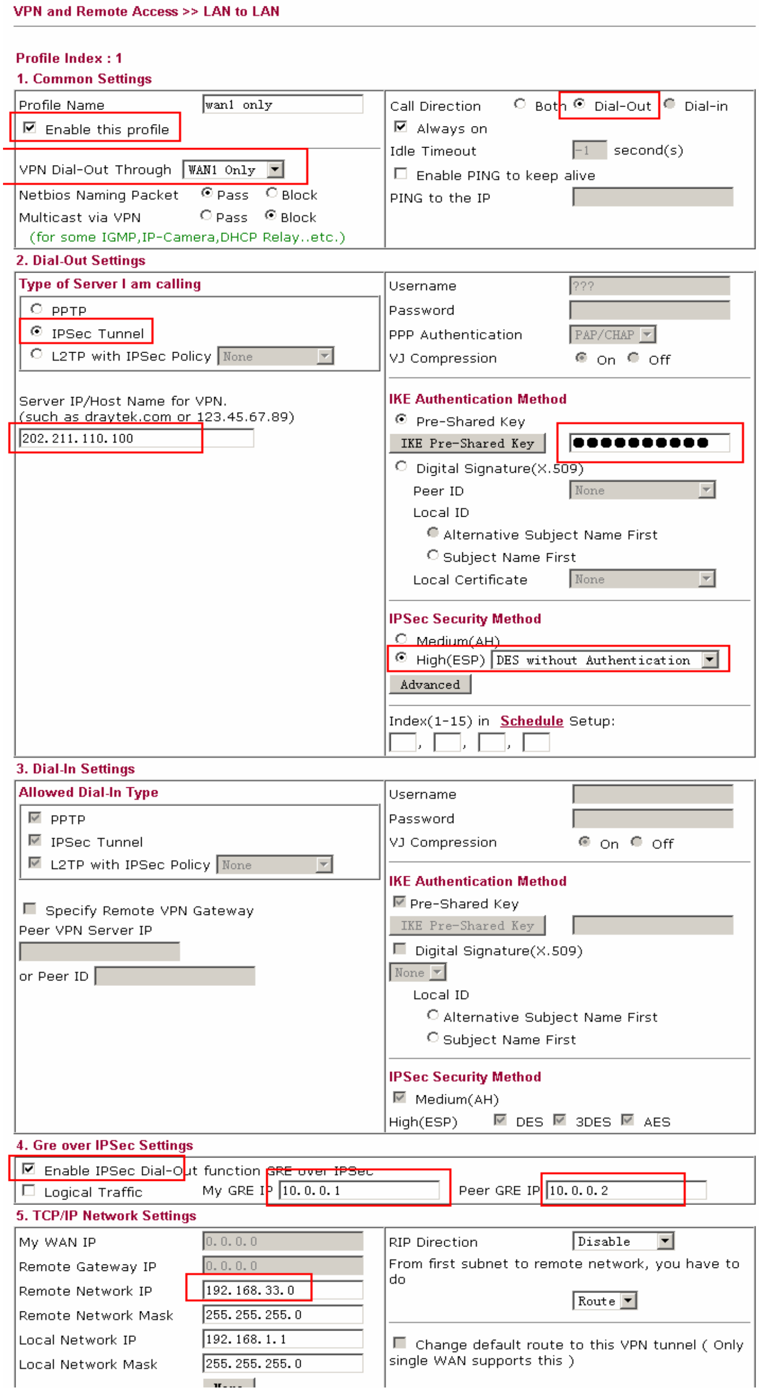


VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | Set to Factory Default |

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X

2. In the following page, please configure the settings as the following figure.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: wan1 only
☑ Enable this profile
VPN Dial-Out Through: WAN1 Only
Netbios Naming Packet: ● Pass ○ Block
Multicast via VPN: ○ Pass ● Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ● Dial-Out ○ Dial-in
☑ Always on
Idle Timeout: -1 second(s)
□ Enable PING to keep alive
PING to the IP:

2. Dial-Out Settings

Type of Server I am calling
○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
202.211.110.100

Username: ???
Password:
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE 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
Advanced

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

3. Dial-In Settings

Allowed Dial-In Type
☑ PPTP
☑ IPSec Tunnel
☑ L2TP with IPSec Policy: None

□ Specify Remote VPN Gateway
Peer VPN Server IP:
or Peer ID:

Username:
Password:
VJ Compression: ● On ○ Off

IKE Authentication Method
☑ Pre-Shared Key
IKE Pre-Shared Key:
□ Digital Signature(X.509)
None
Local ID
○ Alternative Subject Name First
○ Subject Name First

IPSec Security Method
☑ Medium(AH)
High(ESP): ☑ DES ☑ 3DES ☑ AES

4. Gre over IPSec Settings

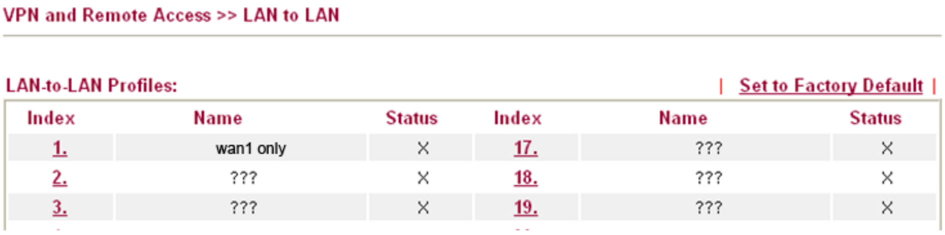
☑ Enable IPSec Dial-Out function GRE over IPSec
□ Logical Traffic
My GRE IP: 10.0.0.1
Peer GRE IP: 10.0.0.2

5. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 0.0.0.0
Remote Network IP: 192.168.33.0
Remote Network Mask: 255.255.255.0
Local Network IP: 192.168.1.1
Local Network Mask: 255.255.255.0

RIP Direction: Disable
From first subnet to remote network, you have to do
Route
□ Change default route to this VPN tunnel (Only single WAN supports this)

3. Click **OK** to save the configuration and return to previous page. Choose Index number **2** for configuring another VPN LAN to LAN profile.

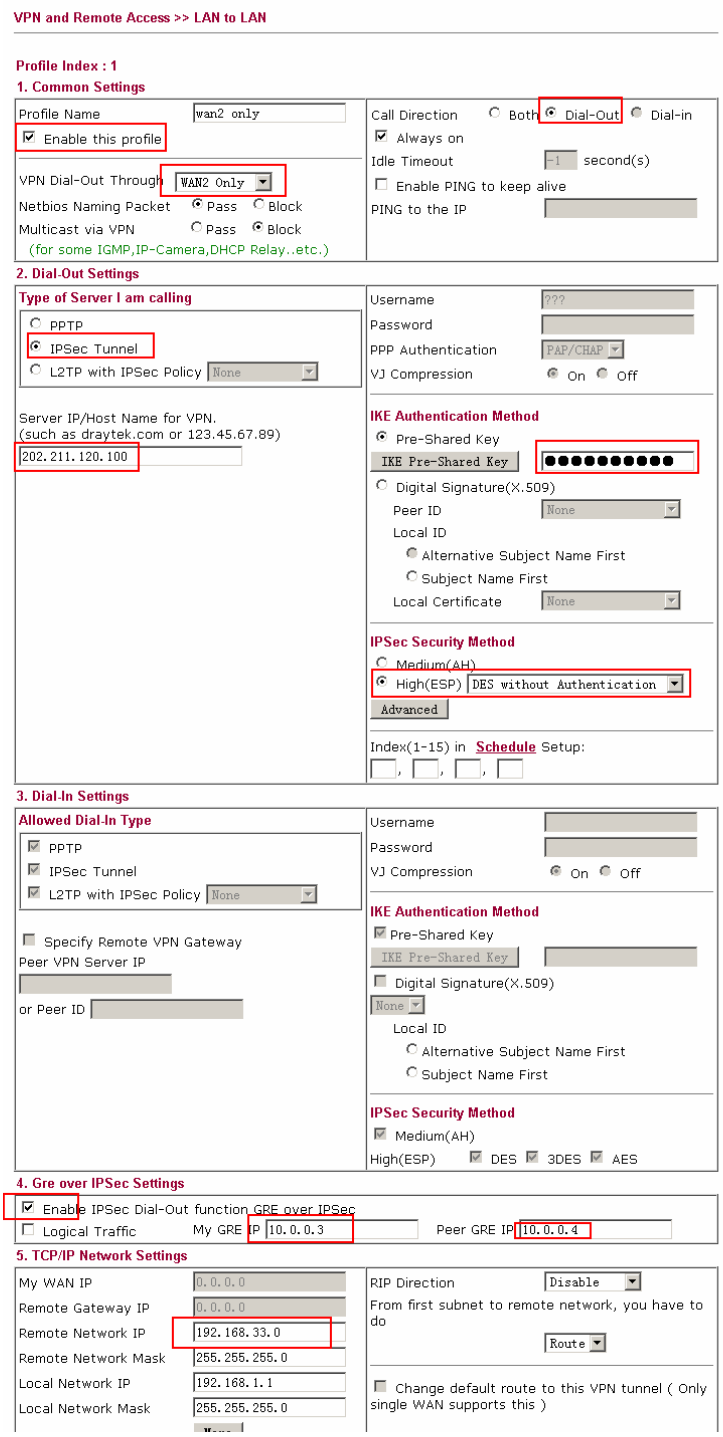


VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | Set to Factory Default |

Index	Name	Status	Index	Name	Status
1.	wan1 only	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X

