DrayTek

Vigor2130 Series

High Speed Gigabit Router

Your reliable networking solutions partner

User's Guide

V 1.1

Vigor2130 Series
High Speed Gigabit Router
User's Guide

Version: 1.1

Date: 25/11/2009

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 County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor2130 Series Router

DrayTek Corp. declares that Vigor2130 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 use 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 form 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 Preface

The Vigor2130 series are the routers with high speed in data transmission through WAN port and LAN ports. With hardware NAT acceleration, the rate of Vigor2130 series can be greater than 900Mbps almost.

With the development of NGN (Next Generation Network), you may recently hear the news about FTTx deployment in your local area or even have already subscribed the unbundling last mile service (e.g. VDSL2) from local ITSP for FTTx. As adopting FTTx, the main question for end users is whether your legacy router could fully utilize its bandwidth or not.

For example, you purchase a 120 Mbps Internet connection from your ISP but your existing router cannot support 90 Mbps throughput. That's why DrayTek launches Vigor 2130 series – High speed Gigabit router, perfectly complied with VDSL2 environment including Vigor2130, Vigor2130n and Vigor2130Vn for speed-wanted customers. With high throughput performance and secured broadband connectivity provided by Vigor 2130 series, you can simultaneously engage these bandwidth-intensive applications, such as high-definition video streaming, online gaming, and Internet telephony / access.

1.1 Web Configuration Buttons Explanation

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

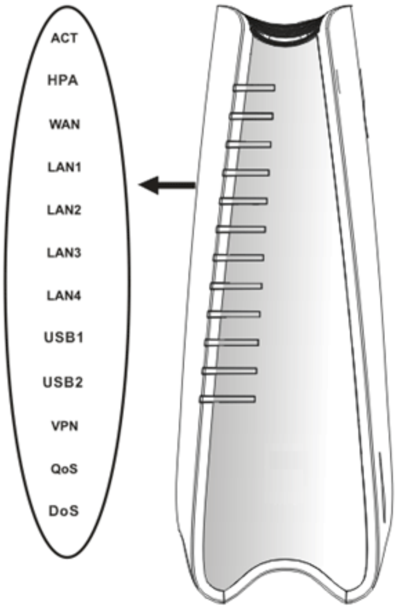
OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified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

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

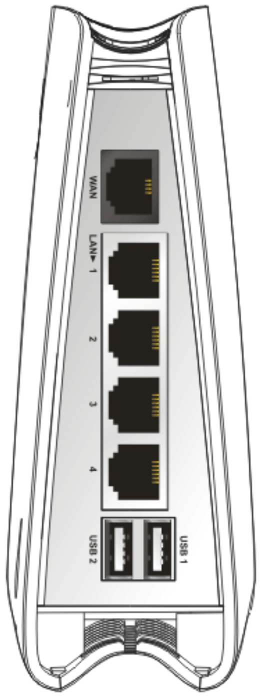
1.2 LED Indicators and Connectors

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

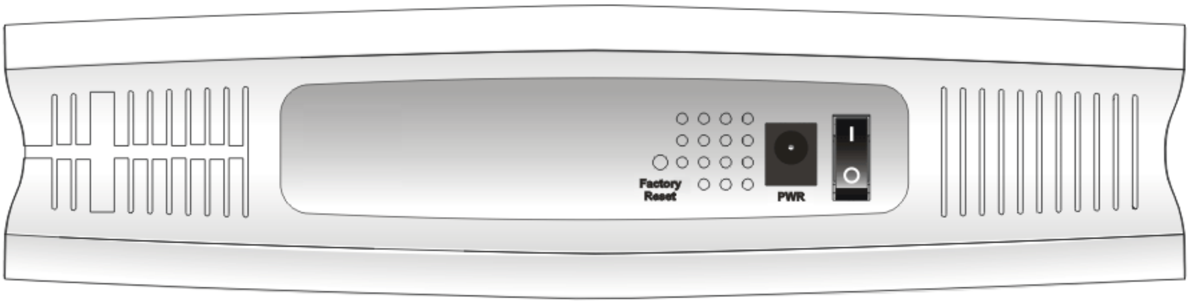
1.2.1 For Vigor2130



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
HPA	On	Hardware NAT is enabled.
	Off	Hardware NAT is disabled.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.
LAN1/2/3/4	On	The port is connected.
	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB1/2	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.

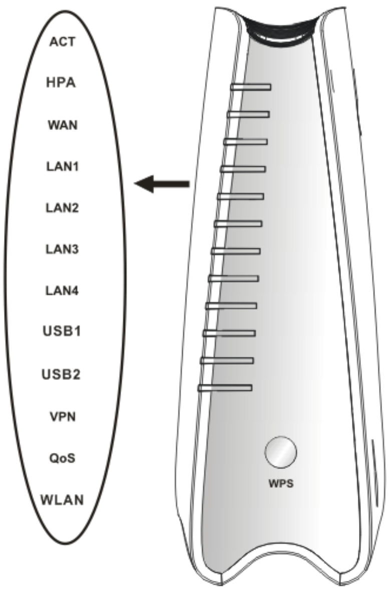


Interface	Description
WAN	Connector for accessing the Internet.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.

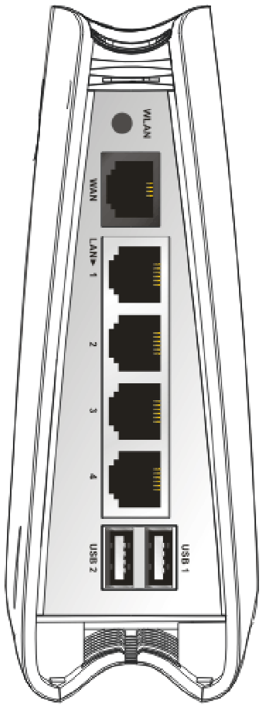


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

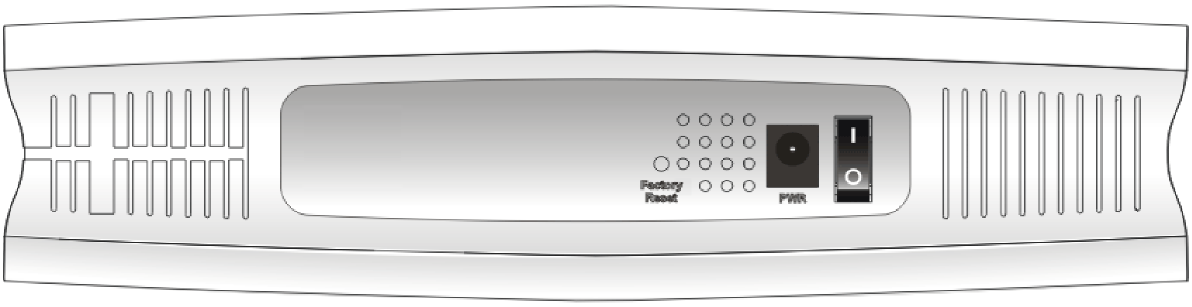
1.2.2 For Vigor2130n



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
HPA	On	Hardware NAT is enabled.
	Off	Hardware NAT is disabled.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.
LAN1/2/3/4	On	The port is connected.
	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB1/2	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes through.
WPS Button	On	Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS connection will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about two minutes.

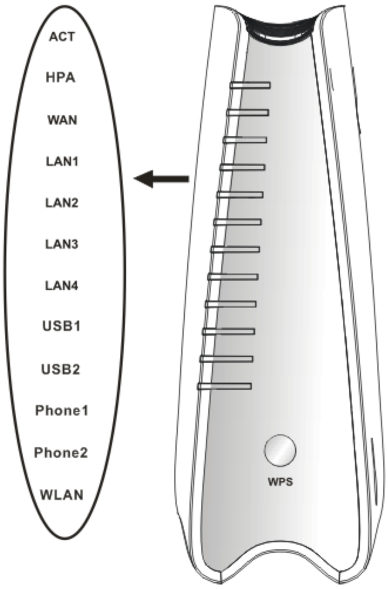


Interface	Description
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
WAN	Connector for accessing the Internet.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for USB storage (Pen Driver /Mobile HD) or printer.

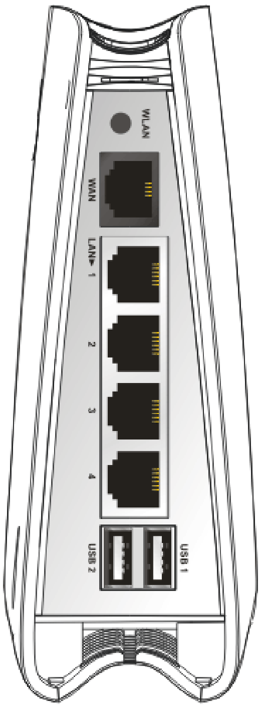


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

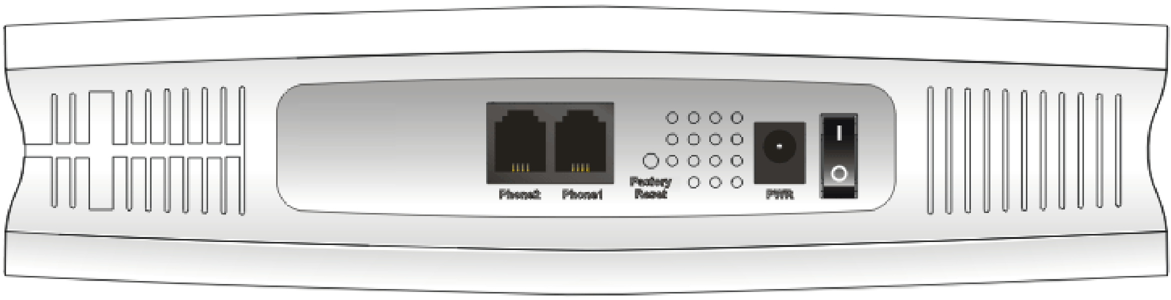
1.2.3 For Vigor2130Vn



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
HPA	On	Hardware NAT is enabled.
	Off	Hardware NAT is disabled.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.
LAN1/2/3/4	On	The port is connected.
	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB1/2	On	A USB device is connected and active.
	Blinking	The data is transmitting.
Phone1/ Phone2	On	The phone connected to this port is off-hook.
	Off	The phone connected to this port is on-hook.
	Blinking	A phone call comes.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes through.
WPS Button	On	Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS connection will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about two minutes.



Interface	Description
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
WAN	Connector for accessing the Internet.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for USB storage (Pen Driver/Mobile HD) or printer.

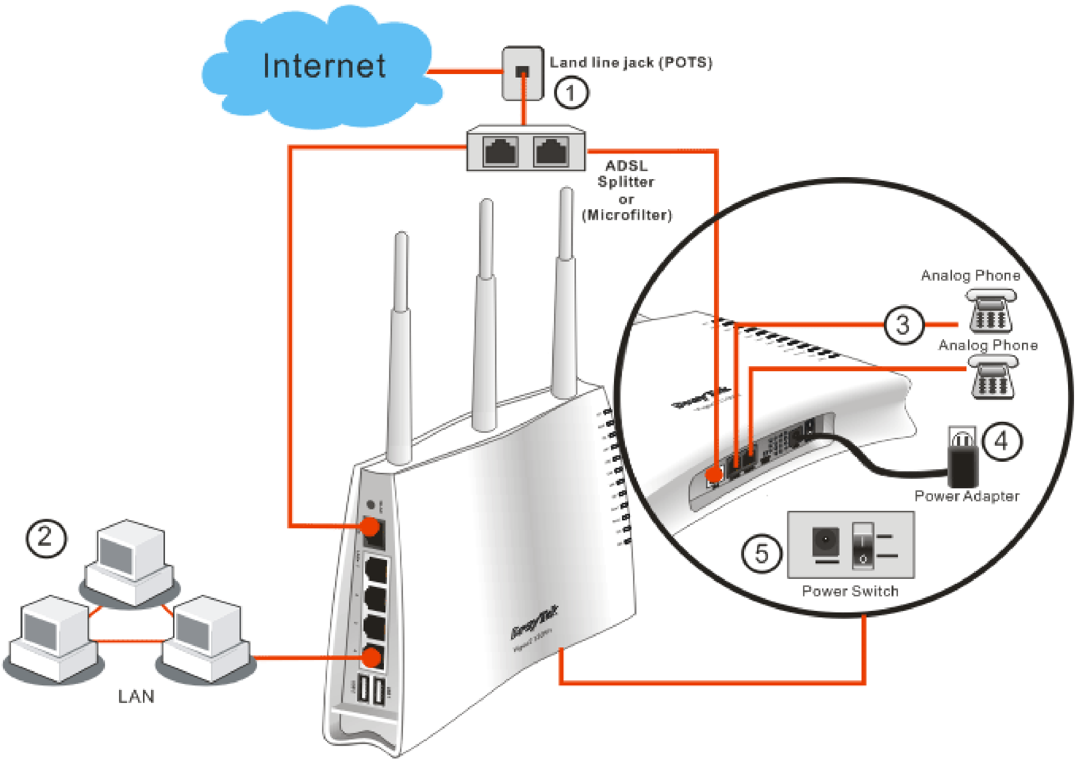


Interface	Description
Phone2/Phone1	Connector of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector 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 Line port to land line jack with a RJ-11 cable (Vn model).
2. Connect this device to a modem with an Ethernet cable.
3. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
4. Connect Phone port to a conventional analog telephone.
5. Connect detachable antennas to the router for Vigor2130 series (n model).
6. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
7. Power on the router.
8. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connections.



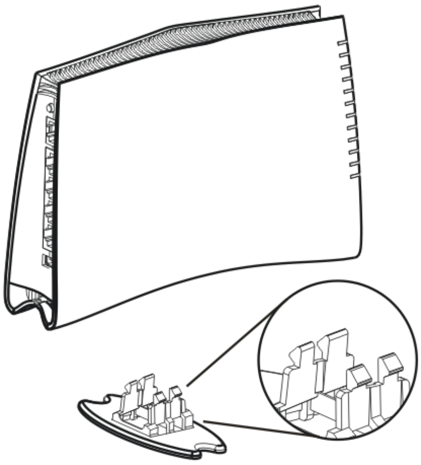
(For the detailed information of LED status, please refer to section 1.1.)

> **Caution**:
> 1. Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the land line jack. Such connection might damage your router.
> 2. When the power is shutdown, VoIP phone will be disconnected. However, a phone set connected to Phone 2 port can be used as the traditional telephone for the line will be guided to land line jack via the router (loop through).

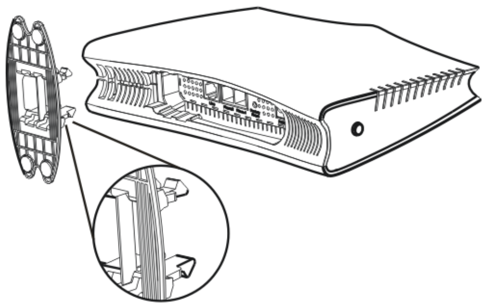
Stand Installation

The Vigor2130 must be placed erectly. Therefore you have to install a stand onto the router to make it standing firmly. Please follow the figures listed below to finish the installation.

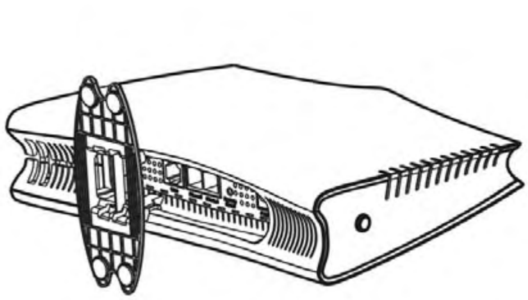
①



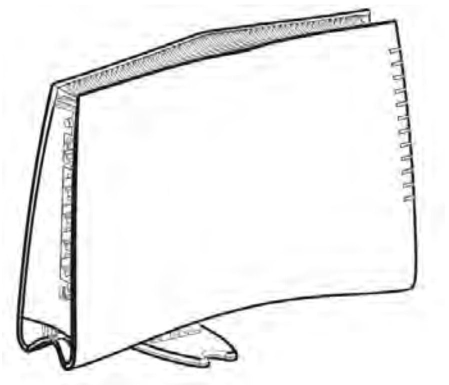
②



③

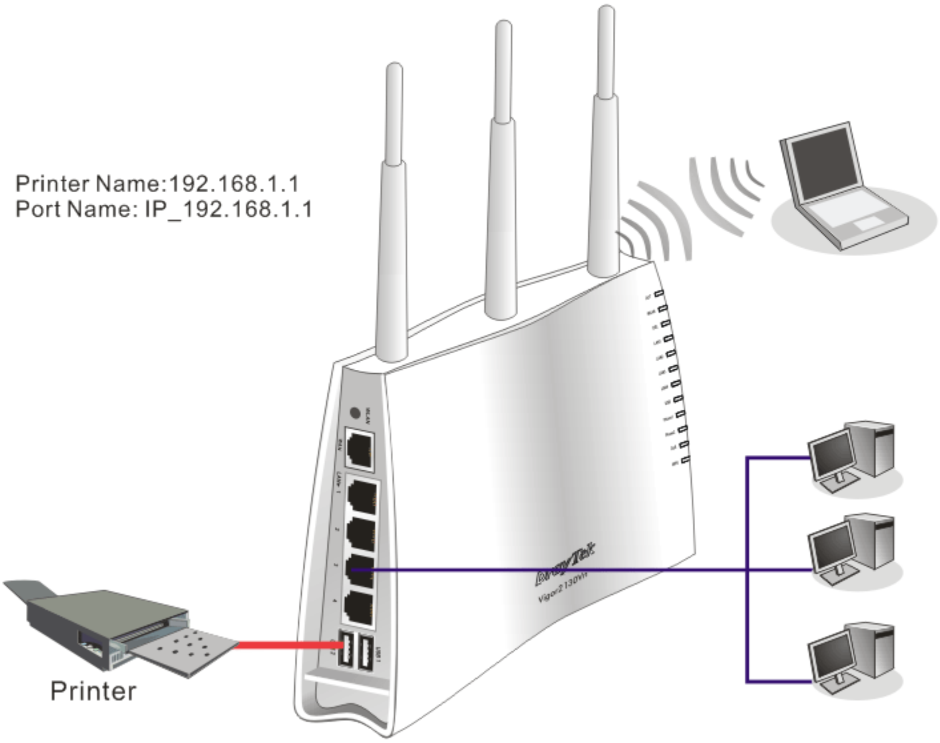


④



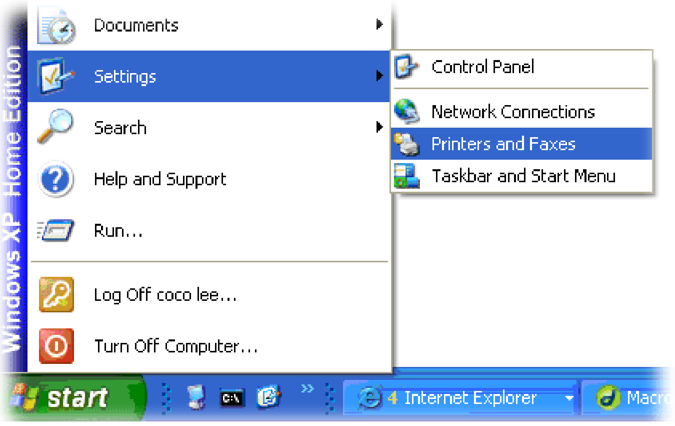
1.4 Printer Installation

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**.

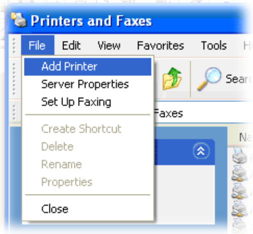


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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



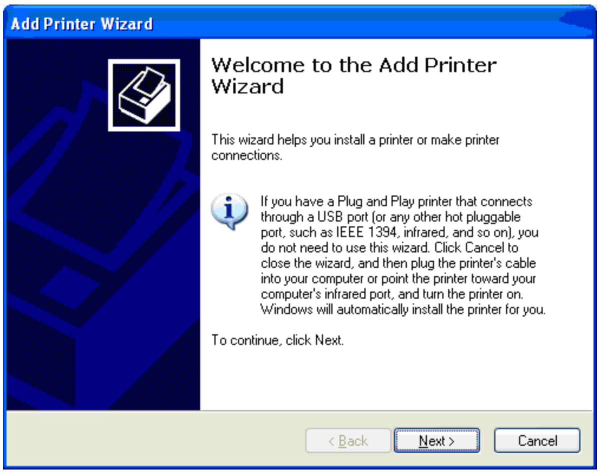
3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



Printers and Faxes

File Edit View Favorites Tools

Add Printer
Server Properties
Set Up Faxing
Create Shortcut
Delete
Rename
Properties
Close



Add Printer Wizard

Welcome to the Add Printer Wizard

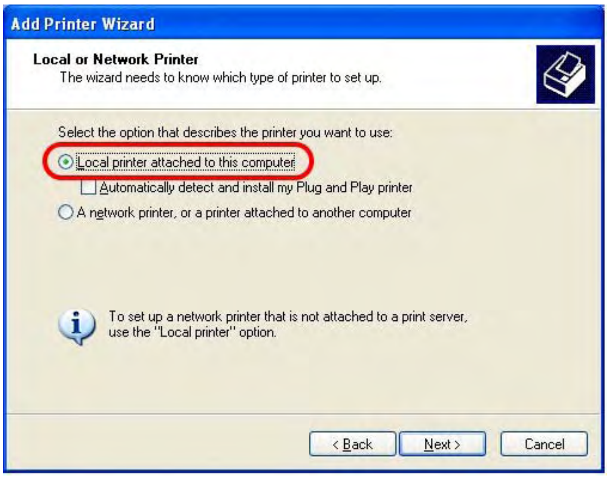
This wizard helps you install a printer or make printer connections.

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.

< Back | Next > | Cancel

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.

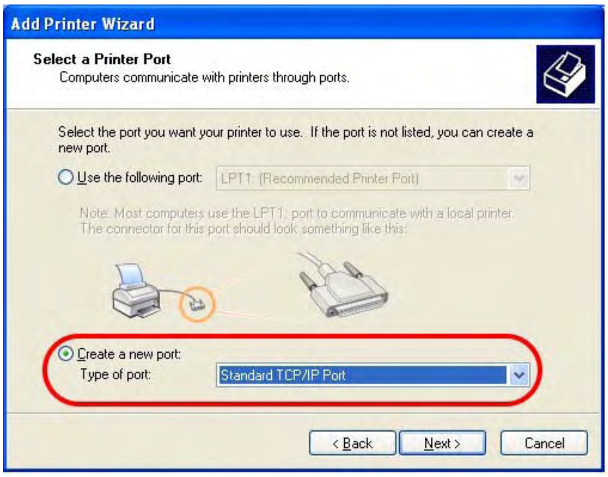
Select the option that describes the printer you want to use:

● 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.

< Back | Next > | Cancel

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.

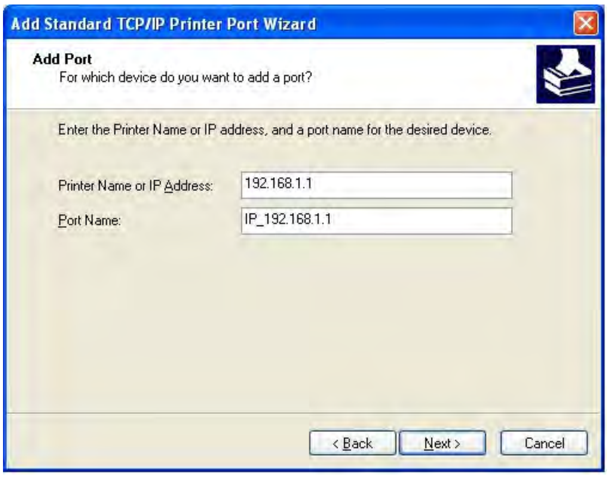
○ Use the following port: LPT1: (Recommended Printer Port)

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

< Back | Next > | Cancel

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

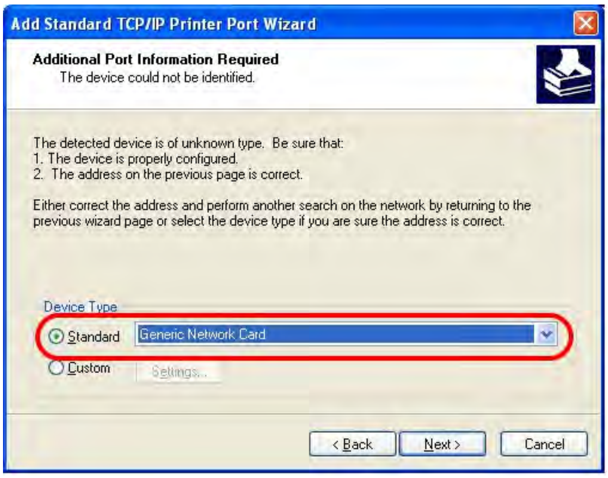
Add Port
For which device do you want to add a port?

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

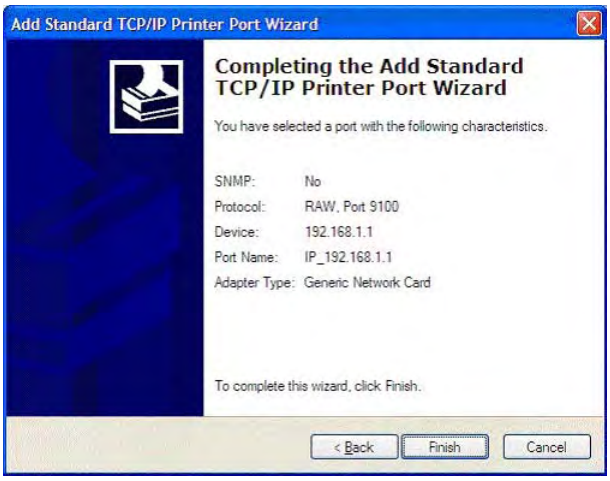
Additional Port Information Required
The device could not be identified.

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 Settings...

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



Add Standard TCP/IP Printer Port Wizard

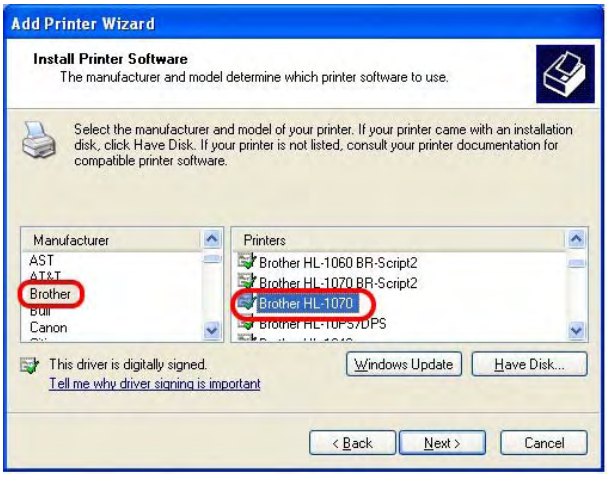
Completing the Add Standard TCP/IP Printer Port Wizard

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

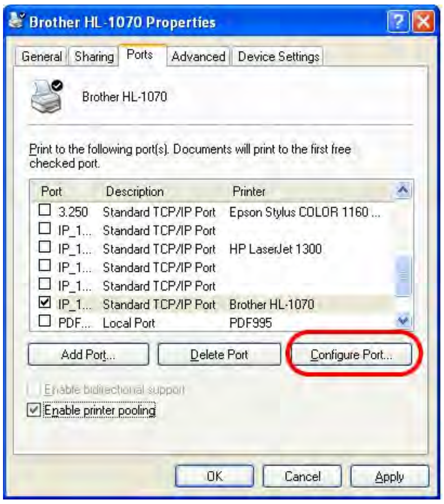
Install Printer Software
The manufacturer and model determine which printer software to use.

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

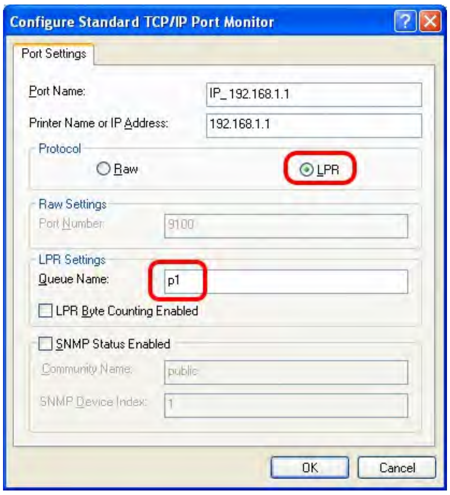
Brother HL-1070

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 UPR 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

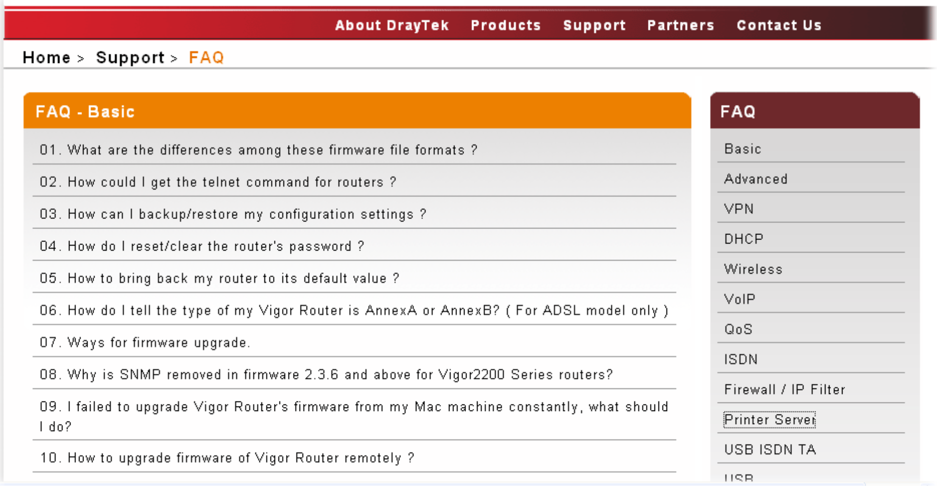
LPR Settings
Queue Name: p1

□ 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 click the **What types of printers are compatible with Vigor router**? link.



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 ?

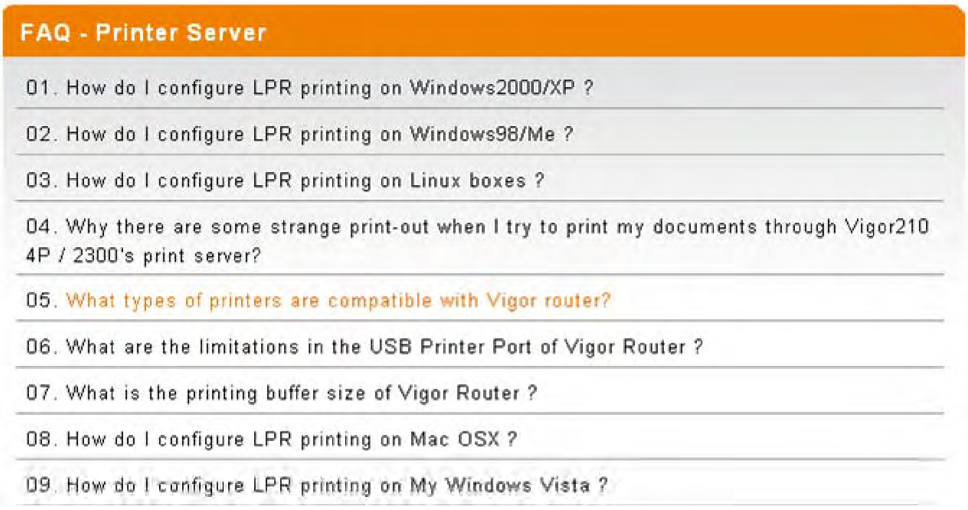
06. How do I tell the type of my Vigor Router is AnnexA or AnnexB? (For ADSL model only)

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 LAN ports but not WAN port.

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.

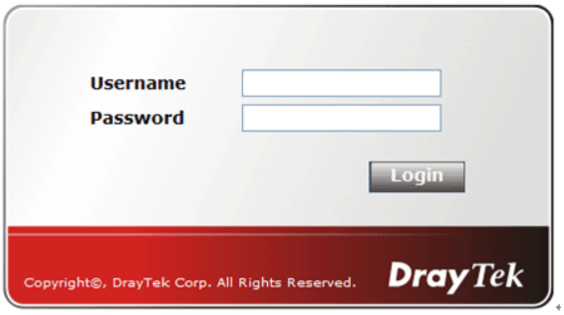
For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type “admin/admin” on Username/Password and click **Login** for full configuration.

2.2 Accessing Web Page

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

Notice: 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.

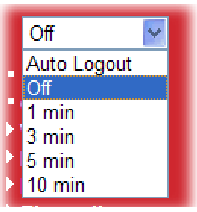
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.



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.

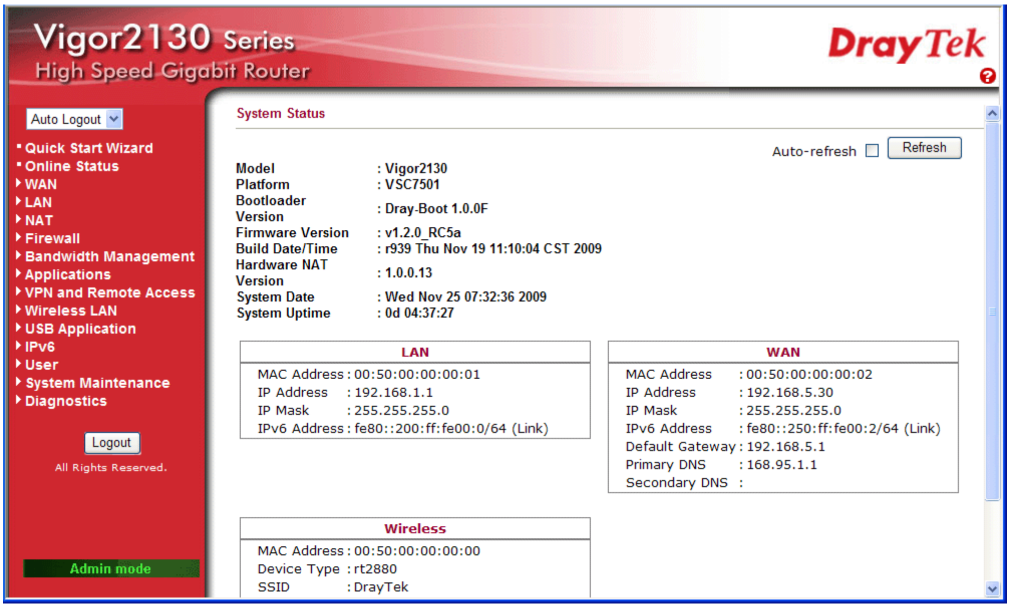
4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



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

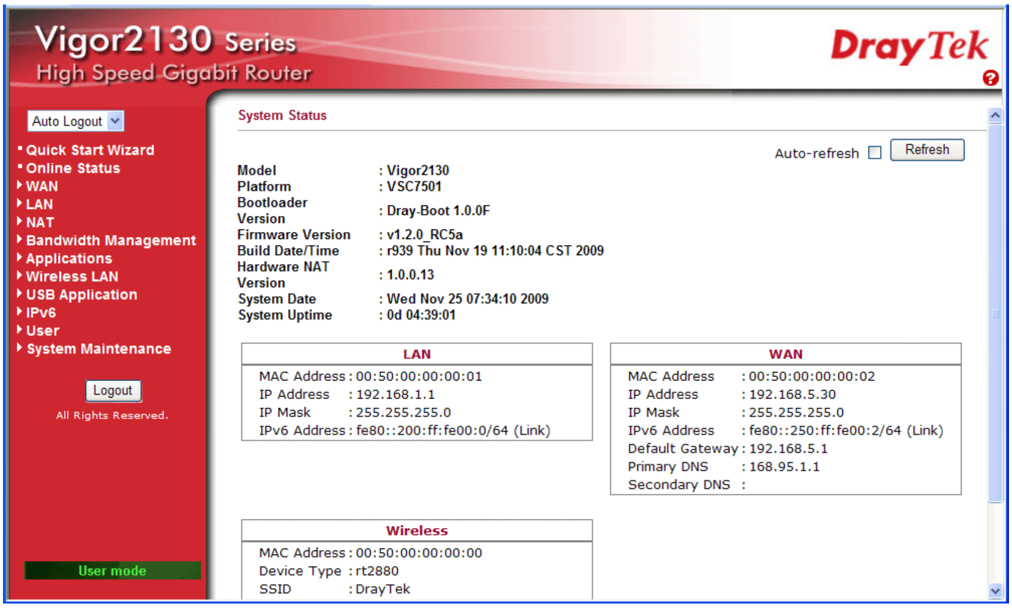
Model : Vigor2130
Platform : VSC7501
Bootloader Version : Dray-Boot 1.0.0F
Firmware Version : v1.2.0_RC5a
Build Date/Time : r939 Thu Nov 19 11:10:04 CST 2009
Hardware NAT Version : 1.0.0.13
System Date : Wed Nov 25 07:32:36 2009
System Uptime : 0d 04:37:27

LAN
MAC Address : 00:50:00:00:00:01
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::200:ff:fe00:0/64 (Link)

WAN
MAC Address : 00:50:00:00:00:02
IP Address : 192.168.5.30
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:ff:fe00:2/64 (Link)
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

Wireless
MAC Address : 00:50:00:00:00:00
Device Type : rt2880
SSID : DrayTek

Main screen for admin mode operation (full configuration)



System Status

Model : Vigor2130
Platform : VSC7501
Bootloader Version : Dray-Boot 1.0.0F
Firmware Version : v1.2.0_RC5a
Build Date/Time : r939 Thu Nov 19 11:10:04 CST 2009
Hardware NAT Version : 1.0.0.13
System Date : Wed Nov 25 07:34:10 2009
System Uptime : 0d 04:39:01

LAN
MAC Address : 00:50:00:00:00:01
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::200:ff:fe00:0/64 (Link)

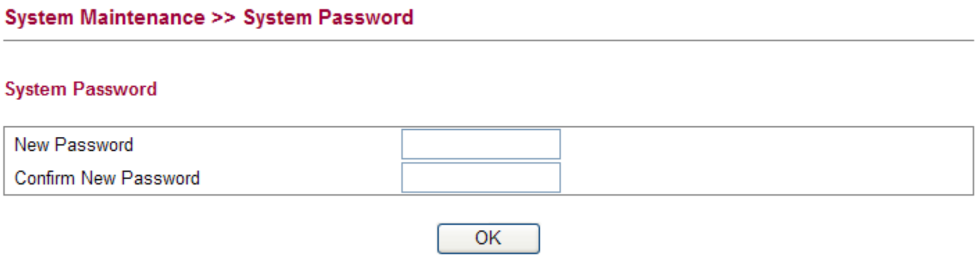
WAN
MAC Address : 00:50:00:00:00:02
IP Address : 192.168.5.30
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:ff:fe00:2/64 (Link)
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

Wireless
MAC Address : 00:50:00:00:00:00
Device Type : rt2880
SSID : DrayTek

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 **System Password/User Password**.



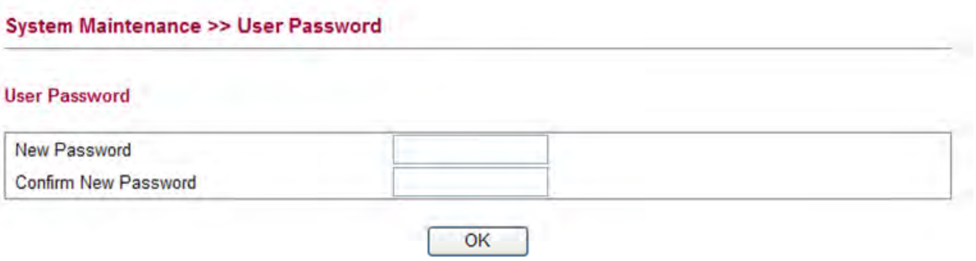
System Maintenance >> System Password

System Password

New Password

Confirm New Password

Or



System Maintenance >> User Password

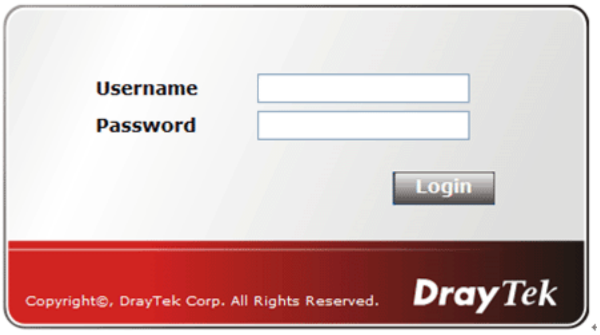
User Password

New Password

Confirm New Password

5. Type **New Password** in New Password and Confirm New Password fields. 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.



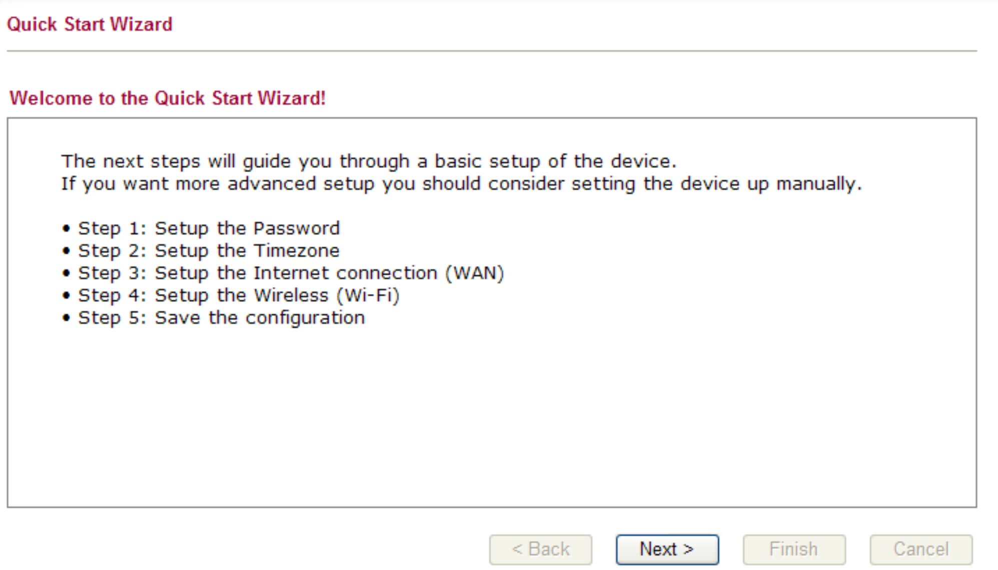
Username

Password

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 welcome page, please click **Next**.



Quick Start Wizard

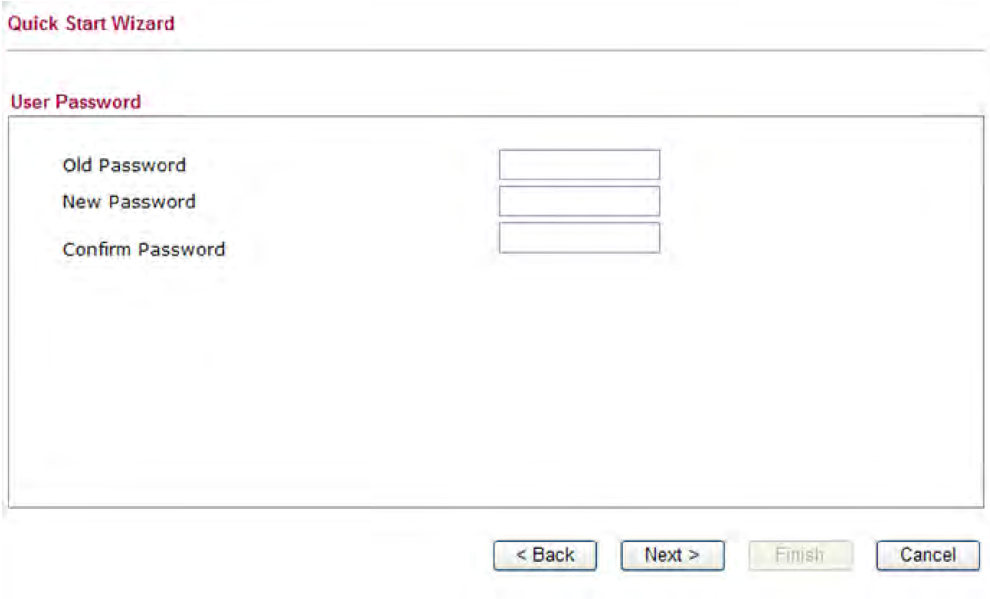
Welcome to the Quick Start Wizard!

The next steps will guide you through a basic setup of the device.
If you want more advanced setup you should consider setting the device up manually.

- Step 1: Setup the Password
- Step 2: Setup the Timezone
- Step 3: Setup the Internet connection (WAN)
- Step 4: Setup the Wireless (Wi-Fi)
- Step 5: Save the configuration

2.4.1 Setting up the Password

The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.



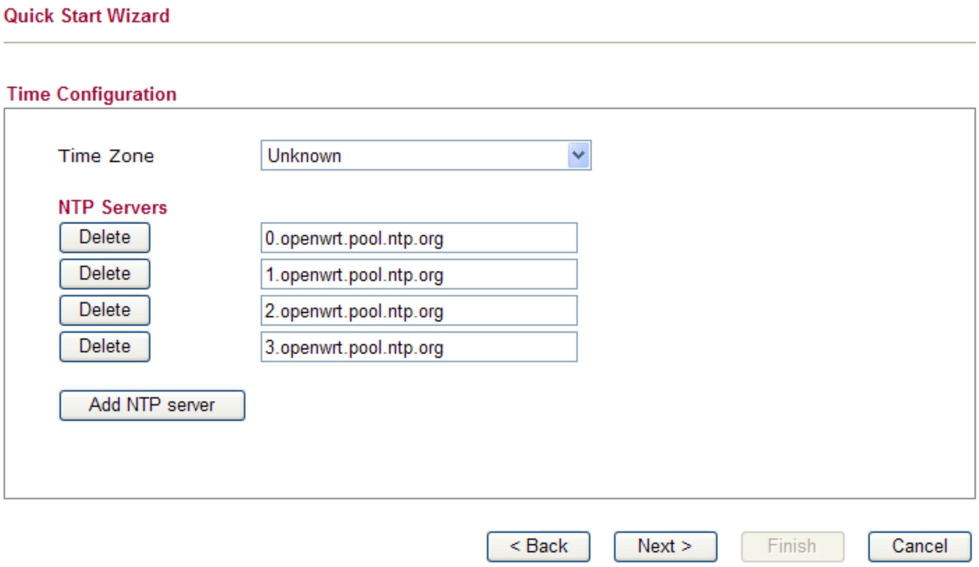
Quick Start Wizard

User Password

Old Password
New Password
Confirm Password

2.4.2 Setting up the Time Zone

On the next page as shown below, please select the Time Zone for the router installed and specify the NTP server(s). Then click **Next** for next step.



Quick Start Wizard

Time Configuration

Time Zone: Unknown

NTP Servers

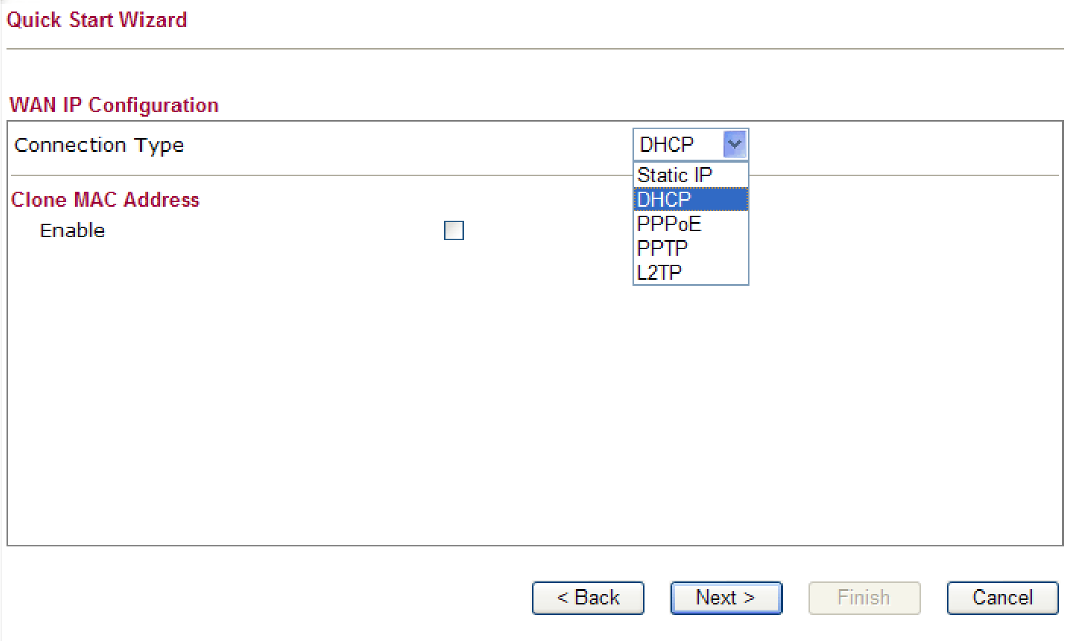
Delete 0.openwrt.pool.ntp.org
Delete 1.openwrt.pool.ntp.org
Delete 2.openwrt.pool.ntp.org
Delete 3.openwrt.pool.ntp.org

Add NTP server

< Back | Next > | Finish | Cancel

2.4.3 Setting up the Internet Connection

On the next page as shown below, please select the appropriate connection type according to the information from your ISP. There are five types offered in this page. Each connection type will bring out different web page.



Quick Start Wizard

WAN IP Configuration

Connection Type: DHCP

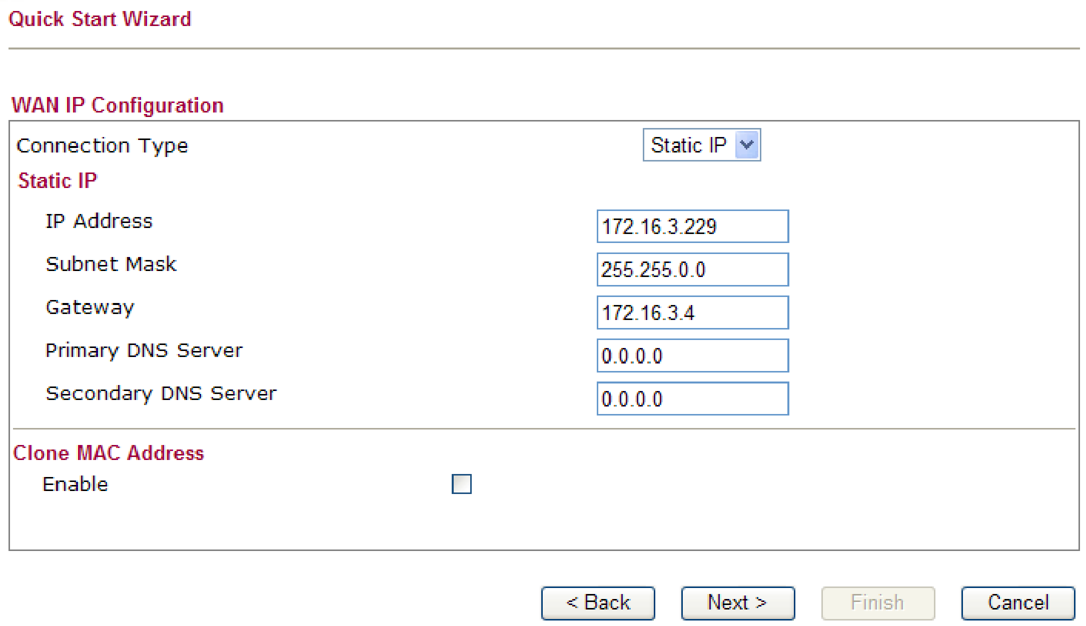
Clone MAC Address

Enable □

< Back | Next > | Finish | Cancel

Static IP

You will 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.



Quick Start Wizard

WAN IP Configuration

Connection Type: Static IP

Static IP

IP Address: 172.16.3.229

Subnet Mask: 255.255.0.0

Gateway: 172.16.3.4

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Clone MAC Address

Enable □

IP Address Type the IP address.

Subnet Mask Type the subnet mask.

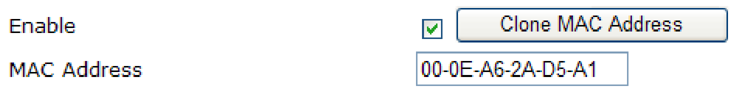
Gateway Type the gateway IP address.

Primary DNS Server Type in the primary IP address for the router

Secondary DNS Server Type in secondary IP address for necessity in the future.

Enable The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.

Clone MAC Address It is available when the box of Enable is checked. Click Clone PC Address. The result will be displayed in the field of MAC Address.



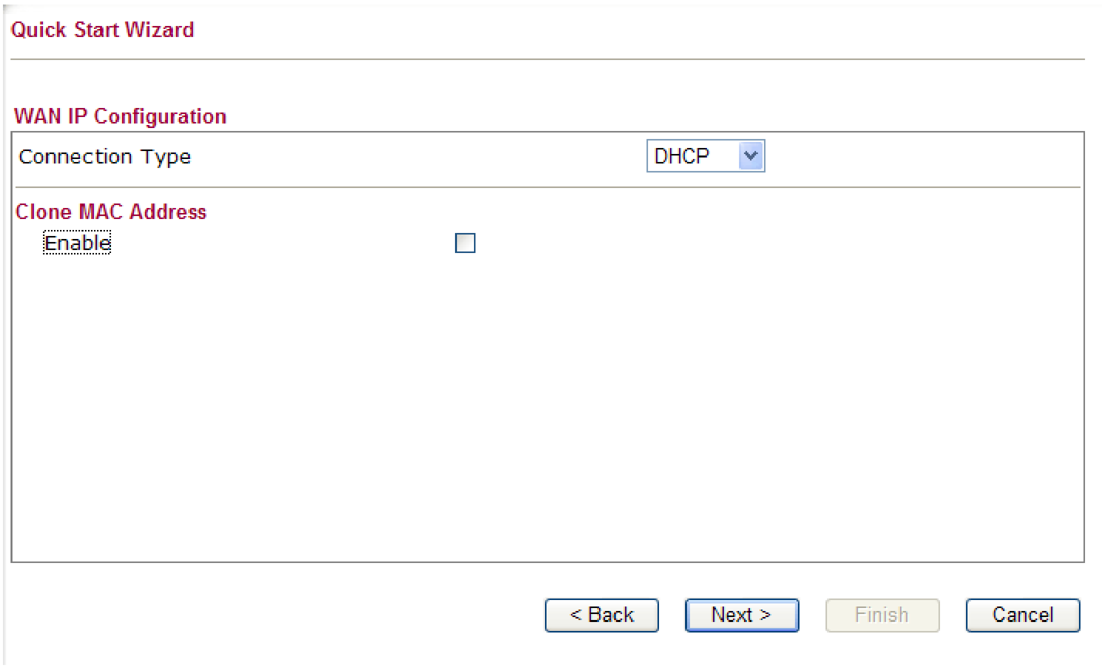
Enable ☑

MAC Address: 00-0E-A6-2A-D5-A1

After finishing the settings here, please click **Next.**

DHCP

It is not necessary for you to type any IP address manually. Simply choose this type and the system will obtain the IP address automatically from DHCP server.



Quick Start Wizard

WAN IP Configuration

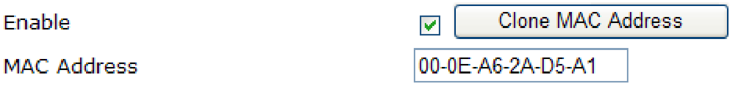
Connection Type: DHCP

Clone MAC Address

Enable □

Enable The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.

Clone MAC Address It is available when the box of Enable is checked. Click Clone PC Address. The result will be displayed in the field of MAC Address.



Enable ☑

MAC Address: 00-0E-A6-2A-D5-A1

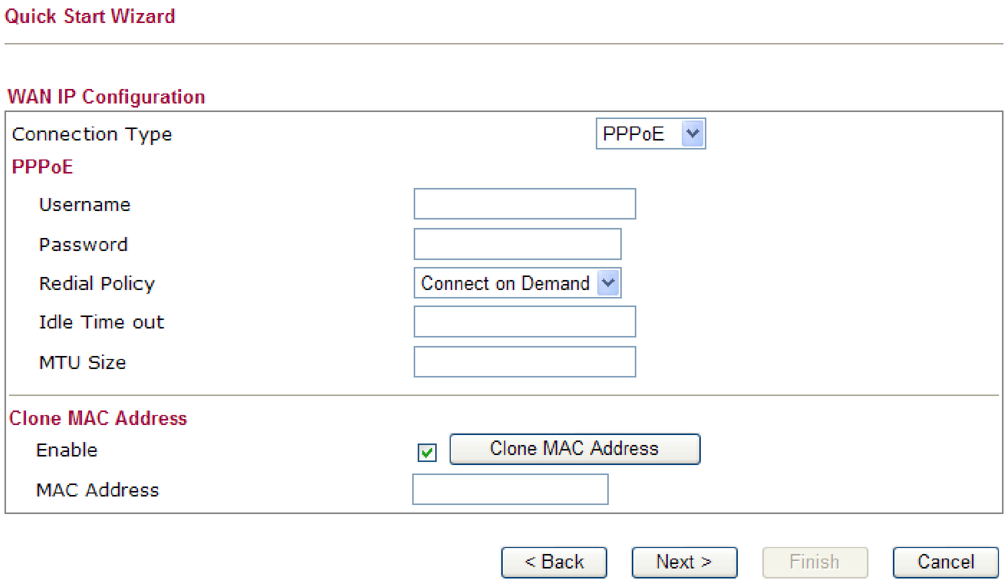
After finishing the settings here, please click **Next.**

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

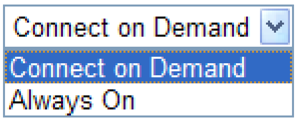
WAN IP Configuration

Connection Type	PPPoE
PPPoE	
Username	
Password	
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	
Clone MAC Address	
Enable	☑ Clone MAC Address
MAC Address	

User Name Assign a specific valid user name provided by the ISP.

Password Assign a valid password provided by the ISP.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.



Idle Time Out Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds. The range is XX ~ XX.

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

Enable The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.

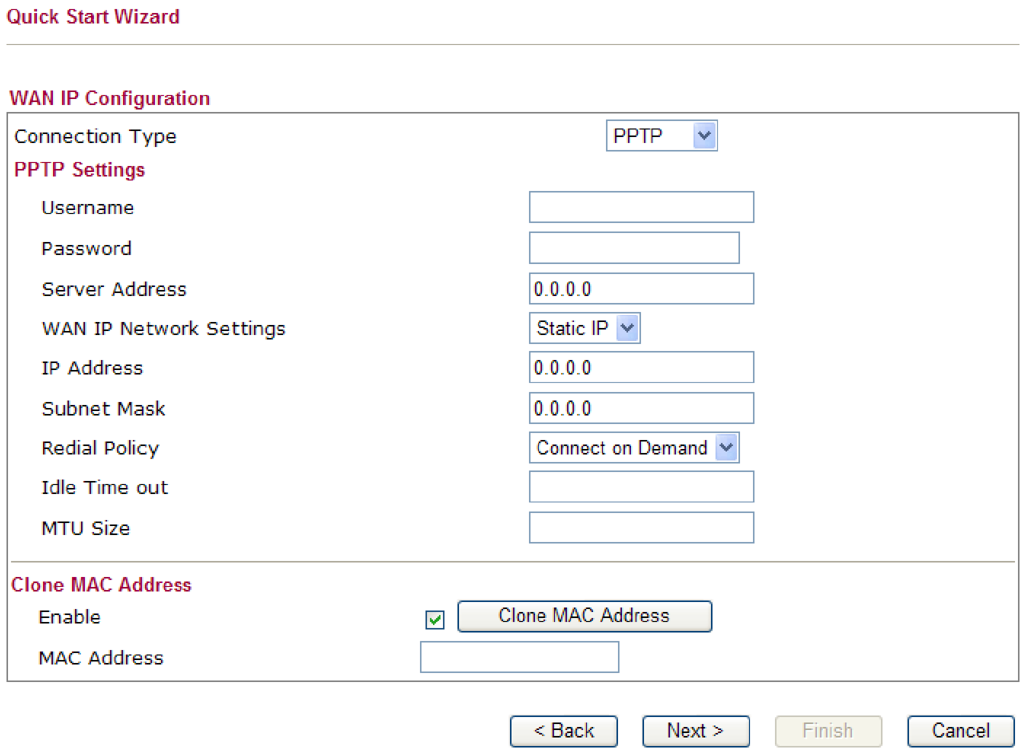
Clone MAC Address It is available when the box of Enable is checked. Click Clone PC Address. The result will be displayed in the field of MAC Address.

Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

After finishing the settings here, please click **Next.**

PPTP/L2TP

if you click PPTP/L2TP as the protocol, please manually enter the Username/Password provided by your ISP and all the required information.



Quick Start Wizard

WAN IP Configuration

Connection Type	PPTP
PPTP Settings	
Username	
Password	
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	
Clone MAC Address	
Enable	☑ Clone MAC Address
MAC Address	

User Name Assign a specific valid user name provided by the ISP.

Password Assign a valid password provided by the ISP.

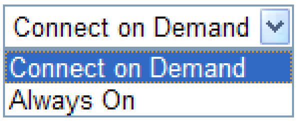
Server Address Specify the IP address of the PPTP server.

WAN IP Network Settings You can choose Static IP or DHCP as WAN IP network setting.

IP Address Type the IP address if you choose Static IP as the WAN IP network setting.

Subnet Mask Type the subnet mask if you chose Static IP as the WAN IP.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.

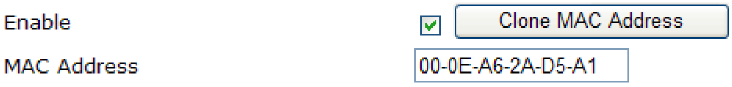


Idle Time Out Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds. The range is XX ~ XX.

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

Enable The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.

Clone MAC Address It is available when the box of Enable is checked. Click Clone PC Address. The result will be displayed in the field of MAC Address.



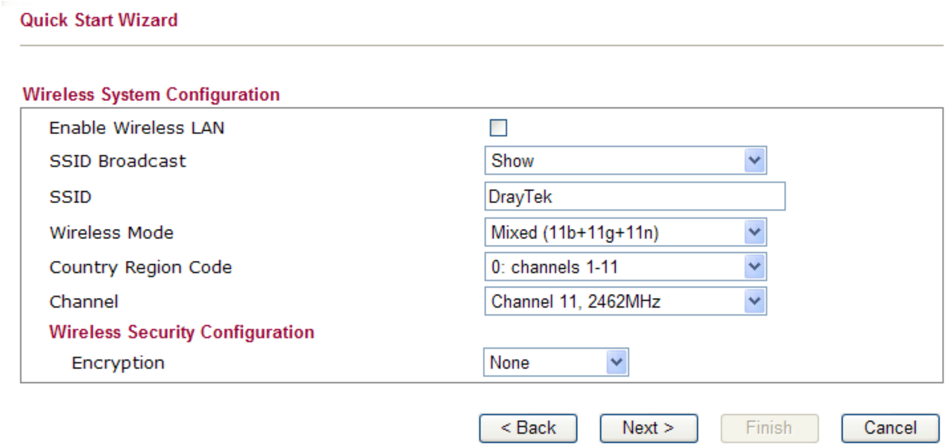
Enable ☑

MAC Address 00-0E-A6-2A-D5-A1

After finishing the settings here, please click **Next.**

2.4.4 Setting up the Wireless Connection

Now, you have to set up the wireless connection. For the user of Vigor2130, please skip this step.



Quick Start Wizard

Wireless System Configuration

Enable Wireless LAN	□
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz

Wireless Security Configuration

Encryption	None

Enable Wireless LAN Check the box to enable the wireless function.

SSID Broadcast Choose **Show** to make the SSID being seen by wireless clients. Choose **Hide** to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.

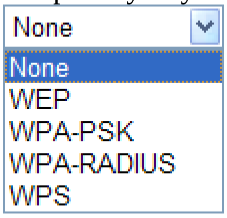
SSID It means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.

Wireless Mode Choose the wireless mode for this router. At present, only 802.11B/B/N mix is available.

Country Region Code Use the drop down list to choose the one that this router supports.

Channel It means the channel of frequency of the wireless LAN. The default channel is 11. 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.

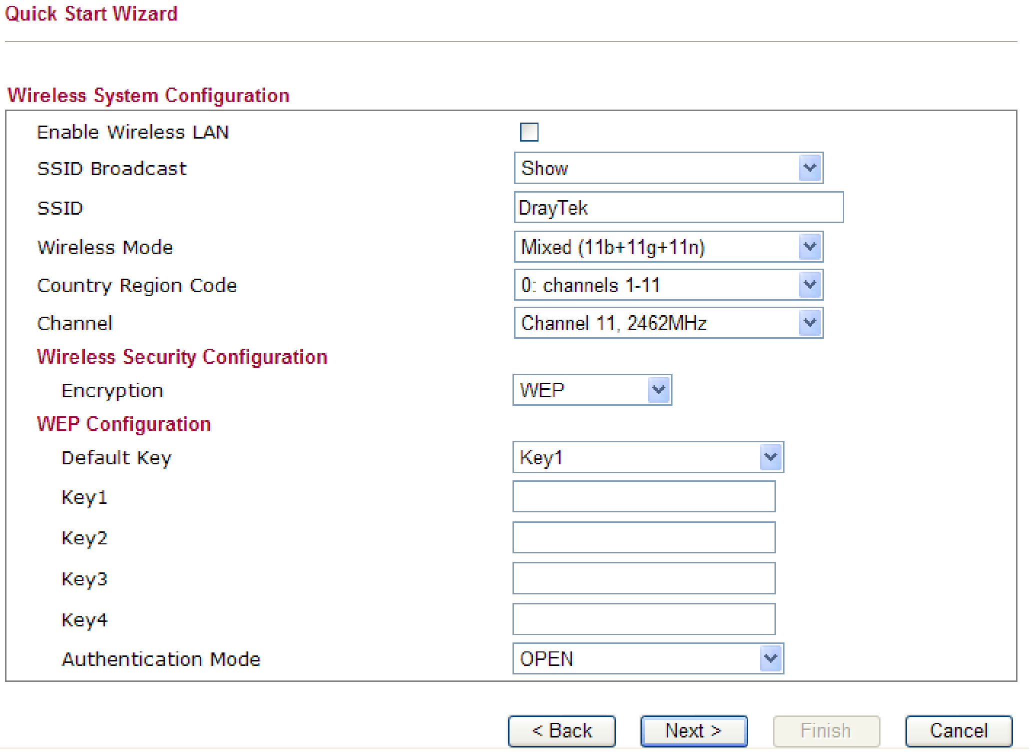
Encryption Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.



Each encryption mode will bring out different web page and ask you to offer additional configuration.

WEP

If you choose WEP as the security configuration, you have to specify encryption key (Key 1 ~ Key 4) and authentication mode (open or shared). All wireless devices must support the same WEP encryption bit size and have the same key.



Quick Start Wizard

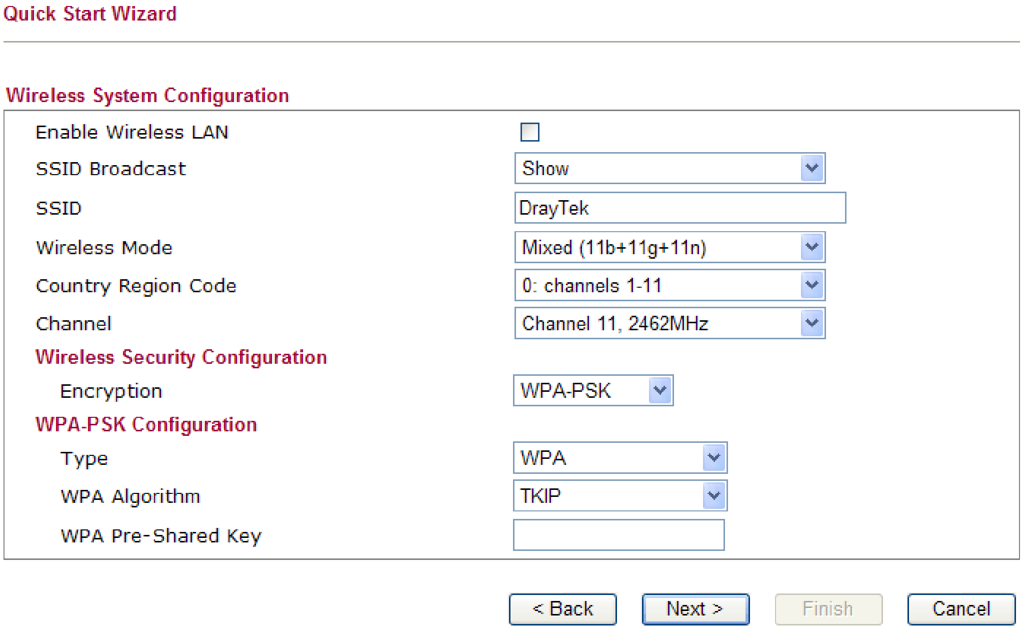
Wireless System Configuration

Enable Wireless LAN	□
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
Wireless Security Configuration	
Encryption	WEP
WEP Configuration	
Default Key	Key1
Key1	
Key2	
Key3	
Key4	
Authentication Mode	OPEN

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. Choose the key you wish to use by using the Default Key drop down list.

WPA-PSK

If you choose WPA-PSK as the security configuration, you have to specify WPA mode, algorithm and pre-shared key.

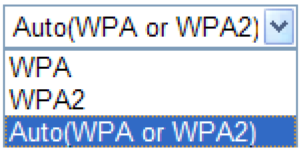


Quick Start Wizard

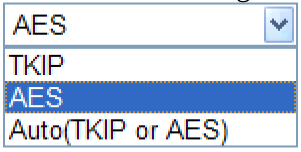
Wireless System Configuration

Enable Wireless LAN	□
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
Wireless Security Configuration	
Encryption	WPA-PSK
WPA-PSK Configuration	
Type	WPA
WPA Algorithm	TKIP
WPA Pre-Shared Key	

Type 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. Select WPA, WPA2 or Auto as WPA mode.



WPA Algorithm Choose the WPA algorithm, TKIP, AES or Auto.



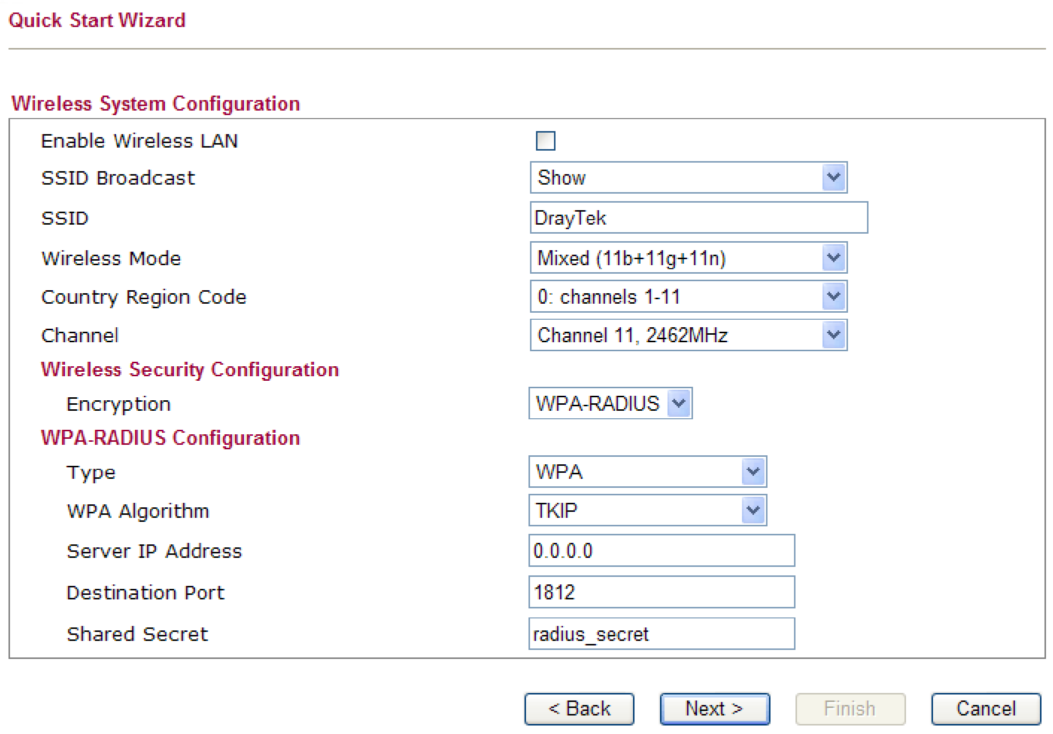
WPA Pre-shared Key The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

WPA- 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.

If you choose WPA-Radius as the security configuration, you have to specify WPA mode, algorithm, Radius server, Radius server port and Radius server secret respectively.

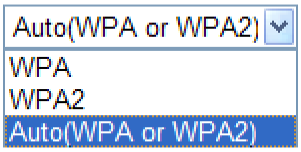


Quick Start Wizard

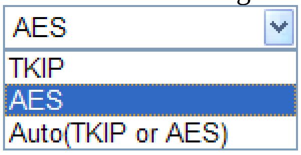
Wireless System Configuration

Enable Wireless LAN	☐
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
Wireless Security Configuration	
Encryption	WPA-RADIUS
WPA-RADIUS Configuration	
Type	WPA
WPA Algorithm	TKIP
Server IP Address	0.0.0.0
Destination Port	1812
Shared Secret	radius_secret

Type 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. Select WPA, WPA2 or Auto as WPA mode.



WPA Algorithm Choose the WPA algorithm, TKIP, AES or Auto.



Server IP Address Enter the IP address of RADIUS server.

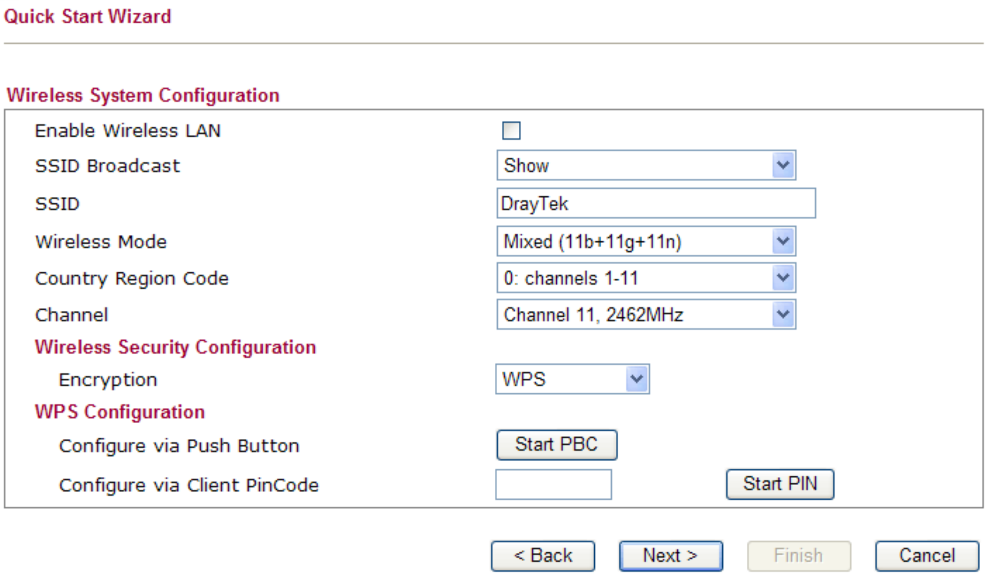
Destination Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

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.

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.

If you choose WPS as the security configuration, you can press Start WPS PIN and Start WPS PBC to complete the wireless connection.



Quick Start Wizard

Wireless System Configuration

Enable Wireless LAN	□
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
Wireless Security Configuration	
Encryption	WPS
WPS Configuration	
Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

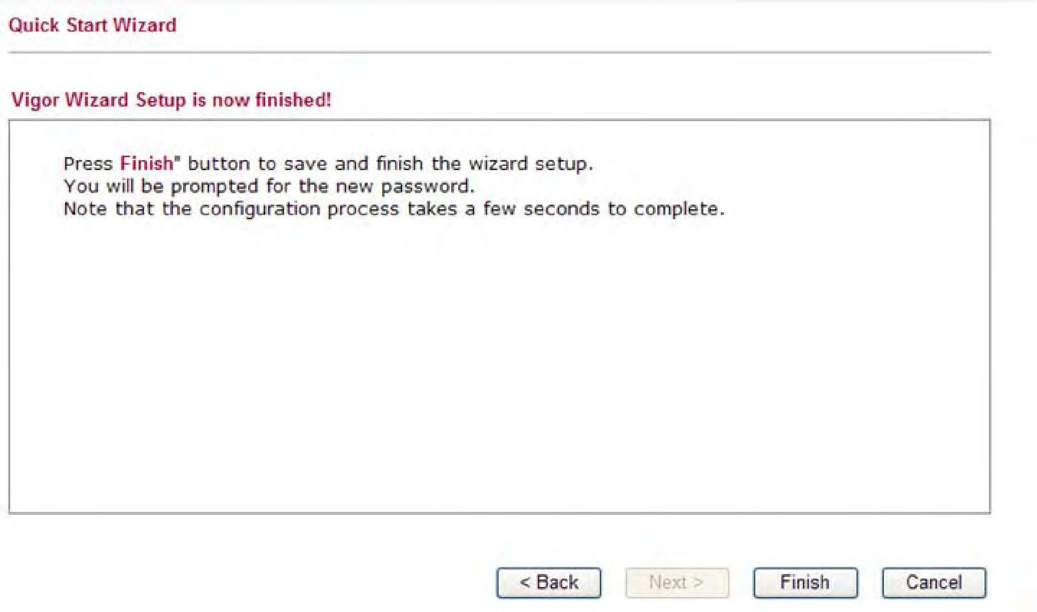
Configure via Push Button Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

Configure via Client PinCode Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN 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)

After finishing the settings here, please click **Next.**

2.4.5 Saving the Wizard Configuration

Now you can see the following screen. It indicates that the setup is complete. Different types of connection modes will have different summary. Click **Finish** and then restart the router.



Quick Start Wizard

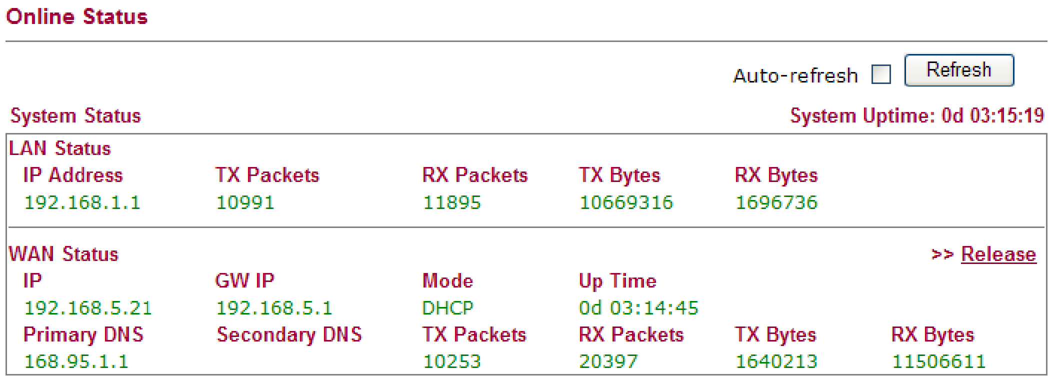
Vigor Wizard Setup is now finished!

Press Finish" button to save and finish the wizard setup.
You will be prompted for the new password.
Note that the configuration process takes a few seconds to complete.

2.5 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 for DHCP



Online Status

Auto-refresh □ Refresh

System Status — System Uptime: 0d 03:15:19

LAN Status

IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.1	10991	11895	10669316	1696736

WAN Status — >> Release

IP	GW IP	Mode	Up Time		
192.168.5.21	192.168.5.1	DHCP	0d 03:14:45		
Primary DNS	Secondary DNS	TX Packets	RX Packets	TX Bytes	RX Bytes
168.95.1.1		10253	20397	1640213	11506611

Detailed explanation is shown below:

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.

WAN Status

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

Name Displays the name set in WAN1/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.

