DrayTek

Vigor1000 Series

High Speed Gigabit Fiber Router

Your reliable networking solutions partner

User's Guide

V1.0

Vigor1000 Series
High Speed Gigabit Fiber Router
User's Guide

Version: 1.0

Firmware Version: V1.5.2_RC1M

Date: 12/01/2012

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: Vigor1000 Series Router

DrayTek Corp. declares that Vigor1000 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 Vigor1000 series are the routers with high speed in data transmission through WAN port and LAN ports. With hardware NAT acceleration, the rate of Vigor1000 series can be ideal for multi-media application.

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 Vigor1000 series –High speed Gigabit router, perfectly complied with VDSL2 environment including Vigor1000, Vigor1000n and Vigor1000Vn for speed-wanted customers. With high throughput performance and secured broadband connectivity provided by Vigor1000 series, you can simultaneously engage these bandwidth-intensive applications, such as high-definition video streaming, online gaming, and Internet telephony access.

1.1 Features

- Fiber (WAN) port and embedded hardware NAT deliver ultra-fast speed from WAN to LAN
- LAN ports stream content to wired devices with unprecedented speeds
- 2 USB ports provides fast access to an external USB hard drive
- Embedded DLNA server/iTune server supports stream content to Media Players
- Up to 800 Mpbs throughput for downstream
- Advanced QoS for Data, Music, VoIP and Video
- Easy-to-use firewall
- VoIP facilities for low cost call (V model)

1.2 Web Configuration Buttons Explanation

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

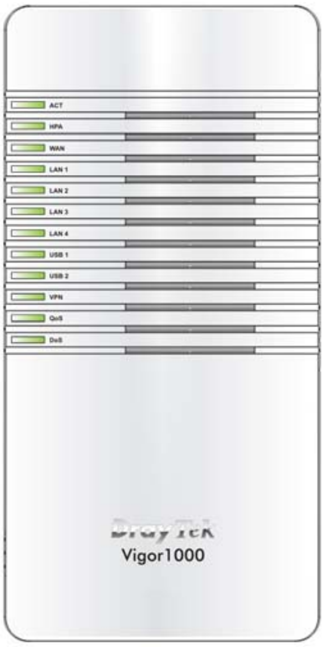
OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified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

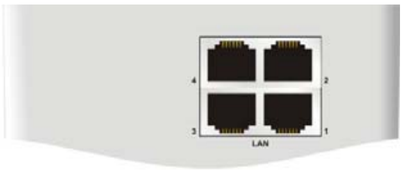
1.3 LED Indicators and Connectors

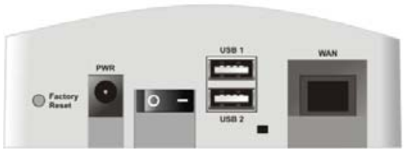
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

1.3.1 For Vigor1000



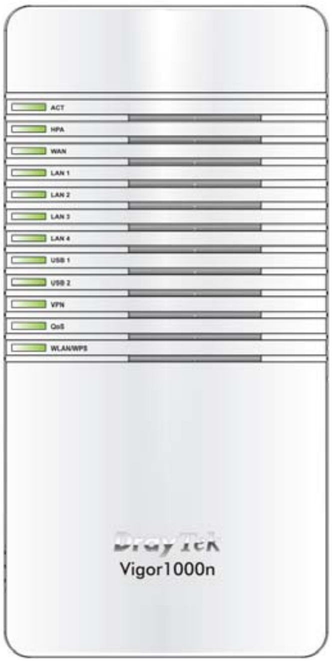
LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
HPA (Hardware Packet Accelerate)	On	Hardware NAT is enabled.
	Off	Hardware NAT is disabled.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.
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.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
DoS	On	The DoS/DDoS function is active.



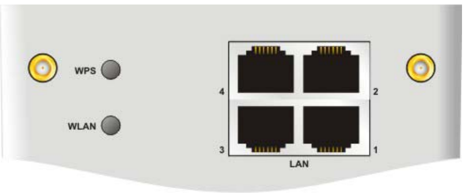


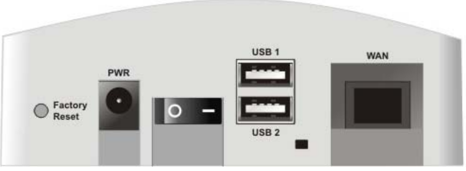
Interface	Description
LAN (1-4)	Connectors for local networked devices.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector for a power adapter.
ON/OFF	Power switch.
USB (1-2)	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.
WAN	Connector for accessing the Internet.

1.3.2 For Vigor1000n



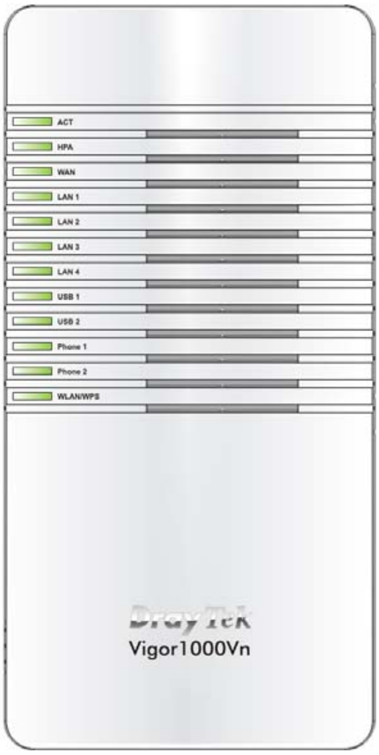
LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
HPA (Hardware Packet Accelerate)	On	Hardware NAT is enabled.
	Off	Hardware NAT is disabled.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.
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.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
WLAN /WPS	On (Green)	Wireless access point is ready.
	Blinking (Green)	Data transmitting via WLAN.
	Blinking (Orange)	Quickly: WPS function is enabled. Slowly: Data transmitting via WPS.
	Off	Wireless access point is turned off.



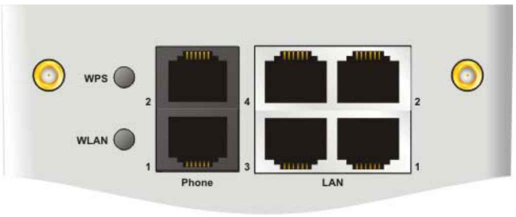


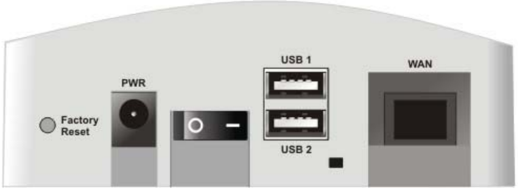
Interface	Description
WPS	Press WPS Button to wait for client device making network connection through WPS. When the LED lights up, the WPS connection will be on.
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
LAN (1-4)	Connectors for local networked devices.
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.
USB (1-2)	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.
WAN	Connector for accessing the Internet.

1.3.3 For Vigor1000Vn



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
HPA (Hardware Packet Accelerate)	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/ WPS	On (Green)	Wireless access point is ready.
	Blinking (Green)	Data transmitting via WLAN.
	Blinking (Orange)	Quickly: WPS function is enabled. Slowly: Data transmitting via WPS.
	Off	Wireless access point is turned off.



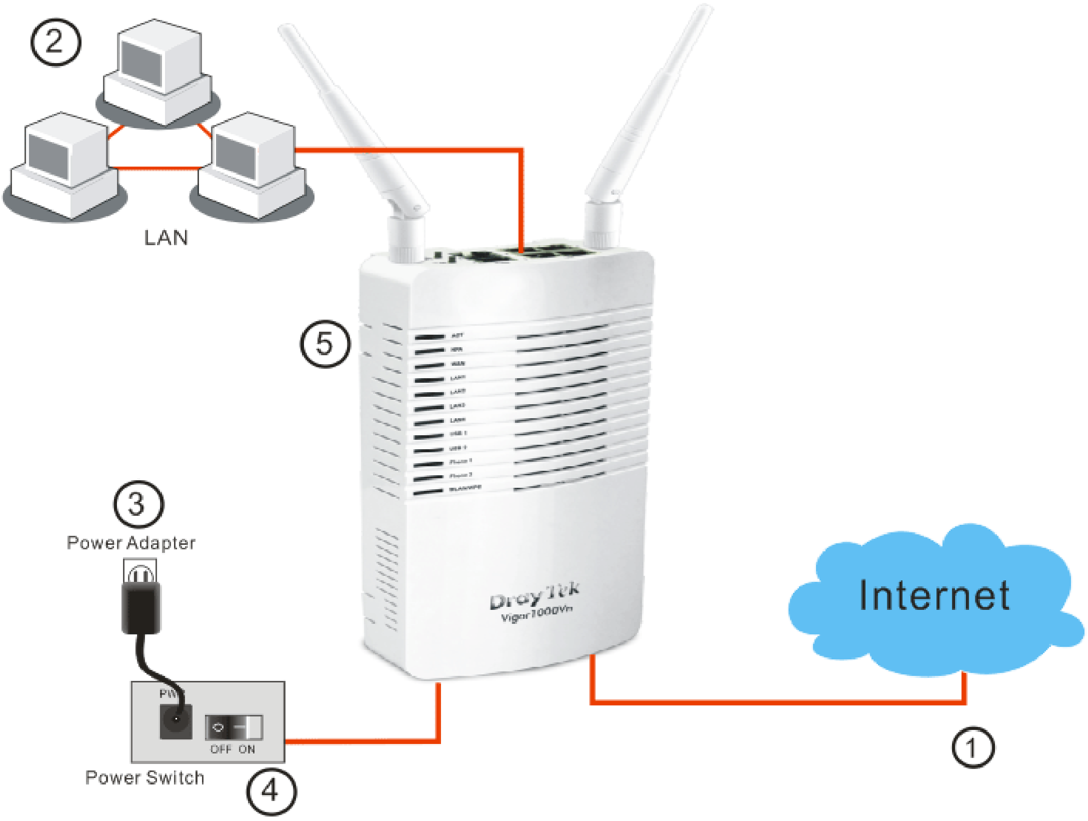


Interface	Description
WPS	Press WPS Button to wait for client device making network connection through WPS. When the LED lights up, the WPS connection will be on.
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Phone2/Phone1	Connector of analog phone for VoIP communication.
LAN (1-4)	Connectors for local networked devices.
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.
USB (1-2)	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.
WAN	Connector for accessing the Internet.

1.4 Hardware Installation

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

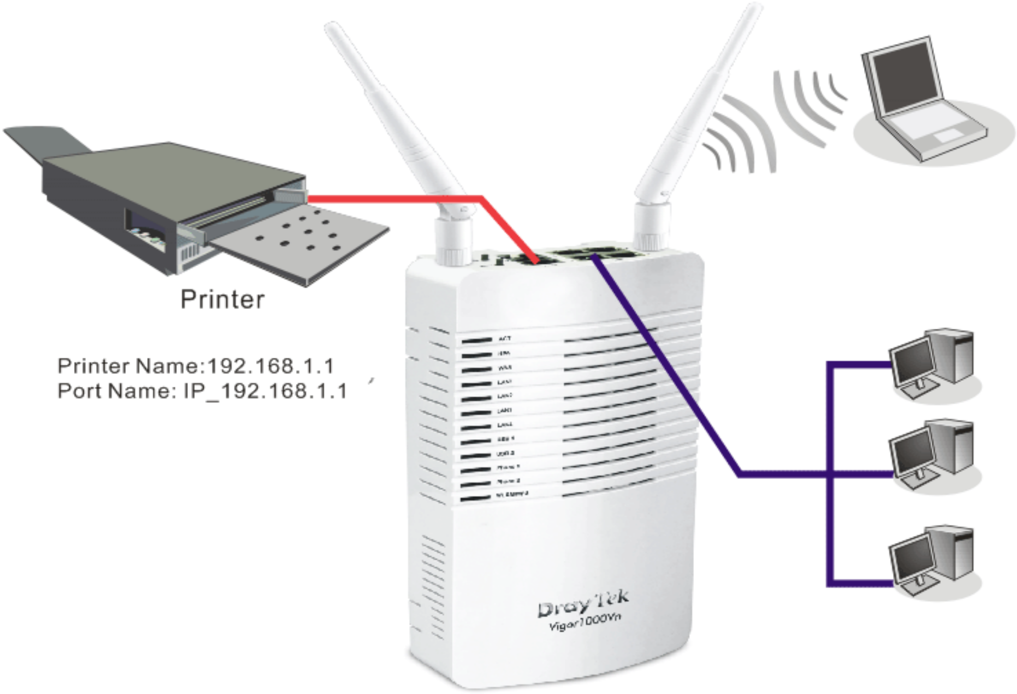
1. Connect the fiber-optic cable to this device.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the router.
5. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connections.



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

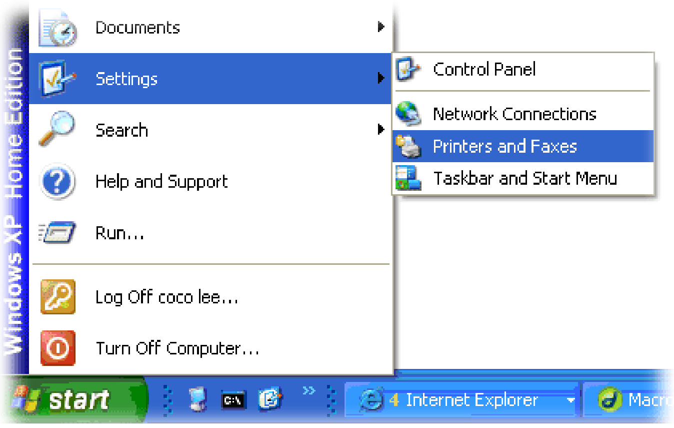
1.5 Printer Installation

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**.

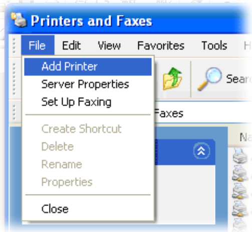


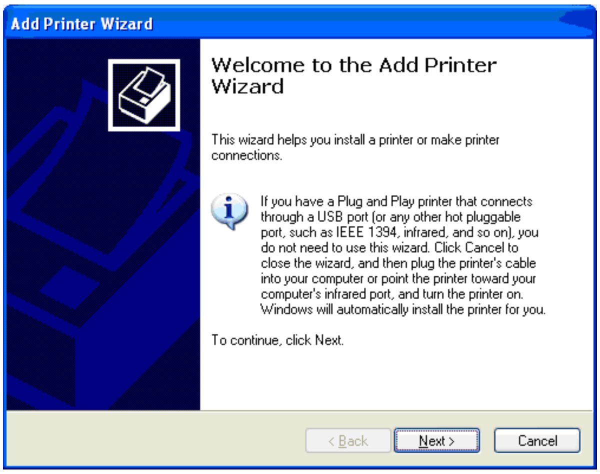
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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**.





Add Printer Wizard

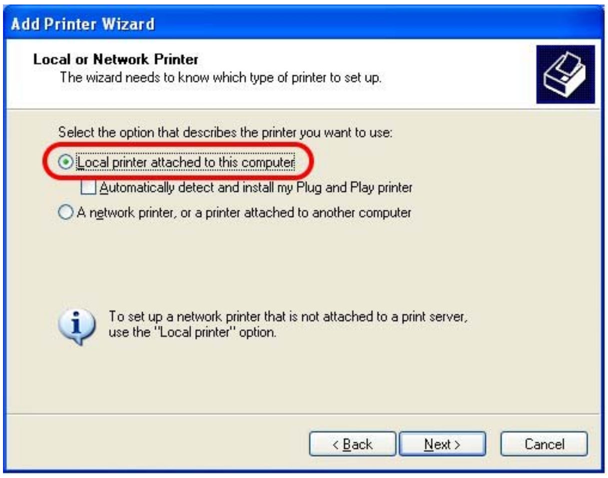
Welcome to the Add Printer Wizard

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

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

To continue, click Next.

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



Add Printer Wizard

Local or Network Printer

The wizard needs to know which type of printer to set up.

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

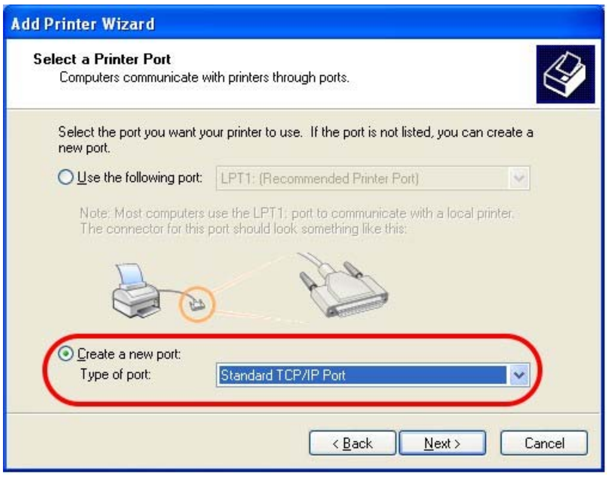
● Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

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

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



Add Printer Wizard

Select a Printer Port

Computers communicate with printers through ports.

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

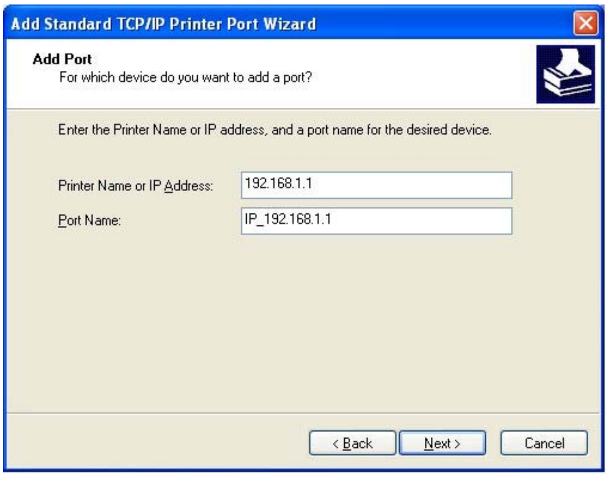
○ Use the following port: LPT1: (Recommended Printer Port)

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

● Create a new port:

Type of port: Standard TCP/IP Port

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



Add Port

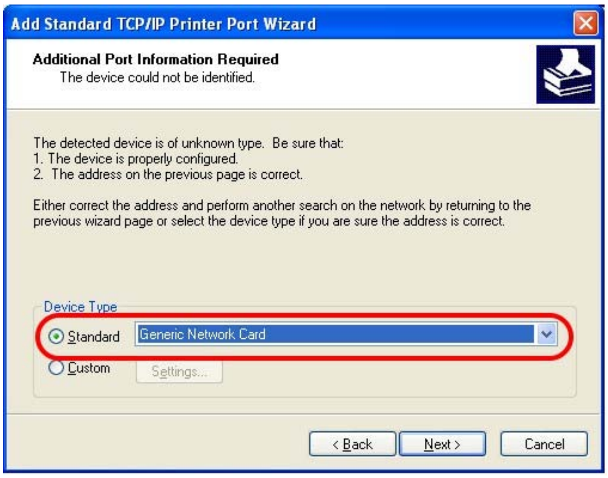
For which device do you want to add a port?

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.



Additional Port Information Required

The device could not be identified.

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

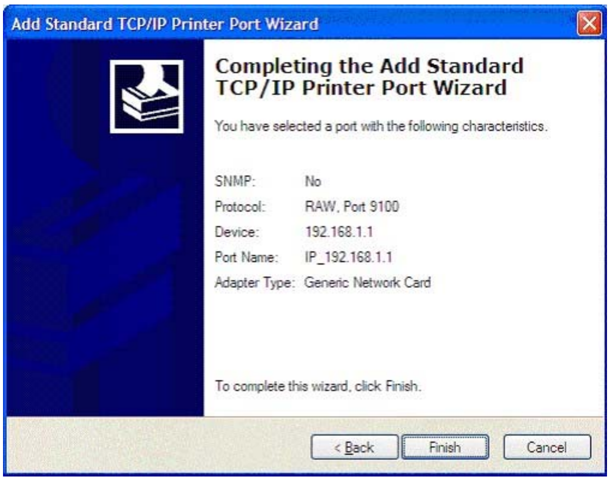
Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type

● Standard: Generic Network Card

○ Custom

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



Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP: No

Protocol: RAW, Port 9100

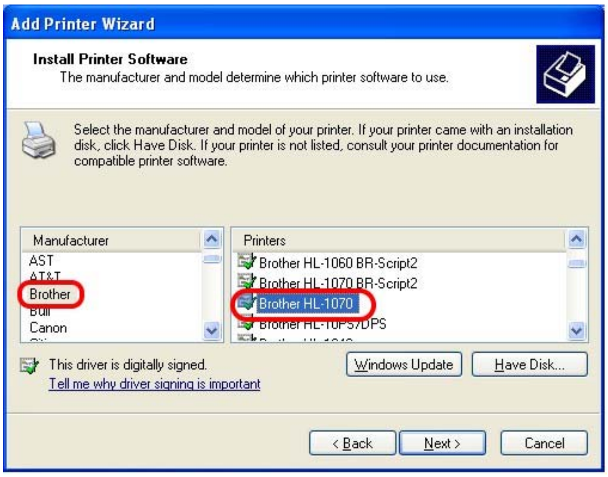
Device: 192.168.1.1

Port Name: IP_192.168.1.1

Adapter Type: Generic Network Card

To complete this wizard, click Finish.

9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



Add Printer Wizard

Install Printer Software

The manufacturer and model determine which printer software to use.

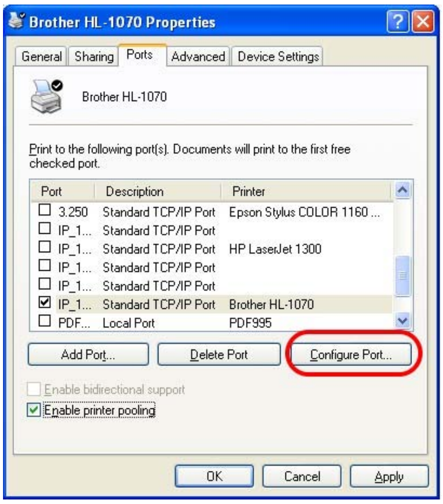
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

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

This driver is digitally signed.