4. In this page, please configure the settings as the following figure.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: wan2 only
☑ Enable this profile
VPN Dial-Out Through: WAN2 Only
Netbios Naming Packet: ● Pass ○ Block
Multicast via VPN: ○ Pass ● Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ● Dial-Out ○ Dial-in
☑ Always on
Idle Timeout: -1 second(s)
☐ Enable PING to keep alive
PING to the IP:

2. Dial-Out Settings

Type of Server I am calling
○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
202.211.120.100

Username: ???
Password:
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE 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
Advanced

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

3. Dial-In Settings

Allowed Dial-In Type
☑ PPTP
☑ IPSec Tunnel
☑ L2TP with IPSec Policy: None

☐ Specify Remote VPN Gateway
Peer VPN Server IP:
or Peer ID:

Username:
Password:
VJ Compression: ● On ○ Off

IKE Authentication Method
☑ Pre-Shared Key
IKE Pre-Shared Key:
☐ Digital Signature(X.509)
None
Local ID
○ Alternative Subject Name First
○ Subject Name First

IPSec Security Method
☑ Medium(AH)
High(ESP): ☑ DES ☑ 3DES ☑ AES

4. Gre over IPSec Settings

☑ Enable IPSec Dial-Out function GRE over IPSec
☐ Logical Traffic   My GRE IP: 10.0.0.3   Peer GRE IP: 10.0.0.4

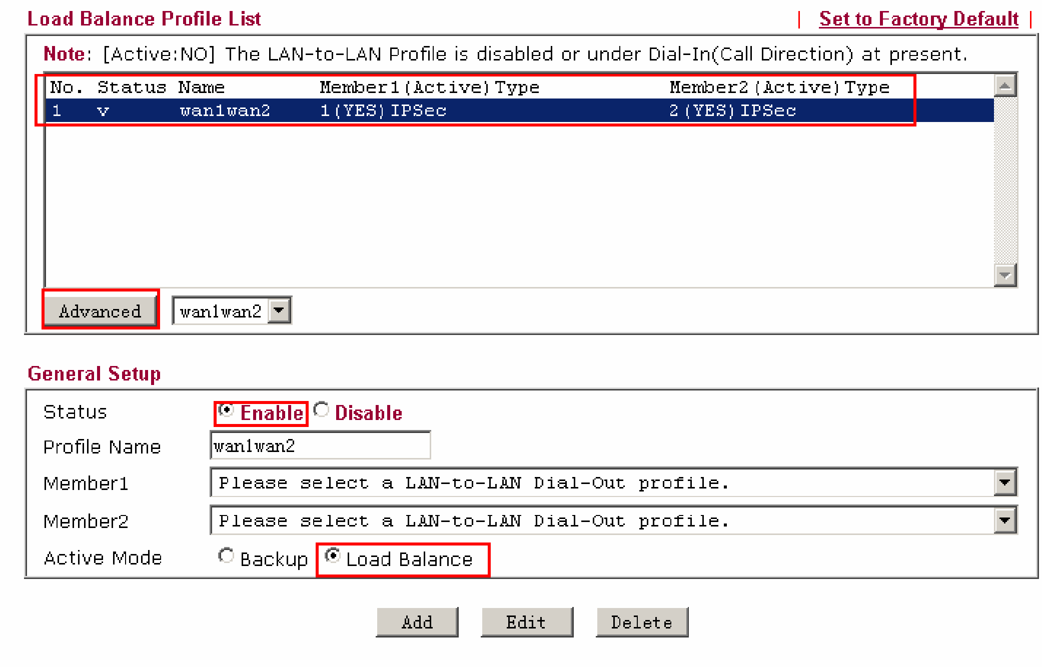
5. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 0.0.0.0
Remote Network IP: 192.168.33.0
Remote Network Mask: 255.255.255.0
Local Network IP: 192.168.1.1
Local Network Mask: 255.255.255.0

RIP Direction: Disable
From first subnet to remote network, you have to do: Route
☐ Change default route to this VPN tunnel (Only single WAN supports this)

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

6. Open **VPN and Remote Access>>VPN TRUNK Management**. Add these VPN profiles to the VPN Trunk and set **Load Balance** as the **Attribute Mode**.



Load Balance Profile List | Set to Factory Default |

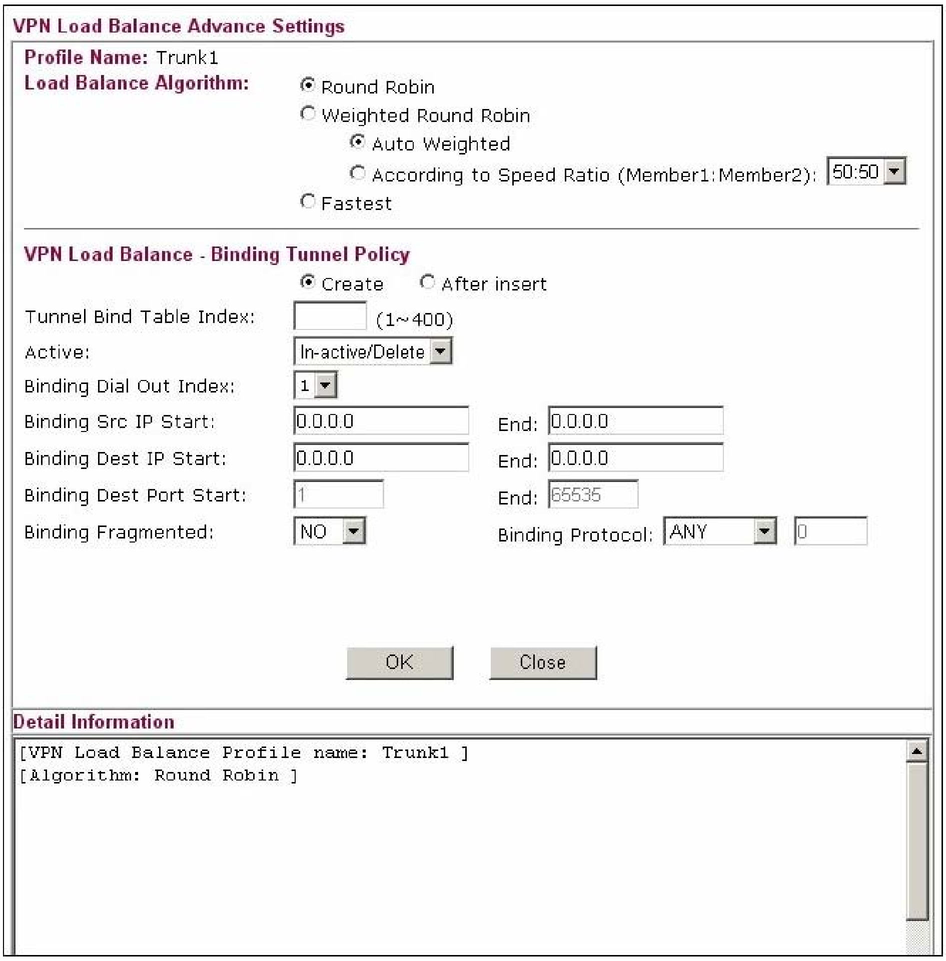
Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type
1	v	wan1wan2	1(YES)IPSec	2(YES)IPSec

General Setup

Status	● Enable ○ Disable
Profile Name	wan1wan2
Member1	Please select a LAN-to-LAN Dial-Out profile.
Member2	Please select a LAN-to-LAN Dial-Out profile.
Active Mode	○ Backup ● Load Balance

7. Click **Advanced** for specifying **Load Balance Algorithm**.



VPN Load Balance Advance Settings

Profile Name: Trunk1

Load Balance Algorithm:
- ● Round Robin
- ○ Weighted Round Robin
  - ● Auto Weighted
  - ○ According to Speed Ratio (Member1:Member2): 50:50
- ○ Fastest