2.6 Saving Configuration

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

Status: Ready

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

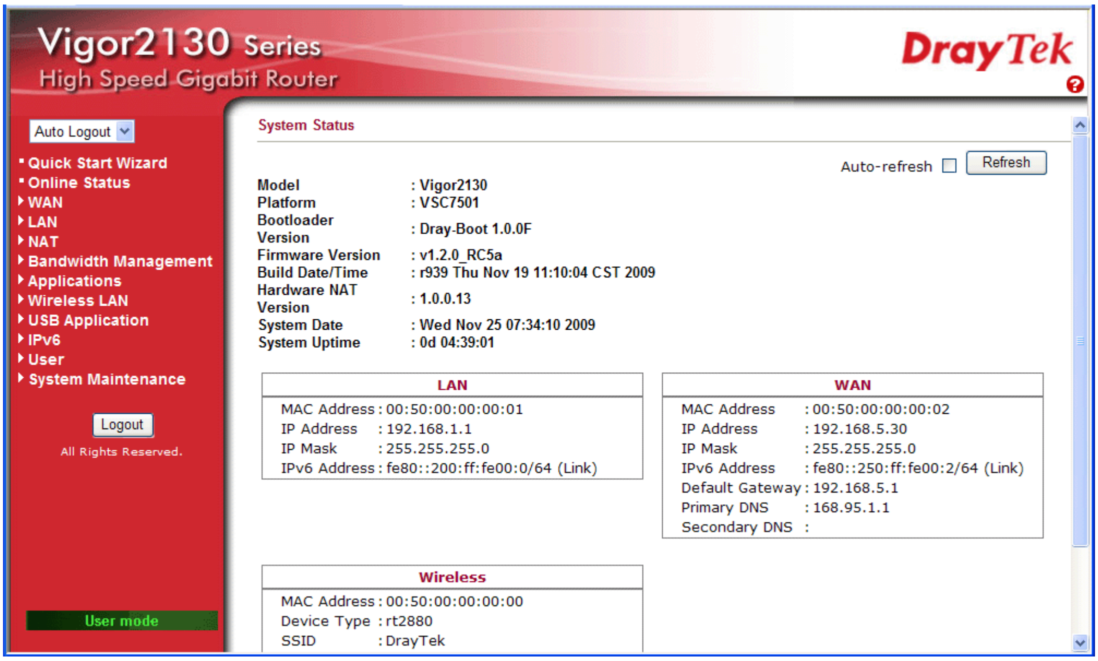
Settings Saved means your settings are saved once you click **Finish** or **OK** button.

3 User Mode Operation

This chapter will guide users to execute simple configuration through user mode operation.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. **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 : Vigor2130
Platform : VSC7501
Bootloader Version : Dray-Boot 1.0.0F
Firmware Version : v1.2.0_RC5a
Build Date/Time : r939 Thu Nov 19 11:10:04 CST 2009
Hardware NAT Version : 1.0.0.13
System Date : Wed Nov 25 07:34:10 2009
System Uptime : 0d 04:39:01

LAN

MAC Address : 00:50:00:00:00:01
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::200:ff:fe00:0/64 (Link)

WAN

MAC Address : 00:50:00:00:00:02
IP Address : 192.168.5.30
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:ff:fe00:2/64 (Link)
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

Wireless

MAC Address : 00:50:00:00:00:00
Device Type : rt2880
SSID : DrayTek

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.

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.

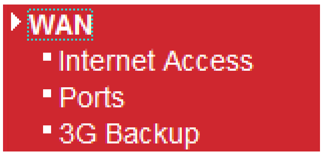
When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information 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, Vigor router adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor router, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor router with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via SuperG wireless function of Vigor router, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor router.

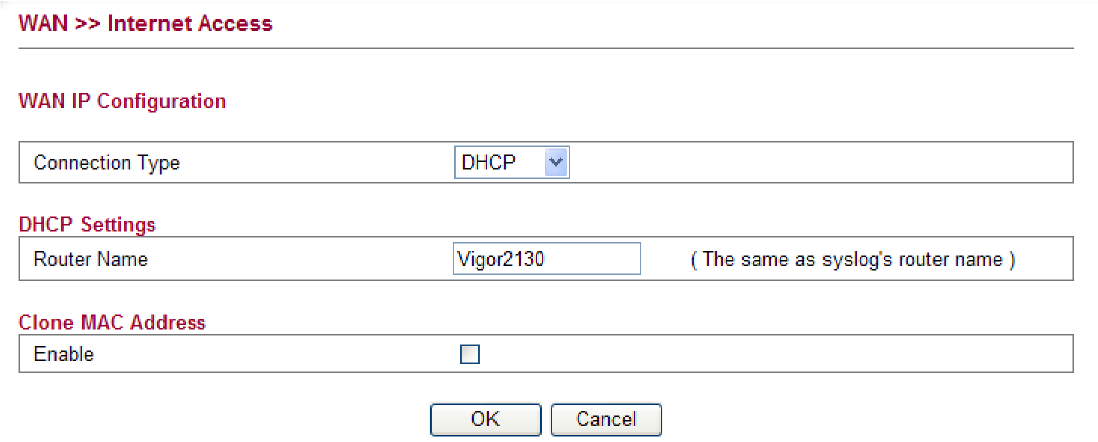
After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem also can be used as backup device. Therefore, when WAN is not available, the router will use 3.5G 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**.



3.1.1 Internet Access

This page allows you to set WAN configuration with different modes. Use the Connection Type drop down list to choose one of the WAN modes. The corresponding page will be displayed.



WAN >> Internet Access

WAN IP Configuration

Connection Type	DHCP

DHCP Settings

Router Name	Vigor2130	(The same as syslog's router name)

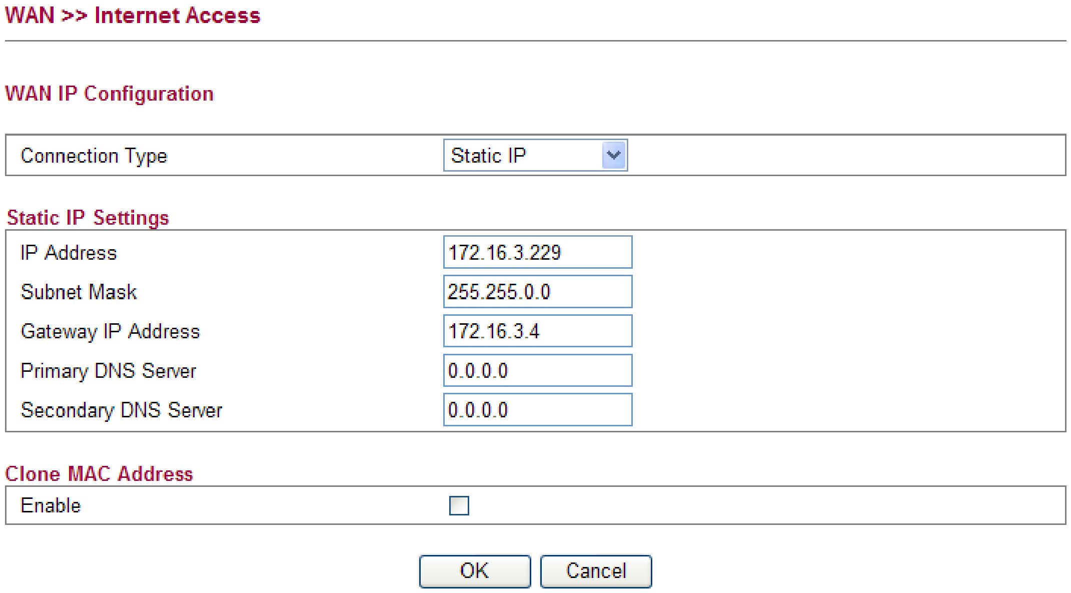
Clone MAC Address

Enable	□

Static

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** as the accessing protocol of the internet, please choose **Static** mode from **Connection Type** drop down menu. The following web page will be shown.



WAN >> Internet Access

WAN IP Configuration

Connection Type	Static IP

Static IP Settings

IP Address	172.16.3.229
Subnet Mask	255.255.0.0
Gateway IP Address	172.16.3.4
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Clone MAC Address

Enable	□

IP Address Type the IP address.

Subnet Mask Type the subnet mask.

Gateway IP Address Type the gateway IP address.

Primary DNS Server Type in the primary IP address for the router if you want to use **Static IP** mode.

Secondary DNS Server Type in secondary IP address for using in the future if necessary.

Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

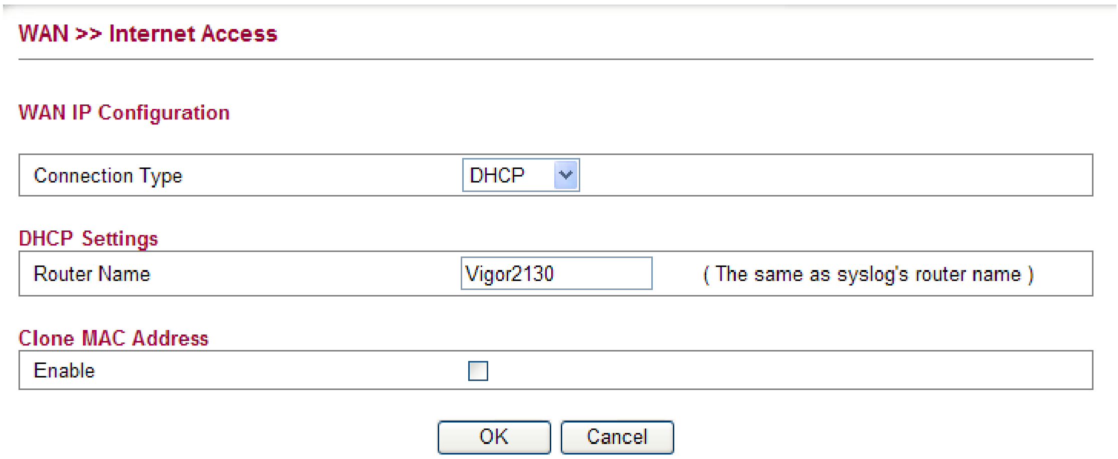
Enable ☑ Clone MAC Address

MAC Address 00-0E-A6-2A-D5-A1

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

DHCP

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for your router automatically. It is not necessary for you to assign any setting,



WAN >> Internet Access

WAN IP Configuration

Connection Type	DHCP

DHCP Settings

Router Name	Vigor2130	(The same as syslog's router name)

Clone MAC Address

Enable	□

Router Name Type in a name for the router. It must be the same as the name used in Syslog.

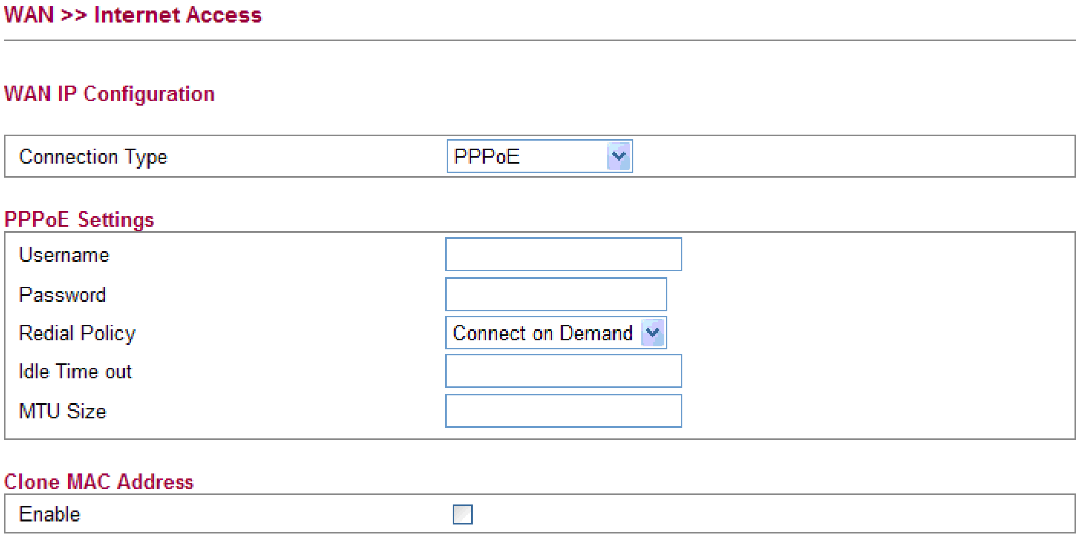
Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

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

PPPoE

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 IP Configuration

Connection Type	PPPoE

PPPoE Settings

Username	
Password	
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	

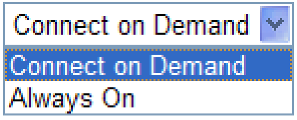
Clone MAC Address

Enable	□

Username Type in the username provided by ISP in this field.

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

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.

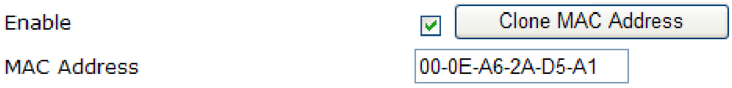


Idle Time Out Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.

MTU Size It means Max Transmit Unit for packet. The default setting is 1442. Leave blank for default value.

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.

Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.



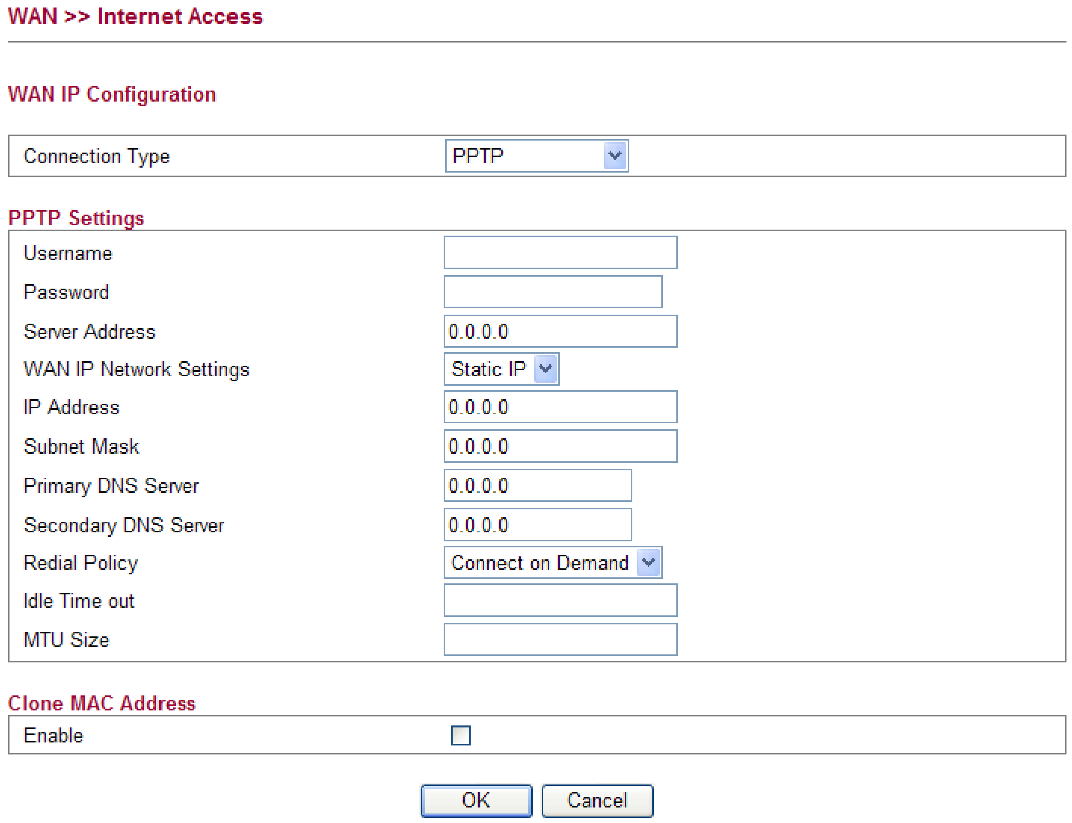
Enable ☑ Clone MAC Address

MAC Address 00-0E-A6-2A-D5-A1

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

PPTP/L2TP

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



WAN >> Internet Access

WAN IP Configuration

Connection Type	PPTP

PPTP Settings

Username	
Password	
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	

Clone MAC Address

Enable	□

Username Type in the username provided by ISP in this field.

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

Server Address Type in the IP address for PPTP /L2TP server.

WAN IP Network Settings You can choose Static IP or DHCP as WAN IP network setting.

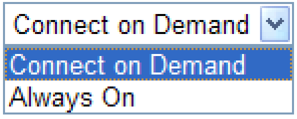
IP Address Type the IP address if you choose Static IP as the WAN IP network setting.

Subnet Mask Type the subnet mask if you chose Static IP as the WAN IP.

Primary DNS Server If you choose **Static IP** for WAN IP Network Settings, 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 apply a default DNS Server automatically.

Secondary DNS Server If you choose **Static IP** for WAN IP Network Settings, 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 apply a default secondary DNS Server automatically.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand** and



Idle Time Out Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.

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

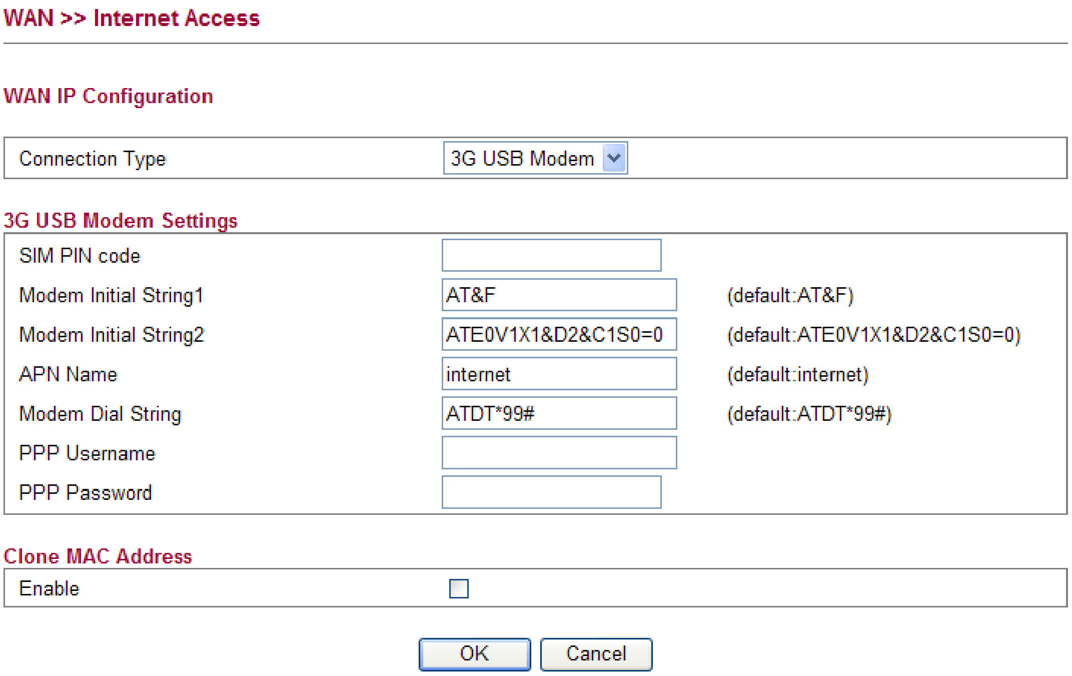
Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	☑ [Clone MAC Address]
MAC Address	00-0E-A6-2A-D5-A1

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

3G USB Modem

If your router connects to a 3G modem and you want to access Internet via 3G modem, choose 3G as connection type and type the required information in this web page.



WAN >> Internet Access

WAN IP Configuration

Connection Type	3G USB Modem

3G USB Modem Settings

SIM PIN code		
Modem Initial String1	AT&F	(default:AT&F)
Modem Initial String2	ATE0V1X1&D2&C1S0=0	(default:ATE0V1X1&D2&C1S0=0)
APN Name	internet	(default:internet)
Modem Dial String	ATDT*99#	(default:ATDT*99#)
PPP Username		
PPP Password		

Clone MAC Address

Enable	□

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

Modem Initial String1/2 Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

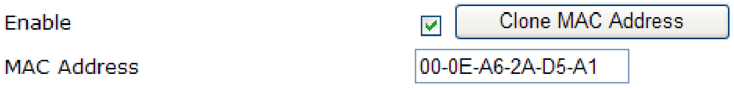
APN Name APN means Access Point Name which is provided and required by some ISPs.

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).

Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

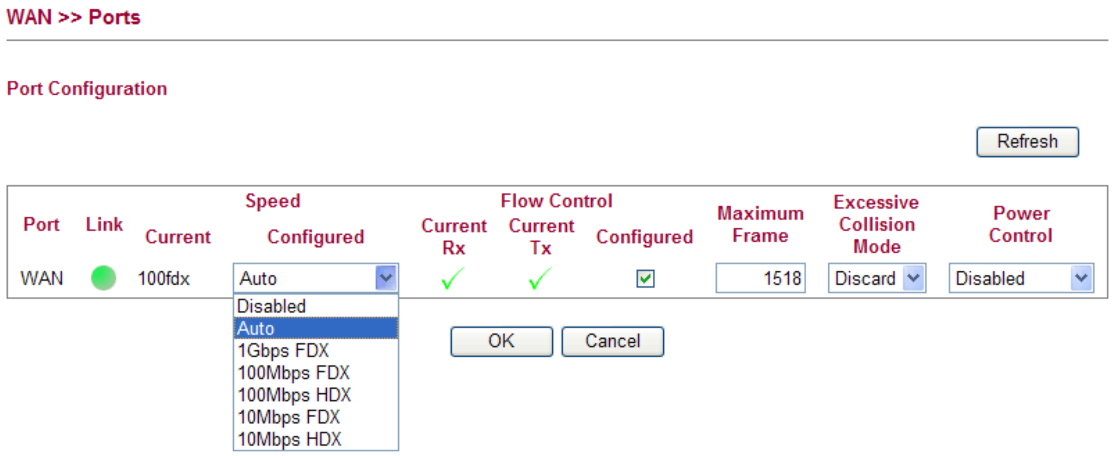


Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

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

3.1.2 Ports

Ports page is used to change the setting for WAN port. You can set or reset the following items. All of them are described in detail below.



WAN >> Ports

Port Configuration

Refresh

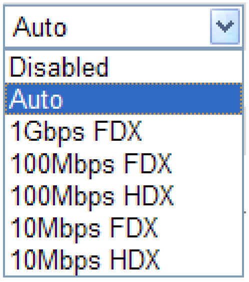
Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
WAN	●	100fdx	Auto	✓	✓	☑	1518	Discard	Disabled

Port It displays current network interface.

Link It displays current connection status. Green light means the WAN connection is successful.

Current It displays current speed that the router uses.

Speed Configured It can set the speed and duplex of the port. You can use the drop down list to choose the required speed for the router. If you have no idea in configuring speed, simple use the default setting, **Auto**.



Flow Control

If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.
Current Rx: indicates whether pause frames on the port are obeyed.
Current Tx: indicates whether pause frames on the port are transmitted.

Maximum Frame

This module offers 1518~9600 (Bytes) length to make the long packet for data transmission.

Excessive Collision Mode

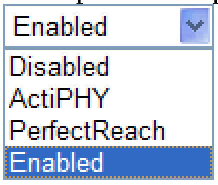
There are two modes for you to choose when excessive collision happened in half-duplex condition.

Discard - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

Restart - It determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Standard 802.3, but is useful in non-dropping half-duplex flow control operation.

Power Control

The Configured column allows for changing the power savings mode parameters per port.



Disabled: All power savings mechanisms disabled.
ActiPHY: Link down power savings enabled.
PerfectReach: Link up power savings enabled.
Enabled: Both link up and link down power savings enabled.

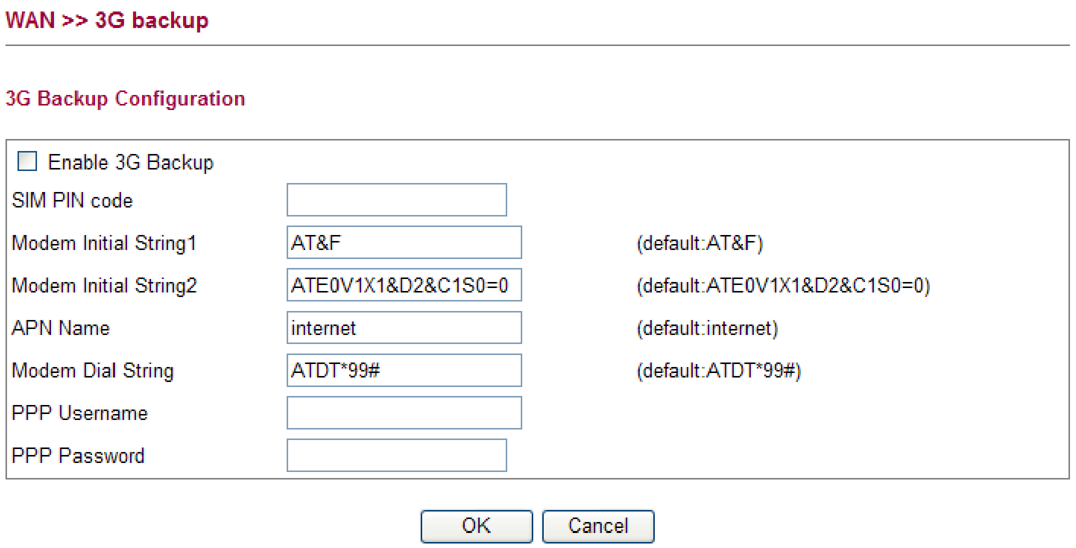
Refresh

Click this button to refresh the information for WAN port.

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

3.1.3 3G Backup

This page is used to setup 3G backup function. If you enable 3G backup, make sure your WAN connection type is not in 3G mode. When the WAN connection is broken, router will try to keep the connection with 3G mode. After WAN connection is recovered, router will disconnect the 3G connection automatically.



WAN >> 3G backup

3G Backup Configuration

□ Enable 3G Backup		
SIM PIN code		
Modem Initial String1	AT&F	(default:AT&F)
Modem Initial String2	ATE0V1X1&D2&C1S0=0	(default:ATE0V1X1&D2&C1S0=0)
APN Name	internet	(default:internet)
Modem Dial String	ATDT*99#	(default:ATDT*99#)
PPP Username		
PPP Password		

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

Modem Initial String1/2 Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

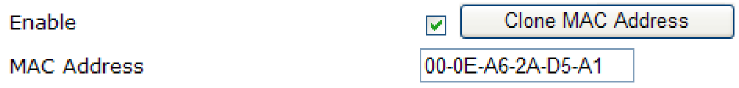
APN Name APN means Access Point Name which is provided and required by some ISPs.

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).

Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.



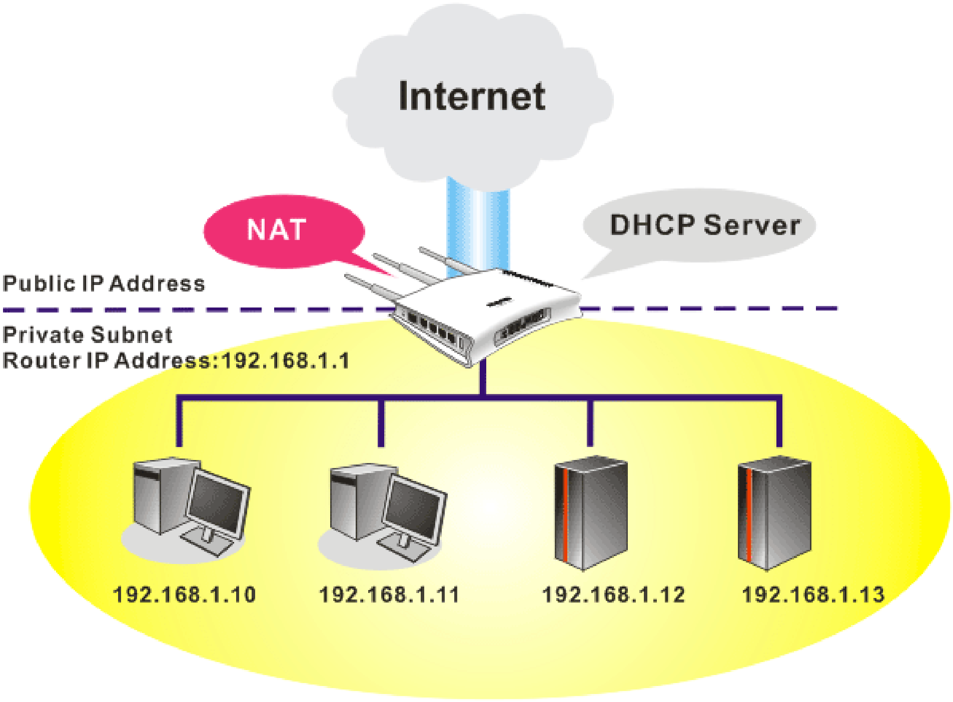
Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

3.2 LAN

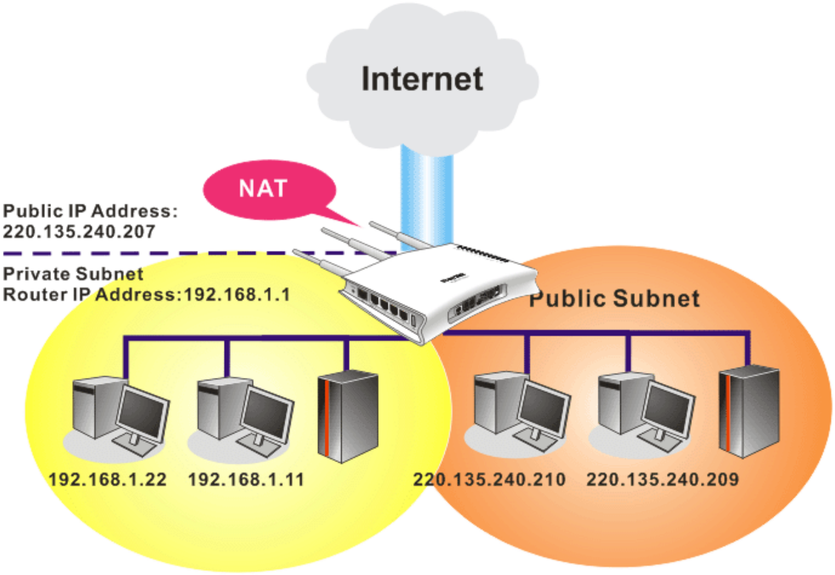
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

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.

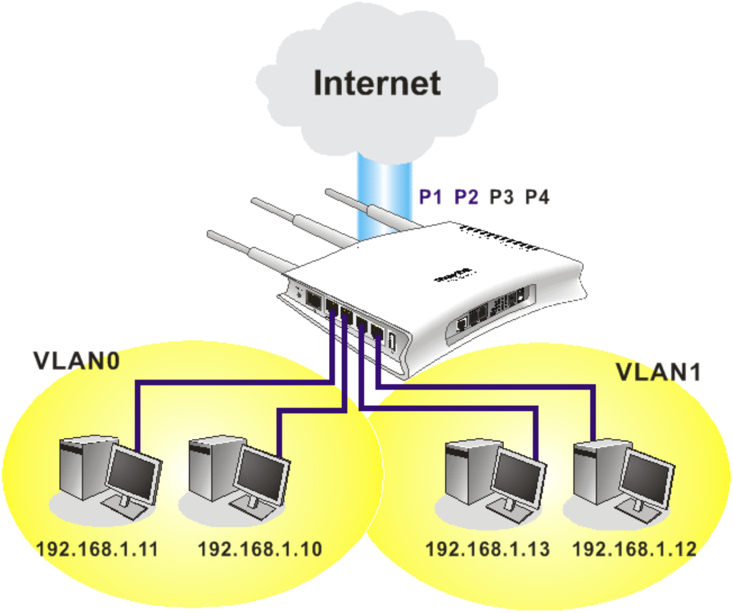


What is Routing Information Protocol (RIP)

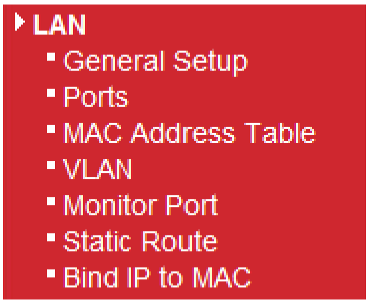
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What are Virtual LANs and Rate Control

You can group local hosts by physical ports 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.



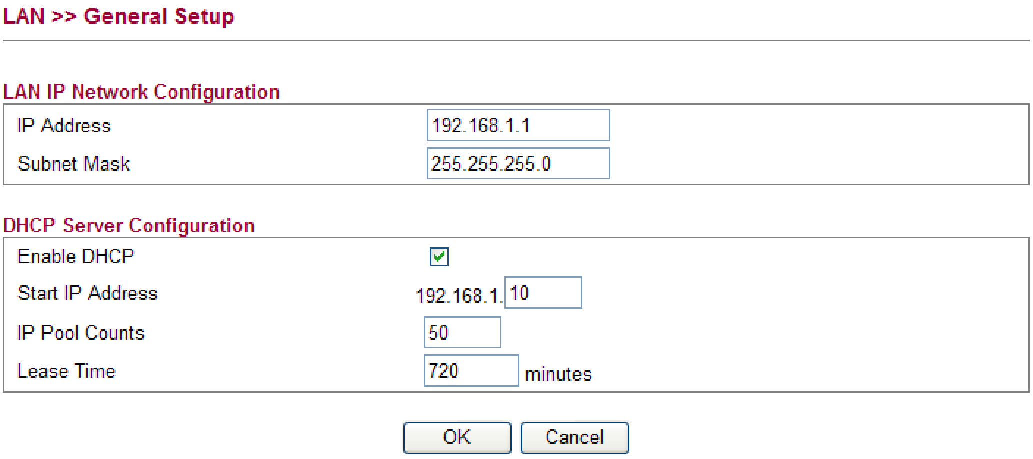
Below shows the LAN menu:



3.2.1 General Setup

This page provides you the general settings for LAN.

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



LAN >> General Setup

LAN IP Network Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

DHCP Server Configuration

Enable DHCP	☑
Start IP Address	192.168.1. 10
IP Pool Counts	50
Lease Time	720 minutes

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)

Enable DHCP 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.
You can configure the router to serve as a DHCP server for the 2nd subnet. Check the box to enable DHCP server setting.

Start IP Address Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

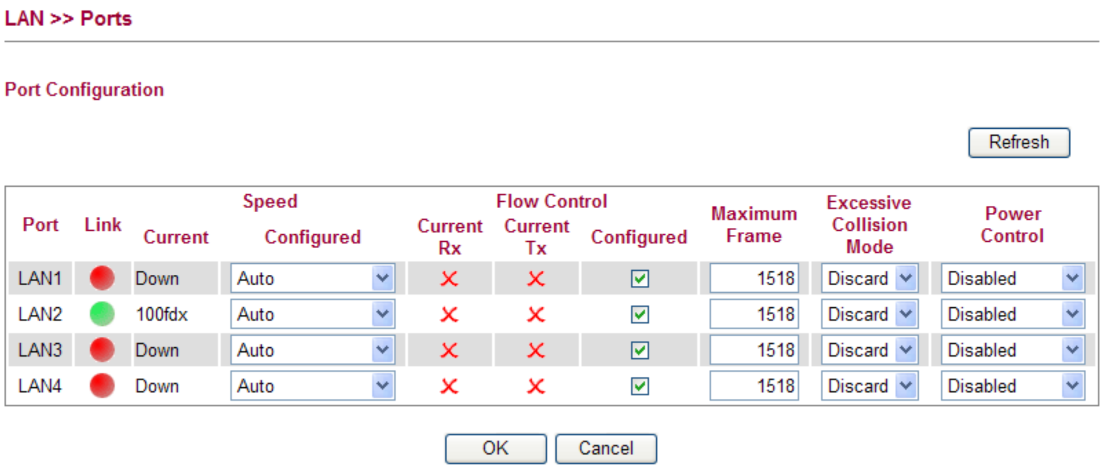
IP Pool Counts Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

Lease Time It allows you to set the leased time for the specified PC.

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

3.2.2 Ports

Ports page is used to change the setting for LAN ports. You can set or reset the following items. All of them are described in detail below.



LAN >> Ports

Port Configuration

Refresh

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
LAN1	🔴	Down	Auto	✗	✗	☑	1518	Discard	Disabled
LAN2	🟢	100fdx	Auto	✗	✗	☑	1518	Discard	Disabled
LAN3	🔴	Down	Auto	✗	✗	☑	1518	Discard	Disabled
LAN4	🔴	Down	Auto	✗	✗	☑	1518	Discard	Disabled

OK Cancel

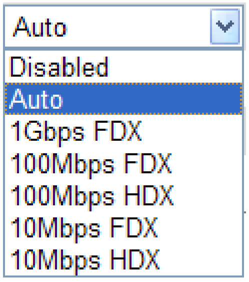
Port It displays current network interface.

Link It displays current connection status. Green light means the LAN connection is successful.

Current It displays current speed that the router uses.

Speed Configured It can set the speed and duplex of the port. You can use the drop down list to choose the required speed for the router. If you have no idea in configuring speed, simple use the default setting,

Auto.



Flow Control

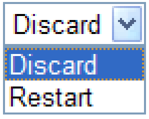
If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.
Current Rx: indicates whether pause frames on the port are obeyed.
Current Tx: indicates whether pause frames on the port are transmitted.

Maximum Frame

This module offers 1518~9600 (Bytes) length to make the long packet for data transmission.

Excessive Collision Mode

There are two modes for you to choose when excessive collision happened in half-duplex condition.

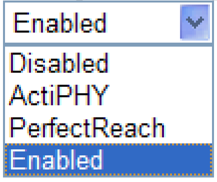


Discard - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

Restart - It determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Standard 802.3, but is useful in non-dropping half-duplex flow control operation.

Power Control

The Configured column allows for changing the power savings mode parameters per port.



Disabled: All power savings mechanisms disabled.
ActiPHY: Link down power savings enabled.
PerfectReach: Link up power savings enabled.
Enabled: Both link up and link down power savings enabled.

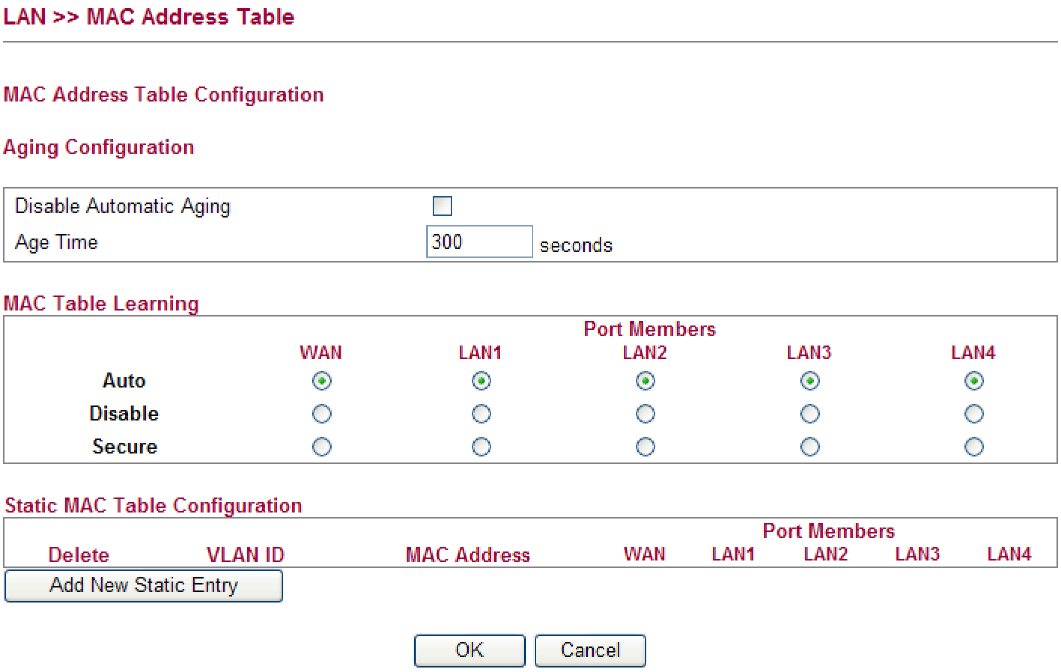
Refresh

Click this button to refresh the information for LAN ports.

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

3.2.3 MAC Address Table

This page allows you to set timeouts for entries in dynamic MAC Table and configure the static MAC table here.



LAN >> MAC Address Table

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Age Time	300 seconds

MAC Table Learning

	Port Members				
	WAN	LAN1	LAN2	LAN3	LAN4
Auto	●	●	●	●	●
Disable	○	○	○	○	○
Secure	○	○	○	○	○

Static MAC Table Configuration

			Port Members				
Delete	VLAN ID	MAC Address	WAN	LAN1	LAN2	LAN3	LAN4

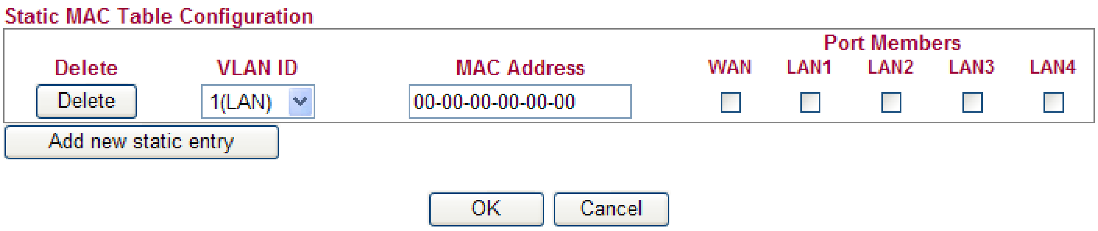
Disable Automatic Aging Stop the MAC table aging timer, the learned MAC address will not age out automatically. The default setting is enabled. Check the box to disable this function if required.

Age Time Delete a MAC address idling for a period of time from the following MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.

MAC Table Learning List the port members which apply dynamic learning mechanism or not.
Auto - Enable this port MAC address dynamic learning mechanism.
Disable - Disable this port MAC address dynamic learning mechanism, only support static MAC address setting.
Secure - Disable this port MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU.

Static MAC Table Config.. Specify static MAC address with VLAN ID to apply aging configuration.
Delete - Click the button to remove the VLAN setting.
VLAN ID - Specify the interface for the port members.
MAC Address - It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 – 02.
WAN/LAN1~4 - Check the port to apply this VLAN setting.

To add a new static MAC entry, click **Add new static entry**. A new entry will be shown as follows. Choose VLAN ID and type a new MAC address. Next, specify port member for this table. Finally, click OK to save the changes.



Static MAC Table Configuration

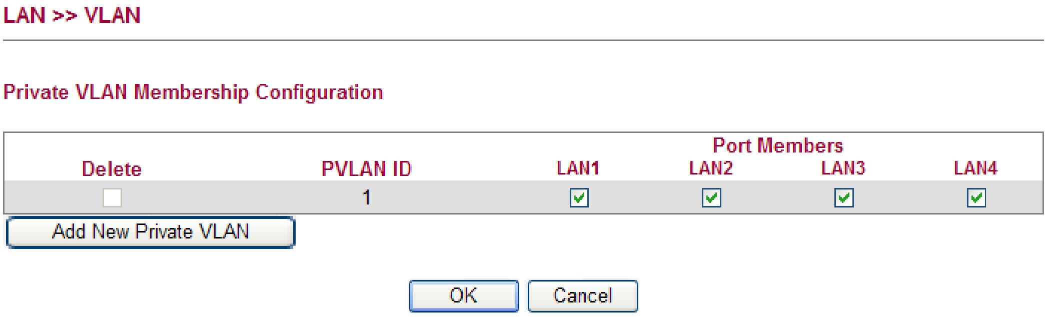
			Port Members				
Delete	VLAN ID	MAC Address	WAN	LAN1	LAN2	LAN3	LAN4
Delete	1(LAN)	00-00-00-00-00-00	□	□	□	□	□

Add new static entry

OK Cancel

3.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to **LAN** page and select **VLAN**. The following page will appear. VLAN function is enabled in default.



LAN >> VLAN

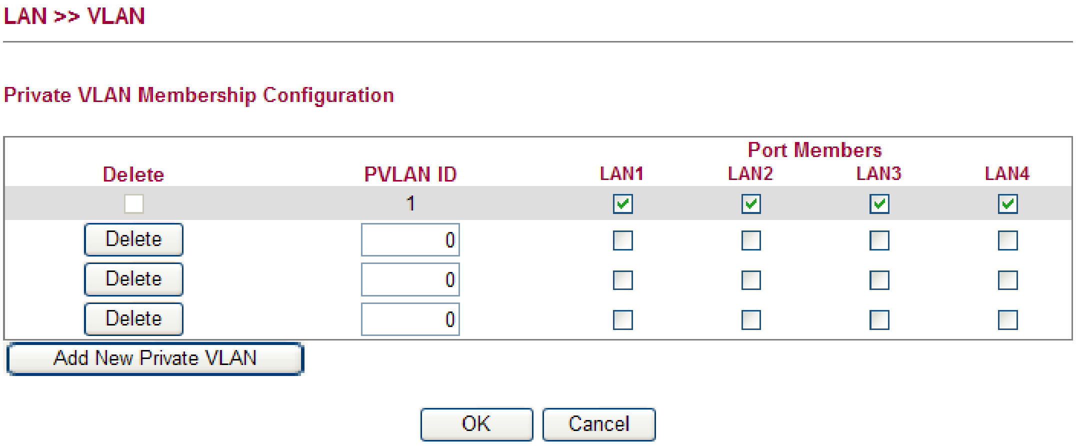
Private VLAN Membership Configuration

		Port Members			
Delete	PVLAN ID	LAN1	LAN2	LAN3	LAN4
□	1	☑	☑	☑	☑

Add New Private VLAN

OK Cancel

Add New Private VLAN Click this button to add a new private VLAN. The router allows you to add up to 4 VLAN.



LAN >> VLAN

Private VLAN Membership Configuration

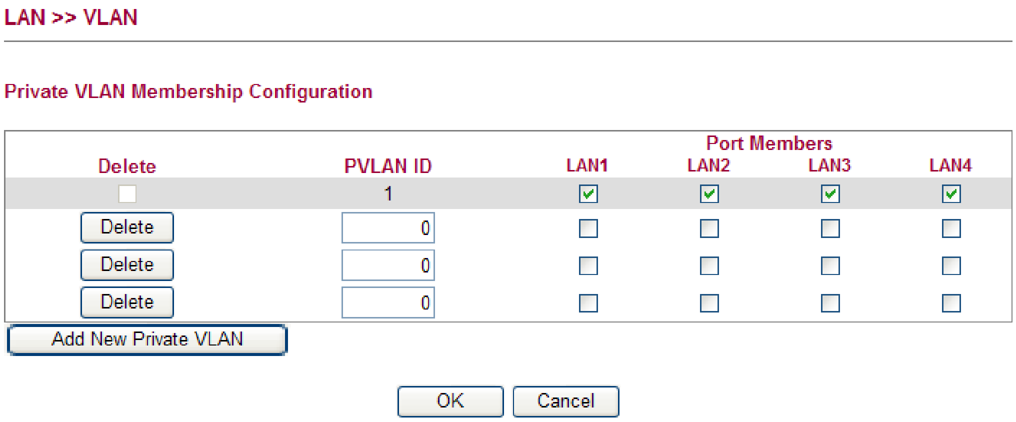
		Port Members			
Delete	PVLAN ID	LAN1	LAN2	LAN3	LAN4
□	1	☑	☑	☑	☑
Delete	0	□	□	□	□
Delete	0	□	□	□	□
Delete	0	□	□	□	□

Add New Private VLAN

OK Cancel

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

1. VLAN 1 is consisted of hosts linked to P1 ~ P4.
2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below.



LAN >> VLAN

Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members			
		LAN1	LAN2	LAN3	LAN4
□	1	☑	☑	☑	☑
Delete	0	□	□	□	□
Delete	0	□	□	□	□
Delete	0	□	□	□	□

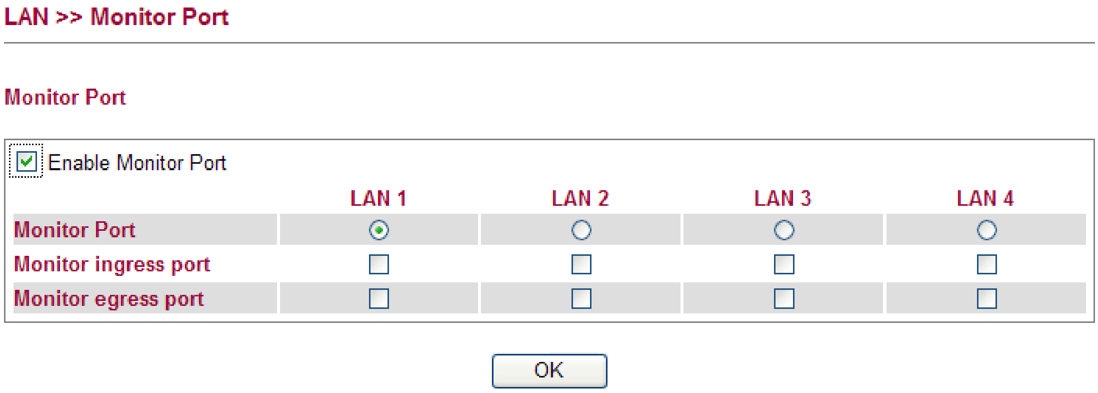
Add New Private VLAN

OK Cancel

3. To remove VLAN, click the **Delete** button for the one you want to remove and click **OK** to save the results.

3.2.5 Monitor Port

It is used to monitor the traffic of the network. For example, we assume that LAN1 and LAN2 are Monitor Port and Monitor ingress Port respectively, thus, the traffic received by LAN2 will be copied to LAN1 for monitoring.



LAN >> Monitor Port

Monitor Port

☑ Enable Monitor Port

	LAN 1	LAN 2	LAN 3	LAN 4
Monitor Port	●	○	○	○
Monitor ingress port	□	□	□	□
Monitor egress port	□	□	□	□

OK

Enable Monitor Port Check to enable this function.

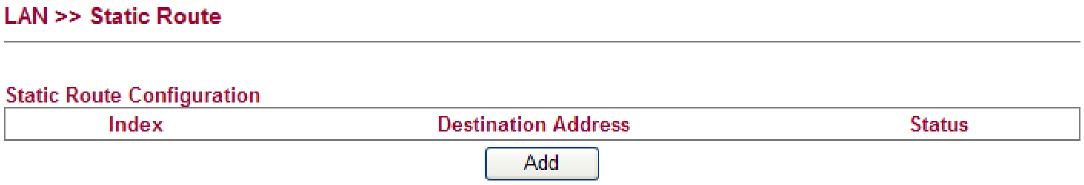
Monitor Port Click the one of the LAN ports to specify it for monitoring.

Monitor ingress port Check to set up the port(s) for being monitored. It only monitors the packets **received by** the port you set up.

Monitor egress port Check to set up the port(s) for being monitored. It only monitors the packets **transmitted** by the port you set up.

3.2.6 Static Route

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



LAN >> Static Route

Static Route Configuration

Index	Destination Address	Status

Add

Index The number (1 to 10) under Index displays current static router.

Destination Address Display the destination address of the static route.

Status Display the status of the static route.

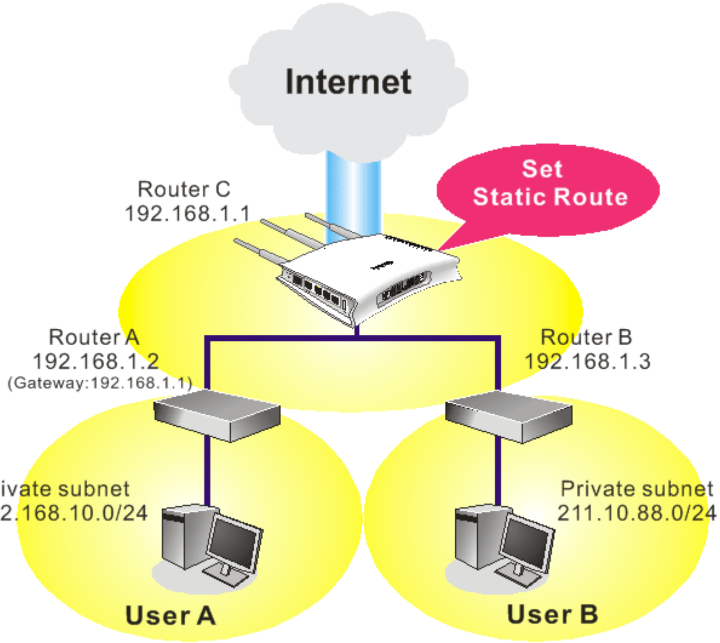
Add Add a new static route.

Add Static Routes to Private and Public Networks

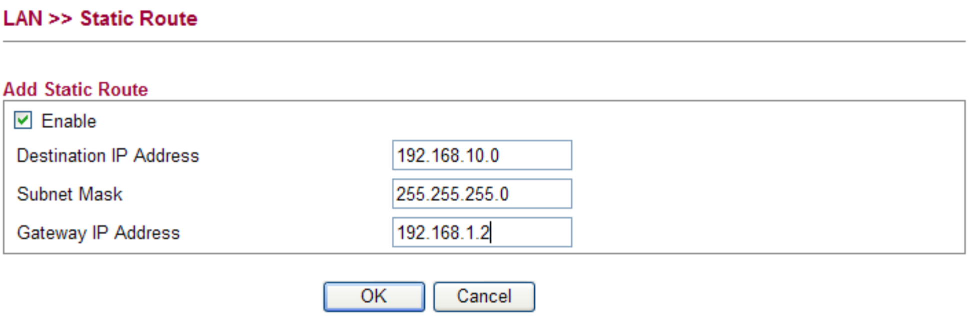
Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- 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.


Internet
Set Static Route
Router C 192.168.1.1
Router A 192.168.1.2 (Gateway:192.168.1.1)
Router B 192.168.1.3
Private subnet 192.168.10.0/24
Private subnet 211.10.88.0/24
User A
User B

1. Click the **LAN - Static Route** and click **Add.** 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**.



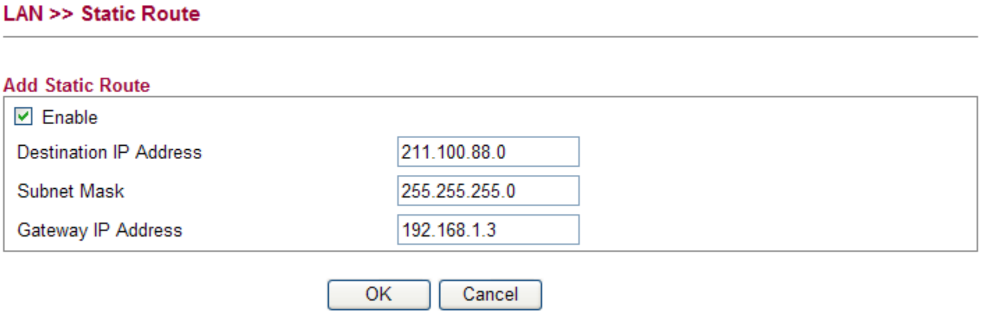
LAN >> Static Route

Add Static Route

☑ Enable

Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2

2. Return to **Static Route** page. Click **Add** again 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.

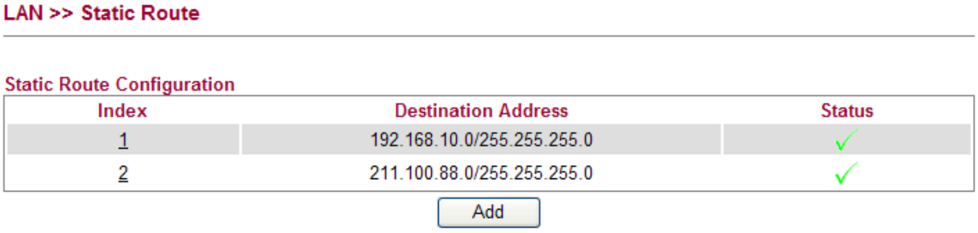


LAN >> Static Route

Add Static Route

☑ Enable	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3

3. Verify current routing table.



LAN >> Static Route

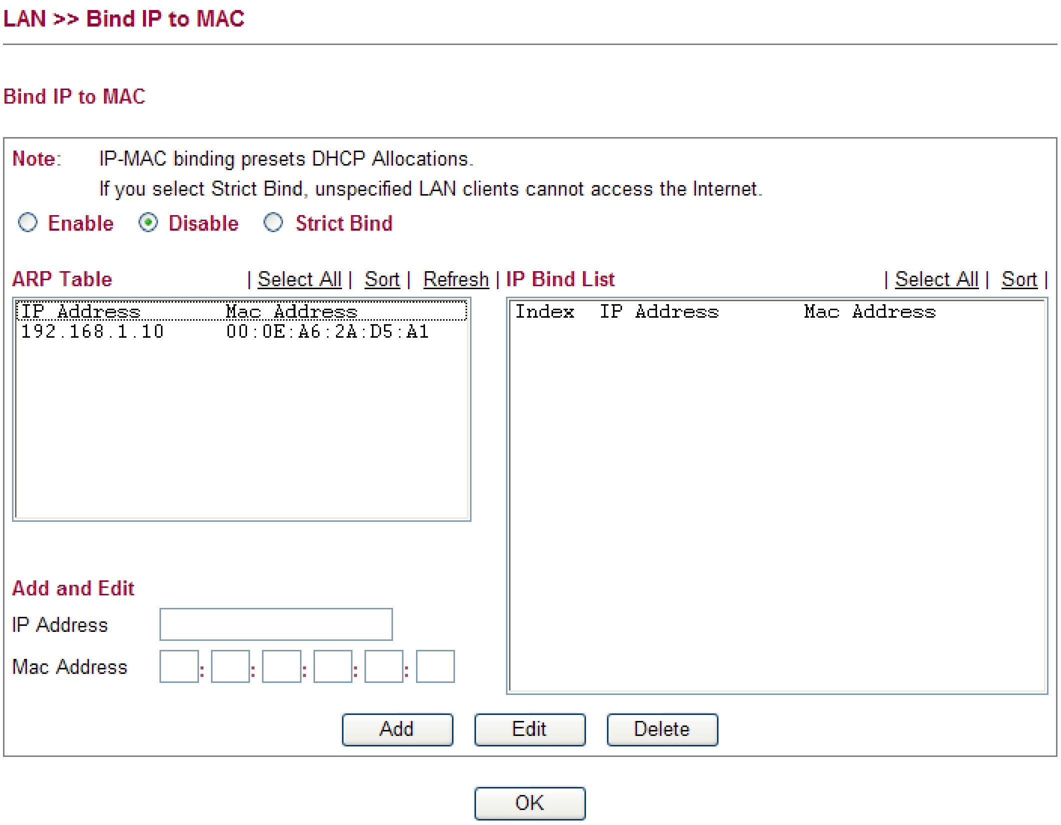
Static Route Configuration

Index	Destination Address	Status
1	192.168.10.0/255.255.255.0	✓
2	211.100.88.0/255.255.255.0	✓

3.2.7 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

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

○ Enable ● Disable ○ Strict Bind

ARP Table | Select All | Sort | Refresh |

```
IP Address          Mac Address
192.168.1.10        00:0E:A6:2A:D5:A1
```

IP Bind List | Select All | Sort |

```
Index   IP Address          Mac Address
```

Add and Edit

IP Address

Mac Address

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.

Remove	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Remove**. 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.

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.

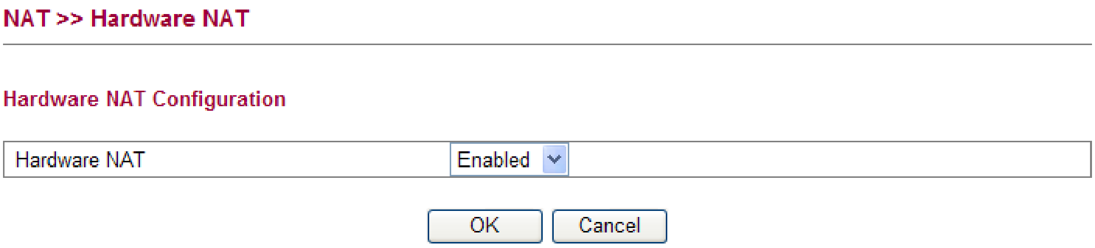
Below shows the menu items for NAT.

3.3.1 Hardware NAT

Hardware-base Acceleration Engine, also named Protocol Processing Engine API is the function that Draytek provides to extremely speed up the NAT performance.

While the hardware acceleration mechanism is activated, most of the bandwidth usage will be concentrated on the specific sessions which increase transmission speed to get ultimately accelerated.

With Hardware NAT, LAN to WAN NAT throughput can be over 900M bps. But be sure that your PC has Giga Ethernet and connect with CAT6 Ethernet cable.



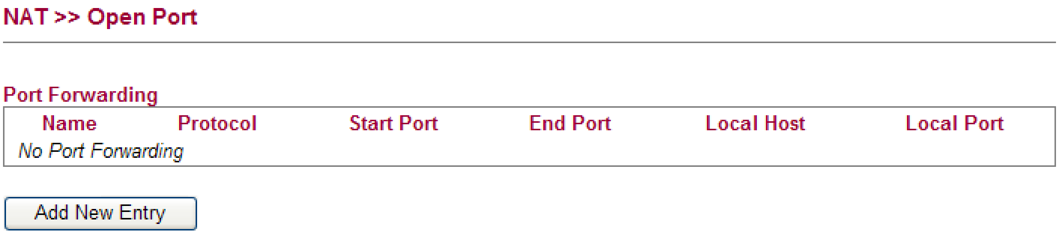
NAT >> Hardware NAT

Hardware NAT Configuration

Hardware NAT	Enabled

3.3.2 Open Ports

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



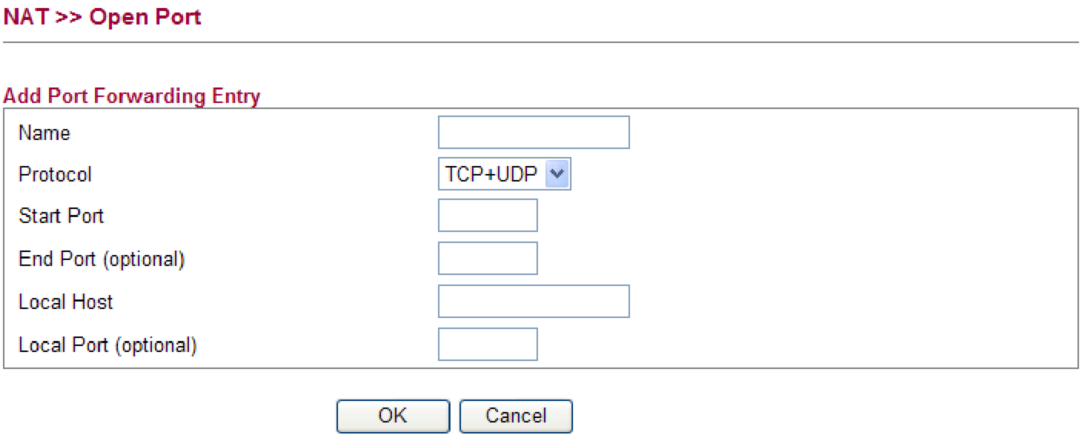
NAT >> Open Port

Port Forwarding

Name	Protocol	Start Port	End Port	Local Host	Local Port
No Port Forwarding					

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.

To add a new open port, click **Add new entry**.



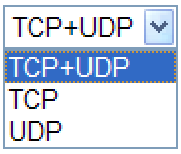
NAT >> Open Port

Add Port Forwarding Entry

Name	
Protocol	TCP+UDP
Start Port	
End Port (optional)	
Local Host	
Local Port (optional)	

Name Specify the name for the defined network service.

Protocol Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**.



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

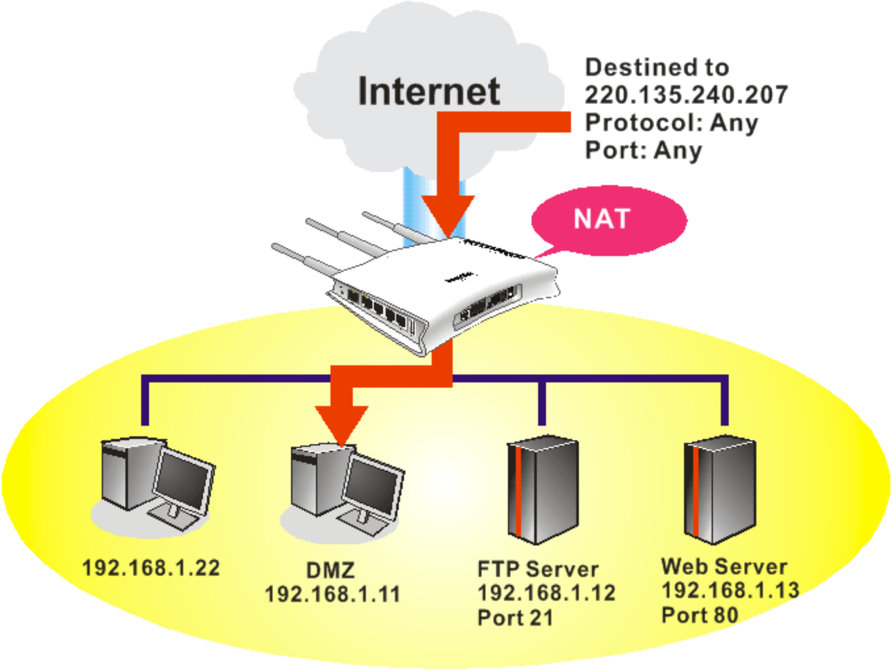
End Port (optional) Specify the ending port number of the service offered by the local host.

Local Host Enter the private IP address of the local host.

Local Port (optional) If it is configured, the forwarded traffic is mapped to this port on the local host.

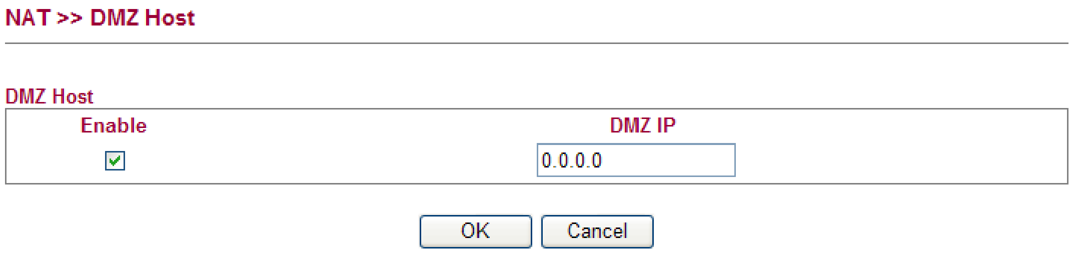
3.3.3 DMZ Host

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.



Note: 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:



NAT >> DMZ Host

DMZ Host

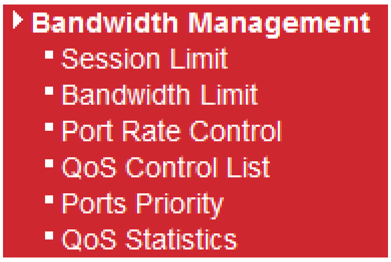
Enable	DMZ IP
☑	0.0.0.0

Enable Check to enable the DMZ Host function.

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

3.4 Bandwidth Management

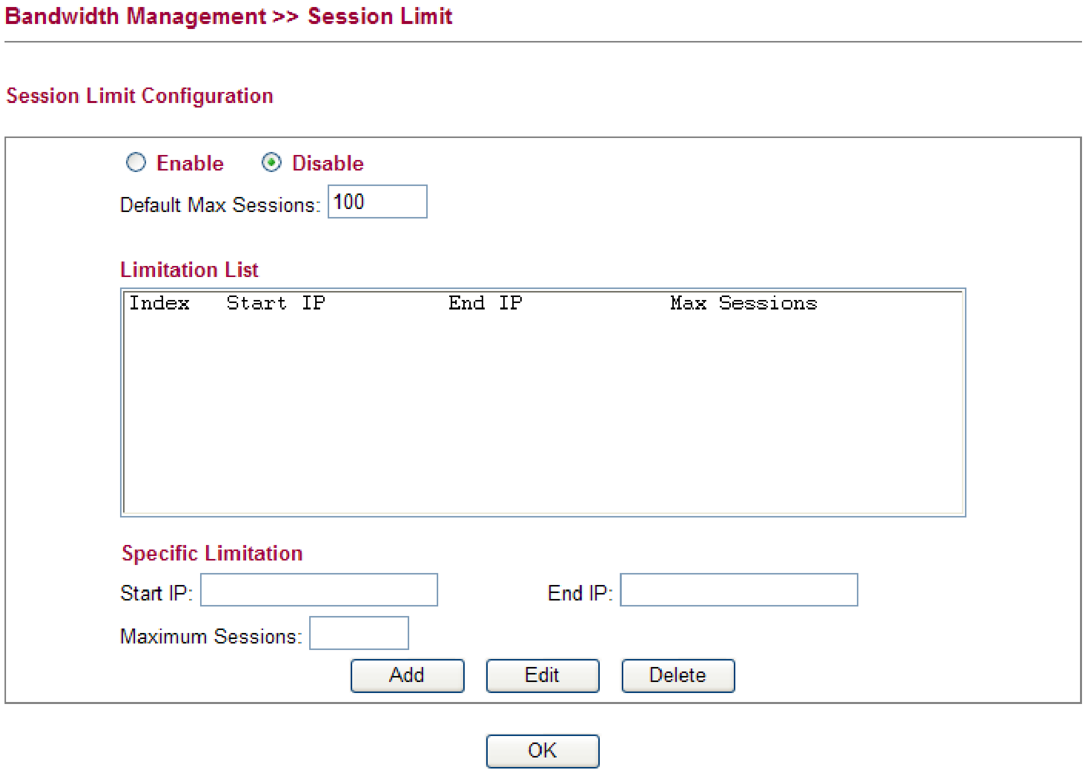
Below shows the menu items for Bandwidth Management.



3.4.1 Session 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 >> Session Limit

Session Limit Configuration

○ Enable ● Disable

Default Max Sessions: 100

Limitation List

```
Index   Start IP          End IP            Max Sessions
```

Specific Limitation

Start IP: End IP:

Maximum Sessions:

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 Max Sessions Defines the default session number used for each computer in LAN.

Limitation List Displays a list of specific limitations that you set on this web page.

Start IP Defines the start LAN IP address for limit session.

End IP Defines the end LAN IP address for limit session.

Maximum Sessions Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.

Add Adds the specific session limitation onto the list above.

Edit Allows you to edit the settings for the selected limitation.

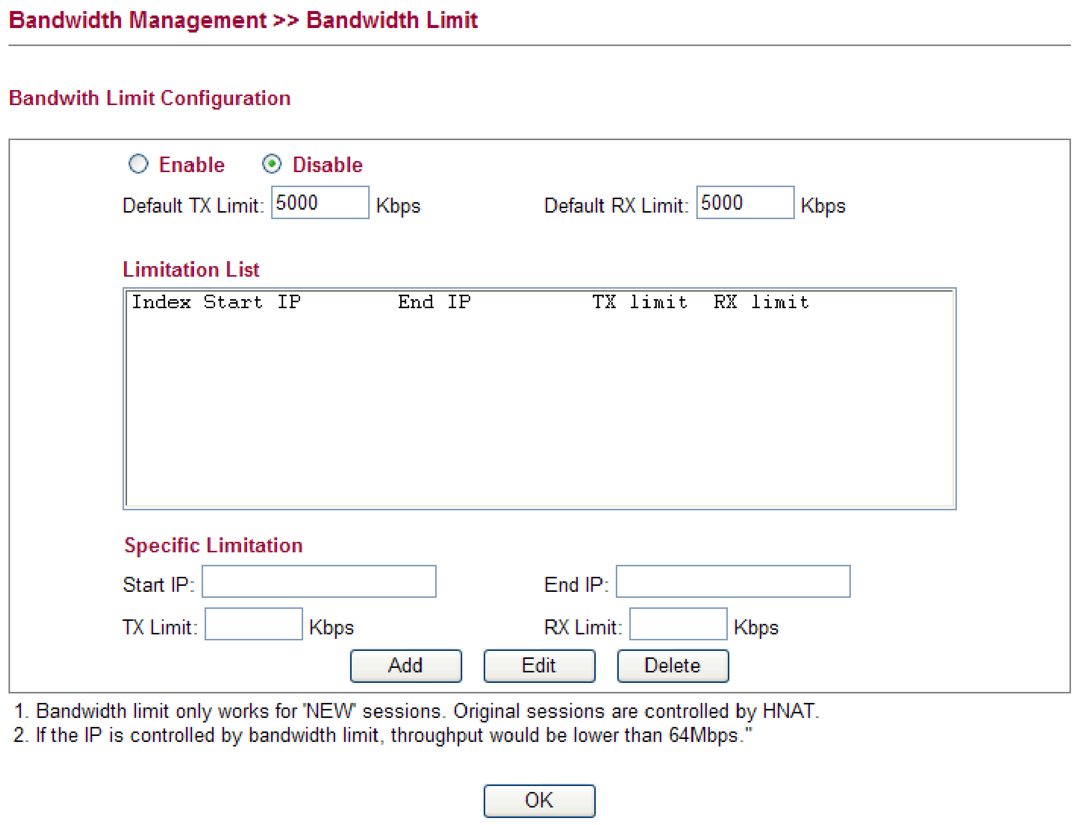
Delete Remove the selected settings existing on the limitation list.

When you finish adding a new session limit, simply click **OK**.

3.4.2 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

Bandwith Limit Configuration

○ Enable ● Disable

Default TX Limit: 5000 Kbps   Default RX Limit: 5000 Kbps

Limitation List

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

Specific Limitation

Start IP: ______   End IP: ______

TX Limit: ______ Kbps   RX Limit: ______ Kbps

1. Bandwidth limit only works for 'NEW' sessions. Original sessions are controlled by HNAT.
2. If the IP is controlled by bandwidth limit, throughput would be lower than 64Mbps."

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.

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 Bandwidth limit can be applied on certain IP range. That's, only the PCs within the range will be influenced by the bandwidth limitation set here. Please define the start IP address for the specific limitation.

End IP Define the end IP address for the specific limitation.

TX Limit Define the limitation for the speed of the upstream to be applied as specific limitation. 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 to be applied as specific limitation. 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.

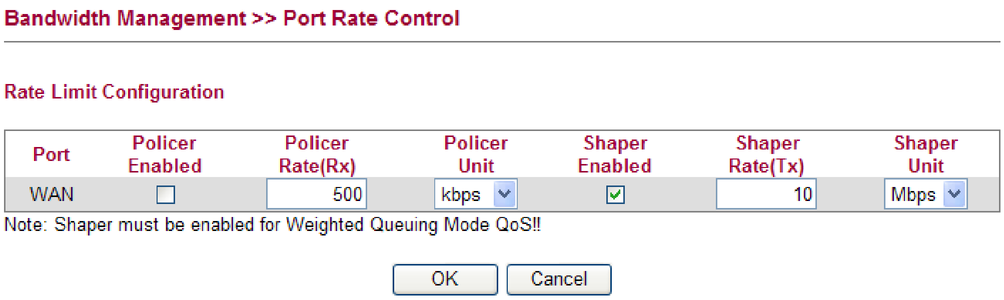
Edit Allows you to edit the settings for the selected limitation.

Delete Remove the selected settings existing on the limitation list.

When you finish adding a new bandwidth limit, simply click **OK**.

3.4.3 Port Rate Control

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue. And a shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues. This page allows you to configure the switch port rate limit for Policers and Shapers.



Bandwidth Management >> Port Rate Control

Rate Limit Configuration

Port	Policer Enabled	Policer Rate(Rx)	Policer Unit	Shaper Enabled	Shaper Rate(Tx)	Shaper Unit
WAN	□	500	kbps	☑	10	Mbps

Note: Shaper must be enabled for Weighted Queuing Mode QoS!!

Port Represent LAN or WAN interface.

Policer Enabled Check this box to enable policer function.

Policer Rate(Rx) Type the number for policer function. The default value is 500. It is restricted to 500-1000000 when the Policer Unit is set in kbps, and it is restricted to 1-1000 when the Policer Unit is set in Mbps.

Policer Unit Determine the unit (kbps/Mbps) for policer.

Shaper Enabled Check this box to enable shaper function.

Shaper Rate (Tx) Type the number for shaper function. The default value is 500. It is restricted to 500-1000000 when the Shaper Unit is set in kbps, and it is restricted to 1-1000 when the Shaper Unit is set in Mbps.

Shaper Unit Determine the unit (kbps/Mbps) for shaper function.

3.4.4 QoS Control List

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?

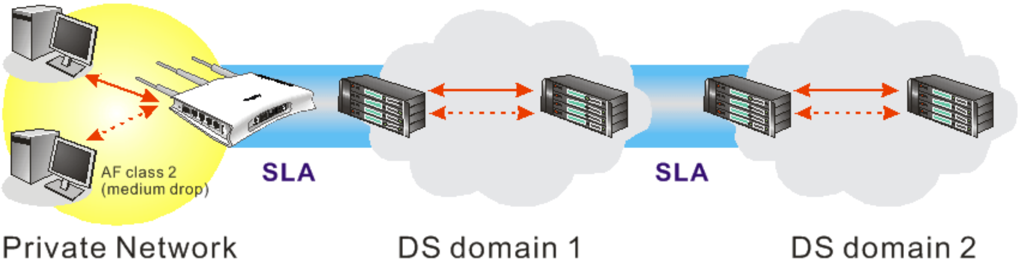
There are two components within Primary configuration of QoS deployment:

- 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.

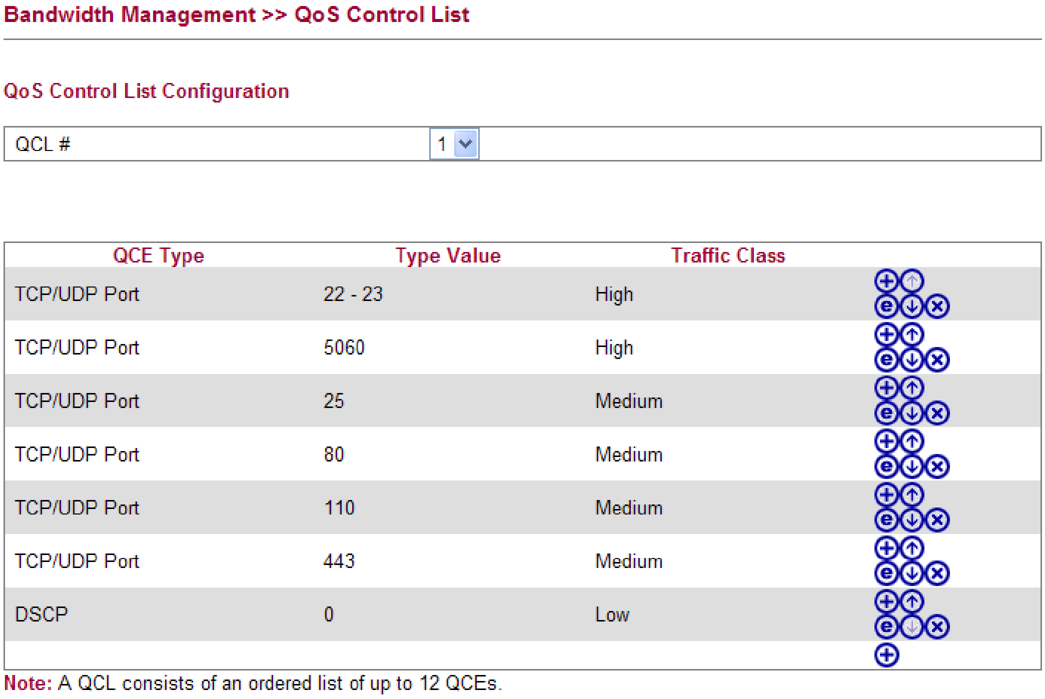
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes 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 **QoS Control List** (QCL) to open the web page.



Bandwidth Management >> QoS Control List

QoS Control List Configuration

QCL #	1

QCE Type	Type Value	Traffic Class	
TCP/UDP Port	22 - 23	High	⊕ ⓔ ⓧ
TCP/UDP Port	5060	High	⊕ ⓔ ⓧ
TCP/UDP Port	25	Medium	⊕ ⓔ ⓧ
TCP/UDP Port	80	Medium	⊕ ⓔ ⓧ
TCP/UDP Port	110	Medium	⊕ ⓔ ⓧ
TCP/UDP Port	443	Medium	⊕ ⓔ ⓧ
DSCP	0	Low	⊕ ⓔ ⓧ
			⊕

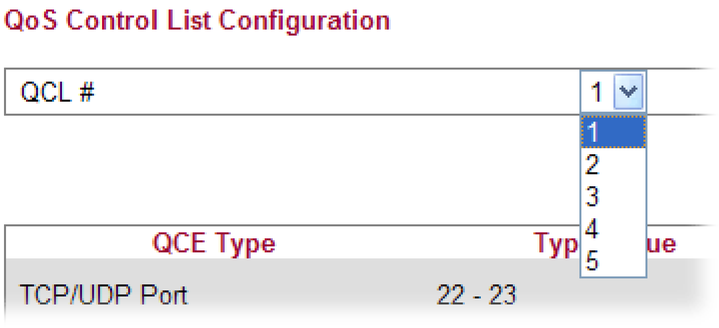
Note: A QCL consists of an ordered list of up to 12 QCEs.

QCE Type Display the type of that QCE (QoS Control Entries).

Type Value Display the value specified for the QCE.

Traffic Class Display the class of the data transmission for the QCE.

QoS Control List allows users to set up to **five** groups of QCL. Each QCL group can contain 12 QCE settings.