Tell me why driver signing is important

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



Brother HL-1070 Properties

Brother HL-1070

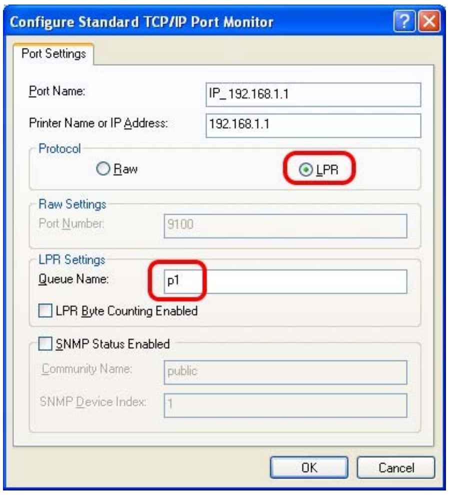
Print to the following port(s). Documents will print to the first free checked port.

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

☐ Enable bidirectional support

☑ Enable printer pooling

11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: p1

☐ LPR Byte Counting Enabled

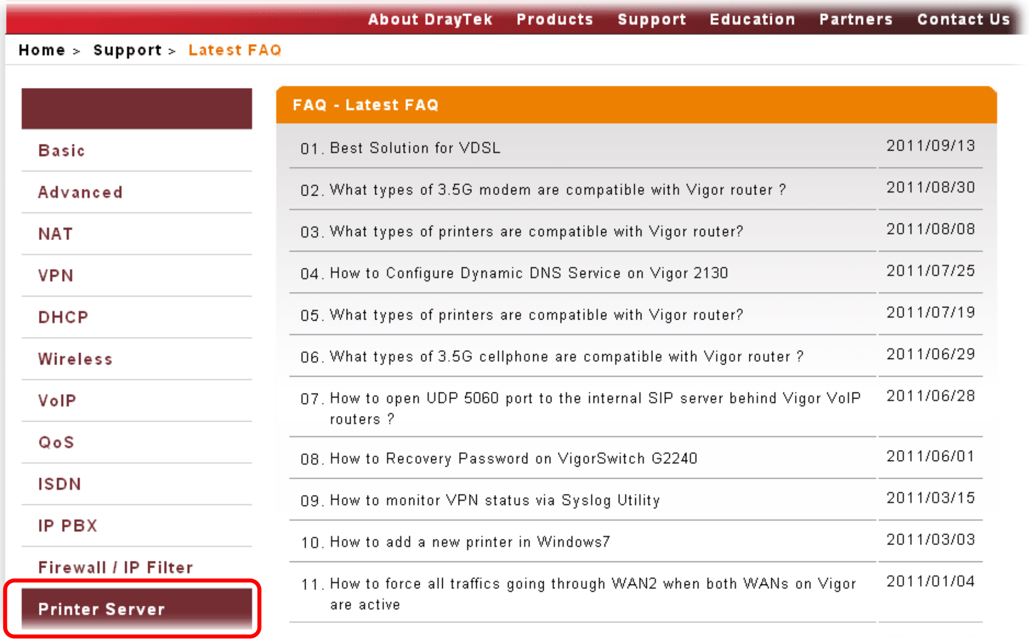
☐ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

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

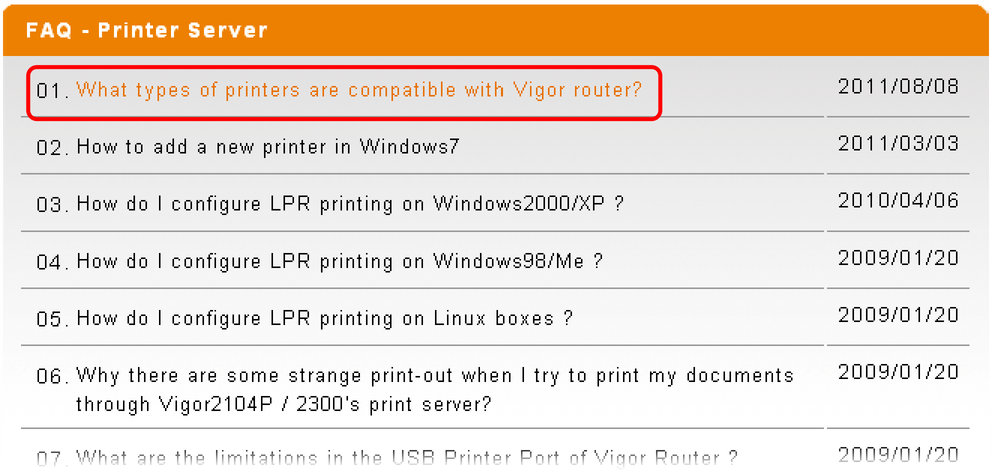
Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ**; find out the link of **Printer Server** and click it.



FAQ - Latest FAQ

01. Best Solution for VDSL	2011/09/13
02. What types of 3.5G modem are compatible with Vigor router ?	2011/08/30
03. What types of printers are compatible with Vigor router?	2011/08/08
04. How to Configure Dynamic DNS Service on Vigor 2130	2011/07/25
05. What types of printers are compatible with Vigor router?	2011/07/19
06. What types of 3.5G cellphone are compatible with Vigor router ?	2011/06/29
07. How to open UDP 5060 port to the internal SIP server behind Vigor VoIP routers ?	2011/06/28
08. How to Recovery Password on VigorSwitch G2240	2011/06/01
09. How to monitor VPN status via Syslog Utility	2011/03/15
10. How to add a new printer in Windows7	2011/03/03
11. How to force all traffics going through WAN2 when both WANs on Vigor are active	2011/01/04

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



FAQ - Printer Server

01. What types of printers are compatible with Vigor router?	2011/08/08
02. How to add a new printer in Windows7	2011/03/03
03. How do I configure LPR printing on Windows2000/XP ?	2010/04/06
04. How do I configure LPR printing on Windows98/Me ?	2009/01/20
05. How do I configure LPR printing on Linux boxes ?	2009/01/20
06. Why there are some strange print-out when I try to print my documents through Vigor2104P / 2300's print server?	2009/01/20
07. What are the limitations in the USB Printer Port of Vigor Router ?	2009/01/20

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

2 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.

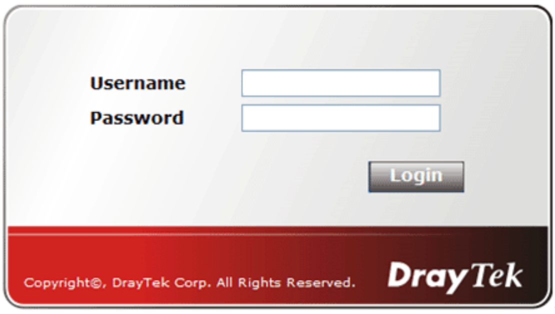
This chapter explains how to setup a password for accessing into the web configurator of Vigor router and how to adjust settings for accessing Internet successfully.

2.1 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.

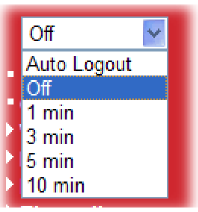
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.



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

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

4. 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.



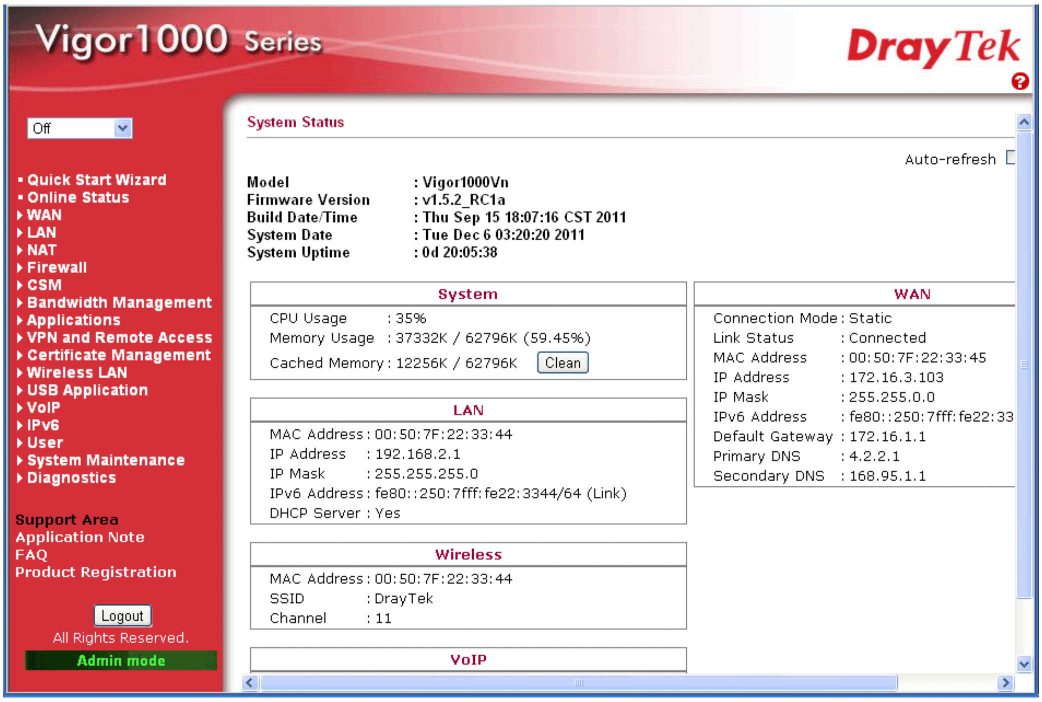
2.2 Changing Password

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

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

2. Please type “admin/admin” as Username/Password for accessing into the web configurator with admin mode.

3. Now, the **Main Screen** will appear.



System Status

Auto-refresh □

```
Model             : Vigor1000Vn
Firmware Version  : v1.5.2_RC1a
Build Date/Time   : Thu Sep 15 18:07:16 CST 2011
System Date       : Tue Dec 6 03:20:20 2011
System Uptime     : 0d 20:05:38
```

System

```
CPU Usage       : 35%
Memory Usage    : 37332K / 62796K (59.45%)
Cached Memory : 12256K / 62796K
```

WAN

```
Connection Mode : Static
Link Status     : Connected
MAC Address     : 00:50:7F:22:33:45
IP Address      : 172.16.3.103
IP Mask         : 255.255.0.0
IPv6 Address    : fe80::250:7fff:fe22:33
Default Gateway : 172.16.1.1
Primary DNS     : 4.2.2.1
Secondary DNS   : 168.95.1.1
```

LAN

```
MAC Address : 00:50:7F:22:33:44
IP Address    : 192.168.2.1
IP Mask       : 255.255.255.0
IPv6 Address : fe80::250:7fff:fe22:3344/64 (Link)
DHCP Server : Yes
```

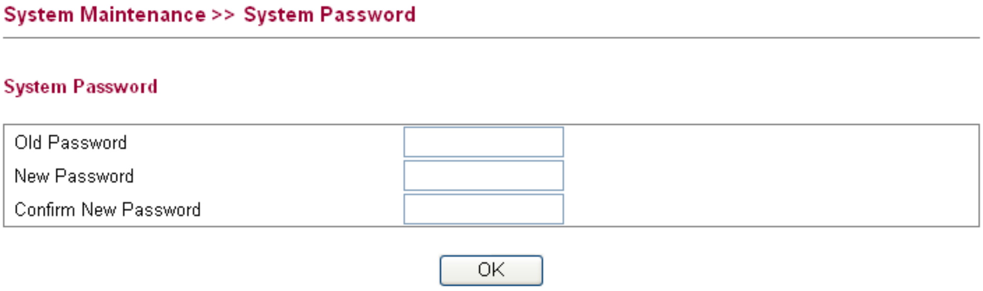
Wireless

```
MAC Address : 00:50:7F:22:33:44
SSID          : DrayTek
Channel       : 11
```

VoIP

> **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**.



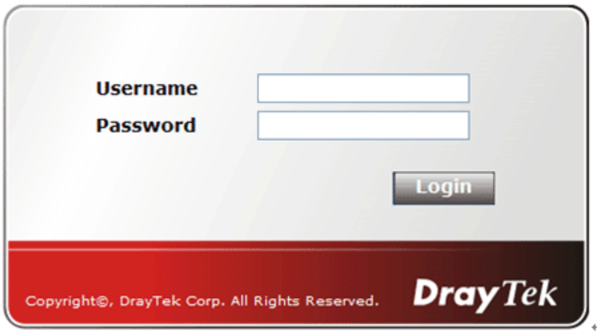
System Maintenance >> System Password

System Password

Old Password	
New Password	
Confirm New Password	

5. Type a new password in **New Password** and **Confirm New Password** fields. Then click **OK** to continue.

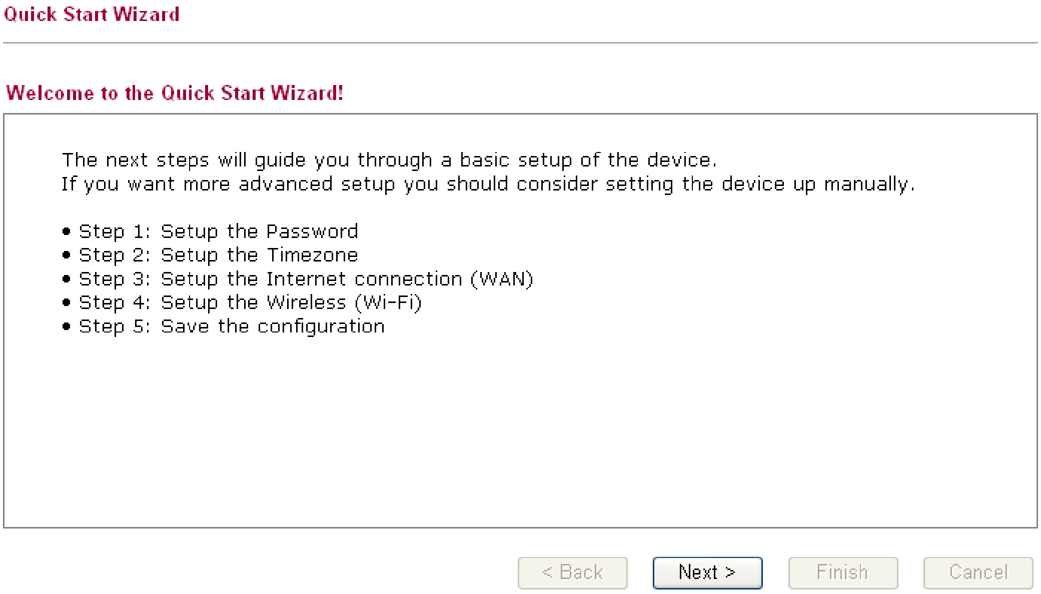
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.



2.3 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**.

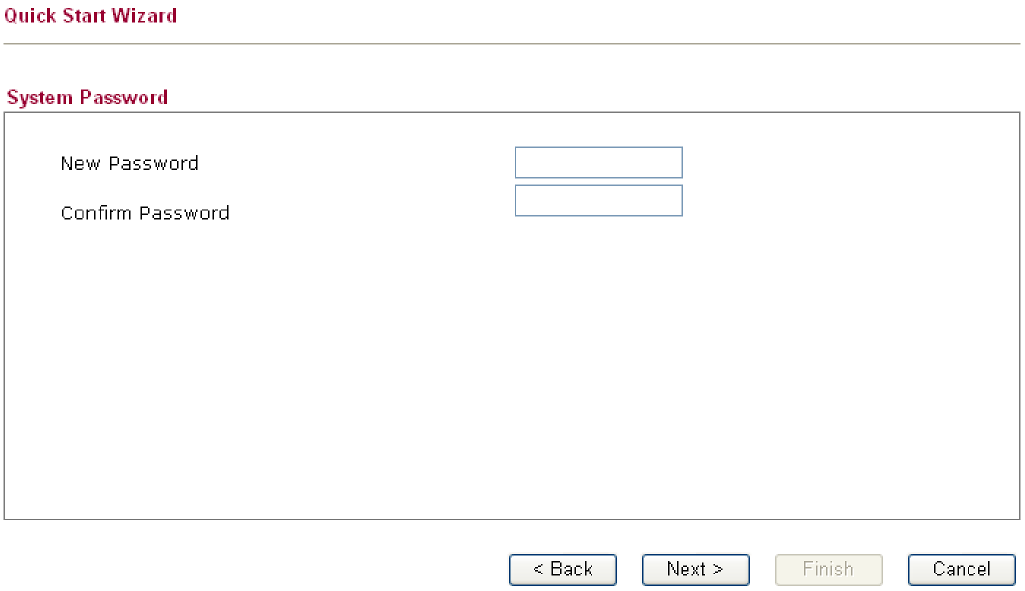


The next steps will guide you through a basic setup of the device.
If you want more advanced setup you should consider setting the device up manually.

- 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

2.3.1 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

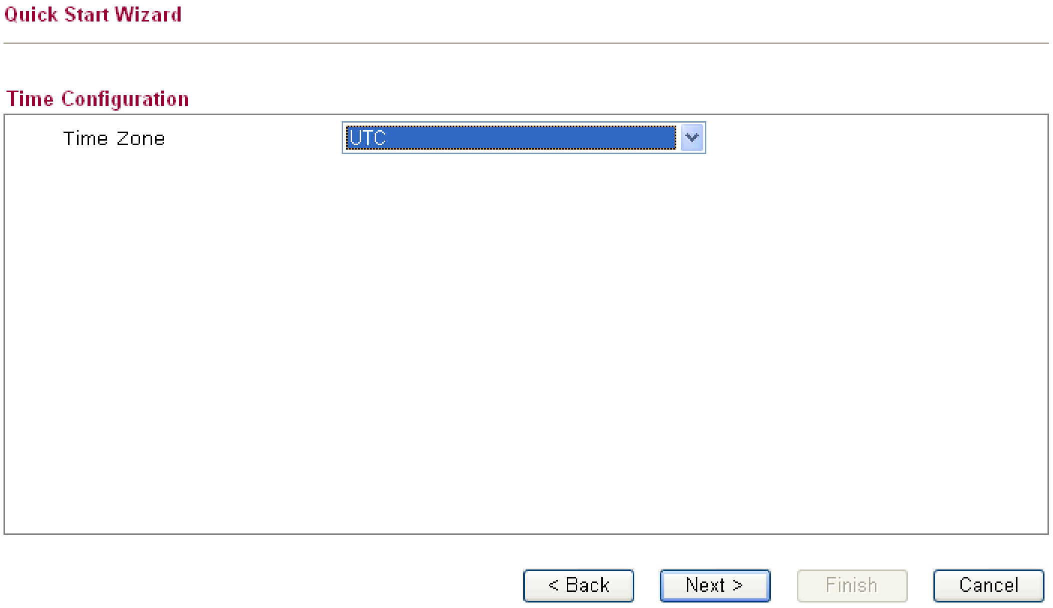
System Password

New Password

Confirm Password

2.3.2 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.