VPN Load Balance - Binding Tunnel Policy

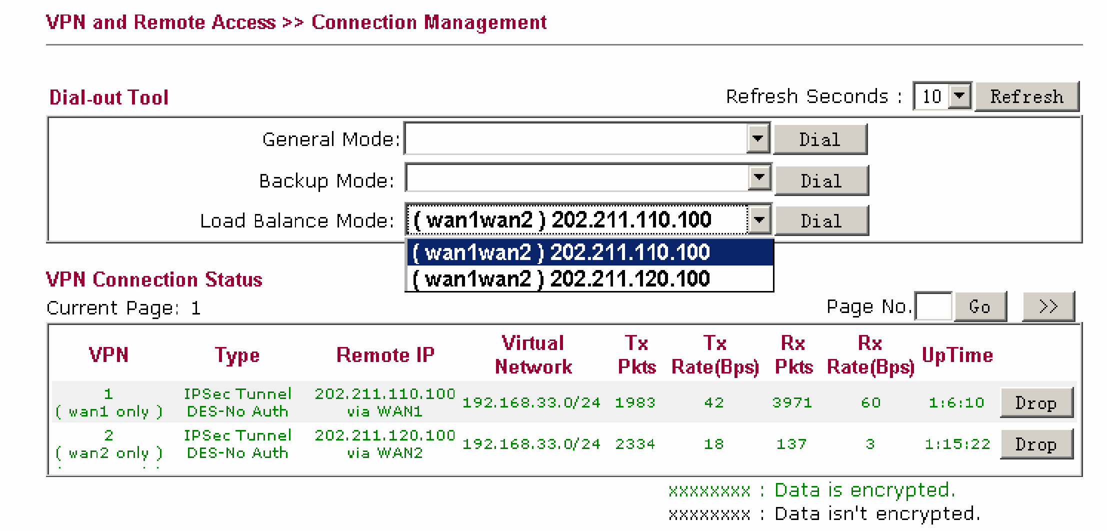
● Create ○ After insert

Tunnel Bind Table Index:	(1~400)		
Active:	In-active/Delete		
Binding Dial Out Index:	1		
Binding Src IP Start:	0.0.0.0	End:	0.0.0.0
Binding Dest IP Start:	0.0.0.0	End:	0.0.0.0
Binding Dest Port Start:	1	End:	65535
Binding Fragmented:	NO	Binding Protocol:	ANY 0

Detail Information

```
[VPN Load Balance Profile name: Trunk1 ]
[Algorithm: Round Robin ]
```

8. When the VPN trunk is successfully connected, you may check the connection status by viewing the page of **VPN and Remote Access>>Connection Management**. Transferred packets (Tx Pkts) will keep increasing through both tunnels when outgoing packets sent to the remote VPN network.



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

General Mode:		Dial
Backup Mode:		Dial
Load Balance Mode:	(wan1wan2) 202.211.110.100	Dial

(wan1wan2) 202.211.110.100
(wan1wan2) 202.211.120.100

VPN Connection Status

Current Page: 1

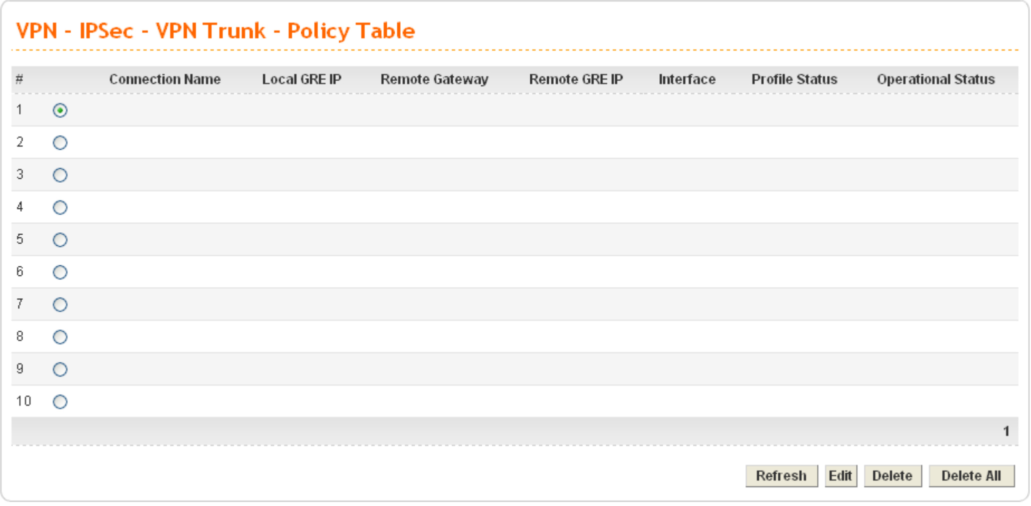
Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (wan1 only)	IPSec Tunnel DES-No Auth	202.211.110.100 via WAN1	192.168.33.0/24	1983	42	3971	60	1:6:10	Drop
2 (wan2 only)	IPSec Tunnel DES-No Auth	202.211.120.100 via WAN2	192.168.33.0/24	2334	18	137	3	1:15:22	Drop

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

Settings for Vigor3300:

1. Open **VPN>>IPSec>>VPN Trunk>>Policy Table**. Choose Index **1** and click **Edit**.

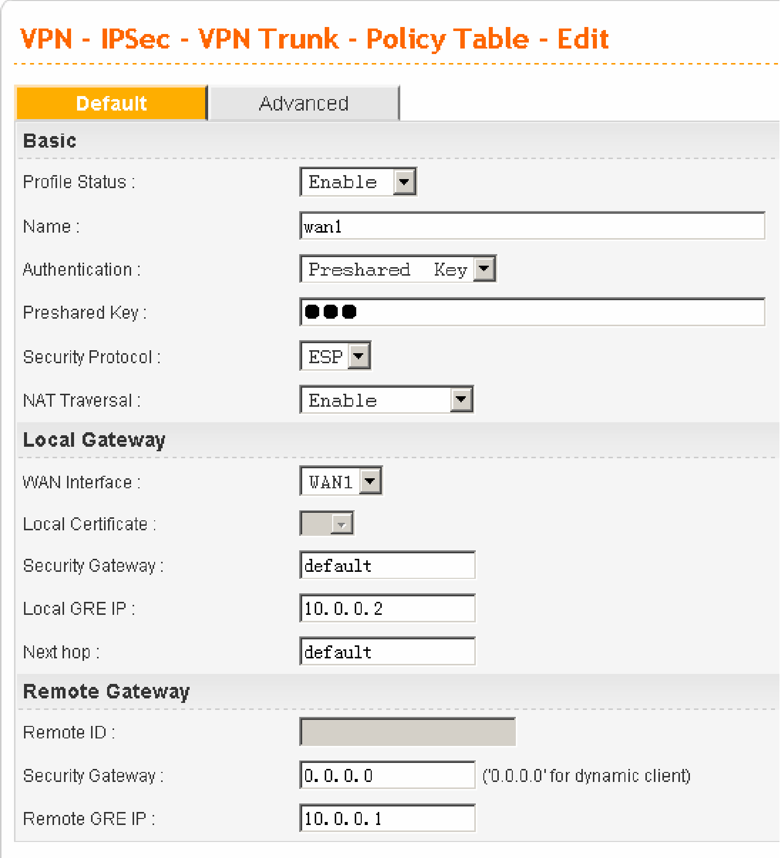


VPN - IPSec - VPN Trunk - Policy Table

#		Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1	●							
2	○							
3	○							
4	○							
5	○							
6	○							
7	○							
8	○							
9	○							
10	○							

1

2. In this page, please configure the settings as the following figure.



VPN - IPSec - VPN Trunk - Policy Table - Edit

Basic

Profile Status :	Enable
Name :	wan1
Authentication :	Preshared Key
Preshared Key :	●●●
Security Protocol :	ESP
NAT Traversal :	Enable

Local Gateway

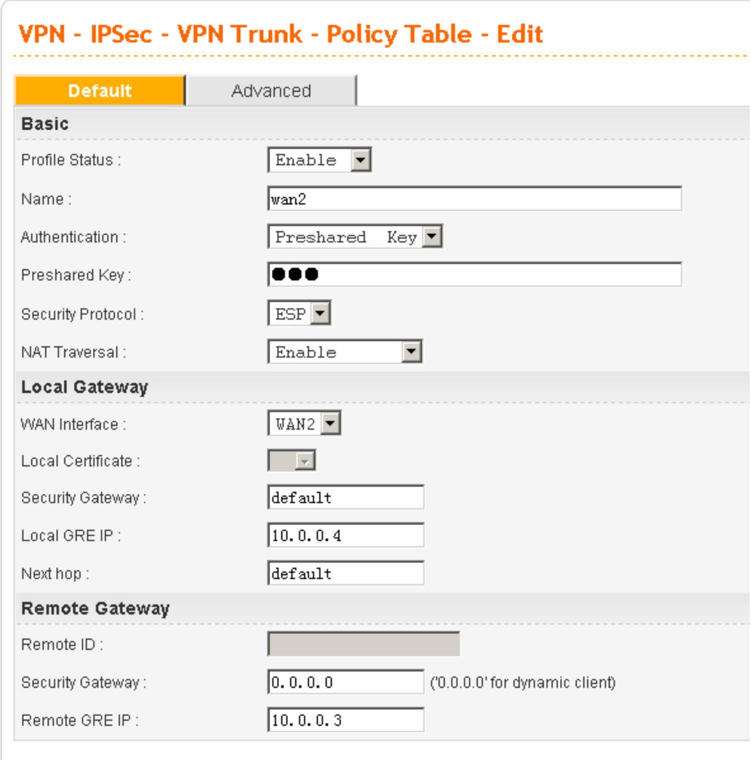
WAN Interface :	WAN1
Local Certificate :	
Security Gateway :	default
Local GRE IP :	10.0.0.2
Next hop :	default

Remote Gateway

Remote ID :	
Security Gateway :	0.0.0.0 ('0.0.0.0' for dynamic client)
Remote GRE IP :	10.0.0.1

3. Click **Apply** to save the configuration and return to previous page. Choose Index **2** for configuring another VPN Trunk policy.