QoS Control List Configuration

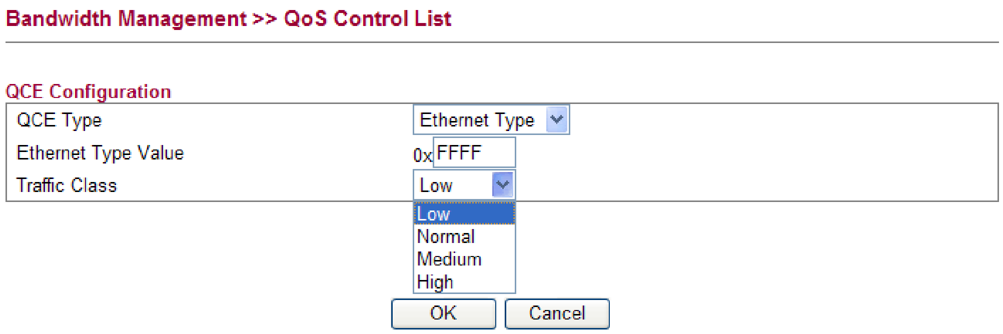
QCL #	1 1 2 3 4 5

QCE Type	Typ ue
TCP/UDP Port	22 - 23

Adding a New QCE

Click ⊕ to add a new QCE onto this page. Different QCE type will bring out different web settings.

- If you choose **Ethernet Type** as QCE Type, you have to type value for it and specify traffic class from Low, Normal, Medium and High.



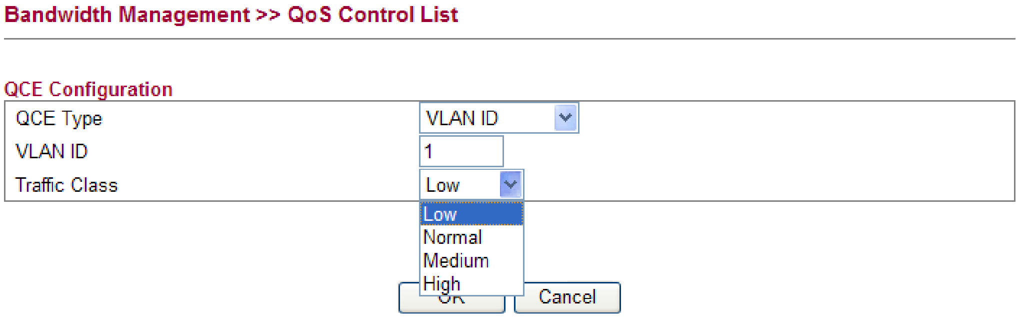
Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	Ethernet Type
Ethernet Type Value	0x FFFF
Traffic Class	Low Low Normal Medium High

Ethernet Type Value Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

- If you choose **VLAN ID** as QCE Type, you have to type the ID number for it and specify traffic class from Low, Normal, Medium and High.

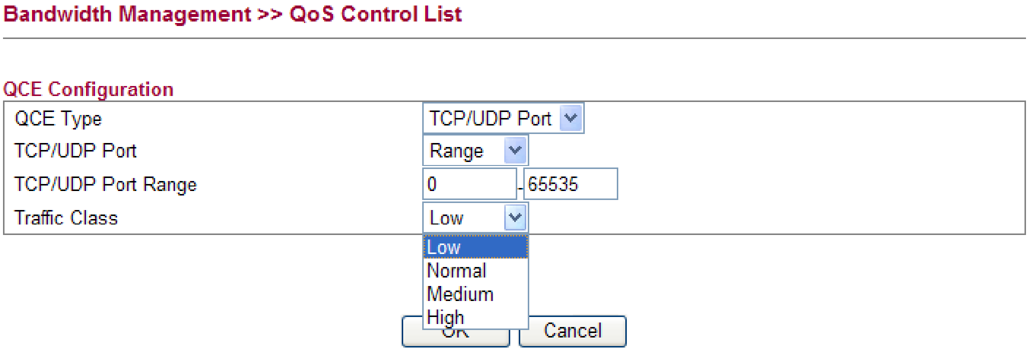


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	VLAN ID
VLAN ID	1
Traffic Class	Low Low Normal Medium High

- If you choose **TCP/UDP Port** as QCE Type, you have to type the port number for it and specify traffic class from Low, Normal, Medium and High.



Bandwidth Management >> QoS Control List

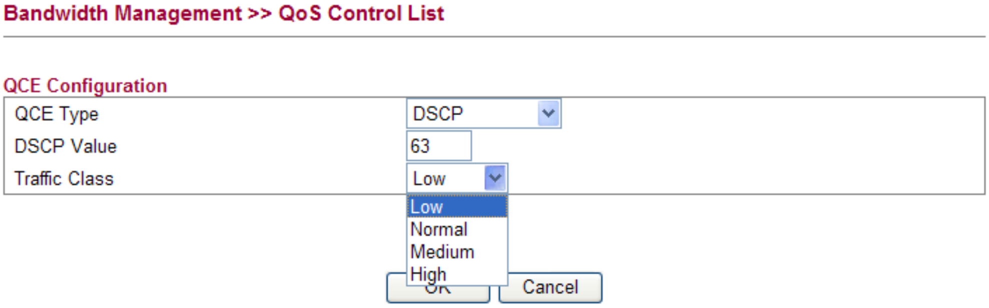
QCE Configuration

QCE Type	TCP/UDP Port
TCP/UDP Port	Range
TCP/UDP Port Range	0 - 65535
Traffic Class	Low

TCP/UDP Port Click **Single** or **Range**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.

TCP/UDP Port Range Type in the starting port number and the end porting number here if you choose Range as the type.

- If you choose **DSCP** as QCE Type, you have to type value for it and specify traffic class from Low, Normal, Medium and High.

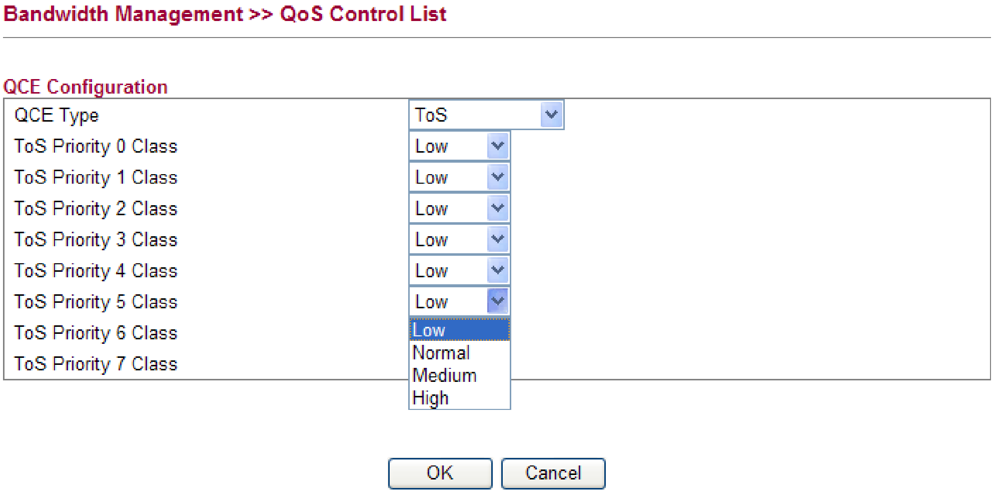


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	DSCP
DSCP Value	63
Traffic Class	Low

- If you choose **ToS** as QCE Type, you have to specify priority class from Low, Normal, Medium and High.

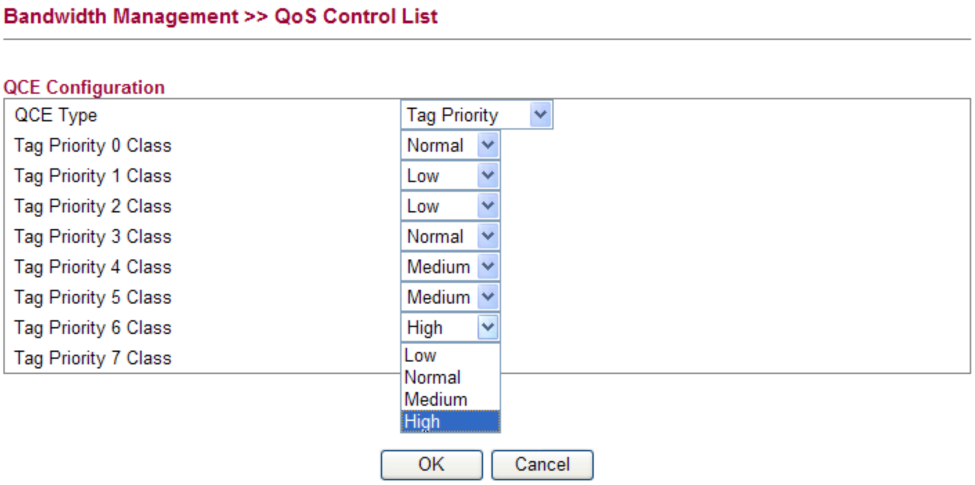


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	ToS
ToS Priority 0 Class	Low
ToS Priority 1 Class	Low
ToS Priority 2 Class	Low
ToS Priority 3 Class	Low
ToS Priority 4 Class	Low
ToS Priority 5 Class	Low
ToS Priority 6 Class	Low
ToS Priority 7 Class	

- If you choose **Tag Priority** as QCE Type, you have to specify priority class from Low, Normal, Medium and High.


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	Tag Priority
Tag Priority 0 Class	Normal
Tag Priority 1 Class	Low
Tag Priority 2 Class	Low
Tag Priority 3 Class	Normal
Tag Priority 4 Class	Medium
Tag Priority 5 Class	Medium
Tag Priority 6 Class	High
Tag Priority 7 Class	High

Editing a QCE

Click ⓔ to modify the settings of an existing QCE on this page.

Moving Up/Down a QCE

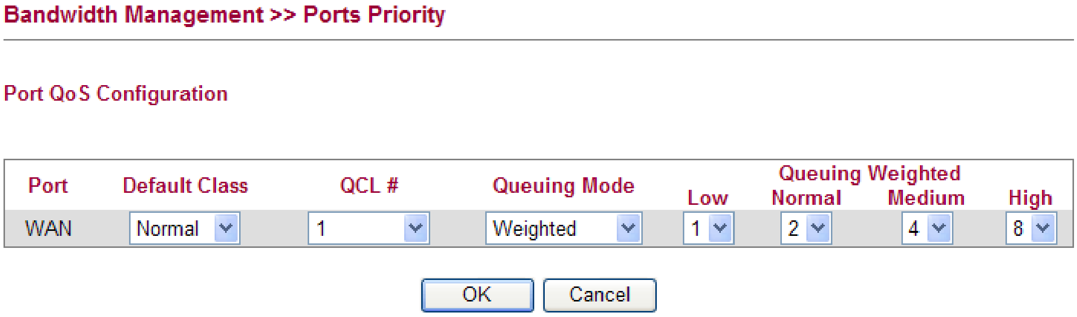
Click ⬇ and ⬆ to move a QCE up and down.

Deleting a QCE

To delete a QCE in the list, simply click ⊗ of that one. It will be removed immediately.

3.4.5 Ports Priority

This page allows you to configure QoS settings for each port. The classification is controlled by a QCL (Quality Control List) that is assigned to each port. A QCL consists of an ordered list of up to 12 QCEs (Quality Control Entry). Each QCE can be used to classify certain frames to a specific QoS class. This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS class for the port.

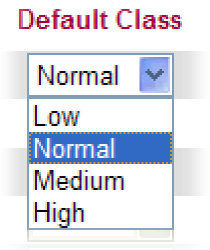

Bandwidth Management >> Ports Priority

Port QoS Configuration

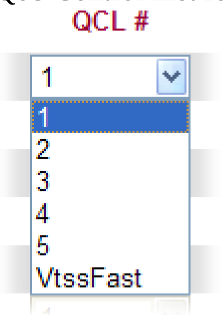
Port	Default Class	QCL #	Queuing Mode	Queuing Weighted Low	 Normal	 Medium	 High
WAN	Normal	1	Weighted	1	2	4	8

Port Indicate the interface for the physical port, WAN port, LAN port and Wireless Port.

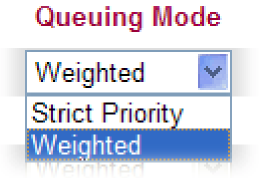
Default Class Use the drop down list to choose the priority for each port.



QCL Use the drop down list to choose the QCL number defined in QoS Control List for the port.



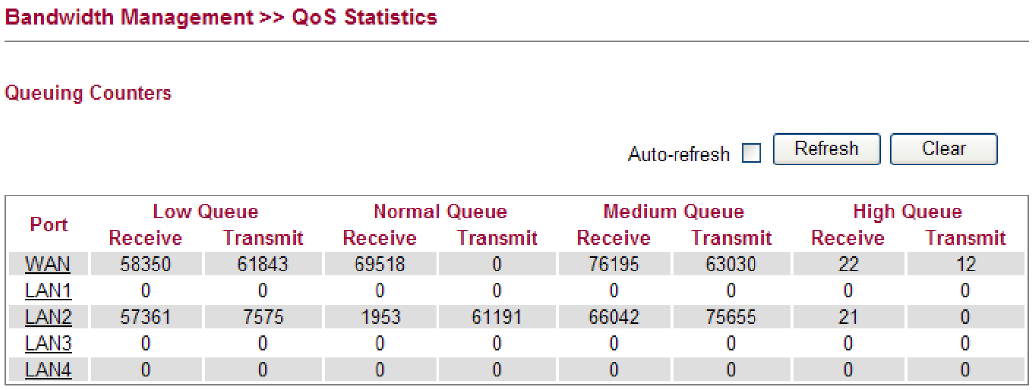
Queuing Mode Use the drop down list to choose suitable mode.



Queue Weighted Use the drop down list to choose 1, 2, 4, or 8 as the queue weighted number.

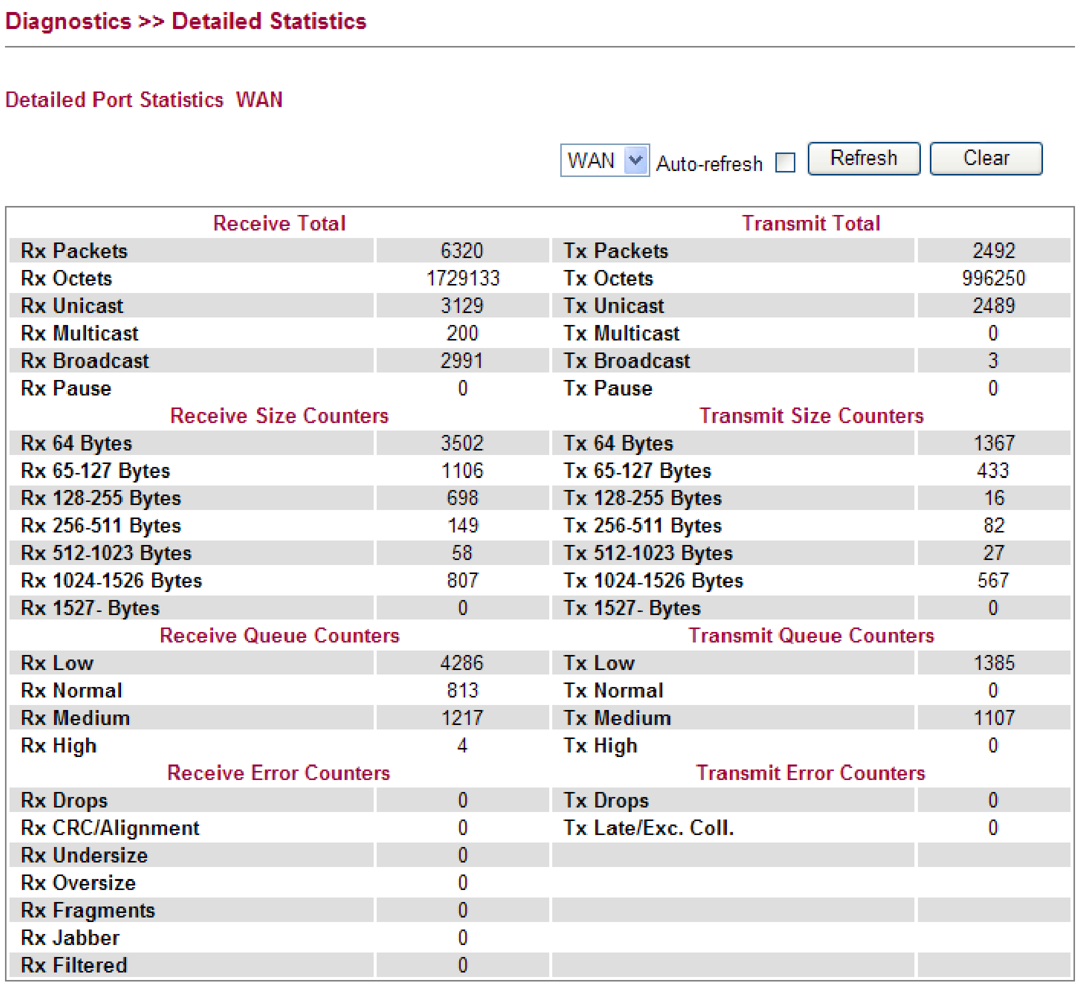
3.4.6 QoS Statistics

This page displays statistics for QoS setting. Click WAN/LAN link to check detailed information for each interface.



Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
WAN	58350	61843	69518	0	76195	63030	22	12
LAN1	0	0	0	0	0	0	0	0
LAN2	57361	7575	1953	61191	66042	75655	21	0
LAN3	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0

Click **WAN/LAN** link to check detailed information for each interface.



Diagnostics >> Detailed Statistics

Detailed Port Statistics WAN

Receive Total		Transmit Total	
Rx Packets	6320	Tx Packets	2492
Rx Octets	1729133	Tx Octets	996250
Rx Unicast	3129	Tx Unicast	2489
Rx Multicast	200	Tx Multicast	0
Rx Broadcast	2991	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	3502	Tx 64 Bytes	1367
Rx 65-127 Bytes	1106	Tx 65-127 Bytes	433
Rx 128-255 Bytes	698	Tx 128-255 Bytes	16
Rx 256-511 Bytes	149	Tx 256-511 Bytes	82
Rx 512-1023 Bytes	58	Tx 512-1023 Bytes	27
Rx 1024-1526 Bytes	807	Tx 1024-1526 Bytes	567
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	4286	Tx Low	1385
Rx Normal	813	Tx Normal	0
Rx Medium	1217	Tx Medium	1107
Rx High	4	Tx High	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Rx Packets Display the counting number of the packet received.

Rx Octets Display the total received bytes.

Rx Unicast Display the counting number of the received unicast packet.

Rx Broadcast Display the counting number of the received broadcast packet.

Rx Pause Display the counting number of the received pause packet.

RX 64 Bytes Display the number of 64-byte frames in good and bad packets received.

RX 65-127 Bytes Display the number of 65 ~ 127-byte frames in good and bad packets received.

RX 128-255 Bytes Display the number of 128 ~ 255-byte frames in good and bad packets received.

RX 256-511 Bytes Display the number of 256 ~ 511-byte frames in good and bad packets received.

RX 512-1023 Bytes Display the number of 512 ~ 1023-byte frames in good and bad packets received.

RX 1024- 1526 Bytes Display the number of 1024-1522-byte frames in good and bad packets received.

RX 1527 Bytes Display the number of 1527-byte frames in good and bad packets received.

Rx Low Display the low queue counter of the packet received.

Rx Normal Display the normal queue counter of the packet received.

Rx Medium Display the medium queue counter of the packet received.

Rx High Display the high queue counter of the packet received.

Rx Drops Display the number of frames dropped due to the lack of receiving buffer.

Rx CRC/Alignment Display the number of Alignment errors packets received.

Rx Undersize Display the number of short frames (<64 Bytes) with valid CRC.

Rx Oversize Display the number of long frames (according to max_length register) with valid CRC.

Rx Fragments Display the number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber Display the number of long frames (according tomax_length register) with invalid CRC.

Rx Filtered Display the filtered number of the packet received.

Tx Packets Display the counting number of the packet transmitted.

Tx Octets Display the total transmitted bytes.

Tx Unicast Display the show the counting number of the transmitted unicast packet.

Tx Multicast Display the show the counting number of the transmitted multicast packet.

Tx Broadcast Display the counting number of the transmitted broadcast packet.

Tx Pause Show the counting number of the transmitted pause packet.

Tx 64 Bytes Display the number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes Display the number of 65 ~ 127-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes Display the number of 128 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes Display the number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes Display the number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024- 1526 Bytes Display the number of 1024 ~ 1522-byt frames in good and bad packets transmitted.

Tx 1527 Bytes: Display the number of 1527-byte frames in good and bad packets transmitted.

Tx Low Display the low queue counter of the packet transmitted.

Tx Normal Display the normal queue counter of the packet transmitted.

Tx Medium Display the medium queue counter of the packet received.

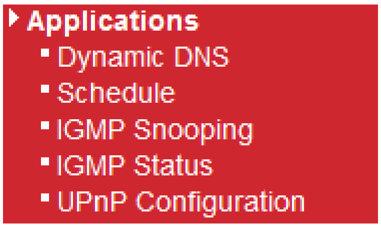
Tx High Display the high queue counter of the packet received.

Tx Drops Display the number of frames dropped due to excessive collision, late collision, or frame aging.

Tx lat/Exc.Coll. Display the number of Frames late collision or excessive collision Error, which switch transmitted

3.5 Applications

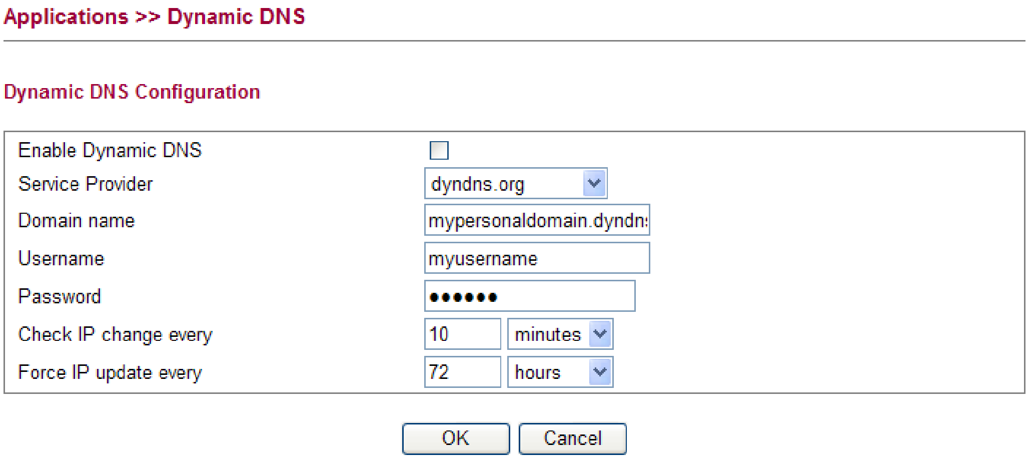
Below shows the menu items for Applications.



3.5.1 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.


Applications >> Dynamic DNS

Dynamic DNS Configuration

Enable Dynamic DNS	□
Service Provider	dyndns.org
Domain name	mypersonaldomain.dyndn:
Username	myusername
Password	••••••
Check IP change every	10 minutes
Force IP update every	72 hours

Enable Dynamic DNS Check this box to enable the current account.

DynDNS Service Select the service provider for the DDNS account.

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

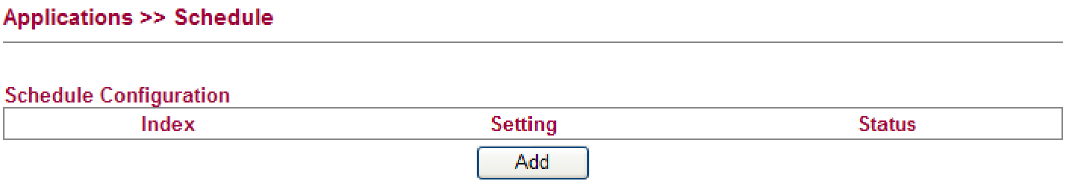
Username	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Check IP change every	Set the interval for checking the information.
Force IP update every	Force the router updates its information to DDNS server with the interval set here.

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

3.5.2 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.

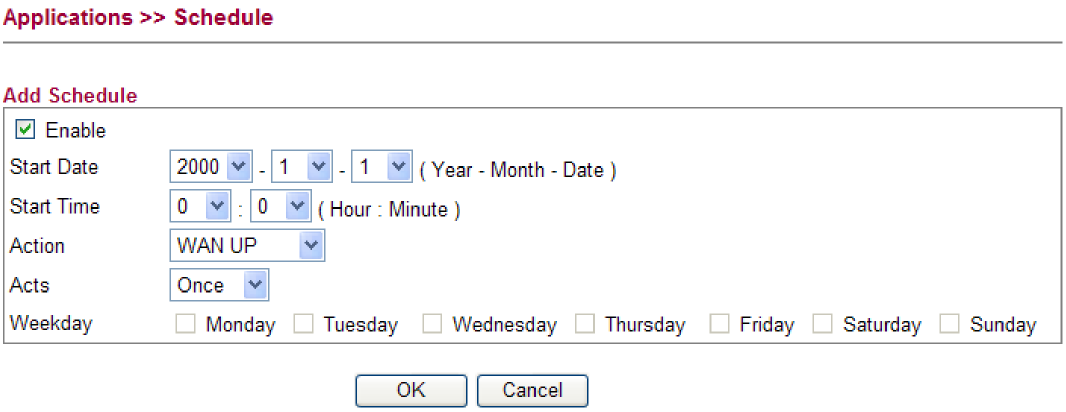
You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry 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 Configuration

Index	Setting	Status

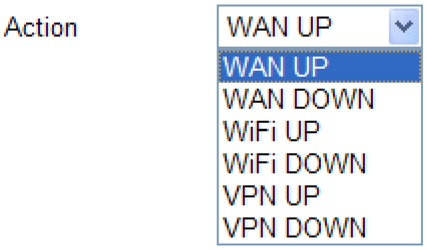
You can set up to 15 schedules. To add a schedule profile, please click **Add**.


Applications >> Schedule

Add Schedule

☑ Enable	
Start Date	2000 - 1 - 1 (Year - Month - Date)
Start Time	0 : 0 (Hour : Minute)
Action	WAN UP
Acts	Once
Weekday	□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Enable	Check to enable the schedule.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
Action	Specify which action should be applied during the period of the schedule.



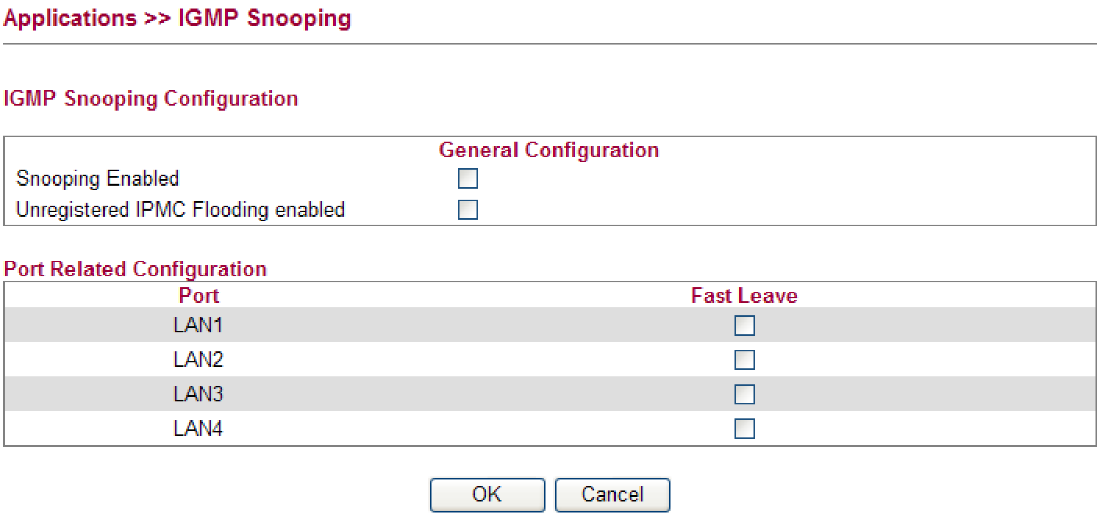
Action WAN UP

WAN UP/DOWN – WAN connection will be activated / inactivated based on the time schedule configured here.
WiFi UP/DOWN – Wireless Wi-Fi connection will be activated / inactivated based on the time schedule configured here.
VPN UP/DOWN - VPN connection will be activated / inactivated based on the time schedule configured here.

Acts Specify how often the schedule will be applied
Once -The schedule will be applied just once
Routine or **Weekdays** -Specify which days in one week should perform the schedule.

3.5.3 IGMP Snooping

IGMP snooping means multicast traffic will be forwarded to ports that have members of that group. If you disable IGMP snooping, the system will make multicast traffic treated in the same manner as broadcast traffic.



Applications >> IGMP Snooping

IGMP Snooping Configuration

General Configuration

Snooping Enabled	□
Unregistered IPMC Flooding enabled	□

Port Related Configuration

Port	Fast Leave
LAN1	□
LAN2	□
LAN3	□
LAN4	□

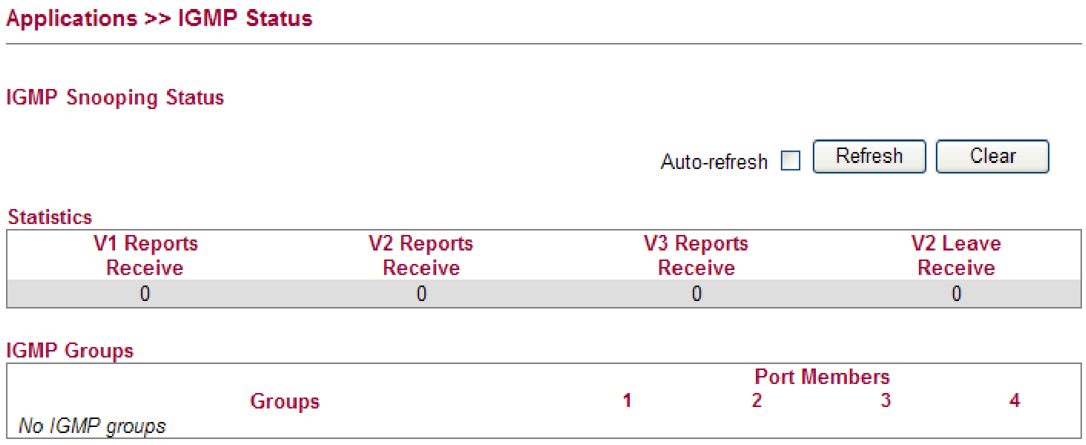
Snooping Enabled Check the box to enable this function.

Unregistered IPMC… Check the box to enable unregistered IPMC traffic flooding.

Fast Leave Check the box to Fast Leave on the LAN port.

3.5.4 IGMP Status

This page display current IGMP snooping status.



Applications >> IGMP Status

IGMP Snooping Status

Auto-refresh □ Refresh Clear

Statistics

V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
0	0	0	0

IGMP Groups

Groups	Port Members 1	2	3	4
No IGMP groups				

V1~3 Reports Receive Display the number of Received V1 – V3 Reports.

V2 Leave Receive Display the number of Received V2 Leave.

Groups Display current IGMP groups. Maximum number of group for each VLAN can be set is 128.

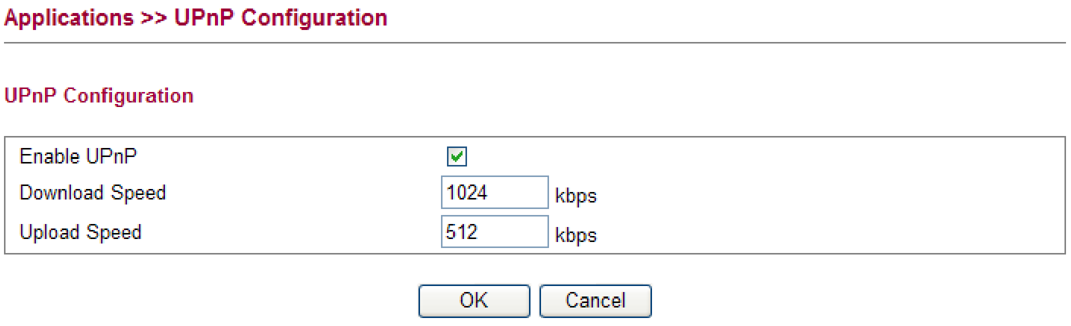
Port Members Display the LAN ports in this group.

Refresh Click this button to refresh the page immediately.

Clear Click this button to clear the settings on this page.

3.5.5 UPnP Configuration

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 Configuration

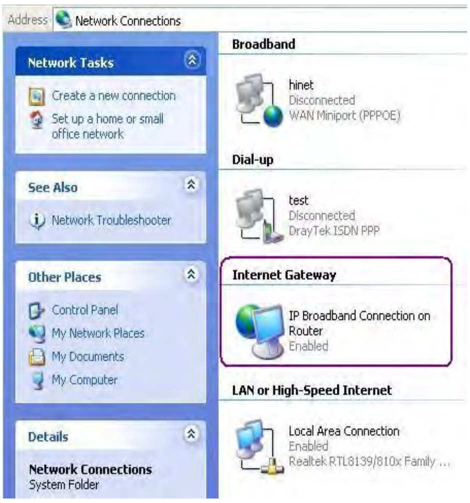
UPnP Configuration

Enable UPnP	☑
Download Speed	1024 kbps
Upload Speed	512 kbps

OK Cancel

Enable UPNP Enable UPnP function. You have to type the download and upload speed.

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

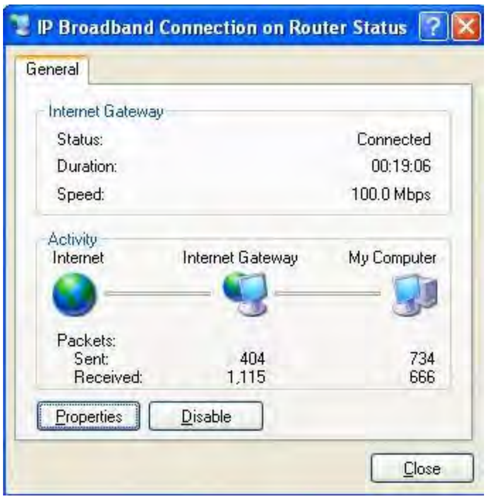
Network Connections
System Folder

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

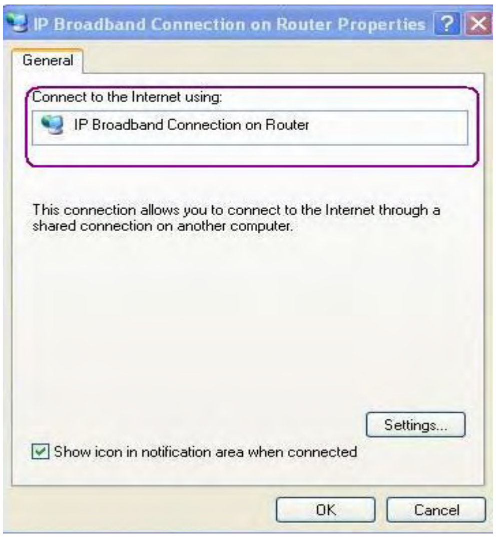
Internet Gateway

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

Activity

Packets:	Internet Gateway	My Computer
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

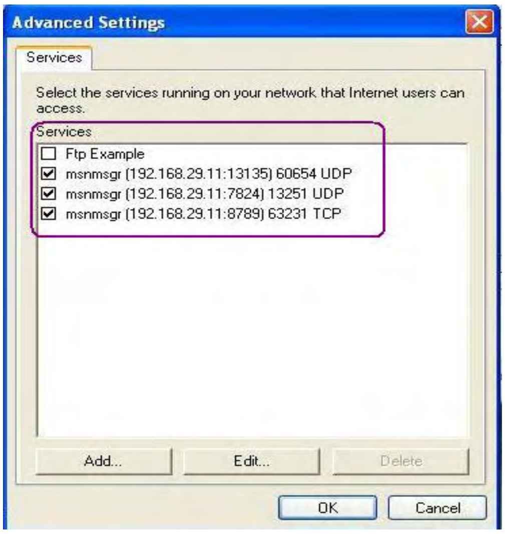
General

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.

3.6 Wireless LAN

This function is used for “n” models.

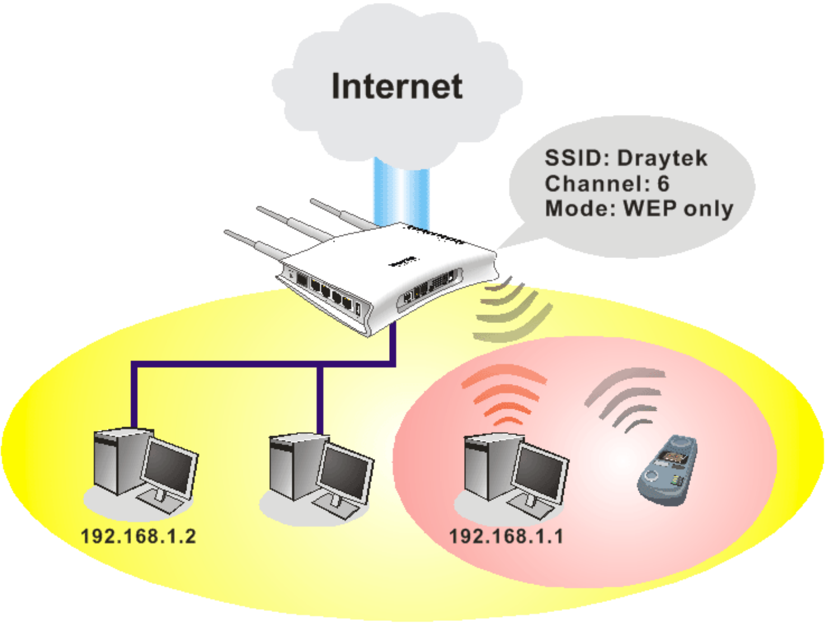
3.6.1 Basic Concepts

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.

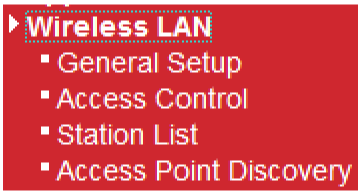
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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.

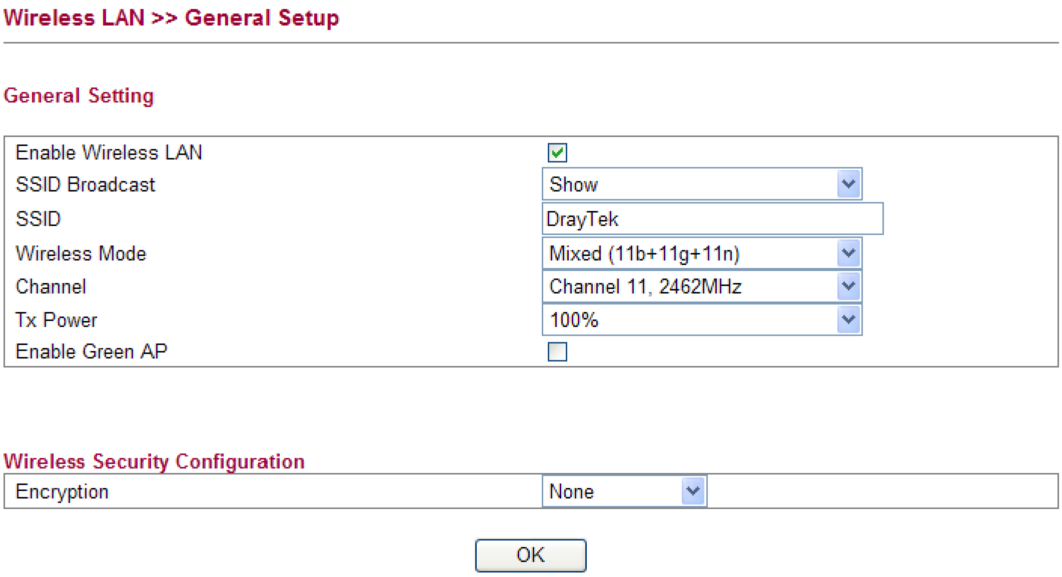
Below shows the menu items for Wireless LAN.



3.6.2 General Setup

By clicking the **General Setup**, 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

Enable Wireless LAN	☑
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Channel	Channel 11, 2462MHz
Tx Power	100%
Enable Green AP	□

Wireless Security Configuration

Encryption	None

Enable Wireless LAN Check the box to enable the wireless function.

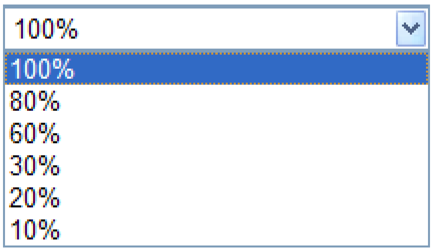
SSID Broadcast Choose **Show** to make the SSID being seen by wireless clients. Choose **Hide** to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.

SSID It 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.

Wireless Mode Choose the wireless mode for this router. At present, only 802.11B/B/N mix is available.

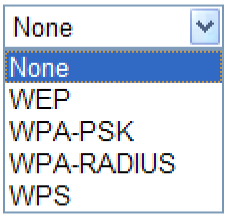
Channel It means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **Auto** to let system determine for you.

Tx Power Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.



Enable Green AP Such function is used to reduce the power consumption (Green AP) for the access point. When there is no station connected, the power consumption of access point will be reduced.

Encryption Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.



Each encryption mode will bring out different web page and ask you to offer additional configuration.

Wireless Security Configuration

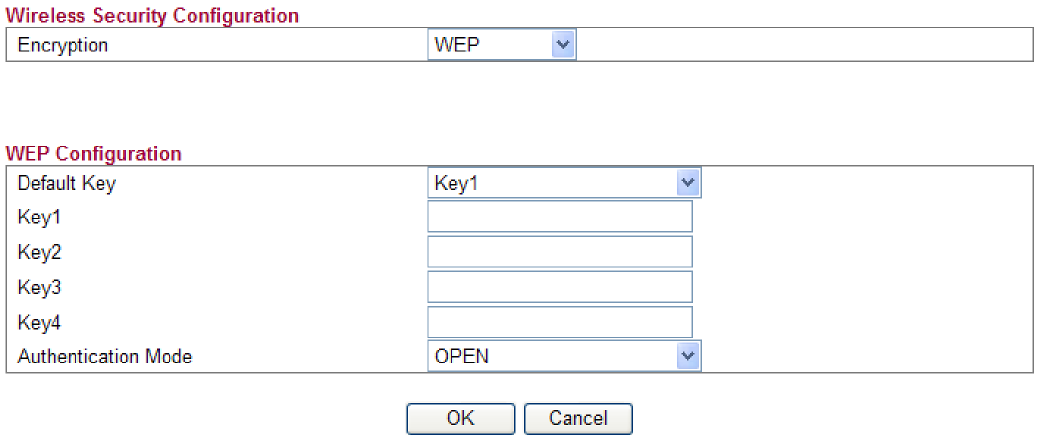
For the security of your system, choose the proper encryption for data transmission. Different encryption mode will bring out different setting encryption ways.

- **None**

  The encryption mechanism is turned off.

- **WEP**

  Accepts only WEP clients and the encryption key should be entered in WEP Key.



Wireless Security Configuration

Encryption	WEP

WEP Configuration

Default Key	Key1
Key1	
Key2	
Key3	
Key4	
Authentication Mode	OPEN

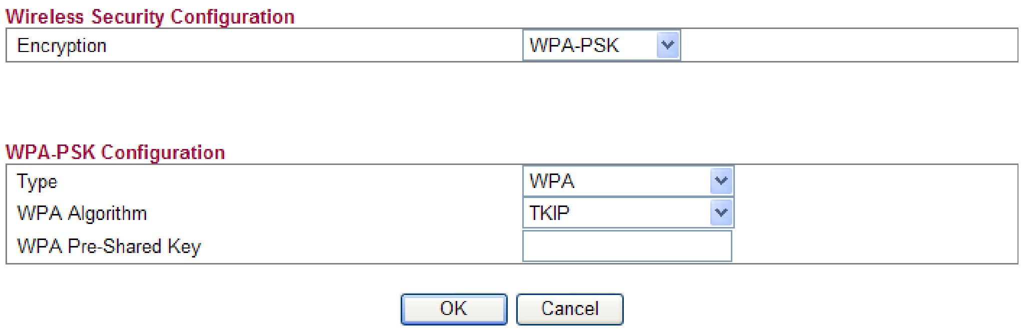
Default Key All wireless devices must support the same WEP encryption bit size and have the same key.

Key1-Key4 **Four keys** can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ',' .

Authentication Mode Choose OPEN or SHARED as the authentication mode.
OPEN: Set wireless to authentication open mode.
SHARED: Set wireless to authentication shared mode.

- **WPA-PSK**

Accepts only WPA clients and the encryption key should be entered in PSK. 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.



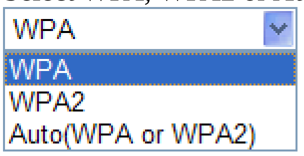
Wireless Security Configuration

Encryption	WPA-PSK

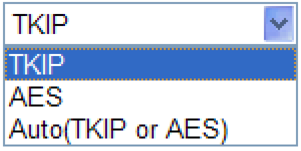
WPA-PSK Configuration

Type	WPA
WPA Algorithm	TKIP
WPA Pre-Shared Key	

WPA Mode Select WPA, WPA2 or Auto as the type.



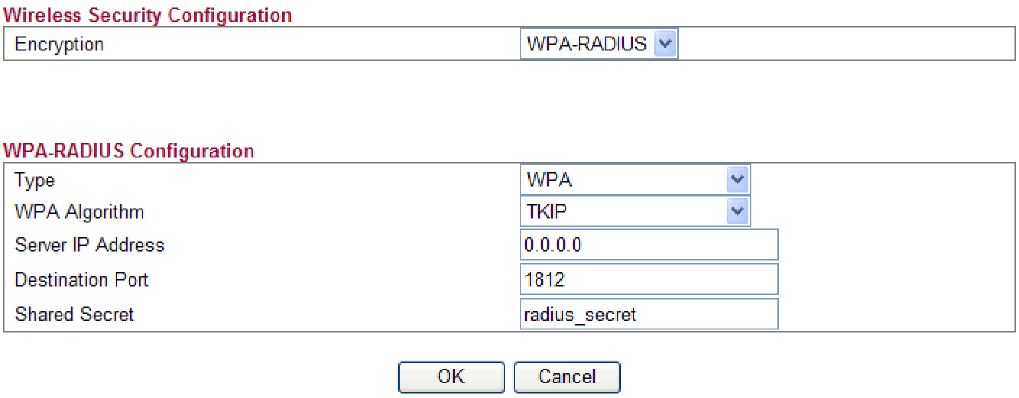
WPA Algorithm Select TKIP, AES or auto as the algorithm for WPA.



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

- **WPA-RADIUS**

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.



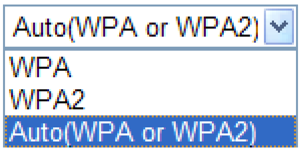
Wireless Security Configuration

Encryption	WPA-RADIUS

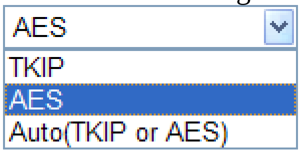
WPA-RADIUS Configuration

Type	WPA
WPA Algorithm	TKIP
Server IP Address	0.0.0.0
Destination Port	1812
Shared Secret	radius_secret

Type 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. Select WPA, WPA2 or Auto as WPA mode.



WPA Algorithm Choose the WPA algorithm, TKIP, AES or Auto.



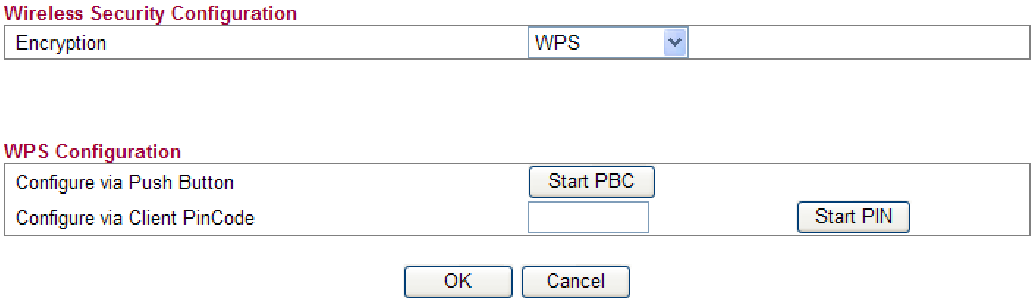
Server IP Address Enter the IP address of RADIUS server.

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.

- **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.



Wireless Security Configuration

Encryption	WPS

WPS Configuration

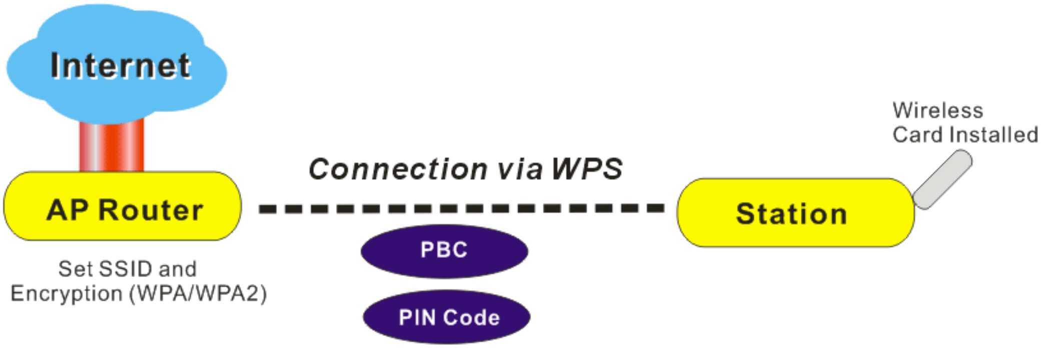
Configure via Push Button	Start PBC	
Configure via Client PinCode		Start PIN

OK Cancel

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 Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN 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

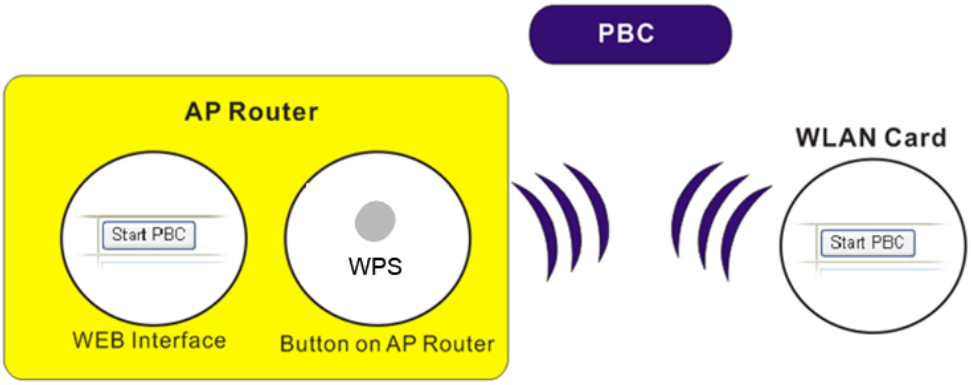
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.



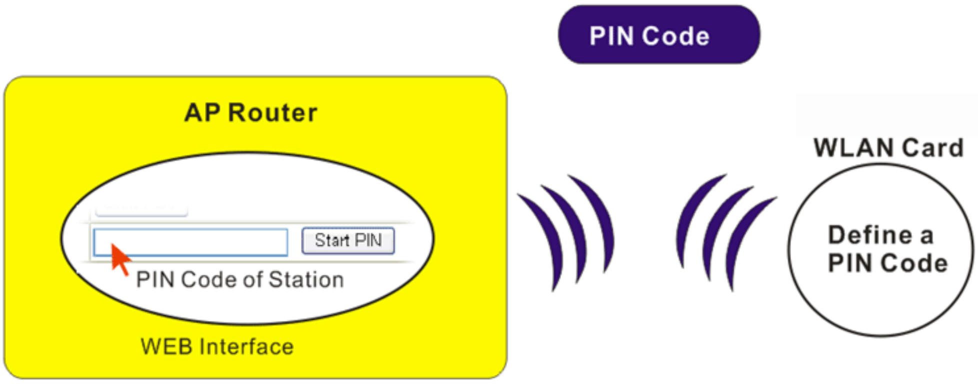
Note: Such function is available for the wireless station with WPS supported.

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 2130 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.

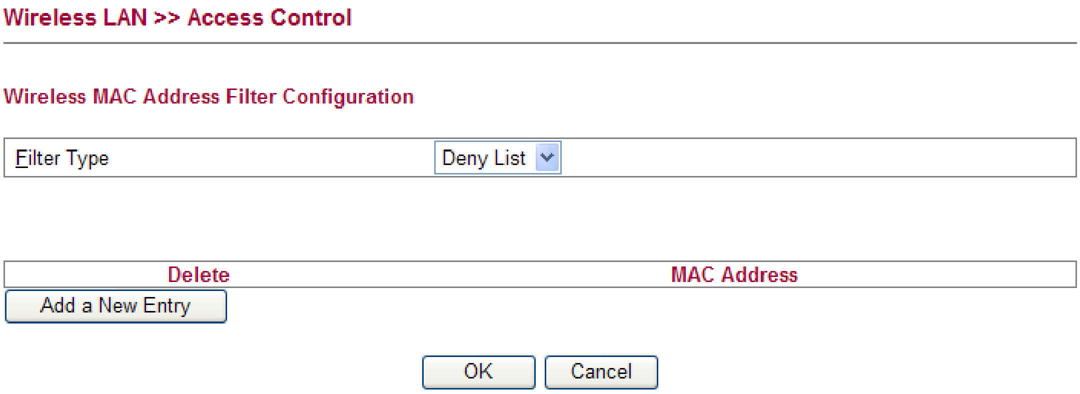


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



3.6.3 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 (deny or allow).



Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type	Deny List

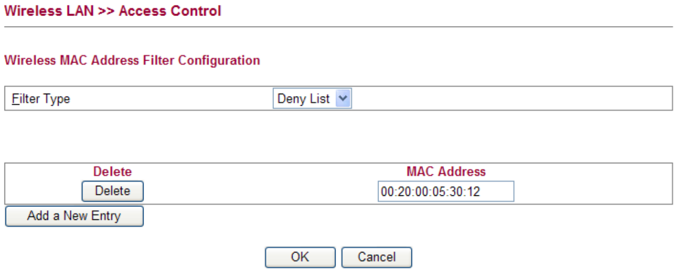
Delete	MAC Address

Filter Type Choose the rule for the MAC addresses displayed in this page.
Allow List – all the MAC address of wireless clients listed here are allowed to do wireless connection.

Deny List – all the MAC address of wireless clients listed here will be blocked.

Add a New Entry Add a new MAC address into the list.

Delete Delete the selected MAC address in the list. This button will appear only an entry of MAC Address has been typed.



Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type	Deny List

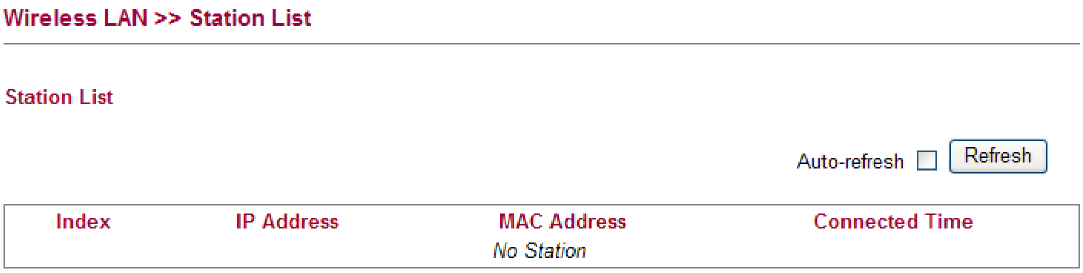
Delete	MAC Address
Delete	00:20:00:05:30:12

Cancel Give up the configuration.

OK Click it to save the configuration.

3.6.4 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.



Wireless LAN >> Station List

Station List

Auto-refresh □

Index	IP Address	MAC Address	Connected Time
		No Station	

Index Display the number of the connecting client.

IP Address Display the WAN IP address for the connecting client.

MAC Address Display the MAC Address for the connecting client.

Connected Time Display the connection time for the connecting client.

Auto-refresh Check this box to force the system refreshing the table automatically**.**

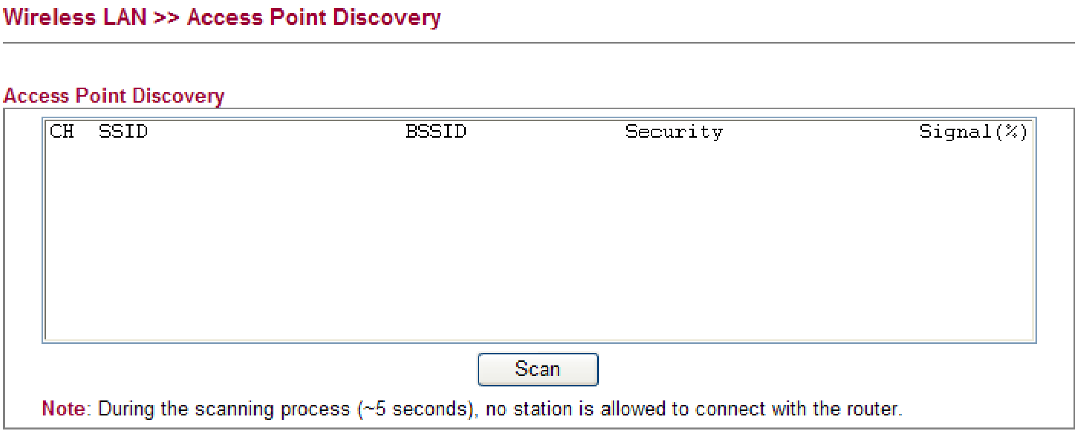
Refresh Click this button to refresh current page.

3.6.5 Access Point 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.

> **Note:** During the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

The table will list channel, SSID, BSSID, Security and the Signal strength of working APs in the neighborhood.



Wireless LAN >> Access Point Discovery

Access Point Discovery

CH	SSID	BSSID	Security	Signal(%)

Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

CH Display the channel for the scanned AP.

SSID Display the SSID of the scanned AP.

BSSID Display the MAC address of the scanned AP.

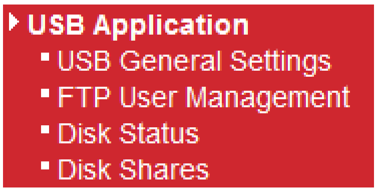
Security Display the encryption type of the scanned AP.

Signal Display the strength (in percentage) of the signal of the scanned AP.

Scan It is used to discover all the connected AP. The results will be shown on the box above this button.

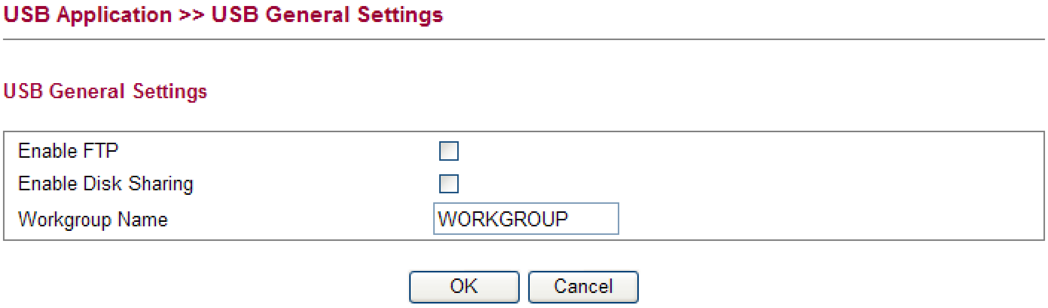
3.7 USB Application

USB diskette can be regarded as an FTP server. By way of Vigor router, uses on LAN/WAN can access, write and read data stored in USB diskette. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>FTP User Management** on the FTP client software. Thus, the client can use the FTP site (USB diskette) through Vigor router.



3.7.1 USB General Settings

At present, the Vigor router can support USB diskette with versions 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

Enable FTP	□
Enable Disk Sharing	□
Workgroup Name	WORKGROUP

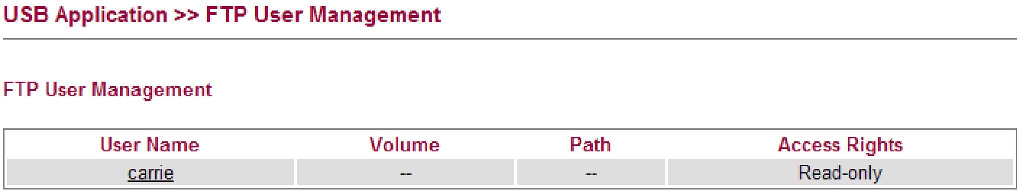
Enable FTP Check this box to enable FTP connection.

Enable Disk Sharing Check this box to enable Samba file sharing.

Workgroup Name Type the name for FTP 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.

3.7.2 FTP User Management

This page allows you to change user setting for USB storage disk. Before modifying settings in this page, please insert a USB diskette and configure settings in **User>>User Configuration** first. Otherwise, an error message will appear to warn you.

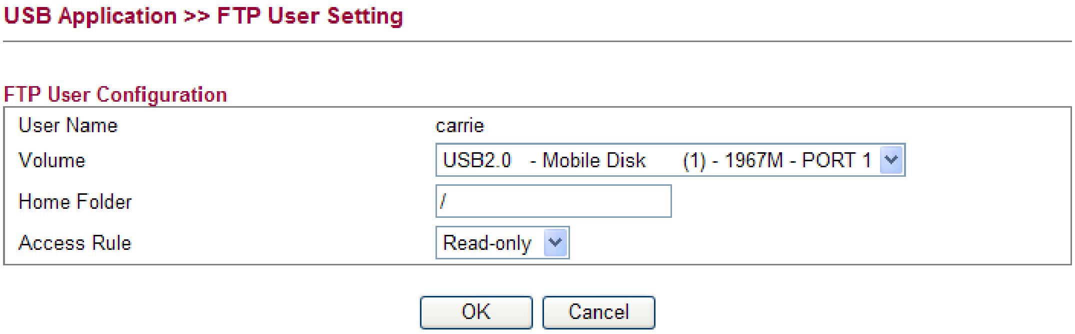


USB Application >> FTP User Management

FTP User Management

User Name	Volume	Path	Access Rights
carrie	--	--	Read-only

Click the name link under User Name to open the setting web page.



USB Application >> FTP User Setting

FTP User Configuration

User Name	carrie
Volume	USB2.0 - Mobile Disk (1) - 1967M - PORT 1
Home Folder	/
Access Rule	Read-only

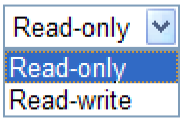
User Name It displays the username that user uses to login to the FTP server.

Volume Select the proper volume for the connected USB diskette.

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.

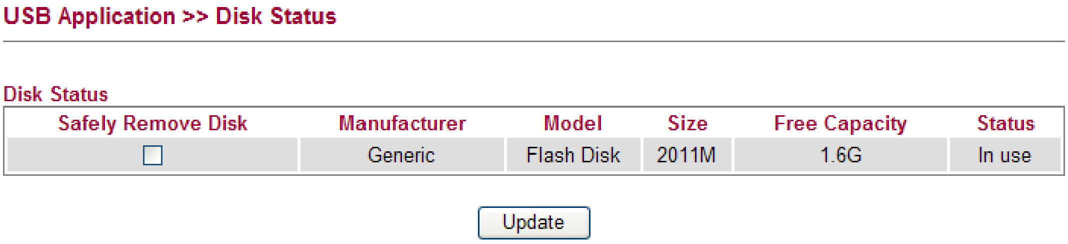
Access Rule Select the access right for the USB diskette.



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

3.7.3 Disk Status

This page can display current using status of the USB diskette. If you want to remove the diskette from USB port in router, please check the box of Safely Remove Disk first. And then, remove the USB diskette later.



USB Application >> Disk Status

Disk Status

Safely Remove Disk	Manufacturer	Model	Size	Free Capacity	Status
□	Generic	Flash Disk	2011M	1.6G	In use

Safely Remove Disk Check this box and then you can remove the USB diskette safely.

Manufacturer Display the manufacturer of the disk.

Model Display the type of the disk.

Size Display the storage space of the diskette(s).

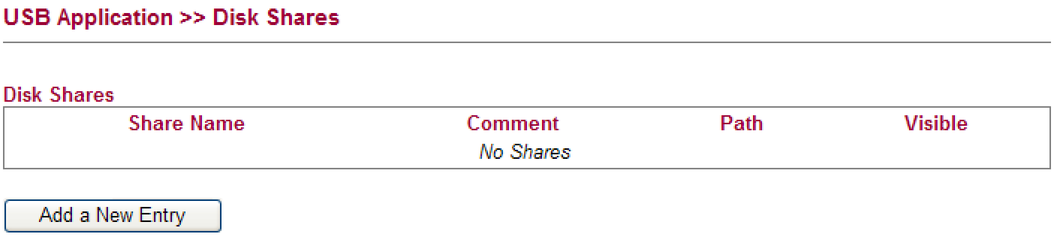
Free Capacity Display the free disk space of the diskette(s).

Status Display current usage status of the diskette(s)

Update Click this button to refresh the disk status.

3.7.4 Disk Shares

This page can define the folder which will be shared while Samba File Sharing is enabled.

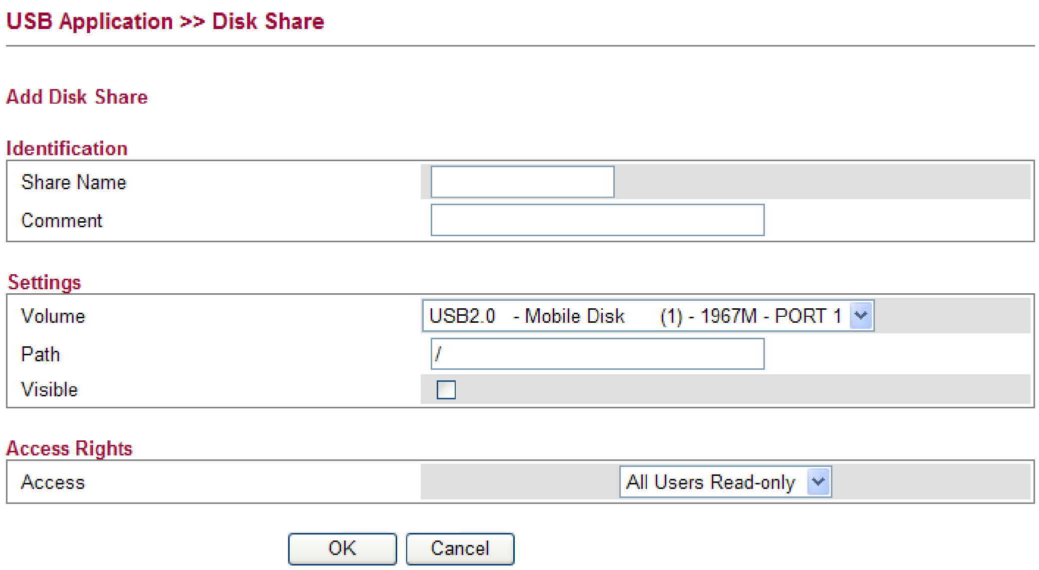


USB Application >> Disk Shares

Disk Shares

Share Name	Comment	Path	Visible
	No Shares		

To add a new entry for disk sharing, please click **Add a New Entry** to open the following page.



USB Application >> Disk Share

Add Disk Share

Identification

Share Name	
Comment	

Settings

Volume	USB2.0 - Mobile Disk (1) - 1967M - PORT 1
Path	/
Visible	□

Access Rights

Access	All Users Read-only

Share Name Type a name to be used as shared folder name in Samba service. The name must not contain spaces or special characters.

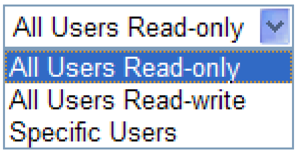
Comment Type the brief description for the disk sharing. The words here will be seen in Network Neighborhood on Windows client computers

Volume Select the proper volume for the connected USB diskette.

Path 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.

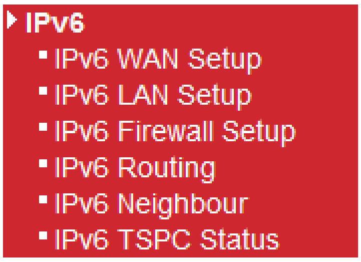
Visible Check this box to make the shared folder to be seen in Network Neighborhood on Windows of clients in local network.

Access Rights Specify the access right and apply to all the wireless clients that want to connect to the attached USB diskette.



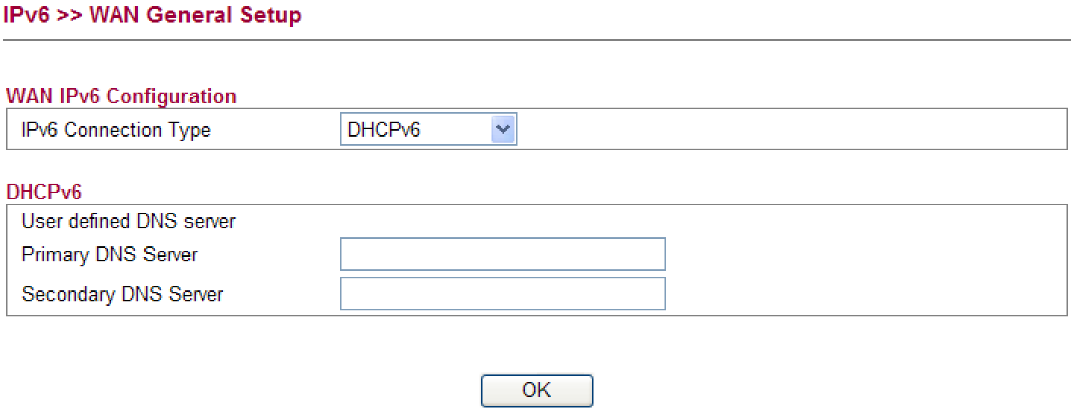
All Users Read-only - everyone has read-only access to the share disk.
All Users Read-write - everyone has read-write access to the share disk.
Specific Users – Only specific user(s) can access into the share disk.

3.8 IPv6



3.8.1 IPv6 WAN Setup

This page defines the IPv6 connection types for WAN interface. Possible types contain Link-Local only, Static IPv6, DHCPv6 and TSPC. Each type requires different parameter settings.



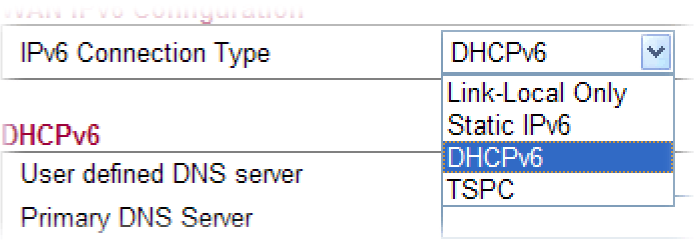
IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	DHCPv6

DHCPv6

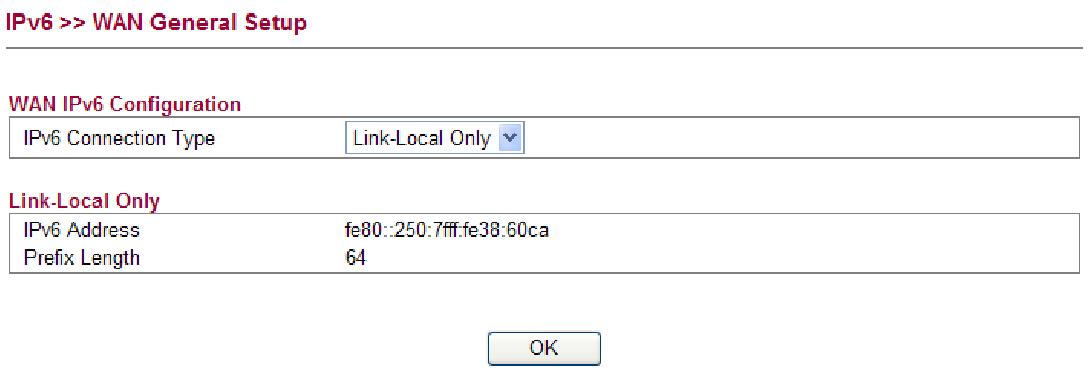
User defined DNS server	
Primary DNS Server	
Secondary DNS Server	



IPv6 Connection Type: DHCPv6

Link-Local Only

Link-Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/10**. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type: Link-Local Only

Link-Local Only

IPv6 Address: fe80::250:7fff:fe38:60ca

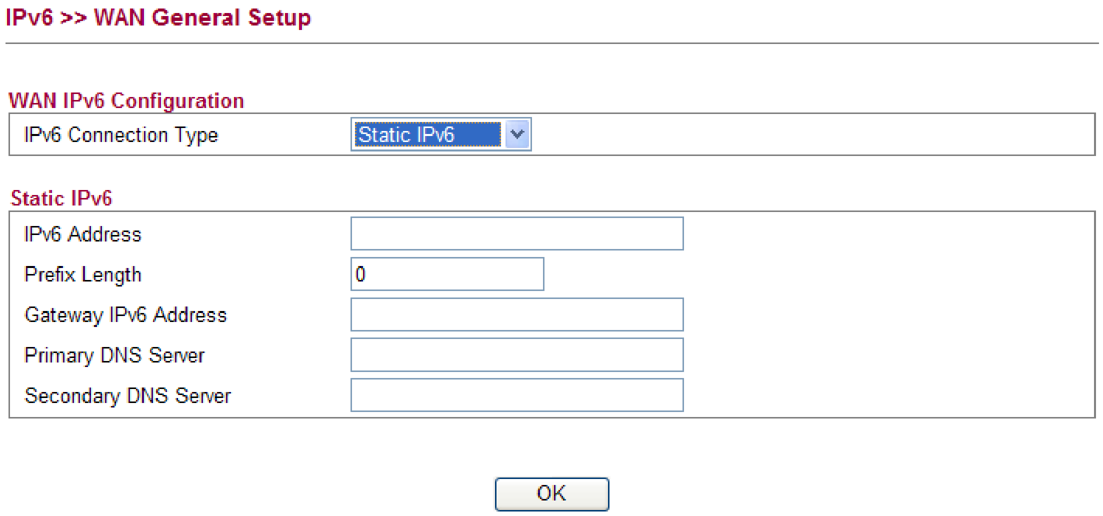
Prefix Length: 64

IPv6 Address The least significant 64 bits are usually chosen as the interface hardware address constructed in modified EUI-64 format.

Prefix Length Display the fixed value (64) for prefix length.

Static IPv6

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type: Static IPv6

Static IPv6

IPv6 Address:

Prefix Length: 0

Gateway IPv6 Address:

Primary DNS Server:

Secondary DNS Server:

IPv6 Address Type your IPv6 static IP here.

Prefix Length Type your IPv6 address prefix length here.

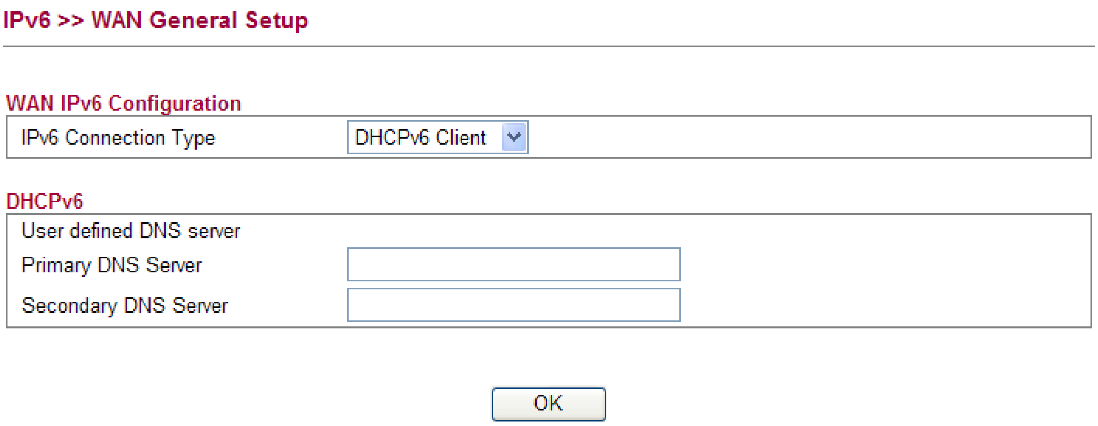
Gateway IPv6 Server Type your IPv6 gateway address here.

Primary DNS Server Type your IPv6 primary DNS Server address here.

Secondary DNS Server Type your IPv6 secondary DNS Server address here.

DHCPv6 Client

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	DHCPv6 Client

DHCPv6

User defined DNS server	
Primary DNS Server	
Secondary DNS Server	

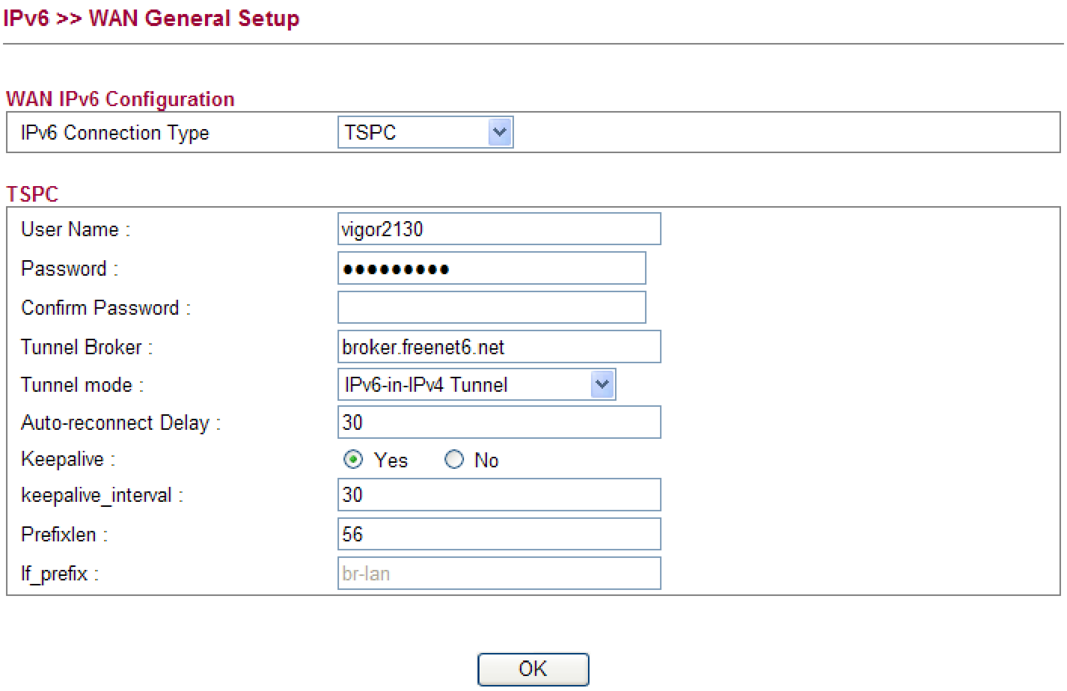
Primary DNS Server	Type primary DNS Server address here.
Secondary DNS Server	Type secondary DNS Server address here

TSPC

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

Please make sure your IPv4 WAN connection is OK and apply one free account from hexage (http://go6.net/4105/register.asp) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	TSPC

TSPC

User Name :	vigor2130
Password :	●●●●●●●●●
Confirm Password :	
Tunnel Broker :	broker.freenet6.net
Tunnel mode :	IPv6-in-IPv4 Tunnel
Auto-reconnect Delay :	30
Keepalive :	● Yes ○ No
keepalive_interval :	30
Prefixlen :	56
If_prefix :	br-lan

Username	Type the name obtained from the broker. “vigor2130” is a default username applied from

http://go6.net/4105/register.asp. It is suggested for you to apply another username and password.

Password Type the password assigned with the user name.

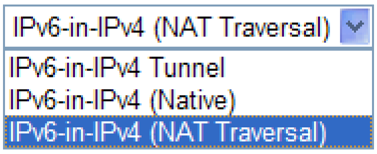
Confirm Password Type the password again to make the confirmation.

Tunnel Broker Type the address for the tunnel broker IP, FQDN or an optional port number.

Tunnel Mode **IPv6-in-IPv4 Tunnel-** Let the broker choose the tunnel mode appropriate for the client.

IPv6-in-IPv4 (Native) - Request an IPv6 in IPv4 tunnel.

IPv6-in-IPv4 (NAT Traversal - Request an IPv6 in UDP of IPv4 tunnel (for clients behind a NAT).



Auto-reconnect Delay After passing the time set here, the client will retry to connect in case of failure or keepalive timeout.
0 means not retry.

Keepalive **Yes** – Keep the connection between TSPC and tunnel broker always on. TSPC will send ping packet to make sure the connection between both ends is normal.
No - The client will not send keepalives.