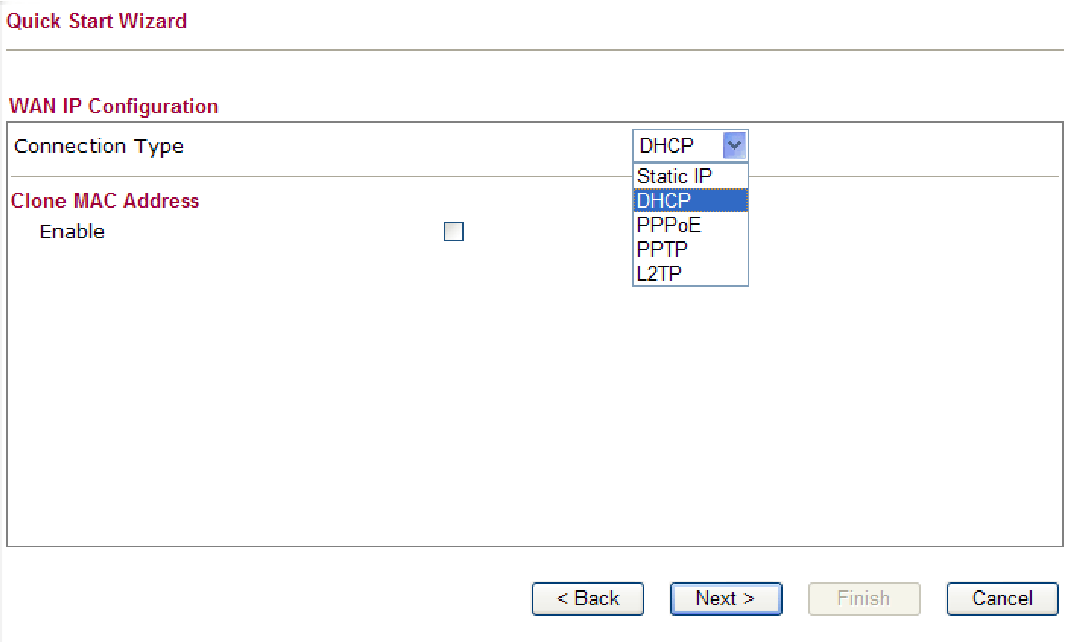
Quick Start Wizard

Time Configuration

Time Zone: UTC

2.3.3 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

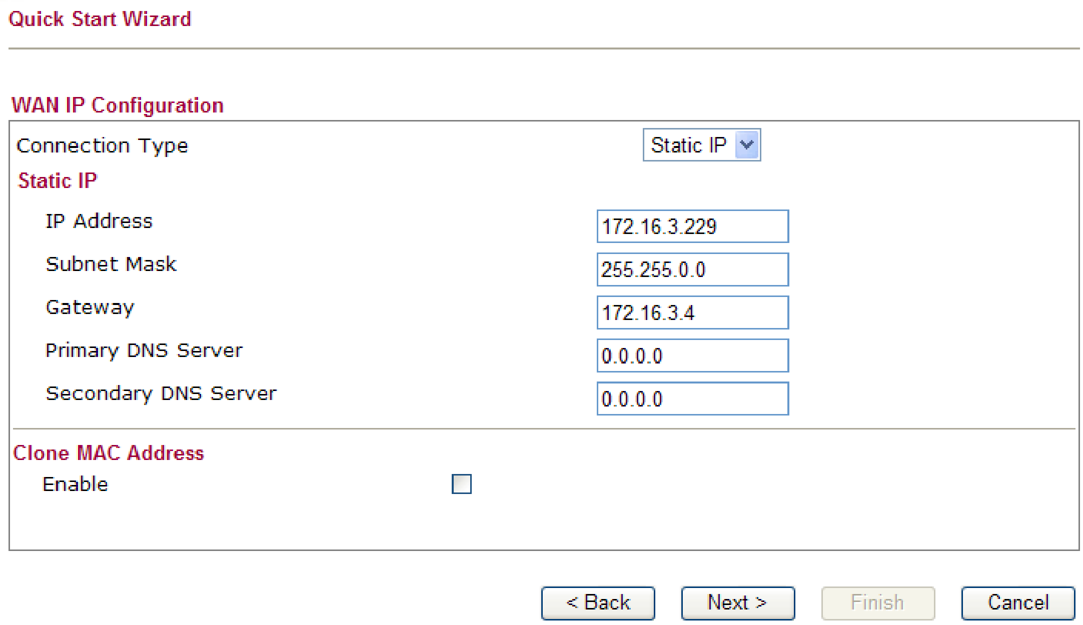
Connection Type: DHCP

Clone MAC Address

Enable □

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 □

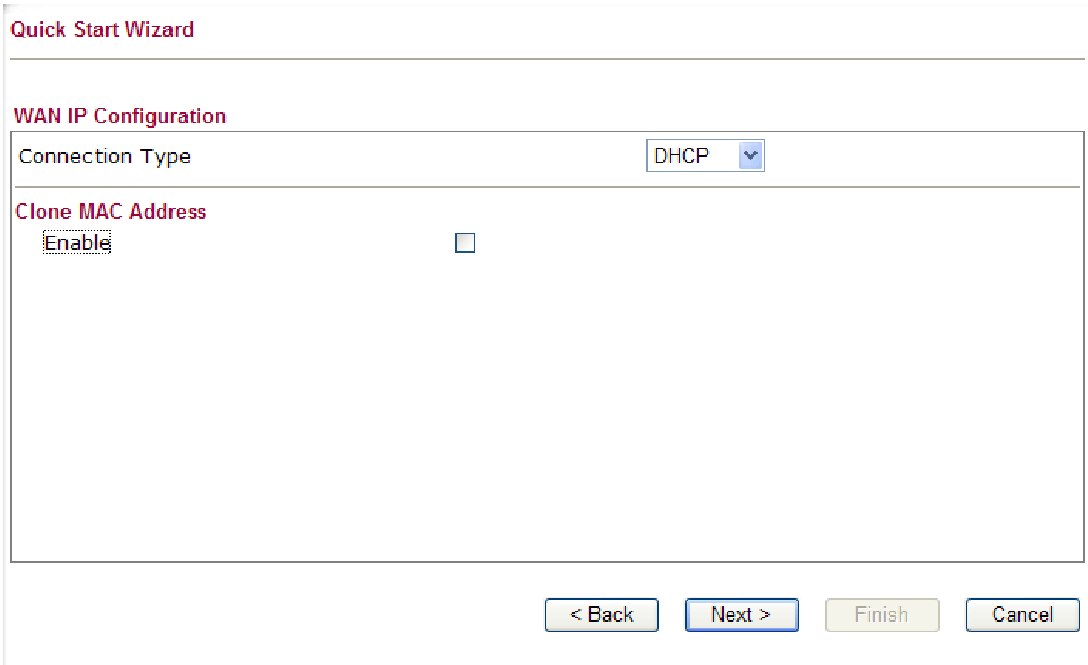
Available settings are explained as follows:

Item	Description
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 ☑ Clone MAC Address 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 ☐

Available settings are explained as follows:

Item	Description
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

Item	Description
	of MAC Address. Enable ☑ Clone MAC Address MAC Address 00-0E-A6-2A-D5-A1

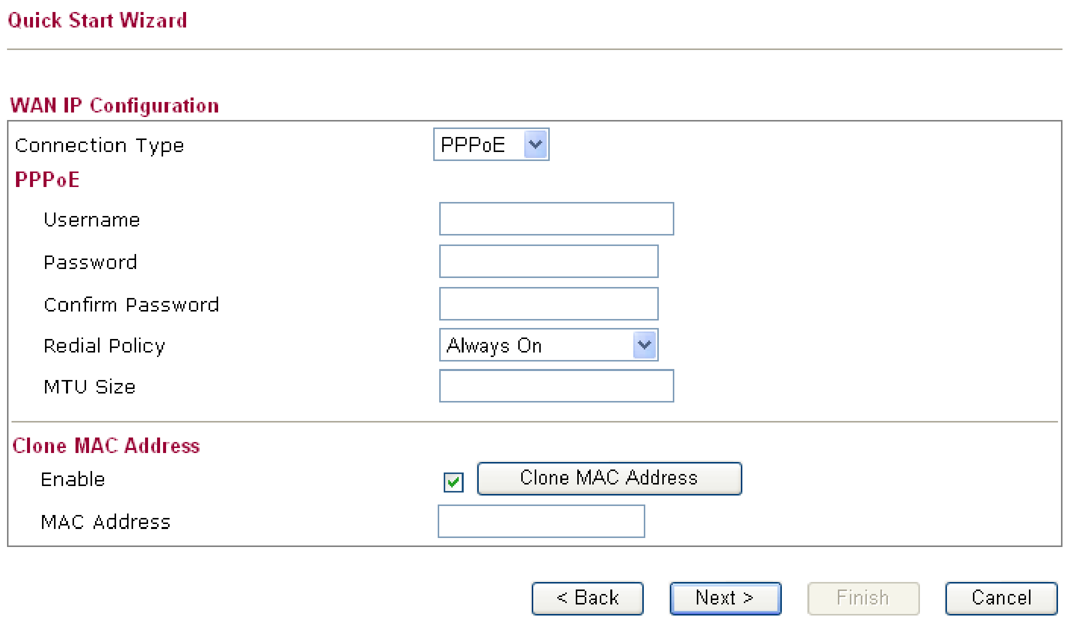
After finishing the settings here, please click **Next.**

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:

Confirm Password:

Redial Policy: Always On

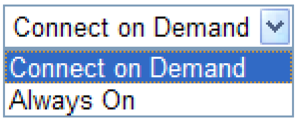
MTU Size:

Clone MAC Address

Enable ☑ Clone MAC Address

MAC Address:

Available settings are explained as follows:

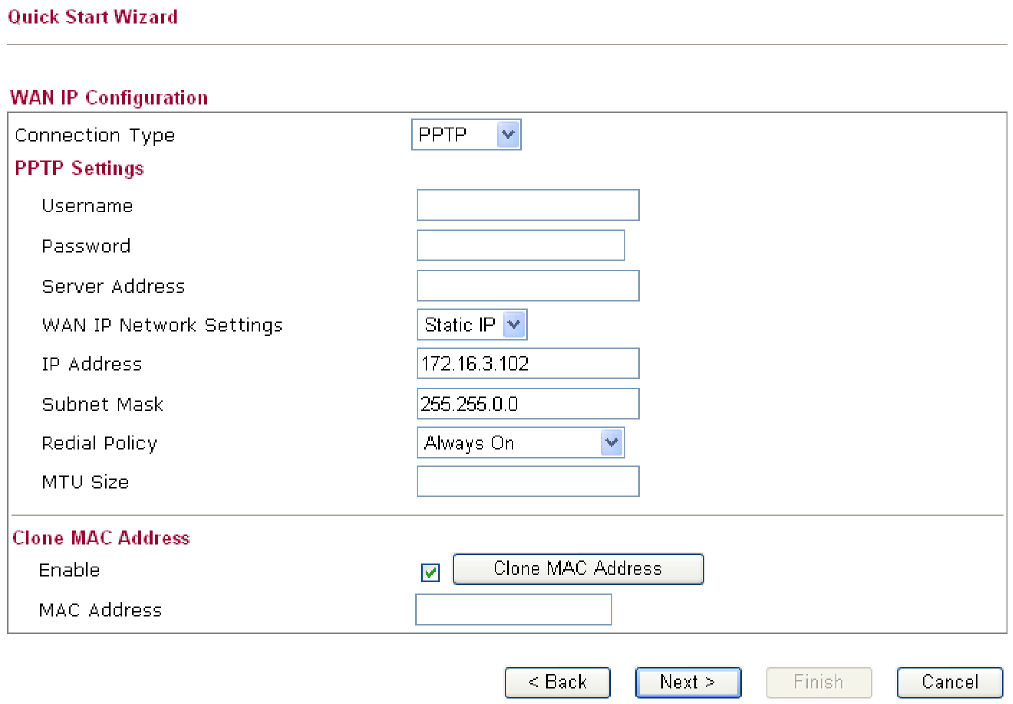
Item	Description
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Redial Policy	If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.  Connect on Demand Connect on Demand Always On

Item	Description
Idle Time Out	Set the timeout for breaking down the Internet after passing through the time without any action.
MTU Size	It means Max Transmit Unit for packet. The default setting will be specified by the system automatically. Therefore, keep this field in blank.
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.



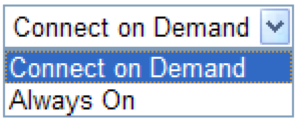
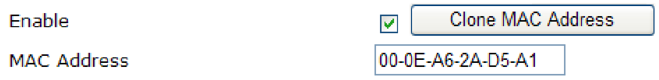
Quick Start Wizard

WAN IP Configuration

Connection Type	PPTP
PPTP Settings	
Username	
Password	
Server Address	
WAN IP Network Settings	Static IP
IP Address	172.16.3.102
Subnet Mask	255.255.0.0
Redial Policy	Always On
MTU Size	
Clone MAC Address	
Enable	☑ Clone MAC Address
MAC Address	

Available settings are explained as follows:

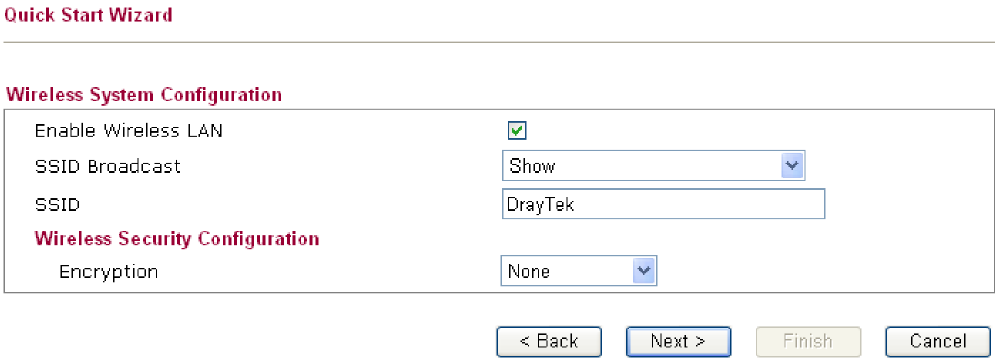
Item	Description
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Server Address	Specify the IP address of the PPTP server.
WAN IP Network Settings	You can choose Static IP or DHCP as WAN IP network setting.

Item	Description
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**.  Connect on Demand Connect on Demand Always On
Idle Time Out	Set the timeout for breaking down the Internet after passing through the time without any action.
MTU Size	It means Max Transmit Unit for packet. The default setting will be specified by the system automatically. Therefore, keep this field in blank.
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.**

2.3.4 Setting up the Wireless Connection

Now, you have to set up the wireless connection. For the user of Vigor1000, please skip this step.



Quick Start Wizard

Wireless System Configuration

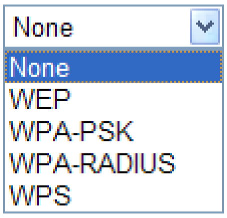
Enable Wireless LAN	☑
SSID Broadcast	Show
SSID	DrayTek

Wireless Security Configuration

Encryption	None

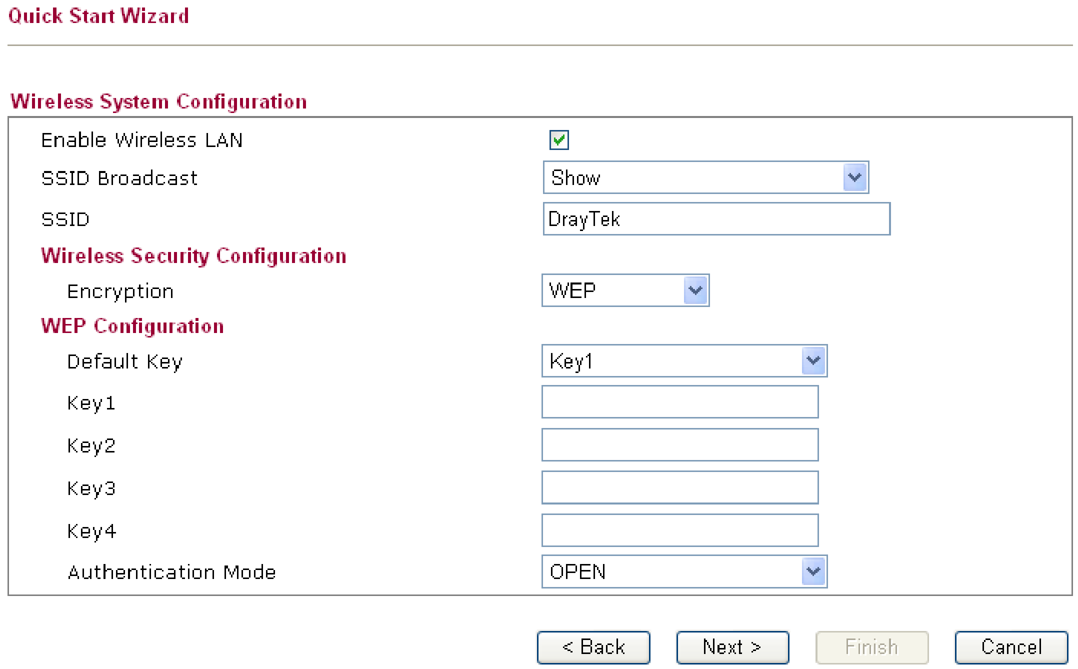
Available settings are explained as follows:

Item	Description
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

Item	Description
	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.
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

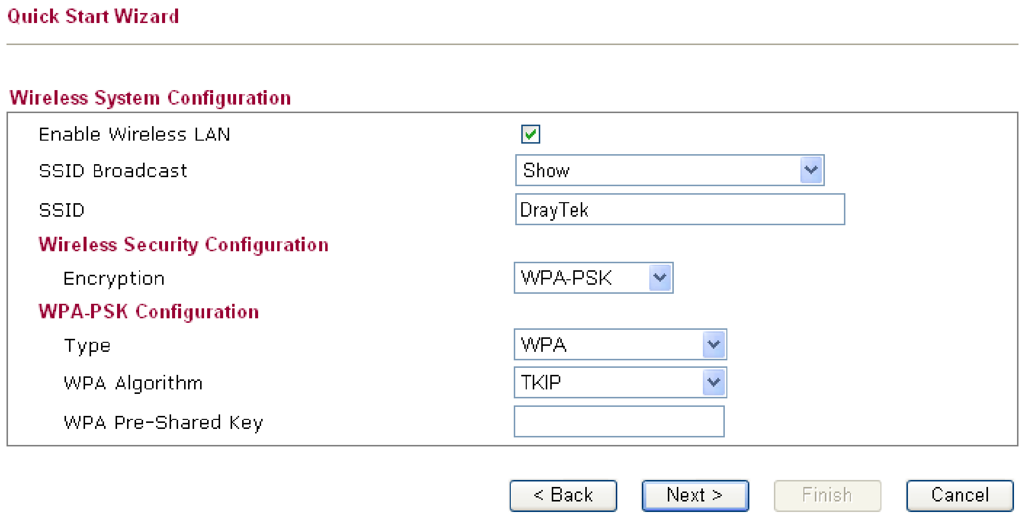
Wireless System Configuration

Enable Wireless LAN	☑
SSID Broadcast	Show
SSID	DrayTek
Wireless 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.

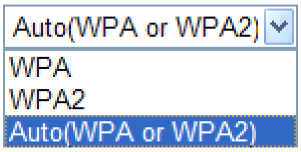
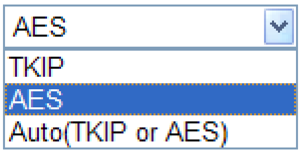


Quick Start Wizard

Wireless System Configuration

Enable Wireless LAN	☑
SSID Broadcast	Show
SSID	DrayTek
Wireless Security Configuration	
Encryption	WPA-PSK
WPA-PSK Configuration	
Type	WPA
WPA Algorithm	TKIP
WPA Pre-Shared Key	

Available settings are explained as follows:

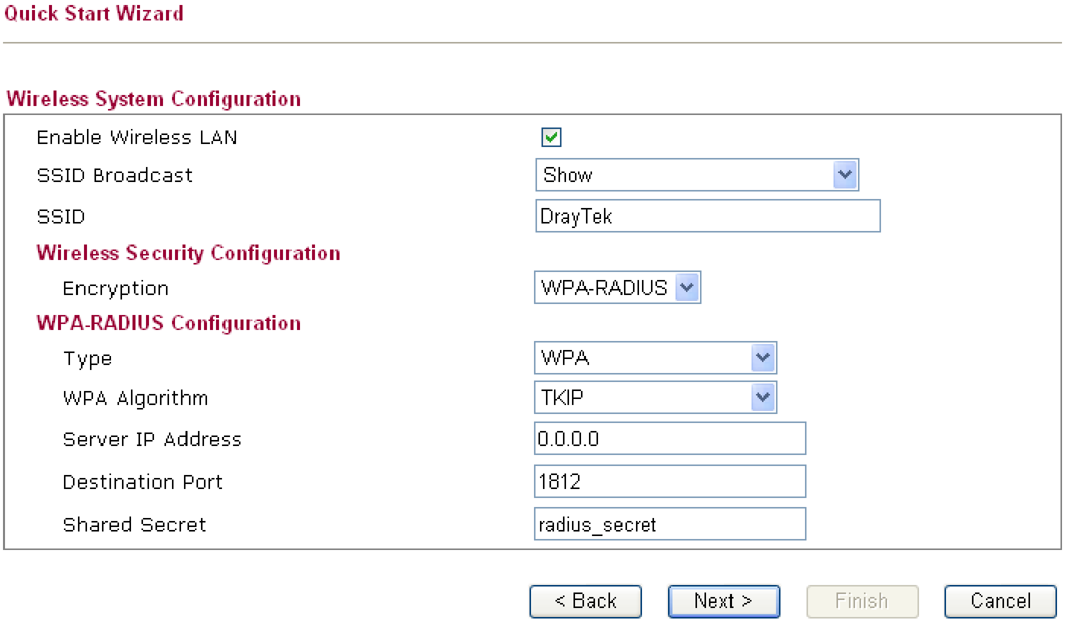
Item	Description
Type	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. 
WPA Algorithm	Choose the WPA algorithm, TKIP, 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.

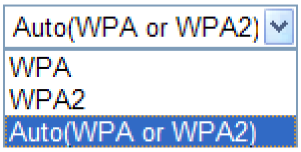
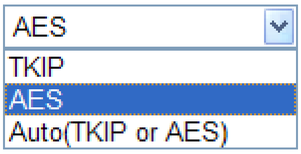


Quick Start Wizard

Wireless System Configuration

Enable Wireless LAN	☑
SSID Broadcast	Show
SSID	DrayTek
Wireless 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

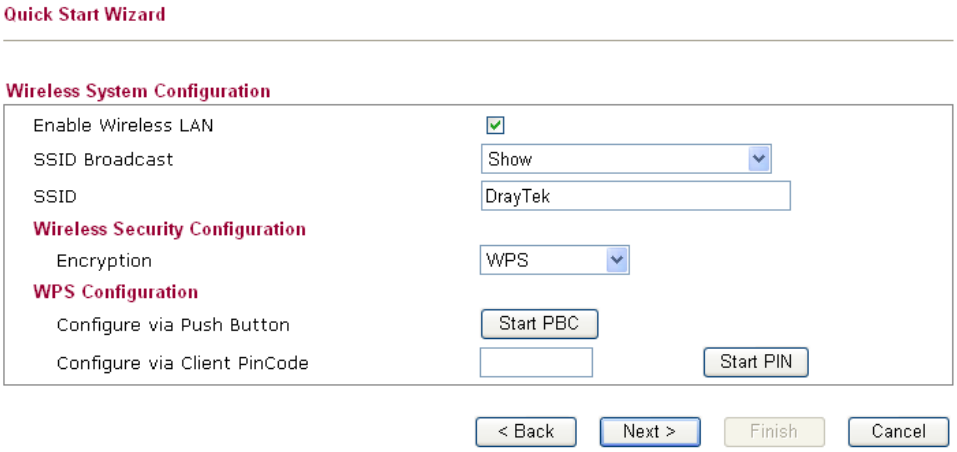
Available settings are explained as follows:

Item	Description
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 Security Configuration

Encryption	WPS

WPS Configuration

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

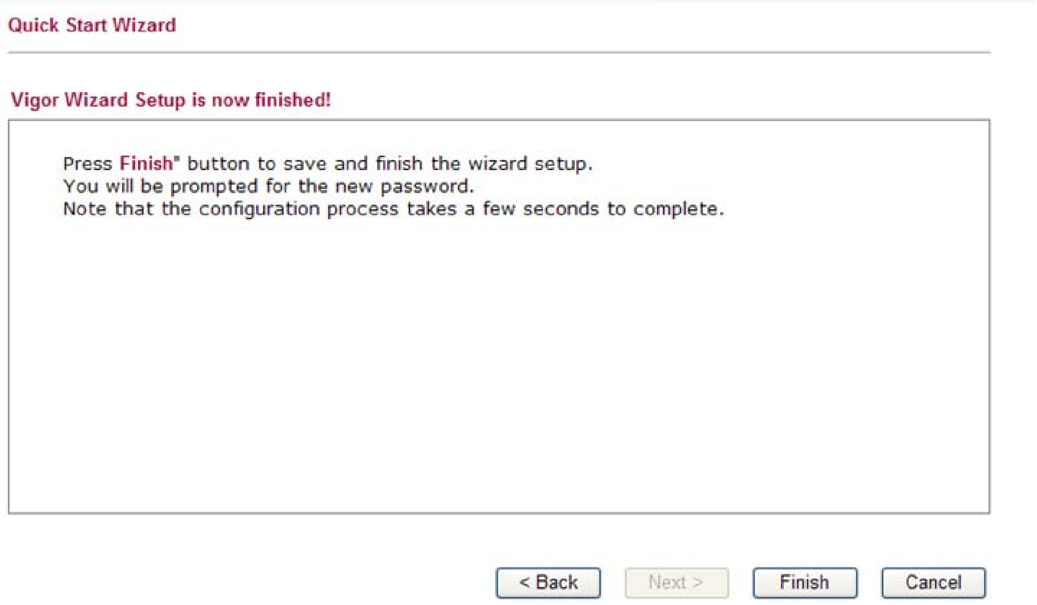
Available settings are explained as follows:

Item	Description
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.**

2.3.5 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.