4. In this page, please configure the settings as the following figure.



VPN - IPSec - VPN Trunk - Policy Table - Edit

Basic

Profile Status :	Enable
Name :	wan2
Authentication :	Preshared Key
Preshared Key :	●●●
Security Protocol :	ESP
NAT Traversal :	Enable

Local Gateway

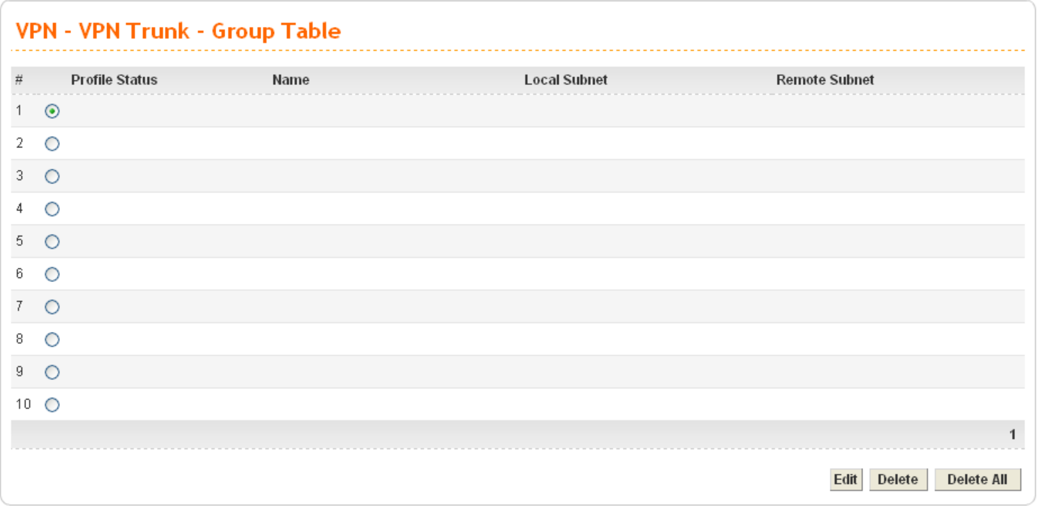
WAN Interface :	WAN2
Local Certificate :	
Security Gateway :	default
Local GRE IP :	10.0.0.4
Next hop :	default

Remote Gateway

Remote ID :	
Security Gateway :	0.0.0.0 ('0.0.0.0' for dynamic client)
Remote GRE IP :	10.0.0.3

5. Click **Apply** to save the configuration.

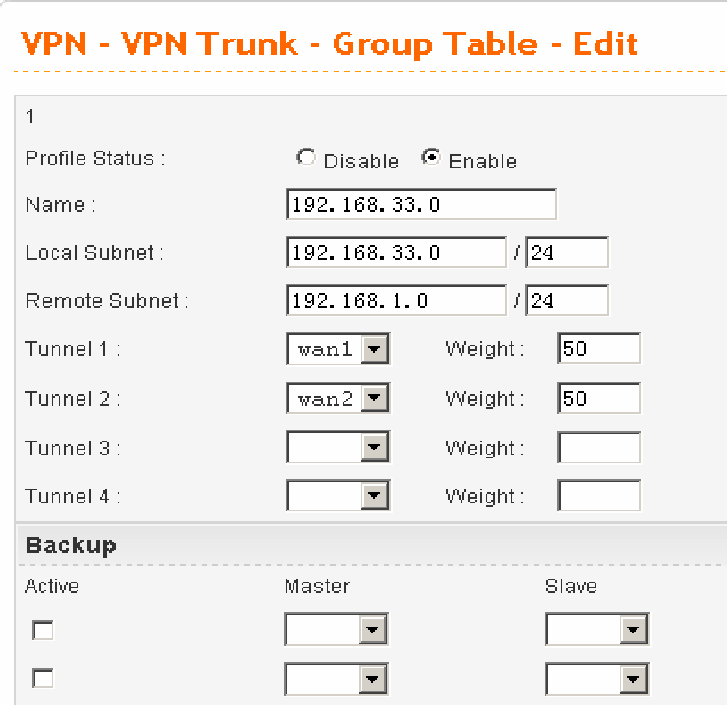
6. Open **VPN>>VPN Trunk>>Group Table** to group these two VPN policies.



VPN - VPN Trunk - Group Table

#	Profile Status	Name	Local Subnet	Remote Subnet
1	●			
2	○			
3	○			
4	○			
5	○			
6	○			
7	○			
8	○			
9	○			
10	○			

7. Choose Index 1 and click **Edit**. Add these two VPN profiles (wan1 and wan2) to a VPN Trunk.



VPN - VPN Trunk - Group Table - Edit

1

Profile Status : ○ Disable ● Enable

Name : 192.168.33.0

Local Subnet : 192.168.33.0 / 24

Remote Subnet : 192.168.1.0 / 24

Tunnel 1 : wan1 Weight : 50

Tunnel 2 : wan2 Weight : 50

Tunnel 3 : Weight :

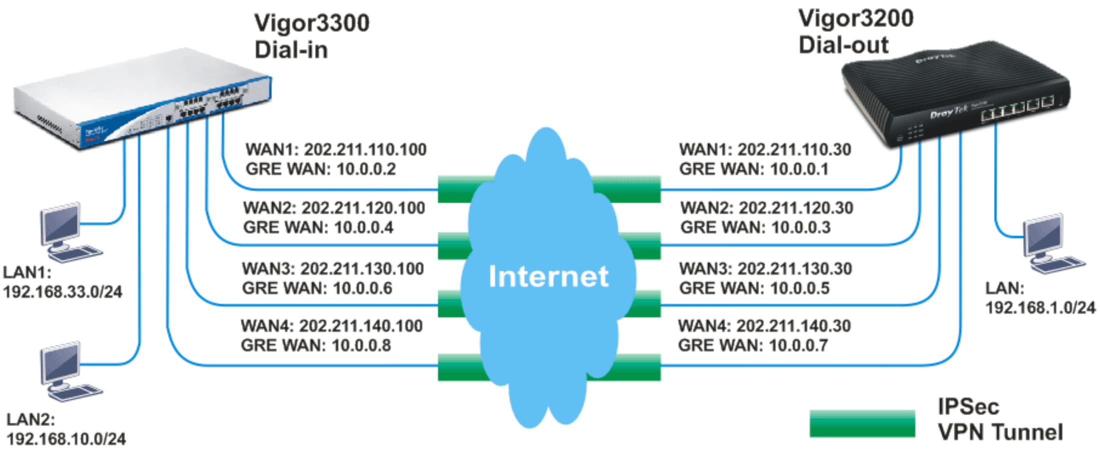
Tunnel 4 : Weight :

Backup

Active	Master	Slave
□		
□		

Now, one-pair VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24) has be established.

Scenario 2: Two-pair VPN Trunk

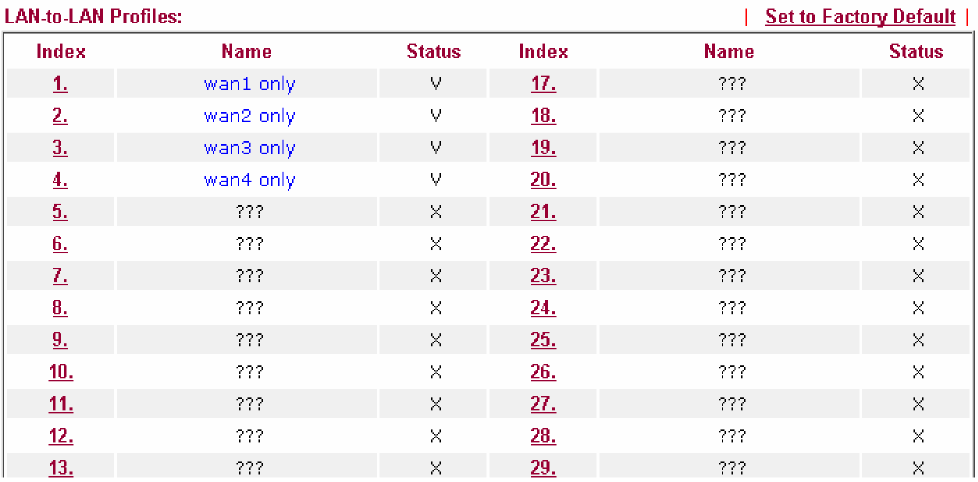


Vigor3200 as VPN client (dial out site)
LAN: 192.168.1.0/24
WAN 1 IP: 202.211.110.30 (My GRE IP, 10.0.0.1, Peer GRE IP, 10.0.0.2)
WAN 2 IP: 202.211.120.30 (My GRE IP, 10.0.0.3, Peer GRE IP, 10.0.0.4)
WAN 3 IP: 202.211.130.30 (My GRE IP, 10.0.0.5, Peer GRE IP, 10.0.0.6)
WAN 4 IP: 202.211.140.30 (My GRE IP, 10.0.0.7, Peer GRE IP, 10.0.0.8)