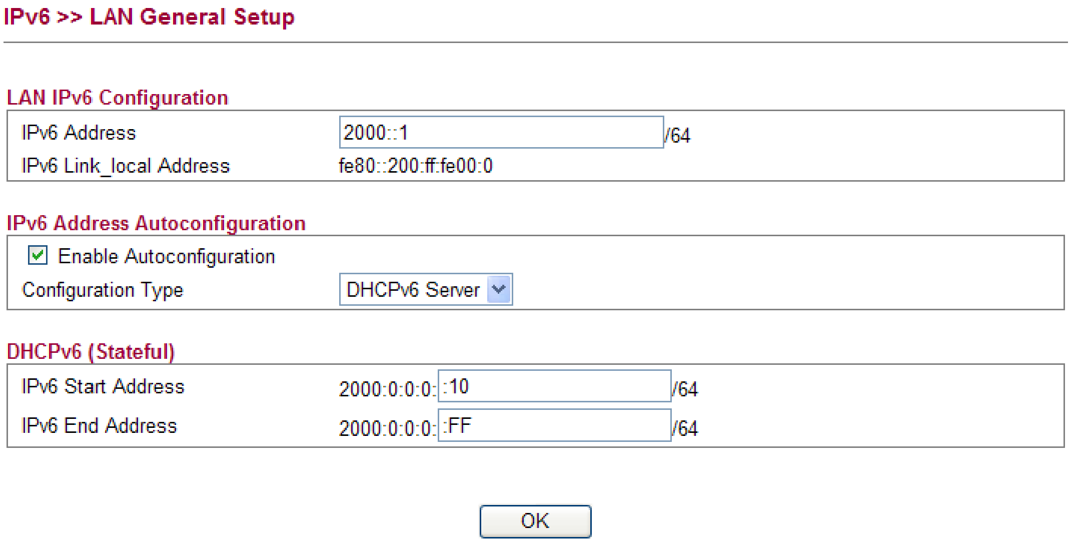
Keepalive_interval Type the time for the interval between two keepalive messages transferring from the client to the broker.

Prefixlen Type the required prefix length for the client network.

If_prefix Display LAN interface name. The name of the OS interface that will be configured with the first 64 of the received prefix from the broker and the router advertisement daemon is started to advertise that prefix on the if_prefix interface.

3.8.2 IPv6 LAN Setup

This page defines the IPv6 connection types for LAN interface. Possible types contain DHCPv6 and RADVD. Each type requires different parameter settings.



IPv6 >> LAN General Setup

LAN IPv6 Configuration

IPv6 Address	2000::1 /64
IPv6 Link_local Address	fe80::200:ff:fe00:0

IPv6 Address Autoconfiguration

☑ Enable Autoconfiguration

Configuration Type: DHCPv6 Server

DHCPv6 (Stateful)

IPv6 Start Address	2000:0:0:0: :10 /64
IPv6 End Address	2000:0:0:0: :FF /64

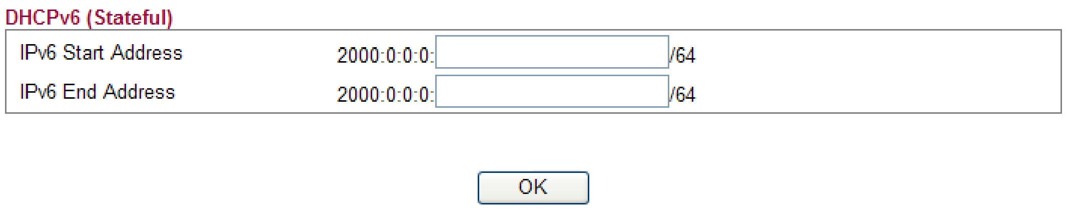
IPv6 Address Type static IPv6 address for LAN.

IPv6 Link_local Address It is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix fe80::/10. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.

Enable Autoconfiguration Check this box to enable the auto-configuration function for IPv6 connection.

Configuration Type Vigor2130 provides 2 daemons for LAN side IPv6 address configuration. One is **RADVD**(stateless) and the other is **DHCPv6 Server** (Stateful).

DHCPv6 Server - DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.

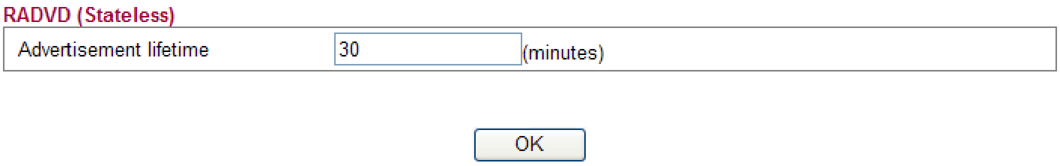


DHCPv6 (Stateful)

IPv6 Start Address	2000:0:0:0: /64
IPv6 End Address	2000:0:0:0: /64

IPv6 Start Address/IPv6 End Address- Type the start and end address for IPv6 server.

RADVD - The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless autoconfiguration.



RADVD (Stateless)

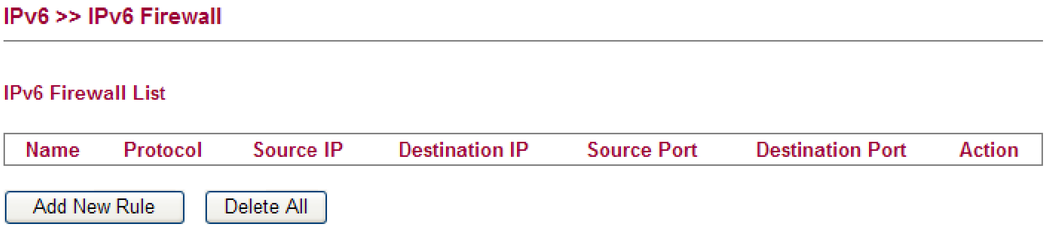
Advertisement lifetime: 30 (minutes)

Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.

3.8.3 IPv6 Firewall Setup

This page allows users to set firewall for the protocol of IPv6.

Note: Section 4.4 **Firewall** is configured for IPv4 packets only.



IPv6 >> IPv6 Firewall

IPv6 Firewall List

Name	Protocol	Source IP	Destination IP	Source Port	Destination Port	Action

Name Display the name of the rule.

Protocol Display the protocol (TCP/UDP/ICMPv6) the rule uses.

Source IP Display the source IP address of such rule.

Destination IP Display the destination IP address of such rule.

Source Port Display the source port number of such rule.

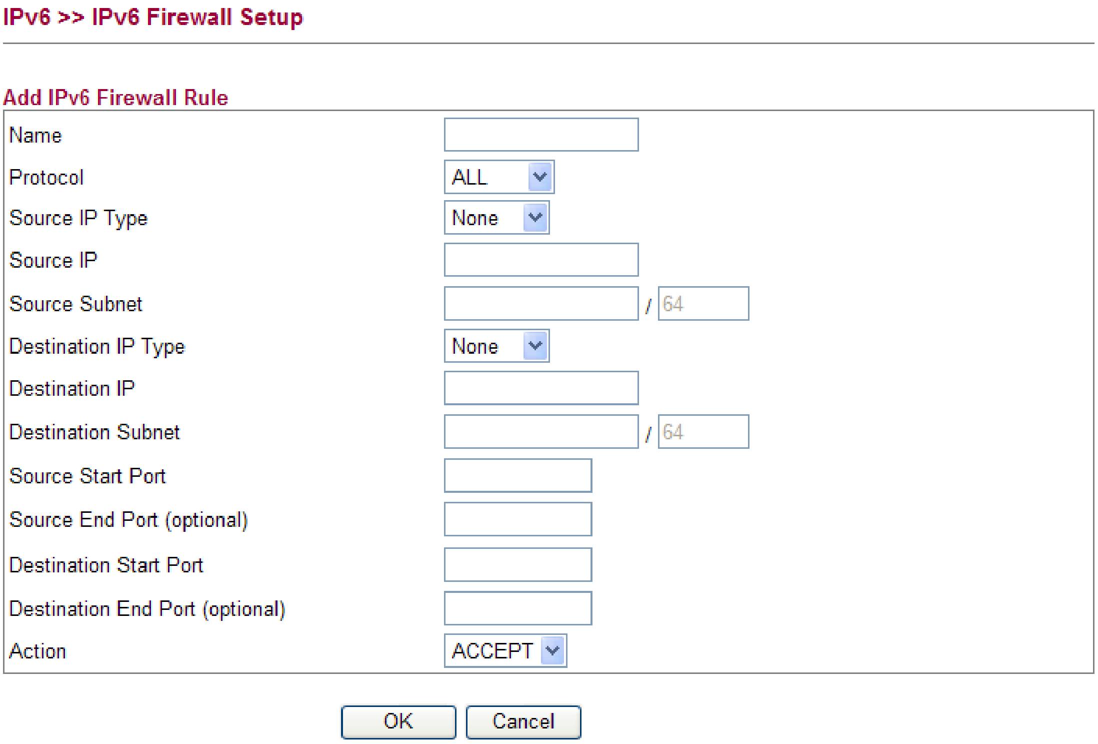
Destination Port Display the destination port number of such rule.

Action Display the status (accept or drop) of such rule.

Adding a New Rule

Click **Add New Rule** to configure a new rule for IPv6 Firewall.

> **Note:** You can set up to 20 sets of IPv6 rules.



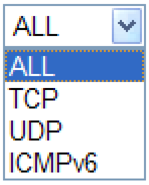
IPv6 >> IPv6 Firewall Setup

Add IPv6 Firewall Rule

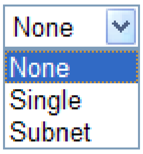
Name	
Protocol	ALL
Source IP Type	None
Source IP	
Source Subnet	/ 64
Destination IP Type	None
Destination IP	
Destination Subnet	/ 64
Source Start Port	
Source End Port (optional)	
Destination Start Port	
Destination End Port (optional)	
Action	ACCEPT

Name Type a name for the rule.

Protocol Specify a protocol for this rule.



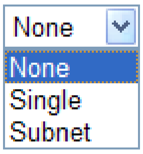
Source IP Type Determine the IP type as the source.



Source IP Type the IP address here if you choose **Single** as **Source IP Type**.

Source Subnet Type the subnet mask here if you choose **Subnet** as **Source IP Type**.

Destination IP Type Determine the IP type as the destination.



Destination IP Type the IP address here if you choose **Single** as **Destination IP Type**.

Destination Subnet Type the subnet mask here if you choose **Subnet** as **Destination IP Type**.

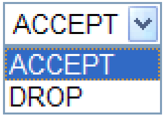
Source Start Port Type a value as the source start port. Such value will be available only TCP/UDP is selected as the protocol.

Source End Port (optional) Type a value as the source end port. Such value will be available only TCP/UDP is selected as the protocol.

Destination Start Port Type a value as the destination start port. Such value will be available only TCP/UDP is selected as the protocol.

Destination End Port (optional) Type a value as the destination end port. Such value will be available only TCP/UDP is selected as the protocol.

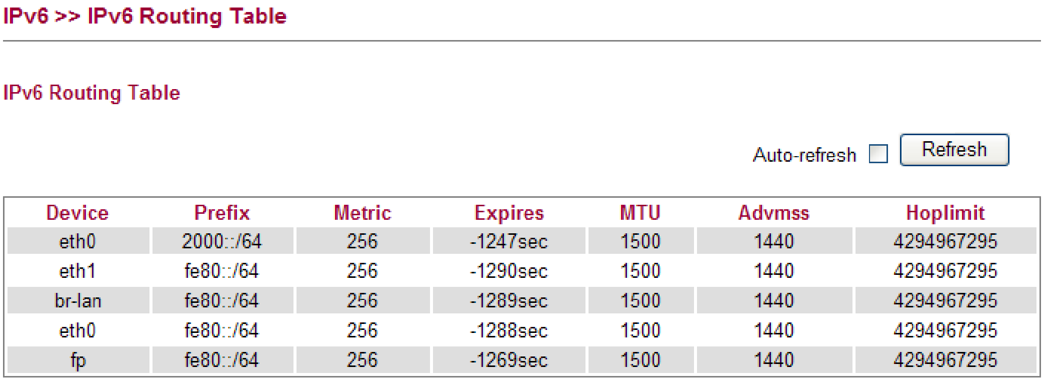
Action Set the action that the router will perform for the packets through the protocol of IPv6.



Accept – If the IPv6 packets fit the condition listed in this page, the router will let it pass through.
Drop - If the IPv6 packets fit the condition listed in this page, the router will block it.

3.8.4 IPv6 Routing

This page displays the routing table for the protocol of IPv6.



IPv6 >> IPv6 Routing Table

IPv6 Routing Table

Auto-refresh □ Refresh

Device	Prefix	Metric	Expires	MTU	Advmss	Hoplimit
eth0	2000::/64	256	-1247sec	1500	1440	4294967295
eth1	fe80::/64	256	-1290sec	1500	1440	4294967295
br-lan	fe80::/64	256	-1289sec	1500	1440	4294967295
eth0	fe80::/64	256	-1288sec	1500	1440	4294967295
fp	fe80::/64	256	-1269sec	1500	1440	4294967295

Device Display the interface name (eth0, eth1, fp, etc..)that used to transfer packets with addresses matching the prefix.

Prefix The IPv6 address prefix.

Metric Display the distance to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

Expires Display the lifetime of the route.

MTU Display the largest size (in bytes) of a packet.

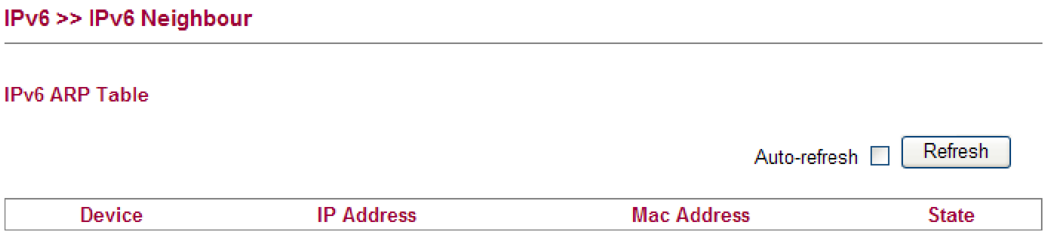
Advmss Display the largest size (in bytes) of an unfragmented piece of a routing advertisement.

Hoplimit Display the number of network segments on which the packet is allowed to travel before discarded.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.

3.8.5 IPv6 Neighbour

IPv6 uses neighbor discovery protocol to find out neighbors on the same link.



IPv6 >> IPv6 Neighbour

IPv6 ARP Table

Auto-refresh □ Refresh

Device	IP Address	Mac Address	State

Device The interface name of the link where the neighbor is on.

IP Address The IPv6 address of the neighbor.

MAC Address The link-layer address of the neighbor.

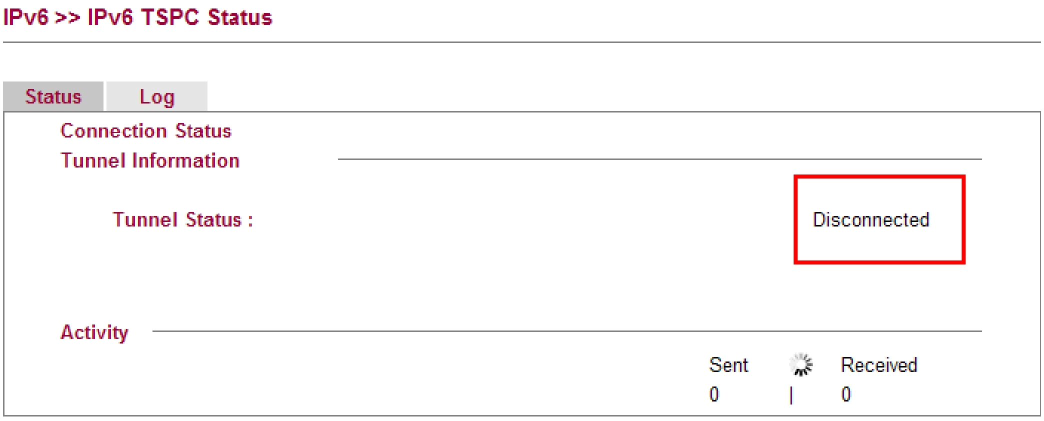
State Possible states include:
incomplete - address resolution is in progress.
reachable - neighbor is reachable.
stale – neighbor(s) may be unreachable but not verified until a packet is sent).
delay - neighbor may be unreachable and a packet was sent.
probe - neighbor may be unreachable and probes are sent to verify the reachability.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.

3.8.6 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC. TSPC log contains some debug information from program.

If TSPC has not configured properly, the router will display the following page when the user tries to connect through TSPC connection.



IPv6 >> IPv6 TSPC Status

Status | Log

Connection Status

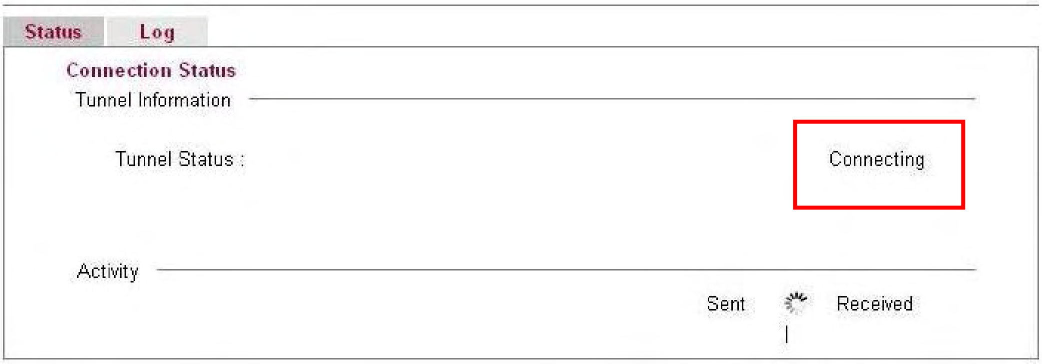
Tunnel Information

Tunnel Status : Disconnected

Activity

Sent 0 | Received 0

When TSPC configuration has been done, the router will start to connect. The connecting page will be shown as below:



Connection Status

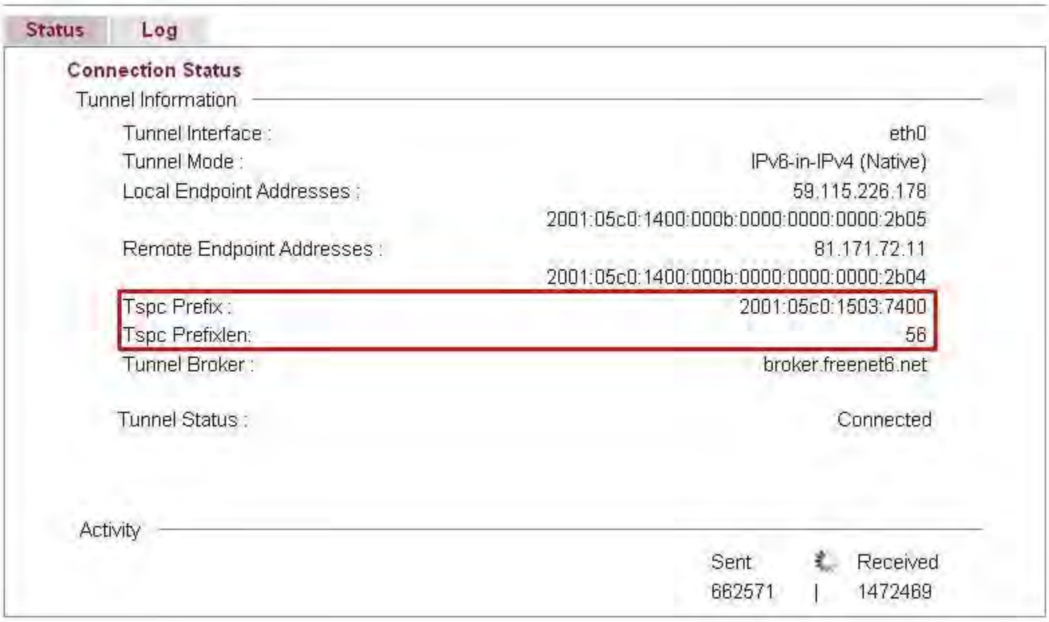
Tunnel Information

Tunnel Status : Connecting

Activity

Sent | Received

When the router detects all the information, the screen will be shown as follows. One set of **TSPC prefix** and **prefix length** will be obtained after the connection between TSPC and Tunnel broker built.



Connection Status

Tunnel Information

Tunnel Interface : eth0
Tunnel Mode : IPv6-in-IPv4 (Native)
Local Endpoint Addresses : 59.115.226.178
2001:05c0:1400:000b:0000:0000:0000:2b05
Remote Endpoint Addresses : 81.171.72.11
2001:05c0:1400:000b:0000:0000:0000:2b04
Tspc Prefix : 2001:05c0:1503:7400
Tspc Prefixlen: 56
Tunnel Broker : broker.freenet6.net

Tunnel Status : Connected

Activity

Sent | Received
662571 | 1472469

Connection Status

It will bring out different pages to represent IPv6 disconnection, connecting and connected.

Tunnel Information

Display interface name (used to send TSPC prefix), tunnel mode, local endpoint addresses, remote endpoint address, TSPC Prfix, TSPC Prefixlen (prefix length), tunnel broker and so on.

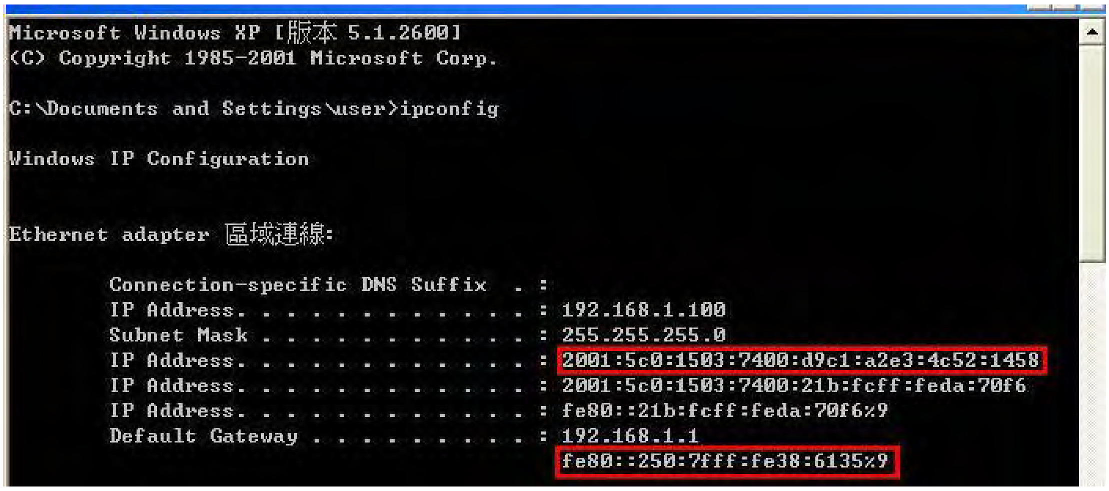
Tunnel Status

Disconnected - The remote client doesn't connect to the tunnel server.
Connecting - The remote client is connecting to the tunnel server.
Connected – The remote client has been connected to the tunnel server.

Activity

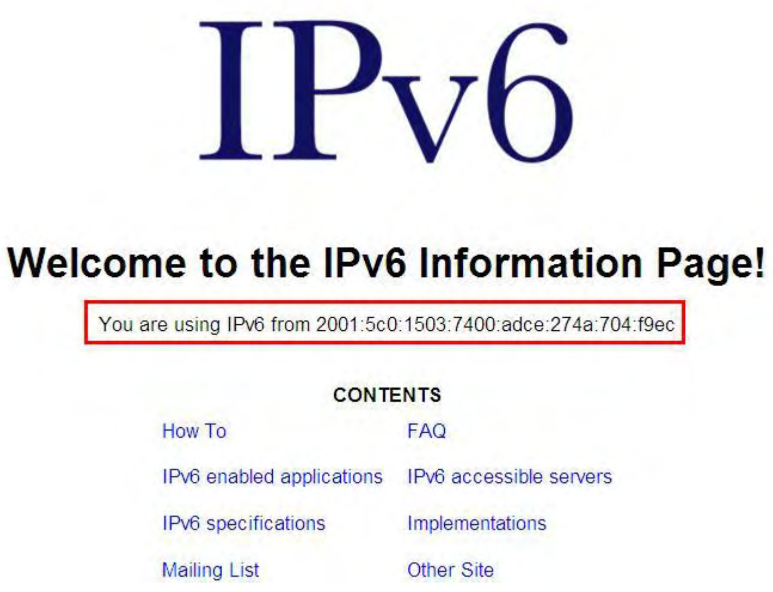
Sent - sent to the tunnel (RX bytes).
Received - received from the tunnel (RX bytes).

When the router connects to the tunnel broker, the router will use RADVD to transmit the prefix to the PC on LAN. Next, the PC will generate one set of IPv6 public IP (see the figure below). Users can use such IP for connecting to IPv6 network.



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

C:\Documents and Settings\user>ipconfig

Windows IP Configuration


Ethernet adapter 區域連線:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:5c0:1503:7400:d9c1:a2e3:4c52:1458
        IP Address. . . . . . . . . . . . : 2001:5c0:1503:7400:21b:fcff:feda:70f6
        IP Address. . . . . . . . . . . . : fe80::21b:fcff:feda:70f6%9
        Default Gateway . . . . . . . . . : 192.168.1.1
                                            fe80::250:7fff:fe38:6135%9
```

When your PC obtains the IPv6 address, please connect to http://www.ipv6.org. If your PC access Internet via IPv6 connection, your IPv6 address will be shown on the web page immediately. Refer to the following figure.



IPv6

Welcome to the IPv6 Information Page!

You are using IPv6 from 2001:5c0:1503:7400:adce:274a:704:f9ec

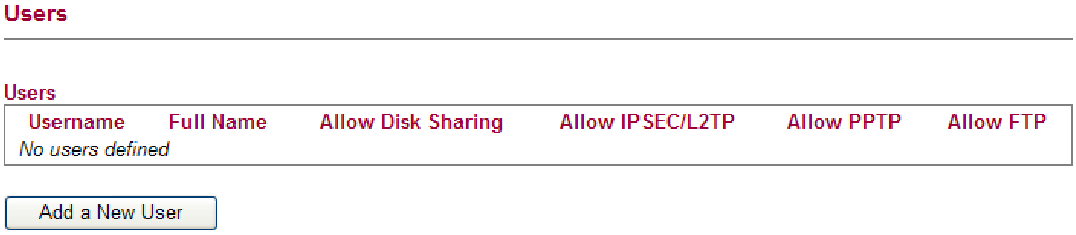
CONTENTS

How To	FAQ
IPv6 enabled applications	IPv6 accessible servers
IPv6 specifications	Implementations
Mailing List	Other Site

3.9 User

3.9.1 User Configuration

This page allows you to set user's setting that allowed to use PPTP, FTP, IPSEC/L2TP connection.



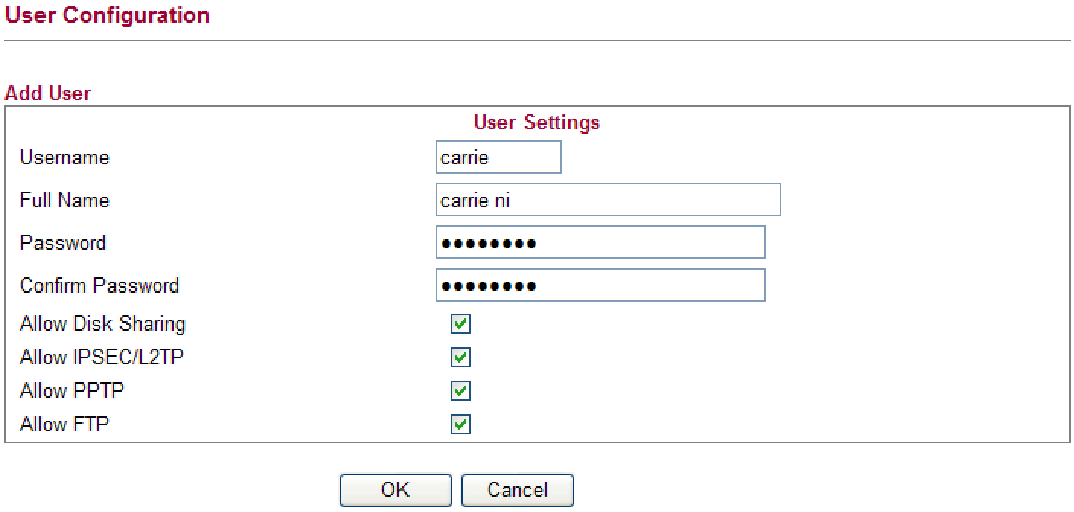
Users

Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
No users defined					

Adding a New User

Click **Add a New User** to open the following page.



User Configuration

Add User

User Settings	
Username	carrie
Full Name	carrie ni
Password	••••••••
Confirm Password	••••••••
Allow Disk Sharing	☑
Allow IPSEC/L2TP	☑
Allow PPTP	☑
Allow FTP	☑

Username Type a name for this user.

Full Name Type full name for this user.

Password Type the password for this user.

Password (again) Type the password again for confirmation.

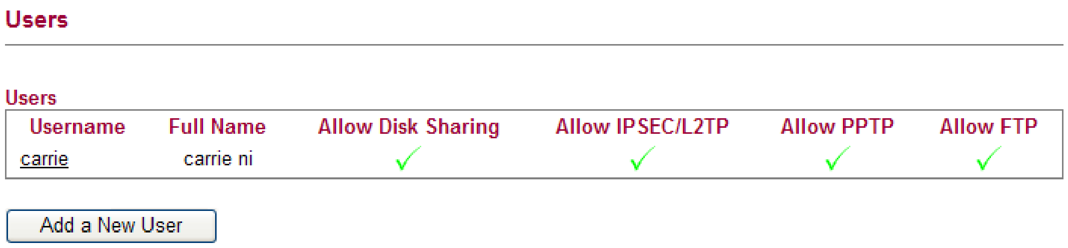
Allow Disk Sharing Check this box to enable Samba file sharing.

Allow IPSEC/L2TP Check this box to let the user connect via IPSEC/L2TP.

Allow PPTP Check this box to let the user connect via PPTP.

Allow FTP Check this box to let the user connect to FTP server.

When you finish the settings, simply click **OK** to save the configuration. The new user will be created and displayed on the page.



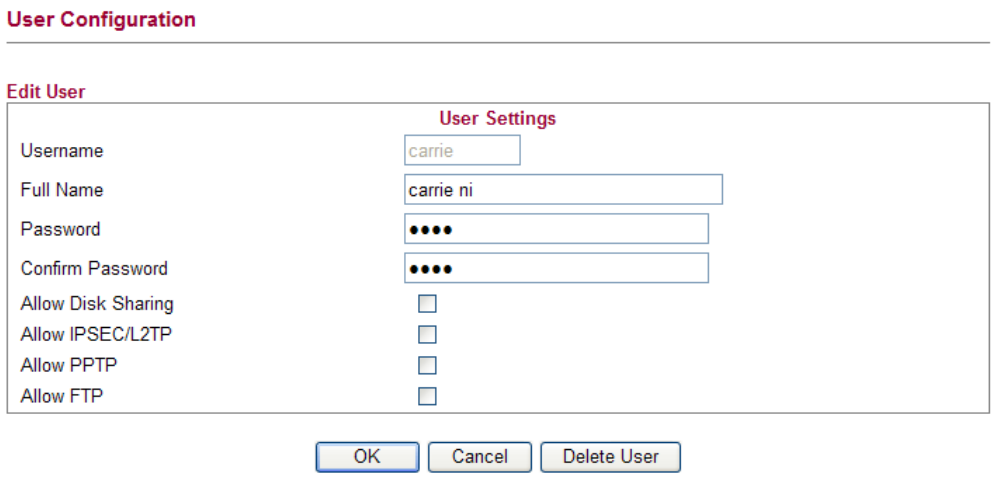
Users

Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
carrie	carrie ni	✓	✓	✓	✓

Editing/Deleting User Settings

To edit a user, click the name link under Username to open the following page. Modify the settings except Username and then click **OK** to save and exit it. If you want to remove such user settings, simply click **Delete User**.



User Configuration

Edit User

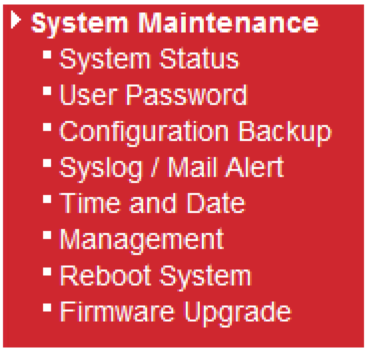
User Settings

Username	carrie
Full Name	carrie ni
Password	••••
Confirm Password	••••
Allow Disk Sharing	□
Allow IPSEC/L2TP	□
Allow PPTP	□
Allow FTP	□

3.10 System Maintenance

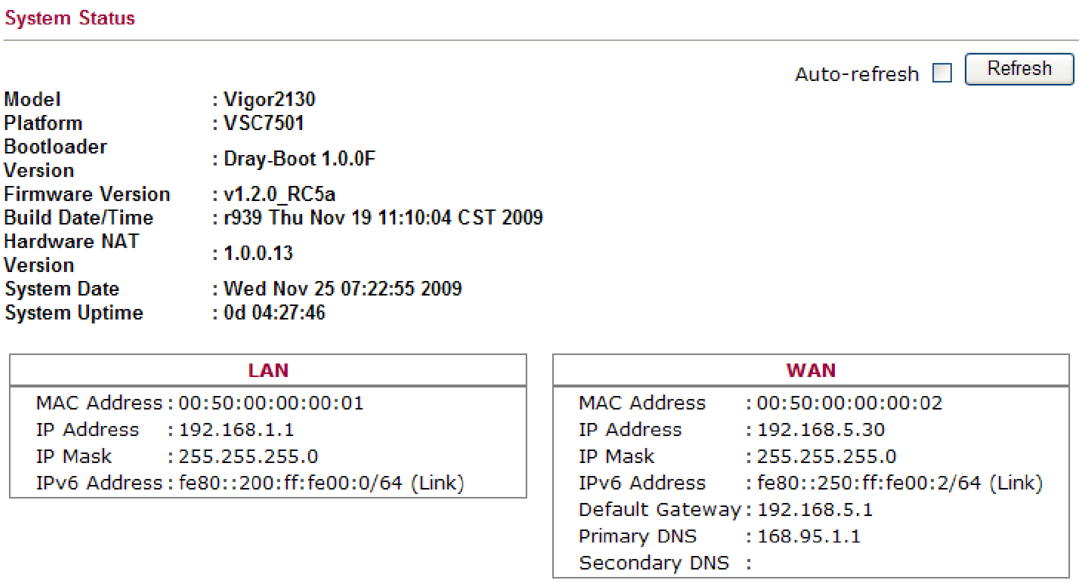
For the system setup, there are several items that you have to know the way of configuration: Status, User Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Management, Reboot System and Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.10.1 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

Auto-refresh □ Refresh

Model : Vigor2130
Platform : VSC7501
Bootloader Version : Dray-Boot 1.0.0F
Firmware Version : v1.2.0_RC5a
Build Date/Time : r939 Thu Nov 19 11:10:04 CST 2009
Hardware NAT Version : 1.0.0.13
System Date : Wed Nov 25 07:22:55 2009
System Uptime : 0d 04:27:46

LAN

MAC Address : 00:50:00:00:00:01
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::200:ff:fe00:0/64 (Link)

WAN

MAC Address : 00:50:00:00:00:02
IP Address : 192.168.5.30
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:ff:fe00:2/64 (Link)
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

Model Name Display the model name of the router.

Platform Display the hardware type that this device is built upon.

Bootloader Version Display the bootloader version of the router.

Firmware Version Display the firmware version of the router.

Build Date/Time Display the date and time of the current firmware build.

Hardware NAT Version Display the hardware acceleration NAT version.

System Date Display current time and date for the system server.

System Uptime Display the connection time for the system server.

LAN-------

MAC Address Display the MAC address of the LAN Interface.

IP Address Display the IP address of the LAN interface.

IP Mask Display the subnet mask address of the LAN interface.

WAN-------

MAC Address Display the MAC address of the WAN Interface.

IP Address Display the IP address of the WAN interface.

IP Mask Display the subnet mask address of the WAN interface.

IPv6 Address Display the IPv6 address of the WAN interface.

Default Gateway Display the gateway address of the WAN interface.

Primary DNS Display the specified primary DNS setting.

Secondary DNS Display the specified secondary DNS setting.

Wireless LAN-------

MAC Address Display the MAC address of the wireless LAN.

Device Type Display the device type used for wireless LAN.

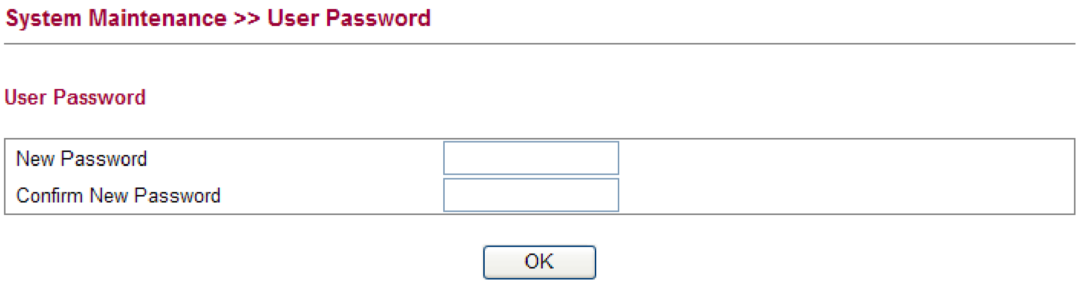
SSID Display the SSID of the router.

Channel Display the channel that wireless LAN used.

Manufacturer	Display the manufacturer of the disk.
Model	Display the model of the disk.
Size	Display the storage size of the USB diskette.
Status	Display current status of the USB diskette.

3.10.2 User Password

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



System Maintenance >> User Password

User Password

New Password
Confirm New Password

Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

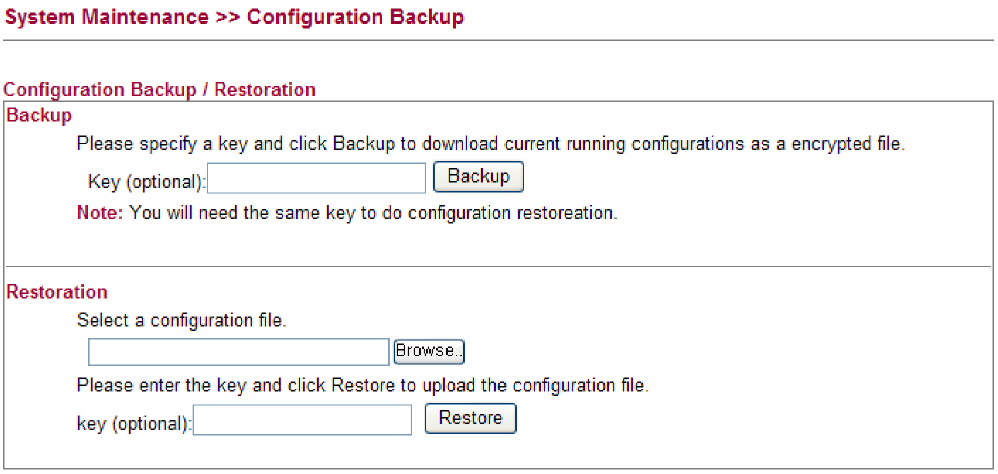
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.10.3 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

Backup

Please specify a key and click Backup to download current running configurations as a encrypted file.

Key (optional):

Note: You will need the same key to do configuration restoreation.

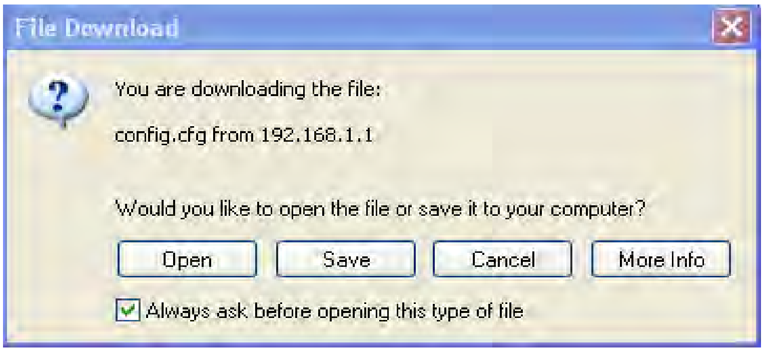
Restoration

Select a configuration file.

Please enter the key and click Restore to upload the configuration file.

key (optional):

2. Type a key arbitrarily for encrypting the file. Keep the key in mind. You will need it whenever you want to restore such file. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



File Download

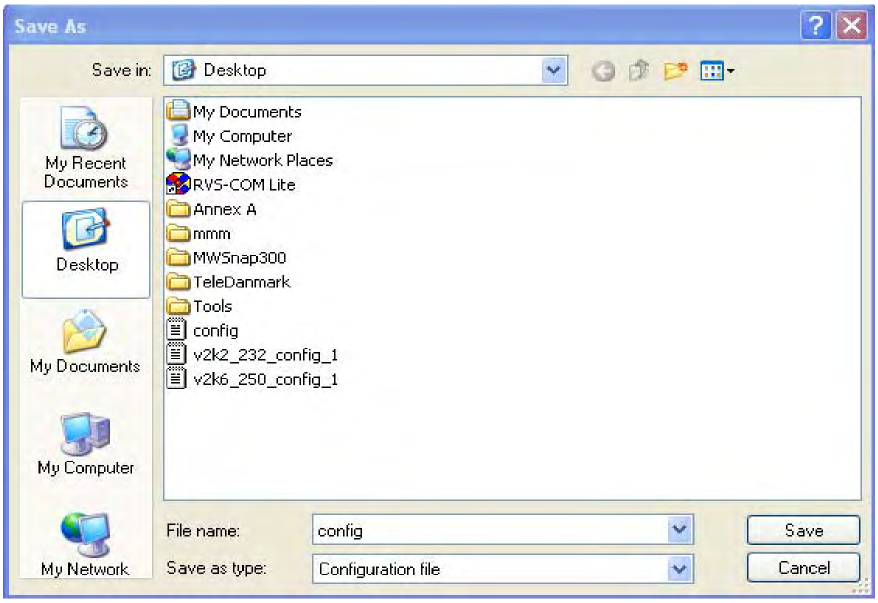
You are downloading the file:

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

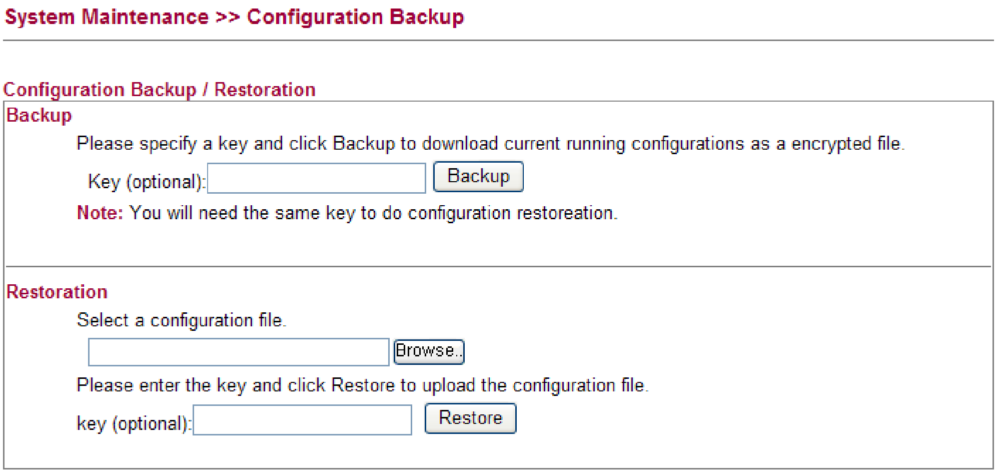
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

Backup

Please specify a key and click Backup to download current running configurations as a encrypted file.

Key (optional): [ ] Backup

Note: You will need the same key to do configuration restoreation.

Restoration

Select a configuration file.

[ ] Browse..

Please enter the key and click Restore to upload the configuration file.

key (optional): [ ] Restore

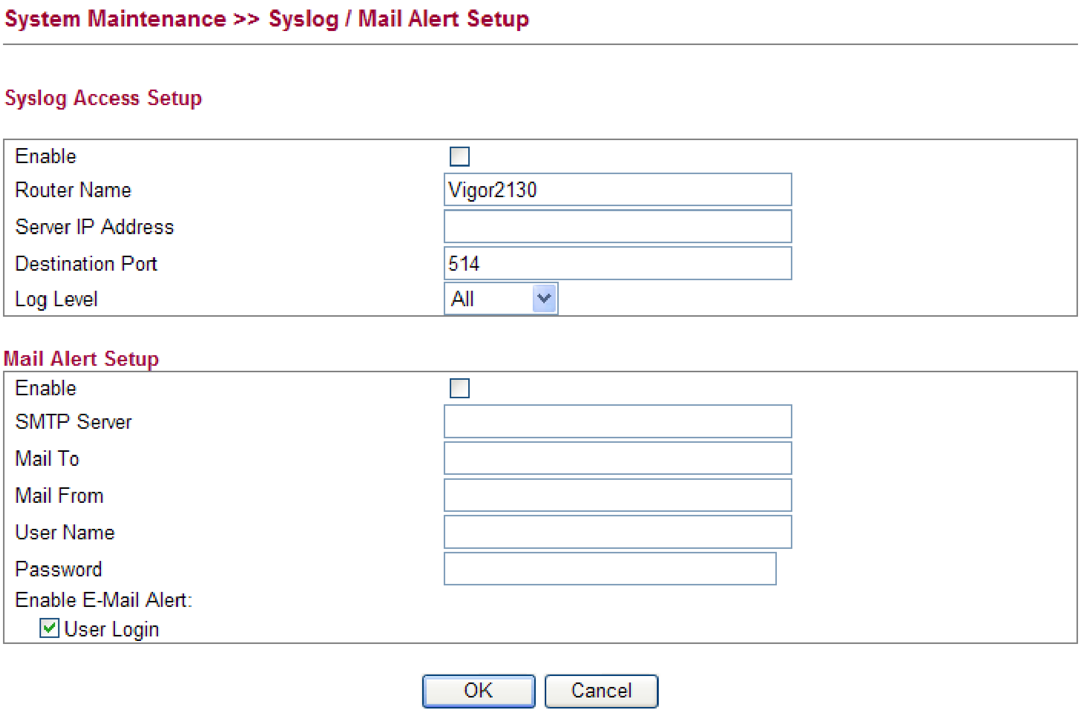
2. Click **Browse** button to choose the correct configuration file for uploading to the router.

Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

> **Note:** If the file you want to restore has been encrypted, you will be asked to type the encrypted key before clicking **Restore**.

3.10.4 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 Access Setup

Enable	□
Router Name	Vigor2130
Server IP Address	
Destination Port	514
Log Level	All

Mail Alert Setup

Enable	□
SMTP Server	
Mail To	
Mail From	
User Name	
Password	
Enable E-Mail Alert:	
☑ User Login	

OK Cancel

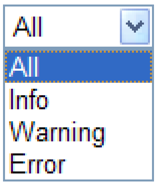
Enable (Syslog Access…) Check the box to activate function of syslog.

Router Name Type a name of this device.

Server IP Address The IP address of the Syslog server.

Destination Port Type a port for the Syslog protocol.

Log Level Choose the severity level for the system log entry.



Enable (Mail Alert…) Check the box 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.

Mail From Assign a path for receiving the mail from outside.

User Name Type the user name for authentication.

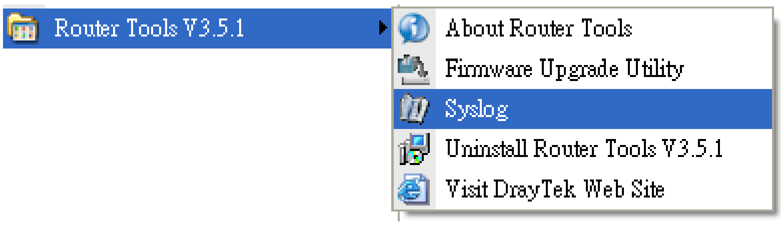
Password Type the password for authentication.

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

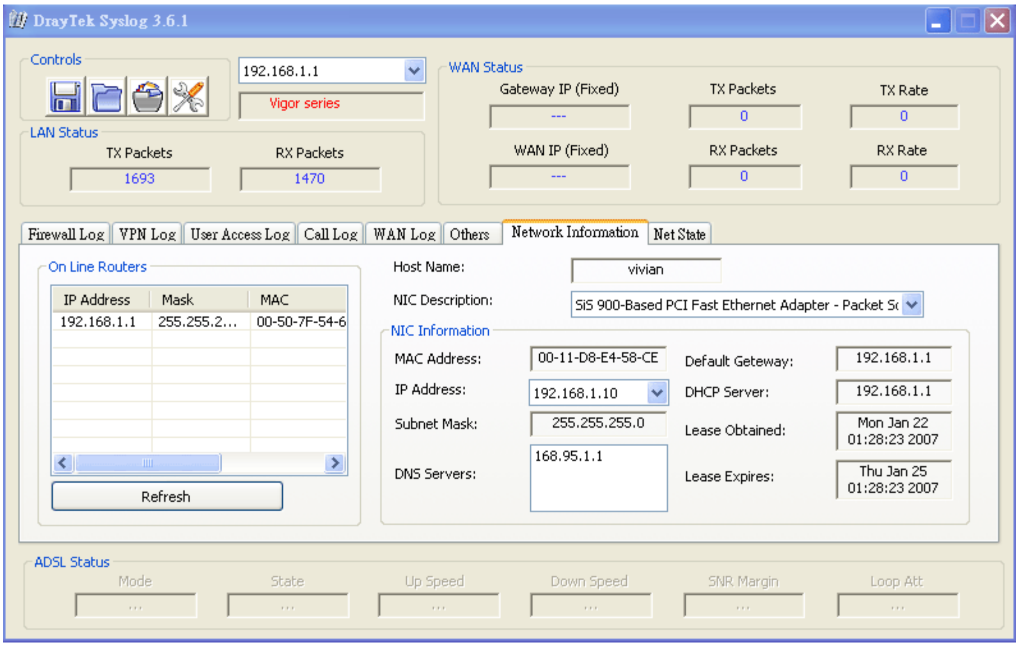
Click **OK** to save these settings.

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.



DrayTek Syslog 3.6.1

Controls

192.168.1.1

Vigor series

LAN Status

TX Packets	RX Packets
1693	1470

WAN Status

Gateway IP (Fixed)	TX Packets	TX Rate
---	0	0
WAN IP (Fixed)	**RX Packets**	**RX Rate**
---	0	0

On Line Routers

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

NIC Information

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

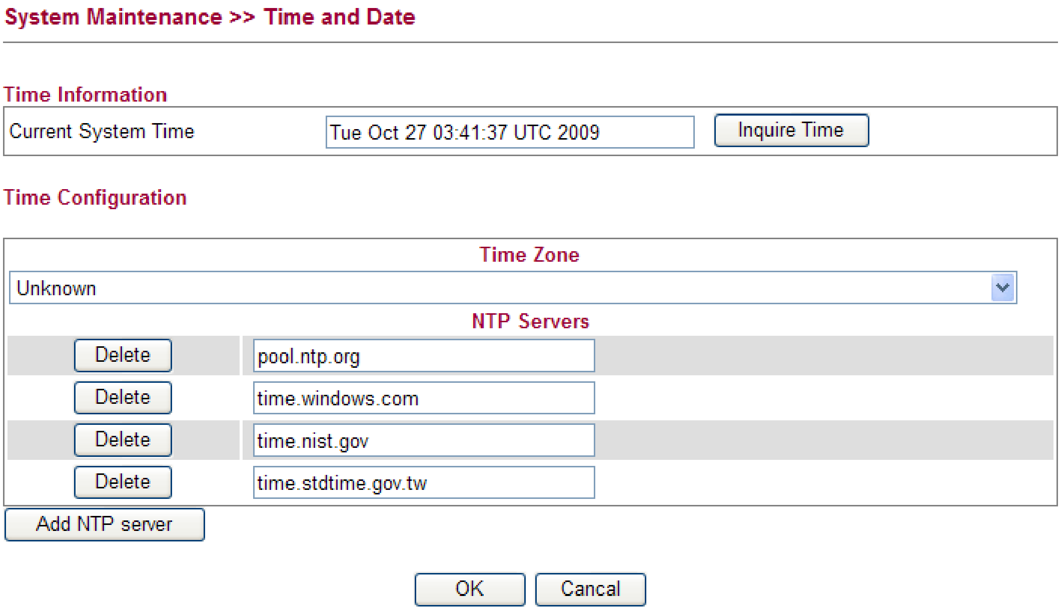
Lease Expires: Thu Jan 25 01:28:23 2007

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
...	...	...	...	...	...

3.10.5 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: Tue Oct 27 03:41:37 UTC 2009

Time Configuration

Time Zone: Unknown

NTP Servers

Delete	pool.ntp.org
Delete	time.windows.com
Delete	time.nist.gov
Delete	time.stdtime.gov.tw

Current System Time Click **Inquire Time** to get the current time.

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

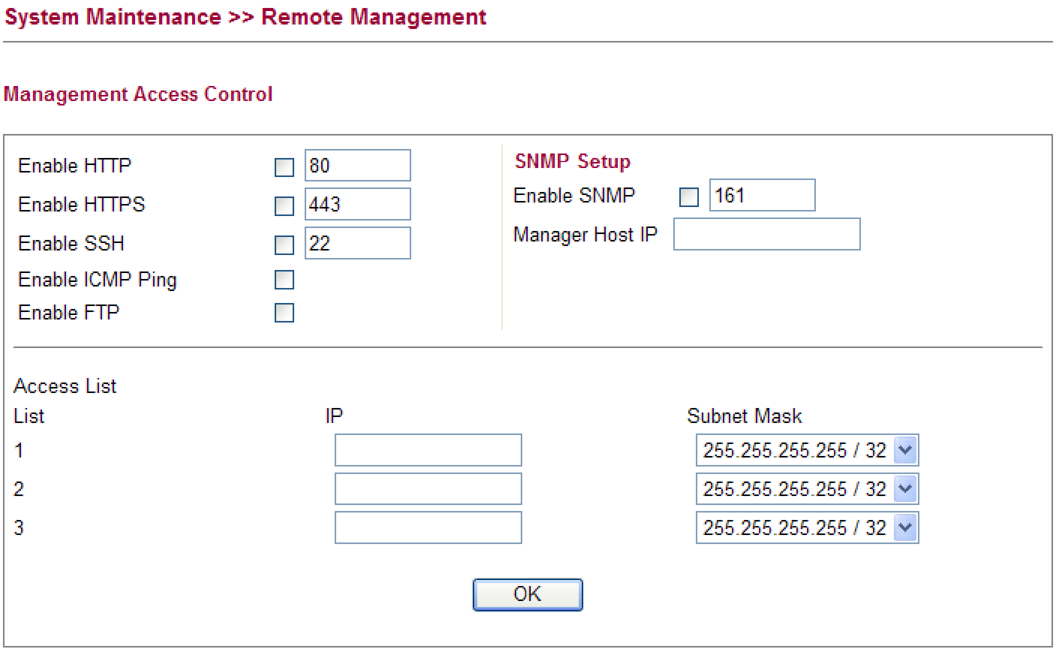
Add NTP server Click the button to add a new NTP server.

Delete Click this button to remove an NTP server.

Click **OK** to save these settings.

3.10.6 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. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.



System Maintenance >> Remote Management

Management Access Control

Enable HTTP	□	80
Enable HTTPS	□	443
Enable SSH	□	22
Enable ICMP Ping	□	
Enable FTP	□	

SNMP Setup

Enable SNMP	□	161
Manager Host IP		

Access List

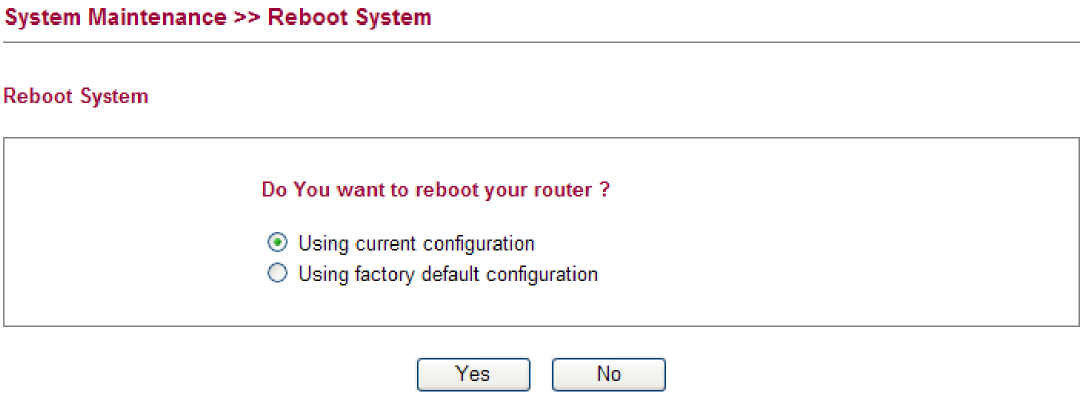
List	IP	Subnet Mask
1		255.255.255.255 / 32
2		255.255.255.255 / 32
3		255.255.255.255 / 32

Enable HTTP/HTTPS/SSH/ICMP Ping/FTP/SNMP 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.
Manager Host IP – Type the IP address for the host to perform the remote management.

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.

3.10.7 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

○ Using factory default configuration

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

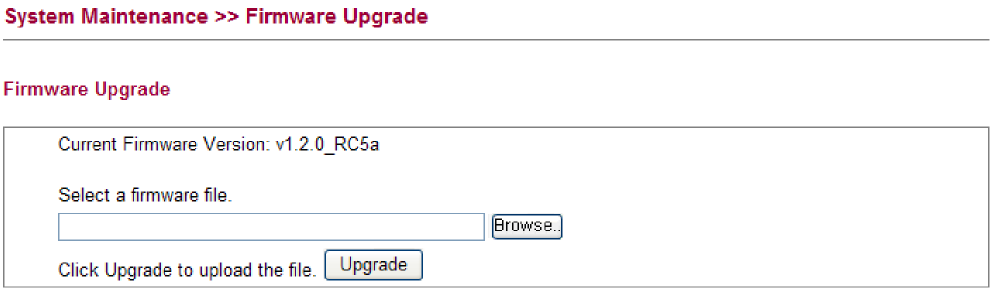
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

3.10.8 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 **Maintenance**>> **Firmware Upgrade** to launch the Firmware Upgrade Utility.



System Maintenance >> Firmware Upgrade

Firmware Upgrade

Current Firmware Version: v1.2.0_RC5a

Select a firmware file.

Click Upgrade to upload the file.

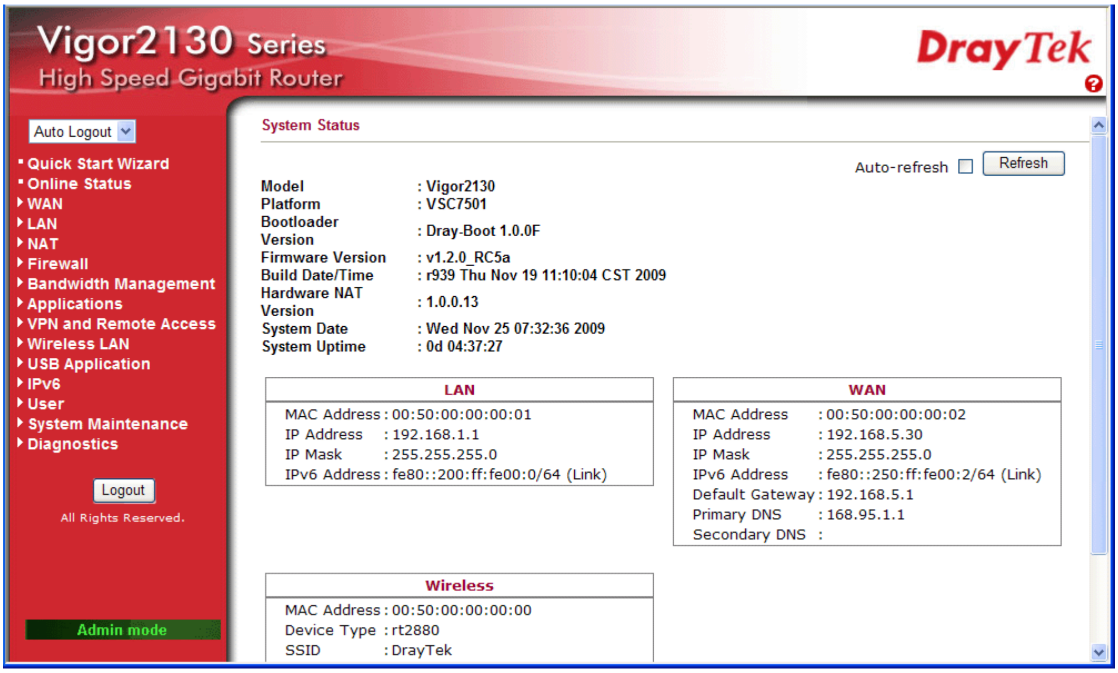
Click **Browse..** to locate the newest firmware and click **Upgrade**. During the process of upgrade, do not turn off your router.

4 Admin Mode Operation

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

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

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



System Status

Model : Vigor2130
Platform : VSC7501
Bootloader Version : Dray-Boot 1.0.0F
Firmware Version : v1.2.0_RC5a
Build Date/Time : r939 Thu Nov 19 11:10:04 CST 2009
Hardware NAT Version : 1.0.0.13
System Date : Wed Nov 25 07:32:36 2009
System Uptime : 0d 04:37:27

LAN

MAC Address : 00:50:00:00:00:01
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::200:ff:fe00:0/64 (Link)

WAN

MAC Address : 00:50:00:00:00:02
IP Address : 192.168.5.30
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:ff:fe00:2/64 (Link)
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

Wireless

MAC Address : 00:50:00:00:00:00
Device Type : rt2880
SSID : DrayTek

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 **Internet Access** group.

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

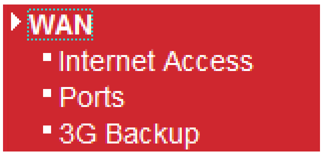
For 3G mobile communication through Access Point is popular more and more, Vigor router adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor router, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor router with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via SuperG wireless function of Vigor router, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor router.

Mobile Coffee shop
Internet
VoIP
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 second WAN port. However, the original Ethernet WAN 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 WAN is not available, the router will use 3.5G for supporting automatically. The supported 3G USB

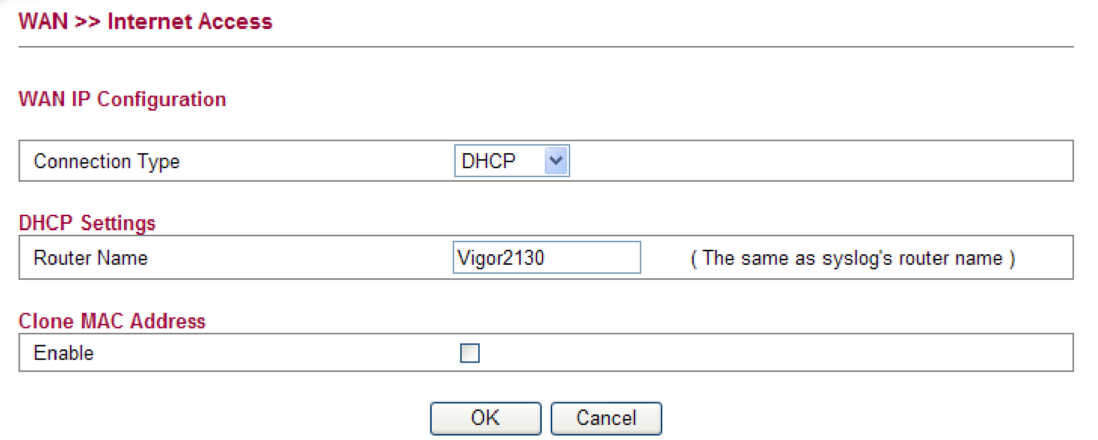
Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

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



4.1.1 Internet Access

This page allows you to set WAN configuration with different modes. Use the Connection Type drop down list to choose one of the WAN modes. The corresponding page will be displayed.



WAN >> Internet Access

WAN IP Configuration

Connection Type	DHCP

DHCP Settings

Router Name	Vigor2130	(The same as syslog's router name)

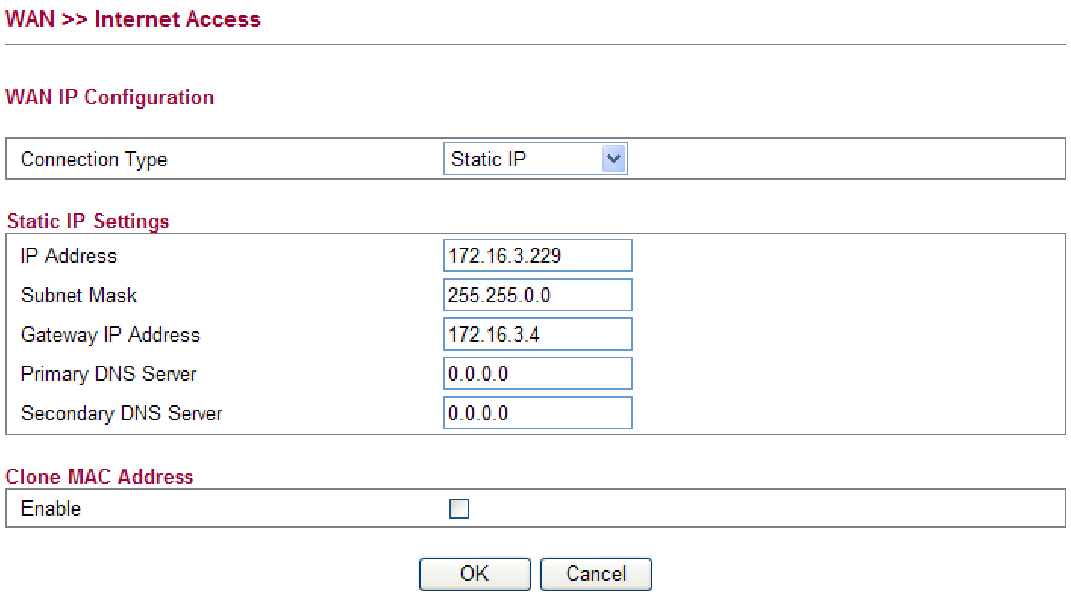
Clone MAC Address

Enable	□

Static

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** as the accessing protocol of the internet, please choose **Static** mode from **Connection Type** drop down menu. The following web page will be shown.



WAN >> Internet Access

WAN IP Configuration

Connection Type	Static IP

Static IP Settings

IP Address	172.16.3.229
Subnet Mask	255.255.0.0
Gateway IP Address	172.16.3.4
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Clone MAC Address

Enable	□

IP Address Type the IP address.

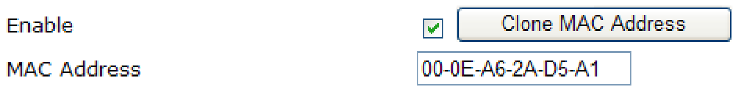
Subnet Mask Type the subnet mask.

Gateway IP Address Type the gateway IP address.

Primary DNS Server 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: 198.95.1.1 to this field.

Secondary DNS Server 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: 4.2.2.1 to this field.

Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

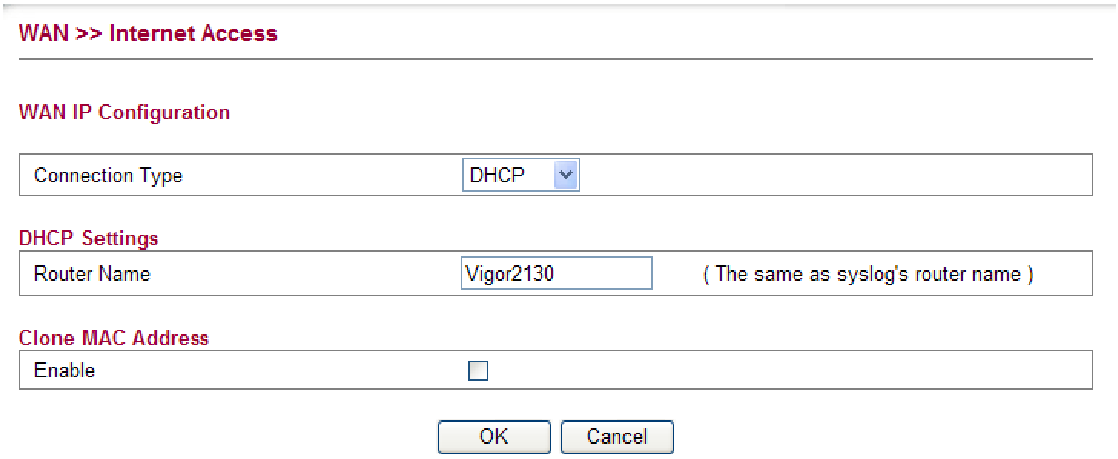


Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

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

DHCP

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for your router automatically. It is not necessary for you to assign any setting,



WAN >> Internet Access

WAN IP Configuration

Connection Type	DHCP

DHCP Settings

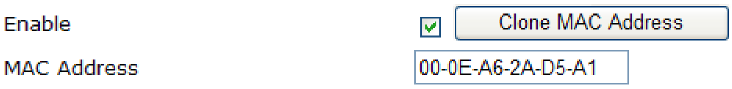
Router Name	Vigor2130	(The same as syslog's router name)

Clone MAC Address

Enable	□

Router Name Type in a name for the router. It must be the same as the name used in Syslog.

Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

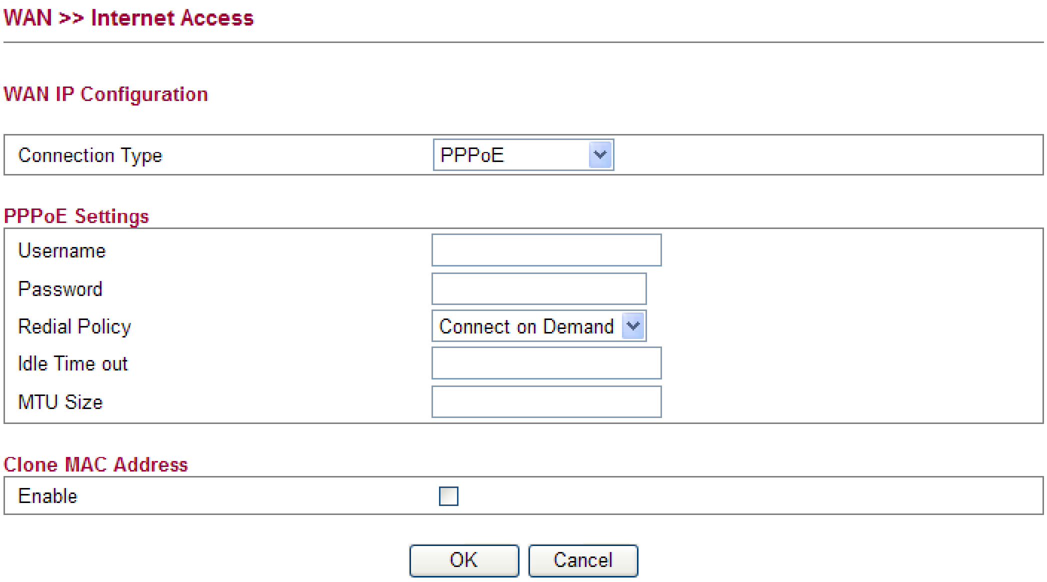


Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

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

PPPoE

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 IP Configuration

Connection Type	PPPoE

PPPoE Settings

Username	
Password	
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	

Clone MAC Address

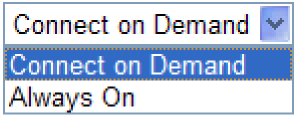
Enable	□

Username Type in the username provided by ISP in this field.

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

Redial Policy

If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.



Idle Time Out

Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.

MTU Size

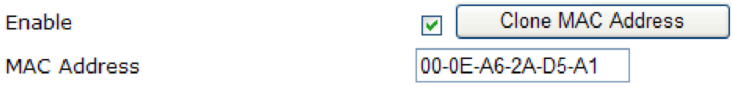
It means Max Transmit Unit for packet. The default setting is 1442.

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.

Clone MAC Address

It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.



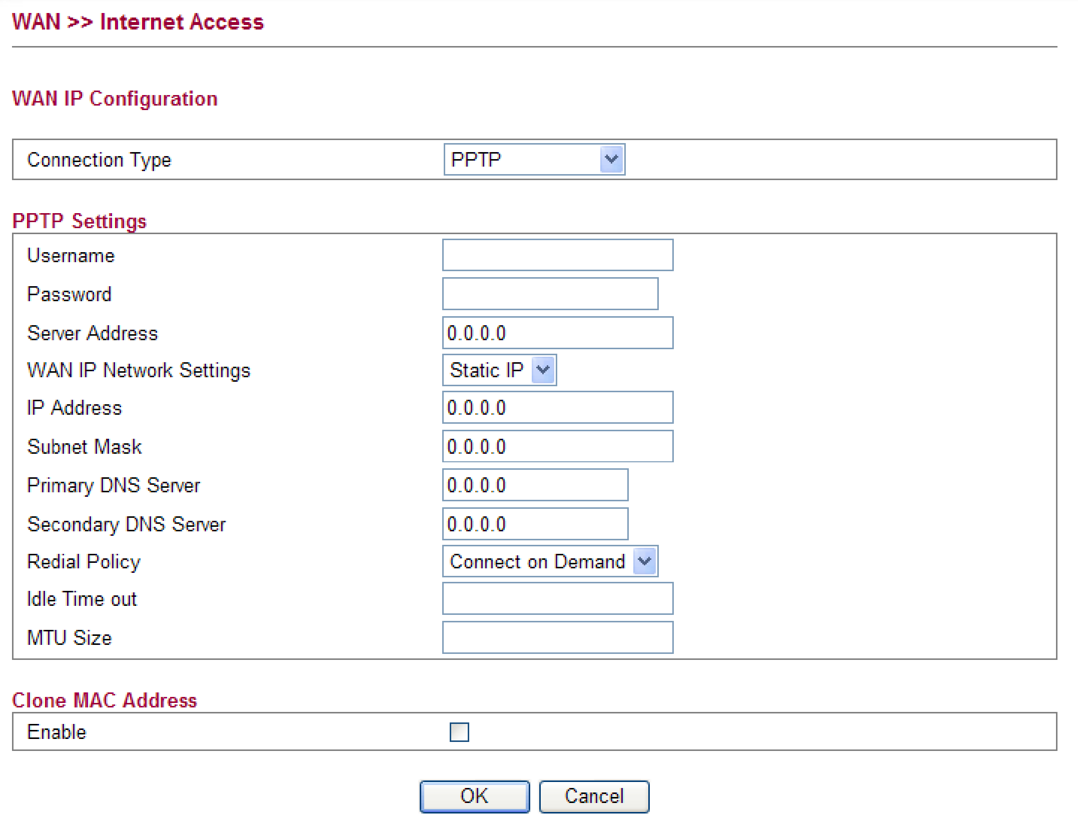
Enable ☑ Clone MAC Address

MAC Address 00-0E-A6-2A-D5-A1

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

PPTP/L2TP

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



WAN >> Internet Access

WAN IP Configuration

Connection Type	PPTP

PPTP Settings

Username	
Password	
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	

Clone MAC Address

Enable	□

Username Type in the username provided by ISP in this field.

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

Server Address Type in the IP address for PPTP /L2TP server.

WAN IP Network Settings You can choose Static IP or DHCP as WAN IP network setting.

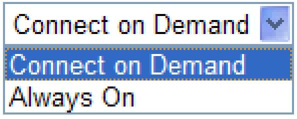
IP Address Type the IP address if you choose Static IP as the WAN IP network setting.

Subnet Mask Type the subnet mask if you chose Static IP as the WAN IP.

Primary DNS Server 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 DNS Server 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.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand** and



Idle Time Out Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.

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

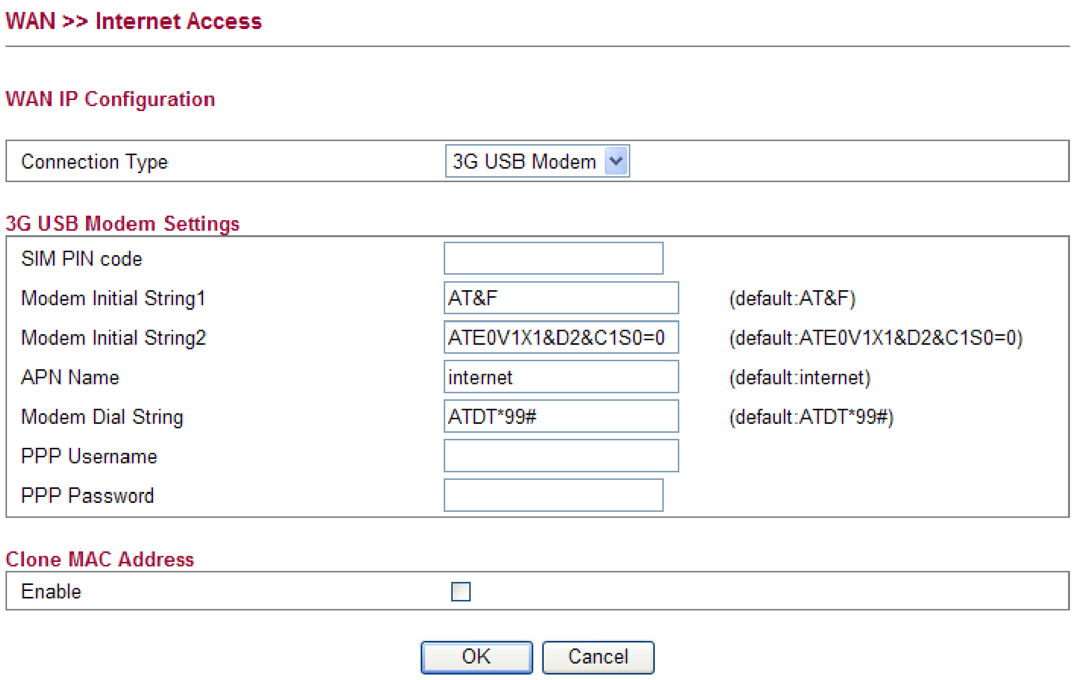
Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

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

3G USB Modem

If your router connects to a 3G modem and you want to access Internet via 3G modem, choose 3G as connection type and type the required information in this web page.



WAN >> Internet Access

WAN IP Configuration

Connection Type	3G USB Modem

3G USB Modem Settings

SIM PIN code		
Modem Initial String1	AT&F	(default:AT&F)
Modem Initial String2	ATE0V1X1&D2&C1S0=0	(default:ATE0V1X1&D2&C1S0=0)
APN Name	internet	(default:internet)
Modem Dial String	ATDT*99#	(default:ATDT*99#)
PPP Username		
PPP Password		

Clone MAC Address

Enable	□

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

Modem Initial String1/2 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.

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).

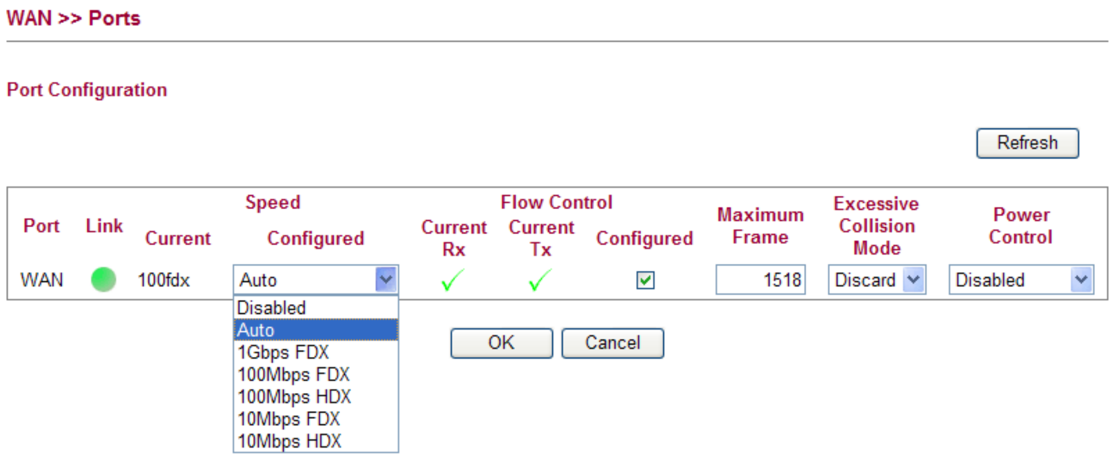
Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	☑ Clone MAC Address
MAC Address	00-0E-A6-2A-D5-A1

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

4.1.2 Ports

Ports page is used to change the setting for WAN port. You can set or reset the following items. All of them are described in detail below.



WAN >> Ports

Port Configuration

Refresh

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
WAN	●	100fdx	Auto	✓	✓	☑	1518	Discard	Disabled

Disabled
Auto
1Gbps FDX
100Mbps FDX
100Mbps HDX
10Mbps FDX
10Mbps HDX

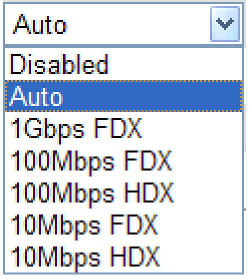
OK Cancel

Port It displays current network interface.

Link It displays current connection status. Green light means the WAN connection is successful.

Current It displays current speed that the router uses.

Speed Configured You can use the drop down list to choose the required speed for the router. If you have no idea in configuring speed, simple use the default setting, **Auto**.



Auto

Disabled
Auto
1Gbps FDX
100Mbps FDX
100Mbps HDX
10Mbps FDX
10Mbps HDX

Flow Control If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.
Current Rx: indicates whether pause frames on the port are obeyed.

Current Tx: indicates whether pause frames on the port are transmitted.

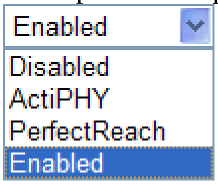
Maximum Frame This module offers 1518~9600 (Bytes) length to make the long packet for data transmission.

Excessive Collision Mode There are two modes for you to choose when excessive collision happened in half-duplex condition.

Discard - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

Restart - It determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Standard 802.3, but is useful in non-dropping half-duplex flow control operation.

Power Control The Configured column allows for changing the power savings mode parameters per port.



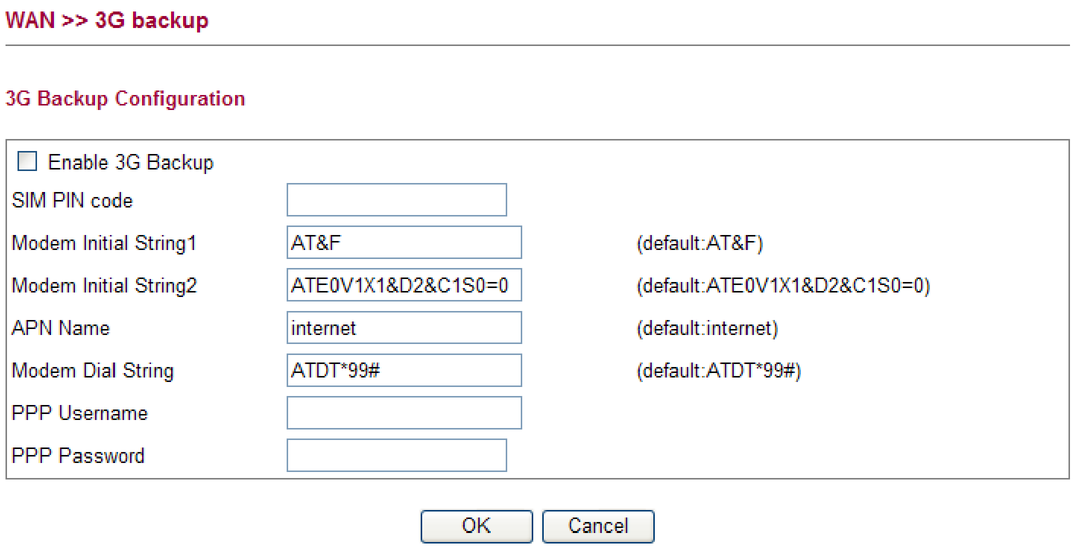
Disabled: All power savings mechanisms disabled.
ActiPHY: Link down power savings enabled.
PerfectReach: Link up power savings enabled.
Enabled: Both link up and link down power savings enabled.

Refresh Click this button to refresh the information for WAN port.

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

4.1.3 3G Backup

This page is used to setup 3G backup function. If you enable 3G backup, make sure your WAN connection type is not in 3G mode. When the WAN connection is broken, router will try to keep the connection with 3G mode. After WAN connection is recovered, router will disconnect the 3G connection automatically.


WAN >> 3G backup

3G Backup Configuration

☐ Enable 3G Backup

SIM PIN code		
Modem Initial String1	AT&F	(default:AT&F)
Modem Initial String2	ATE0V1X1&D2&C1S0=0	(default:ATE0V1X1&D2&C1S0=0)
APN Name	internet	(default:internet)
Modem Dial String	ATDT*99#	(default:ATDT*99#)
PPP Username		
PPP Password		

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

Modem Initial String1/2 Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

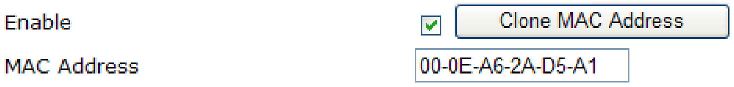
APN Name APN means Access Point Name which is provided and required by some ISPs.

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).

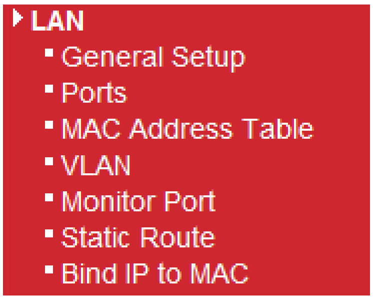
Clone MAC Address It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.


Enable ☑

MAC Address 00-0E-A6-2A-D5-A1

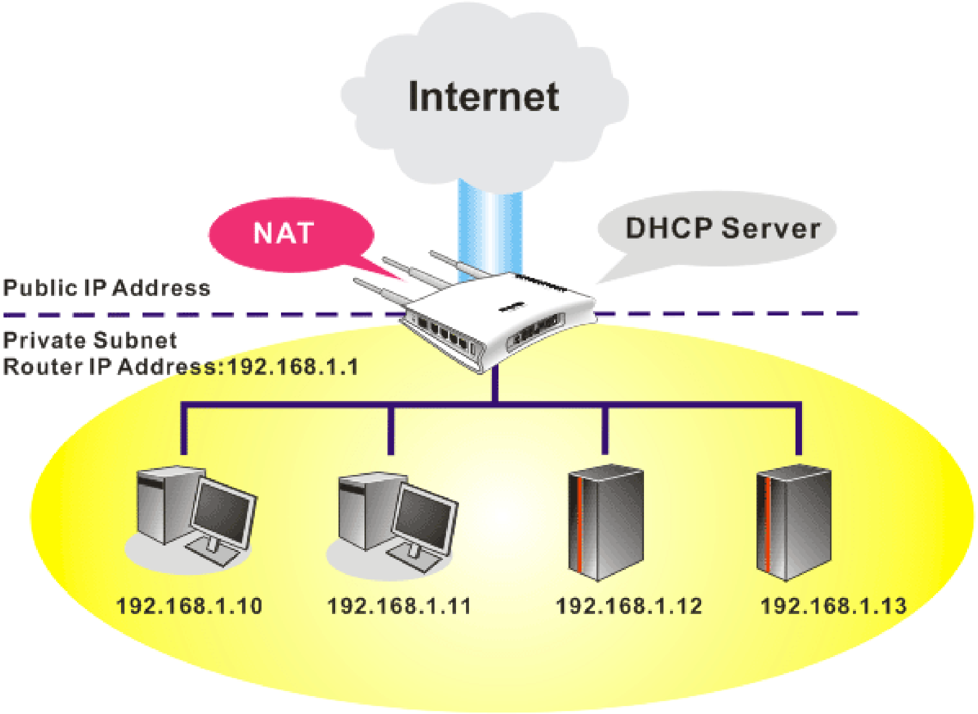
4.2 LAN

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.

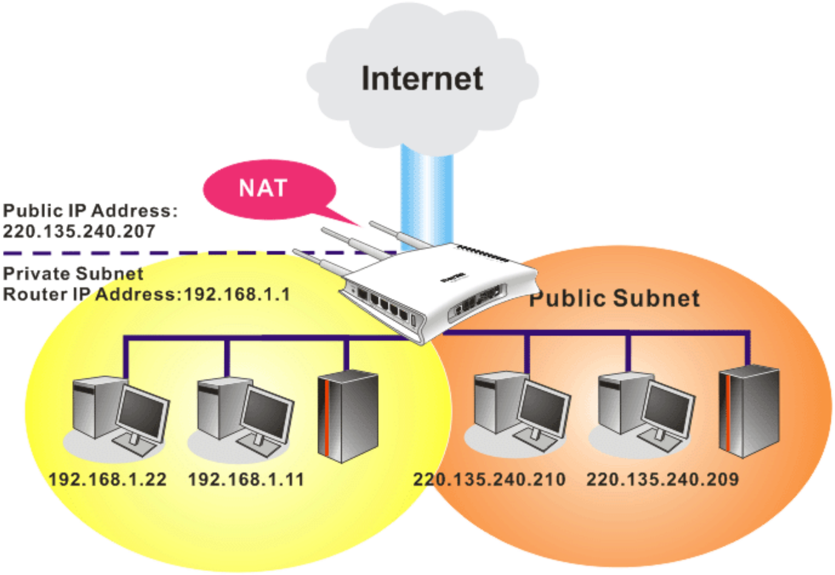


Basics of LAN

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)

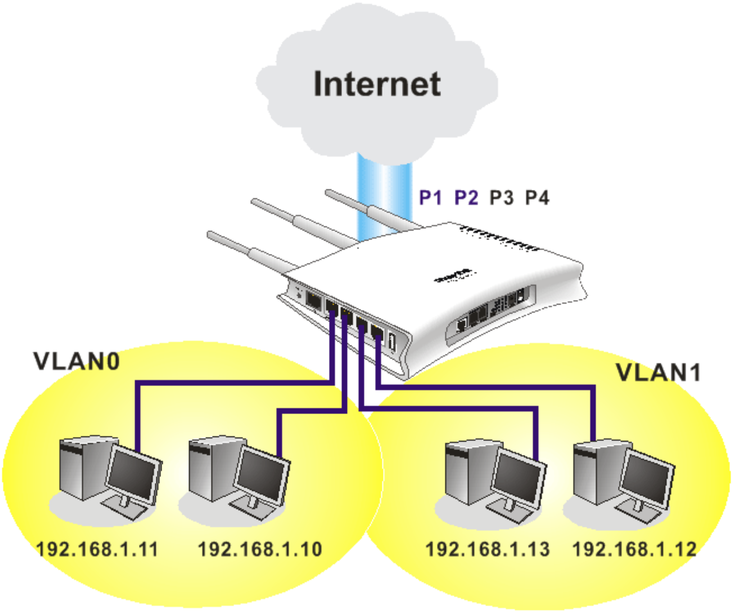
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

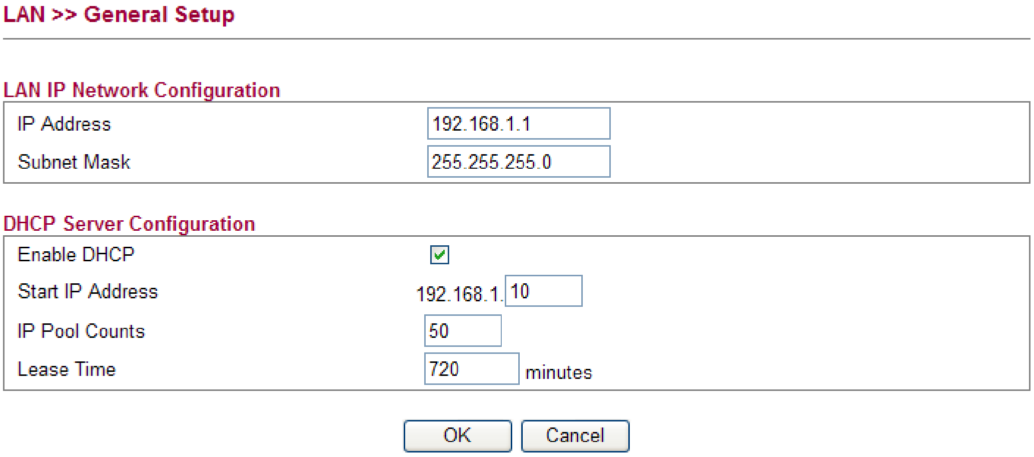
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



4.2.1 General Setup

This page provides you the general settings for LAN.

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



LAN >> General Setup

LAN IP Network Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

DHCP Server Configuration

Enable DHCP	☑
Start IP Address	192.168.1. 10
IP Pool Counts	50
Lease Time	720 minutes

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)

Enable DHCP 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.
You can configure the router to serve as a DHCP server for the 2nd subnet. Check the box to enable DHCP server setting.

Start IP Address Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

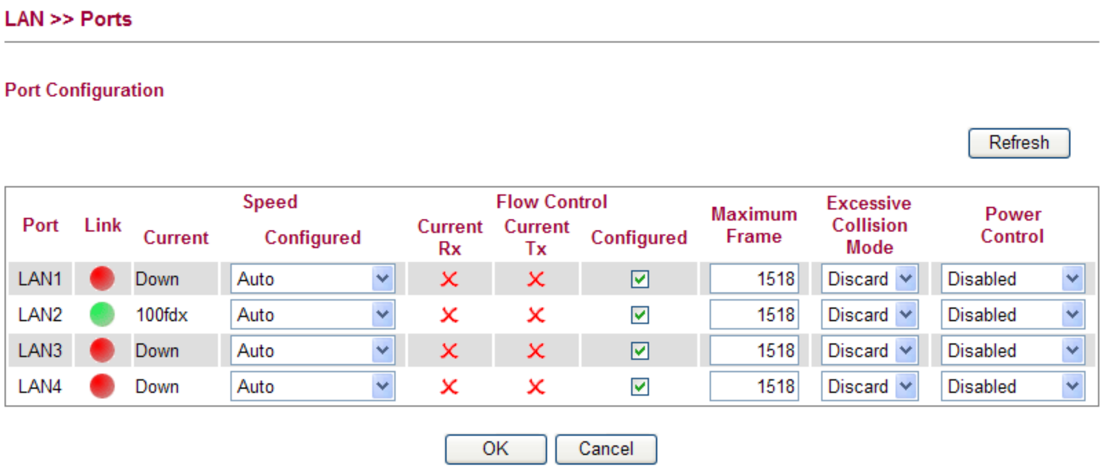
IP Pool Counts Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

Lease Time It allows you to set the leased time for the specified PC.

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

4.2.2 Ports

Ports page is used to change the setting for LAN ports. You can set or reset the following items. All of them are described in detail below.



LAN >> Ports

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
LAN1	🔴	Down	Auto	✗	✗	☑	1518	Discard	Disabled
LAN2	🟢	100fdx	Auto	✗	✗	☑	1518	Discard	Disabled
LAN3	🔴	Down	Auto	✗	✗	☑	1518	Discard	Disabled
LAN4	🔴	Down	Auto	✗	✗	☑	1518	Discard	Disabled

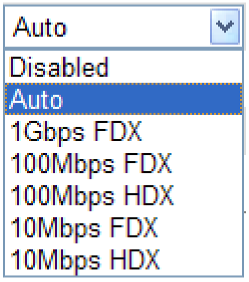
Port It displays current network interface.

Link It displays current connection status. Green light means the LAN connection is successful.

Current It displays current speed that the router uses.

Speed Configured It can set the speed and duplex of the port. You can use the drop down list to choose the required speed for the router. If you have no idea in configuring speed, simple use the default setting,

Auto.



Flow Control

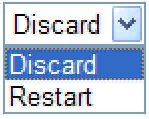
If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.
Current Rx: indicates whether pause frames on the port are obeyed.
Current Tx: indicates whether pause frames on the port are transmitted.

Maximum Frame

This module offers 1518~9600 (Bytes) length to make the long packet for data transmission.

Excessive Collision Mode

There are two modes for you to choose when excessive collision happened in half-duplex condition.

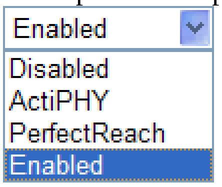


Discard - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

Restart - It determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Standard 802.3, but is useful in non-dropping half-duplex flow control operation.

Power Control

The Configured column allows for changing the power savings mode parameters per port.



Disabled: All power savings mechanisms disabled.
ActiPHY: Link down power savings enabled.
PerfectReach: Link up power savings enabled.
Enabled: Both link up and link down power savings enabled.

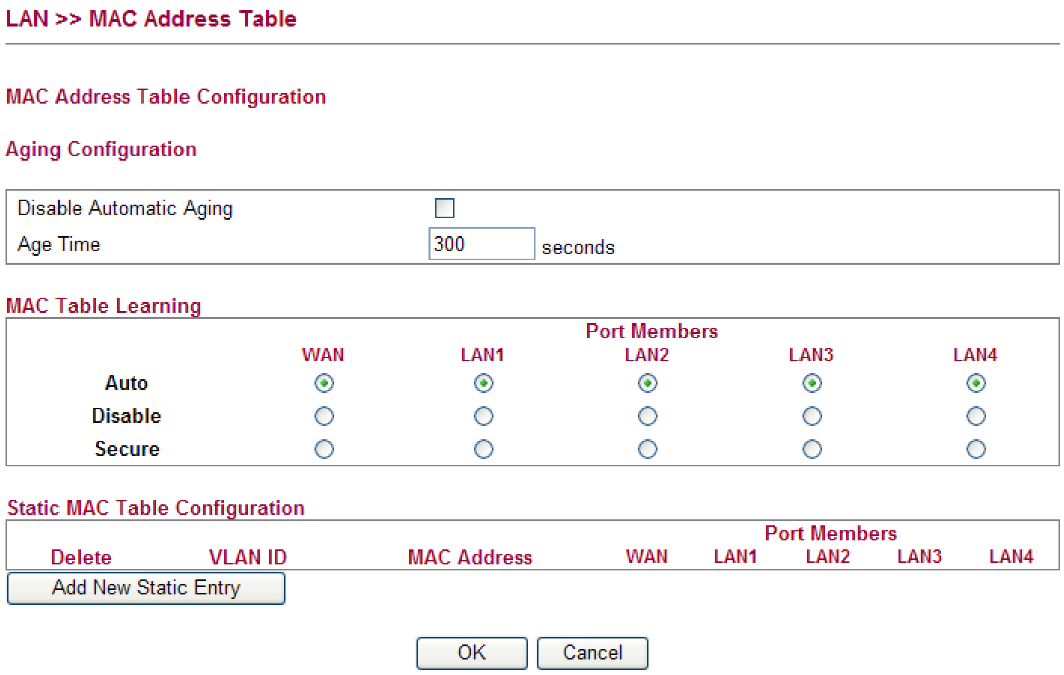
Refresh

Click this button to refresh the information for LAN ports.

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

4.2.3 MAC Address Table

This page allows you to set timeouts for entries in dynamic MAC Table and configure the static MAC table here.



LAN >> MAC Address Table

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Age Time	300 seconds

MAC Table Learning

	Port Members WAN	LAN1	LAN2	LAN3	LAN4
Auto	●	●	●	●	●
Disable	○	○	○	○	○
Secure	○	○	○	○	○

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members WAN	LAN1	LAN2	LAN3	LAN4

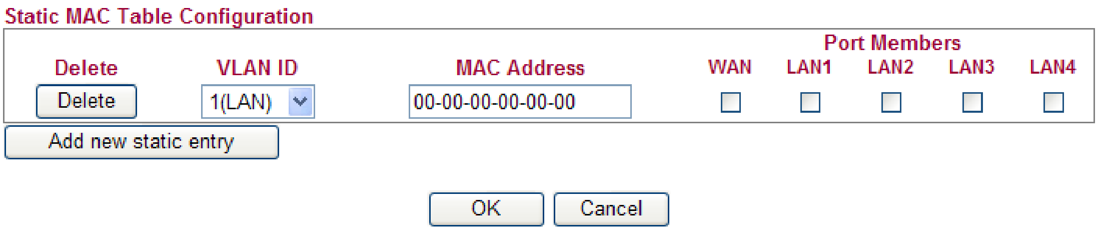
Disable Automatic Aging Stop the MAC table aging timer, the learned MAC address will not age out automatically. The default setting is enabled. Check the box to disable this function if required.

Age Time Delete a MAC address idling for a period of time from the following MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.

MAC Table Learning List the port members which apply dynamic learning mechanism or not.
Auto - Enable this port MAC address dynamic learning mechanism.
Disable - Disable this port MAC address dynamic learning mechanism, only support static MAC address setting.
Secure - Disable this port MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU.

Static MAC Table Config.. Specify static MAC address with VLAN ID to apply aging configuration.
Delete - Click the button to remove the VLAN setting.
VLAN ID - Specify the interface for the port members.
MAC Address - It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 – 02.
WAN/LAN1~4 - Check the port to apply this VLAN setting.

To add a new static MAC entry, click **Add new static entry**. A new entry will be shown as follows. Choose VLAN ID and type a new MAC address. Next, specify port member for this table. Finally, click OK to save the changes.

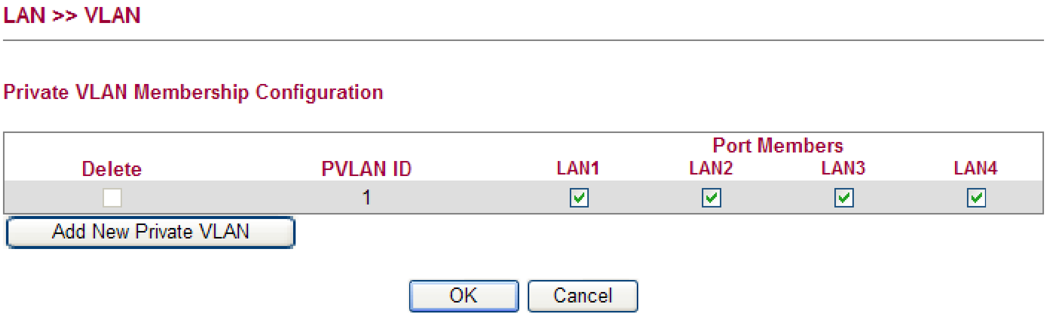


Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members WAN	LAN1	LAN2	LAN3	LAN4
Delete	1(LAN)	00-00-00-00-00-00	□	□	□	□	□

4.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to **LAN** page and select **VLAN**. The following page will appear. VLAN function is enabled in default.

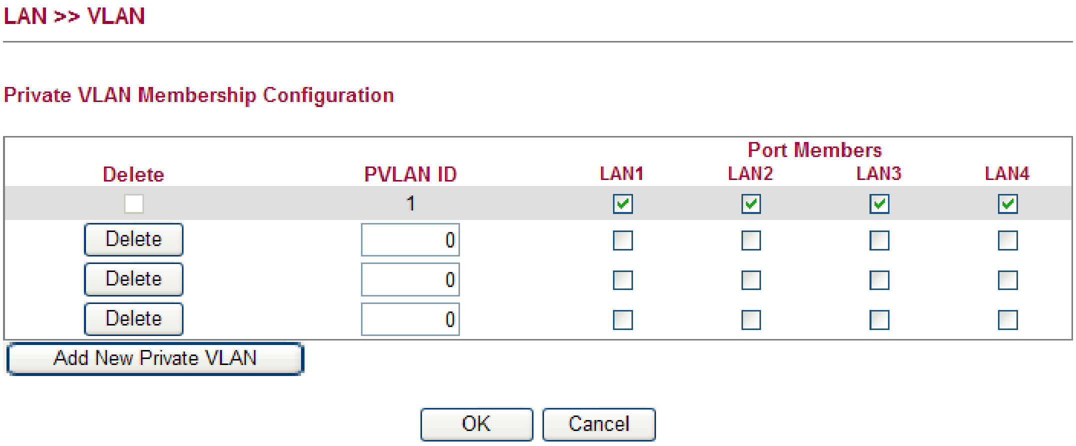


LAN >> VLAN

Private VLAN Membership Configuration

Delete	PVLAN ID	LAN1	Port Members LAN2	LAN3	LAN4
□	1	☑	☑	☑	☑

Add New Private VLAN Click this button to add a new private VLAN. The router allows you to add up to 4 VLAN.



LAN >> VLAN

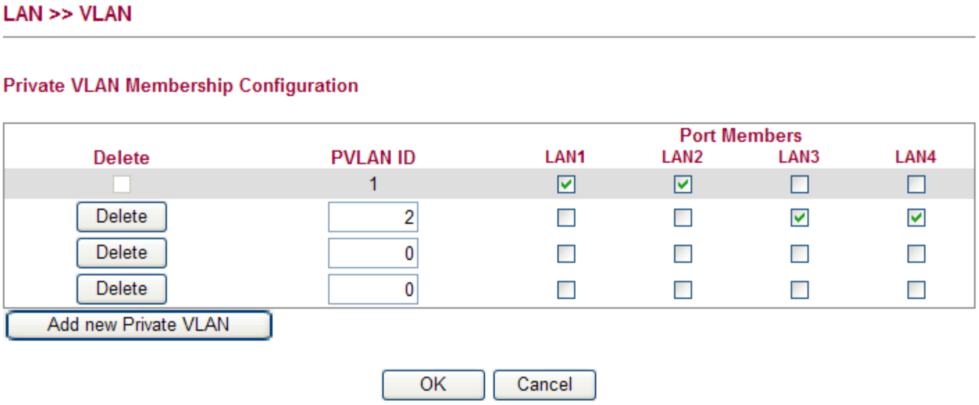
Private VLAN Membership Configuration

Delete	PVLAN ID	LAN1	Port Members LAN2	LAN3	LAN4
□	1	☑	☑	☑	☑
Delete	0	□	□	□	□
Delete	0	□	□	□	□
Delete	0	□	□	□	□

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

1. VLAN 1 is consisted of hosts linked to P1 ~ P4.

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



LAN >> VLAN

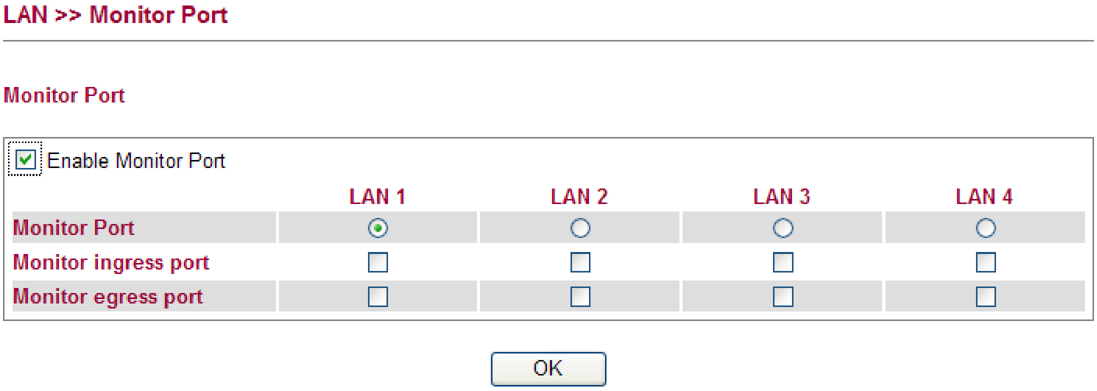
Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members			
		LAN1	LAN2	LAN3	LAN4
□	1	☑	☑	□	□
Delete	2	□	□	☑	☑
Delete	0	□	□	□	□
Delete	0	□	□	□	□

3. To remove VLAN, click the Delete button for the one you want to remove and click **OK** to save the results.

4.2.5 Monitor Port

It is used to monitor the traffic of the network. For example, we assume that LAN1 and LAN2 are Monitor Port and Monitor ingress Port respectively, thus, the traffic received by LAN2 will be copied to LAN1 for monitoring.



LAN >> Monitor Port

Monitor Port

☑ Enable Monitor Port

	LAN 1	LAN 2	LAN 3	LAN 4
Monitor Port	●	○	○	○
Monitor ingress port	□	□	□	□
Monitor egress port	□	□	□	□

Enable Monitor Port Check to enable this function.

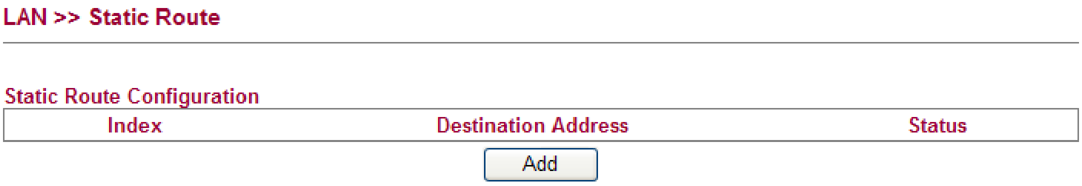
Monitor Port Click the one of the LAN ports to specify it for monitoring.

Monitor ingress port Check to set up the port(s) for being monitored. It only monitors the packets **received b**y the port you set up.

Monitor egress port Check to set up the port(s) for being monitored. It only monitors the packets **transmitted** by the port you set up.

4.2.6 Static Route

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



LAN >> Static Route

Static Route Configuration

Index	Destination Address	Status

Index The number (1 to 10) under Index displays current static router.

Destination Address Display the destination address of the static route.

Status Display the status of the static route.

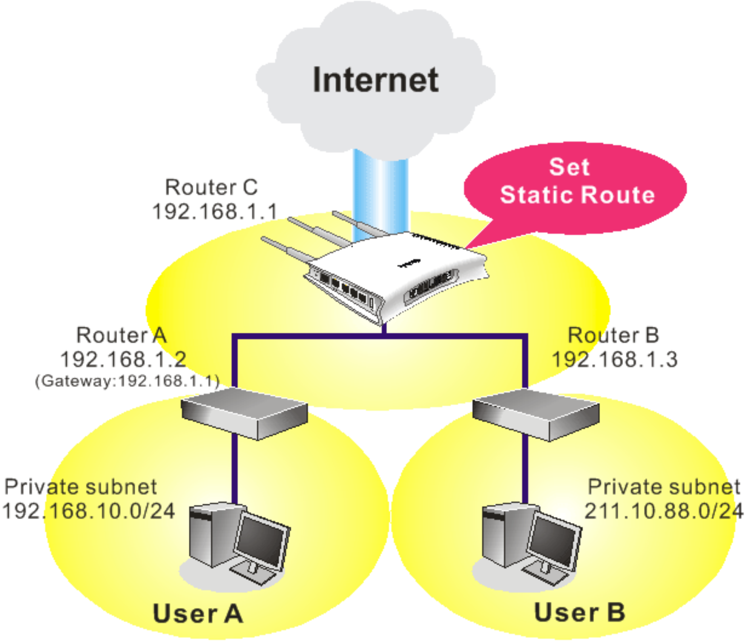
Add To add a new static route.

Add Static Routes to Private and Public Networks

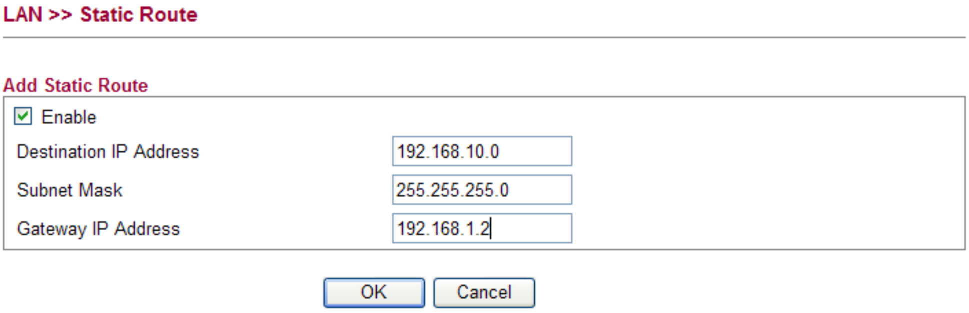
Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- 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. Click the **LAN - Static Route** and click **Add.** 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**.

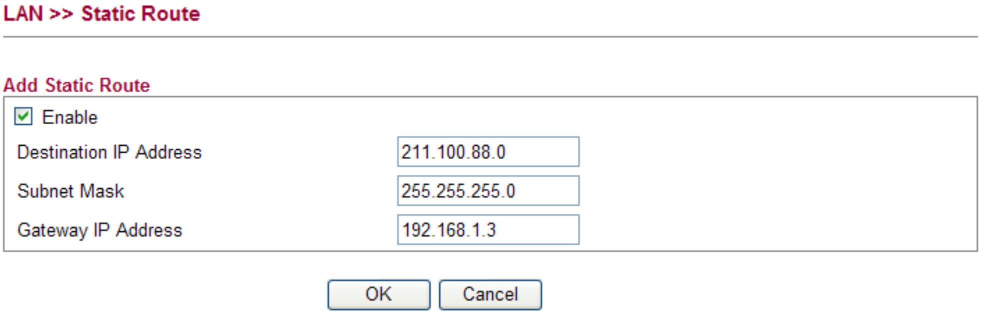

LAN >> Static Route

Add Static Route

☑ Enable

Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2

2. Return to **Static Route** page. Click **Add** again 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.

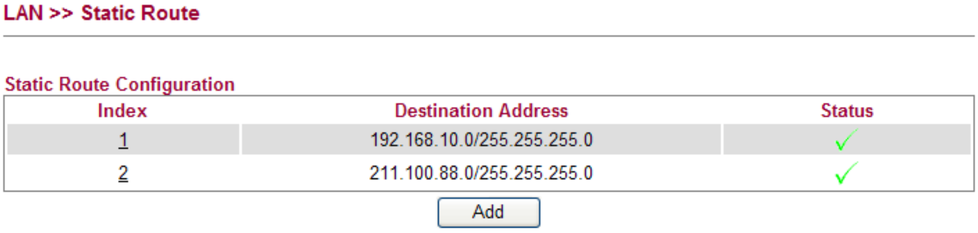


LAN >> Static Route

Add Static Route

☑ Enable	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3

3. Verify current routing table.



LAN >> Static Route

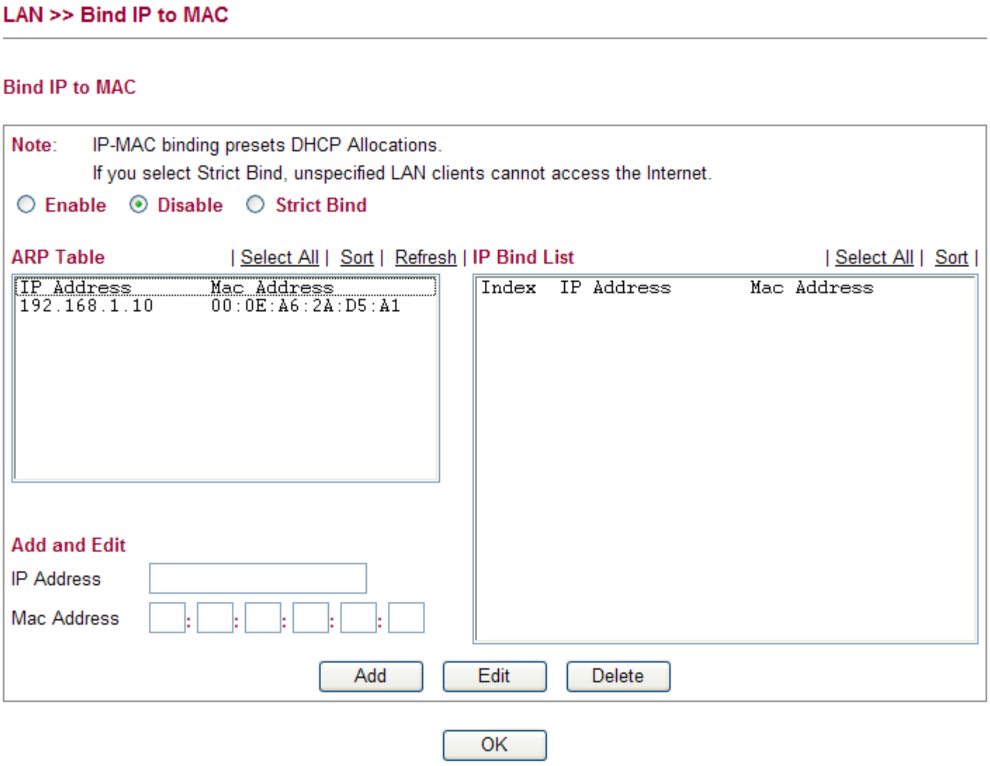
Static Route Configuration

Index	Destination Address	Status
1	192.168.10.0/255.255.255.0	✓
2	211.100.88.0/255.255.255.0	✓

4.2.7 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

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

○ Enable ● Disable ○ Strict Bind

ARP Table | Select All | Sort | Refresh |