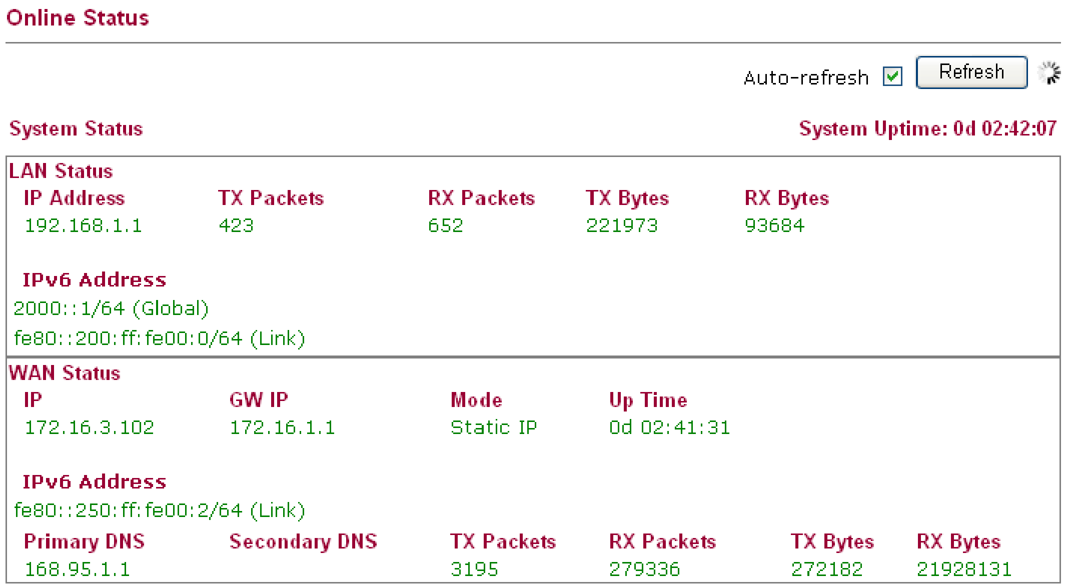
Quick Start Wizard

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.

2.4 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

Auto-refresh ☑ Refresh

System Status

System Uptime: 0d 02:42:07

LAN Status

IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.1	423	652	221973	93684

IPv6 Address
2000::1/64 (Global)
fe80::200:ff:fe00:0/64 (Link)

WAN Status

IP	GW IP	Mode	Up Time
172.16.3.102	172.16.1.1	Static IP	0d 02:41:31

IPv6 Address
fe80::250:ff:fe00:2/64 (Link)

Primary DNS	Secondary DNS	TX Packets	RX Packets	TX Bytes	RX Bytes
168.95.1.1		3195	279336	272182	21928131

Available settings are explained as follows:

Item	Description
LAN Status	**IP Address-**Displays the IP address of the LAN interface. **TX Packets-**Displays the total transmitted packets at the

Item	Description
	LAN interface. **RX Packets**-Displays the total received packets at the LAN interface. **TX Bytes**-Displays the total transmitted bytes at the LAN interface. **RX Bytes**-Displays the total received packets at the LAN interface. **IPv6 Address**-Displays the IPv6 address of the LAN interface.
WAN Status	**IP**-Displays the IP address of the WAN interface. **GW IP**-Displays the IP address of the default gateway. **Mode**-Displays the type of WAN connection (e.g., PPPoE). **Up Time**-Displays the total uptime of the interface. **IPv6 Address**-Displays the IPv6 address of the LAN interface. **Primary DNS**-Displays the primary DNS server address for WAN interface. **Secondary DNS** -Displays the secondary DNS server address for WAN interface. **TX Packets**-Displays the total transmitted packets at the WAN interface. **RX Packets**-Displays the total number of received packets at the WAN interface. **TX Bytes**-Displays the total transmitted bytes at the WAN interface. **RX Bytes**-Displays the total received packets 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.

2.5 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 Tutorials and Applications

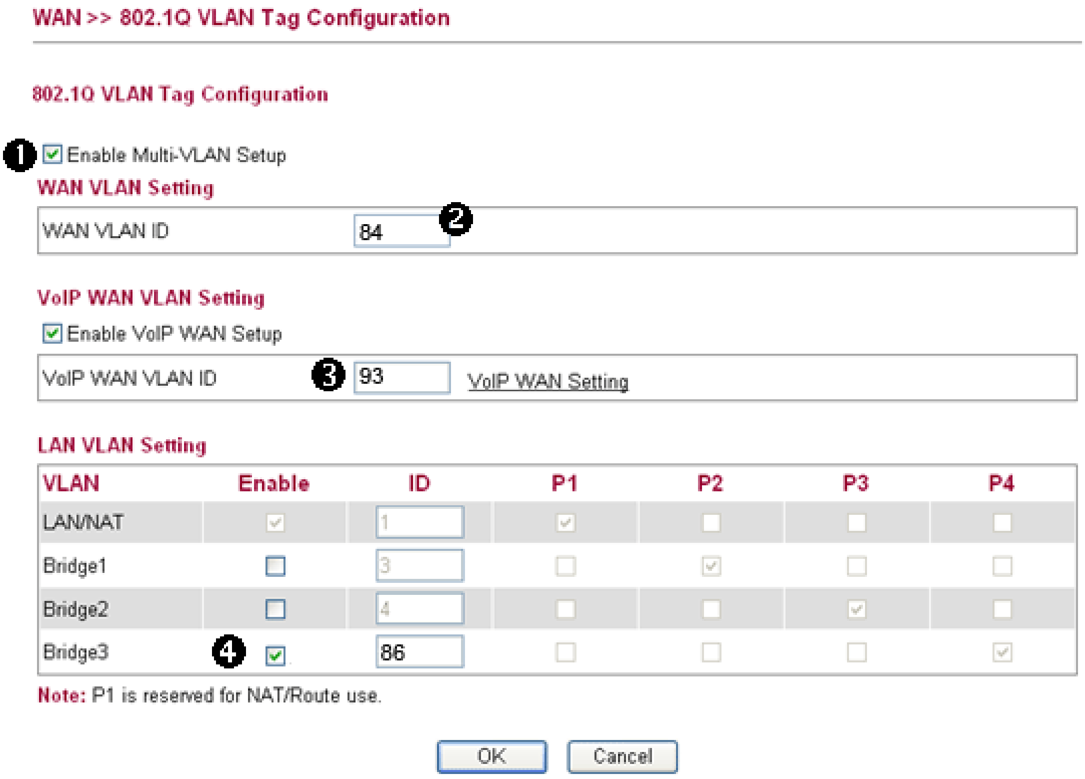
3.1 How to Configure Multi-VLAN in Vigor Router

Vigor1000 supports the function of Multi-VLAN (firmware version: 1.4.0 and after). It can specify a VLAN ID for WAN port and offers more advanced environmental application for the users through the bridge technique in WAN port and LAN port.

I. Way to Configure

To enable such function, please do the following:

1. Open **WAN>>802.1Q VLAN Tag Configuration**. Check the box of **Enable Multi-VLAN Setup**.
2. Fill in the VLAN ID number in the field of WAN VLAN ID.
3. If the router you have supports VoIP, you can configure VoIP WAN setting for using by VoIP interface of the router.
4. In LAN VLAN setting, check the box of **Enable** (LAN to WAN in bridge mode) and type a different VLAN ID number.



WAN >> 802.1Q VLAN Tag Configuration

802.1Q VLAN Tag Configuration

☑ Enable Multi-VLAN Setup

WAN VLAN Setting

WAN VLAN ID	84

VoIP WAN VLAN Setting

☑ Enable VoIP WAN Setup

VoIP WAN VLAN ID	93	VoIP WAN Setting

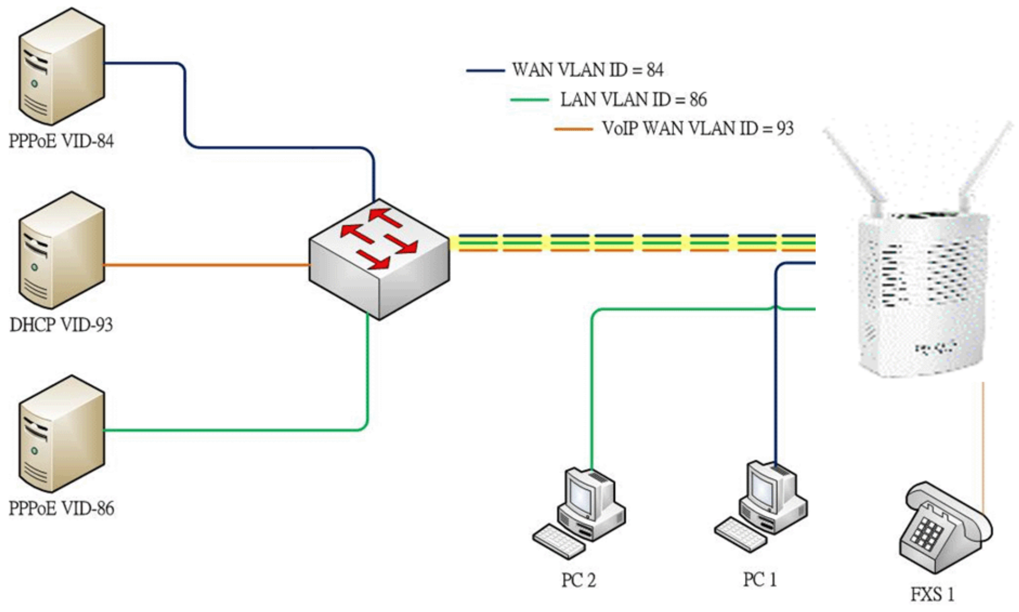
LAN VLAN Setting

VLAN	Enable	ID	P1	P2	P3	P4
LAN/NAT	☑	1	☑	□	□	□
Bridge1	□	3	□	☑	□	□
Bridge2	□	4	□	□	☑	□
Bridge3	☑	86	□	□	□	☑

Note: P1 is reserved for NAT/Route use.

II. Example

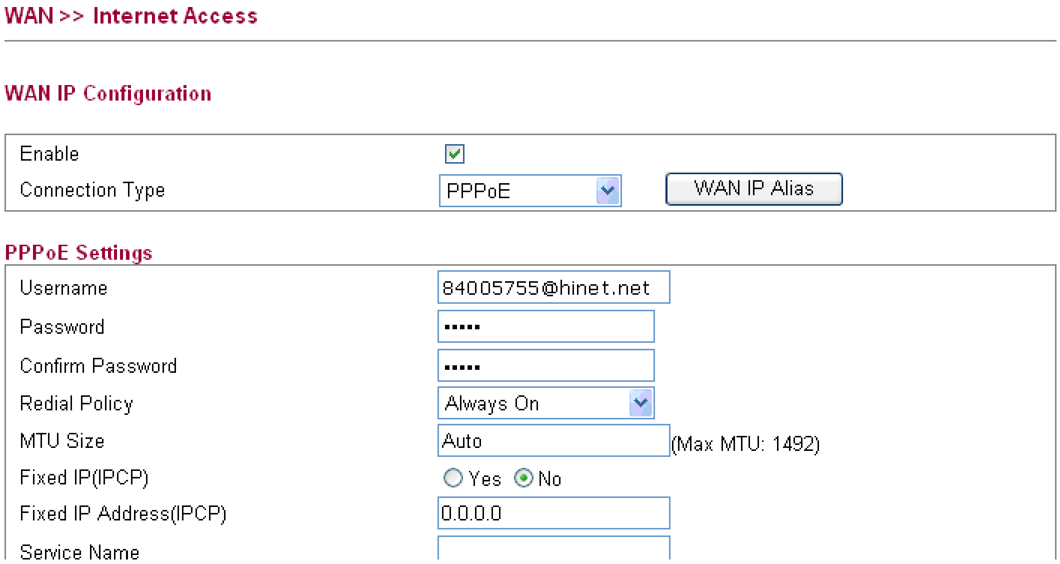
Chart of Structure



- PC 1 connects to the first LAN port of Vigor1000 and accesses Internet with WAN VLAN.
- PC 2 connects to the forth LAN port of Vigor1000 and accesses Internet with LAN VLAN.
- FXS 1 Phone connects to the FXS 1 port of Vigor1000, registers, sends and receives phone call with VoIP WAN.

Functions Configuration

1. Open **WAN>>Internet**. Set **PPPoE** as the **Connection Type** and fill in the Username and Password offered by your ISP.



WAN >> Internet Access

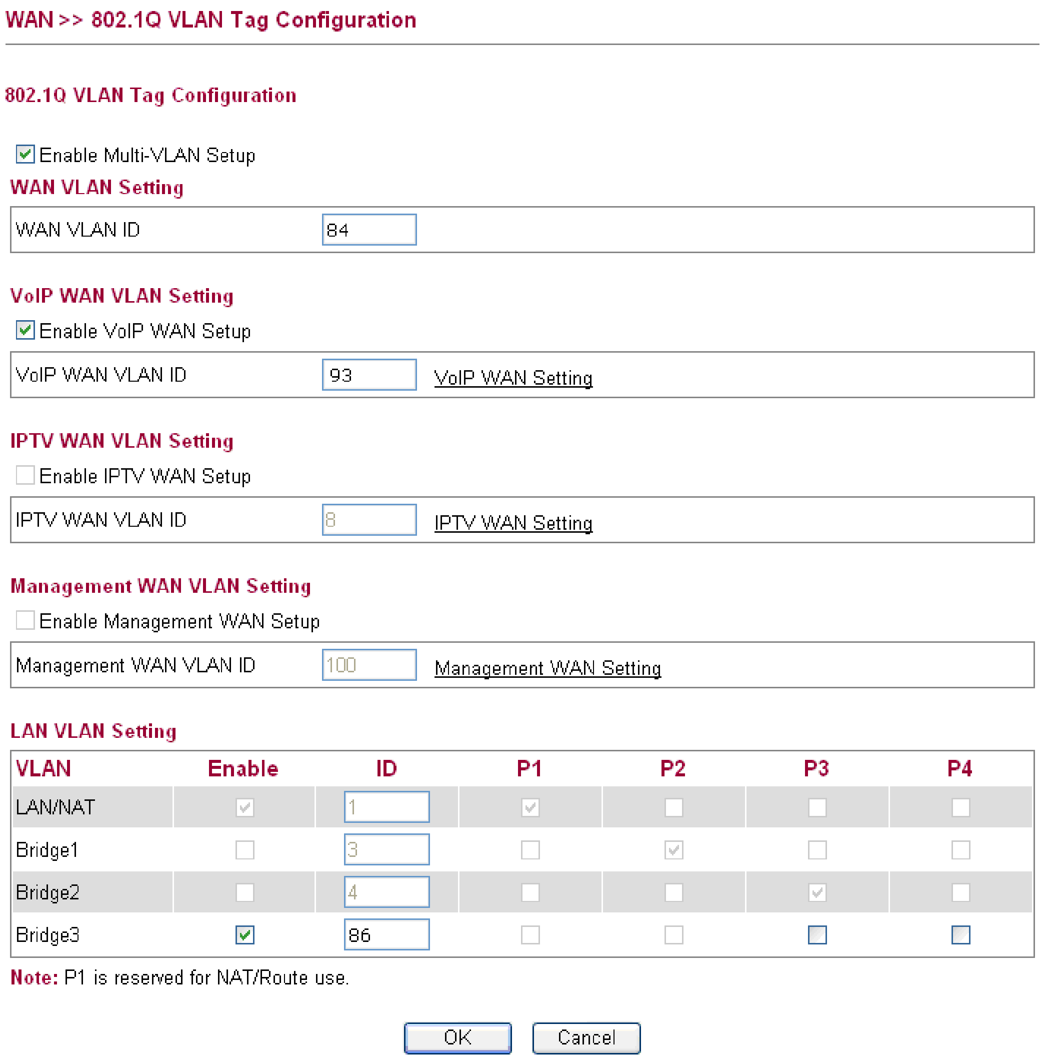
WAN IP Configuration

Enable	☑	
Connection Type	PPPoE	WAN IP Alias

PPPoE Settings

Username	84005755@hinet.net
Password	•••••
Confirm Password	•••••
Redial Policy	Always On
MTU Size	Auto (Max MTU: 1492)
Fixed IP(IPCP)	○ Yes ● No
Fixed IP Address(IPCP)	0.0.0.0
Service Name	

2. Open **WAN>>802.1Q VLAN Tag Configuration** to configure Multi-VLAN. Refer to the following graphic.



WAN >> 802.1Q VLAN Tag Configuration

802.1Q VLAN Tag Configuration

☑ Enable Multi-VLAN Setup

WAN VLAN Setting

WAN VLAN ID	84

VoIP WAN VLAN Setting

☑ Enable VoIP WAN Setup

VoIP WAN VLAN ID	93	VoIP WAN Setting

IPTV WAN VLAN Setting

□ Enable IPTV WAN Setup

IPTV WAN VLAN ID	8	IPTV WAN Setting

Management WAN VLAN Setting

□ Enable Management WAN Setup

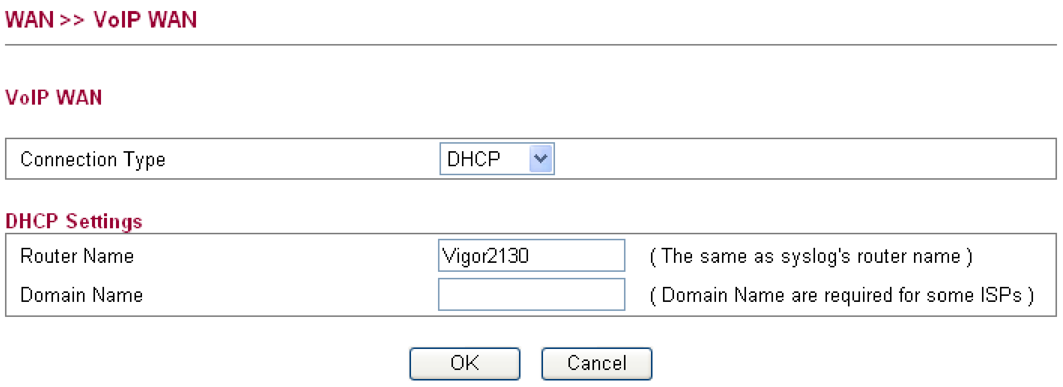
Management WAN VLAN ID	100	Management WAN Setting

LAN VLAN Setting

VLAN	Enable	ID	P1	P2	P3	P4
LAN/NAT	☑	1	☑	□	□	□
Bridge1	□	3	□	☑	□	□
Bridge2	□	4	□	□	☑	□
Bridge3	☑	86	□	□	□	□

Note: P1 is reserved for NAT/Route use.

3. Open **WAN>>VoIP WAN** to configure VoIP WAN Setting.



WAN >> VoIP WAN

VoIP WAN

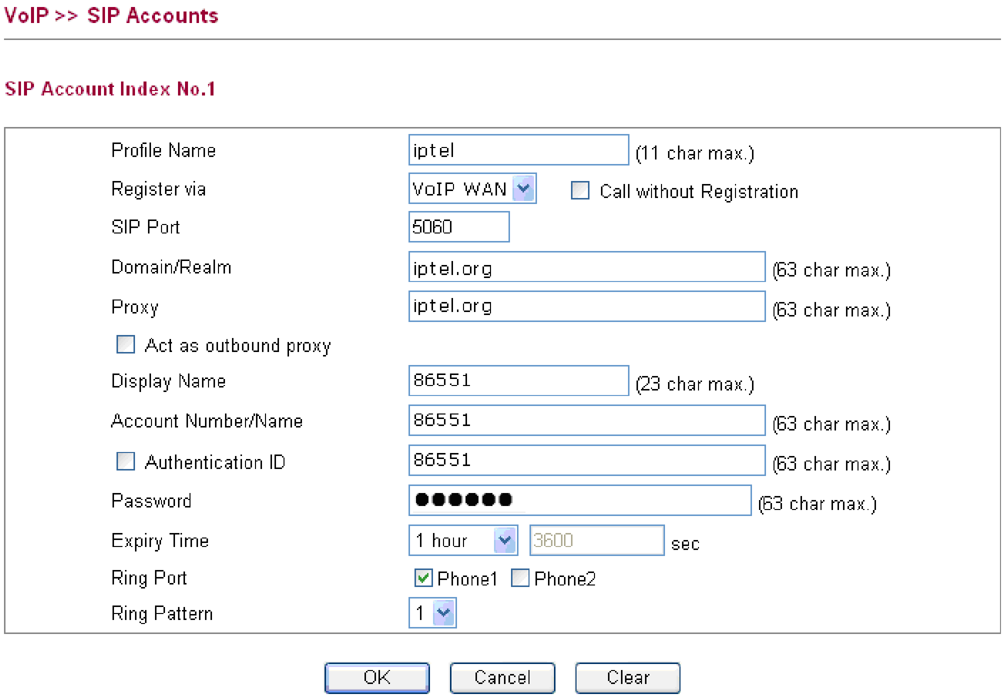
Connection Type	DHCP

DHCP Settings

Router Name	Vigor2130	(The same as syslog's router name)
Domain Name		(Domain Name are required for some ISPs)

Note: At present, only DHCP, PPPoE and Static connection types are available.