Vigor3300 as VPN server (dial in site),
LAN1: 192.168.33.0/24
LAN2: 192.168.10.0/24
WAN 1 IP: 202.211.110.100 (Local GRE IP, 10.0.0.2, Remote GRE IP, 10.0.0.1)
WAN 2 IP: 202.211.120.100 (Local GRE IP, 10.0.0.4, Remote GRE IP, 10.0.0.3)
WAN 3 IP: 202.211.130.100 (Local GRE IP, 10.0.0.6, Remote GRE IP, 10.0.0.5)
WAN 4 IP: 202.211.140.100 (Local GRE IP, 10.0.0.8, Remote GRE IP, 10.0.0.7)

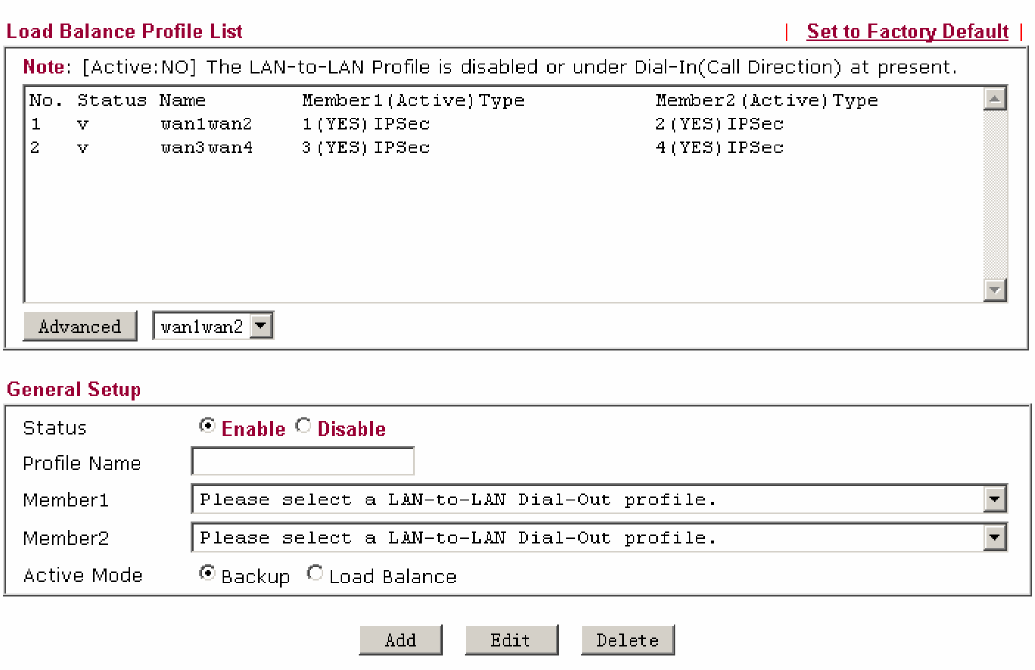
Settings for Vigor 3200:

1. Open **VPN and Remote Access>>>LAN to LAN**.
2. Create LAN to LAN profile 1-4. Setting configuration is the same as Scenario 1. The differences are, Remote Network IP of Profile 1 and Profile 2 must be 192.168.33.0/24 and Remote Network IP of Profile 3 and Profile 4 must be 192.168.10.0/24.


LAN-to-LAN Profiles: | Set to Factory Default |

Index	Name	Status	Index	Name	Status
1.	wan1 only	V	17.	???	X
2.	wan2 only	V	18.	???	X
3.	wan3 only	V	19.	???	X
4.	wan4 only	V	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

3. Open **VPN and Remote Access>>VPN TRUNK Management**. Add these VPN profiles to the VPN Trunk and set **Load Balance** as the **Attribute Mode**. Setting configuration is the same as Scenario 1. Profile 1 and Profile 2 are one pair; Profile 3 and Profile 4 are the other pair.



Load Balance Profile List | Set to Factory Default |

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

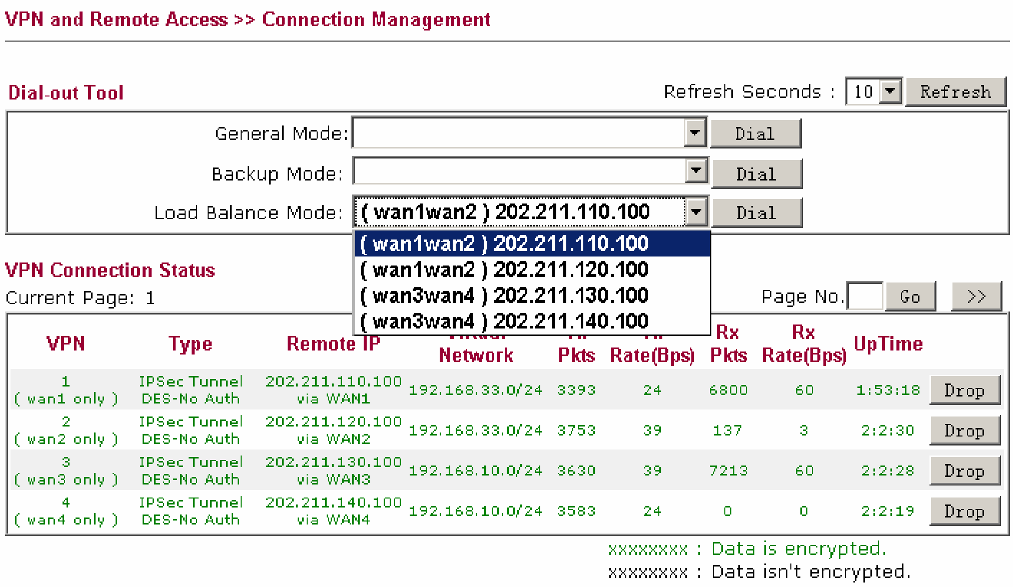
```
No. Status Name       Member1(Active)Type        Member2(Active)Type
1   v      wan1wan2   1(YES)IPSec                2(YES)IPSec
2   v      wan3wan4   3(YES)IPSec                4(YES)IPSec
```

Advanced | wan1wan2

General Setup

Status	● Enable ○ Disable
Profile Name	
Member1	Please select a LAN-to-LAN Dial-Out profile.
Member2	Please select a LAN-to-LAN Dial-Out profile.
Active Mode	● Backup ○ Load Balance

4. When the VPN trunk is successfully connected, you may check the connection status by viewing the page of **VPN and Remote Access>>Connection Management**. Transferred packets (Tx Pkts) will keep increasing through both tunnels when outgoing packets sent to the remote VPN network.



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

General Mode:	
Backup Mode:	
Load Balance Mode:	(wan1wan2) 202.211.110.100

(wan1wan2) 202.211.110.100
(wan1wan2) 202.211.120.100
(wan3wan4) 202.211.130.100
(wan3wan4) 202.211.140.100

VPN Connection Status

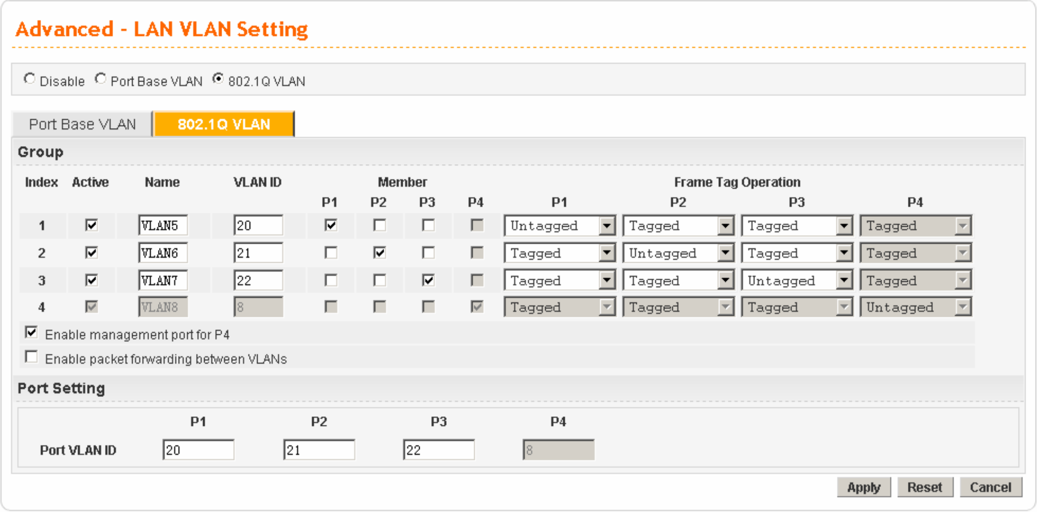
Current Page: 1

VPN	Type	Remote IP	Network	Pkts	Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (wan1 only)	IPSec Tunnel DES-No Auth	202.211.110.100 via WAN1	192.168.33.0/24	3393	24	6800	60	1:53:18	Drop
2 (wan2 only)	IPSec Tunnel DES-No Auth	202.211.120.100 via WAN2	192.168.33.0/24	3753	39	137	3	2:2:30	Drop
3 (wan3 only)	IPSec Tunnel DES-No Auth	202.211.130.100 via WAN3	192.168.10.0/24	3630	39	7213	60	2:2:28	Drop
4 (wan4 only)	IPSec Tunnel DES-No Auth	202.211.140.100 via WAN4	192.168.10.0/24	3583	24	0	0	2:2:19	Drop