```
IP Address        Mac Address
192.168.1.10      00:0E:A6:2A:D5:A1
```

IP Bind List | Select All | Sort |

```
Index  IP Address         Mac Address
```

Add and Edit

IP Address

Mac Address

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.

Remove You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Remove**. 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.

4.3 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.

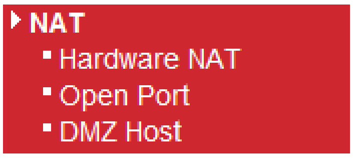
The benefit of the NAT includes:

- **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.

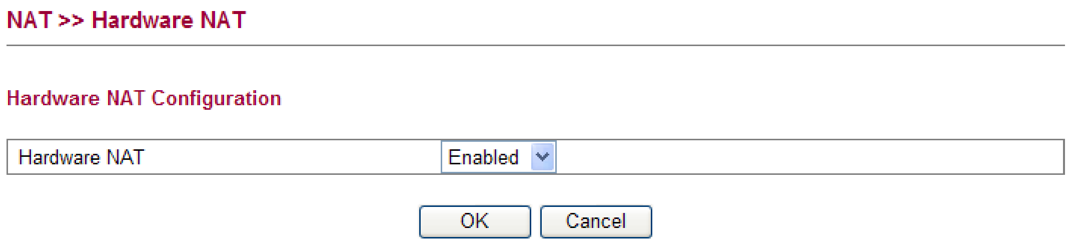


4.3.1 Hardware NAT

Hardware-base Acceleration Engine, also named Protocol Processing Engine API is the function that Draytek provides to extremely speed up the NAT performance.

While the hardware acceleration mechanism is activated, most of the bandwidth usage will be concentrated on the specific sessions which increase transmission speed to get ultimately accelerated.

With Hardware NAT, LAN to WAN NAT throughput can be over 900M bps. But be sure that your PC has Giga Ethernet and connect with CAT6 Ethernet cable.



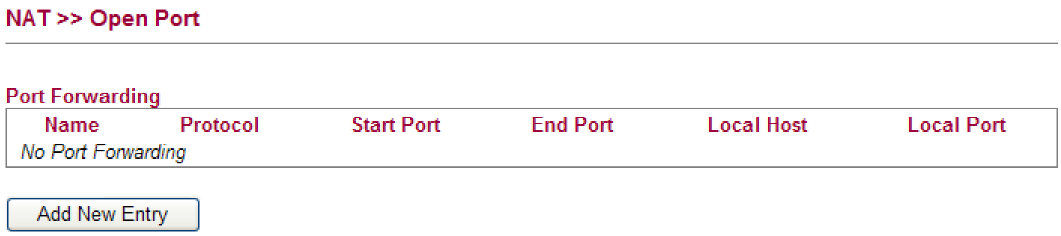
NAT >> Hardware NAT

Hardware NAT Configuration

Hardware NAT	Enabled

4.3.2 Open Ports

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



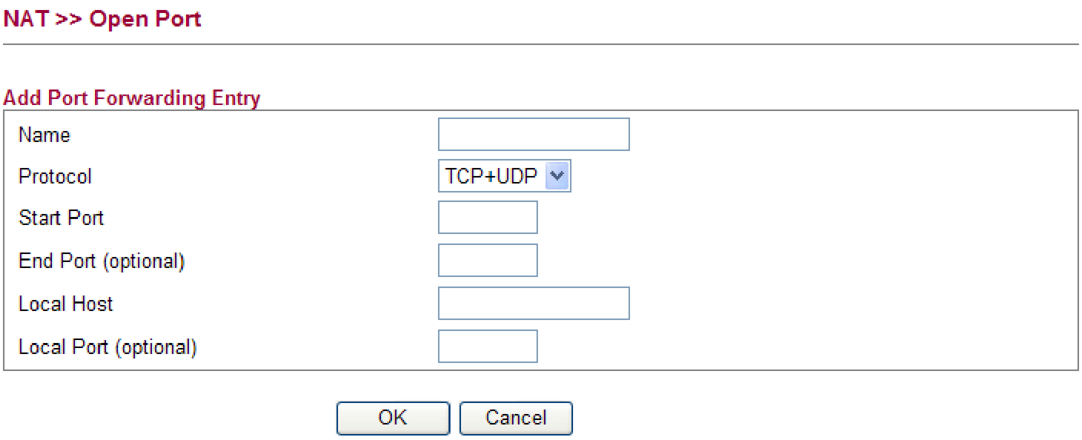
NAT >> Open Port

Port Forwarding

Name	Protocol	Start Port	End Port	Local Host	Local Port
No Port Forwarding					

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.

To add a new open port, click **Add new entry**.



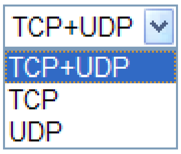
NAT >> Open Port

Add Port Forwarding Entry

Name	
Protocol	TCP+UDP
Start Port	
End Port (optional)	
Local Host	
Local Port (optional)	

Name Specify the name for the defined network service.

Protocol Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**.



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

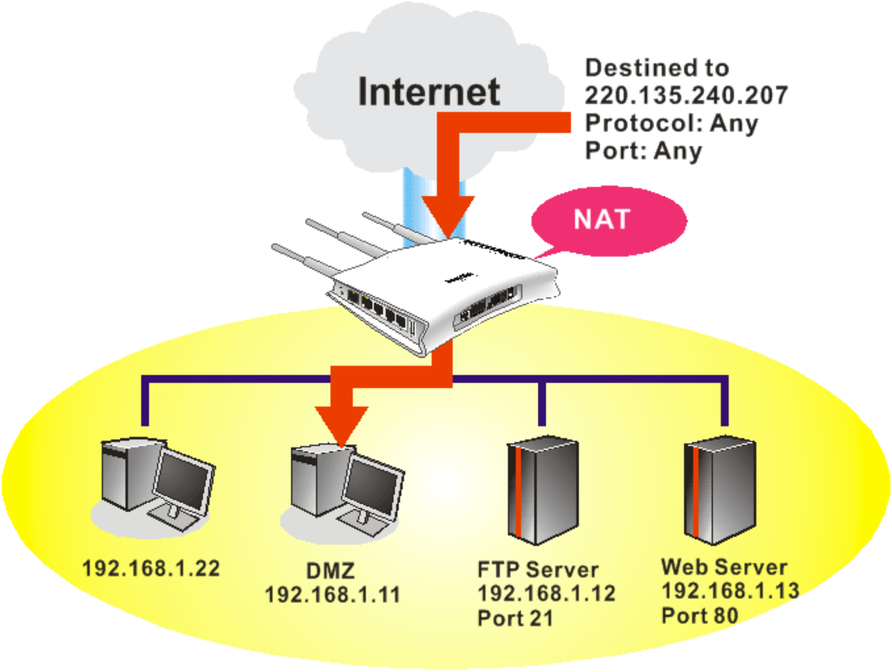
End Port (optional) Specify the ending port number of the service offered by the local host.

Local Host Enter the private IP address of the local host.

Local Port (optional) If it is configured, the forwarded traffic is mapped to this port on the local host.

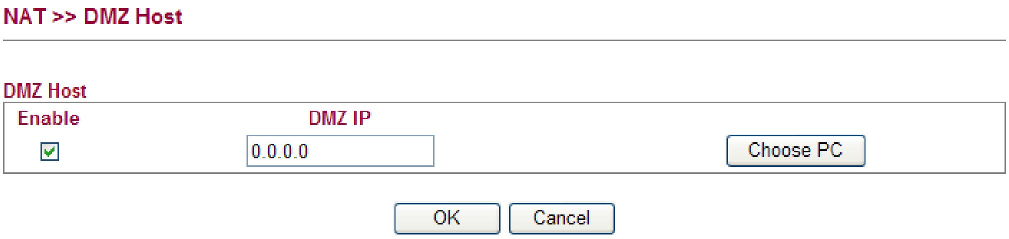
4.3.3 DMZ Host

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:



NAT >> DMZ Host

DMZ Host

Enable	DMZ IP	
☑	0.0.0.0	Choose PC

Enable Check to enable the DMZ Host function.

DMZ IP Enter the private IP address of the DMZ host, or click **Choose PC** to specify a suitable one.

4.4 Firewall

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.

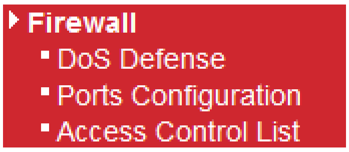
Denial of Service (DoS) Defense

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.

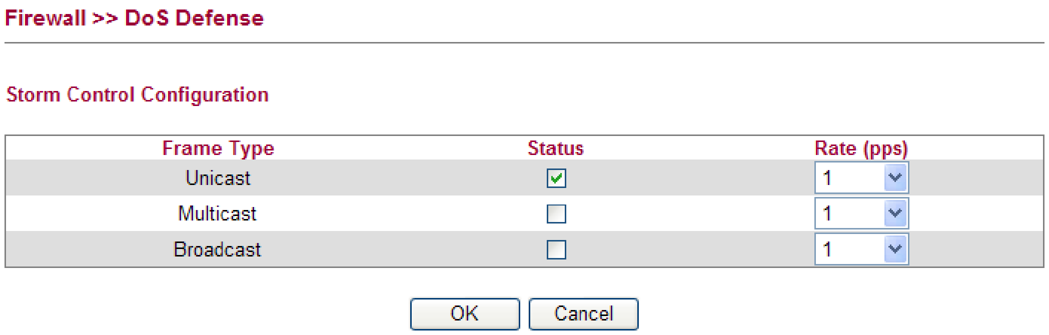
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

Below shows the menu items for Firewall.



4.4.1 DoS Defense

Click **Firewall** and click **DoS Defense** to open the setup page. Storm control for the switch is configured on this page.



Firewall >> DoS Defense

Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	☑	1
Multicast	□	1
Broadcast	□	1

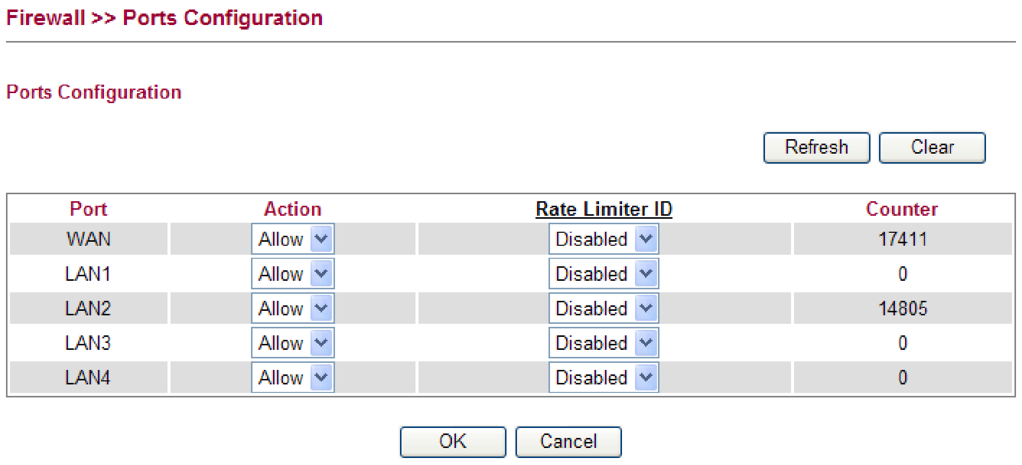
Frame Type Set the Unicast storm rate control, multicast storm rate control, and a broadcast storm rate control for your router.

Status Check this box to enable storm control status for the frame type.

Rate The unit is packet per second (pps). Use the drop down list to set the rate for data transmission. The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

4.4.2 Ports Configuration

This page is used to configure the ACL (Access Control List) parameters for each port. These parameters will affect data packets received on a port unless the data packets match a specific ACE (Access Control Entry).



Firewall >> Ports Configuration

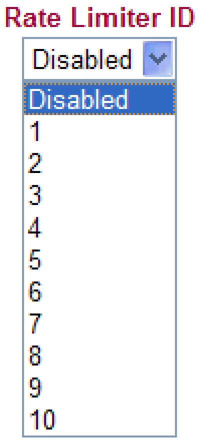
Ports Configuration

Port	Action	Rate Limiter ID	Counter
WAN	Allow	Disabled	17411
LAN1	Allow	Disabled	0
LAN2	Allow	Disabled	14805
LAN3	Allow	Disabled	0
LAN4	Allow	Disabled	0

Port There is one WAN port and 4 LAN ports in Vigor2130. Here each port will be configured with different ID, action, rate limiter ID, port copy and etc.

Action Select whether forwarding is permitted ("Allow") or denied ("Deny"). The default value is "Allow".

Rate Limiter ID Select a rate limiter to apply to this port. Available settings include **Disabled**, and 1 to 10. The default value is **Disabled**.



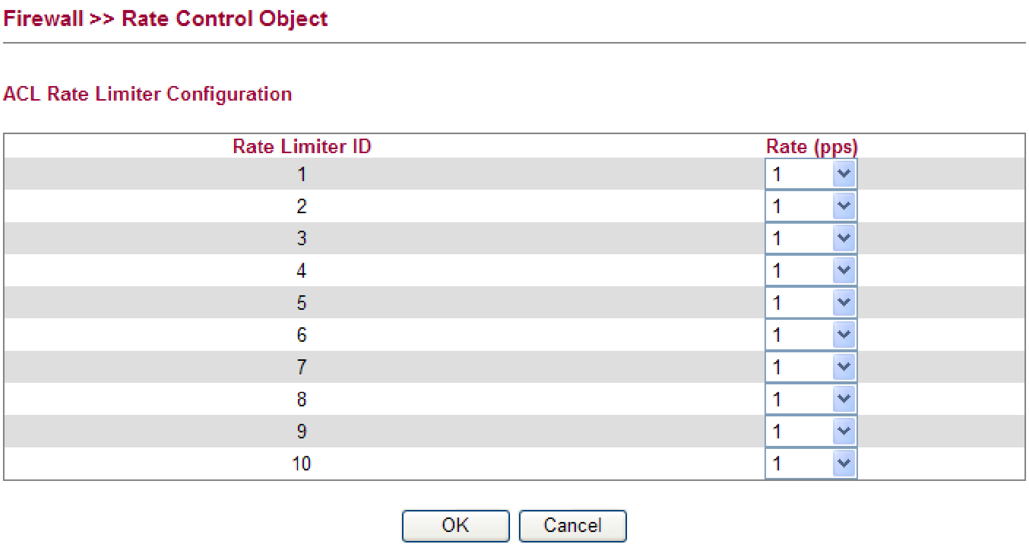
Counter Counts the number of frames that match this Access Control Entry (ACE).

Refresh Click this button to refresh the number of the counter immediately.

Clear Click this button to clear the number of the counter on this page.

Rate Limiter ID

Configure the rate limiter for the ACL (Access Control List) of the router. Please click **Rate Limiter ID** link to access into the following page.



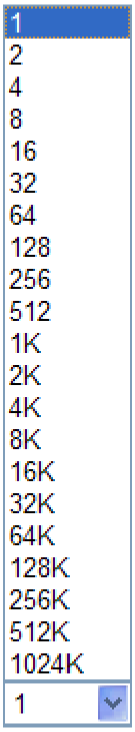
Firewall >> Rate Control Object

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1

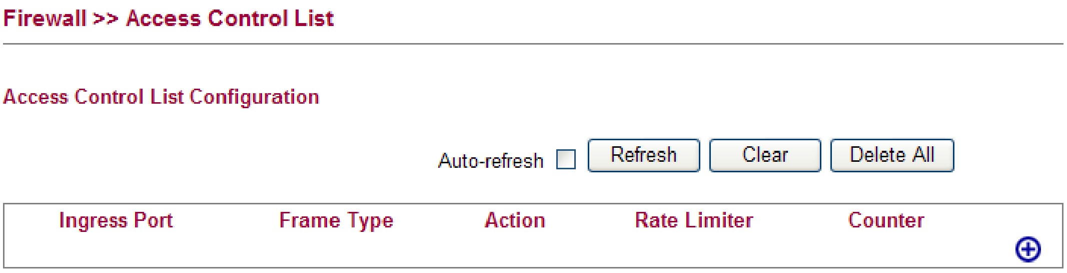
Rate Limiter ID Rate limiter ID will be applied to WAN port and LAN port. Please specify a rate number for each ID. The default setting is “1”(packet per second).

Rate Define the rate by choosing from the following drop down list.



4.4.3 Access Control List

This page can define which kind of packet can access the router. The packet can be defined with input port, Frame type, Rate, MAC type, VLAN ID, tag and etc.. For IPv4, we can also define the protocol type, source IP and destination IP.



Firewall >> Access Control List

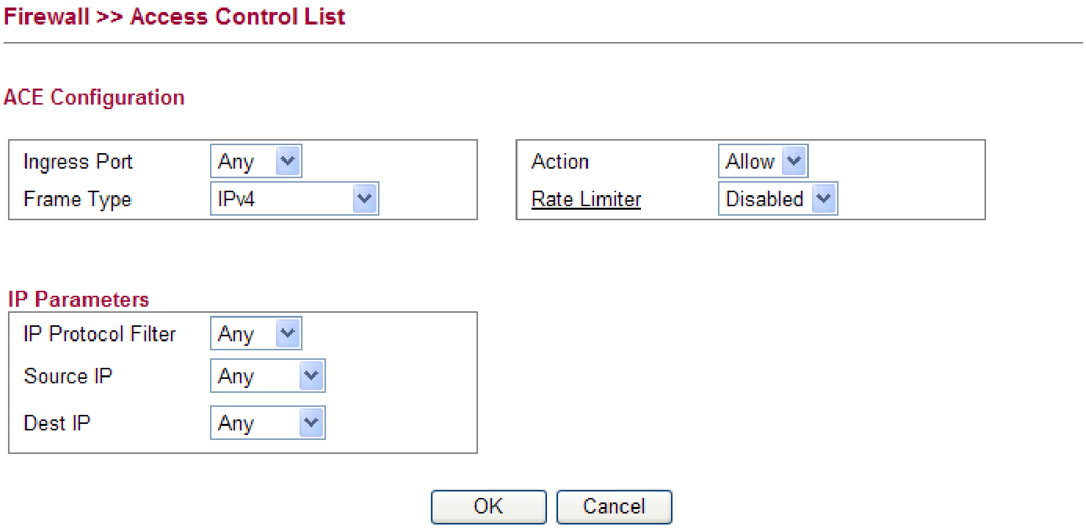
Access Control List Configuration

Auto-refresh □ Refresh Clear Delete All

Ingress Port	Frame Type	Action	Rate Limiter	Counter

Adding a New Access Control Profile

Click ⊕ to add a new specific session limitation onto the list.



Firewall >> Access Control List

ACE Configuration

Ingress Port	Any
Frame Type	IPv4
Action	Allow
Rate Limiter	Disabled

IP Parameters

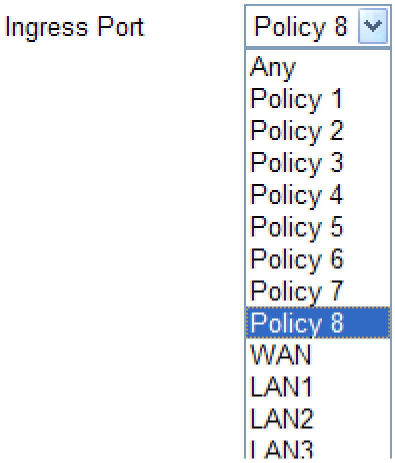
IP Protocol Filter	Any
Source IP	Any
Dest IP	Any

OK Cancel

Define which port the packet from.

ACE Configuration

Ingress Port – define which port the packet coming from. The policy IDs are defined in **Firewall>>Port Configuration**. Each Policy ID might have more than one port grouped.



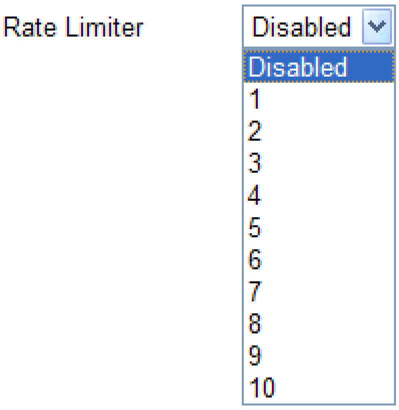
Ingress Port: Policy 8

Frame Type - Such option differs according to the selection you choose, we will explain it in detailed later.

Action – it means the session limitation for this access control list will be applied to if matching with the rule defined in this page.

Action: Allow

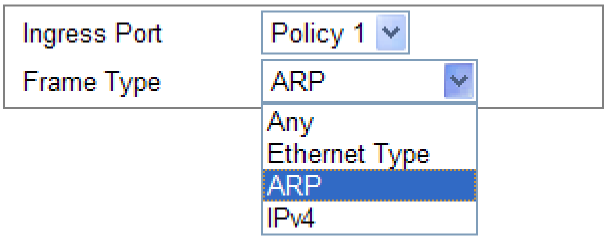
Rate Limiter - Select a rate limiter to apply to this port. Available settings include **Disabled**, and 1 to 10. The default value is **Disabled**. Click the **Rate Limiter** link to configure different rates for each ID.



Rate Limiter: Disabled

Detailed Explanation for Frame Type

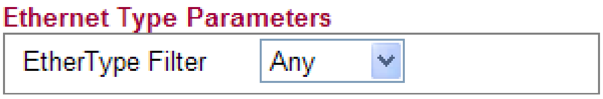
Frame Type selection will lead different options for configuration.



Ingress Port: Policy 1

Frame Type: ARP

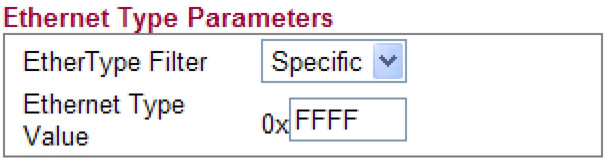
- Choose **Ethernet Type** as the Frame Type, you will get **Ethernet Type Parameters** option as the following:



Ethernet Type Parameters

EtherType Filter: Any

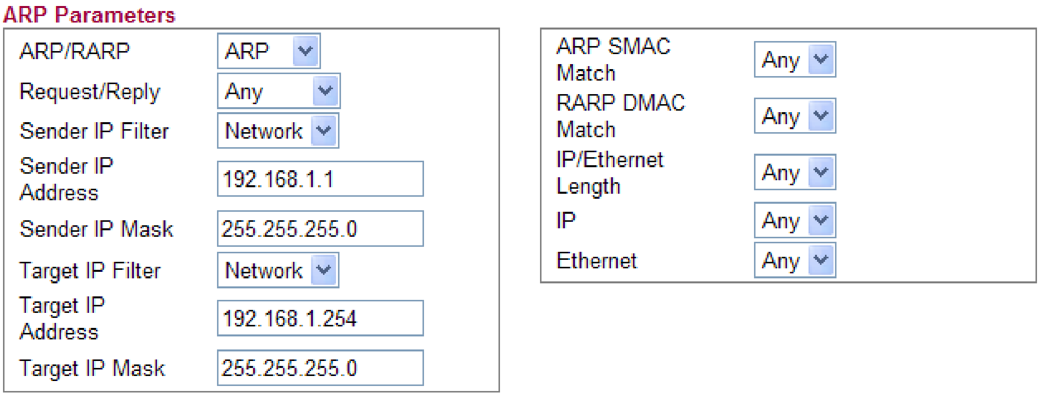
Ethernet Type Filter Choose **Any** to set the parameter with any value set by the router automatically or choose **Specific** to specify certain value (the range is 0x0000 to 0xFFFF).



Ethernet Type Parameters

EtherType Filter	Specific
Ethernet Type Value	0x FFFF

- Choose **ARP** as the Frame Type, you will get **ARP Parameters** option as the following:



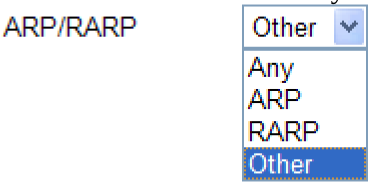
ARP Parameters

ARP/RARP	ARP
Request/Reply	Any
Sender IP Filter	Network
Sender IP Address	192.168.1.1
Sender IP Mask	255.255.255.0
Target IP Filter	Network
Target IP Address	192.168.1.254
Target IP Mask	255.255.255.0

ARP SMAC Match	Any
RARP DMAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

ARP/RARP

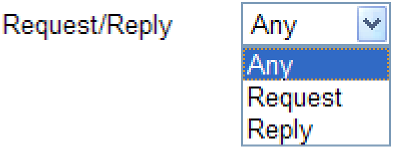
Choose the ARP/RARP that you want to filter.



ARP/RARP: Other

Request/Reply

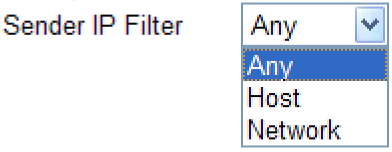
Choose the request or replay that you want to filter.



Request/Reply: Any

Sender IP Filter

Specify the sender IP filter for this ACE.



Sender IP Filter: Any

Choose **Any** to filter all of the packets.
Choose **Host** to filter the packets from the host with the address typed in Sender IP Address filed.
Choose **Network** to filter the packets within the network defined in **Sender IP Address** and **Sender IP Mask** fields.

Sender IP Address

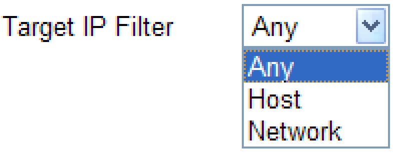
Type the Sender IP Address here. This option is available when you choose **Host** or **Network** as Sender IP Filter.

Sender IP Mask

Type the Sender IP Mask here. This option is available only when you choose **Network** as Sender IP Filter.

Target IP Filter

Specify the target IP filter for this specific ACE.



Target IP Filter: Any

Choose **Any** to filter all of the packets.
Choose **Host** to filter the packets from the host with the address typed in Target IP Address filed.
Choose **Network** to filter the packets within the network defined in **Target IP Address** and **Target IP Mask** fields.

Target IP Address

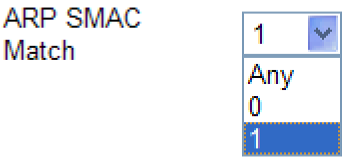
Type the Target IP Address here. This option is available when you choose **Host** or **Network** as Target IP Filter.

Target IP Mask

Type the Target IP Mask here. This option is available only when you choose **Network** as Target IP Filter.

ARP SMAC Match

Specify whether frames/packets can meet the action according to the sender hardware address field (SHA) settings.

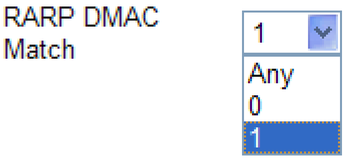


ARP SMAC Match: 1

0: means sender hardware address is not equal to the SMAC address.
1: means sender hardware address is equal to the SMAC address.
Any: means any value is allowed.

RARP DMAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

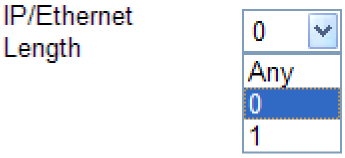


RARP DMAC Match: 1

0: means target hardware address is not equal to the SMAC address.
1: means s target hardware address is equal to the SMAC address.
Any: means any value is allowed.

IP/Ethernet Length

Specify whether frames/packets can meet the action according to the ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

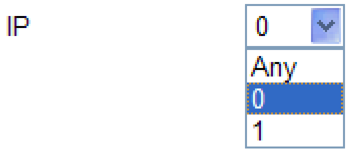


IP/Ethernet Length: 0

0**:** means ARP/RARP frames/packets where the hardware address length is equal to Ethernet (0x06) and the protocol address length is equal to IPv4 (0x04) **must not** match this entry.

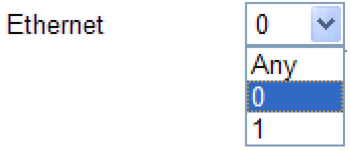
1**:** means ARP/RARP frames/packets where the hardware address length is equal to Ethernet (0x06) and the protocol address length is equal to IPv4 (0x04) **must** match this entry.
Any: Any value is allowed

IP Specify whether frames/packets can meet the action according to their ARP/RARP hardware address space (HRD) settings.



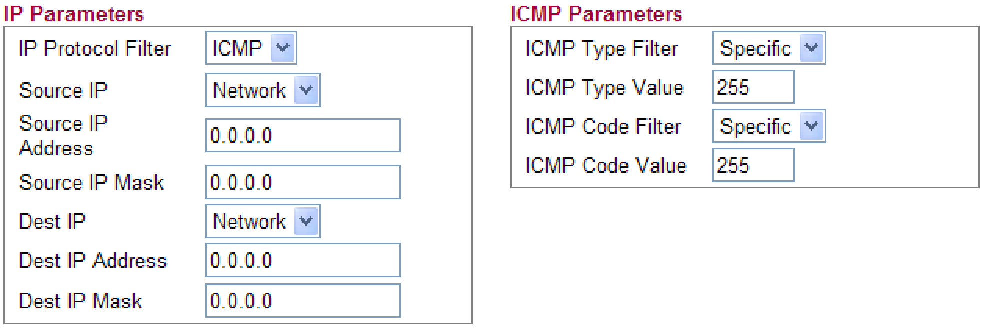
0**:** ARP/RARP frames where the hardware address space is equal to Ethernet (1) must not match this entry.
1**:** ARP/RARP frames where the hardware address space is equal to Ethernet (1) must match this entry.
Any: Any value is allowed.

Ethernet Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.



0: ARP/RARP frames where the protocol address space is equal to IP (0x800) must not match this entry.
1: ARP/RARP frames where the protocol address space is equal to IP (0x800) must match this entry.
Any: Any value is allowed.

- Choose **IPv4** as the Frame Type. You will see **IP Parameters** on the bottom of the page. If you choose **ICMP** as **IP Protocol Filter**, you will get the page as the following:



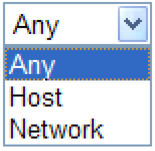
IP Parameters

IP Protocol Filter	ICMP
Source IP	Network
Source IP Address	0.0.0.0
Source IP Mask	0.0.0.0
Dest IP	Network
Dest IP Address	0.0.0.0
Dest IP Mask	0.0.0.0

ICMP Parameters

ICMP Type Filter	Specific
ICMP Type Value	255
ICMP Code Filter	Specific
ICMP Code Value	255

Source IP Specify the Source IP filter for this ACE.



Any: No source IP filter is specified.
Host: Source IP filter is set to Host. Specify the source IP address in the Source IP Address field that appears.
Network: Source IP filter is set to Network. Specify the

source IP address and source IP mask in the Source IP Address and Source IP Mask fields that appear.

Source IP Address

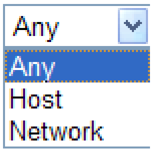
Type the Source IP Address here. This option is available when you choose **Host** or **Network** as Source IP.

Source IP Mask

Type the Source IP Mask here. This option is available only when you choose **Network** as source Source IP.

Dest IP Filter

Specify the destination IP filter for this ACE.



Any: No destination IP filter is specified.
Host: Destination IP filter is set to Host. Specify the destination IP address in the Dest IP Address field that appears.
Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and Dest IP Mask fields that appear.

Dest IP Address

Type the Dest IP Address here. This option is available when you choose **Host** or **Network** as destination Dest IP.

Dest IP Mask

Type the Dest IP Mask here. This option is available only when you choose **Network** as destination Dest IP.

ICMP Type Filter

Specify the ICMP filter for this ACE.

Any: No ICMP filter is specified.
Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

If you choose **Specific** as ICMP Type Filter, you have to type the ICMP Type Value manually. The allowed range is 0 to 255. A frame meeting this ACE matches this ICMP value.

ICMP Code Filter

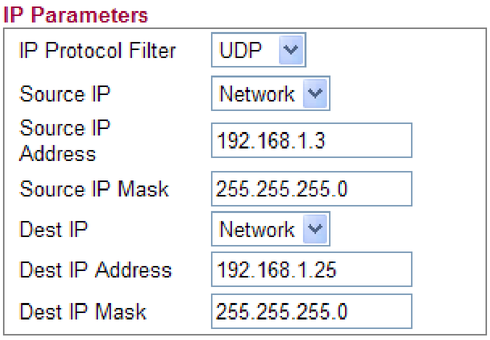
Specify the ICMP code filter for this ACE.

Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").
Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value

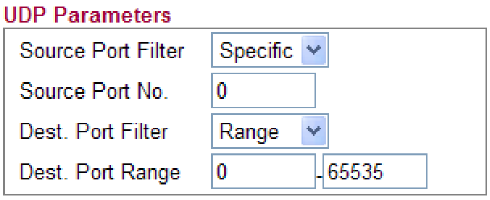
If you choose Specific as ICMP Code Filter, you have to type the ICMP Type Value manually. The allowed range is 0 to 255. A frame meeting this ACE matches this ICMP value.

- Choose **IPv4** as the Frame Type. You will see **IP Parameters** on the bottom of the page. If you choose **UDP** as **IP Protocol Filter**, you will get the page as the following:



IP Parameters

IP Protocol Filter	UDP
Source IP	Network
Source IP Address	192.168.1.3
Source IP Mask	255.255.255.0
Dest IP	Network
Dest IP Address	192.168.1.25
Dest IP Mask	255.255.255.0

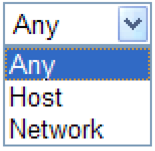


UDP Parameters

Source Port Filter	Specific
Source Port No.	0
Dest. Port Filter	Range
Dest. Port Range	0 - 65535

Source IP

Specify the source IP filter for this ACE.



Any: No source IP filter is specified.
Host: Source IP filter is set to Host. Specify the source IP address in the Source IP Address field that appears.
Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the Source IP Address and Source IP Mask fields that appear.

Source IP Address

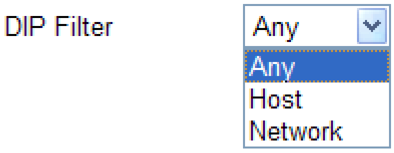
Type the Source IP Address here. This option is available when you choose **Host** or **Network** as source Source IP.

Source IP Mask

Type the Source IP Mask here. This option is available only when you choose **Network** as source Source IP.

Dest IP

Specify the destination IP filter for this ACE.



Any: No destination IP filter is specified.
Host: Destination IP filter is set to Host. Specify the destination IP address in the destination IP Address field that appears.
Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the destination IP Address and destination IP Mask fields that appear.

Dest IP Address

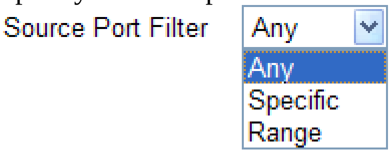
Type the destination IP Address here. This option is available when you choose **Host** or **Network** as destination IP.

Dest IP Mask

Type the DIP Mask here. This option is available only when you choose **Network** as destination DIP.

Source Port Filter

Specify the UDP port source filter for this ACE.



Any: No UDP source filter is specified.
Specific: If you want to filter a specific UDP source filter with this ACE, you can enter a specific UDP source value. A field for entering a UDP source value appears.
Range: If you want to filter a specific UDP source range filter with this ACE, you can enter a specific UDP source range value. A field for entering a UDP source port range appears.

Source Port No.

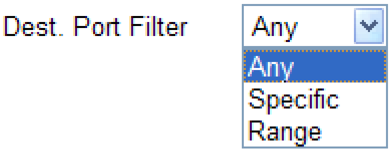
Type the value if you choose **Specific** as the Source Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this UDP source value.

Source Port Range

Type the value if you choose **Range** as the Source Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this UDP source value.

Dest. Port Filter

Specify the UDP port destination filter for this ACE.



Any: No UDP destination filter is specified.
Specific: If you want to filter a specific UDP destination filter with this ACE, you can enter a specific UDP destination value. A field for entering a UDP destination value appears.
Range: If you want to filter a specific UDP destination range filter with this ACE, you can enter a specific UDP destination range value. A field for entering a UDP destination port range appears.

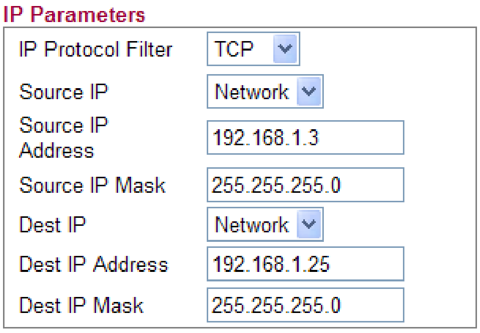
Dest. Port No.

Type the value if you choose **Specific** as the Dest. Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this UDP source value.

Dest. Port Range

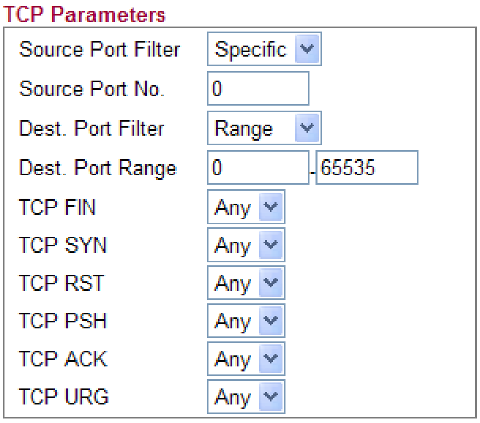
Type the value if you choose **Range** as the Dest. Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this UDP source value.

- Choose **IPv4** as the Frame Type. You will see **IP Parameters** on the bottom of the page. If you choose **TCP** as **IP Protocol Filter**, you will get the page as the following:



IP Parameters

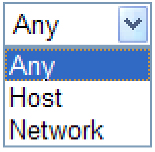
IP Protocol Filter	TCP
Source IP	Network
Source IP Address	192.168.1.3
Source IP Mask	255.255.255.0
Dest IP	Network
Dest IP Address	192.168.1.25
Dest IP Mask	255.255.255.0



TCP Parameters

Source Port Filter	Specific
Source Port No.	0
Dest. Port Filter	Range
Dest. Port Range	0 - 65535
TCP FIN	Any
TCP SYN	Any
TCP RST	Any
TCP PSH	Any
TCP ACK	Any
TCP URG	Any

Source IP Specify the source IP filter for this ACE.

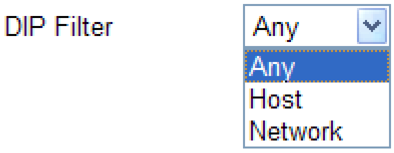


Any: No source IP filter is specified.
Host: Source IP filter is set to Host. Specify the source IP address in the source IP Address field that appears.
Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the source IP Address and source IP Mask fields that appear.

Source IP Address Type the source IP Address here. This option is available when you choose **Host** or **Network** as source source IP filter.

Source IP Mask Type the SIP Mask here. This option is available only when you choose **Network** as source IP filter.

Dest IP Filter Specify the destination IP filter for this ACE.



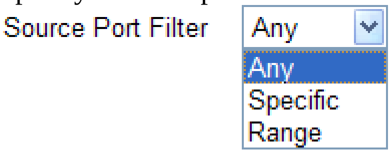
Any: No destination IP filter is specified.
Host: Destination IP filter is set to Host. Specify the destination IP address in the destination IP Address field that appears.
Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the destination IP Address and destination IP Mask fields that appear.

Dest IP Address Type the destination IP Address here. This option is available when you choose **Host** or **Network** as destination IP filter.

Dest IP Mask Type the destination IP Mask here. This option is available only when you choose **Network** as destination IP filter.

Source Port Filter

Specify the TCP port source filter for this ACE.


Source Port Filter: Any

Any: No TCP source filter is specified.
Specific: If you want to filter a specific TCP source filter with this ACE, you can enter a specific TCP source value. A field for entering a TCP source value appears.
Range: If you want to filter a specific TCP source range filter with this ACE, you can enter a specific TCP source range value. A field for entering a TCP source port range appears.

Source Port No.

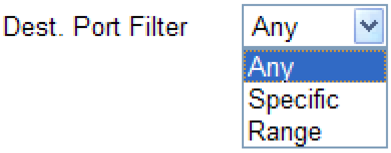
Type the value if you choose **Specific** as the Source Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this TCP source value.

Source Port Range

Type the value if you choose **Range** as the Source Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this TCP source value.

Dest. Port Filter

Specify the TCP port destination filter for this ACE.


Dest. Port Filter: Any

Any: No TCP destination filter is specified.
Specific: If you want to filter a specific TCP destination filter with this ACE, you can enter a specific TCP destination value. A field for entering a TCP destination value appears.
Range: If you want to filter a specific TCP destination range filter with this ACE, you can enter a specific TCP destination range value. A field for entering a TCP destination port range appears.

Dest. Port No.

Type the value if you choose **Specific** as the Dest. Port filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this TCP source value.

Dest. Port Range

Type the value if you choose **Range** as the Dest. Port filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this TCP source value.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

Any

0: TCP frames where the FIN field is set must not be able to match this entry.
1: TCP frames where the FIN field is set must be able to match this entry.
Any: Any value is allowed.

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

0: TCP frames where the SYN field is set must not be able to match this entry.

1: TCP frames where the SYN field is set must be able to match this entry.

Any: Any value is allowed.

TCP RST

Specify the TCP RST value for this ACE.

0: TCP frames where the RST field is set must not be able to match this entry.

1: TCP frames where the RST field is set must be able to match this entry.

Any: Any value is allowed.

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

0: TCP frames where the PSH field is set must not be able to match this entry.

1: TCP frames where the PSH field is set must be able to match this entry.

Any: Any value is allowed.

TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

0: TCP frames where the ACK field is set must not be able to match this entry.

1: TCP frames where the ACK field is set must be able to match this entry.

Any: Any value is allowed

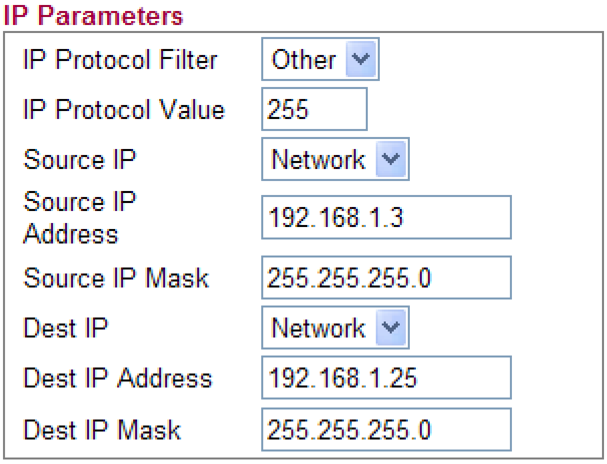
TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

0: TCP frames where the URG field is set must not be able to match this entry.

1: TCP frames where the URG field is set must be able to match this entry.
Any: Any value is allowed.

- Choose **IPv4** as the Frame Type. You will see **IP Parameters** on the bottom of the page. If you choose **Other** as **IP Protocol Filter**, you will get the page as the following:

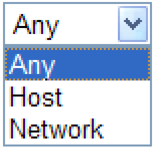


IP Parameters

IP Protocol Filter	Other
IP Protocol Value	255
Source IP	Network
Source IP Address	192.168.1.3
Source IP Mask	255.255.255.0
Dest IP	Network
Dest IP Address	192.168.1.25
Dest IP Mask	255.255.255.0

IP Protocol Value When "Other" is selected for the IP protocol filter, you can enter a specific value here. The range is 0 to 255. The default value is “255”.A frame meeting this ACE matches this IP protocol value.

Source IP Specify the source IP filter for this ACE.

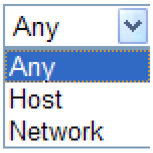


Any: No source IP filter is specified.
Host: Source IP filter is set to Host. Specify the source IP address in the source IP Address field that appears.
Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the source IP Address and source IP Mask fields that appear.

Source IP Address Type the source IP Address here. This option is available when you choose **Host** or **Network** as source IP Filter.

Source IP Mask Type the source IP Mask here. This option is available only when you choose **Network** as source IP.

Dest IP Specify the destination IP filter for this ACE.



Any: No destination IP filter is specified.
Host: Destination IP filter is set to Host. Specify the destination IP address in the destination IP Address field that appears.
Network: Destination IP is set to Network. Specify the destination IP address and destination IP mask in the

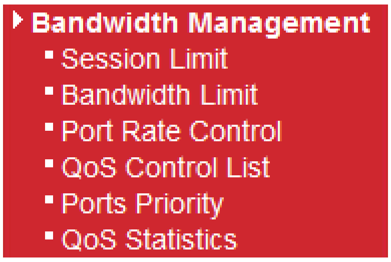
destination IP address and destination IP mask fields that appear.

Dest IP Address Type the Dest IP Address here. This option is available when you choose **Host** or **Network** as destination IP filter.

Dest IP Mask Type the Dest IP Mask here. This option is available only when you choose **Network** as destination IP filter.

4.5 Bandwidth Management

Below shows the menu items for Bandwidth Management.

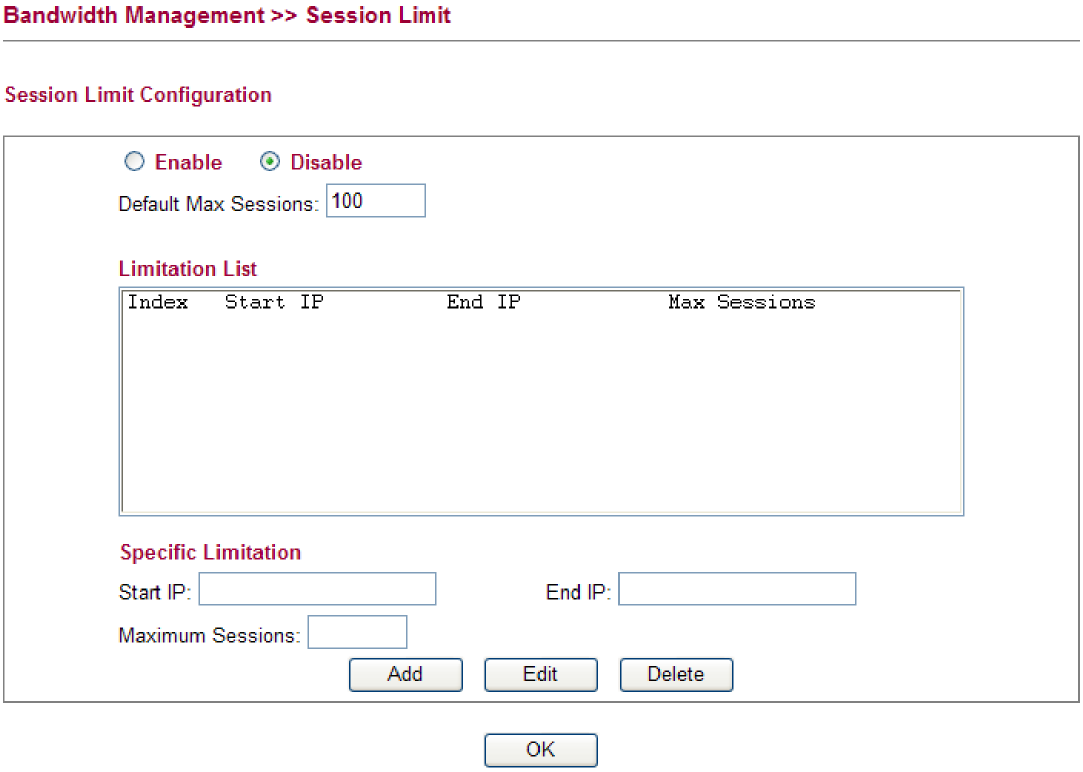


- Bandwidth Management
  - Session Limit
  - Bandwidth Limit
  - Port Rate Control
  - QoS Control List
  - Ports Priority
  - QoS Statistics

4.5.1 Session 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 >> Session Limit

Session Limit Configuration

○ Enable ● Disable

Default Max Sessions: 100

Limitation List