4. Open **VoIP >>SIP Accounts**. Specify the connection interface for VoIP in the field of **Register via**.



VoIP >> SIP Accounts

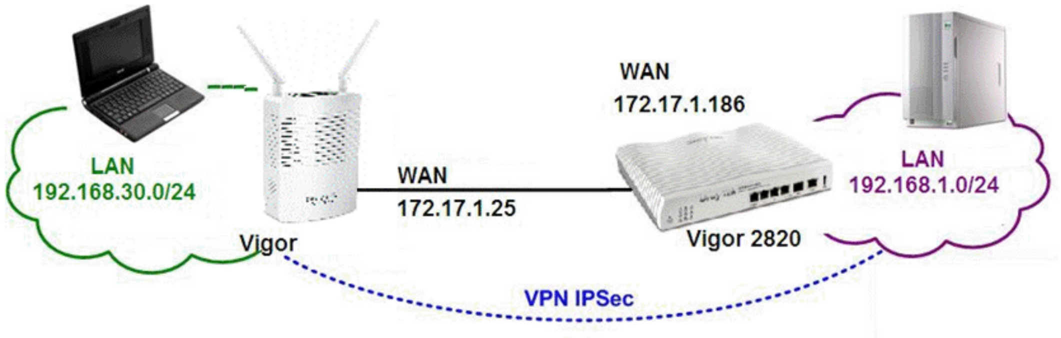
SIP Account Index No.1

Profile Name	iptel	(11 char max.)
Register via	VoIP WAN	□ Call without Registration
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
□ Act as outbound proxy		
Display Name	86551	(23 char max.)
Account Number/Name	86551	(63 char max.)
□ Authentication ID	86551	(63 char max.)
Password	●●●●●●	(63 char max.)
Expiry Time	1 hour 3600 sec	
Ring Port	☑ Phone1 □ Phone2	
Ring Pattern	1	

5. Connect your PC or network device to the forth LAN port and type the username and password for PPPoE connection mode.

3.2 LAN to LAN IPSec VPN between Vigor1000 and Vigor2820 using Main mode

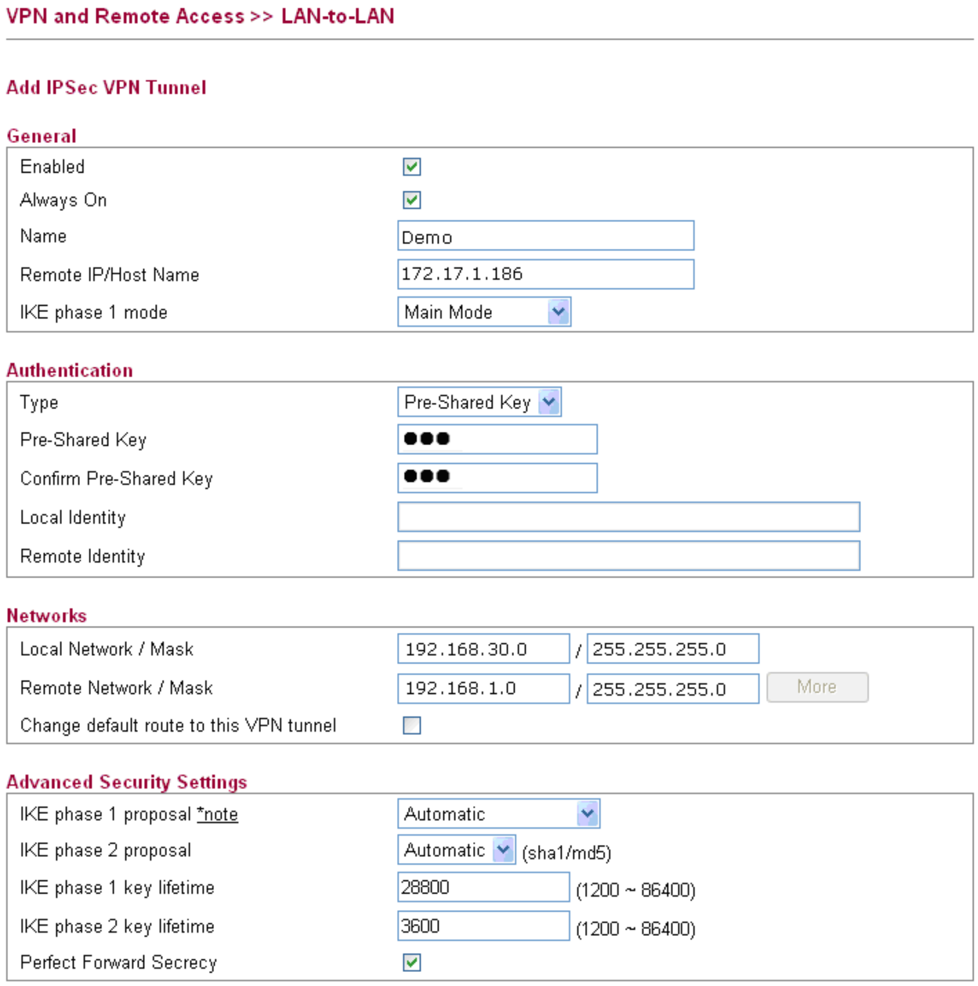
In this document we will introduce how to create a LAN to LAN IPSec VPN between Vigor1000 and a Vigor2820 using Main mode. We use the following scenario.



Case 1: VPN direction from Vigor1000 to Vigor2820

VPN configuration on Vigor1000

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN-to-LAN

Add IPSec VPN Tunnel

General

Enabled	☑
Always On	☑
Name	Demo
Remote IP/Host Name	172.17.1.186
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	192.168.30.0 /	255.255.255.0	
Remote Network / Mask	192.168.1.0 /	255.255.255.0	More
Change default route to this VPN tunnel	☐		

Advanced Security Settings

IKE phase 1 proposal *note	Automatic	
IKE phase 2 proposal	Automatic	(sha1/md5)
IKE phase 1 key lifetime	28800	(1200 ~ 86400)
IKE phase 2 key lifetime	3600	(1200 ~ 86400)
Perfect Forward Secrecy	☑	

2. Enable it and give it a name. In this example the profile name is “Demo”.

3. Enter Vigor2820's WAN IP address in the **Remote IP** field.

4. Select **Main Mode** as **IKE phase 1 mode**.

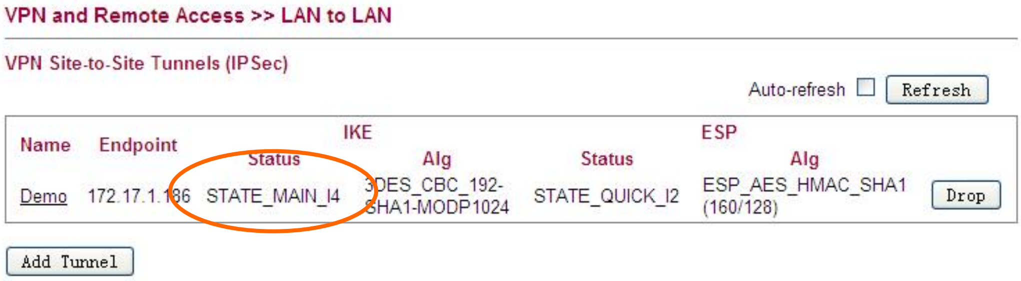
5. Setup a **pre-shared key**, which must be the same as in Vigor2820.

6. Enter Vigor1000's private network in the **Local Network / Mask** field. Enter Vigor2820's private network in the **Remote Network / Mask** field.

7. Use default value "**Automatic**" for **IKE phase 1** and **phase 2 proposals**.

8. Click **OK**.

9. Accessing the VPN network of Vigor2820 from a PC behind Vigor1000 to initiate the VPN connection, for example, ping 192.168.1.x from a PC (192.168.30.x). Vigor1000 will be triggered to dial the IPSec VPN to Vigor2820. After the VPN is connected, you can monitor the status.



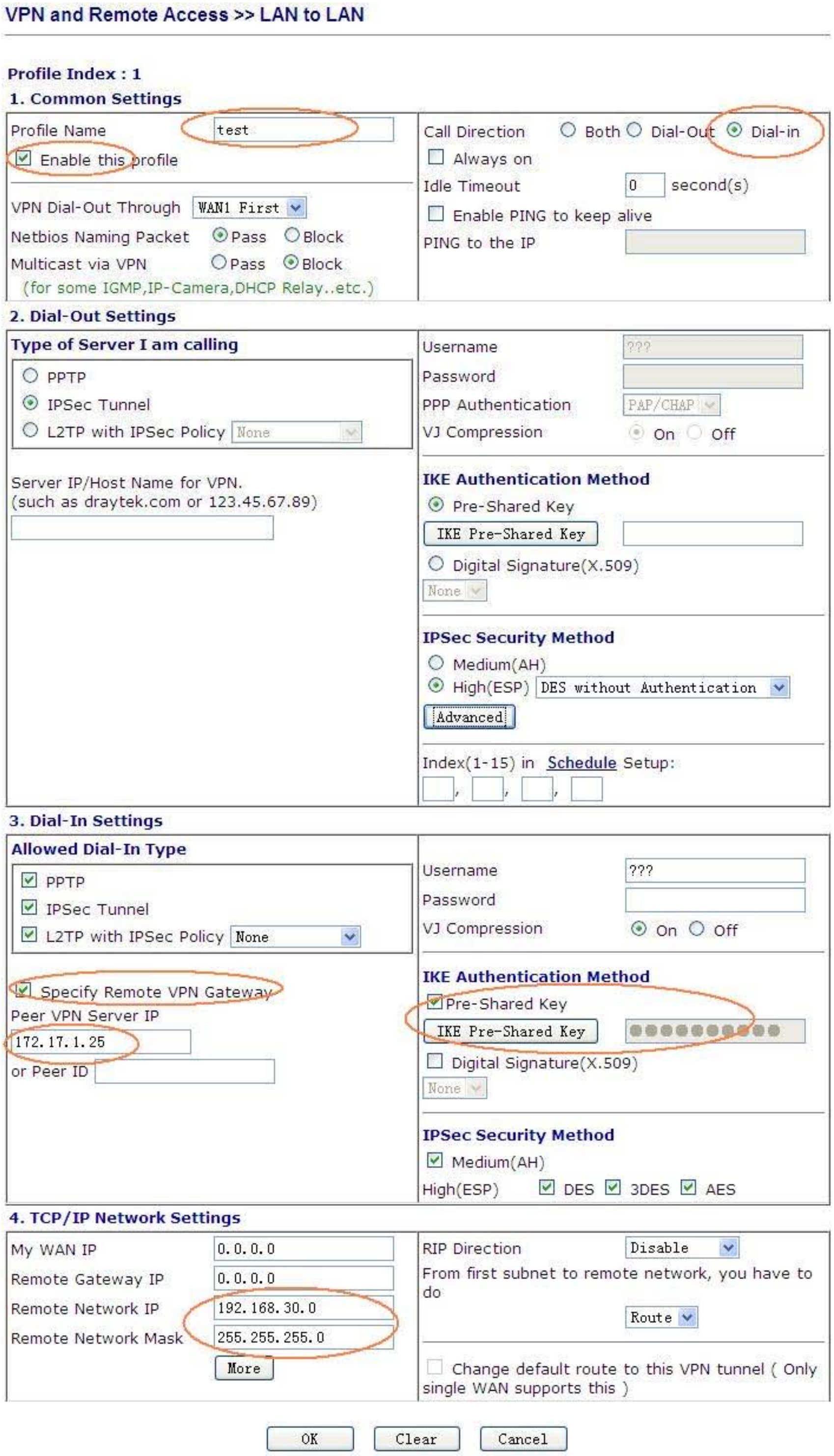
VPN and Remote Access >> LAN to LAN

VPN Site-to-Site Tunnels (IPSec)

Name	Endpoint	IKE		ESP		
		Status	Alg	Status	Alg	
Demo	172.17.1.186	STATE_MAIN_I4	3DES_CBC_192-SHA1-MODP1024	STATE_QUICK_I2	ESP_AES_HMAC_SHA1 (160/128)	Drop

VPN configuration on Vigor2820

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: test ☑ Enable this profile VPN Dial-Out Through: WAN1 First Netbios Naming Packet: ● Pass ○ Block Multicast via VPN: ○ Pass ● Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction: ○ Both ○ Dial-Out ● Dial-in □ Always on Idle Timeout: 0 second(s) □ Enable PING to keep alive PING to the IP:

2. Dial-Out Settings

Type of Server I am calling ○ PPTP ● IPSec Tunnel ○ L2TP with IPSec Policy: None Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	Username: ??? Password: PPP Authentication: PAP/CHAP VJ Compression: ● On ○ Off IKE Authentication Method ● Pre-Shared Key IKE Pre-Shared Key ○ Digital Signature(X.509) None IPSec Security Method ○ Medium(AH) ● High(ESP): DES without Authentication Advanced Index(1-15) in Schedule Setup: , , ,

3. Dial-In Settings

Allowed Dial-In Type ☑ PPTP ☑ IPSec Tunnel ☑ L2TP with IPSec Policy: None ☑ Specify Remote VPN Gateway Peer VPN Server IP: 172.17.1.25 or Peer ID:	Username: ??? Password: VJ Compression: ● On ○ Off IKE Authentication Method ☑ Pre-Shared Key IKE Pre-Shared Key: ●●●●●●●●●●● □ Digital Signature(X.509) None IPSec Security Method ☑ Medium(AH) High(ESP): ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0 Remote Gateway IP: 0.0.0.0 Remote Network IP: 192.168.30.0 Remote Network Mask: 255.255.255.0 More	RIP Direction: Disable From first subnet to remote network, you have to do: Route □ Change default route to this VPN tunnel (Only single WAN supports this)

2. Enable it and give it a name. In this example the profile name is “test”.

3. Select **Dial-in** as **Call Direction**.

4. In **Dial-Out Settings** part, select **IPSec Tunnel** and press the **Advanced** button.

5. In **Dial-In Settings** part, please enable **Specify Remote VPN Gateway** and enter WAN IP address of Vigor1000 in the **Peer VPN Server ID** field.

6. Setup a **pre-shared key**, which must be the same as in Vigor1000.

7. Enter Vigor1000's private network in the **Remote Network IP / Mask** field.

8. Click **OK**.

Note: Vigor1000 supports the following proposals by default.

For phase 1,

Mode Selection	Proposals will be sent

When you select **Automatic**	3DES, MD5, Group 5;
	3DES, SHA1, Group 5;
	3DES, SHA1, Group 2;
	3DES, MD5, Group 2;

When you select **3DES**	3DES, MD5, Group 5;
	3DES, SHA1, Group 5;
	3DES, SHA1, Group 2;
	3DES, MD5, Group 2;

When you select **AES(any)**	AES, MD5, Group 5;
	AES, SHA1, Group 5;
	AES, MD5, Group 2;
	AES, SHA1, Group 2;

When you select **AES-128**	AES-128, MD5, Group 5;
	AES-128, SHA1, Group 5;
	AES-128, MD5, Group 2;
	AES-128, SHA1, Group 2;

When you select **AES-192**	AES-192, MD5, Group 5;
	AES-192, SHA1, Group 5;
	AES-192, MD5, Group 2;
	AES-192, SHA1, Group 2;

When you select **AES-256**	AES-256, MD5, Group 5;
	AES-256, SHA1, Group 5;
	AES-256, MD5, Group 2;
	AES-256, SHA1, Group 2;

For phase 2,

Mode Selection	Proposals will be sent

When you select **Automatic**	AES, SHA1;
	AES, MD5;
	3DES, SHA1;
	3DES, MD5;

When you select **3DES**	3DES, MD5;
	3DES, SHA1;

When you select **AES(any)**	AES-256, MD5;
	AES-256, SHA1;

When you select **AES-128**	AES-128, MD5;
	AES-128, SHA1;

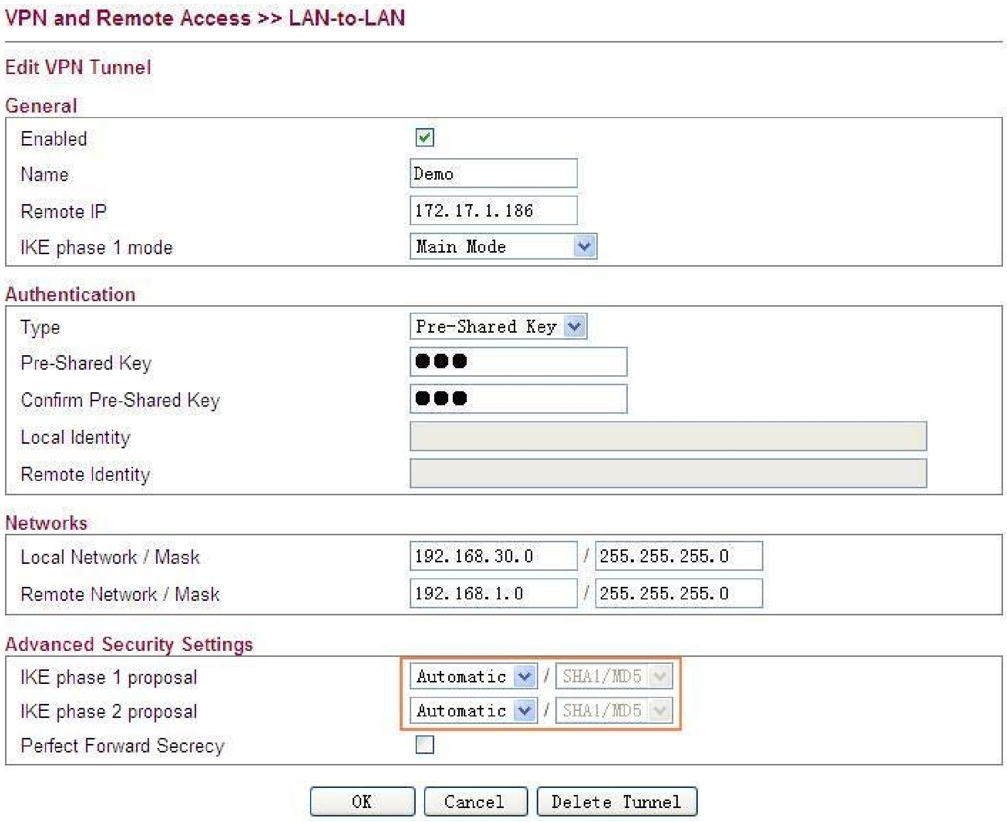
When you select **AES-192**	AES-192, MD5;
	AES-192, SHA1;

When you select **AES-256**	AES-256, MD5;
	AES-256, SHA1;

Case 2: VPN direction from Vigor2820 to Vigor1000

VPN configuration on Vigor1000

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN-to-LAN

Edit VPN Tunnel

General

Enabled	☑
Name	Demo
Remote IP	172.17.1.186
IKE phase 1 mode	Main Mode

Authentication

Type	Pre-Shared Key
Pre-Shared Key	●●●
Confirm Pre-Shared Key	●●●
Local Identity	
Remote Identity	

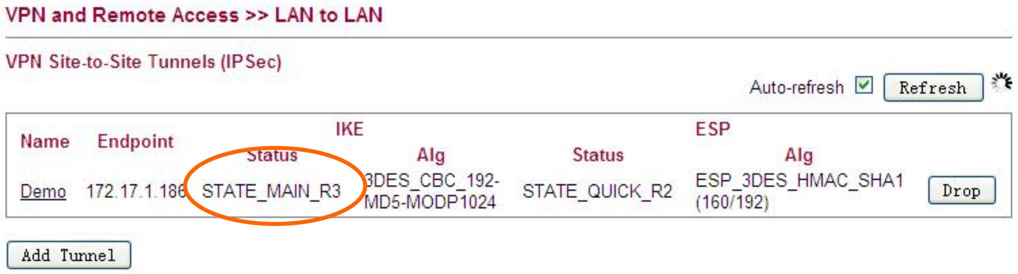
Networks

Local Network / Mask	192.168.30.0 / 255.255.255.0
Remote Network / Mask	192.168.1.0 / 255.255.255.0

Advanced Security Settings

IKE phase 1 proposal	Automatic / SHA1/MD5
IKE phase 2 proposal	Automatic / SHA1/MD5
Perfect Forward Secrecy	□

2. Enable it and give it a name. In this example the profile name is “Demo”.
3. Enter WAN IP address of Vigor2820 in the Remote IP field.
4. Select Main Mode as IKE phase 1 mode.
5. Setup a pre-shared key, which must be the same as in Vigor2820.
6. Enter Vigor1000’s private network in the Local Network / Mask field.
7. Enter Vigor2820’s private network in the Remote Network / Mask field.
8. Use default value “Automatic” for IKE phase 1 and phase 2 proposals.
9. After the VPN is connected, you can monitor the status.