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

Settings for Vigor3300:

1. Open **Advanced>>LAN VLAN**. Choose the tab of **802.1Q VLAN**. Configure the settings as the following figure.



Advanced - LAN VLAN Setting

○ Disable ○ Port Base VLAN ● 802.1Q VLAN

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	☑	VLAN5	20	☑	□	□	□	Untagged	Tagged	Tagged	Tagged
2	☑	VLAN6	21	□	☑	□	□	Tagged	Untagged	Tagged	Tagged
3	☑	VLAN7	22	□	□	☑	□	Tagged	Tagged	Untagged	Tagged
4	☑	VLAN8	8	□	□	□	☑	Tagged	Tagged	Tagged	Untagged

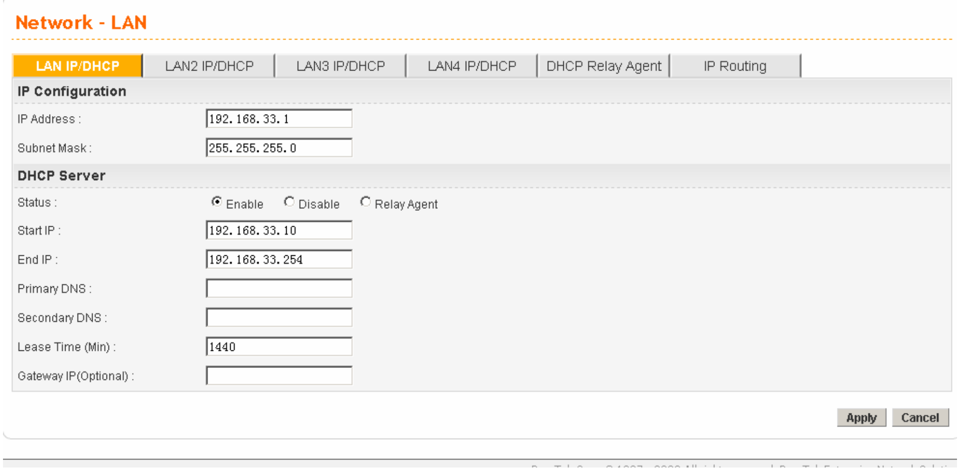
☑ Enable management port for P4

□ Enable packet forwarding between VLANs

Port Setting

	P1	P2	P3	P4
Port VLAN ID	20	21	22	8

2. Next, open **Network>>LAN**. Set two LAN subnet: LAN1 192.168.33.0/24 and LAN2 192.168.10.0/24.



Network - LAN

IP Configuration

IP Address : 192.168.33.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : ● Enable ○ Disable ○ Relay Agent

Start IP : 192.168.33.10

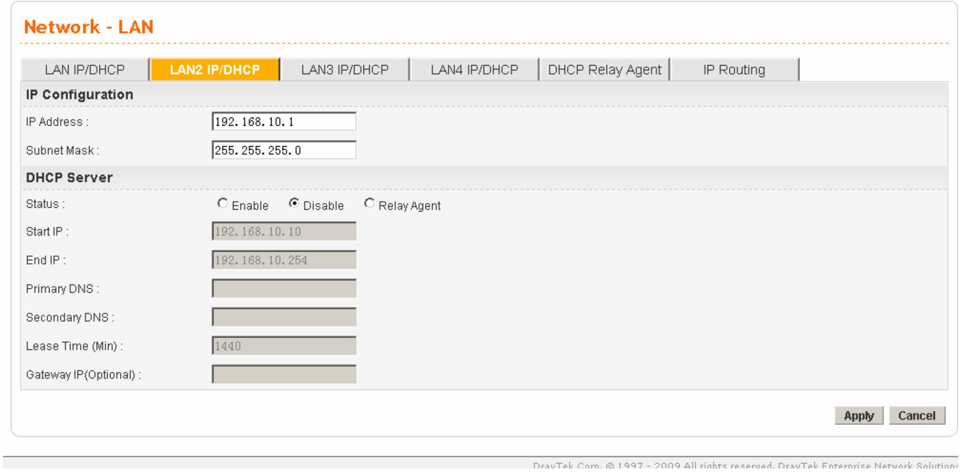
End IP : 192.168.33.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :



Network - LAN

LAN IP/DHCP
LAN2 IP/DHCP
LAN3 IP/DHCP
LAN4 IP/DHCP
DHCP Relay Agent
IP Routing

IP Configuration

IP Address : 192.168.10.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : ○ Enable ● Disable ○ Relay Agent

Start IP : 192.168.10.10

End IP : 192.168.10.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

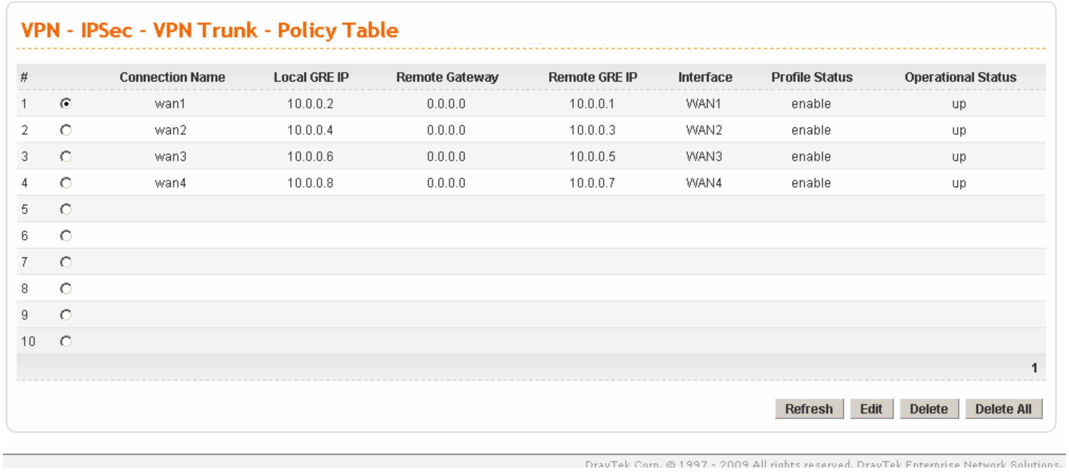
Gateway IP(Optional) :

Apply
Cancel
DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solution

3. Click **Apply**.

4. Open **VPN>>IPSec>>VPN Trunk>>Policy Table** to create VPN Trunk policy. The way

to configure the setting is the same as Scenario 1.

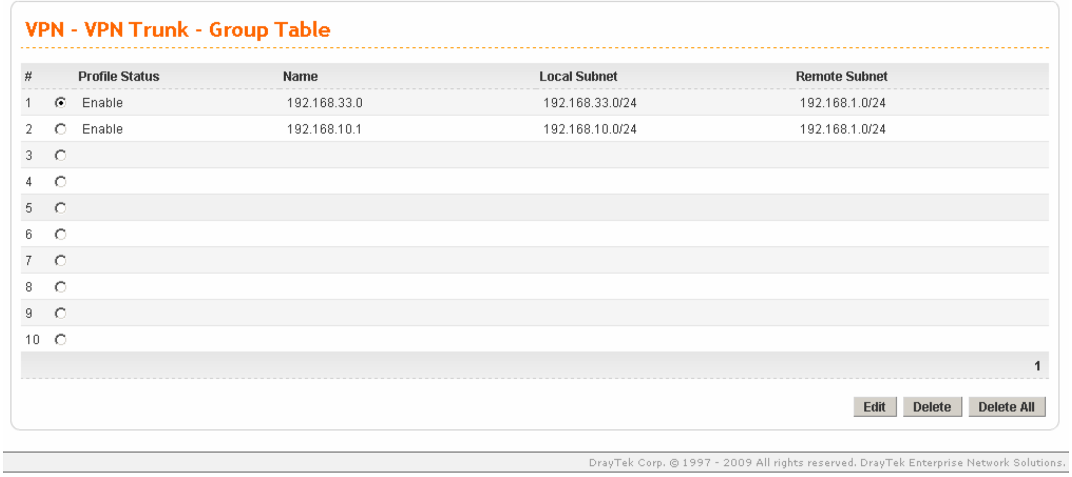


VPN - IPSec - VPN Trunk - Policy Table

#		Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1	●	wan1	10.0.0.2	0.0.0.0	10.0.0.1	WAN1	enable	up
2	○	wan2	10.0.0.4	0.0.0.0	10.0.0.3	WAN2	enable	up
3	○	wan3	10.0.0.6	0.0.0.0	10.0.0.5	WAN3	enable	up
4	○	wan4	10.0.0.8	0.0.0.0	10.0.0.7	WAN4	enable	up
5	○							
6	○							
7	○							
8	○							
9	○							
10	○							

1
Refresh
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solutions.

5. Open **VPN>>VPN Trunk>>Group Table** to group these VPN policies. Group two VPN policies as the following figure and then click **Apply**. The way to configure the setting is the same as Scenario 1.