```
Index   Start IP          End IP            Max Sessions
```

Specific Limitation

Start IP: End IP:

Maximum Sessions:

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 Max Sessions Defines the default session number used for each computer in LAN.

Limitation List Displays a list of specific limitations that you set on this web page.

Start IP Defines the start LAN IP address for limit session.

End IP Defines the end LAN IP address for limit session.

Maximum Sessions Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.

Add Adds the specific session limitation onto the list above.

Edit Allows you to edit the settings for the selected limitation.

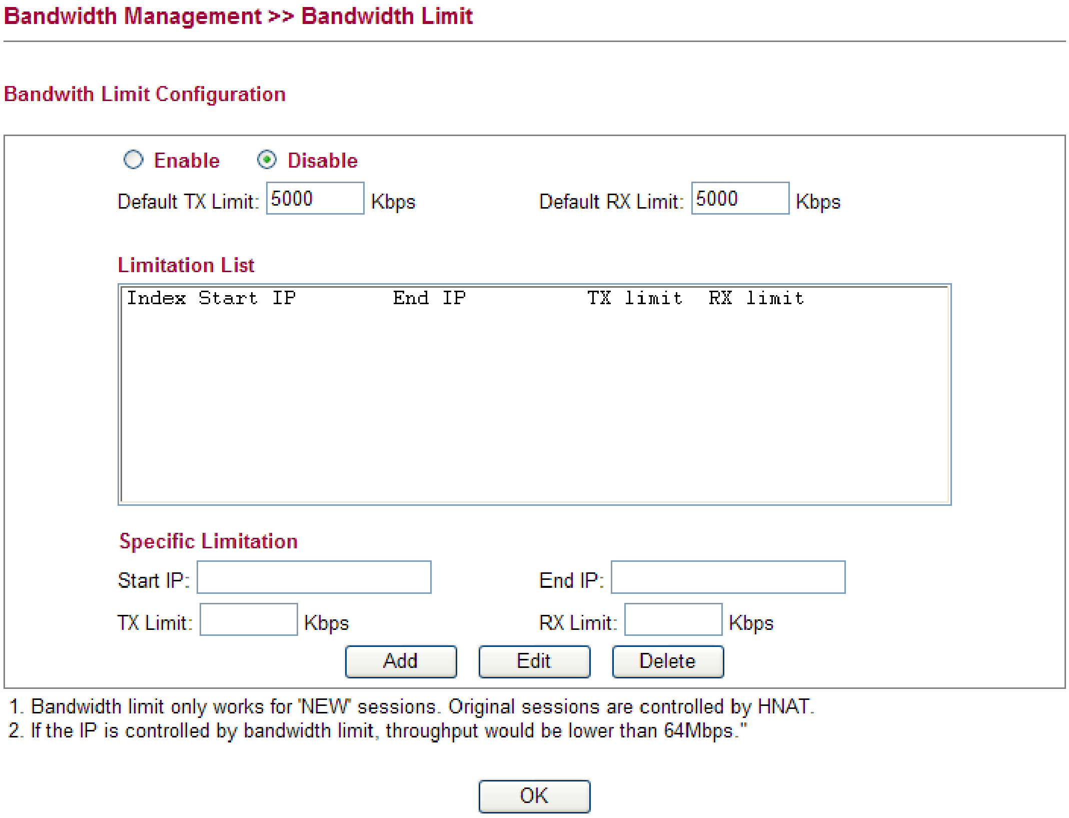
Delete Remove the selected settings existing on the limitation list.

When you finish adding a new session limit, simply click **OK**. The following page will appear for you to check.

4.5.2 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

Bandwith Limit Configuration

○ Enable ● Disable

Default TX Limit: 5000 Kbps Default RX Limit: 5000 Kbps

Limitation List

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

Specific Limitation

Start IP: End IP:

TX Limit: Kbps RX Limit: Kbps

1. Bandwidth limit only works for 'NEW' sessions. Original sessions are controlled by HNAT.
2. If the IP is controlled by bandwidth limit, throughput would be lower than 64Mbps."

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.

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 Bandwidth limit can be applied on certain IP range. That's, only the PCs within the range will be influenced by the bandwidth limitation set here. Please define the start IP address for the specific limitation.

End IP Define the end IP address for the specific limitation.

TX Limit Define the limitation for the speed of the upstream to be applied as specific limitation. 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 to be applied as specific limitation. 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.

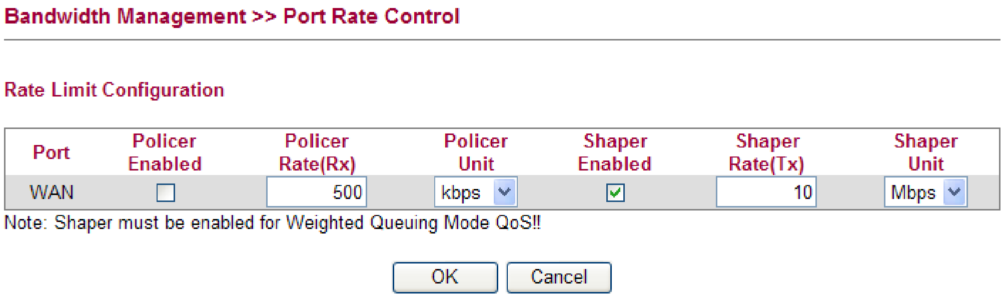
Edit Allows you to edit the settings for the selected limitation.

Delete Remove the selected settings existing on the limitation list.

When you finish adding a new bandwidth limit, simply click **OK**. The following page will appear for you to check.

4.5.3 Port Rate Control

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue. And a shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues. This page allows you to configure the switch port rate limit for Policers and Shapers.



Bandwidth Management >> Port Rate Control

Rate Limit Configuration

Port	Policer Enabled	Policer Rate(Rx)	Policer Unit	Shaper Enabled	Shaper Rate(Tx)	Shaper Unit
WAN	□	500	kbps	☑	10	Mbps

Note: Shaper must be enabled for Weighted Queuing Mode QoS!!

Port Represent LAN or WAN interface.

Policer Enabled Check this box to enable policer function.

Policer Rate(Rx) Type the number for policer function. The default value is 500. It is restricted to 500-1000000 when the Policer Unit is set in kbps, and it is restricted to 1-1000 when the Policer Unit is set in Mbps.

Policer Unit Determine the unit (kbps/Mbps) for policer.

Shaper Enabled Check this box to enable shaper function.

Shaper Rate (Tx) Type the number for shaper function. The default value is 500. It is restricted to 500-1000000 when the Shaper Unit is set in kbps, and it is restricted to 1-1000 when the Shaper Unit is set in Mbps.

Shaper Unit Determine the unit (kbps/Mbps) for shaper function.

4.5.4 QoS Control List

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?

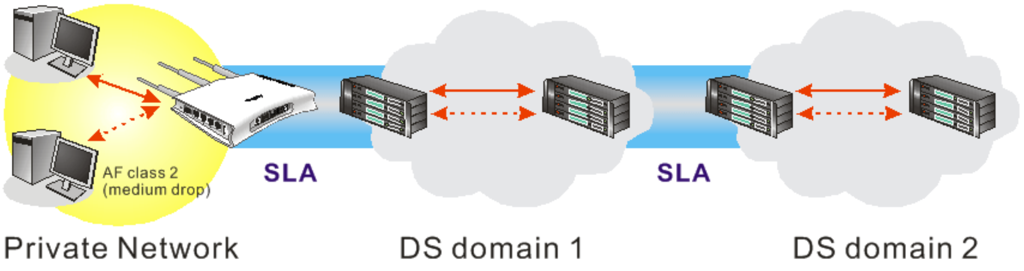
There are two components within Primary configuration of QoS deployment:

- 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.

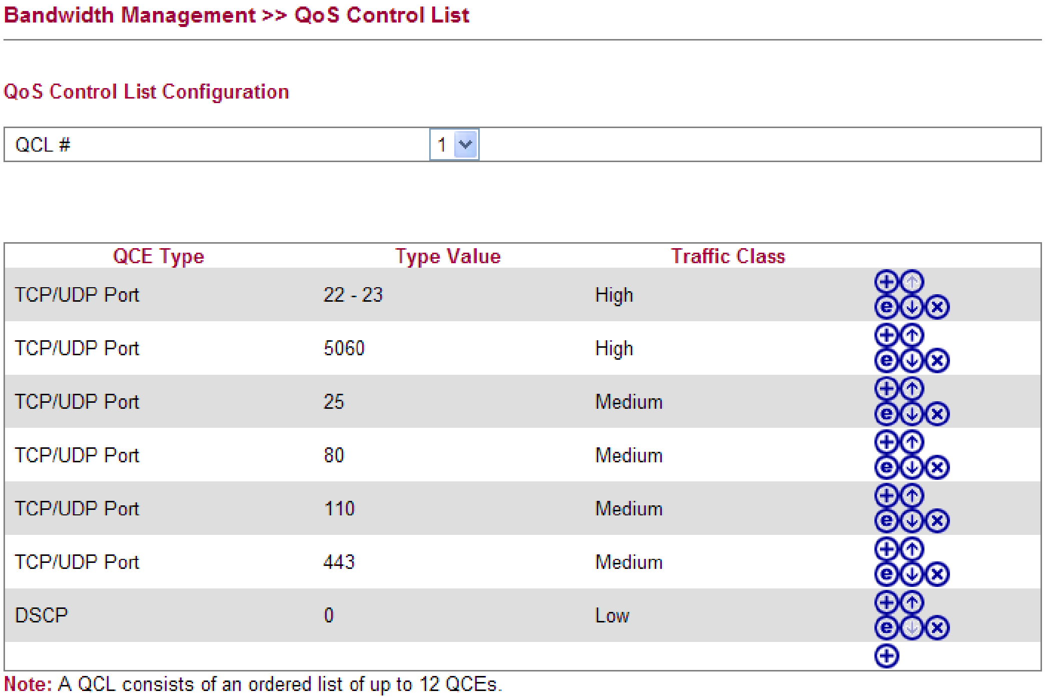
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes 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 **QoS Control List** to open the web page.



Bandwidth Management >> QoS Control List

QoS Control List Configuration

QCL #	1

QCE Type	Type Value	Traffic Class	
TCP/UDP Port	22 - 23	High	⊕ ⊕ ⊕ ⊕ ⊗
TCP/UDP Port	5060	High	⊕ ⊕ ⊕ ⊕ ⊗
TCP/UDP Port	25	Medium	⊕ ⊕ ⊕ ⊕ ⊗
TCP/UDP Port	80	Medium	⊕ ⊕ ⊕ ⊕ ⊗
TCP/UDP Port	110	Medium	⊕ ⊕ ⊕ ⊕ ⊗
TCP/UDP Port	443	Medium	⊕ ⊕ ⊕ ⊕ ⊗
DSCP	0	Low	⊕ ⊕ ⊕ ⊕ ⊗
			⊕

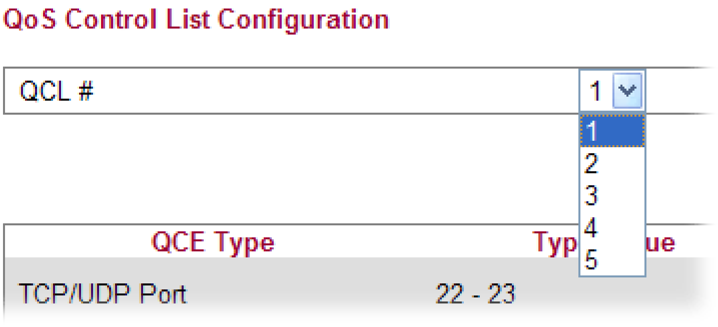
Note: A QCL consists of an ordered list of up to 12 QCEs.

QCE Type Display the type of that QCE (QoS Control Entries).

Type Value Display the value specified for the QCE.

Traffic Class Display the class of the data transmission for the QCE.

QoS Control List allows users to set up to **five** groups of QCL. Each QCL group can contain 12 QCE settings.



QoS Control List Configuration

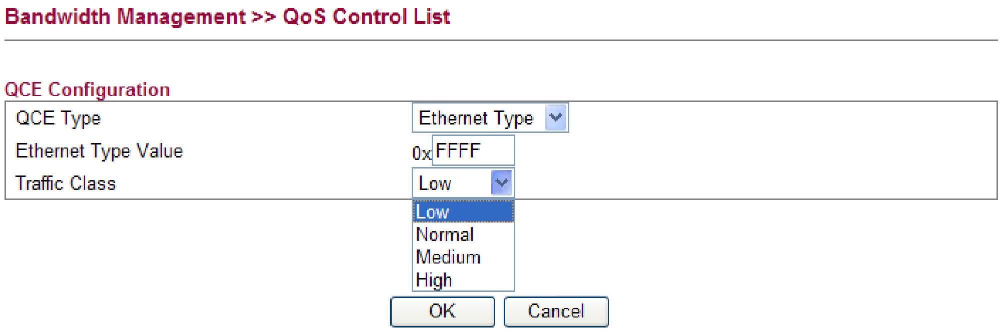
QCL #	1

QCE Type	Typ… …ue
TCP/UDP Port	22 - 23

Adding a New QCE

Click ⊕ to add a new QCE onto this page. Different QCE type will bring out different web settings.

- If you choose **Ethernet Type** as QCE Type, you have to type value for it and specify traffic class from Low, Normal, Medium and High.



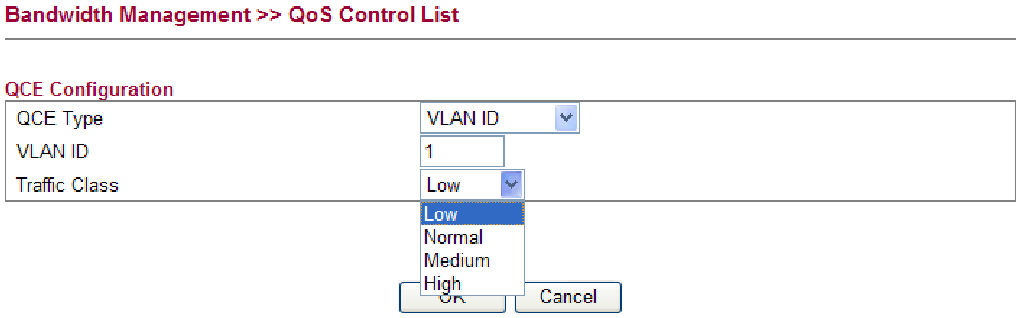
Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	Ethernet Type
Ethernet Type Value	0x FFFF
Traffic Class	Low

Ethernet Type Value Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

- If you choose **VLAN ID** as QCE Type, you have to type the ID number for it and specify traffic class from Low, Normal, Medium and High.

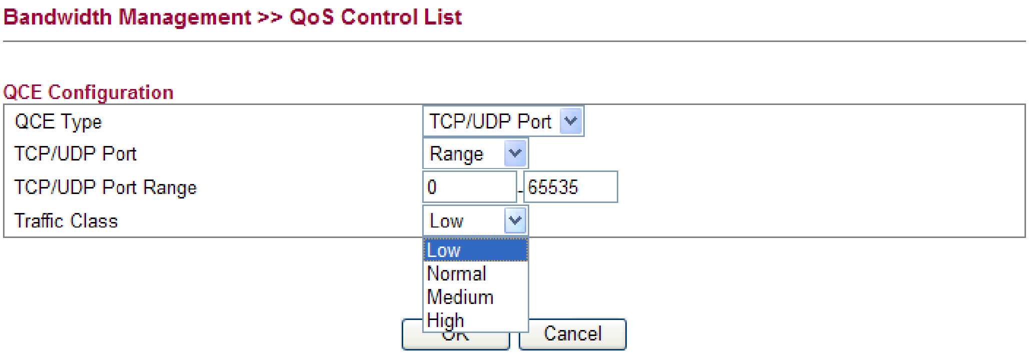


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	VLAN ID
VLAN ID	1
Traffic Class	Low

- If you choose **TCP/UDP Port** as QCE Type, you have to type the port number for it and specify traffic class from Low, Normal, Medium and High.



Bandwidth Management >> QoS Control List

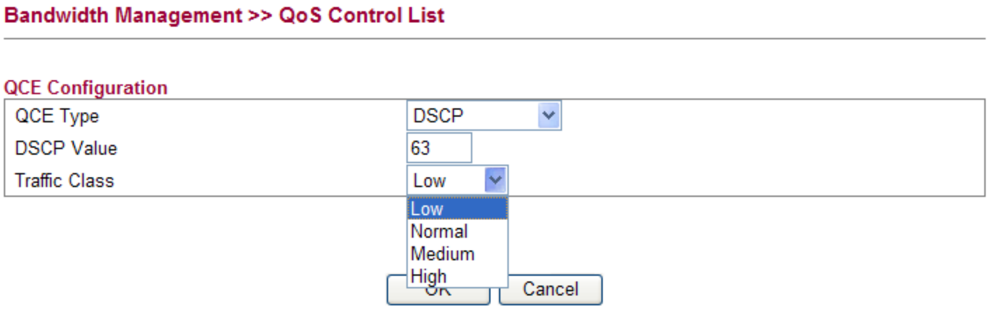
QCE Configuration

QCE Type	TCP/UDP Port
TCP/UDP Port	Range
TCP/UDP Port Range	0 - 65535
Traffic Class	Low

TCP/UDP Port Click **Single** or **Range**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.

TCP/UDP Port Range Type in the starting port number and the end porting number here if you choose Range as the type.

- If you choose **DSCP** as QCE Type, you have to type value for it and specify traffic class from Low, Normal, Medium and High.

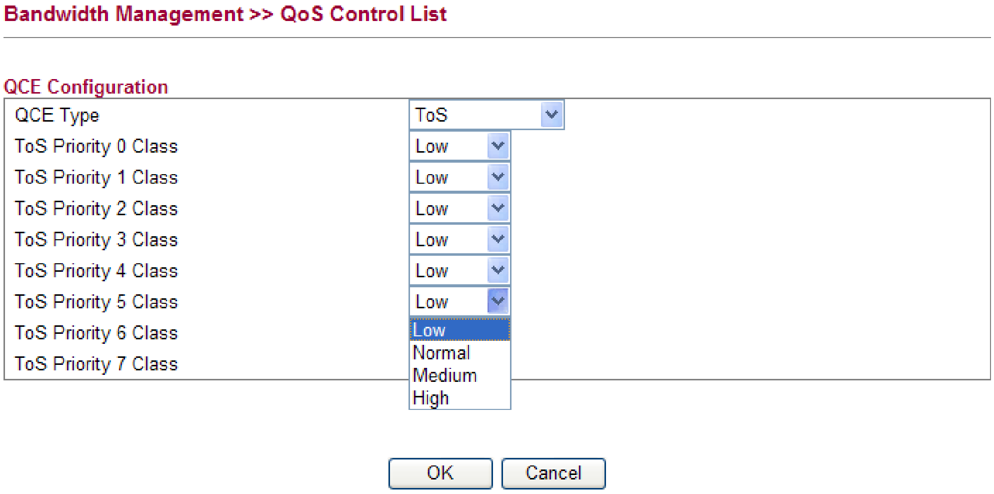


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	DSCP
DSCP Value	63
Traffic Class	Low

- If you choose **ToS** as QCE Type, you have to specify priority class from Low, Normal, Medium and High.

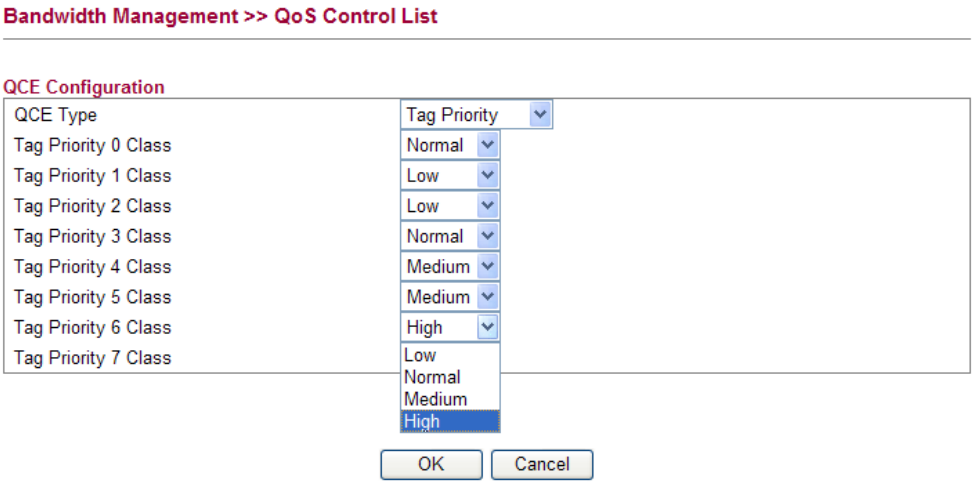


Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	ToS
ToS Priority 0 Class	Low
ToS Priority 1 Class	Low
ToS Priority 2 Class	Low
ToS Priority 3 Class	Low
ToS Priority 4 Class	Low
ToS Priority 5 Class	Low
ToS Priority 6 Class	
ToS Priority 7 Class	

- If you choose **Tag Priority** as QCE Type, you have to specify priority class from Low, Normal, Medium and High.



Bandwidth Management >> QoS Control List

QCE Configuration

QCE Type	Tag Priority
Tag Priority 0 Class	Normal
Tag Priority 1 Class	Low
Tag Priority 2 Class	Low
Tag Priority 3 Class	Normal
Tag Priority 4 Class	Medium
Tag Priority 5 Class	Medium
Tag Priority 6 Class	High
Tag Priority 7 Class	

Editing a QCE

Click ⓔ to modify the settings of an existing QCE on this page.

Moving Up/Down a QCE

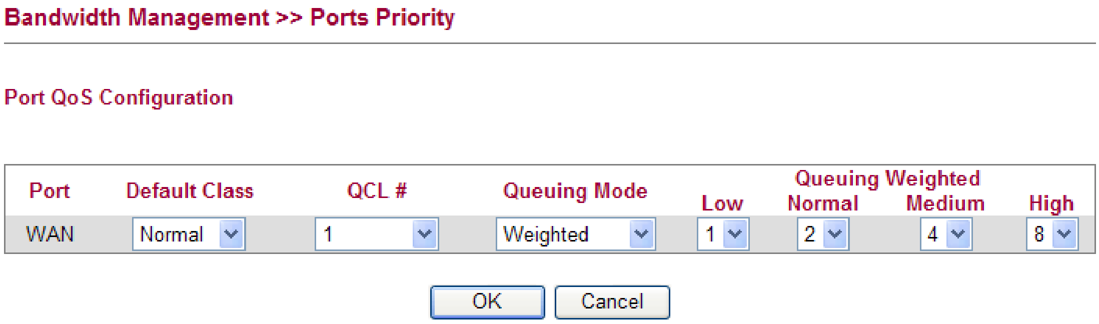
Click ⬇ and ⬆ to move a QCE up and down.

Deleting a QCE

To delete a QCE in the list, simply click ⊗ of that one. It will be removed immediately.

4.5.5 Ports Priority

This page allows you to configure QoS settings for each port. The classification is controlled by a QCL (Quality Control List) that is assigned to each port. A QCL consists of an ordered list of up to 12 QCEs (Quality Control Entry). Each QCE can be used to classify certain frames to a specific QoS class. This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS class for the port.



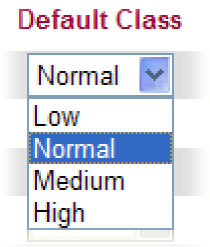
Bandwidth Management >> Ports Priority

Port QoS Configuration

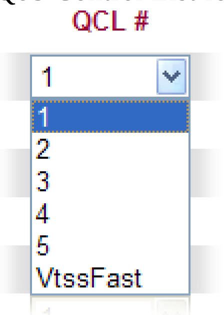
Port	Default Class	QCL #	Queuing Mode	Queuing Weighted Low	 Normal	 Medium	 High
WAN	Normal	1	Weighted	1	2	4	8

Port Indicate the interface for the physical port, WAN port, LAN port and Wireless Port.

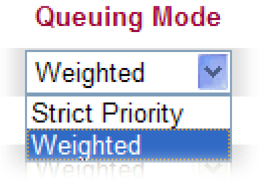
Default Class Use the drop down list to choose the priority for each port.



QCL Use the drop down list to choose the QCL number defined in QoS Control List for the port.



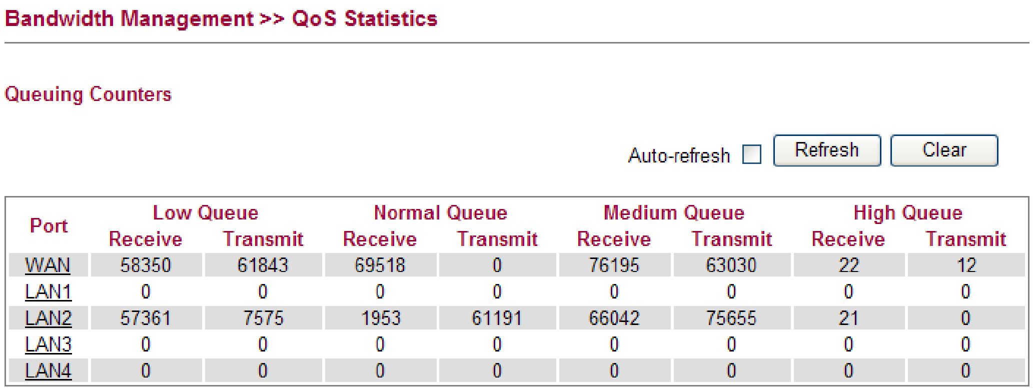
Queuing Mode Use the drop down list to choose suitable mode.



Queue Weighted Use the drop down list to choose 1, 2, 4, or 8 as the queue weighted number.

4.5.6 QoS Statistics

This page displays statistics for QoS setting. Click WAN/LAN link to check detailed information for each interface.



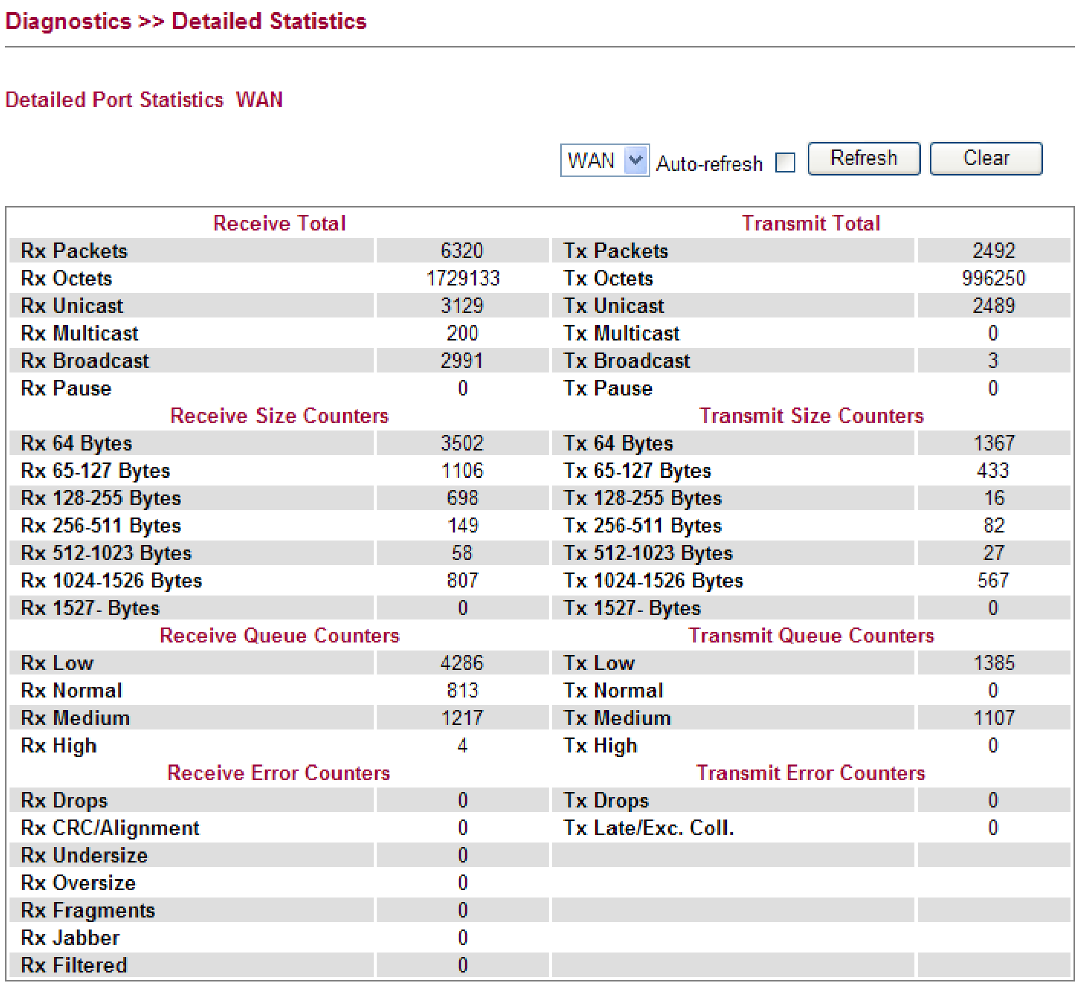
Bandwidth Management >> QoS Statistics

Queuing Counters

Auto-refresh □ Refresh Clear

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
WAN	58350	61843	69518	0	76195	63030	22	12
LAN1	0	0	0	0	0	0	0	0
LAN2	57361	7575	1953	61191	66042	75655	21	0
LAN3	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0

Click **WAN/LAN** link to check detailed information for each interface.



Diagnostics >> Detailed Statistics

Detailed Port Statistics WAN

Receive Total		Transmit Total	
Rx Packets	6320	Tx Packets	2492
Rx Octets	1729133	Tx Octets	996250
Rx Unicast	3129	Tx Unicast	2489
Rx Multicast	200	Tx Multicast	0
Rx Broadcast	2991	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	3502	Tx 64 Bytes	1367
Rx 65-127 Bytes	1106	Tx 65-127 Bytes	433
Rx 128-255 Bytes	698	Tx 128-255 Bytes	16
Rx 256-511 Bytes	149	Tx 256-511 Bytes	82
Rx 512-1023 Bytes	58	Tx 512-1023 Bytes	27
Rx 1024-1526 Bytes	807	Tx 1024-1526 Bytes	567
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Low	4286	Tx Low	1385
Rx Normal	813	Tx Normal	0
Rx Medium	1217	Tx Medium	1107
Rx High	4	Tx High	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Rx Packets Display the counting number of the packet received.

Rx Octets Display the total received bytes.

Rx Unicast Display the counting number of the received unicast packet.

Rx Broadcast Display the counting number of the received broadcast packet.

Rx Pause Display the counting number of the received pause packet.

RX 64 Bytes Display the number of 64-byte frames in good and bad packets received.

RX 65-127 Bytes Display the number of 65 ~ 127-byte frames in good and bad packets received.

RX 128-255 Bytes Display the number of 128 ~ 255-byte frames in good and bad packets received.

RX 256-511 Bytes Display the number of 256 ~ 511-byte frames in good and bad packets received.

RX 512-1023 Bytes Display the number of 512 ~ 1023-byte frames in good and bad packets received.

RX 1024- 1526 Bytes Display the number of 1024-1522-byte frames in good and bad packets received.

RX 1527 Bytes Display the number of 1527-byte frames in good and bad packets received.

Rx Low Display the low queue counter of the packet received.

Rx Normal Display the normal queue counter of the packet received.

Rx Medium Display the medium queue counter of the packet received.

Rx High Display the high queue counter of the packet received.

Rx Drops Display the number of frames dropped due to the lack of receiving buffer.

Rx CRC/Alignment Display the number of Alignment errors packets received.

Rx Undersize Display the number of short frames (<64 Bytes) with valid CRC.

Rx Oversize Display the number of long frames (according to max_length register) with valid CRC.

Rx Fragments Display the number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber Display the number of long frames (according to max_length register) with invalid CRC.

Rx Filtered Display the filtered number of the packet received.

Tx Packets Display the the counting number of the packet transmitted.

Tx Octets Display the total transmitted bytes.

Tx Unicast Display the show the counting number of the transmitted unicast packet.

Tx Multicast Display the show the counting number of the transmitted multicast packet.

Tx Broadcast Display the counting number of the transmitted broadcast packet.

Tx Pause Show the counting number of the transmitted pause packet.

Tx 64 Bytes Display the number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes Display the number of 65 ~ 127-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes Display the number of 128 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes Display the number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes Display the number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024- 1526 Bytes Display the number of 1024 ~ 1522-byt frames in good and bad packets transmitted.

Tx 1527 Bytes: Display the number of 1527-byte frames in good and bad packets transmitted.

Tx Low Display the low queue counter of the packet transmitted.

Tx Normal Display the normal queue counter of the packet transmitted.

Tx Medium Display the medium queue counter of the packet received.

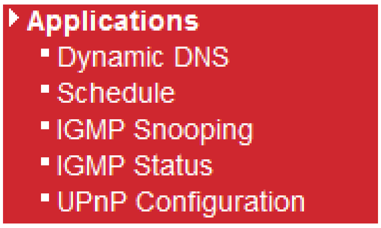
Tx High Display the high queue counter of the packet received.

Tx Drops Display the number of frames dropped due to excessive collision, late collision, or frame aging.

Tx lat/Exc.Coll. Display the number of Frames late collision or excessive collision Error, which switch transmitted.

4.6 Applications

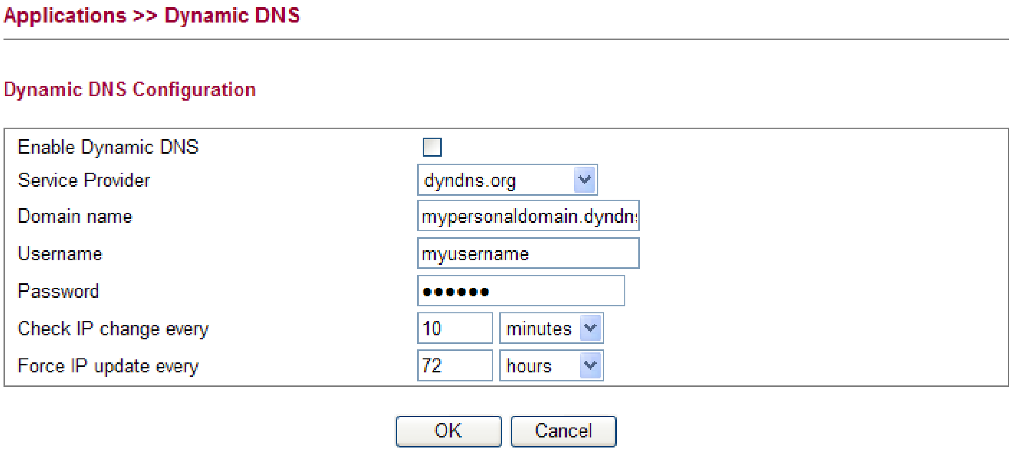
Below shows the menu items for Applications.



4.6.1 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.



Applications >> Dynamic DNS

Dynamic DNS Configuration

Enable Dynamic DNS	□	
Service Provider	dyndns.org	
Domain name	mypersonaldomain.dyndn:	
Username	myusername	
Password	••••••	
Check IP change every	10	minutes
Force IP update every	72	hours

Enable Dynamic DNS Check this box to enable the current account.

DynDNS Service Select the service provider for the DDNS account.

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

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

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

Check IP change every Set the interval for checking the information.

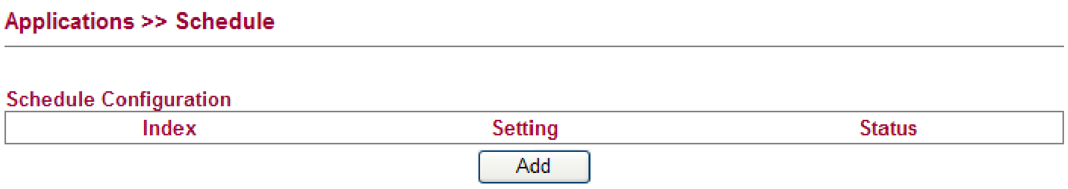
Force IP update every Force the router updates its information to DDNS server with the interval set here.

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

4.6.2 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.

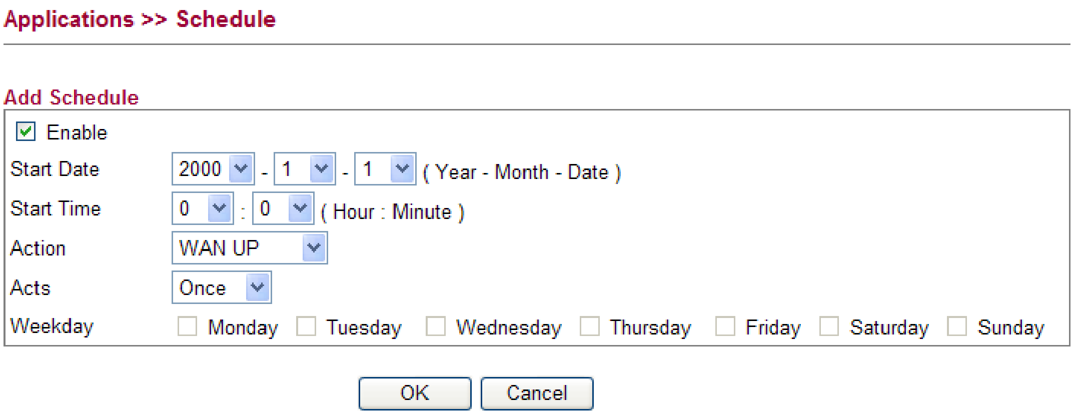


Applications >> Schedule

Schedule Configuration

Index	Setting	Status

You can set up to **15** schedules. To add a schedule profile, please click **Add**.



Applications >> Schedule

Add Schedule

☑ Enable

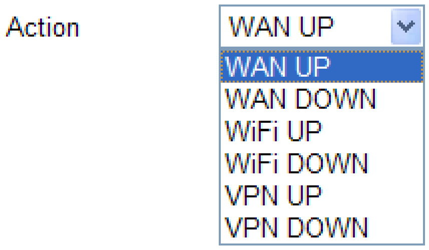
Start Date	2000 - 1 - 1 (Year - Month - Date)
Start Time	0 : 0 (Hour : Minute)
Action	WAN UP
Acts	Once
Weekday	□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Enable Check to enable the schedule.

Start Date Specify the starting date of the schedule.

Start Time Specify the starting time of the schedule.

Action Specify which action should be applied during the period of the schedule.



Action: WAN UP

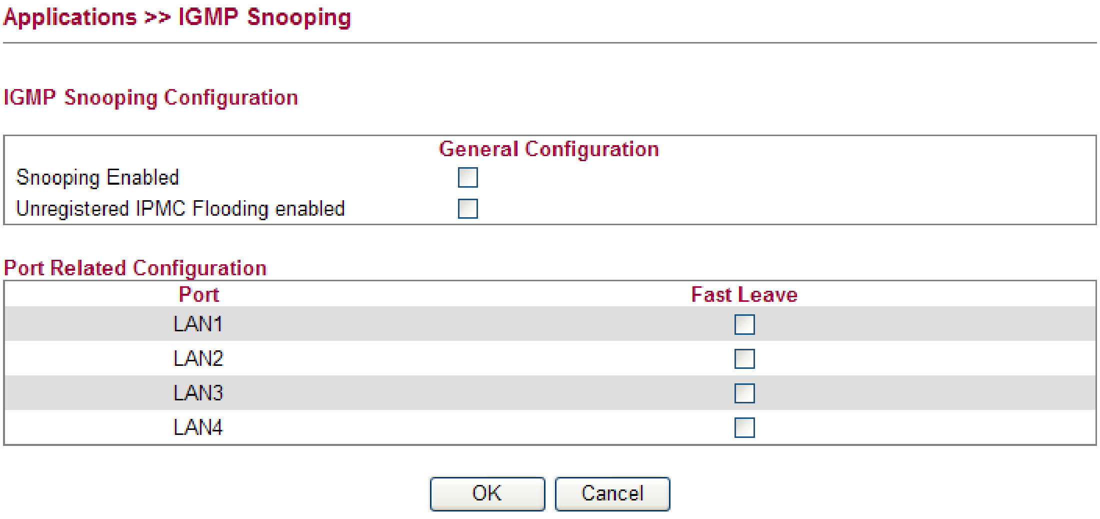
- WAN UP
- WAN DOWN
- WiFi UP
- WiFi DOWN
- VPN UP
- VPN DOWN

WAN UP/DOWN – WAN connection will be activated / inactivated based on the time schedule configured here.
WiFi UP/DOWN – Wireless Wi-Fi connection will be activated / inactivated based on the time schedule configured here.
VPN UP/DOWN - VPN connection will be activated / inactivated based on the time schedule configured here.

Acts Specify how often the schedule will be applied
Once -The schedule will be applied just once
Routine /**Weekday** -Specify which days in one week should perform the schedule.

4.6.3 IGMP Snooping

IGMP snooping means multicast traffic will be forwarded to ports that have members of that group. If you disable IGMP snooping, the system will make multicast traffic treated in the same manner as broadcast traffic.



Applications >> IGMP Snooping

IGMP Snooping Configuration

General Configuration	
Snooping Enabled	□
Unregistered IPMC Flooding enabled	□

Port Related Configuration

Port	Fast Leave
LAN1	□
LAN2	□
LAN3	□
LAN4	□

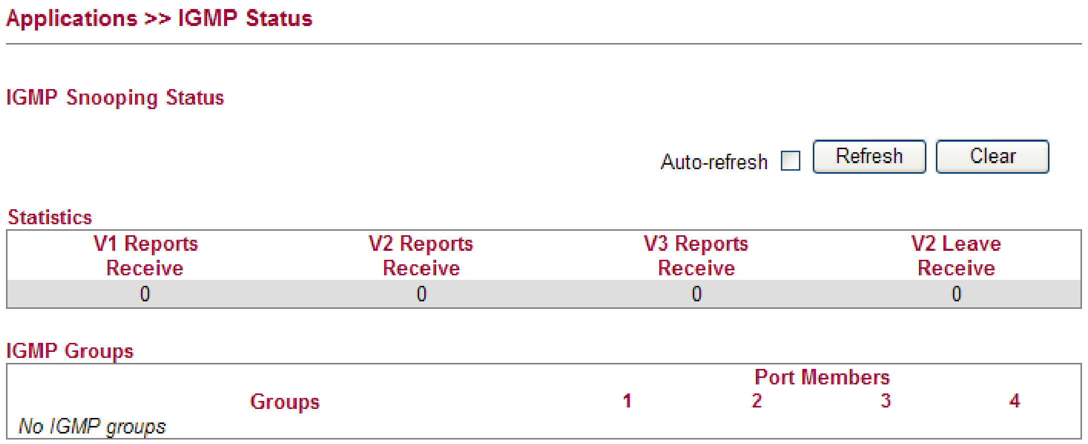
Snooping Enabled Check the box to enable this function.

Unregistered IPMC… Check the box to enable unregistered IPMC traffic flooding

Fast Leave Check the box to Fast Leave on the LAN port.

4.6.4 IGMP Status

This page display current IGMP status.



Applications >> IGMP Status

IGMP Snooping Status

Auto-refresh □ Refresh Clear

Statistics

V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
0	0	0	0

IGMP Groups

Groups	Port Members 1	2	3	4
No IGMP groups				

V1~3 Reports Receive Display the number of Received V1 – V3 Reports.

V2 Leave Receive Display the number of Received V2 Leave.

Groups Display current IGMP groups. Maximum number of group for each VLAN can be set is 128.

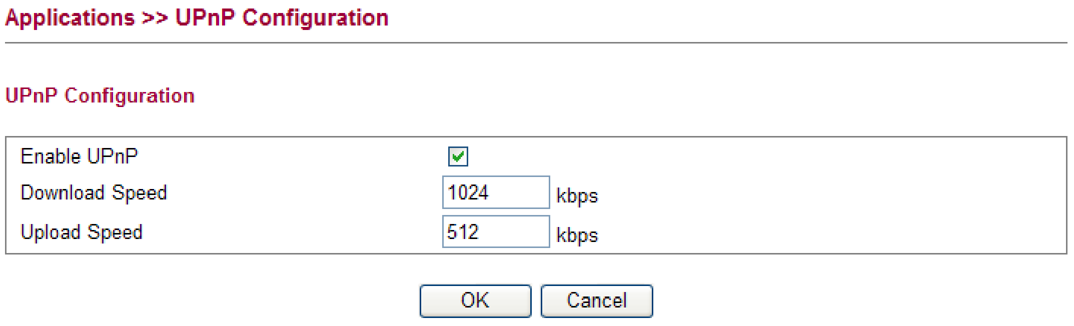
Port Members Display the LAN ports in this group.

Refresh Click this button to refresh the page immediately.

Clear Click this button to clear the settings on this page.

4.6.5 UPnP Configuration

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 Configuration

UPnP Configuration

Enable UPnP	☑
Download Speed	1024 kbps
Upload Speed	512 kbps

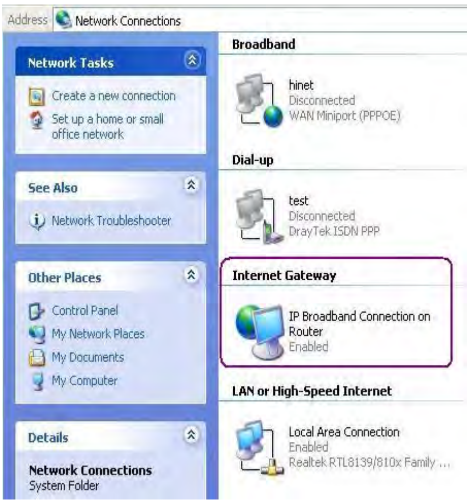
OK Cancel

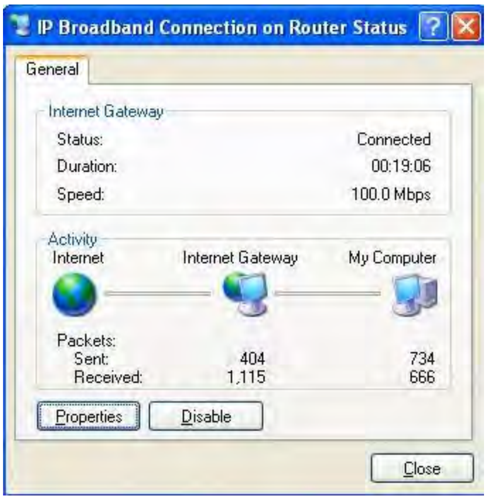
Enable UPnP Enable UPnP function. You have to type the download and upload speed.

Download Speed Enter the maximum sustained WAN download speed in kilobits/second. Such information can be requested by UPnP clients.

Upload Speed Enter the maximum sustained WAN upload speed in kilobits/second. Such information can be requested by UPnP clients.

After setting **Enable UPnP** 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.



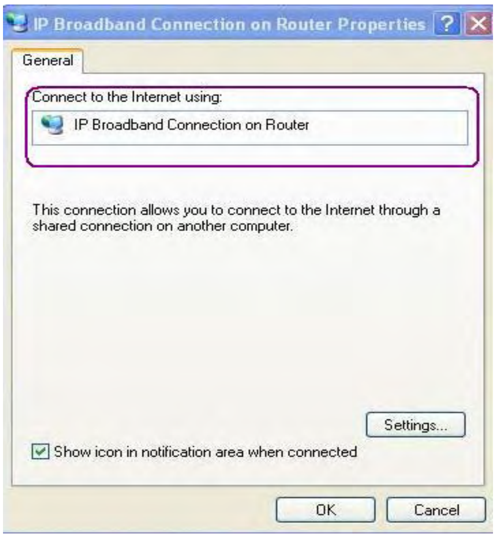


Status: Connected
Duration: 00:19:06
Speed: 100.0 Mbps

Packets:

	Internet Gateway	My Computer
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.

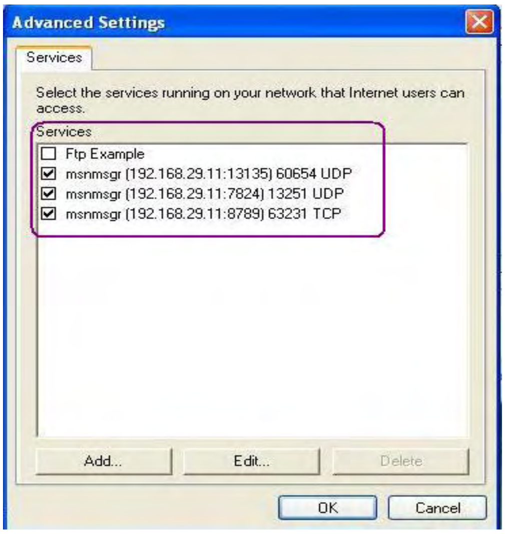


Connect to the Internet using:

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.

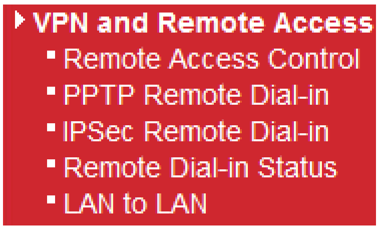
- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

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.

4.7 VPN and Remote Access

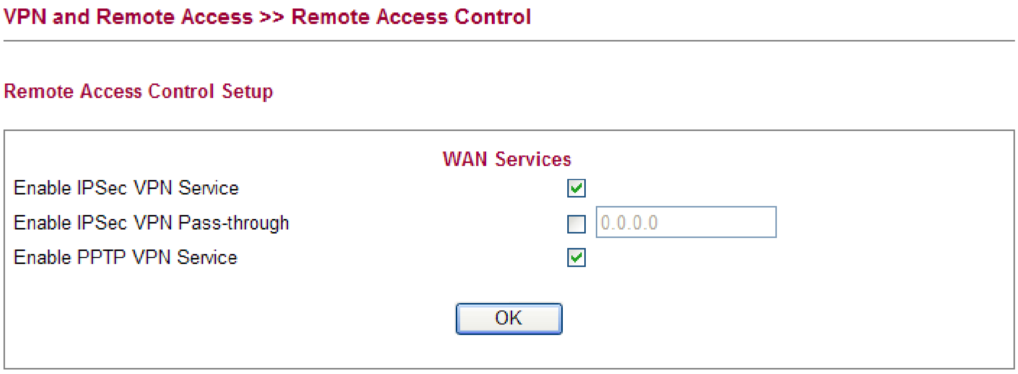
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



4.7.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should enable IPSec VPN Pass-through and specify an IP address to allow VPN tunnel pass through.



VPN and Remote Access >> Remote Access Control

Remote Access Control Setup

	WAN Services
Enable IPSec VPN Service	☑
Enable IPSec VPN Pass-through	□ 0.0.0.0
Enable PPTP VPN Service	☑

Enable IPSec VPN Service If this checkbox is checked, the system firewall will allow VPN (IPSec) remote access from WAN side to the router.

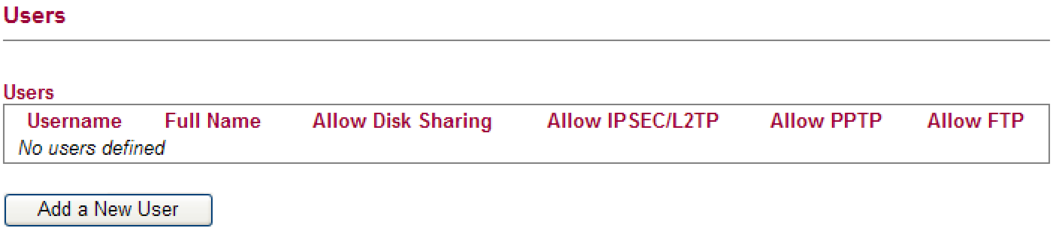
Enable IPSec VPN Pass-through If this checkbox is checked, the system f firewall will allow VPN (IPSec) remote access from WAN side to a VPN device on the LAN. Type the IP address of the VPN device in the field next to the checkbox.

Enable PPTP VPN Service If this checkbox is checked, the system firewall will allow VPN (PPTP) remote access from WAN side to the router.

4.7.2 PPTP Remote Dial-in

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.

The router provides access accounts for dial-in users.



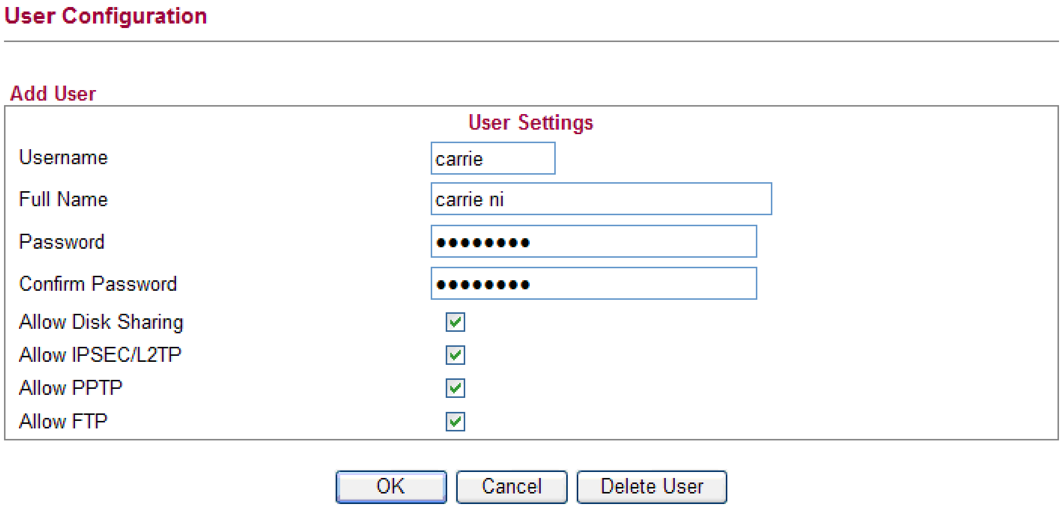
Users

Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
No users defined					

Adding a New User

Click **Add new user** to open the following page.



User Configuration

Add User

User Settings	
Username	carrie
Full Name	carrie ni
Password	••••••••
Confirm Password	••••••••
Allow Disk Sharing	☑
Allow IPSEC/L2TP	☑
Allow PPTP	☑
Allow FTP	☑

Username Type a name for this user.

Full Name Type full name for this user.

Password Type the password for this user.

Password (again) Type the password again for confirmation.

Allow Disk Sharing Check this box to have the remote user share the disk information.

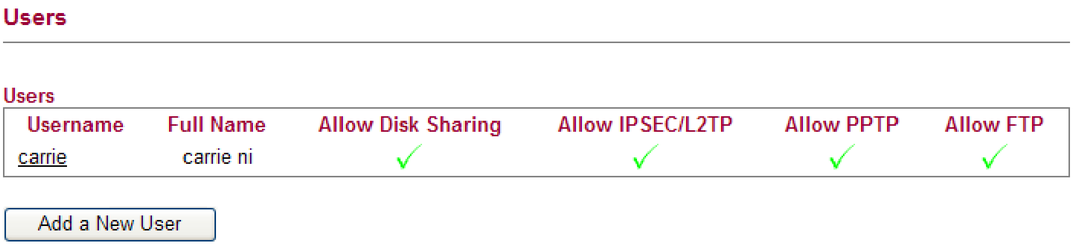
Allow IPSEC/L2TP Check this box to let the remote user connecting to this device through IPSEC/L2TP**.**

Allow PPTP Check this box to let the remote user connecting to this device through PPTP**.**

Allow FTP Check this box to let the remote user connecting to FTP server via this router.

Delete User Remove settings on current page and delete the user. This button is not available for new configuration by pressing **Add a New User**.

When you finish the settings, simply click **OK** to save the configuration. The new user will be created and displayed on the page.



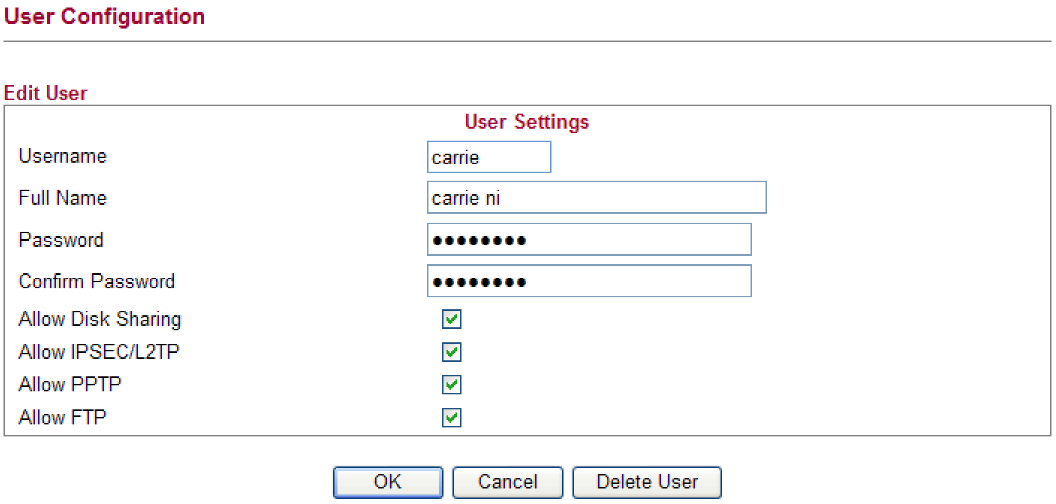
Users

Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
carrie	carrie ni	✓	✓	✓	✓

Editing/Deleting User Settings

To edit a user, click the name link under Username to open the following page. Modify the settings except Username and then click **OK** to save and exit it. If you want to remove such user settings, simply click **Delete User**.



User Configuration

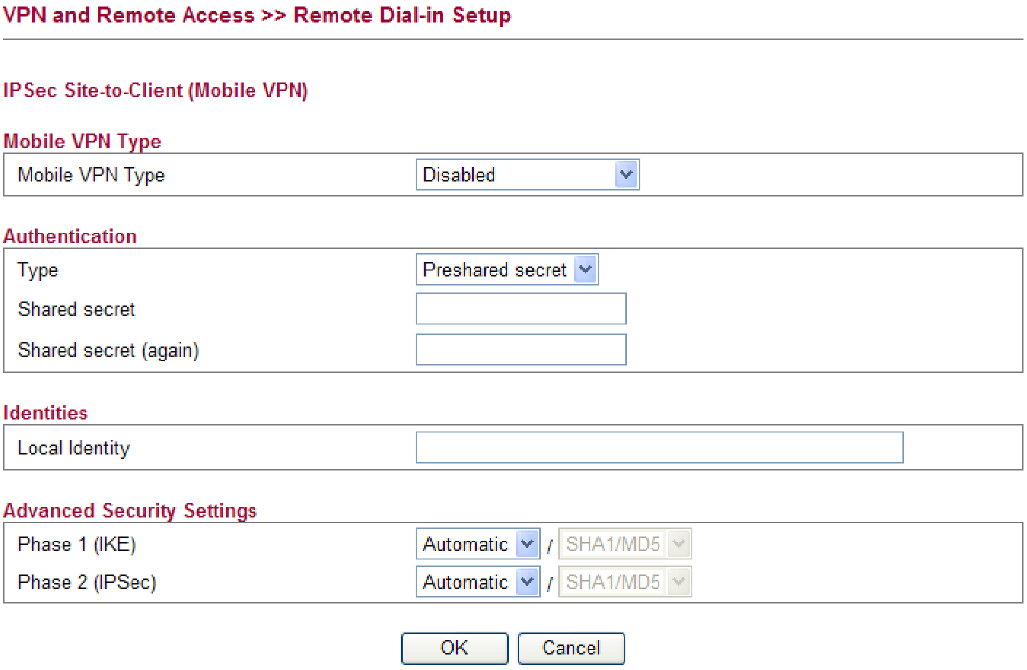
Edit User

User Settings

Username	carrie
Full Name	carrie ni
Password	••••••••
Confirm Password	••••••••
Allow Disk Sharing	☑
Allow IPSEC/L2TP	☑
Allow PPTP	☑
Allow FTP	☑

4.7.3 IPSec Remote Dial-in

This page allows you to configure IPSec Site-to-Client settings.



VPN and Remote Access >> Remote Dial-in Setup

IPSec Site-to-Client (Mobile VPN)

Mobile VPN Type

Mobile VPN Type	Disabled

Authentication

Type	Preshared secret
Shared secret	
Shared secret (again)	

Identities

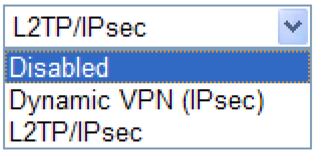
Local Identity	

Advanced Security Settings

Phase 1 (IKE)	Automatic / SHA1/MD5
Phase 2 (IPSec)	Automatic / SHA1/MD5

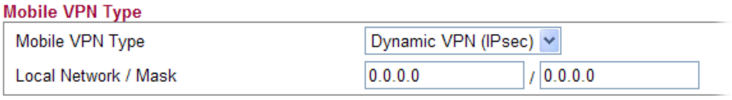
Mobile VPN Type

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.



Disabled – Ignore the configurations set in this page.

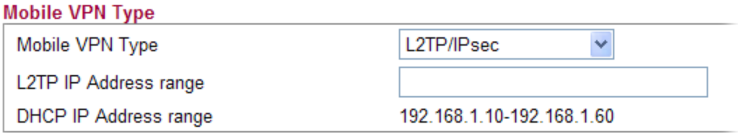
Dynamic VPN (IPSec) – Traffic between this subnet and the client will travel through the VPN tunnel. If you choose this type, please specify the IP address and subnet mask for local network.



Mobile VPN Type

Mobile VPN Type	Dynamic VPN (IPsec)
Local Network / Mask	0.0.0.0 / 0.0.0.0

L2TP/IPSec –The range must not overlap the DHCP address range (if enabled), and must allow for at least one IP address. Example: *10.10.137.240-10.10.137.245*. If you choose this type, please specify the IP address range for L2TP/IPSec mode.

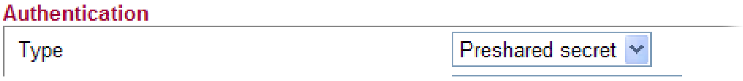


Mobile VPN Type

Mobile VPN Type	L2TP/IPsec
L2TP IP Address range	
DHCP IP Address range	192.168.1.10-192.168.1.60

Authentication

Type - Determine the authentication method for remote dial-in user.



Authentication

Type: Preshared secret

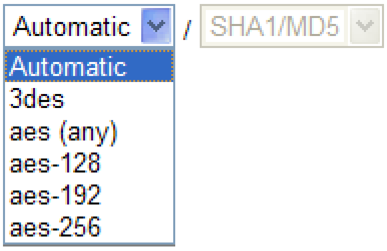
Preshared secret **–** If you choose this one, you have to type the shared secret manually and specify local identity. When using Preshared secret, *all* clients share the same secret.

Identities

Local Identity - 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. It can also be a DNS name or an email address.

Advanced Settings

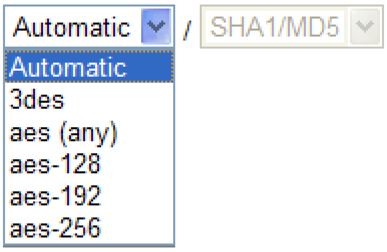
Phase 1 (IKE) - Negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its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



Automatic / SHA1/MD5

Automatic
3des
aes (any)
aes-128
aes-192
aes-256

Phase 2 (IPSec) - 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.

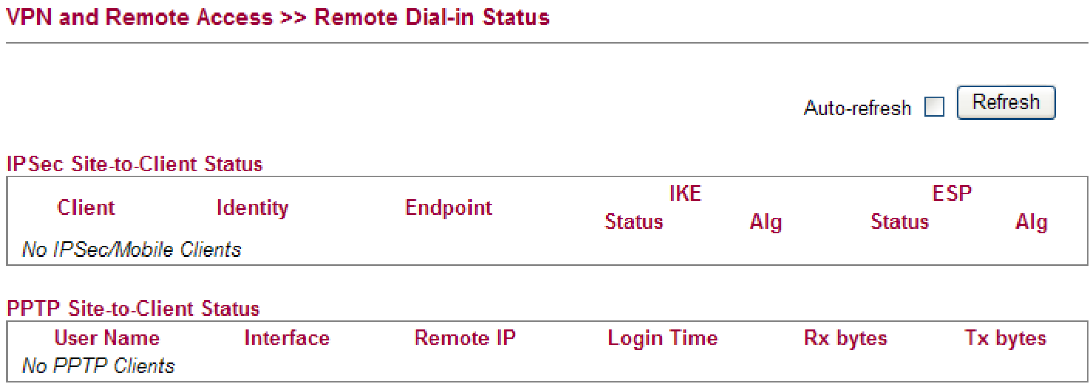


Automatic / SHA1/MD5

Automatic
3des
aes (any)
aes-128
aes-192
aes-256

4.7.4 Remote Dial-in Status

You can find the summary table of all dial-in user status.



VPN and Remote Access >> Remote Dial-in Status

Auto-refresh □ Refresh

IPSec Site-to-Client Status

Client	Identity	Endpoint	IKE		ESP	
			Status	Alg	Status	Alg
No IPSec/Mobile Clients						

PPTP Site-to-Client Status

User Name	Interface	Remote IP	Login Time	Rx bytes	Tx bytes
No PPTP Clients					

Client Display the name of the VPN IPSec/Mobile client.

Identity Display the remote ID of the VPN client.

Endpoint Display the IP address of the VPN client.

IKE Status Display the status of the phase 1 ISAKMP key exchange.

IKE Alg Display the encryption and authentication algorithm used during phase 1 of the VPN connection Establishment. The algorithm is used during exchange of key exchange.

ESP Status Display the status of the phase 2 IPSec ESP key exchange.

ESP Alg Display the encryption and authentication algorithm used during phase 2 of the VPN connection Establishment. This algorithm is used for transporting data, and the choice will affect the performance of the VPN tunnel.

User Name Display the dial-in user account.

Interface Display the connection name assigned by the router.

Remote IP Display IP address of remote client.

Login Time Display the system time that the user logs in.

Rx bytes Display the data total received for such client.

Tx bytes Display the data total transmitted for such client.

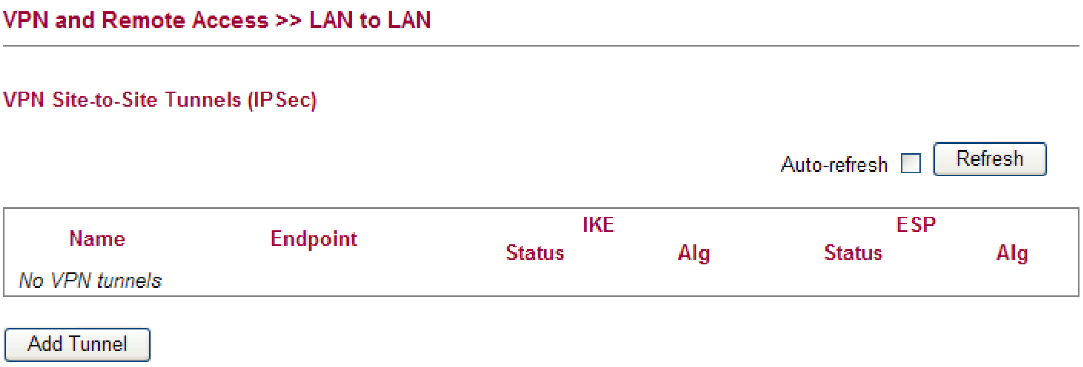
Auto-refresh Check this box to make the system refresh this page automatically.

Refresh Click this button to refresh the page immediately.

4.7.5 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 corresponding security methods, etc.

The router supports 2 VPN tunnels simultaneously and provides up to **2** profiles. The following figure shows the summary table.


VPN and Remote Access >> LAN to LAN

VPN Site-to-Site Tunnels (IPSec)

Auto-refresh □ Refresh

Name	Endpoint	IKE		ESP	
		Status	Alg	Status	Alg
No VPN tunnels					

Name Indicate the name of the LAN-to-LAN profile.

Endpoint Display the IP address of the VPN client.

IKE Status Display the status of the phase 1 ISAKMP key exchange.

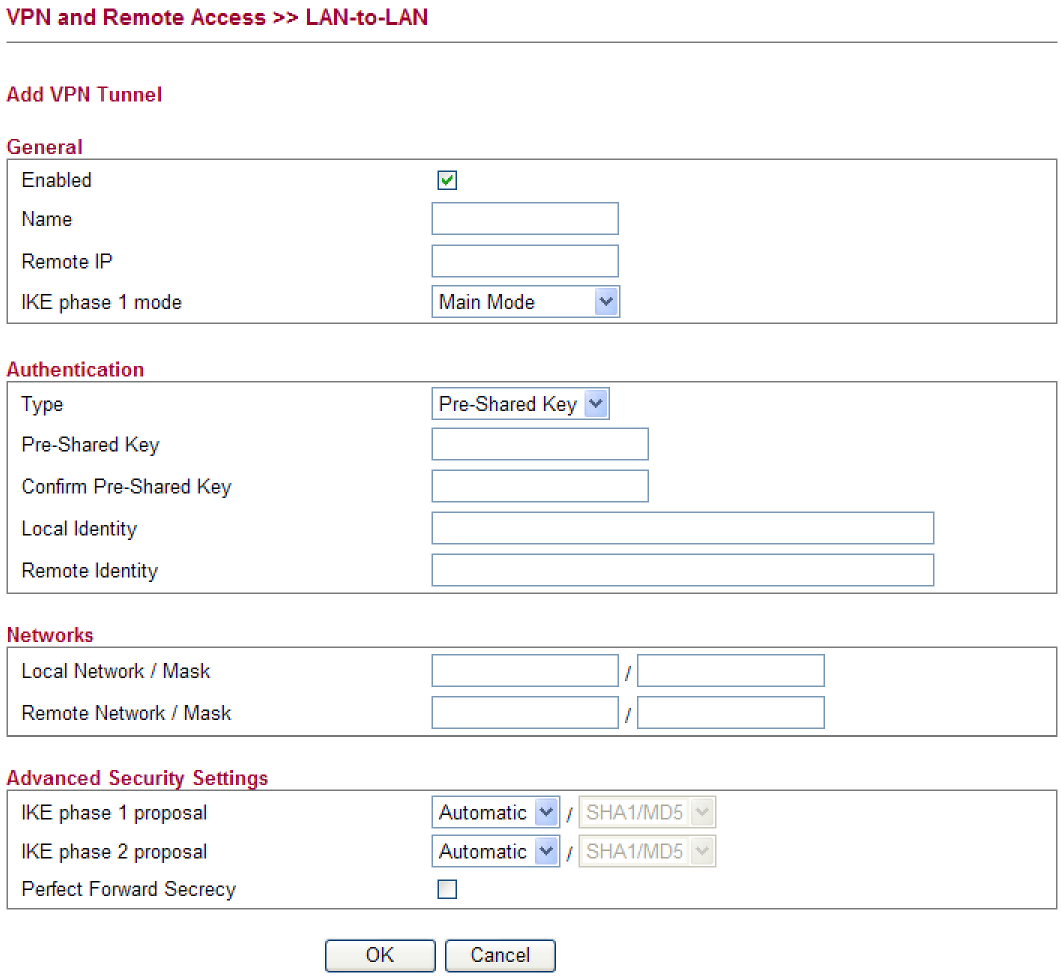
IKE Alg Display the encryption and authentication algorithm used during phase 1 of the VPN connection Establishment. The algorithm is used during exchange of key exchange.

ESP Status Display the status of the phase 2 IPSec ESP key exchange.

ESP Alg Display the encryption and authentication algorithm used during phase 2 of the VPN connection Establishment. This algorithm is used for transporting data, and the choice will affect the performance of the VPN tunnel.

Adding a VPN Tunnel

Click **Add Tunnel** to open the following page.



VPN and Remote Access >> LAN-to-LAN

Add VPN Tunnel

General

Enabled	☑
Name	
Remote IP	
IKE phase 1 mode	Main Mode

Authentication

Type	Pre-Shared Key
Pre-Shared Key	
Confirm Pre-Shared Key	
Local Identity	
Remote Identity	

Networks

Local Network / Mask	/
Remote Network / Mask	/

Advanced Security Settings

IKE phase 1 proposal	Automatic / SHA1/MD5
IKE phase 2 proposal	Automatic / SHA1/MD5
Perfect Forward Secrecy	□

Enabled Check here to activate this tunnel.

Name Specify a name for this tunnel.

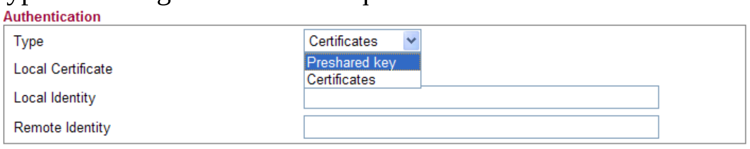
Remote IP Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

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 mode: Main Mode

Main Mode
Aggressive Mode

Type This group of fields is applicable for IPSec Tunnels. Different type will bring out different requirement of information.



Authentication

Type	Certificates
Local Certificate	
Local Identity	
Remote Identity	

Pre-Shared Key Such field will be applicable when Pre-shared key is selected as the Type for the authentication. Input 1-63 characters as pre-shared key.

Confirm Pre-Shared key Such field will be applicable when Pre-shared key is selected as the Type for the authentication. Input 1-63 characters as pre-shared key again to confirm it.

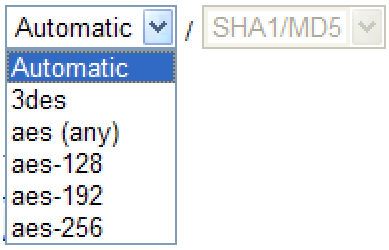
Local Identity Local Identity is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Remote Identity This field defines the identity of the remote end.

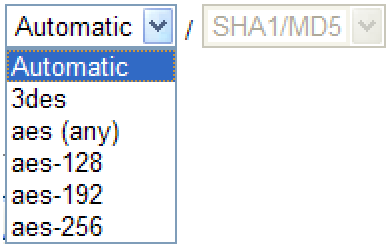
Local Network / Mask Traffic between this subnet and the subnet specified in Remote Network / Mask will travel through the VPN tunnel.

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.

IKE Phase 1 proposal Propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match.



IKE Phase 2 proposal Propose the local available algorithms to the VPN peers, and get its feedback to find a match.



Perfect Forward Secrecy The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

4.8 Wireless LAN

This function is used for “n” models.

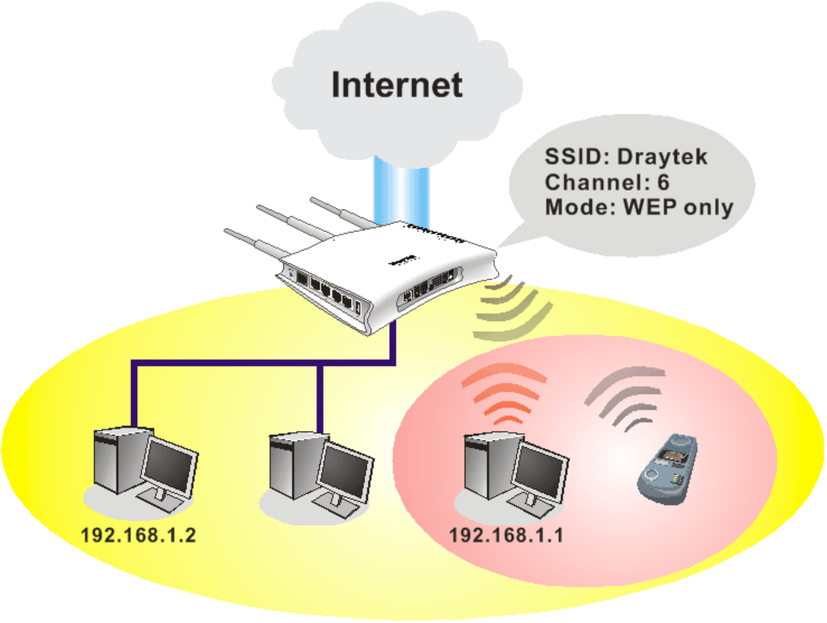
4.8.1 Basic Concepts

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.

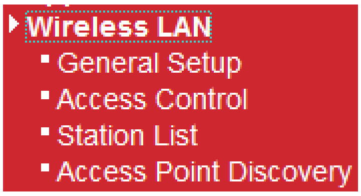
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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.

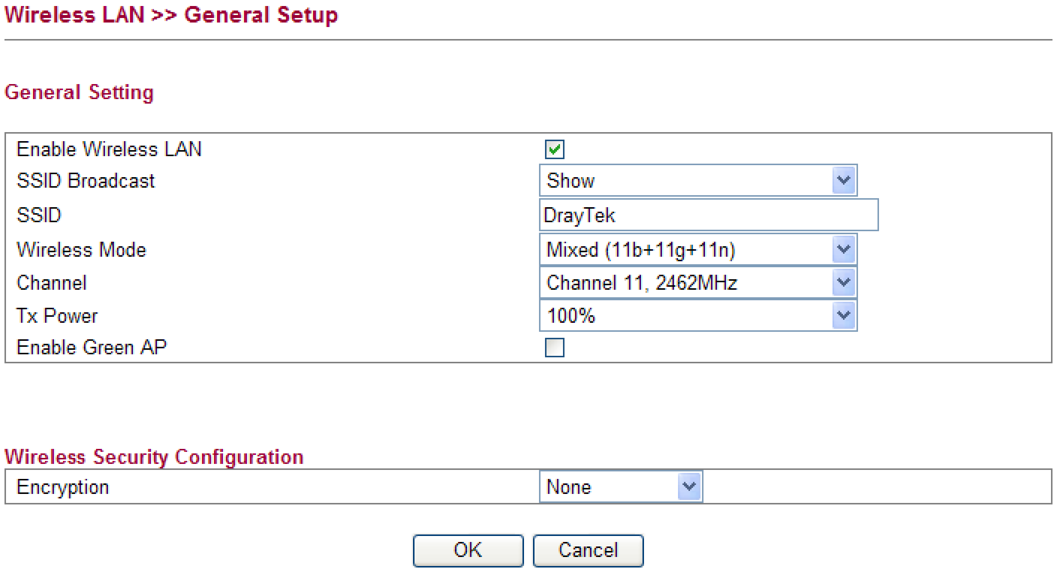
Below shows the menu items for Wireless LAN.



4.8.2 General Setup

By clicking the **General Setup**, 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

Enable Wireless LAN	☑
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Channel	Channel 11, 2462MHz
Tx Power	100%
Enable Green AP	□

Wireless Security Configuration

Encryption	None

Enable Wireless LAN Check the box to enable the wireless function.

SSID Broadcast Choose **Show** to make the SSID being seen by wireless clients. Choose **Hide** to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.

SSID

It 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.

Wireless Mode

Choose the wireless mode for this router. At present, only 802.11B/B/N mix is available.

Country Region Code

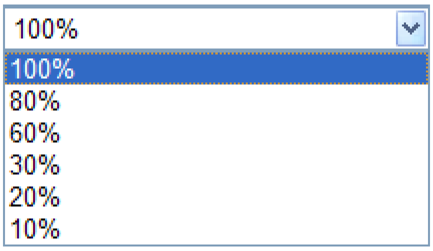
It represents different country region code.
Use the drop down list to choose the one that fit the usage of regulations locally.

Channel

It means the channel of frequency of the wireless LAN. The default channel is 11. 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.

Tx Power

Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.

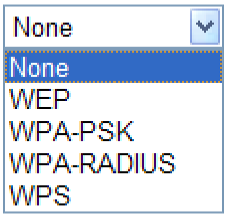


Enable Green AP

Such function is used to reduce the power consumption (Green AP) for the access point. When there is no station connected, the power consumption of access point will be reduced.

Encryption

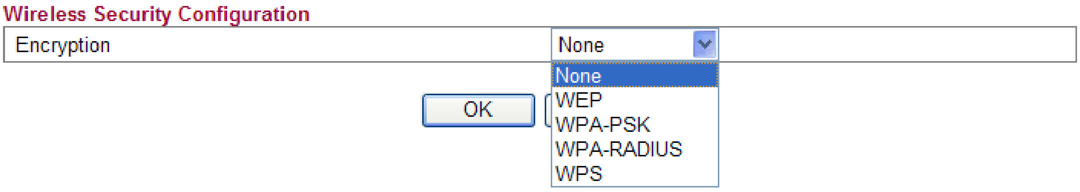
Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.



Each encryption mode will bring out different web page and ask you to offer additional configuration.

Wireless Security Configuration

For the security of your system, choose the proper encryption for data transmission. Different encryption mode will bring out different setting encryption ways.



Wireless Security Configuration

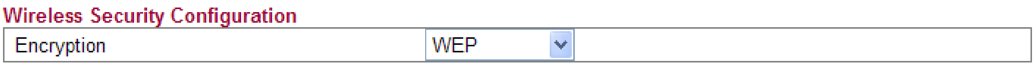
Encryption None

- **None**

  The encryption mechanism is turned off.

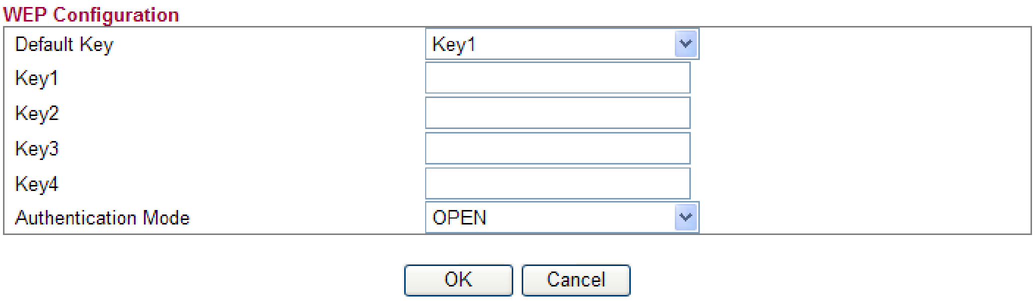
- **WEP**

  Accepts only WEP clients and the encryption key should be entered in WEP Key.



Wireless Security Configuration

Encryption	WEP



WEP Configuration

Default Key	Key1
Key1	
Key2	
Key3	
Key4	
Authentication Mode	OPEN

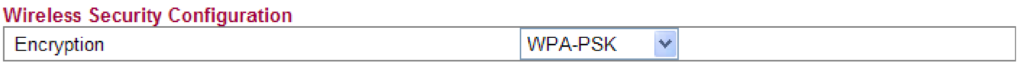
Default Key All wireless devices must support the same WEP encryption bit size and have the same key.

Key1-Key4 **Four keys** can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ',' .

Authentication Mode Choose OPEN or SHARED as the authentication mode.
OPEN: Set wireless to authentication open mode.
SHARED: Set wireless to authentication shared mode.

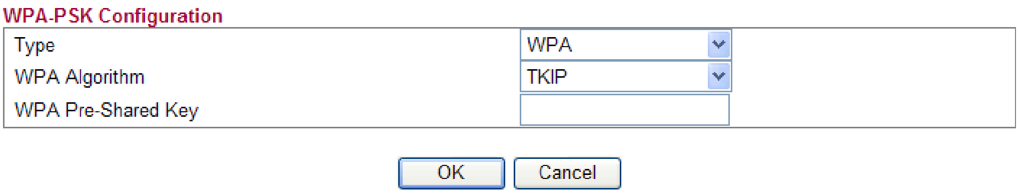
- **WPA-PSK**

  Accepts only WPA clients and the encryption key should be entered in PSK. 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.



Wireless Security Configuration

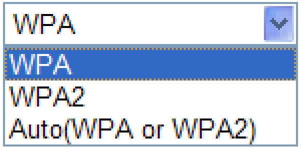
Encryption	WPA-PSK



WPA-PSK Configuration

Type	WPA
WPA Algorithm	TKIP
WPA Pre-Shared Key	

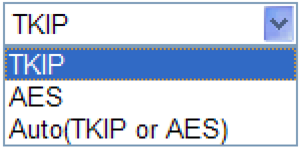
WPA Mode Select WPA, WPA2 or Auto as the type.



WPA

WPA
WPA2
Auto(WPA or WPA2)

WPA Algorithm Select TKIP, AES or auto as the algorithm for WPA.



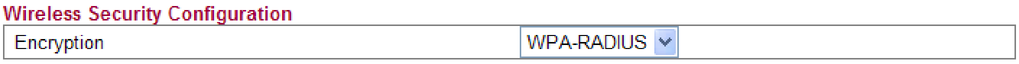
TKIP

TKIP
AES
Auto(TKIP or AES)

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

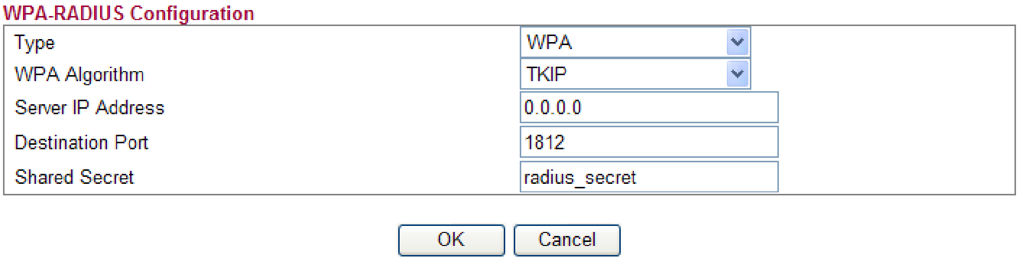
- **WPA-RADIUS**

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.



Wireless Security Configuration

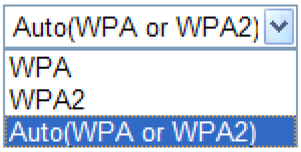
Encryption	WPA-RADIUS



WPA-RADIUS Configuration

Type	WPA
WPA Algorithm	TKIP
Server IP Address	0.0.0.0
Destination Port	1812
Shared Secret	radius_secret

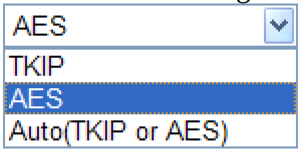
Type The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.



Auto(WPA or WPA2)

WPA
WPA2
Auto(WPA or WPA2)

WPA Algorithm Choose the WPA algorithm, TKIP, AES or Auto.



AES

TKIP
AES
Auto(TKIP or AES)

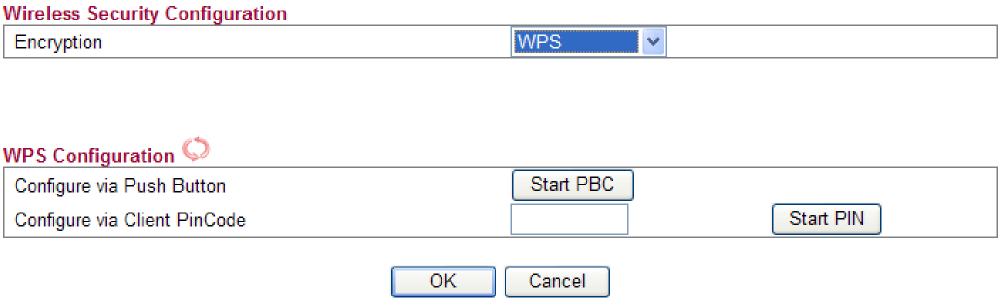
Server IP Address Enter the IP address of RADIUS server.

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.

- **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.


Wireless Security Configuration

Encryption	WPS

WPS Configuration

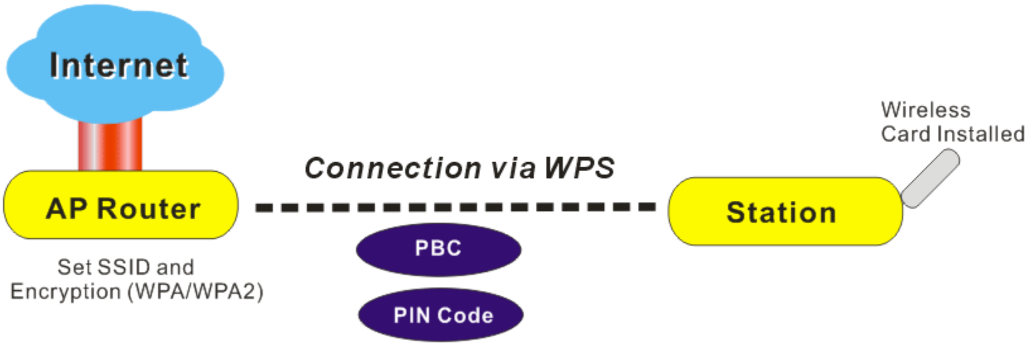
Configure via Push Button	Start PBC	
Configure via Client PinCode		Start PIN

OK Cancel

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 Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN 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.

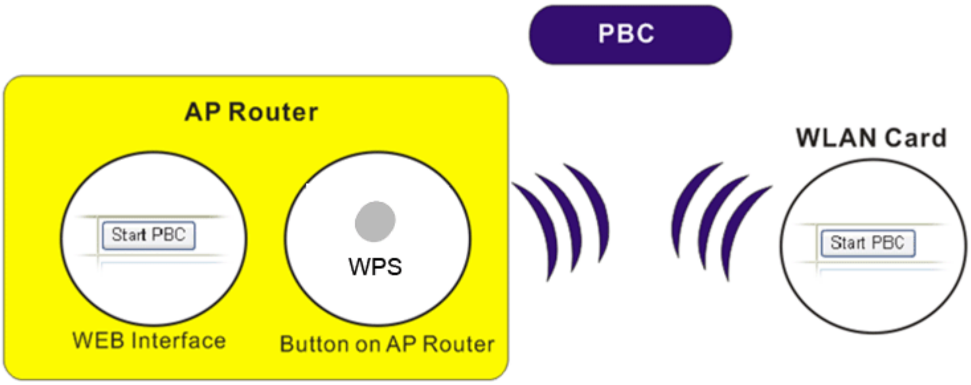
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.



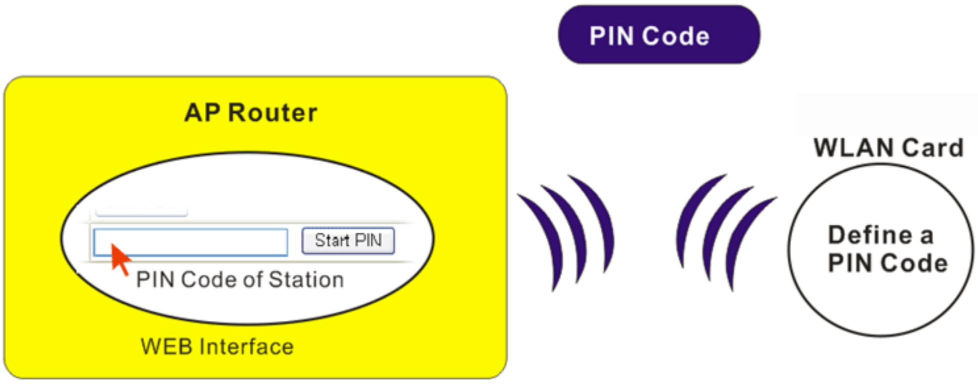
Note: Such function is available for the wireless station with WPS supported.

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 2130 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.

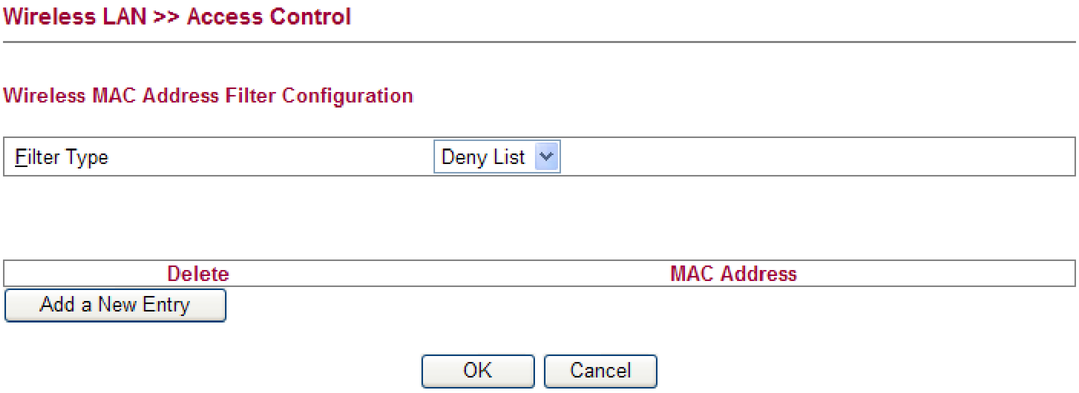


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



4.8.3 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 (deny or allow).



Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type	Deny List

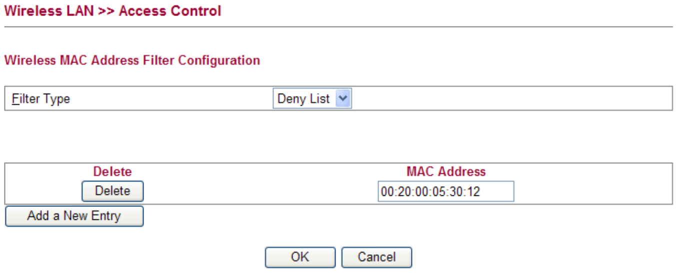
Delete	MAC Address

Filter Type Choose the rule for the MAC addresses displayed in this page.
Allow List – all the MAC address of wireless clients listed here are allowed to do wireless connection.

Deny List – all the MAC address of wireless clients listed here will be blocked.

Add a New Entry Add a new MAC address into the list.

Delete Delete the selected MAC address in the list. This button will appear only an entry of MAC Address has been typed.



Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type	Deny List

Delete	MAC Address
Delete	00:20:00:05:30:12

Add a New Entry

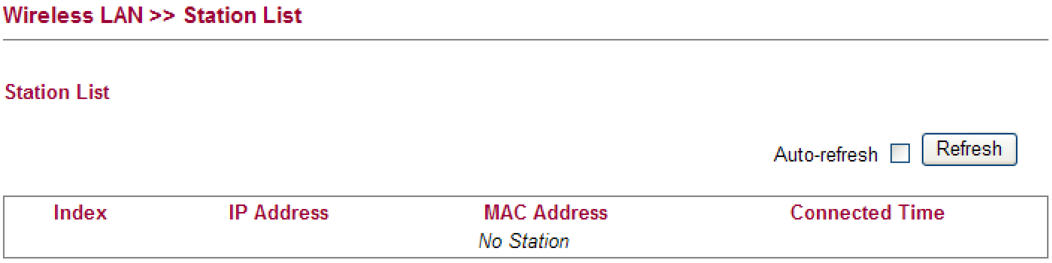
OK Cancel

Cancel Give up the configuration.

OK Click it to save the configuration.

4.8.4 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.



Wireless LAN >> Station List

Station List

Auto-refresh □ Refresh

Index	IP Address	MAC Address	Connected Time
		No Station	

Index Display the number of the connecting client.

IP Address Display the WAN IP address for the connecting client.

MAC Address Display the MAC Address for the connecting client.

Connected Time Display the connection time for the connecting client.

Auto-refresh Check this box to force the system refreshing the table automatically**.**

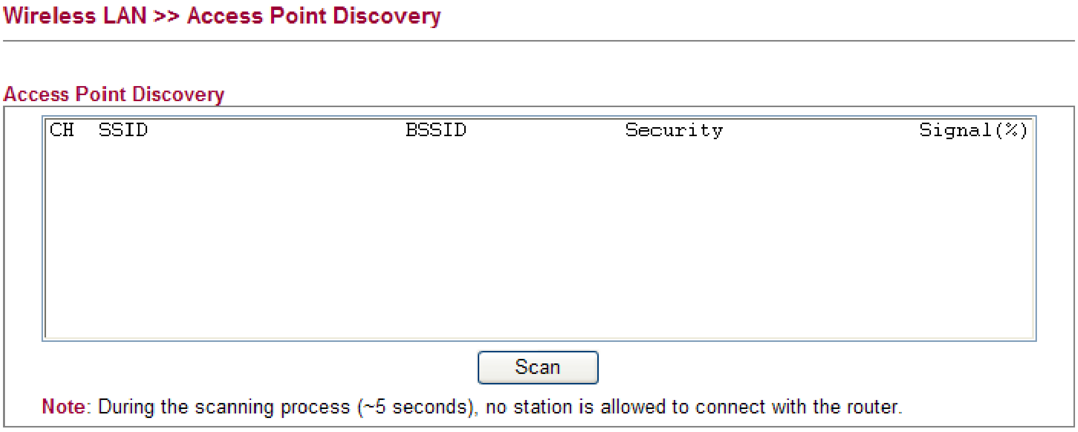
Refresh Click this button to refresh current page.

4.8.5 Access Point 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.

> **Note:** During the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

The table will list channel, SSID, BSSID, Security and the Signal strength of working APs in the neighborhood.

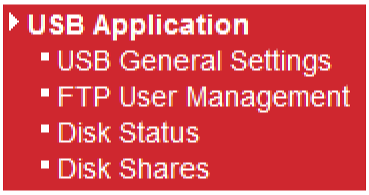


Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

CH	Display the channel for the scanned AP.
SSID	Display the SSID of the scanned AP.
BSSID	Display the MAC address of the scanned AP.
Security	Display the encryption type of the scanned AP.
Signal	Display the strength (in percentage) of the signal of the scanned AP.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.

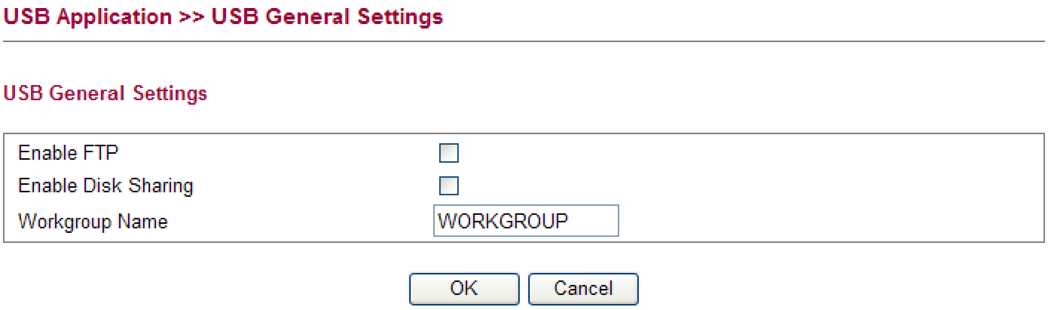
4.9 USB Application

USB diskette can be regarded as an FTP server. By way of Vigor router, clients on LAN can access, write and read data stored in USB diskette. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>FTP User Setting** on the FTP client software. Thus, the client can use the FTP site (USB diskette) through Vigor router.



4.9.1 USB General Settings

This page will determine the number of concurrent FTP connection and default charset for FTP server. At present, the Vigor router can support USB diskette with versions 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

Enable FTP	□
Enable Disk Sharing	□
Workgroup Name	WORKGROUP

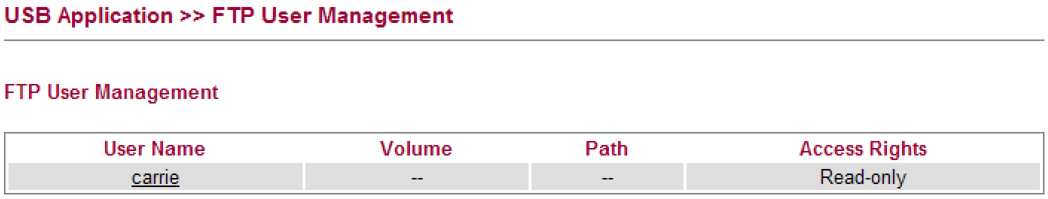
Enable FTP Check this box to enable FTP connection.

Enable Disk Sharing Check this box to share the information on USB disk.

Workgroup Name Type the name for FTP 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.

4.9.2 FTP User Management

This page allows you to change user setting for USB storage disk. Before modifying settings in this page, please insert a USB diskette and configure settings in **User>>User Configuration** first. Otherwise, an error message will appear to warn you.

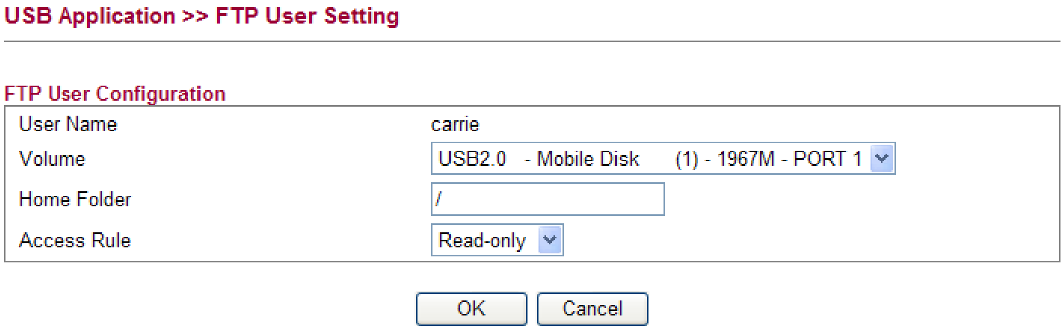


USB Application >> FTP User Management

FTP User Management

User Name	Volume	Path	Access Rights
carrie	--	--	Read-only

Click the name link under User Name to open the setting web page.



USB Application >> FTP User Setting

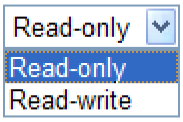
FTP User Configuration

User Name	carrie
Volume	USB2.0 - Mobile Disk (1) - 1967M - PORT 1
Home Folder	/
Access Rule	Read-only

User Name It displays the username that user uses to login to the FTP server.

Volume Select the proper volume for the connected USB diskette.

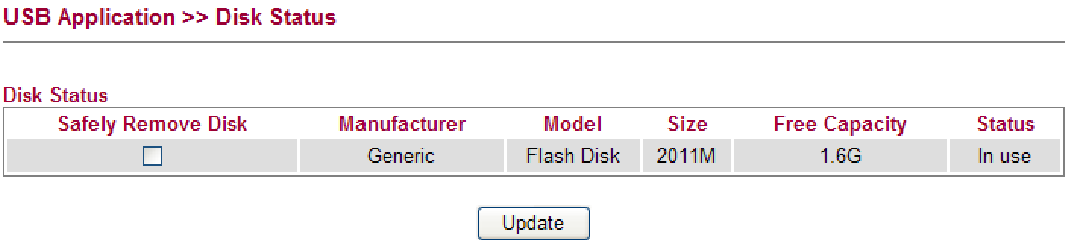
Home Folder It determines the range for the client to access into.
The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB diskette. In addition, if the user types "/" here, he/she can access into all of the disk folders 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.
Access Rule	Select the access right for the USB diskette. 

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

4.9.3 Disk Status

This page can display current using status of the USB diskette. If you want to remove the diskette from USB port in router, please check the box of Safely Remove Disk first. And then, remove the USB diskette later.



USB Application >> Disk Status

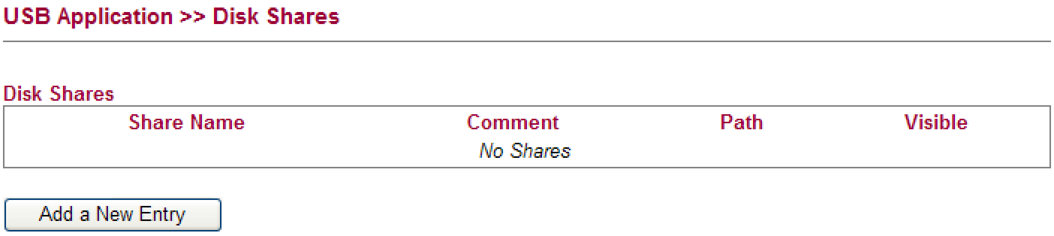
Disk Status

Safely Remove Disk	Manufacturer	Model	Size	Free Capacity	Status
□	Generic	Flash Disk	2011M	1.6G	In use

Safely Remove Disk	Check this box and then you can remove the USB diskette safely.
Manufacturer	Display the manufacturer of the disk.
Model	Display the type of the disk.
Size	Display the storage space of the diskette(s).
Free Capacity	Display the free disk space of the diskette(s).
Status	Display current usage status of the diskette(s)
Update	Click this button to refresh the disk status.

4.9.4 Disk Shares

This page can define the folder which will be shared while Samba File Sharing is enabled.

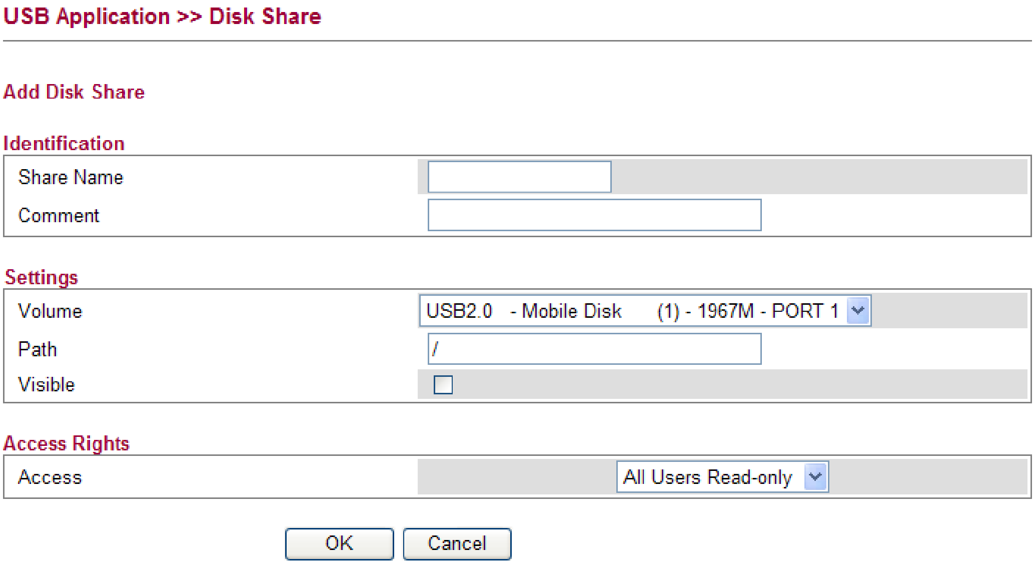


USB Application >> Disk Shares

Disk Shares

Share Name	Comment	Path	Visible
	No Shares		

To add a new entry for disk sharing, please click **Add a New Entry** to open the following page.



USB Application >> Disk Share

Add Disk Share

Identification

Share Name	
Comment	

Settings

Volume	USB2.0 - Mobile Disk (1) - 1967M - PORT 1
Path	/
Visible	□

Access Rights

Access	All Users Read-only

Share Name Type a name to be known by other computers in local network. The name must not contain spaces or special characters.

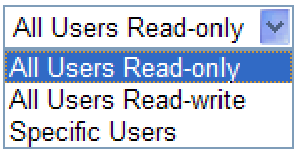
Comment Type the brief description for the disk sharing. The words here will be seen in Network Neighborhood on Windows client computers

Volume Select the proper volume for the connected USB diskette.

Path 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.

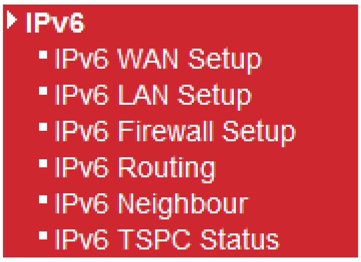
Visible Check this box to make this USB diskette to be seen in Network Neighborhood on Windows of clients in local network.

Access Rights Specify the access right and apply to all the wireless clients that want to connect to the attached USB diskette.



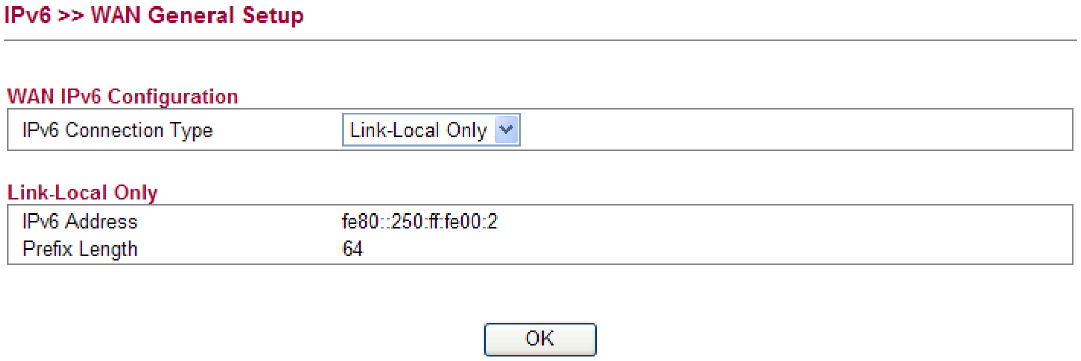
All Users Read-only - everyone has read-only access to the share disk.
All Users Read-write - everyone has read-write access to the share disk.
Specific Users – Only specific user(s) can access into the share disk.

4.10 IPv6



4.10.1 IPv6 WAN Setup

This page defines the IPv6 connection types for WAN interface. Possible types contain Link-Local only, Static IPv6, DHCPv6 and TSPC. Each type requires different parameter settings.



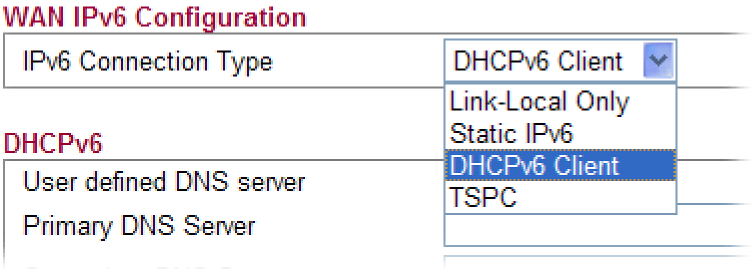
IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	Link-Local Only

Link-Local Only

IPv6 Address	fe80::250:ff:fe00:2
Prefix Length	64



WAN IPv6 Configuration

IPv6 Connection Type	DHCPv6 Client

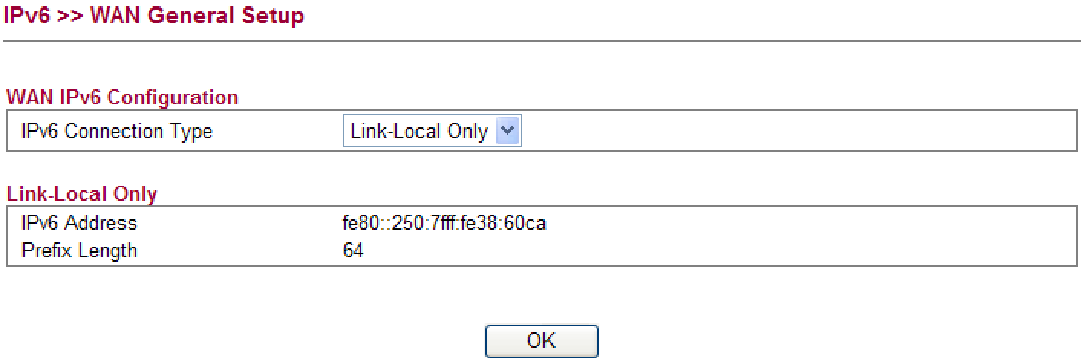
DHCPv6

User defined DNS server

Primary DNS Server

Link-Local Only

Link-Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/10**. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	Link-Local Only

Link-Local Only

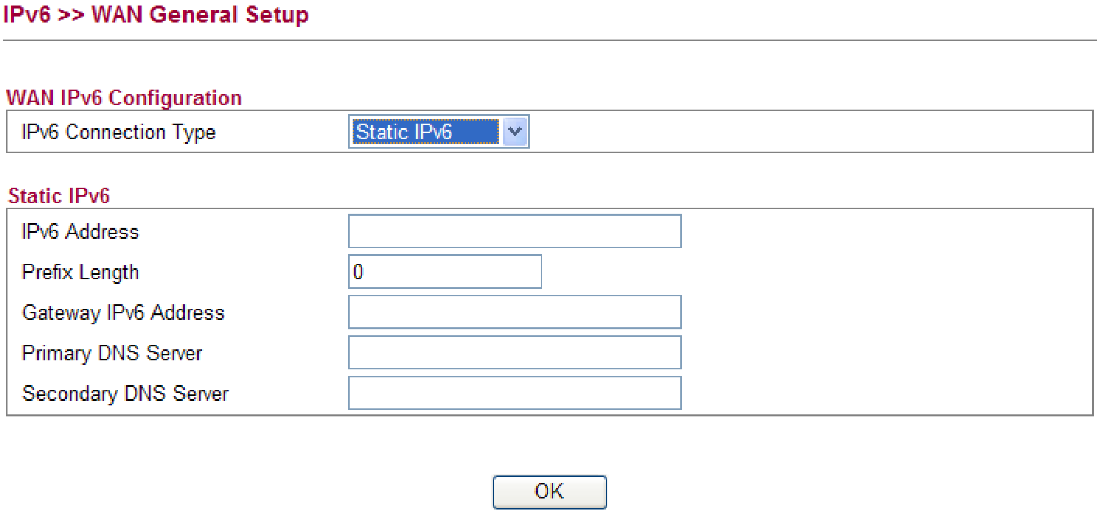
IPv6 Address	fe80::250:7fff:fe38:60ca
Prefix Length	64

IPv6 Address The least significant 64 bits are usually chosen as the interface hardware address constructed in modified EUI-64 format.

Prefix Length Display the fixed value (64) for prefix length.

Static IPv6

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	Static IPv6

Static IPv6

IPv6 Address	
Prefix Length	0
Gateway IPv6 Address	
Primary DNS Server	
Secondary DNS Server	

IPv6 Address Type your IPv6 static IP here.

Prefix Length Type your IPv6 address prefix length here.

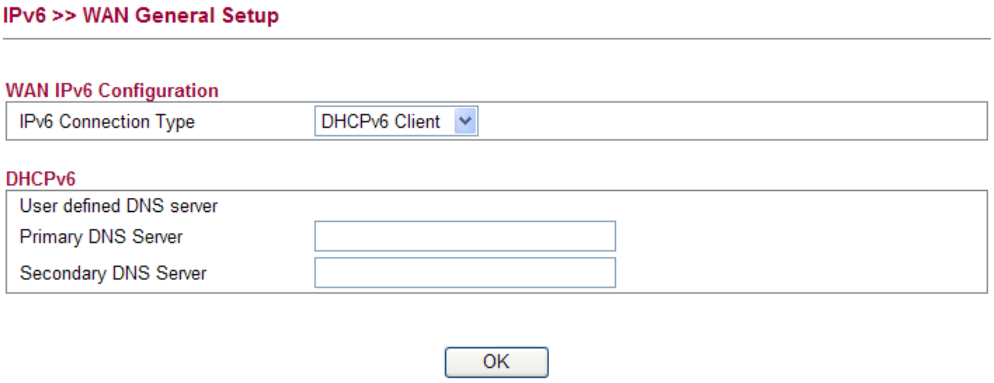
Gateway IPv6 Server Type your IPv6 gateway address here.

Primary DNS Server Type your IPv6 primary DNS Server address here.

Secondary DNS Server Type your IPv6 secondary DNS Server address here.

DHCPv6 Client

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	DHCPv6 Client

DHCPv6

User defined DNS server	
Primary DNS Server	
Secondary DNS Server	

Primary DNS Server Type primary DNS Server address here.

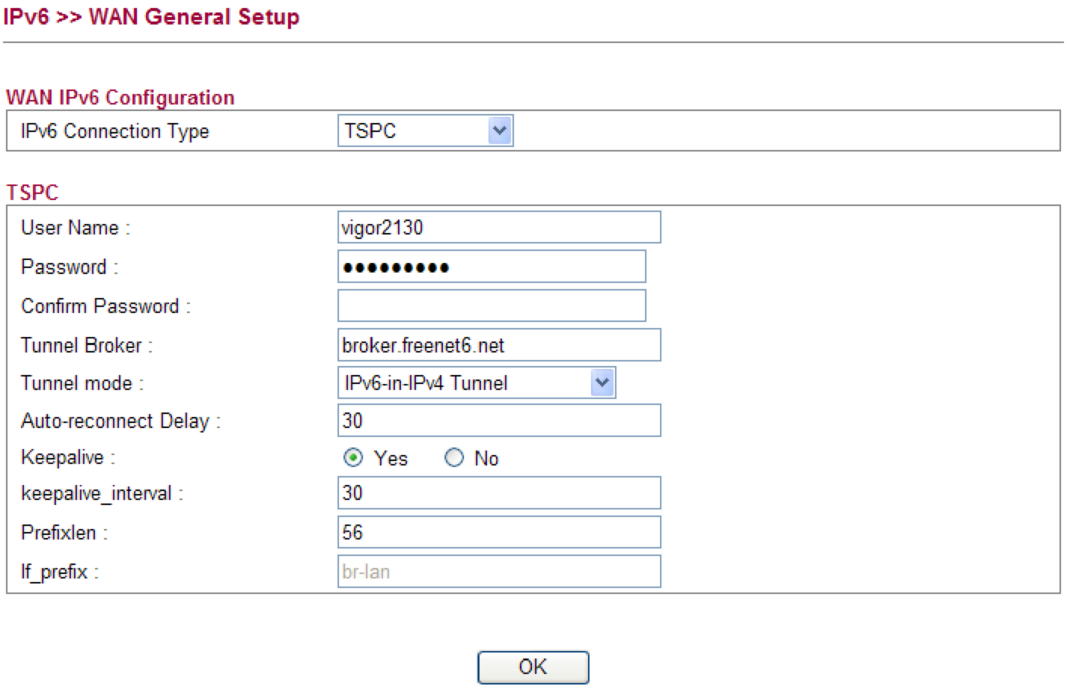
Secondary DNS Server Type secondary DNS Server address here.

TSPC

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

Please make sure your IPv4 WAN connection is OK and apply one free account from hexage (http://go6.net/4105/register.asp) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	TSPC

TSPC

User Name :	vigor2130
Password :	●●●●●●●●●
Confirm Password :	
Tunnel Broker :	broker.freenet6.net
Tunnel mode :	IPv6-in-IPv4 Tunnel
Auto-reconnect Delay :	30
Keepalive :	● Yes ○ No
keepalive_interval :	30
Prefixlen :	56
lf_prefix :	br-lan

Username Type the name obtained from the broker. “vigor2130” is a default username applied from http://go6.net/4105/register.asp. It is suggested for you to apply another username and password.

Password Type the password assigned with the user name.

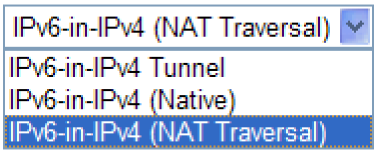
Confirm Password Type the password again to make the confirmation.

Tunnel Broker Type the address for the tunnel broker IP, FQDN or an optional port number.

Tunnel Mode **IPv6-in-IPv4 Tunnel-** Let the broker choose the tunnel mode appropriate for the client.

IPv6-in-IPv4 (Native) - Request an IPv6 in IPv4 tunnel.

IPv6-in-IPv4 (NAT Traversal - Request an IPv6 in UDP of IPv4 tunnel (for clients behind a NAT).



Auto-reconnect Delay

After passing the time set here, the client will retry to connect in case of failure or keepalive timeout.
0 means not retry.

Keepalive

Yes – Keep the connection between TSPC and tunnel broker always on. TSPC will send ping packet to make sure the connection between both ends is normal.
No - The client will not send keepalives.

Keepalive_interval

Type the time for the interval between two keepalive messages transferring from the client to the broker.

Prefixlen

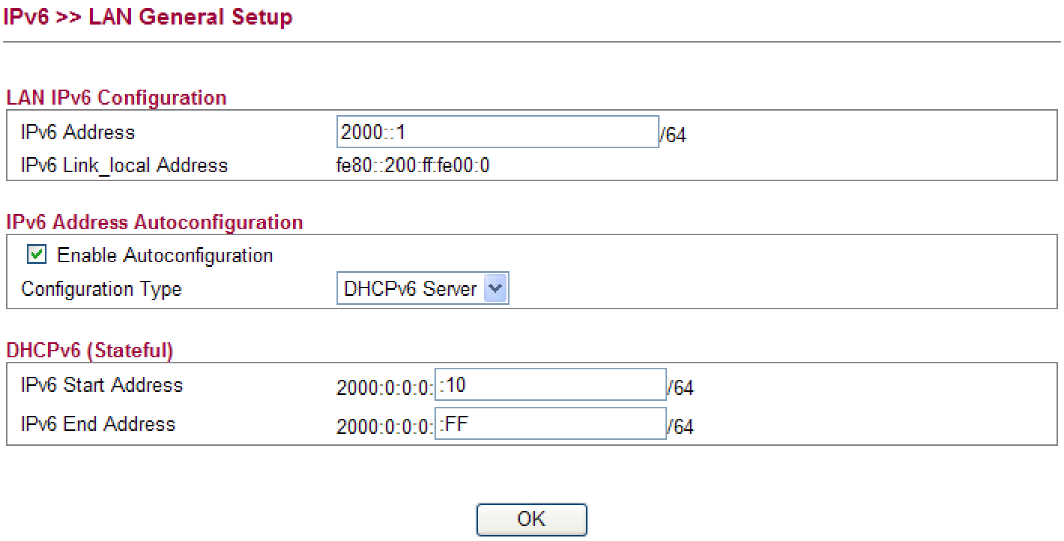
Type the required prefix length for the client network.

If_prefix

Display LAN interface name. The name of the OS interface that will be configured with the first 64 of the received prefix from the broker and the router advertisement daemon is started to advertise that prefix on the if_prefix interface.

4.10.2 IPv6 LAN Setup

This page defines the IPv6 connection types for LAN interface. Possible types contain DHCPv6 Server and RADVD. Each type requires different parameter settings.



IPv6 >> LAN General Setup

LAN IPv6 Configuration

IPv6 Address	2000::1 /64
IPv6 Link_local Address	fe80::200:ff:fe00:0

IPv6 Address Autoconfiguration

☑ Enable Autoconfiguration

Configuration Type: DHCPv6 Server

DHCPv6 (Stateful)

IPv6 Start Address	2000:0:0:0: :10 /64
IPv6 End Address	2000:0:0:0: :FF /64

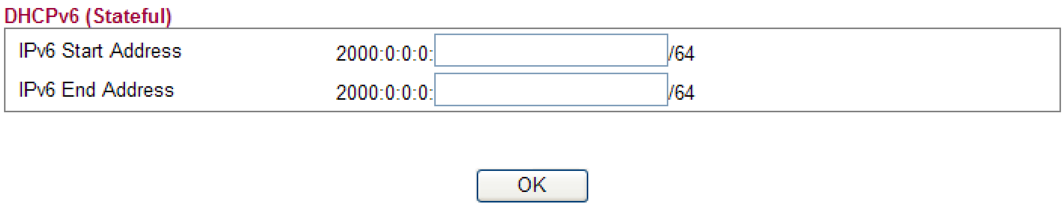
IPv6 Address Type static IPv6 address for LAN.

IPv6 Link_local Address It is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix fe80::/10. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.

Enable Autoconfiguration Check this box to enable the auto-configuration function for IPv6 connection.

Configuration Type Vigor2130 provides 2 daemons for LAN side IPv6 address configuration. One is **RADVD**(stateless) and the other is **DHCPv6 Server** (Stateful).

DHCPv6 Server- DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.

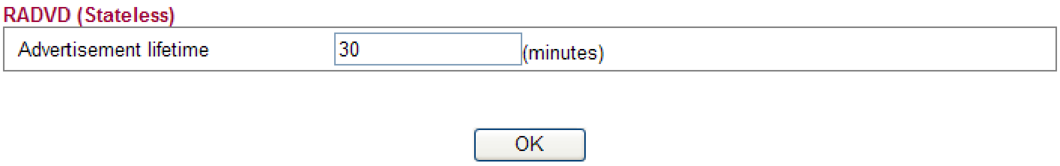


DHCPv6 (Stateful)

IPv6 Start Address	2000:0:0:0: /64
IPv6 End Address	2000:0:0:0: /64

IPv6 Start Address/IPv6 End Address- Type the start and end address for IPv6 server.

RADVD - The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless autoconfiguration.



RADVD (Stateless)

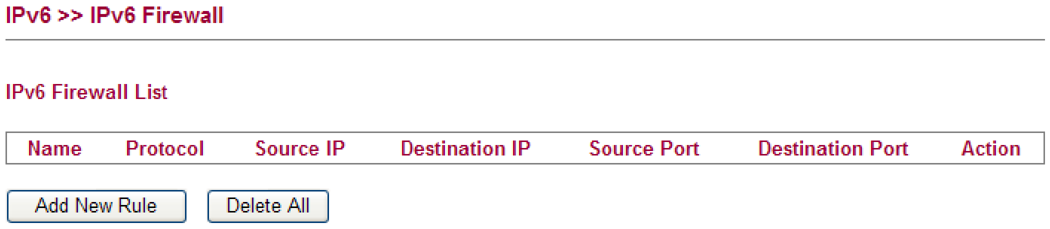
Advertisement lifetime: 30 (minutes)

Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.

4.10.3 IPv6 Firewall Setup

This page allows users to set firewall rules for IPv6 packets.

Note: Section 4.4 **Firewall** is configured for IPv4 packets only.



IPv6 >> IPv6 Firewall

IPv6 Firewall List

Name	Protocol	Source IP	Destination IP	Source Port	Destination Port	Action

Name Display the name of the rule.

Protocol Display the protocol (TCP/UDP/ICMPv6) the rule uses.

Source IP Display the source IP address of such rule.

Destination IP Display the destination IP address of such rule.

Source Port Display the source port number of such rule.

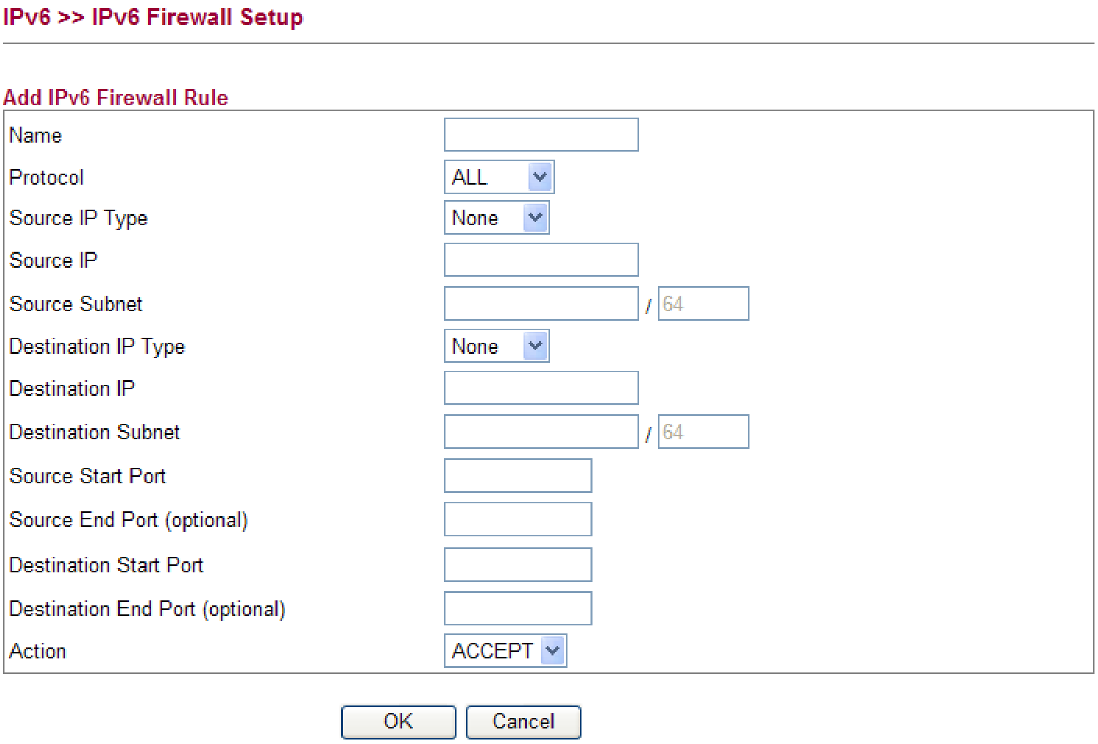
Destination Port Display the destination port number of such rule.

Action Display the status (accept or drop) of such rule.

Adding a New Rule

Click **Add New Rule** to configure a new rule for IPv6 Firewall.

Note: You can set up to 20 sets of IPv6 rules.



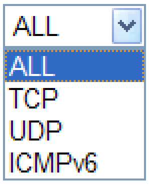
IPv6 >> IPv6 Firewall Setup

Add IPv6 Firewall Rule

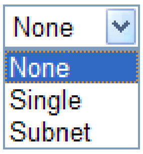
Name	
Protocol	ALL
Source IP Type	None
Source IP	
Source Subnet	/ 64
Destination IP Type	None
Destination IP	
Destination Subnet	/ 64
Source Start Port	
Source End Port (optional)	
Destination Start Port	
Destination End Port (optional)	
Action	ACCEPT

Name Type a name for the rule.

Protocol Specify a protocol for this rule.



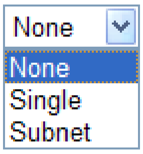
Source IP Type Determine the IP type as the source.



Source IP Type the IP address here if you choose **Single** as **Source IP Type**.

Source Subnet Type the subnet mask here if you choose **Subnet** as **Source IP Type**.

Destination IP Type Determine the IP type as the destination.



Destination IP Type the IP address here if you choose **Single** as **Destination IP Type**.

Destination Subnet Type the subnet mask here if you choose **Subnet** as **Destination IP Type**.

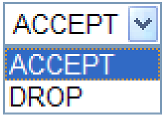
Source Start Port Type a value as the source start port. Such value will be available only TCP/UDP is selected as the protocol.

Source End Port (optional) Type a value as the source end port. Such value will be available only TCP/UDP is selected as the protocol.

Destination Start Port Type a value as the destination start port. Such value will be available only TCP/UDP is selected as the protocol.

Destination End Port (optional) Type a value as the destination end port. Such value will be available only TCP/UDP is selected as the protocol.

Action Set the action that the router will perform for the packets through the protocol of IPv6.



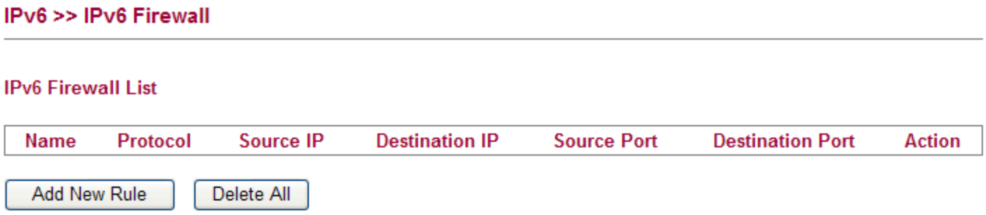
Accept – If the IPv6 packets fit the condition listed in this page, the router will let it pass through.
Drop - If the IPv6 packets fit the condition listed in this page, the router will block it.

Example:

Refer to the following example.

1. Use TSPC mode to connect to IPv6 network.
   PC get ipv6 IP: 2001:5c0:1503:7400:30e4:139d:53c8:3a1e
2. Connect PC to http://www.ipv6.org/ with IPv6 IP address.
   A message will appear from the web page:

   Welcome to the IPv6 Information Page!
   You are using IPv6 from 2001:5c0:1503:7400:30e4:139d:53c8:3a1e
3. Set firewall rule to block all TCP traffic from this IP address.
4. Open **IPv6** >> **IPv6 Firewall Setup** and press **Add New Rule**.

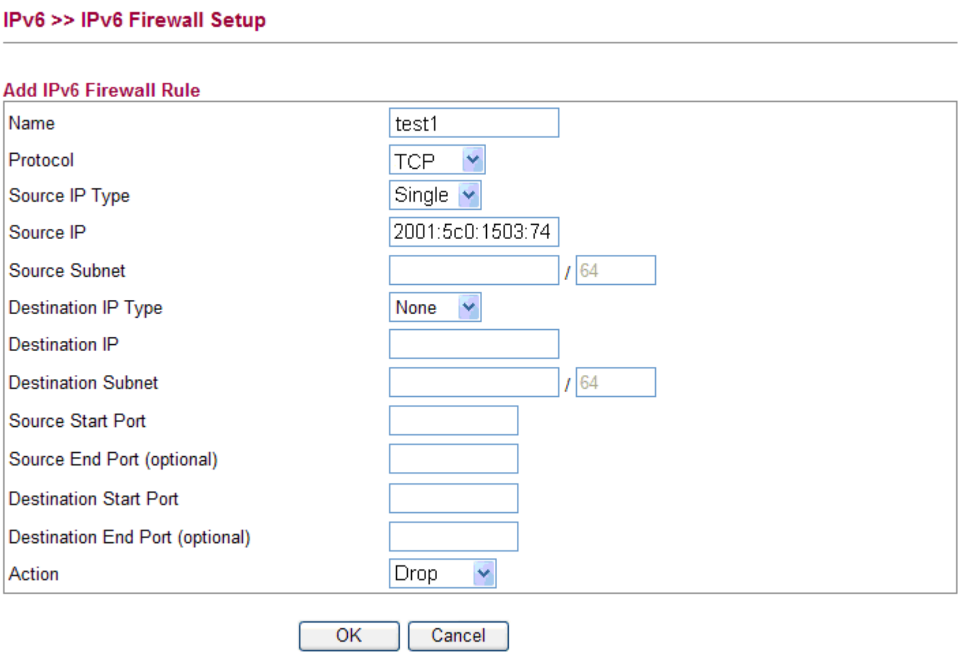


IPv6 >> IPv6 Firewall

IPv6 Firewall List

Name	Protocol	Source IP	Destination IP	Source Port	Destination Port	Action

In the following dialog, please configure the page with the following values.



IPv6 >> IPv6 Firewall Setup

Add IPv6 Firewall Rule

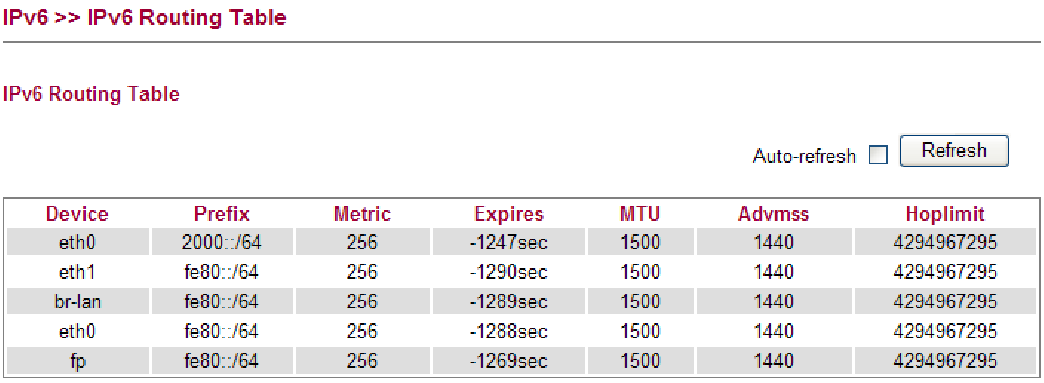
Name	test1
Protocol	TCP
Source IP Type	Single
Source IP	2001:5c0:1503:74
Source Subnet	/ 64
Destination IP Type	None
Destination IP	
Destination Subnet	/ 64
Source Start Port	
Source End Port (optional)	
Destination Start Port	
Destination End Port (optional)	
Action	Drop

5. Connect PC to http://www.ipv6.org/ with IPv6 IP address again.
   A message will appear from web page:

Welcome to the IPv6 Information Page!
You are using IPv4 from 114.37.132.219

4.10.4 IPv6 Routing

This page displays the routing table for the protocol of IPv6.



IPv6 >> IPv6 Routing Table

IPv6 Routing Table

Device	Prefix	Metric	Expires	MTU	Advmss	Hoplimit
eth0	2000::/64	256	-1247sec	1500	1440	4294967295
eth1	fe80::/64	256	-1290sec	1500	1440	4294967295
br-lan	fe80::/64	256	-1289sec	1500	1440	4294967295
eth0	fe80::/64	256	-1288sec	1500	1440	4294967295
fp	fe80::/64	256	-1269sec	1500	1440	4294967295

Device Display the interface name (eth0, eth1, fp, etc..)that used to transfer packets with addresses matching the prefix.

Prefix The IPv6 address prefix.

Metric Display the distance to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

Expires Display the lifetime of the route.

MTU Display the largest size (in bytes) of a packet.

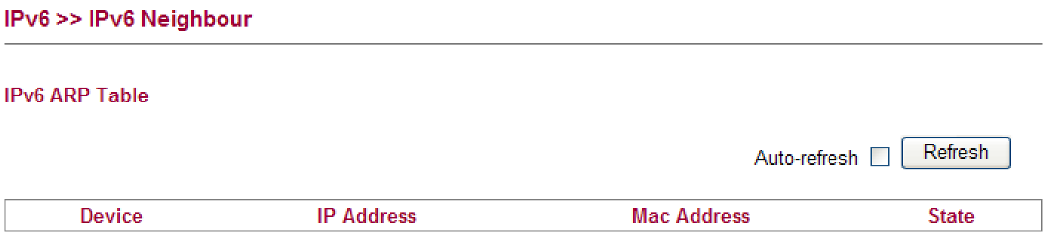
Advmss Display the largest size (in bytes) of an unfragmented piece of a routing advertisement.

Hoplimit Display the number of network segments on which the packet is allowed to travel before discarded.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.

4.10.5 IPv6 Neighbour

IPv6 uses neighbor discovery protocol to find out neighbors on the same link.



IPv6 >> IPv6 Neighbour

IPv6 ARP Table

Auto-refresh □ Refresh

Device	IP Address	Mac Address	State

Device The interface name of the link where the neighbor is on.

IP Address The IPv6 address of the neighbor.

MAC Address The link-layer address of the neighbor.

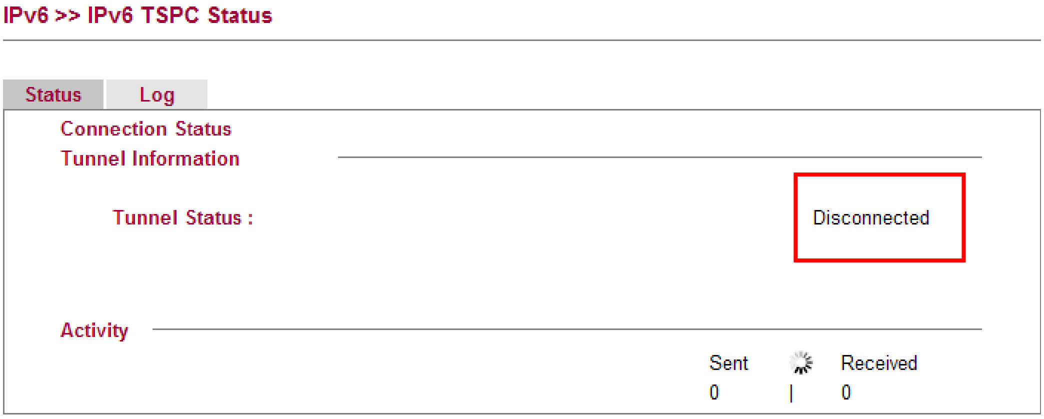
State Possible states include:
incomplete - address resolution is in progress.
reachable - neighbor is reachable.
stale – neighbor(s) may be unreachable but not verified until a packet is sent).
delay - neighbor may be unreachable and a packet was sent.
probe - neighbor may be unreachable and probes are sent to verify the reachability.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.

4.10.6 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC. TSPC log contains some debug information from program.

If TSPC has not configured properly, the router will display the following page when the user tries to connect through TSPC connection.



IPv6 >> IPv6 TSPC Status

Connection Status

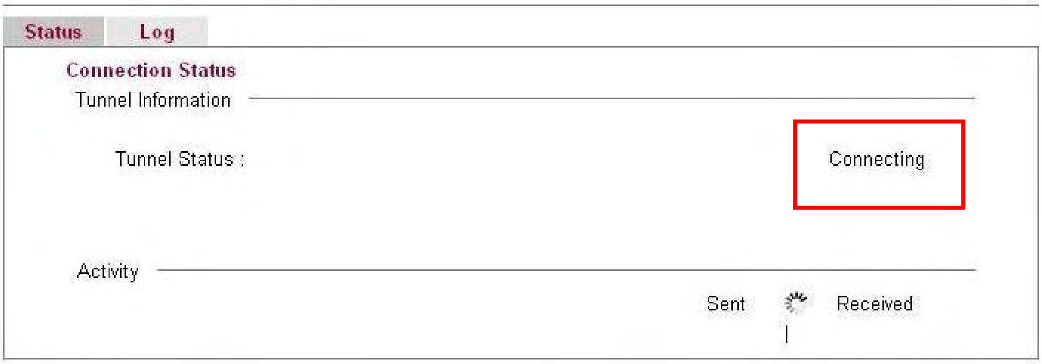
Tunnel Information

Tunnel Status : Disconnected

Activity

Sent 0 | Received 0

When TSPC configuration has been done, the router will start to connect. The connecting page will be shown as below:



Connection Status

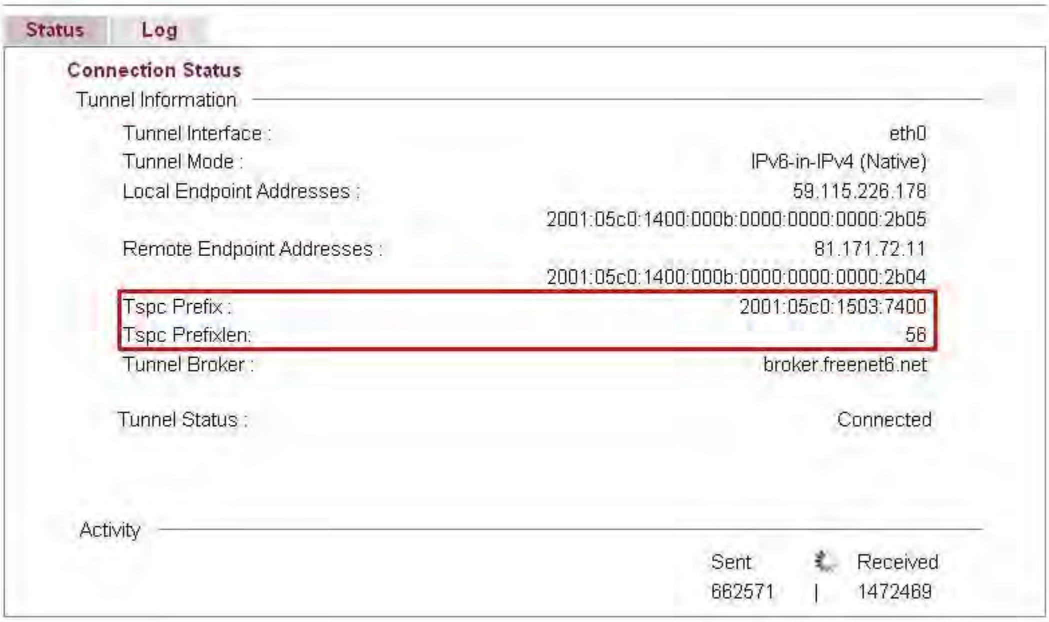
Tunnel Information

Tunnel Status : Connecting

Activity

Sent | Received

When the router detects all the information, the screen will be shown as follows. One set of **TSPC prefix** and **prefix length** will be obtained after the connection between TSPC and Tunnel broker built.



Connection Status

Tunnel Information

Tunnel Interface :	eth0
Tunnel Mode :	IPv6-in-IPv4 (Native)
Local Endpoint Addresses :	59.115.226.178 2001:05c0:1400:000b:0000:0000:0000:2b05
Remote Endpoint Addresses :	81.171.72.11 2001:05c0:1400:000b:0000:0000:0000:2b04
Tspc Prefix :	2001:05c0:1503:7400
Tspc Prefixlen:	56
Tunnel Broker :	broker.freenet6.net
Tunnel Status :	Connected

Activity

Sent 662571 | Received 1472469

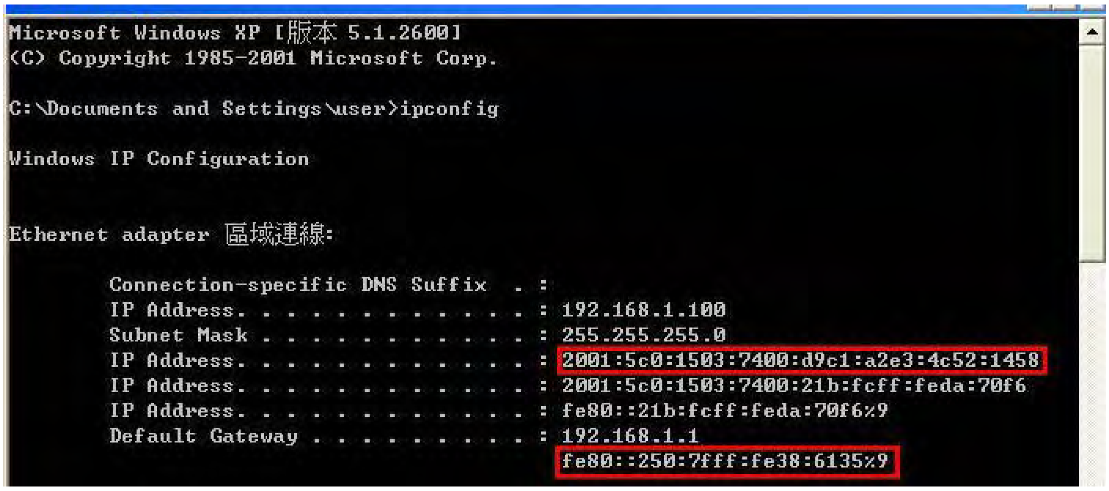
Connection Status It will bring out different pages to represent IPv6 disconnection, connecting and connected.

Tunnel Information Display interface name (used to send TSPC prefix), tunnel mode, local endpoint addresses, remote endpoint address, TSPC Prfix, TSPC Prefixlen (prefix length), tunnel broker and so on.

Tunnel Status **Disconnected -** The remote client doesn't connect to the tunnel server.
Connecting - The remote client is connecting to the tunnel server.
Connected – The remote client has been connected to the tunnel server.

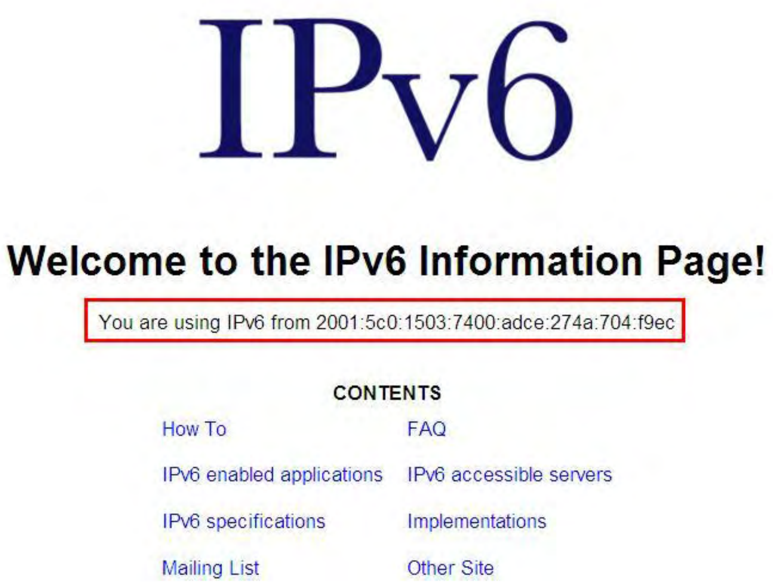
Activity **Sent -** sent to the tunnel (RX bytes).
Received - received from the tunnel (RX bytes).

When the router connects to the tunnel broker, the router will use RADVD to transmit the prefix to the PC on LAN. Next, the PC will generate one set of IPv6 public IP (see the figure below). Users can use such IP for connecting to IPv6 network.



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

C:\Documents and Settings\user>ipconfig

Windows IP Configuration


Ethernet adapter 區域連線:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:5c0:1503:7400:d9c1:a2e3:4c52:1458
        IP Address. . . . . . . . . . . . : 2001:5c0:1503:7400:21b:fcff:feda:70f6
        IP Address. . . . . . . . . . . . : fe80::21b:fcff:feda:70f6%9
        Default Gateway . . . . . . . . . : 192.168.1.1
                                            fe80::250:7fff:fe38:6135%9
```