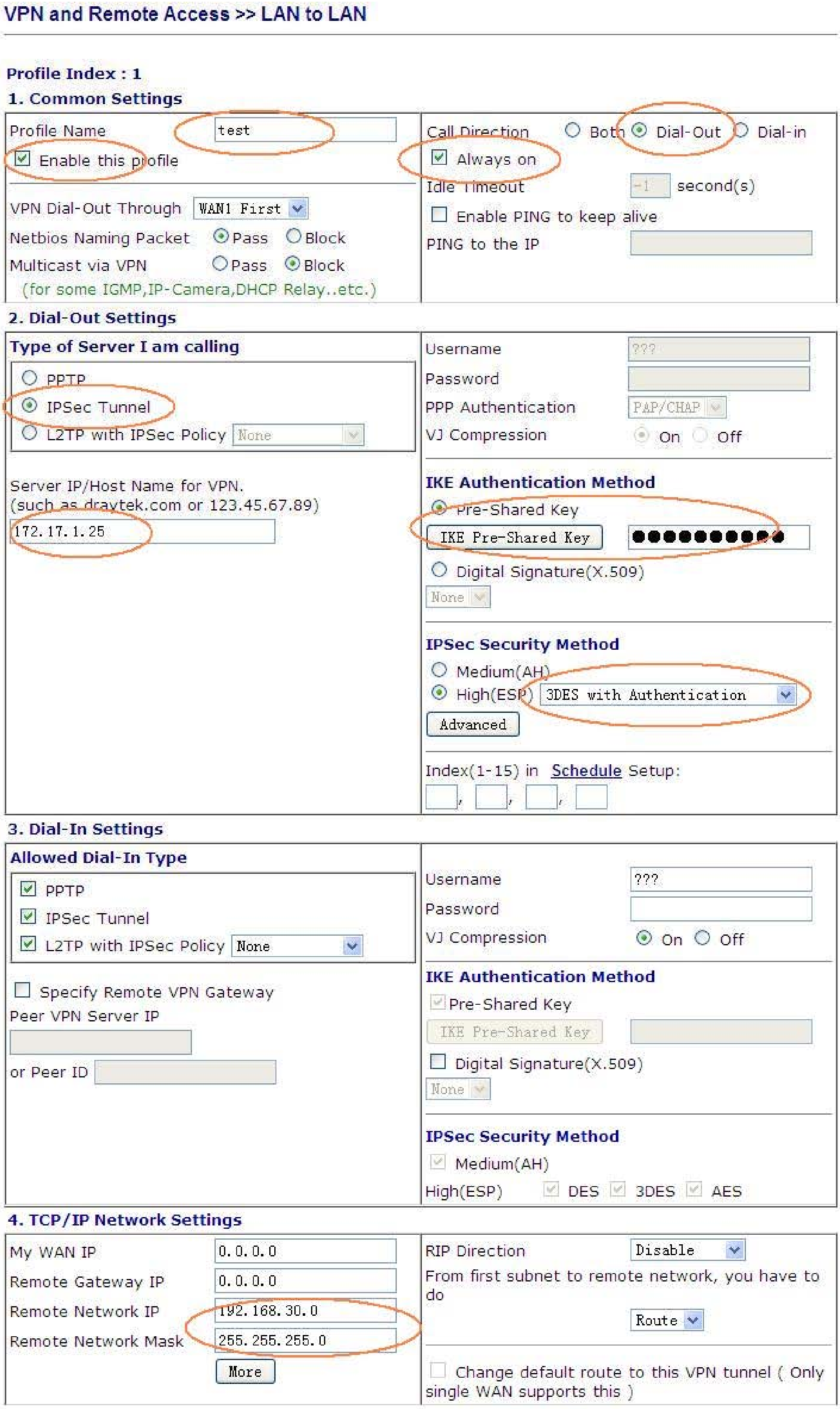
VPN and Remote Access >> LAN to LAN

VPN Site-to-Site Tunnels (IPSec)

		IKE		ESP		
Name	Endpoint	Status	Alg	Status	Alg	
Demo	172.17.1.186	STATE_MAIN_R3	3DES_CBC_192-MD5-MODP1024	STATE_QUICK_R2	ESP_3DES_HMAC_SHA1 (160/192)	Drop

VPN configuration on Vigor2820

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: test

☑ Enable this profile

VPN Dial-Out Through: WAN1 First

Netbios Naming Packet: ● Pass ○ Block

Multicast via VPN: ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ● Dial-Out ○ Dial-in

☑ Always on

Idle Timeout: -1 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
172.17.1.25

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key: ●●●●●●●●●●

○ Digital Signature(X.509)

None

IPSec Security Method

○ Medium(AH)

● High(ESP): 3DES with Authentication

Advanced

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

3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy: None

□ Specify Remote VPN Gateway

Peer VPN Server IP:

or Peer ID:

Username: ???

Password:

VJ Compression: ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key:

□ Digital Signature(X.509)

None

IPSec Security Method

☑ Medium(AH)

High(ESP): ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.30.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: Disable

From first subnet to remote network, you have to do: Route

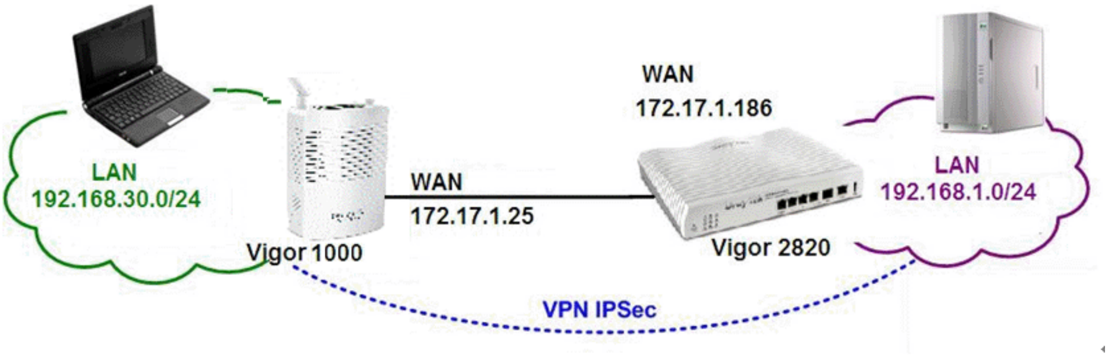
□ Change default route to this VPN tunnel (Only single WAN supports this)

2. Enable it and give it a name. In this example the profile name is “test”.

3. Select **Dial-Out** as **Call Direction** and enable **Always on**.
4. Select **IPSec Tunnel** and enter Vigor1000's WAN IP address in the **Server IP/Host Name for VPN** field.
5. Setup a **pre-shared key**, which must be the same as in Vigor1000.
6. Select **ESP (High)** and **3DES with Authentication**.
7. Enter Vigor1000's private network in the **Remote Network IP / Mask** field.
8. Click **OK**.

3.3 LAN to LAN IPSec VPN between Vigor1000 and Vigor2820 using Agressive mode

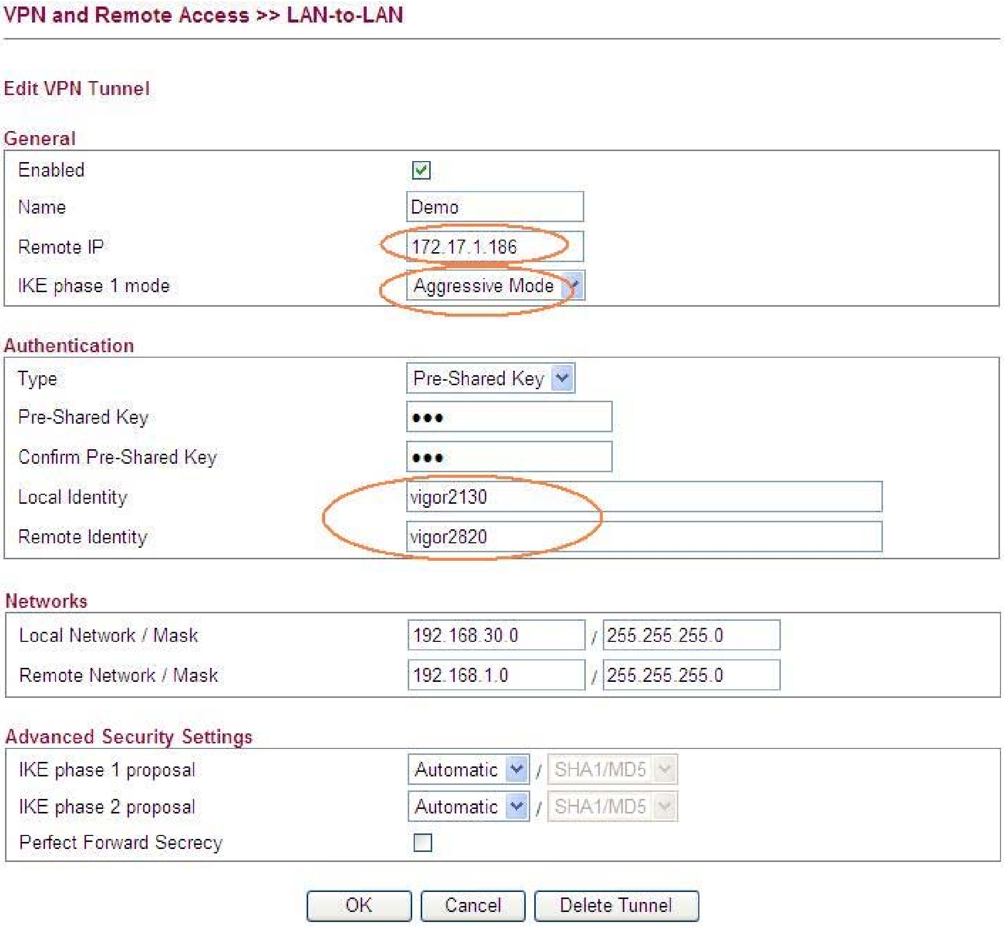
In this document we will introduce how to create a LAN to LAN IPSec VPN between Vigor1000 and a Vigor2820 using Aggressive mode. We use the following scenario.



Case 1: VPN direction from Vigor1000 to Vigor2820

VPN configuration on Vigor1000

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN-to-LAN

Edit VPN Tunnel

General

Enabled	☑
Name	Demo
Remote IP	172.17.1.186
IKE phase 1 mode	Aggressive Mode

Authentication

Type	Pre-Shared Key
Pre-Shared Key	●●●
Confirm Pre-Shared Key	●●●
Local Identity	vigor2130
Remote Identity	vigor2820

Networks

Local Network / Mask	192.168.30.0 / 255.255.255.0
Remote Network / Mask	192.168.1.0 / 255.255.255.0

Advanced Security Settings

IKE phase 1 proposal	Automatic / SHA1/MD5
IKE phase 2 proposal	Automatic / SHA1/MD5
Perfect Forward Secrecy	□

2. Enable it and give it a name. In this example the profile name is “Demo”.
3. Enter Vigor2820’s WAN IP address in the **Remote IP** field.
4. Select **Aggressive Mode** as **IKE phase 1 mode**.

5. Setup a **pre-shared key**, which must be the same as in Vigor2820.

6. Setup the **Local Identity** and **Remote Identity**, which are for Vigor1000 and Vigor2820 respectively.

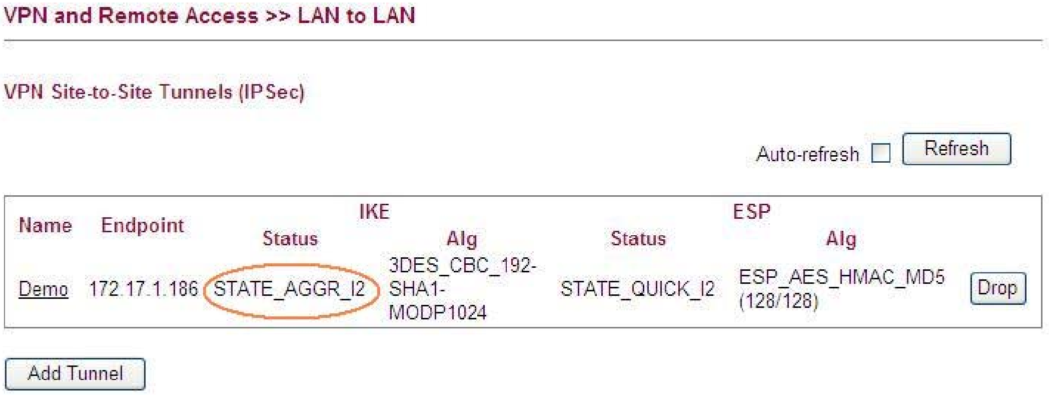
   During IPSec Aggressive mode negotiation, the VPN client must send its identity to the VPN server for verification. The VPN client may also verify the identity of the VPN server, which is optional. In this example we setup ‘Vigor1000’ as the identity of Vigor1000, and ‘vigor2820’ as the identity of Vigor2820.

7. Enter Vigor1000’s private network in the **Local Network / Mask** field. Enter Vigor2820’s private network in the **Remote Network / Mask** field.

8. Use default value “Automatic” for **IKE phase 1 and phase 2 proposals**.

9. Click **OK**.

10. Accessing the VPN network of Vigor2820 from a PC behind Vigor1000 to initiate the VPN connection, for example, ping 192.168.1.x from a PC (192.168.30.x). Vigor1000 will be triggered to dial the IPSec VPN to Vigor2820. After the VPN is connected, you can monitor the status.



VPN and Remote Access >> LAN to LAN

VPN Site-to-Site Tunnels (IPSec)

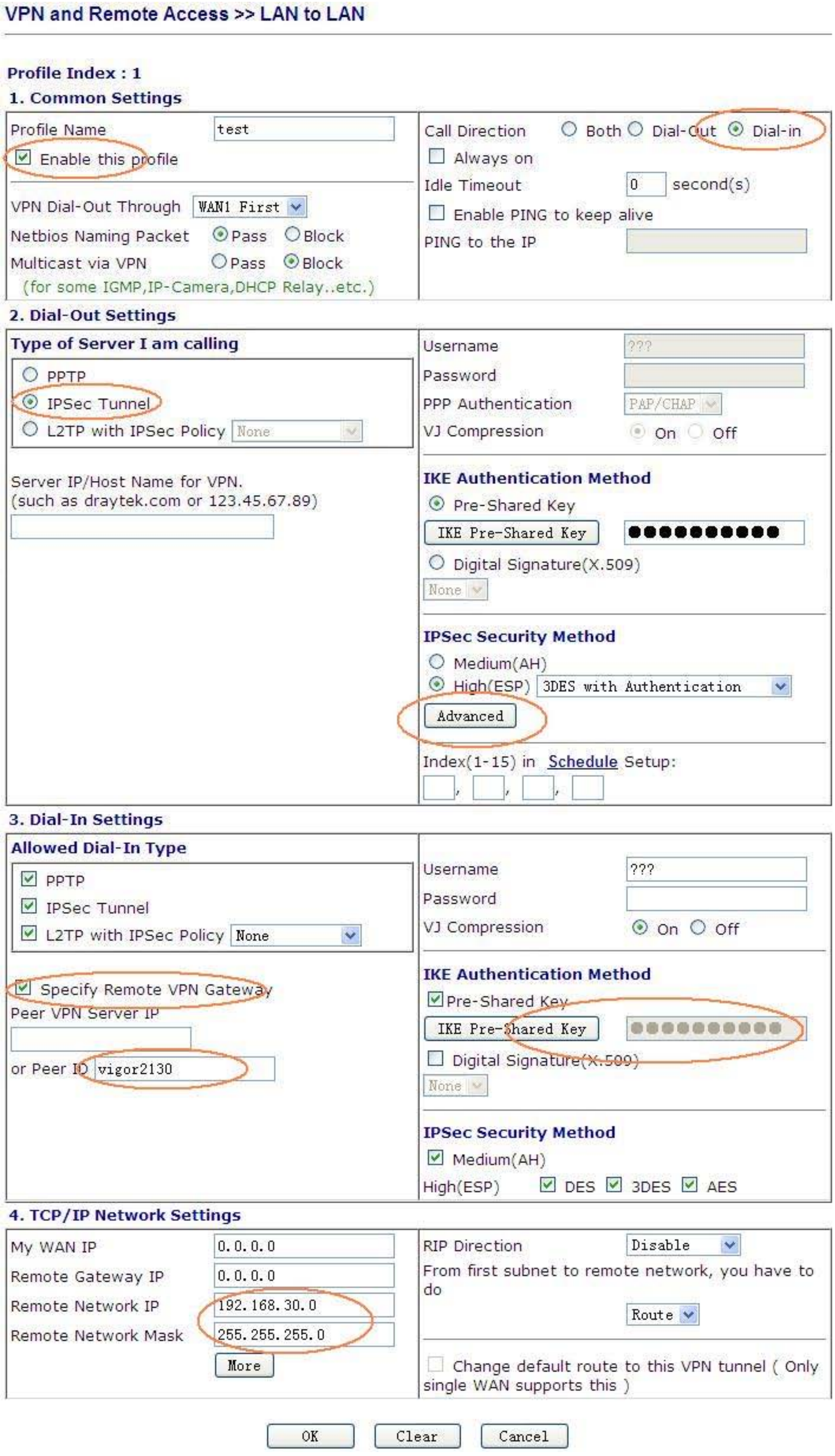
Auto-refresh □ Refresh

Name	Endpoint	IKE		ESP		
		Status	Alg	Status	Alg	
Demo	172.17.1.186	STATE_AGGR_I2	3DES_CBC_192-SHA1-MODP1024	STATE_QUICK_I2	ESP_AES_HMAC_MD5 (128/128)	Drop

Add Tunnel

VPN configuration on Vigor2820

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: test

☑ Enable this profile

VPN Dial-Out Through: WAN1 First

Netbios Naming Packet: ● Pass ○ Block

Multicast via VPN: ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ○ Dial-Out ● Dial-in

□ Always on

Idle Timeout: 0 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key: ●●●●●●●●●●●

○ Digital Signature(X.509)

None

IPSec Security Method

○ Medium(AH)

● High(ESP): 3DES with Authentication

Advanced

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

3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy: None

☑ Specify Remote VPN Gateway

Peer VPN Server IP:

or Peer ID: vigor2130

Username: ???

Password:

VJ Compression: ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key: ●●●●●●●●●●

□ Digital Signature(X.509)

None

IPSec Security Method

☑ Medium(AH)

High(ESP): ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.30.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

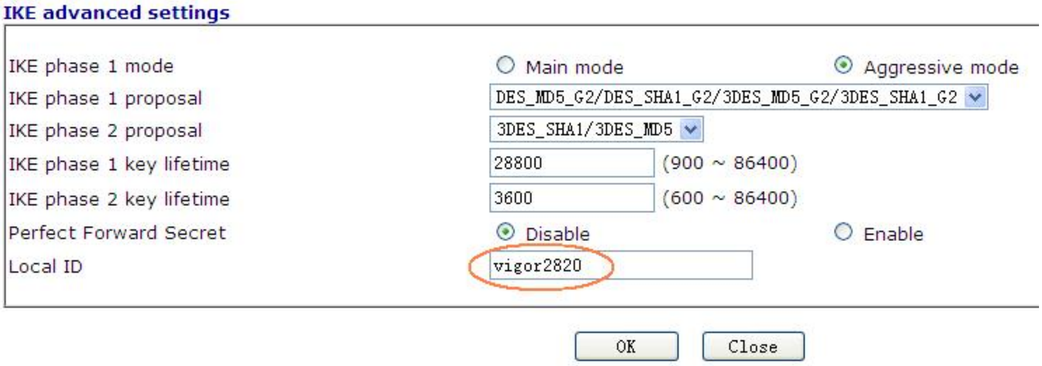
OK | Clear | Cancel

2. Enable it and give it a name. In this example the profile name is “test”.

3. Select Dial-in as **Call Direction**.

4. In **Dial-Out Settings** part, select **IPSec Tunnel** and press the **Advanced** button.

5. In the pop-up window please enter vigor2820 in the **Local ID** field. Click **OK** to return to the profile setting page.



IKE advanced settings

IKE phase 1 mode: ○ Main mode ● Aggressive mode
IKE phase 1 proposal: DES_MD5_G2/DES_SHA1_G2/3DES_MD5_G2/3DES_SHA1_G2
IKE phase 2 proposal: 3DES_SHA1/3DES_MD5
IKE phase 1 key lifetime: 28800 (900 ~ 86400)
IKE phase 2 key lifetime: 3600 (600 ~ 86400)
Perfect Forward Secret: ● Disable ○ Enable
Local ID: vigor2820

6. In **Dial-In Settings** part, please enable **Specify Remote VPN Gateway** and enter Vigor1000 in the **Peer ID** field.

7. Setup a **pre-shared key**, which must be the same as in Vigor1000.

8. Enter Vigor1000's private network in the **Remote Network IP / Mask** field.

9. Click **OK**.

Note: Vigor1000 supports the following proposals by default.