VPN - VPN Trunk - Group Table

#		Profile Status	Name	Local Subnet	Remote Subnet
1	●	Enable	192.168.33.0	192.168.33.0/24	192.168.1.0/24
2	○	Enable	192.168.10.1	192.168.10.0/24	192.168.1.0/24
3	○				
4	○				
5	○				
6	○				
7	○				
8	○				
9	○				
10	○				

1
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solutions.

Now, two-pair VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24) has be established.

6 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.

6.1 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.

ACT
DrayTek
ACT
VPN
CSM
USB
WAN1
WAN3
DoS
WAN2
WAN4
Factory Reset

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.

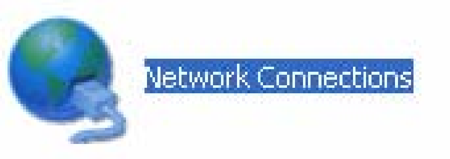
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

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.

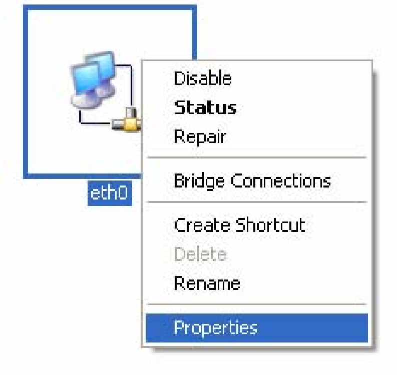
For Windows

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

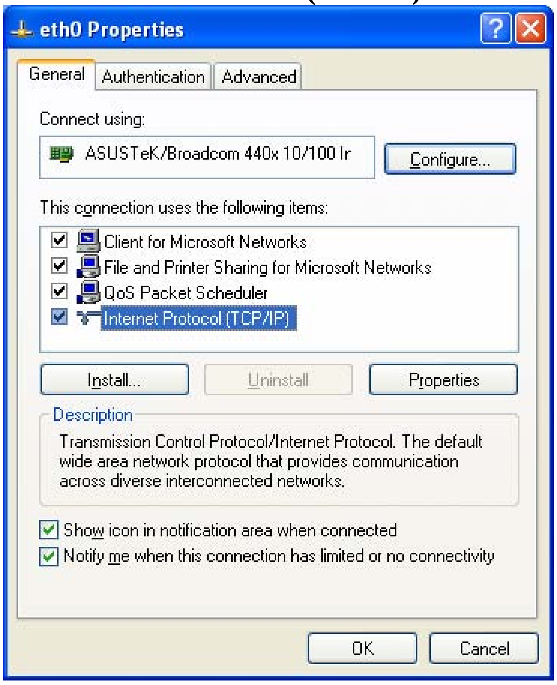
1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on **Local Area Connection** and click on **Properties**.



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



Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir

This connection uses the following items:

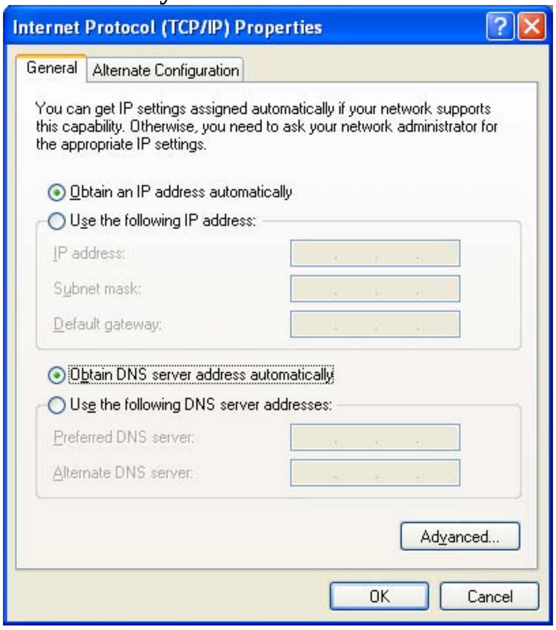
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

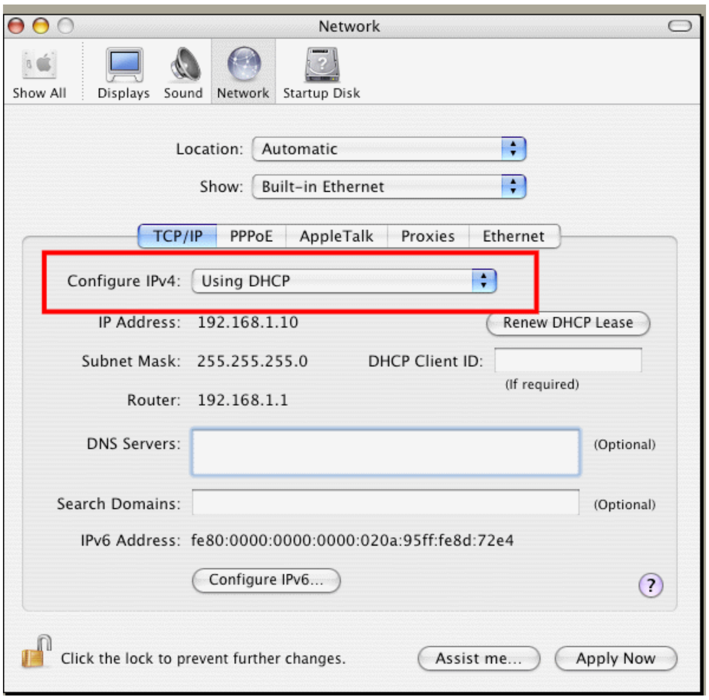
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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.



Network

Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.1

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

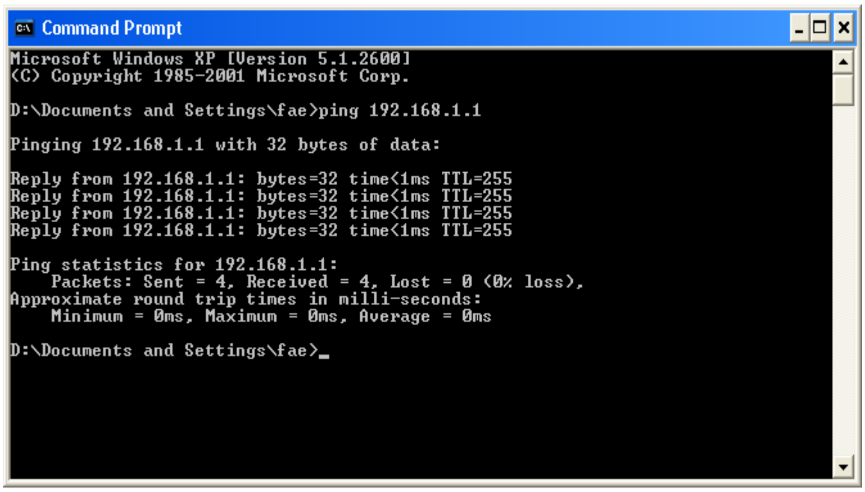
6.3 Pinging the Router from Your Computer

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 6.2)

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). The DOS command dialog will appear.

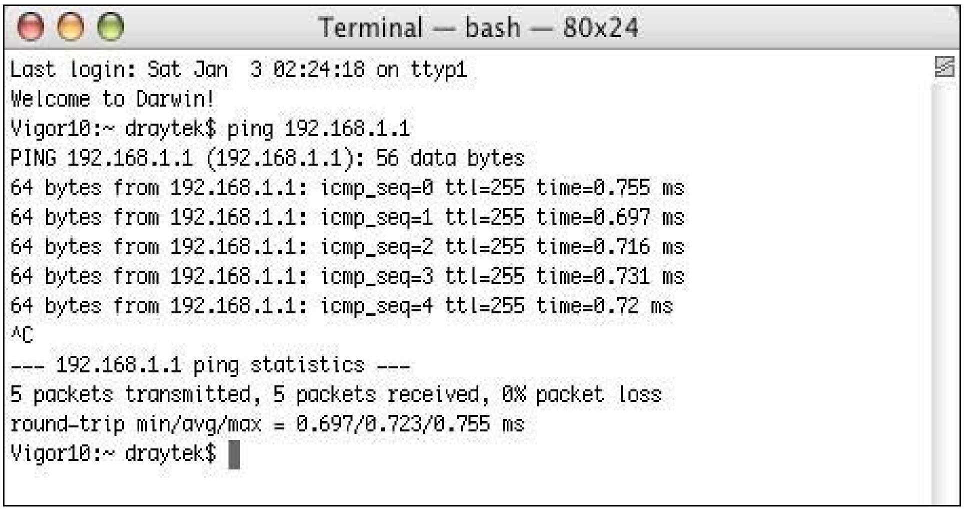


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

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

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

For Mac OS (Terminal)