When your PC obtains the IPv6 address, please connect to http://www.ipv6.org. If your PC access Internet via IPv6 connection, your IPv6 address will be shown on the web page immediately. Refer to the following figure.



IPv6

Welcome to the IPv6 Information Page!

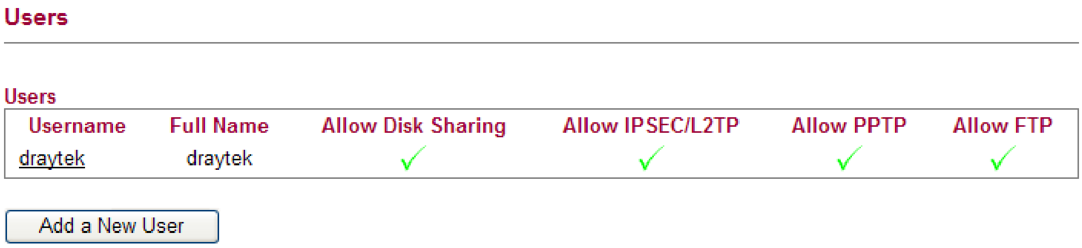
You are using IPv6 from 2001:5c0:1503:7400:adce:274a:704:f9ec

CONTENTS

4.11 User

4.11.1 User Configuration

This page allows you to set user's setting that allowed to use PPTP, FTP, IPSEC/L2TP connection.



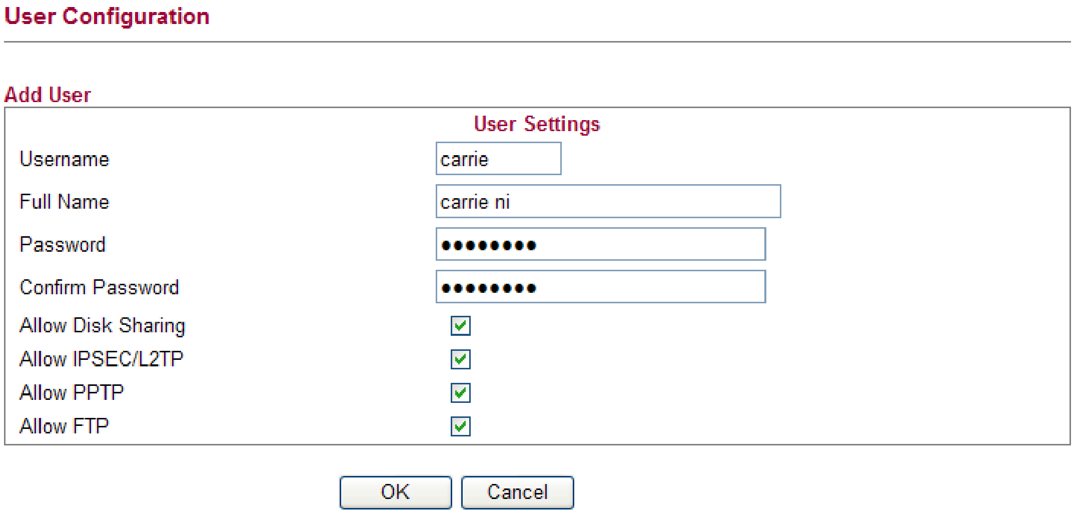
Users

Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
draytek	draytek	✓	✓	✓	✓

Adding a New User

Click **Add a New User** to open the following page.



User Configuration

Add User

User Settings	
Username	carrie
Full Name	carrie ni
Password	••••••••
Confirm Password	••••••••
Allow Disk Sharing	☑
Allow IPSEC/L2TP	☑
Allow PPTP	☑
Allow FTP	☑

Username Type a name for this user.

Full Name Type full name for this user.

Password Type the password for this user.

Confirm Password Type the password again for confirmation.

Allow Disk Sharing Check this box to have the remote user share the disk information.

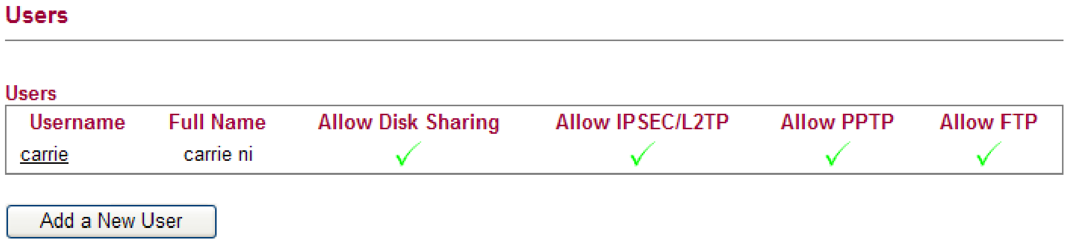
Allow IPSEC/L2TP Check this box to let the remote user connecting to this device through IPSEC/L2TP**.**

Allow PPTP Check this box to let the remote user connecting to this device through PPTP**.**

Allow FTP Check this box to let the remote user connecting to FTP server via this router.

Delete User Remove settings on current page and delete the user. This button is not available for new configuration by pressing **Add a New User**.

When you finish the settings, simply click **OK** to save the configuration. The new user will be created and displayed on the page.



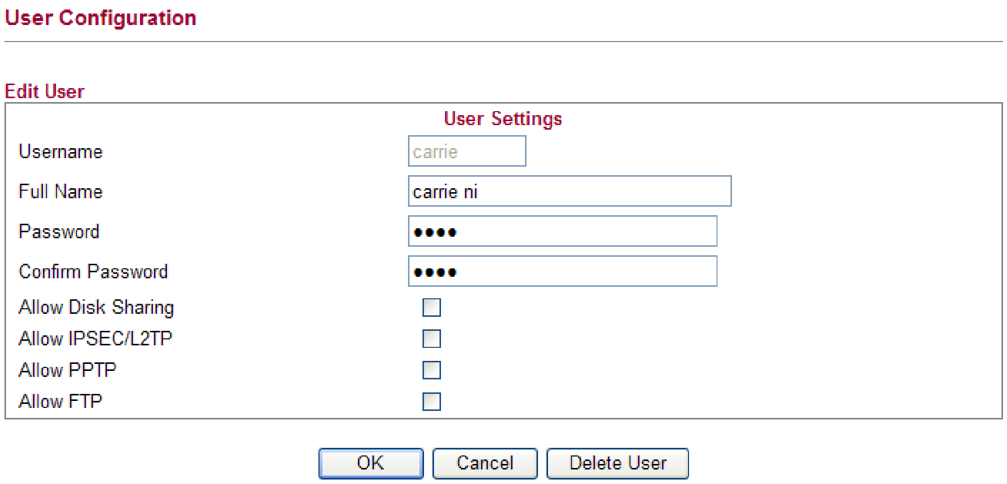
Users

Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
carrie	carrie ni	✓	✓	✓	✓

Editing/Deleting User Settings

To edit a user, click the name link under Username to open the following page. Modify the settings except Username and then click **OK** to save and exit it. If you want to remove such user settings, simply click **Delete User**.



User Configuration

Edit User

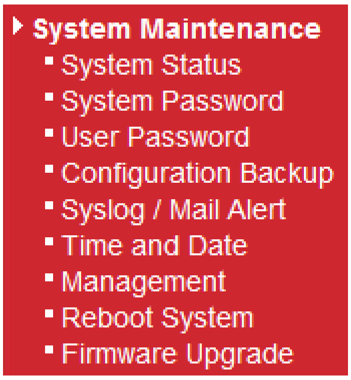
User Settings

Username	carrie
Full Name	carrie ni
Password	••••
Confirm Password	••••
Allow Disk Sharing	□
Allow IPSEC/L2TP	□
Allow PPTP	□
Allow FTP	□

4.12 System Maintenance

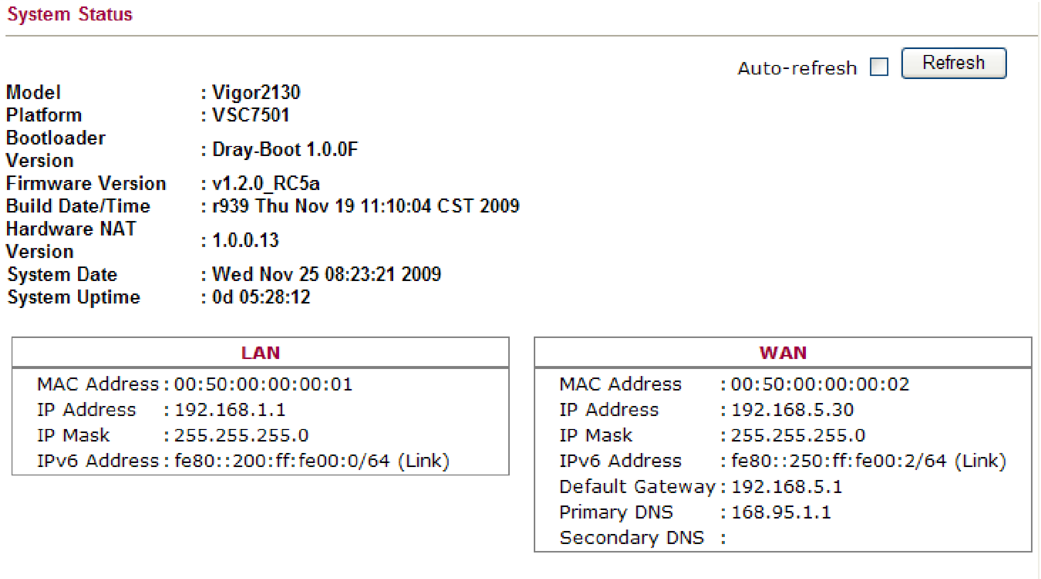
For the system setup, there are several items that you have to know the way of configuration: Status, User Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.12.1 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

Auto-refresh ☐ Refresh

Model : Vigor2130
Platform : VSC7501
Bootloader Version : Dray-Boot 1.0.0F
Firmware Version : v1.2.0_RC5a
Build Date/Time : r939 Thu Nov 19 11:10:04 CST 2009
Hardware NAT Version : 1.0.0.13
System Date : Wed Nov 25 08:23:21 2009
System Uptime : 0d 05:28:12

LAN

MAC Address : 00:50:00:00:00:01
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::200:ff:fe00:0/64 (Link)

WAN

MAC Address : 00:50:00:00:00:02
IP Address : 192.168.5.30
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:ff:fe00:2/64 (Link)
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

Model Name	Display the model name of the router.
Platform	Display the hardware type that this device is built upon.
Bootloader Version	Display the bootloader version of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
Hardware NAT Version	Display the hardware acceleration NAT version.
System Date	Display current time and date for the system server.
System Uptime	Display the connection time for the system server.

LAN-------

MAC Address Display the MAC address of the LAN Interface.

IP Address Display the IP address of the LAN interface.

IP Mask Display the subnet mask address of the LAN interface.

WAN-------

MAC Address Display the MAC address of the WAN Interface.

IP Address Display the IP address of the WAN interface.

IP Mask Display the subnet mask address of the WAN interface.

IPv6 Address Display the IPv6 address of the WAN interface.

Default Gateway Display the gateway address of the WAN interface.

Primary DNS Display the specified primary DNS setting.

Secondary DNS Display the specified secondary DNS setting.

Wireless LAN-------

MAC Address Display the MAC address of the wireless LAN.

Device Type Display the device type used for wireless LAN.

SSID Display the SSID of the router.

Channel Display the channel that wireless LAN used.

Manufacturer Display the manufacturer of the disk.

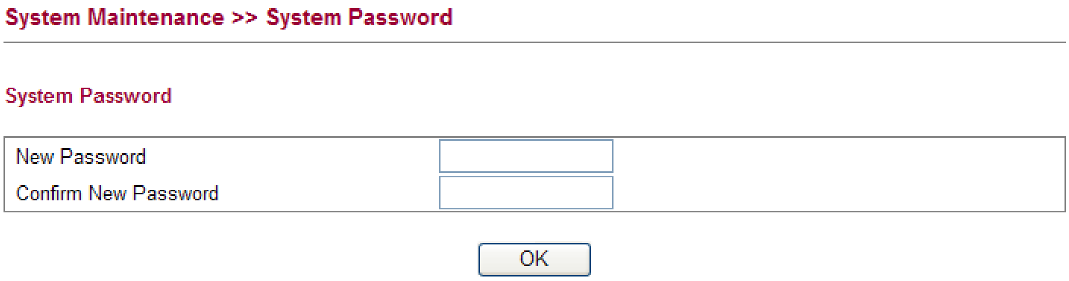
Model Display the type of the disk.

Size Display the storage size of the USB diskette.

Status Display current status of the USB diskette.