For phase 1,

Mode Selection	Proposals will be sent
When you select **Automatic**	3DES, SHA1, Group 2
When you select **3DES**	3DES, MD5, Group 5
When you select **AES(any)**	AES, MD5, Group 5
When you select **AES-128**	AES-128, MD5, Group 5
When you select **AES-192**	AES-192, MD5, Group 5
When you select **AES-256**	AES-256, MD5, Group 5

For phase 2,

Mode Selection	Proposals will be sent

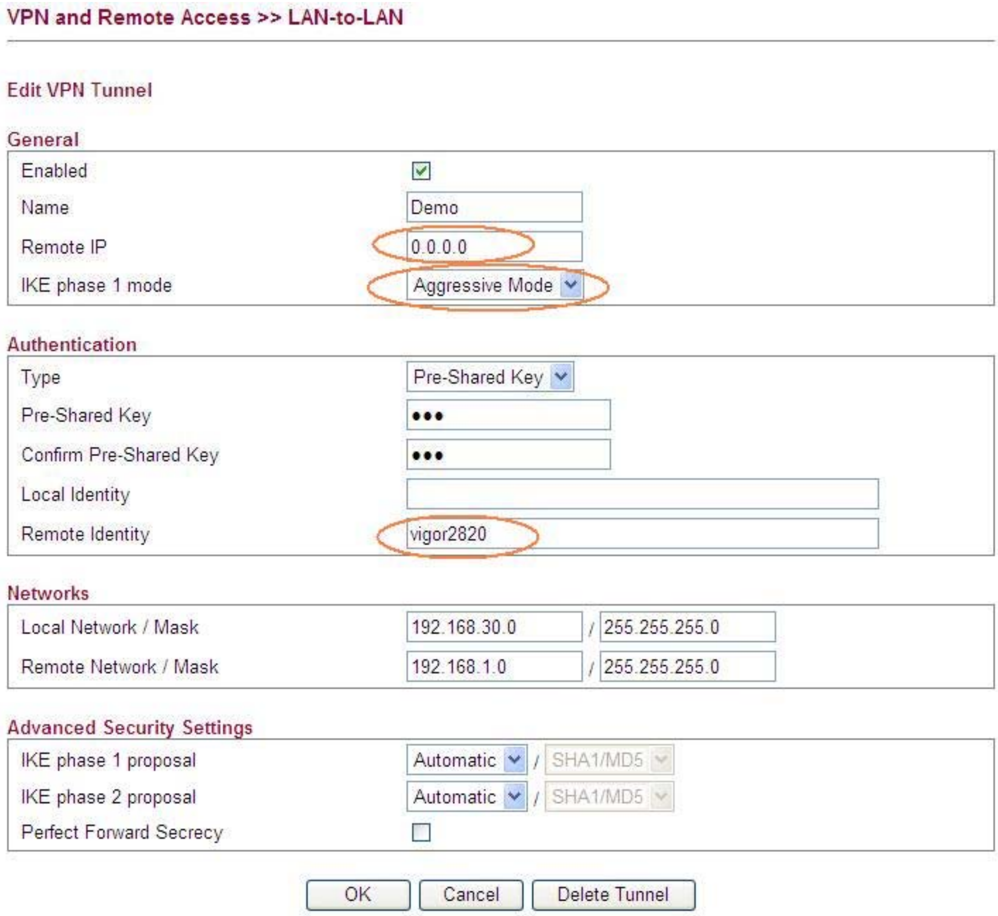
When you select **Automatic**	AES-128, MD5; AES-128, SHA1;
	AES-192, MD5; AES-192, SHA1;
	AES-256, MD5; AES-256, SHA1;
	3DES, SHA1; 3DES, MD5

When you select **3DES**	3DES, MD5; 3DES, SHA1
When you select **AES(any)**	AES-256, MD5; AES-256, SHA1
When you select **AES-128**	AES-128, MD5; AES-128, SHA1
When you select **AES-192**	AES-192, MD5; AES-192, SHA1
When you select **AES-256**	AES-256, MD5; AES-256, SHA1

Case 2: VPN direction from Vigor2820 to Vigor1000

VPN configuration on Vigor1000

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN-to-LAN

Edit VPN Tunnel

General

Enabled	☑
Name	Demo
Remote IP	0.0.0.0
IKE phase 1 mode	Aggressive Mode

Authentication

Type	Pre-Shared Key
Pre-Shared Key	●●●
Confirm Pre-Shared Key	●●●
Local Identity	
Remote Identity	vigor2820

Networks

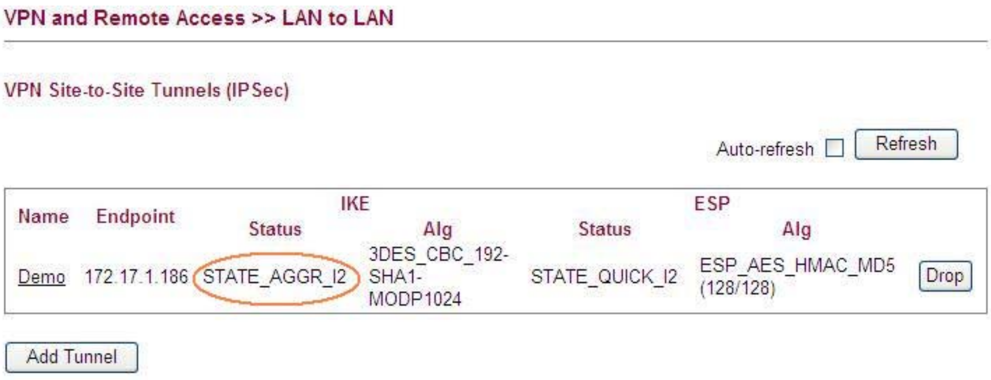
Local Network / Mask	192.168.30.0 / 255.255.255.0
Remote Network / Mask	192.168.1.0 / 255.255.255.0

Advanced Security Settings

IKE phase 1 proposal	Automatic / SHA1/MD5
IKE phase 2 proposal	Automatic / SHA1/MD5
Perfect Forward Secrecy	□

2. Enable it and give it a name. In this example the profile name is “Demo”.
3. Enter 0.0.0.0 in the Remote IP field.
4. Select Aggressive Mode as IKE phase 1 mode.
5. Setup a pre-shared key, which must be the same as in Vigor2820.
6. Setup the Local Identity and Remote Identity, which are for Vigor1000 and Vigor2820 respectively.

   During IPSec Aggressive mode negotiation, the VPN client must send its identity to the VPN server for verification. The VPN client may also verify the identity of the VPN server, which is optional. As VPN client Vigor2820 don’t verify the identity of VPN server. So in this example we just setup ‘vigor2820’ as the identity of Vigor2820.
7. Enter Vigor1000’s private network in the Local Network / Mask field.
8. Enter Vigor2820’s private network in the Remote Network / Mask field.
9. Use default value “Automatic” for IKE phase 1 and phase 2 proposals.
10. After the VPN is connected, you can monitor the status.



VPN and Remote Access >> LAN to LAN

VPN Site-to-Site Tunnels (IPSec)

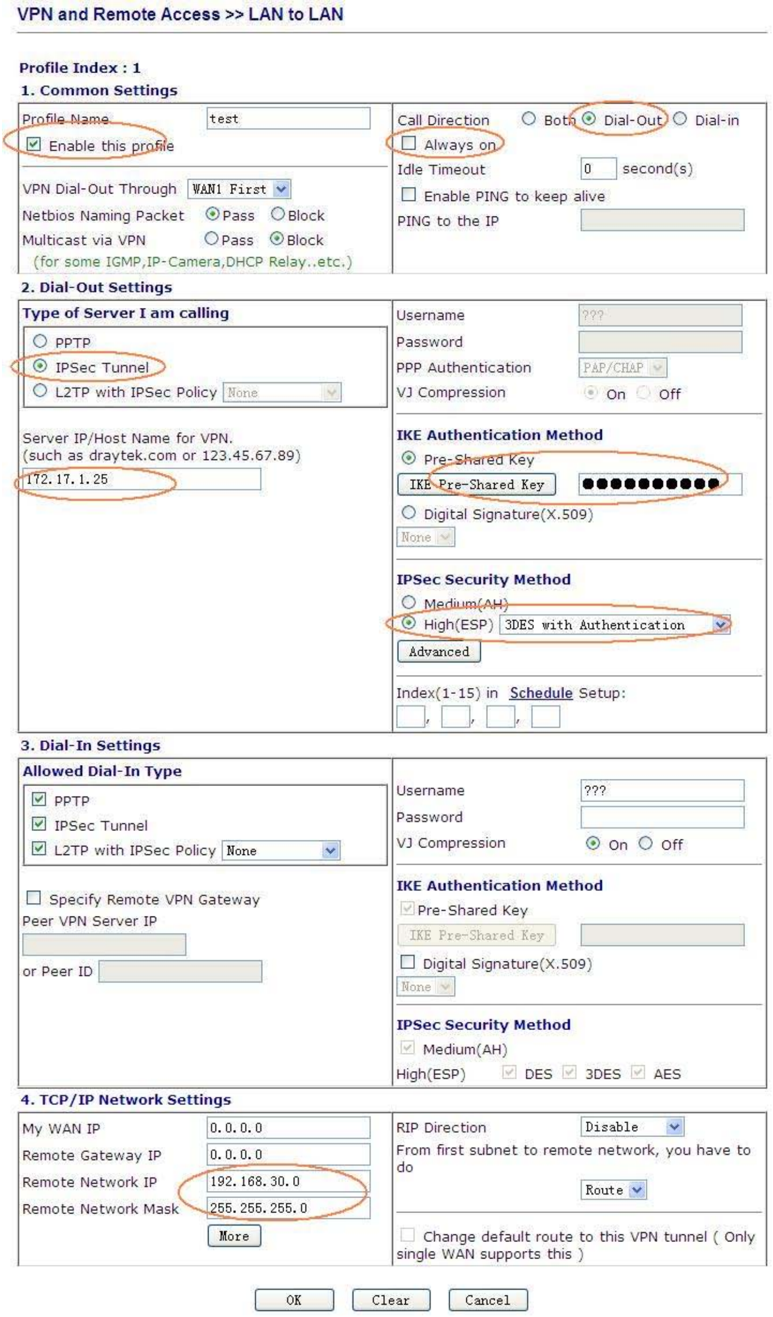
Auto-refresh □ Refresh

Name	Endpoint	IKE Status	IKE Alg	ESP Status	ESP Alg	
Demo	172.17.1.186	STATE_AGGR_I2	3DES_CBC_192-SHA1-MODP1024	STATE_QUICK_I2	ESP_AES_HMAC_MD5 (128/128)	Drop

Add Tunnel

VPN configuration on Vigor2820

1. Create a LAN-to-LAN profile.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: test

☑ Enable this profile

VPN Dial-Out Through: WAN1 First

Netbios Naming Packet: ● Pass ○ Block

Multicast via VPN: ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ● Dial-Out ○ Dial-in

□ Always on

Idle Timeout: 0 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

172.17.1.25

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key: ●●●●●●●●●●

○ Digital Signature(X.509)

None

IPSec Security Method

○ Medium(AH)

● High(ESP): 3DES with Authentication

Advanced

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

3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy: None

□ Specify Remote VPN Gateway

Peer VPN Server IP:

or Peer ID:

Username: ???

Password:

VJ Compression: ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

None

IPSec Security Method

☑ Medium(AH)

High(ESP): ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.30.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

OK Clear Cancel

2. Enable it and give it a name. In this example the profile name is “test”.

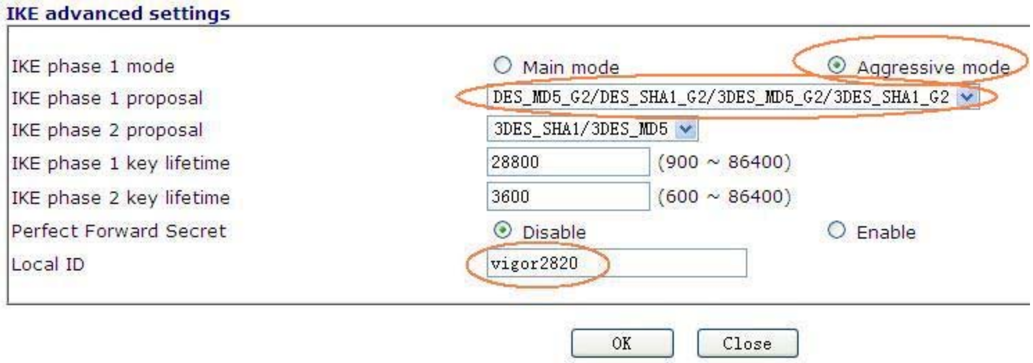
3. Select Dial-Out as **Call Direction** and enable **Always on**.

4. Select **IPSec Tunnel** and enter Vigor1000’s WAN IP address in the **Server IP/Host Name for VPN** field.

5. Setup a **pre-shared key**, which must be the same as in Vigor1000.

6. Select **ESP (High)** and **3DES with Authentication**.

7. Press the **Advanced** button.



IKE advanced settings

IKE phase 1 mode	○ Main mode	● Aggressive mode
IKE phase 1 proposal	DES_MD5_G2/DES_SHA1_G2/3DES_MD5_G2/3DES_SHA1_G2	
IKE phase 2 proposal	3DES_SHA1/3DES_MD5	
IKE phase 1 key lifetime	28800 (900 ~ 86400)	
IKE phase 2 key lifetime	3600 (600 ~ 86400)	
Perfect Forward Secret	● Disable	○ Enable
Local ID	vigor2820	

8. In the pop-up window, please select **Aggressive mode** and select “**DES_MD5_G2/ DES_SHA1_G2/3DES_MD5_G2/3DES_SHA1_G2**” as IKE phase 1 proposal. Enter vigor2820 in the **Local ID** field. Click **OK** to return to the profile setting page.

9. Enter Vigor1000’s private network in the **Remote Network IP / Mask** field.

10. Click **OK**.

3.4 How to configure settings for DLNA Service in Vigor1000

Introduction

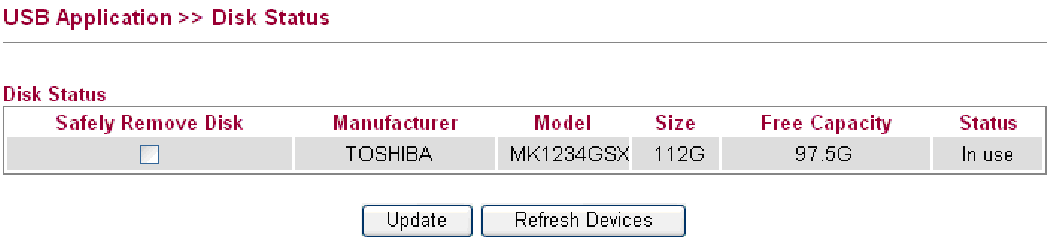
DLNA (Digital Living Network Alliance) is a framework which personal computer, HDD video recorder, television and other digital devices can share each other data through network connection. The DLNA devices are divided into two functions. One is server side which transmits images, music and video, and the other is client side which receives data only. Some devices support both functions. Vigor1000 can install server program onto the connected USB storage device. Clients with equipments supporting DLNA can play the files stored in the USB storage device connected to Vigor1000 through the network.

At present, the supported type and format for Video & Audio are listed as follows:

Supported Video Format:	asf, avi, dv, divx, wmv, mjpg, mjpeg, mpeg, mpg, mpe, mp2p, vob, mp2t, m1v, m2v, m4v, m4p, mp4ps, ts, ogm, mkv, rmvb, mov, qt, hdmov
Supported Audio Format:	aac, ac3, aif, aiff, at3p, au, snd, dts, rmi, mp1, mp2, mp3, mp4, mpa, ogg, wav, pcm, lpcm, l16, wma, mka, ra, rm, ram, flac
Supported Image Format:	bmp, ico, gif, jpeg, jpg, jpe, pcd, png, pnm, ppm, qti, qtf, qtif, tif, tiff

Configuration

1. Insert USB storage device into the USB slot of Vigor1000. Then, open **USB Application>>Disk Status** to check the connection status. If it is connected successfully, the general information of that device will be shown on the screen.

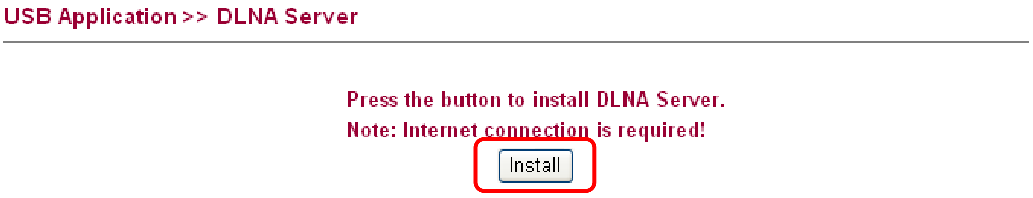


USB Application >> Disk Status

Disk Status

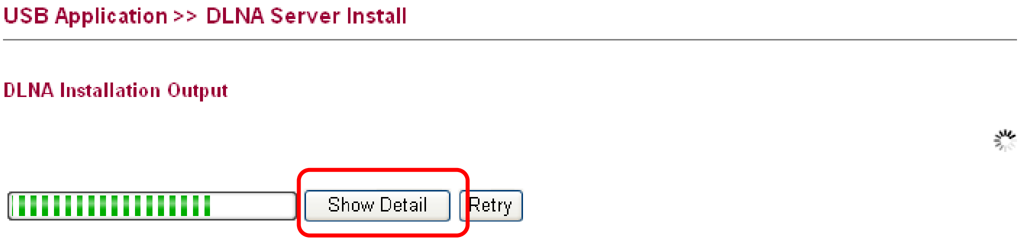
Safely Remove Disk	Manufacturer	Model	Size	Free Capacity	Status
□	TOSHIBA	MK1234GSX	112G	97.5G	In use

2. Make sure Internet connection is done. Open **USB Application>>DLNA Server** and click **Install** to install DLNA service into the USB storage device.



USB Application >> DLNA Server

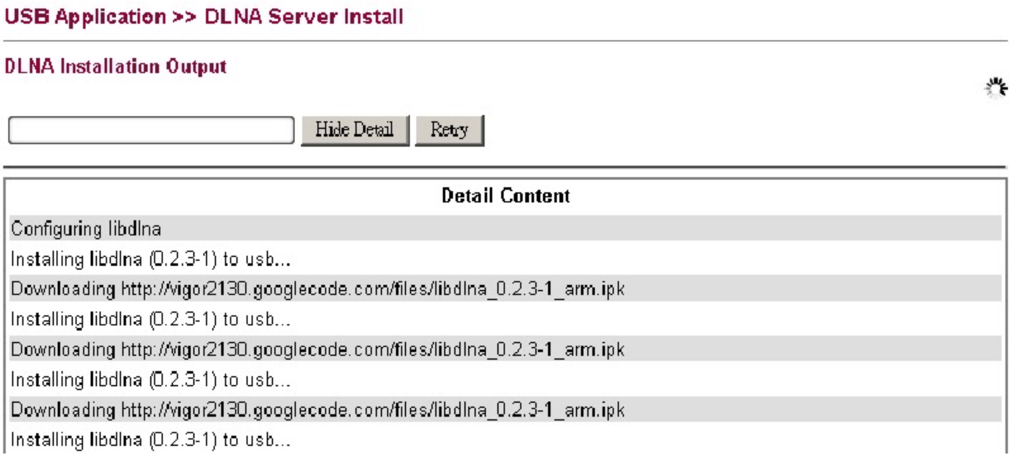
Press the button to install DLNA Server.
Note: Internet connection is required!



USB Application >> DLNA Server Install

DLNA Installation Output

3. During the process of installation, you can click **Show Detail** to view the installation procedure.



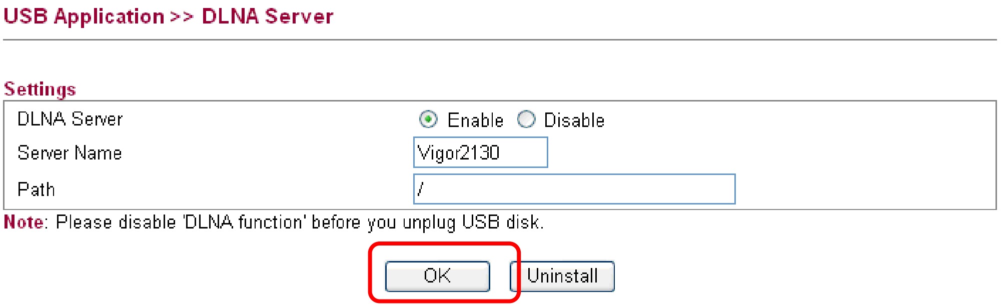
USB Application >> DLNA Server Install

DLNA Installation Output

Detail Content

```
Configuring libdlna
Installing libdlna (0.2.3-1) to usb...
Downloading http://vigor2130.googlecode.com/files/libdlna_0.2.3-1_arm.ipk
Installing libdlna (0.2.3-1) to usb...
Downloading http://vigor2130.googlecode.com/files/libdlna_0.2.3-1_arm.ipk
Installing libdlna (0.2.3-1) to usb...
Downloading http://vigor2130.googlecode.com/files/libdlna_0.2.3-1_arm.ipk
Installing libdlna (0.2.3-1) to usb...
```

4. After finished the service installation, the configuration page will be open automatically. Please click **Enable** and type a name in the field of **Server Name**. Then, click **OK** to activate DLNA service.