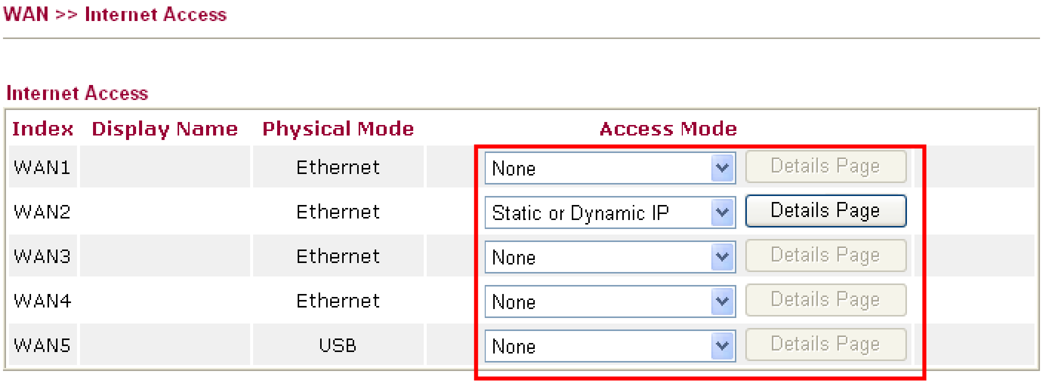
1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0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



```
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$ 
```

6.4 Checking If the ISP Settings are OK or Not

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



Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	None	Details Page
WAN2		Ethernet	Static or Dynamic IP	Details Page
WAN3		Ethernet	None	Details Page
WAN4		Ethernet	None	Details Page
WAN5		USB	None	Details Page

6.5 Problems for 3G Network Connection

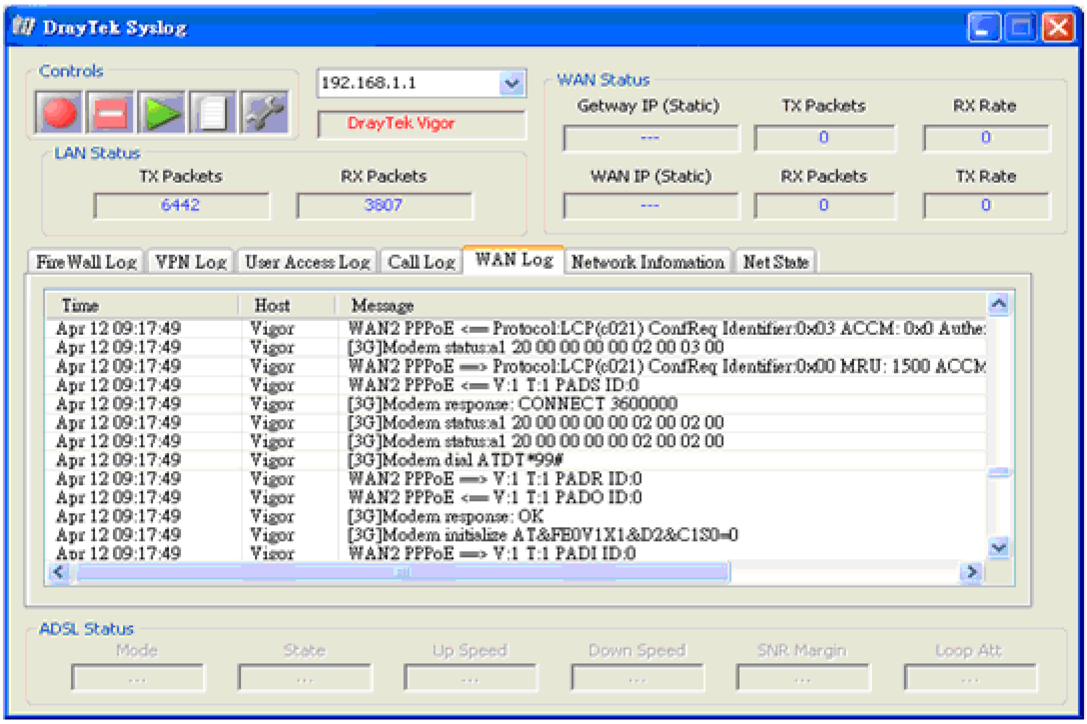
When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor3200. 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 Vigor3200.

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 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.



192.168.1.1

LAN Status: TX Packets 6442, RX Packets 3807

WAN Status: Getway IP (Static) ---, TX Packets 0, RX Rate 0, WAN IP (Static) ---, RX Packets 0, TX Rate 0

```
Time             Host    Message
Apr 12 09:17:49  Vigor   WAN2 PPPoE <== Protocol:LCP(c021) ConfReq Identifier:0x03 ACCM: 0x0 Authe:
Apr 12 09:17:49  Vigor   [3G]Modem status:a1 20 00 00 00 00 02 00 03 00
Apr 12 09:17:49  Vigor   WAN2 PPPoE ==> Protocol:LCP(c021) ConfReq Identifier:0x00 MRU: 1500 ACCM
Apr 12 09:17:49  Vigor   WAN2 PPPoE <== V:1 T:1 PADS ID:0
Apr 12 09:17:49  Vigor   [3G]Modem response: CONNECT 3600000
Apr 12 09:17:49  Vigor   [3G]Modem status:a1 20 00 00 00 00 02 00 02 00
Apr 12 09:17:49  Vigor   [3G]Modem status:a1 20 00 00 00 00 02 00 02 00
Apr 12 09:17:49  Vigor   [3G]Modem dial ATDT*99#
Apr 12 09:17:49  Vigor   WAN2 PPPoE ==> V:1 T:1 PADR ID:0
Apr 12 09:17:49  Vigor   WAN2 PPPoE <== V:1 T:1 PADO ID:0
Apr 12 09:17:49  Vigor   [3G]Modem response: OK
Apr 12 09:17:49  Vigor   [3G]Modem initialize AT&FE0V1X1&D2&C1S0=0
Apr 12 09:17:49  Vigor   WAN2 PPPoE ==> V:1 T:1 PADI ID:0
```

ADSL Status: Mode ..., State ..., Up Speed ..., Down Speed ..., SNR Margin ..., Loop Att ...

Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor3200. In addition, please refer to the manual of 3G 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.

6.6 Backing to Factory Default Setting If Necessary

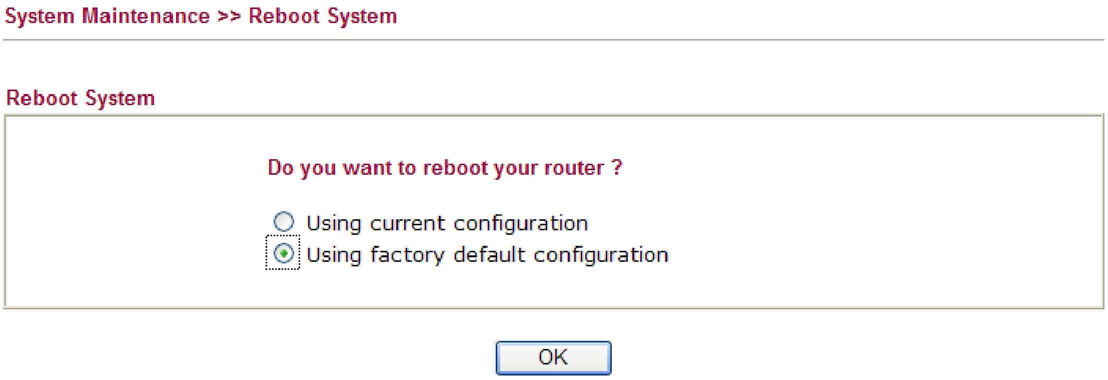
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

> **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. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

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



System Maintenance >> Reboot System

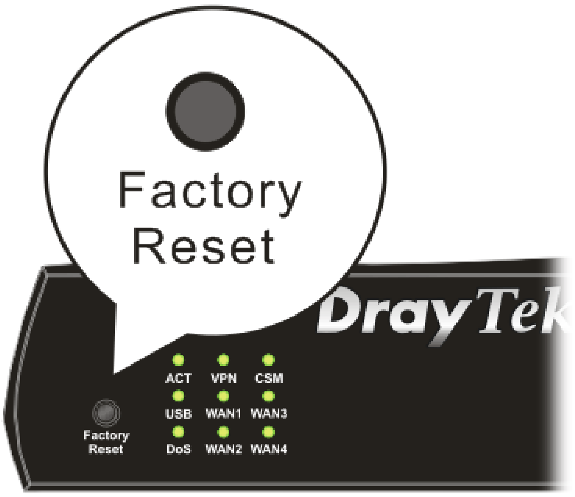
Reboot System

Do you want to reboot your router ?

○ Using current configuration
● Using factory default configuration

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.

6.7 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.