4.12.2 System Password

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



System Maintenance >> System Password

System Password

New Password	
Confirm New Password	

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

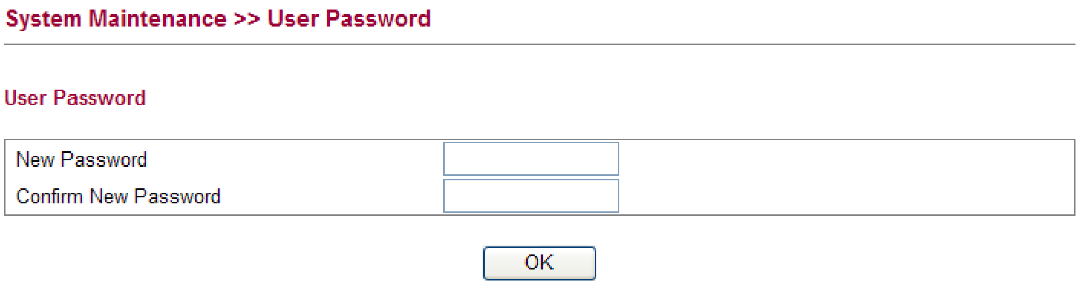
New Password Type in new password in this filed.

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.

4.12.3 User Password

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


System Maintenance >> User Password

User Password

New Password	
Confirm New Password	

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

New Password Type in new password in this filed.

Confirm Password Type in the new password again.

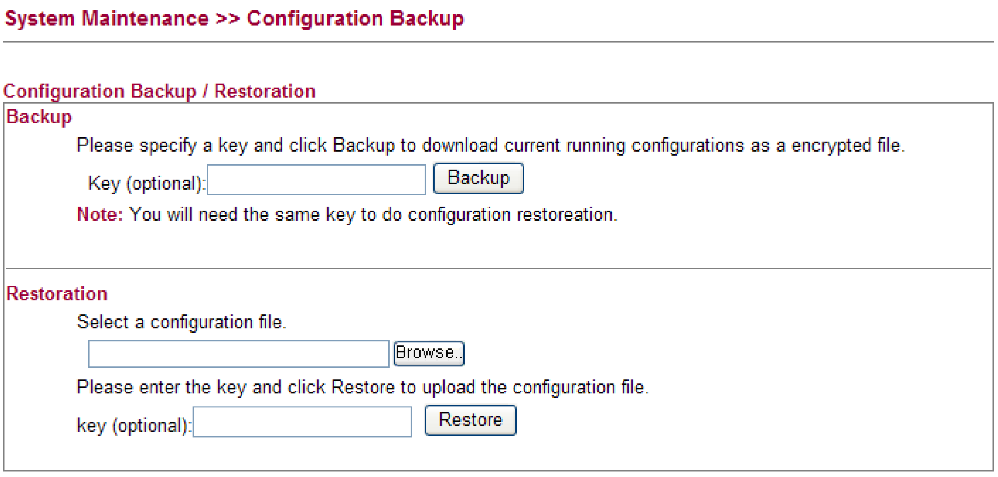
When you click **OK**, the login window will appear. Please use the new password to access into the web configurator again.

4.12.4 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

Backup

Please specify a key and click Backup to download current running configurations as a encrypted file.

Key (optional):

Note: You will need the same key to do configuration restoreation.

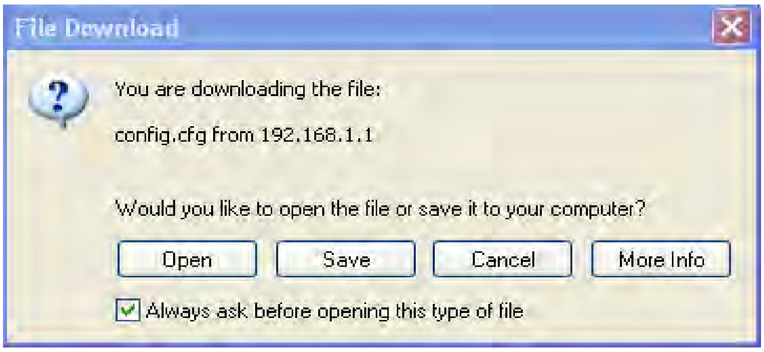
Restoration

Select a configuration file.

Please enter the key and click Restore to upload the configuration file.

key (optional):

2. Type a key arbitrarily for encrypting the file. Keep the key in mind. You will need it whenever you want to restore such file. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



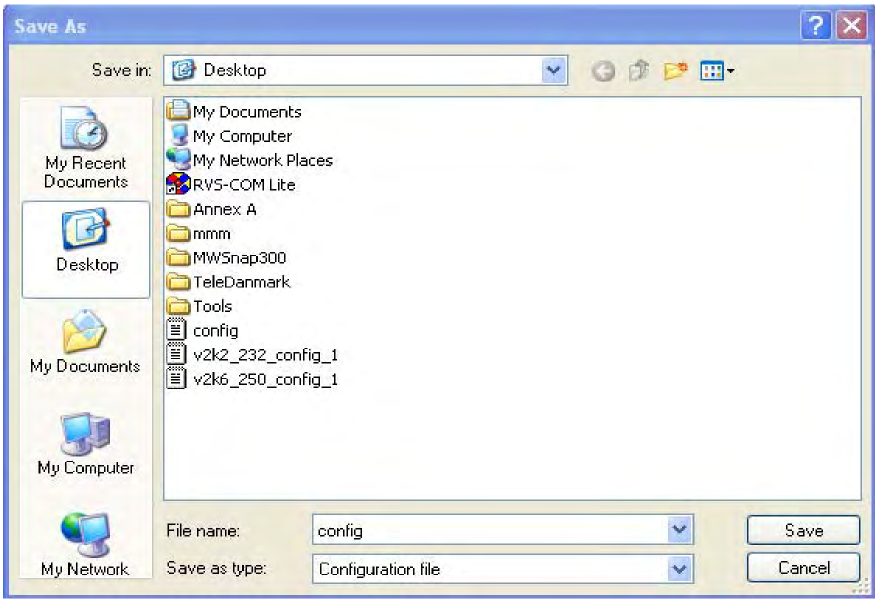
You are downloading the file:

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 in: Desktop

File name: config

Save as type: Configuration file

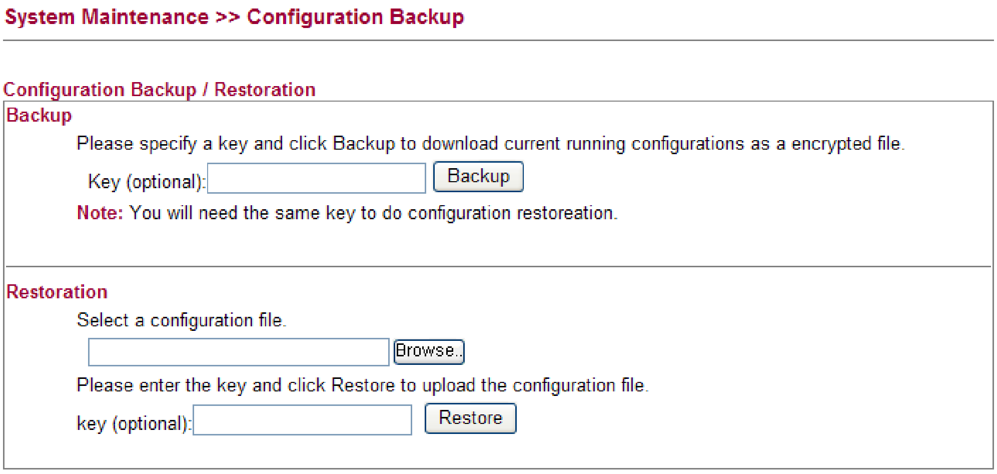
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

Backup

Please specify a key and click Backup to download current running configurations as a encrypted file.

Key (optional): [ ] Backup

Note: You will need the same key to do configuration restoreation.

Restoration

Select a configuration file.

[ ] Browse..

Please enter the key and click Restore to upload the configuration file.

key (optional): [ ] Restore

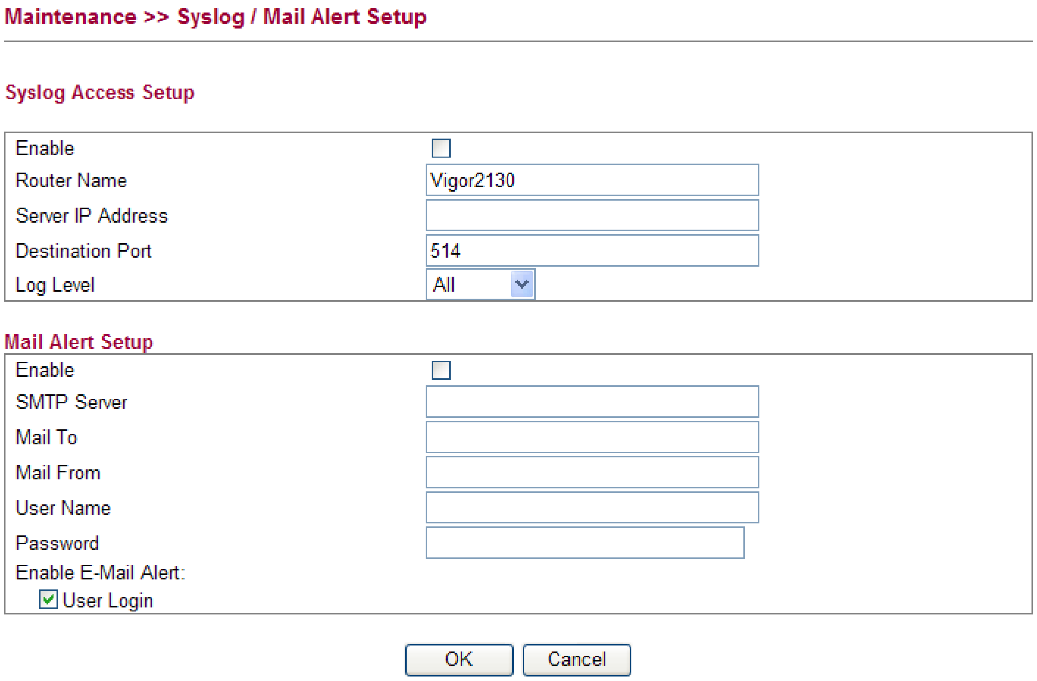
2. Click **Browse** button to choose the correct configuration file for uploading to the router.

3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

> **Note:** If the file you want to restore has been encrypted, you will be asked to type the encrypted key before clicking **Restore**.

4.12.5 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.



Maintenance >> Syslog / Mail Alert Setup

Syslog Access Setup

Enable	□
Router Name	Vigor2130
Server IP Address	
Destination Port	514
Log Level	All

Mail Alert Setup

Enable	□
SMTP Server	
Mail To	
Mail From	
User Name	
Password	
Enable E-Mail Alert:	
☑ User Login	

OK Cancel

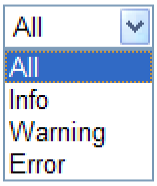
Enable (Syslog Access…) Check "**Enable**" to activate function of syslog.

Router Name Assign a name of this device.

Server IP Address The IP address of the Syslog server.

Destination Port Assign a port for the Syslog protocol.

Log Level Choose the severity level for the system log entry.



Enable (Mail Alert…) Check "**Enable**" to activate function of mail alert.

SMTP Server The IP address of the SMTP server.

Mail To Assign a mail address for sending mails out.

Mail From Assign a path for receiving the mail from outside.

User Name Type the user name for authentication.

Password Type the password for authentication.

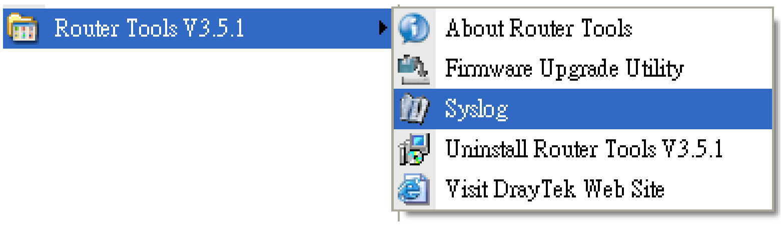
Enable E-mail Alert Check the box of User Login to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

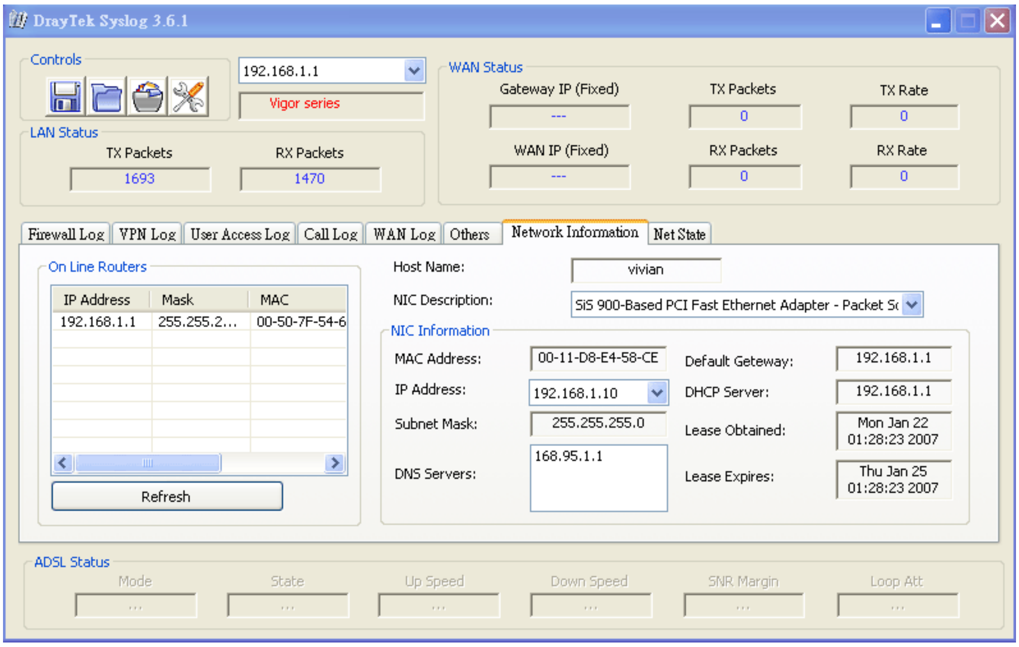
For viewing the Syslog, please do the following:

4. Just set your monitor PC's IP address in the field of Server IP Address

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



6. 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.



DrayTek Syslog 3.6.1

Controls: 192.168.1.1 — Vigor series

LAN Status

TX Packets	RX Packets
1693	1470

WAN Status

Gateway IP (Fixed)	TX Packets	TX Rate
---	0	0
WAN IP (Fixed)	**RX Packets**	**RX Rate**
---	0	0

On Line Routers

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

NIC Information

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

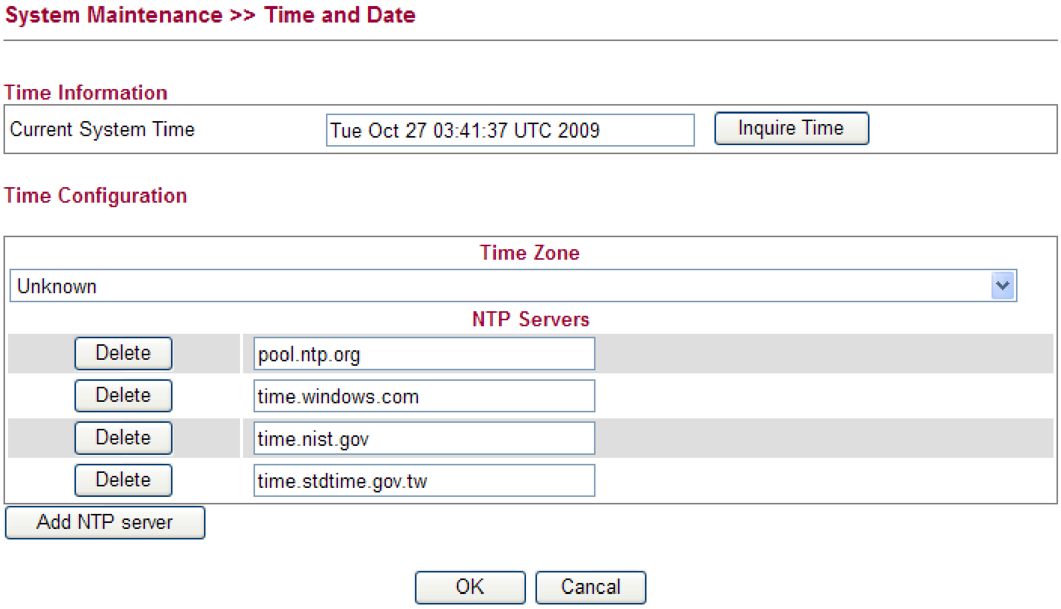
Lease Expires: Thu Jan 25 01:28:23 2007

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
...	...	...	...	...	...

4.12.6 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: Tue Oct 27 03:41:37 UTC 2009

Time Configuration

Time Zone: Unknown

NTP Servers

Delete	pool.ntp.org
Delete	time.windows.com
Delete	time.nist.gov
Delete	time.stdtime.gov.tw

Current System Time Click **Inquire Time** to get the current time.

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

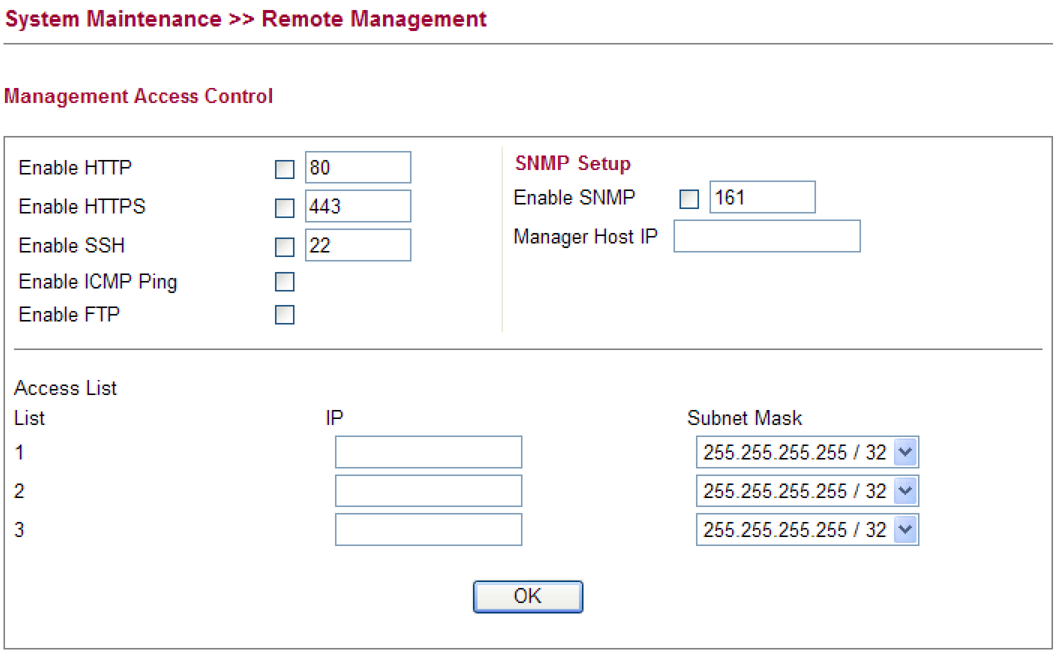
Add NTP server Click the button to add a new NTP server.

Delete Click this button to remove an NTP server.

Click **OK** to save these settings.

4.12.7 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. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.



System Maintenance >> Remote Management

Management Access Control

Enable HTTP	□	80
Enable HTTPS	□	443
Enable SSH	□	22
Enable ICMP Ping	□	
Enable FTP	□	

SNMP Setup

Enable SNMP	□	161
Manager Host IP		

Access List

List	IP	Subnet Mask
1		255.255.255.255 / 32
2		255.255.255.255 / 32
3		255.255.255.255 / 32

Enable HTTP/HTTPS/SSH/ICMP Ping/FTP/SNMP 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.

Manager Host IP – Type the IP address for the host to perform the remote management.

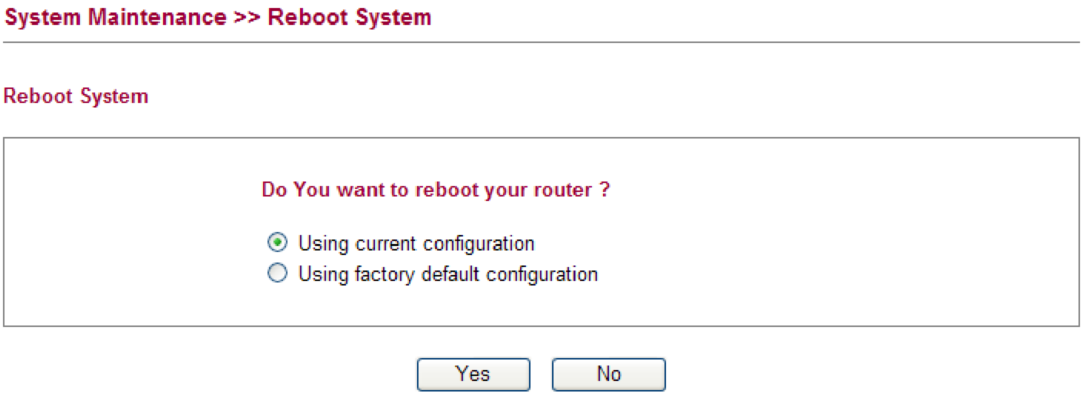
Access List You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.

List IP - Indicate an IP address allowed to login to the router.

Subnet Mask - Represent a subnet mask allowed to login to the router.

4.12.8 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
○ Using factory default configuration

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

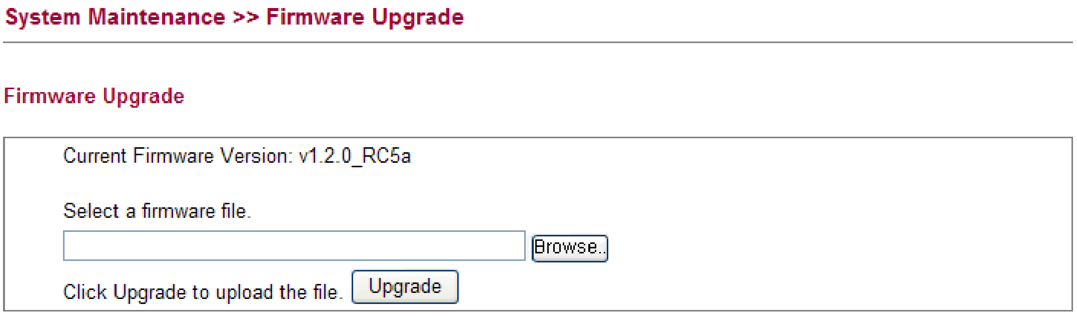
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

4.12.9 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 **Maintenance**>> **Firmware Upgrade** to launch the Firmware Upgrade Utility.


System Maintenance >> Firmware Upgrade

Firmware Upgrade

Current Firmware Version: v1.2.0_RC5a

Select a firmware file.

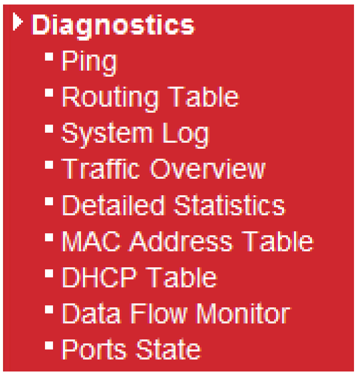
Click Upgrade to upload the file.

Click **Browse..** to locate the newest firmware and click **Upgrade**. During the process of upgrade, do not turn off your router.

4.13 Diagnostics

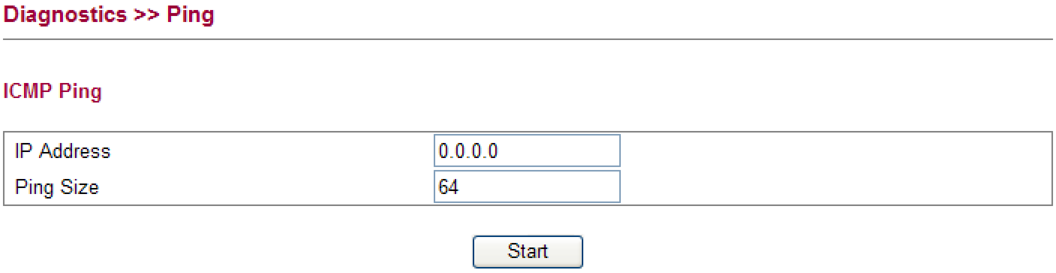
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



4.13.1 Ping

Click **Diagnostics** and click **Ping** to open the web page. It is used to troubleshoot IP connection for your router.



Diagnostics >> Ping

ICMP Ping

IP Address	0.0.0.0
Ping Size	64

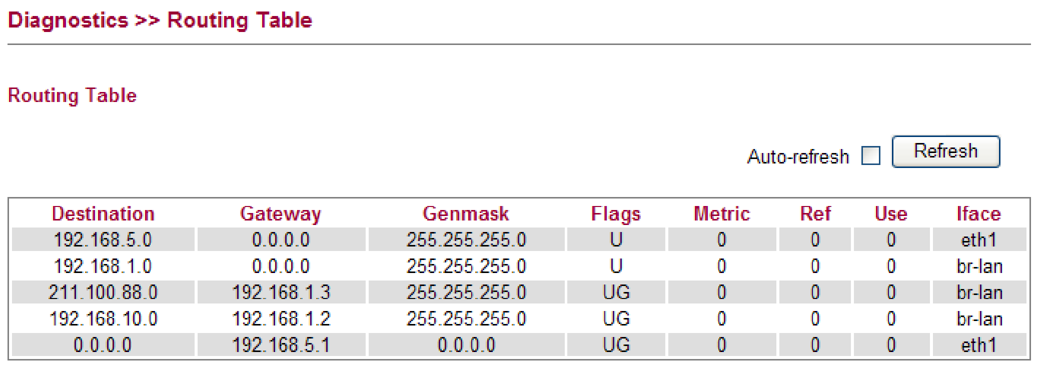
IP Address Type in the IP address of the Host/IP that you want to ping.

Ping Size Type in the payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

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

4.13.2 Routing Table

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



Diagnostics >> Routing Table

Routing Table

Auto-refresh □ Refresh

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.5.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br-lan
211.100.88.0	192.168.1.3	255.255.255.0	UG	0	0	0	br-lan
192.168.10.0	192.168.1.2	255.255.255.0	UG	0	0	0	br-lan
0.0.0.0	192.168.5.1	0.0.0.0	UG	0	0	0	eth1

Destination Display the IP address for destination network or destination host.

Gateway Display the gateway address or "*" if none set.

Genmask Display the netmask for the destination net; '255.255.255.255' is for a host destination and '0.0.0.0' is for the default route.

Flags Different codes represent different routing status.
U - route is up.
H - target is a host
G - use gateway
R - reinstate route for dynamic routing
D - dynamically installed by daemon or redirect
M - modified from routing daemon or redirect
A - installed by addrconf
C - cache entry
! - reject route

Metric Display the distance to the target (usually counted in hops).

Ref Display number of references to this route. (Not used in the Linux kernel.)

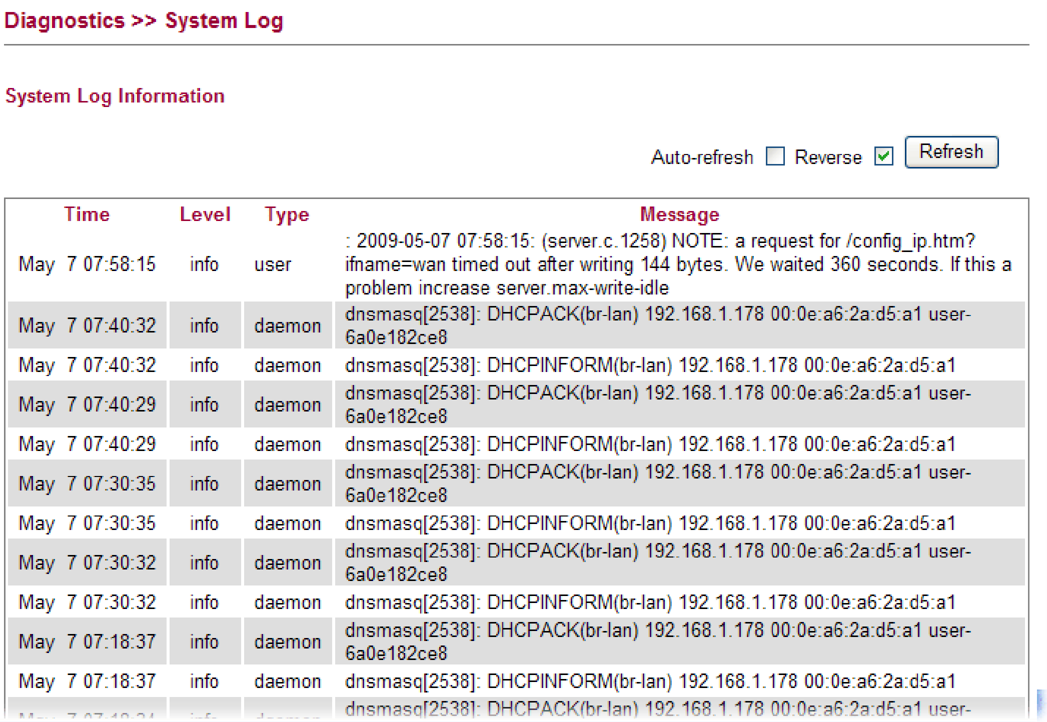
Use Display count of lookups for the route. Depending on the use of -F and –C, this will be either route cache misses (-F) or hits (-C).

Iface Display interface to which packets for this route will be sent.

Refresh Click it to reload the page.

4.13.3 System Log

Click **Diagnostics** and click **System Log** to open the web page.



Diagnostics >> System Log

System Log Information

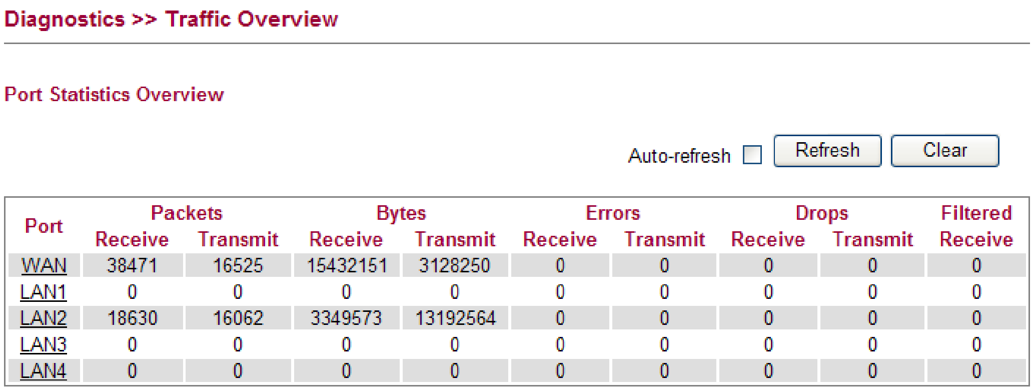
Auto-refresh □ Reverse ☑ Refresh

Time	Level	Type	Message
May 7 07:58:15	info	user	: 2009-05-07 07:58:15: (server.c.1258) NOTE: a request for /config_ip.htm?ifname=wan timed out after writing 144 bytes. We waited 360 seconds. If this a problem increase server.max-write-idle
May 7 07:40:32	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:40:32	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:40:29	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:40:29	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:30:35	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:30:35	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:30:32	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:30:32	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:18:37	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:18:37	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:18:34	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-

Time	Display the time of the system log entry.
Level	Display the severity level of the system log entry.
Type	Display the type or subsystem of the system log entry.
Message	Display a short description of the system log entry.
Auto-refresh	Check it to enable auto-refresh function.
Reverse	Check it to have newest log entries presented first.
Refresh	Click it to reload the page.

4.13.4 Traffic Overview

This page offers an overview of general traffic statistics for all connecting ports.



Diagnostics >> Traffic Overview

Port Statistics Overview

Auto-refresh □ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
WAN	38471	16525	15432151	3128250	0	0	0	0	0
LAN1	0	0	0	0	0	0	0	0	0
LAN2	18630	16062	3349573	13192564	0	0	0	0	0
LAN3	0	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0	0

Port Display the interface that data transmission passing through.

Packets Display the packet sizes for data transmission in receiving and sending.

Bytes Display the number of received and transmitted bytes per port.

Errors Display the number of the error occurred in data receiving and data sending.

Drops Display the number of the data lost in receiving and sending.

Filtered Display the number of received frames filtered by the forwarding process.

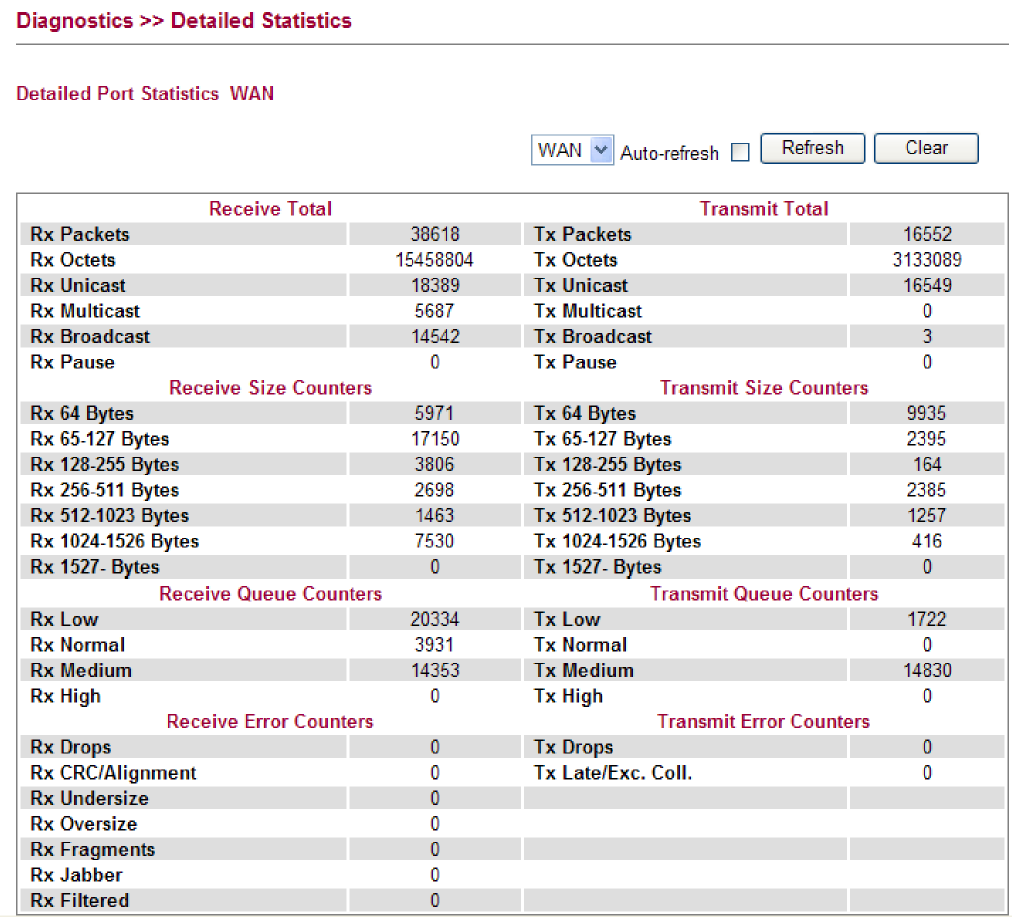
Auto-refresh Check it to enable auto-refresh function.

Refresh Click it to reload the page.

Clear Click it to clear the counters for all ports.

4.13.5 Detailed Statistics

This page display detailed statistics for WAN/LAN interface.



Diagnostics >> Detailed Statistics

Detailed Port Statistics WAN

Receive Total		Transmit Total	
Rx Packets	38618	Tx Packets	16552
Rx Octets	15458804	Tx Octets	3133089
Rx Unicast	18389	Tx Unicast	16549
Rx Multicast	5687	Tx Multicast	0
Rx Broadcast	14542	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	5971	Tx 64 Bytes	9935
Rx 65-127 Bytes	17150	Tx 65-127 Bytes	2395
Rx 128-255 Bytes	3806	Tx 128-255 Bytes	164
Rx 256-511 Bytes	2698	Tx 256-511 Bytes	2385
Rx 512-1023 Bytes	1463	Tx 512-1023 Bytes	1257
Rx 1024-1526 Bytes	7530	Tx 1024-1526 Bytes	416
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	20334	Tx Low	1722
Rx Normal	3931	Tx Normal	0
Rx Medium	14353	Tx Medium	14830
Rx High	0	Tx High	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Rx Packets Display the counting number of the packet received.

Rx Octets Display the total received bytes.

Rx Unicast Display the counting number of the received unicast packet.

Rx Broadcast Display the counting number of the received broadcast packet.

Rx Pause Display the counting number of the received pause packet.

RX 64 Bytes Display the number of 64-byte frames in good and bad packets received.

RX 65-127 Bytes Display the number of 65 ~ 127-byte frames in good and bad packets received.

RX 128-255 Bytes Display the number of 128 ~ 255-byte frames in good and bad packets received.

RX 256-511 Bytes Display the number of 256 ~ 511-byte frames in good and bad packets received.

RX 512-1023 Bytes Display the number of 512 ~ 1023-byte frames in good and bad packets received.

RX 1024- 1526 Bytes Display the number of 1024-1522-byte frames in good and bad packets received.

RX 1527 Bytes Display the number of 1527-byte frames in good and bad packets received.

Rx Low Display the low queue counter of the packet received.

Rx Normal Display the normal queue counter of the packet received.

Rx Medium Display the medium queue counter of the packet received.

Rx High Display the high queue counter of the packet received.

Rx Drops Display the number of frames dropped due to the lack of receiving buffer.

Rx CRC/Alignment Display the number of Alignment errors packets received.

Rx Undersize Display the number of short frames (<64 Bytes) with valid CRC.

Rx Oversize Display the number of long frames (according to max_length register) with valid CRC.

Rx Fragments Display the number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber Display the number of long frames (according tomax_length register) with invalid CRC.

Rx Filtered Display the filtered number of the packet received.

Tx Packets Display the counting number of the packet transmitted.

Tx Octets Display the total transmitted bytes.

Tx Unicast Display the show the counting number of the transmitted unicast packet.

Tx Multicast Display the show the counting number of the transmitted multicast packet.

Tx Broadcast Display the counting number of the transmitted broadcast packet.

Tx Pause	Show the counting number of the transmitted pause packet.
Tx 64 Bytes	Display the number of 64-byte frames in good and bad packets transmitted.
Tx 65-127 Bytes	Display the number of 65 ~ 127-byte frames in good and bad packets transmitted.
Tx 128-255 Bytes	Display the number of 128 ~ 255-byte frames in good and bad packets transmitted.
Tx 256-511 Bytes	Display the number of 256 ~ 511-byte frames in good and bad packets transmitted.
Tx 512-1023 Bytes	Display the number of 512 ~ 1023-byte frames in good and bad packets transmitted.
Tx 1024- 1526 Bytes	Display the number of 1024 ~ 1522-byt frames in good and bad packets transmitted.
Tx 1527 Bytes:	Display the number of 1527-byte frames in good and bad packets transmitted.
Tx Low	Display the low queue counter of the packet transmitted.
Tx Normal	Display the normal queue counter of the packet transmitted.
Tx Medium	Display the medium queue counter of the packet received.
Tx High	Display the high queue counter of the packet received.
Tx Drops	Display the number of frames dropped due to excessive collision, late collision, or frame aging.
Tx lat/Exc.Coll.	Display the number of Frames late collision or excessive collision Error, which switch transmitted
Auto-refresh	Check it to enable auto-refresh function.
Refresh	Click it to reload the page.
Clear	Click it to clear the counters for all ports.

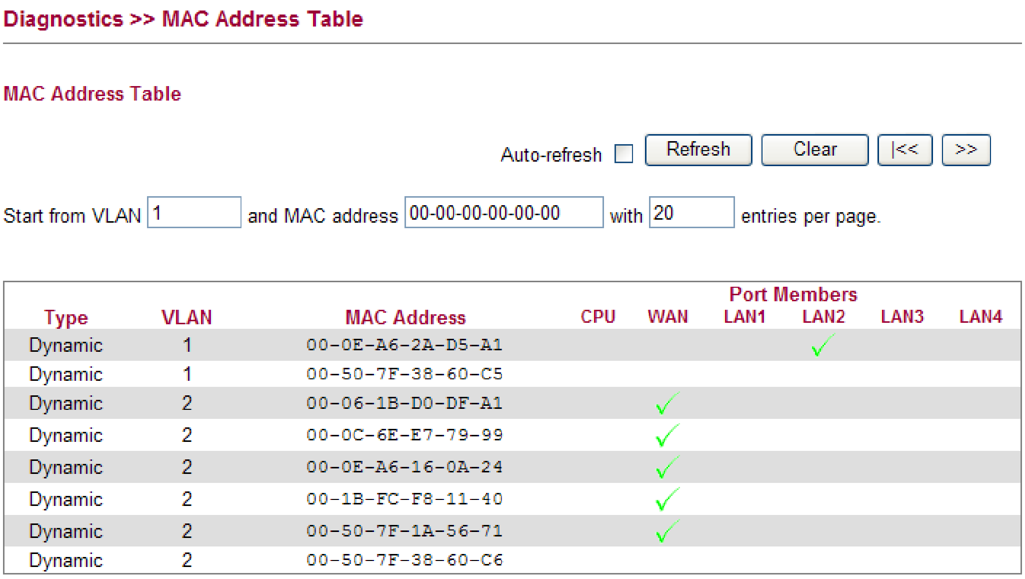
4.13.6 MAC Address Table

The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The **Start from MAC address** and **VLAN** input fields allow the user to select the starting point in the MAC Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The button >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table, use the **l<<** button to start over.



Diagnostics >> MAC Address Table

MAC Address Table

Auto-refresh □ Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

					Port Members			
Type	VLAN	MAC Address	CPU	WAN	LAN1	LAN2	LAN3	LAN4
Dynamic	1	00-0E-A6-2A-D5-A1				✓		
Dynamic	1	00-50-7F-38-60-C5						
Dynamic	2	00-06-1B-D0-DF-A1		✓				
Dynamic	2	00-0C-6E-E7-79-99		✓				
Dynamic	2	00-0E-A6-16-0A-24		✓				
Dynamic	2	00-1B-FC-F8-11-40		✓				
Dynamic	2	00-50-7F-1A-56-71		✓				
Dynamic	2	00-50-7F-38-60-C6						

Type Indicate whether the entry is a static or dynamic entry.

VLAN Display the VLAN ID of that entry.

MAC Address Display the MAC address of that entry.

Port Members Display the port of that entry.

Auto-refresh Check it to enable auto-refresh function.

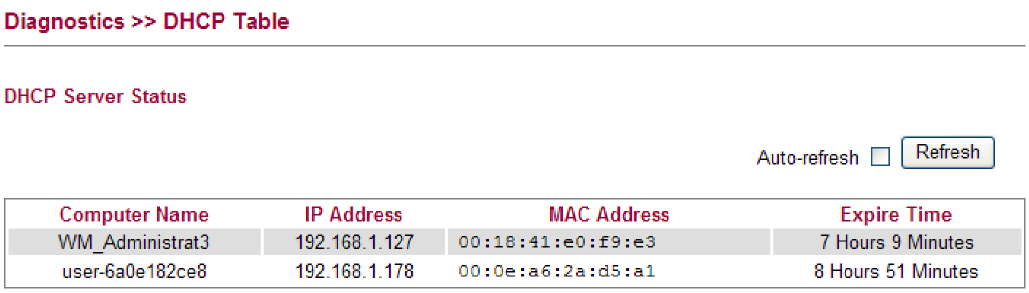
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

4.13.7 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 >> DHCP Table

DHCP Server Status

Computer Name	IP Address	MAC Address	Expire Time
WM_Administrat3	192.168.1.127	00:18:41:e0:f9:e3	7 Hours 9 Minutes
user-6a0e182ce8	192.168.1.178	00:0e:a6:2a:d5:a1	8 Hours 51 Minutes

Computer Name It displays the name of the computer accepted the assigned IP address by this router.

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.

Expire Time It displays the leased time of the specified PC.

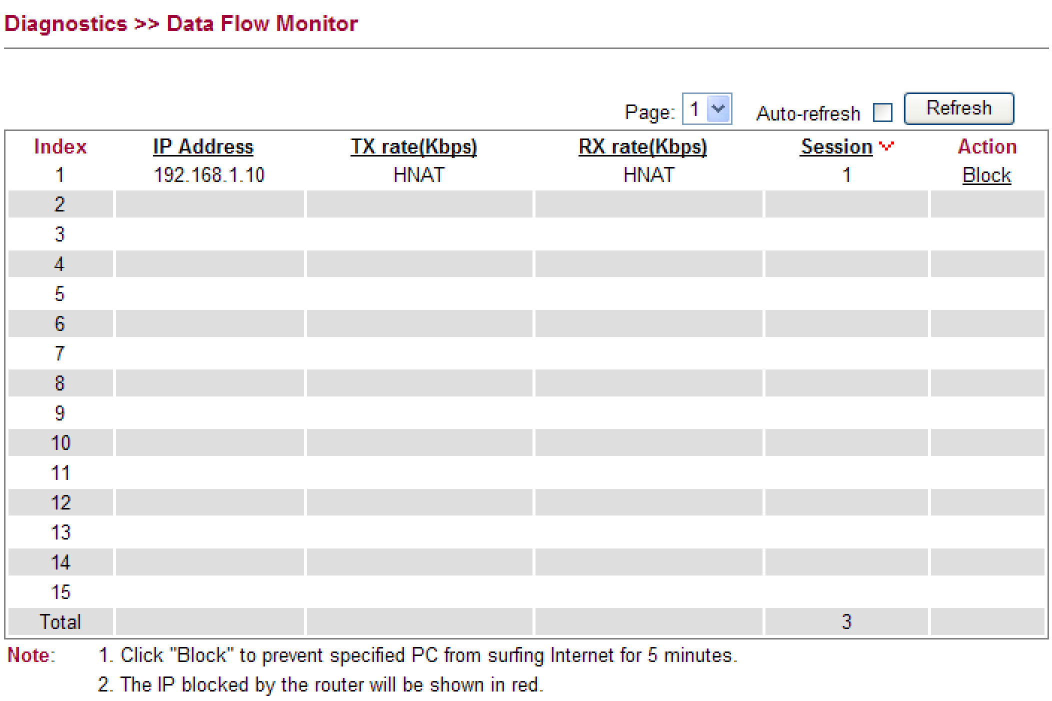
Auto-refresh Check it to enable auto-refresh function.

Refresh Click it to reload the page.

4.13.8 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

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



Diagnostics >> Data Flow Monitor

Page: 1 Auto-refresh □ Refresh

Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Session	Action
1	192.168.1.10	HNAT	HNAT	1	Block
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Total				3	

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.

Auto-refresh Check it to enable auto-refresh function.

Refresh Click this link to refresh this page manually.

Index Display the number of the data flow.

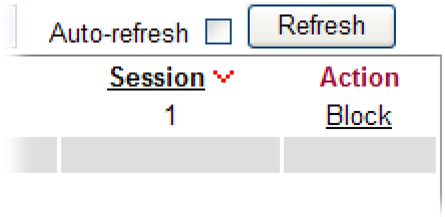
IP Address Display the IP address of the monitored device.

TX rate (kbps) Display the transmission speed of the monitored device. If "HNAT" is shown, that means the transmission is through Hardware NAT can't be computed.

RX rate (kbps) Display the receiving speed of the monitored device. If "HNAT" is shown, that means the transmission is through Hardware NAT can't be computed.

Sessions Display the session number that you specified in Limit Session web page.

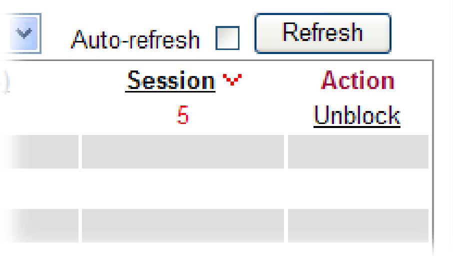
Action **Block -** can prevent specified PC accessing into Internet within 5 minutes.



Auto-refresh □ Refresh

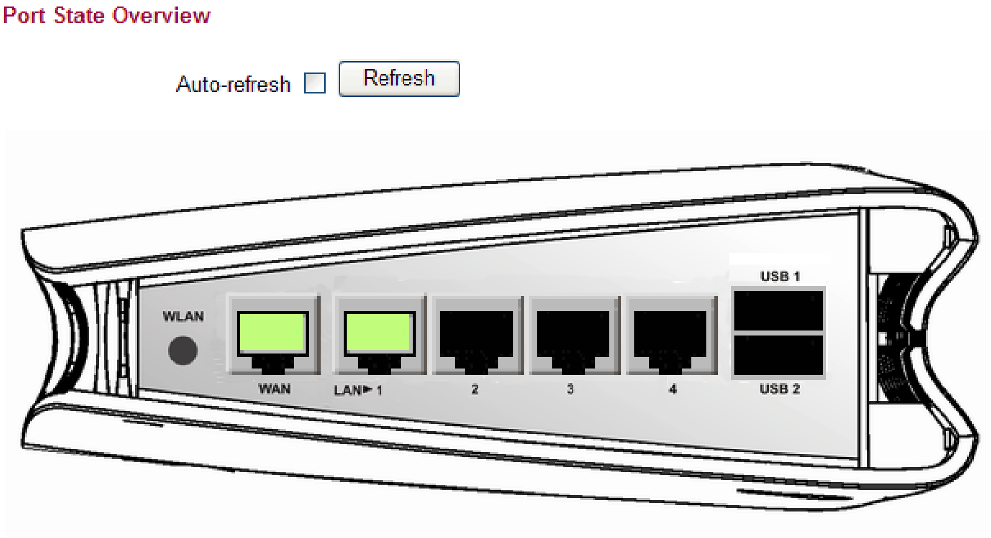
Session	Action
1	Block

Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.



4.13.9 Ports State

Click **Diagnostics** and click **Ports State** to open the list page. There are for LAN ports and one WAN port in your router. Through this page, you can know which port is using and you can get the detailed statistics for each port by moving and clicking the mouse on the connected one.



Auto-refresh Check it to enable auto-refresh function.

Refresh Click it to reload the page if you change the LAN port connection. Or you can check Auto-refresh to reload the page by the system automatically.

This page is left blank.

5 Trouble Shooting

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

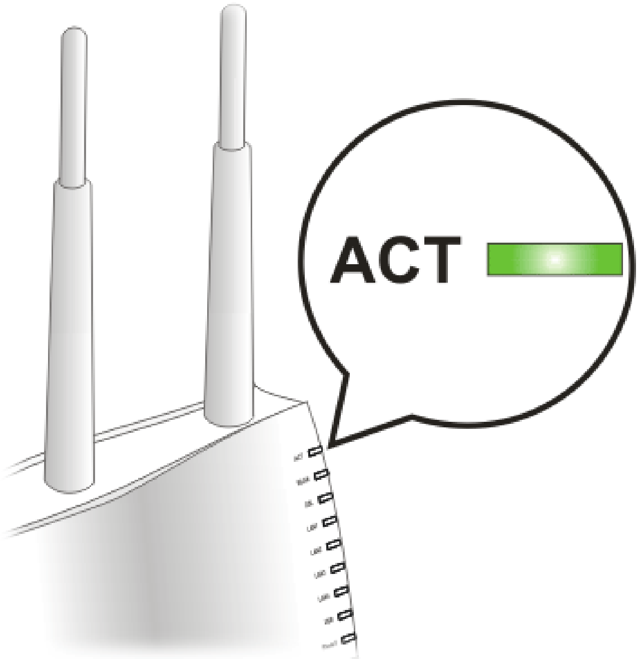
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to “**1.3 Hardware Installation**” for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **“1.3 Hardware Installation”** to execute the hardware installation again. And then, try again.

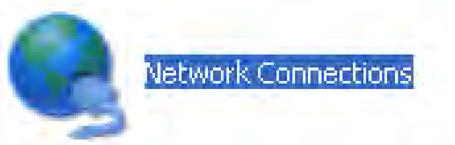
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

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

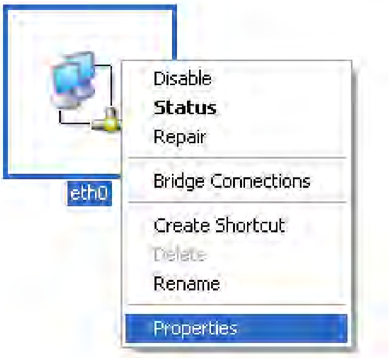
For Windows

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

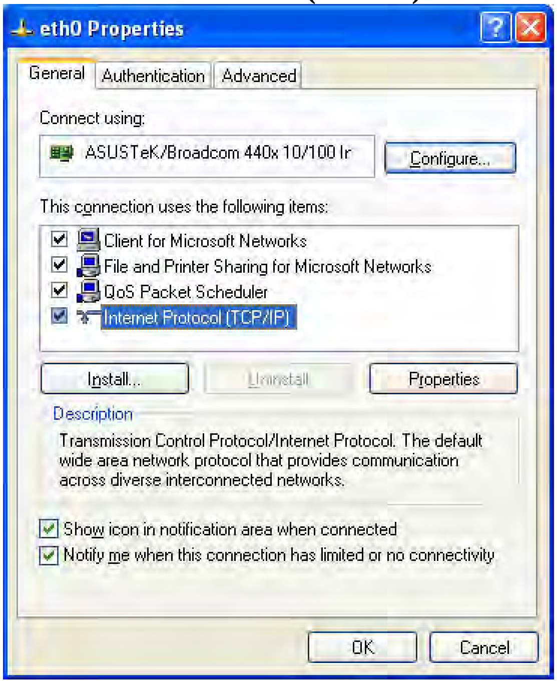
1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on **Local Area Connection** and click on **Properties**.



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



eth0 Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir [Configure...]

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

[Install...] [Uninstall] [Properties]

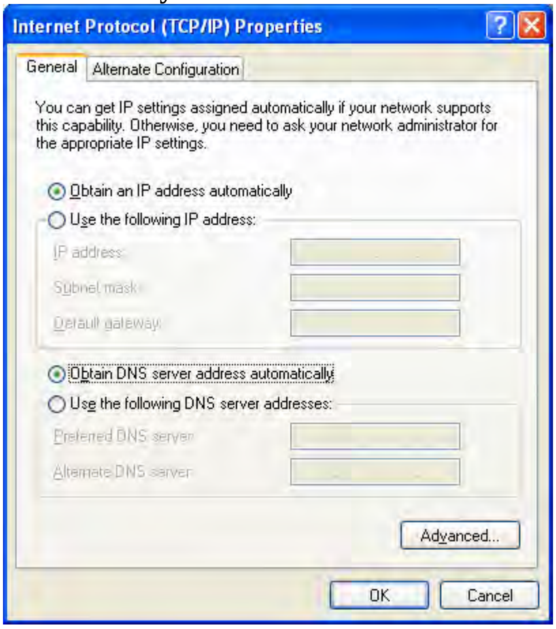
Description

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

[OK] [Cancel]

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

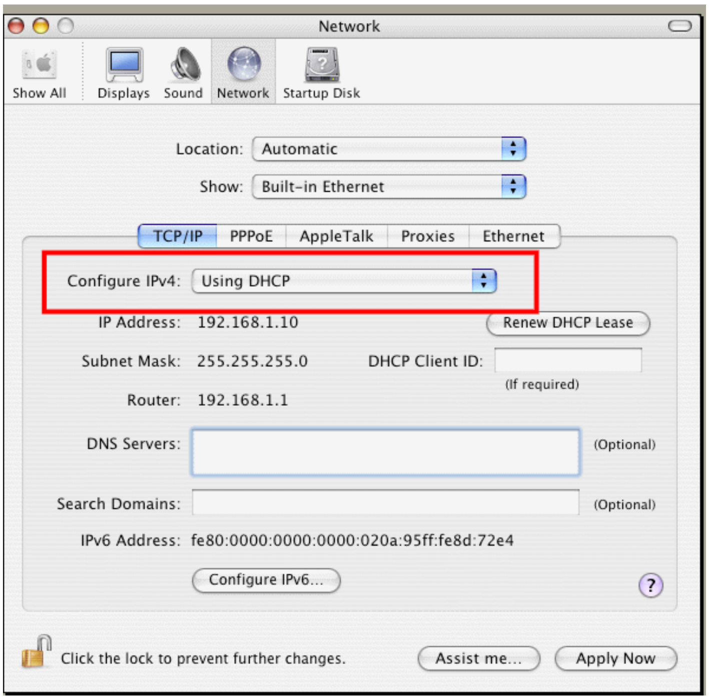
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



Location: Automatic

Show: Built-in Ethernet

TCP/IP | PPPoE | AppleTalk | Proxies | 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.

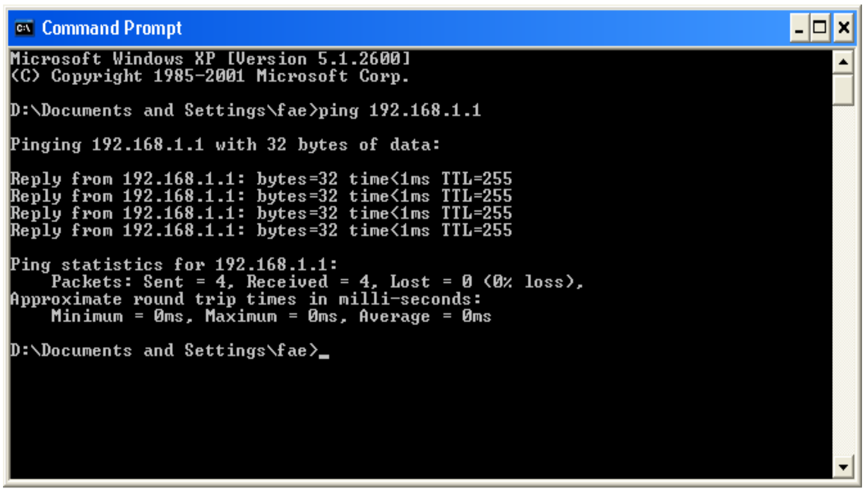
5.3 Pinging the Router from Your Computer

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

Please follow the steps below to ping the router correctly.

For Windows

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

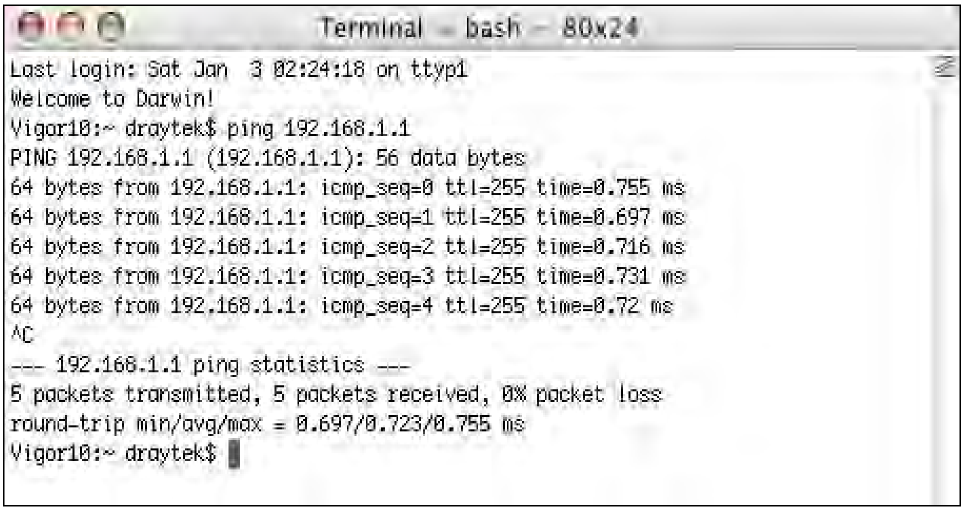


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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 MacOs (Terminal)

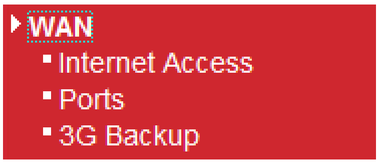
1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0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

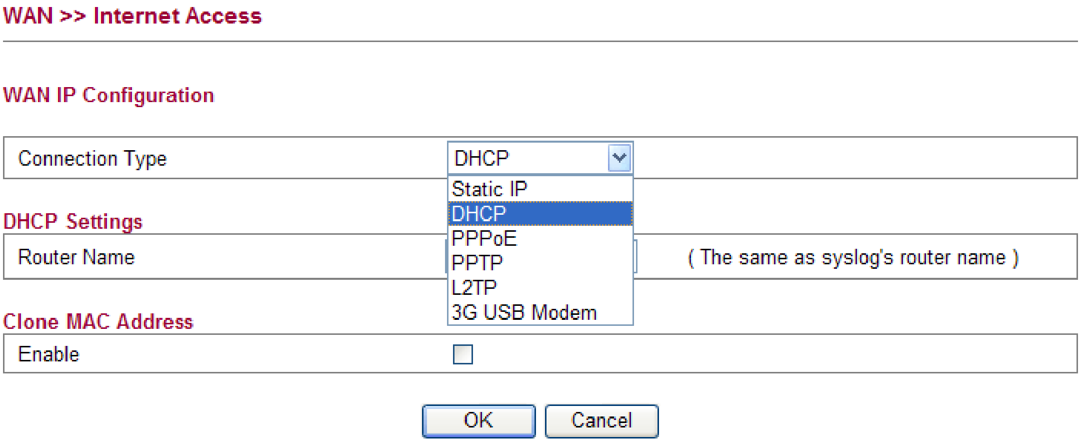


```
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 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$
```

5.4 Checking If the ISP Settings are OK or Not

Open **WAN>>Internet Access** page and then check whether the ISP settings are set correctly. Use the Connection Type drop down list to choose Static IP/DHCP/PPPoE/PPTP/L2TP for reviewing the settings that you configured previously.





WAN >> Internet Access

WAN IP Configuration

Connection Type	DHCP

DHCP Settings

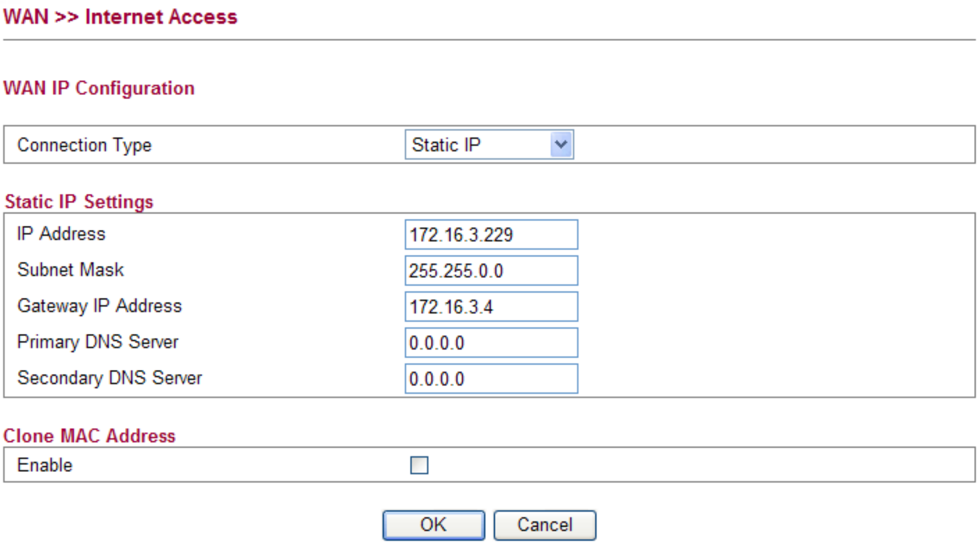
Router Name	(The same as syslog's router name)

Clone MAC Address

Enable	□

For Static Users

1. Choose **Static IP** as the connection type.



WAN >> Internet Access

WAN IP Configuration

Connection Type	Static IP

Static IP Settings

IP Address	172.16.3.229
Subnet Mask	255.255.0.0
Gateway IP Address	172.16.3.4
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

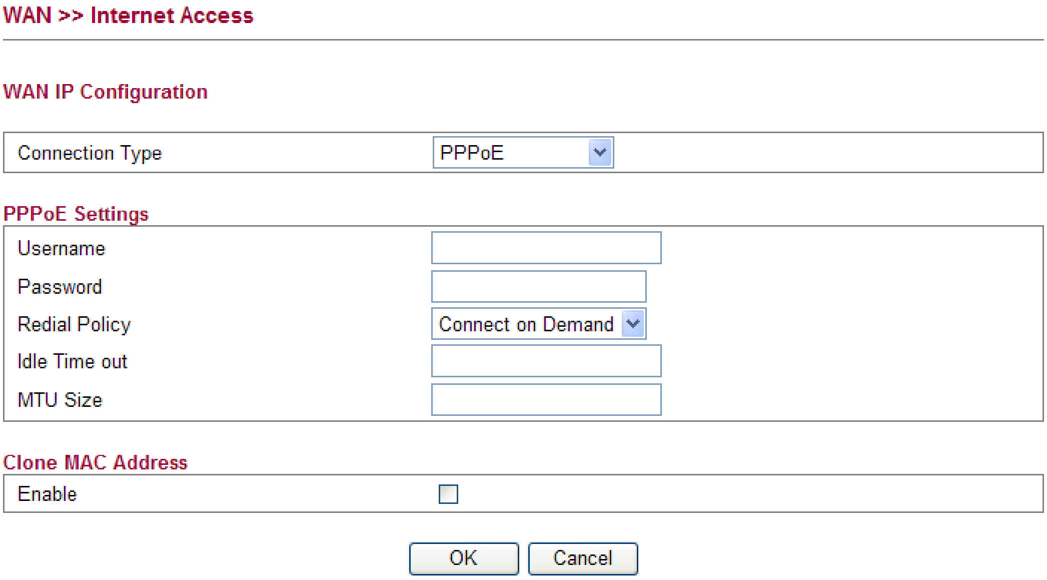
Clone MAC Address

Enable	□

2. Check if **IP Address, IP Mask** and **IP Router** are set correctly (must identify with the values from your ISP).

For PPPoE Users

1. Choose **PPPoE** as the connection type.



WAN >> Internet Access

WAN IP Configuration

Connection Type	PPPoE

PPPoE Settings

Username	
Password	
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	

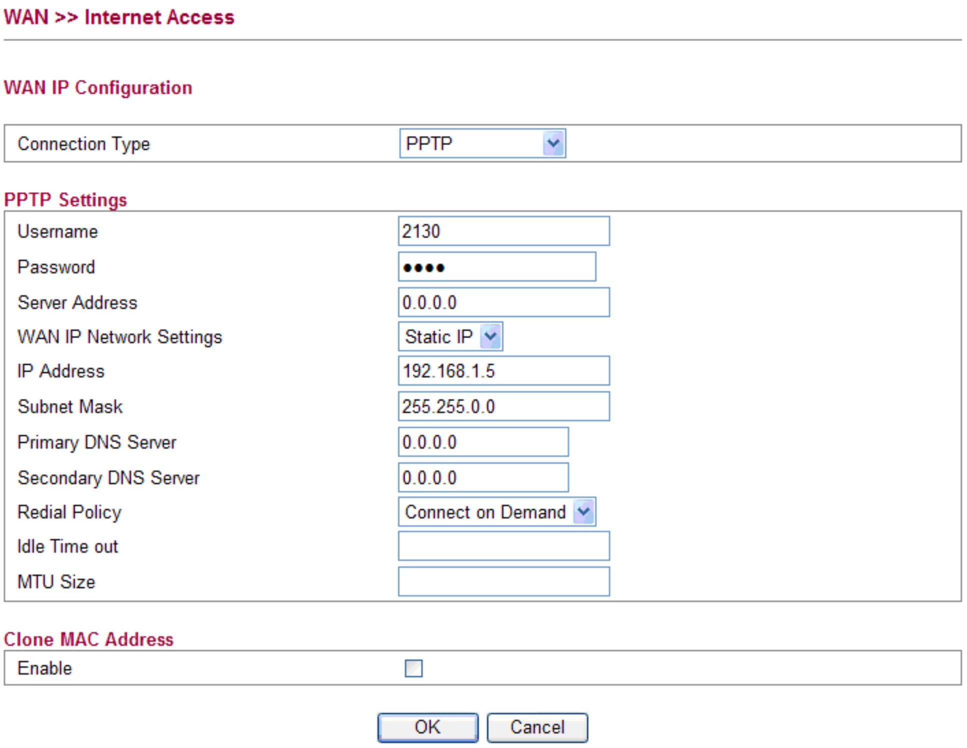
Clone MAC Address

Enable	□

2. Check if **Username** and **Password** are set correctly (must identify with the values from your ISP).

For PPTP/L2TP Users

1. Choose **PPTP/L2TP** as the connection type.



WAN >> Internet Access

WAN IP Configuration

Connection Type	PPTP

PPTP Settings

Username	2130
Password	••••
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	192.168.1.5
Subnet Mask	255.255.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	

Clone MAC Address

Enable	□

2. Check if **Username**, **Password, IP address, Subnet Mask** are entered with correct values that you **get from** your **ISP**.

5.5 Forcing Vigor Router into TFTP Mode for Performing the Firmware Upgrade

1. Press and hold the **Factory Reset** button. The system will power off and power on the Vigor Router.

2. Release the **Factory Reset** button when the ACT LED and its neighbor LED blink simultaneously.

   There are different LED blinking methods in describing TFTP mode status:
   Vigor2130: ACT LED & its neighbor LED blink simultaneously.

3. Change your PC IP address to 192.168.1.10.

4. Open **Firmware Upgrade Utility** and key in Router IP 192.168.1.1 manually.

5. Install **Router Tools** on one computer that connects to Vigor Router's LAN port.

6. Make sure the computer can ping Vigor's LAN IP. (Default IP is 192.168.1.1)

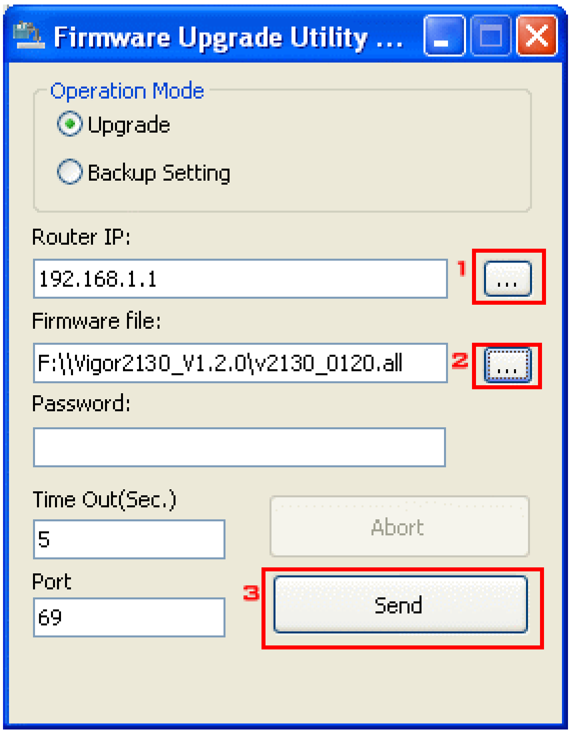
7. Run **Router Tools** >> **Firmware Upgrade Utility**.

8. Input Vigor's LAN IP manually or use the **. .** .button to select.

9. Indicate the firmware location.

> **Note:** There are two firmware types. The *.rst* firmware format will make the configurations be back to default settings after upgrading firmware. The *.all* firmware format will remain the former configurations after upgrading firmware.

10. Input the Password if you have set one, then click **Send**.



Firmware Upgrade Utility ...

Operation Mode

● Upgrade

○ Backup Setting

Router IP: 192.168.1.1

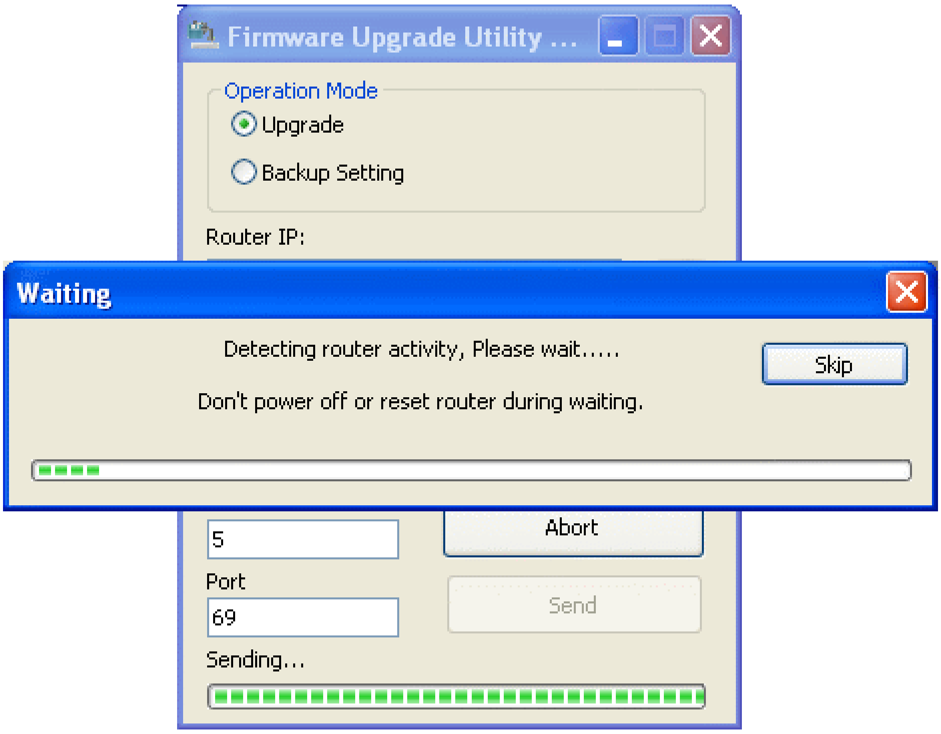
Firmware file: F:\\Vigor2130_V1.2.0\v2130_0120.all

Password:

Time Out(Sec.): 5

Port: 69

11. There is a bar showing the upgrading process.



Firmware Upgrade Utility ...

Operation Mode

● Upgrade

○ Backup Setting

Router IP:

Waiting

Detecting router activity, Please wait.....

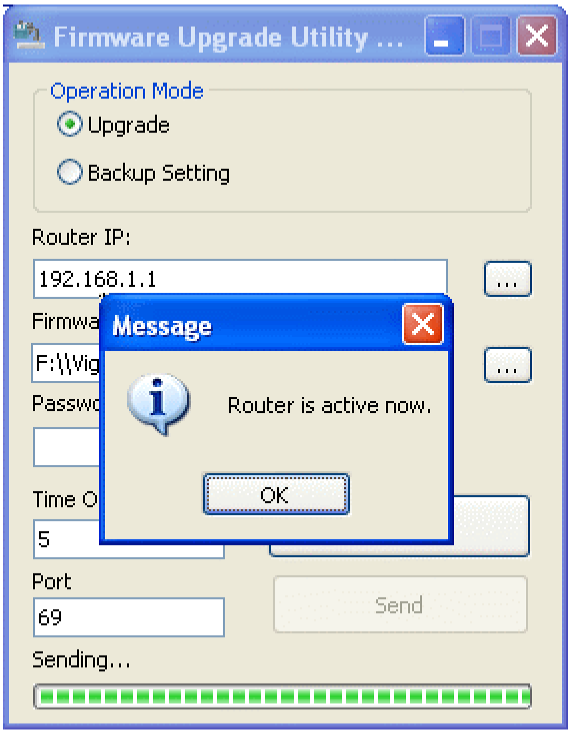
Don't power off or reset router during waiting.

5

Port: 69

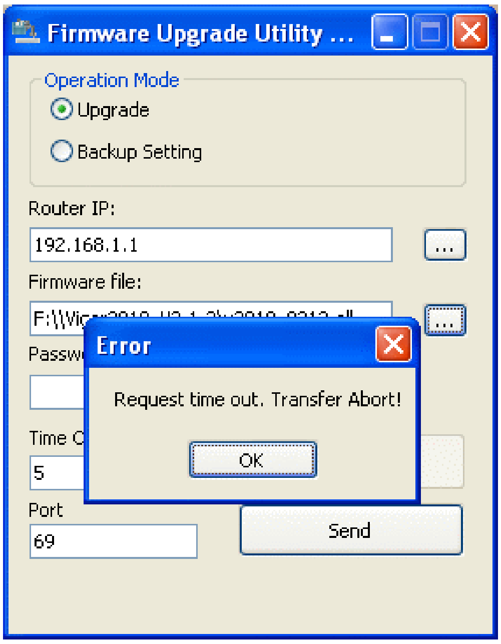
Sending...

12. When the firmware upgrade is successful, the following window will pop up.

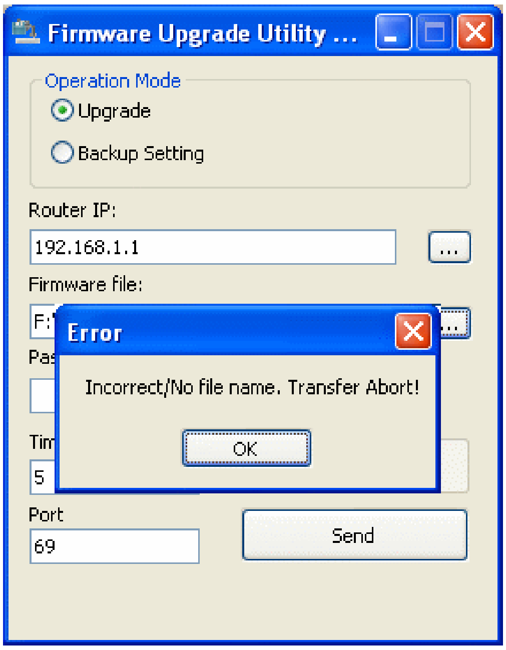


Router is active now.

If the message of **Request Timeout. Transfer Abort !** appears, please check if the connection between the computer and the Vigor is active or not. And, if the message of **Incorrect/No file name. Transfer Abort !** appears, please check if the firmware you download is correct for your Vigor router.



Request time out. Transfer Abort!



Incorrect/No file name. Transfer Abort!

Note: Please turn off the Firewall protection while upgrading the firmware with Windows Vista. The Firewall function can be turned off via **Control Panel** >> **Security Center** >> **Firewall**.

5.6 Backing to Factory Default Setting If Necessary

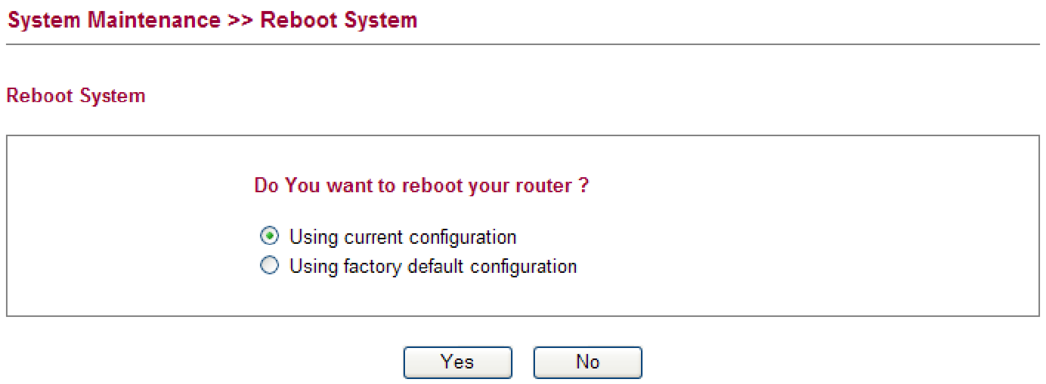
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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

Software Reset

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

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

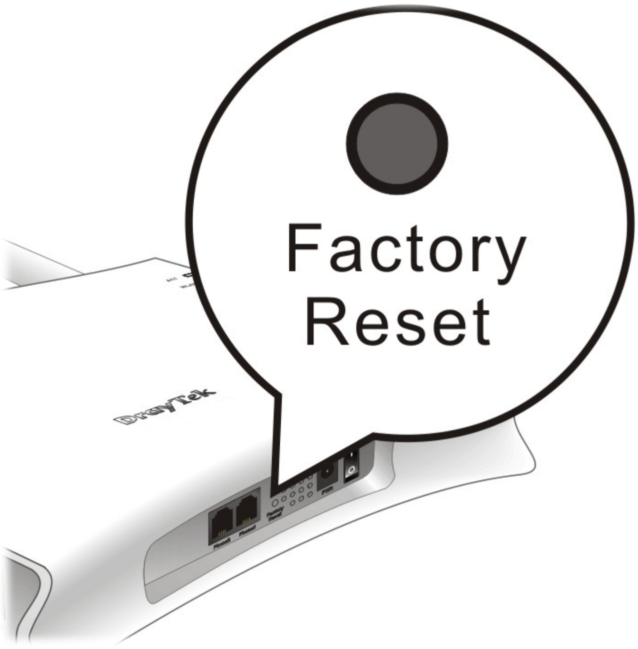
Do You want to reboot your router ?

● 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.

5.7 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.