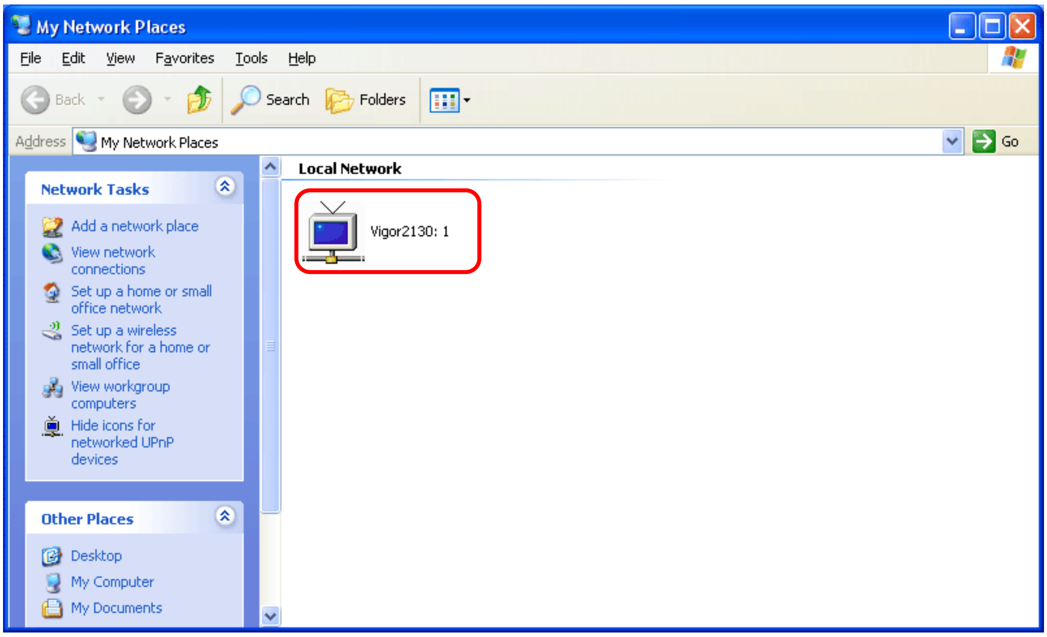
USB Application >> DLNA Server

Settings

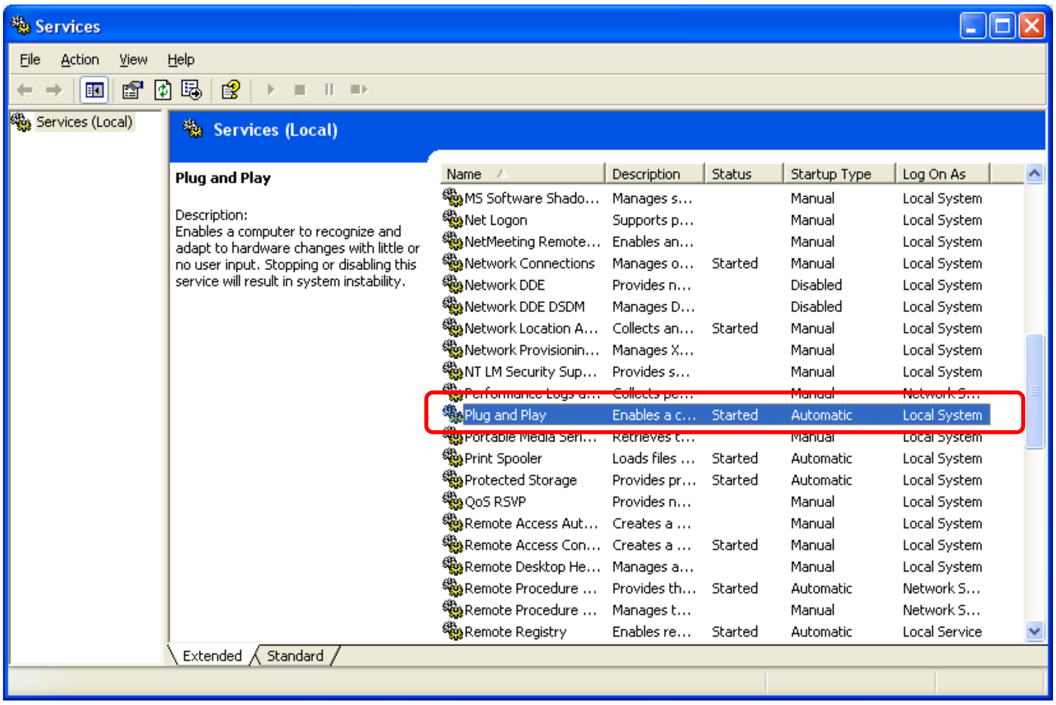
DLNA Server	● Enable ○ Disable
Server Name	Vigor2130
Path	/

Note: Please disable 'DLNA function' before you unplug USB disk.

5. After enabled successfully, new media device can be seen in **My Network Places**. The name of the media device is the Server Name configured in Step 4.



Note: If you cannot see the media device in Network view, please check and make sure the UPnP service has been enabled **Control Panel>>Administrative Tools >>Services**.

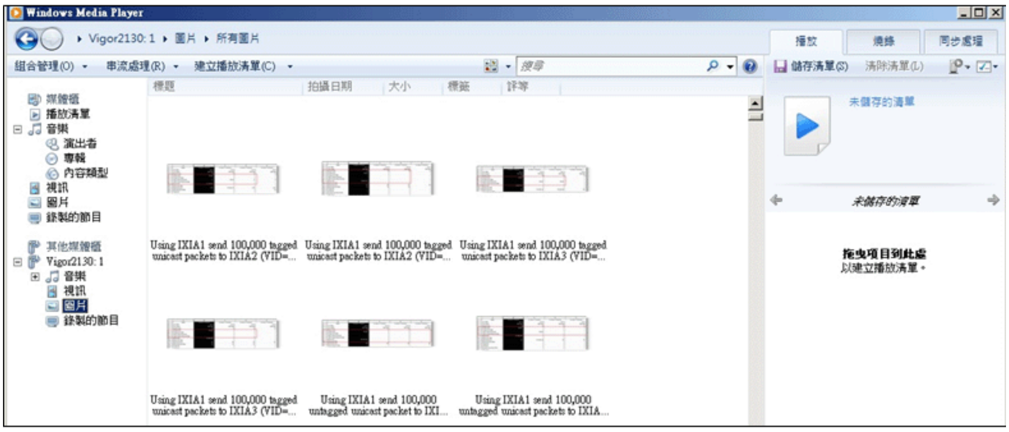


Plug and Play

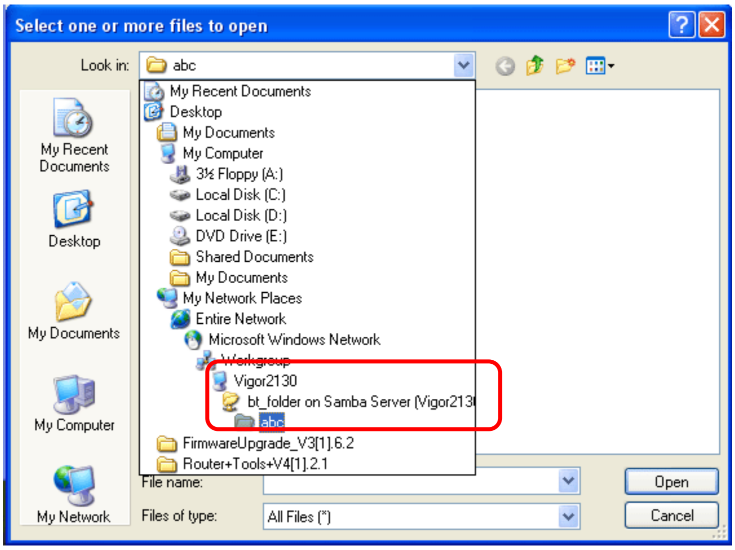
Description:
Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

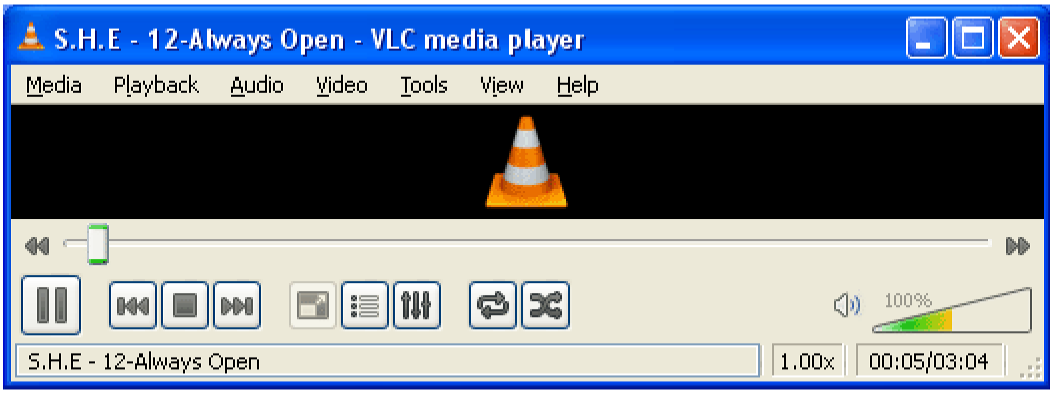
Name	Description	Status	Startup Type	Log On As
MS Software Shado…	Manages s…		Manual	Local System
Net Logon	Supports p…		Manual	Local System
NetMeeting Remote…	Enables an…		Manual	Local System
Network Connections	Manages o…	Started	Manual	Local System
Network DDE	Provides n…		Disabled	Local System
Network DDE DSDM	Manages D…		Disabled	Local System
Network Location A…	Collects an…	Started	Manual	Local System
Network Provisionin…	Manages X…		Manual	Local System
NT LM Security Sup…	Provides s…		Manual	Local System
Performance Logs a…	Collects pe…		Manual	Network S…
Plug and Play	Enables a c…	Started	Automatic	Local System
Portable Media Seri…	Retrieves t…		Manual	Local System
Print Spooler	Loads files …	Started	Automatic	Local System
Protected Storage	Provides pr…	Started	Automatic	Local System
QoS RSVP	Provides n…		Manual	Local System
Remote Access Aut…	Creates a …		Manual	Local System
Remote Access Con…	Creates a …	Started	Manual	Local System
Remote Desktop He…	Manages a…		Manual	Local System
Remote Procedure …	Provides th…	Started	Automatic	Network S…
Remote Procedure …	Manages t…		Manual	Network S…
Remote Registry	Enables re…	Started	Automatic	Local Service

6. For the users of Windows7, please use Windows Media Player (WMP) to browse and play the files stored in the new service device.


Windows Media Player
Vigor2130: 1 ▸ 圖片 ▸ 所有圖片
播放
燒錄
同步處理
組合管理(O)
串流處理(R)
建立播放清單(C)
搜尋
儲存清單(S)
清除清單(L)
標題
拍攝日期
大小
標籤
評等
媒體櫃
播放清單
音樂
演出者
專輯
內容類型
視訊
圖片
錄製的節目
其他媒體櫃
Vigor2130: 1
音樂
視訊
圖片
錄製的節目
Using IXIA1 send 100,000 tagged unicast packets to IXIA2 (VID=...
Using IXIA1 send 100,000 tagged unicast packets to IXIA2 (VID=...
Using IXIA1 send 100,000 tagged unicast packets to IXIA3 (VID=...
Using IXIA1 send 100,000 tagged unicast packets to IXIA3 (VID=...
Using IXIA1 send 100,000 untagged unicast packet to IXI...
Using IXIA1 send 100,000 untagged unicast packets to IXIA...
未儲存的清單
未儲存的清單
拖曳項目到此處
以建立播放清單。

For other systems, please use VLC media player (downloaded from Internet) to browse/locate and play the files.





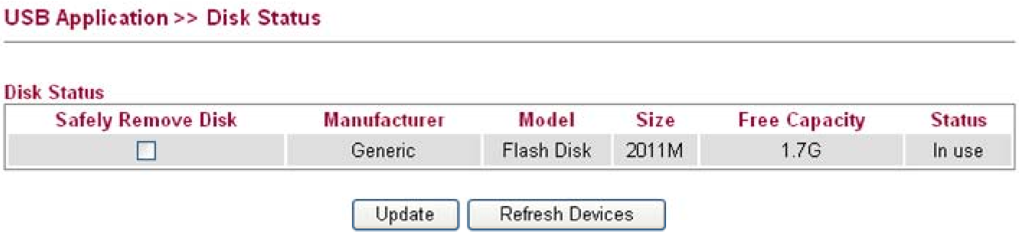
Notes

- Before removing USB storage device, please **DISABLE** DLNA service and then remove the device.
- The audio and video files might not be played normally due to unrecognized equipment set in client.

3.5 How to download BT Torrent to USB Device via Vigor Router

Download BT Torrent

1. Plug USB storage disk into the USB slot of Vigor1000. Access into the web configuration interface of Vigor1000.
2. Open **USB Application>>Disk Status**.
3. Wait for few seconds for the router to detect it. If the disk is detected, it will be shown as the following figure.

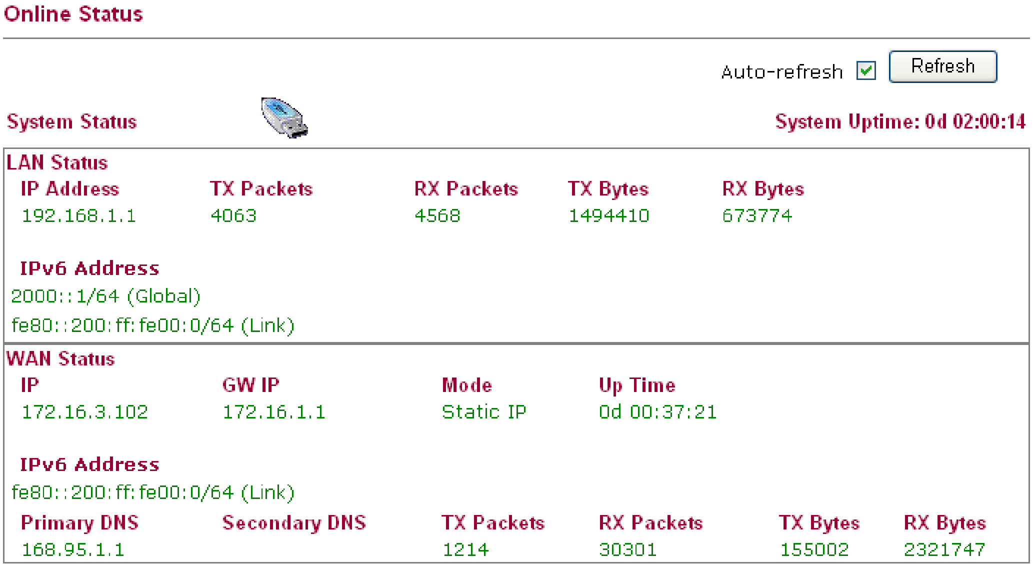


USB Application >> Disk Status

Disk Status

Safely Remove Disk	Manufacturer	Model	Size	Free Capacity	Status
□	Generic	Flash Disk	2011M	1.7G	In use

4. Make sure that WAN connection has been established.



Online Status

Auto-refresh ☑ Refresh

System Status

System Uptime: 0d 02:00:14

LAN Status

IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.1	4063	4568	1494410	673774

IPv6 Address
2000::1/64 (Global)
fe80::200:ff:fe00:0/64 (Link)

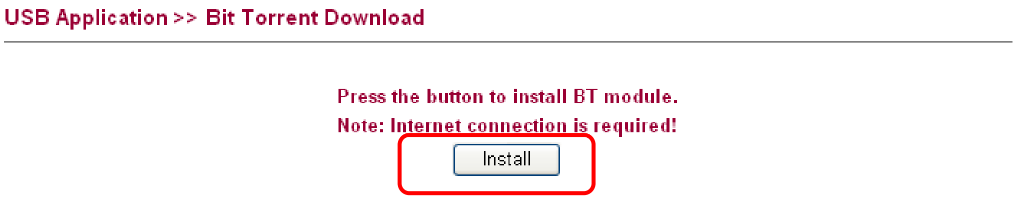
WAN Status

IP	GW IP	Mode	Up Time
172.16.3.102	172.16.1.1	Static IP	0d 00:37:21

IPv6 Address
fe80::200:ff:fe00:0/64 (Link)

Primary DNS	Secondary DNS	TX Packets	RX Packets	TX Bytes	RX Bytes
168.95.1.1		1214	30301	155002	2321747

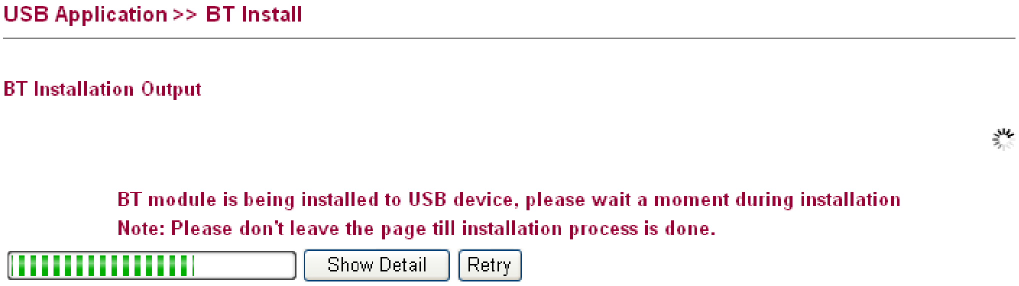
5. Open **USB Application** >> **Bit Torrent Download**. Click **Install** to install BT module from Internet to USB device.



USB Application >> Bit Torrent Download

Press the button to install BT module.
Note: Internet connection is required!

6. Simply wait for a few minutes to finish the installation.



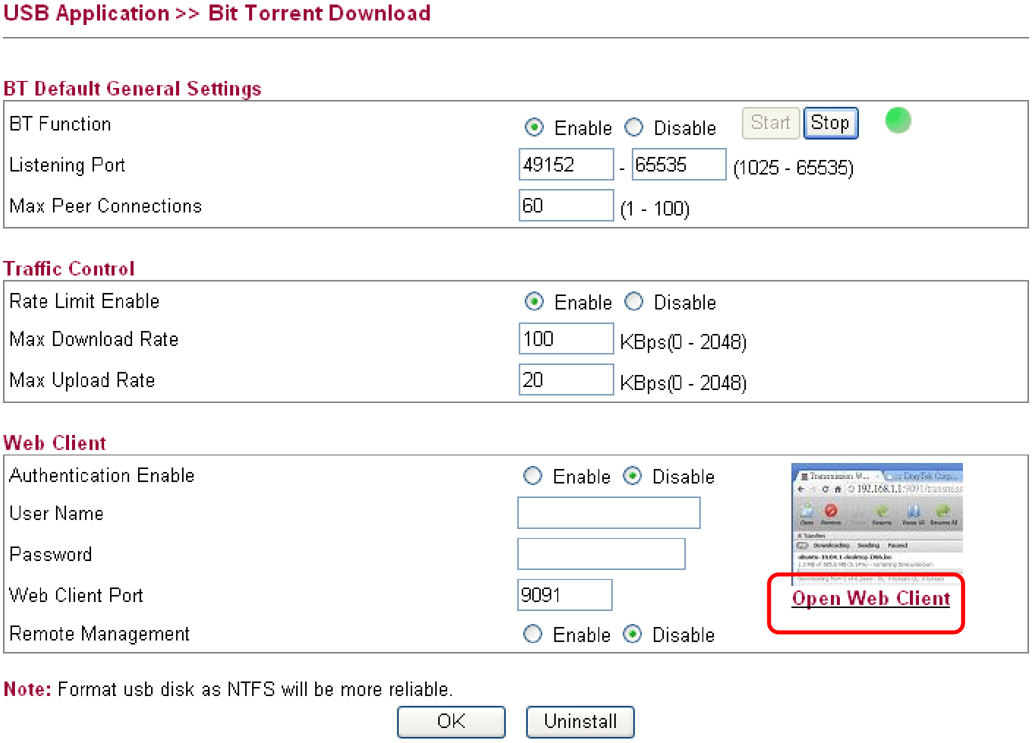
USB Application >> BT Install

BT Installation Output

BT module is being installed to USB device, please wait a moment during installation

Note: Please don't leave the page till installation process is done.

7. When the installation is finished, the following page will be displayed.



USB Application >> Bit Torrent Download

BT Default General Settings

BT Function	● Enable ○ Disable Start Stop
Listening Port	49152 - 65535 (1025 - 65535)
Max Peer Connections	60 (1 - 100)

Traffic Control

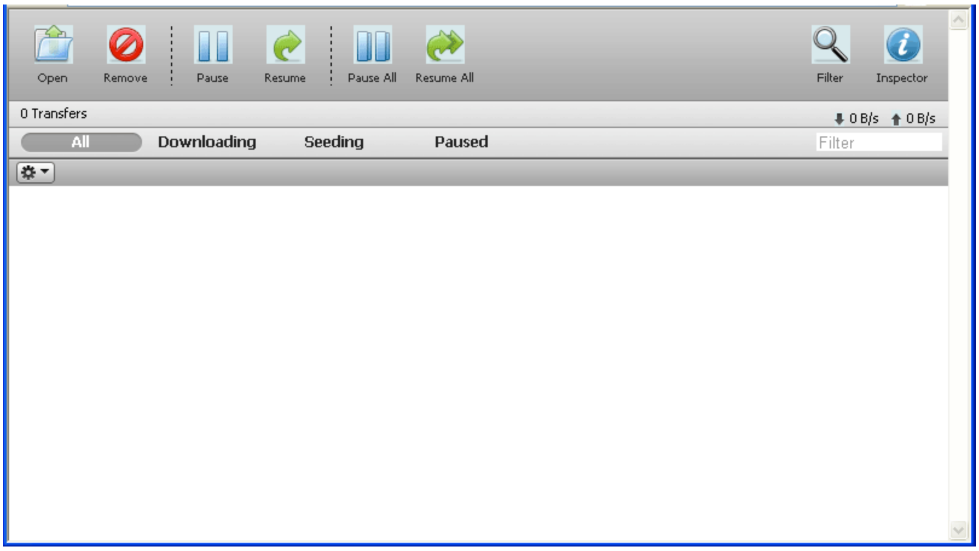
Rate Limit Enable	● Enable ○ Disable
Max Download Rate	100 KBps(0 - 2048)
Max Upload Rate	20 KBps(0 - 2048)

Web Client

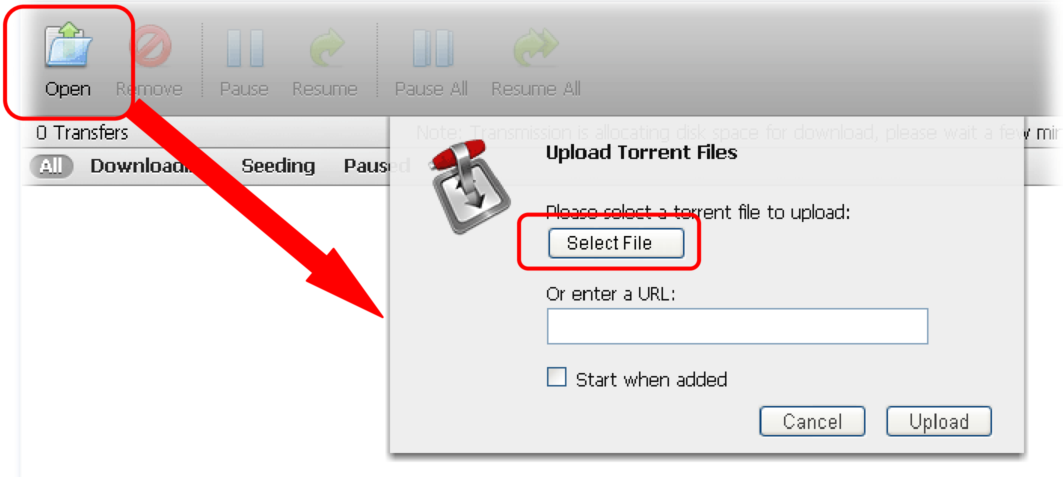
Authentication Enable	○ Enable ● Disable
User Name	
Password	
Web Client Port	9091
Remote Management	○ Enable ● Disable

Note: Format usb disk as NTFS will be more reliable.

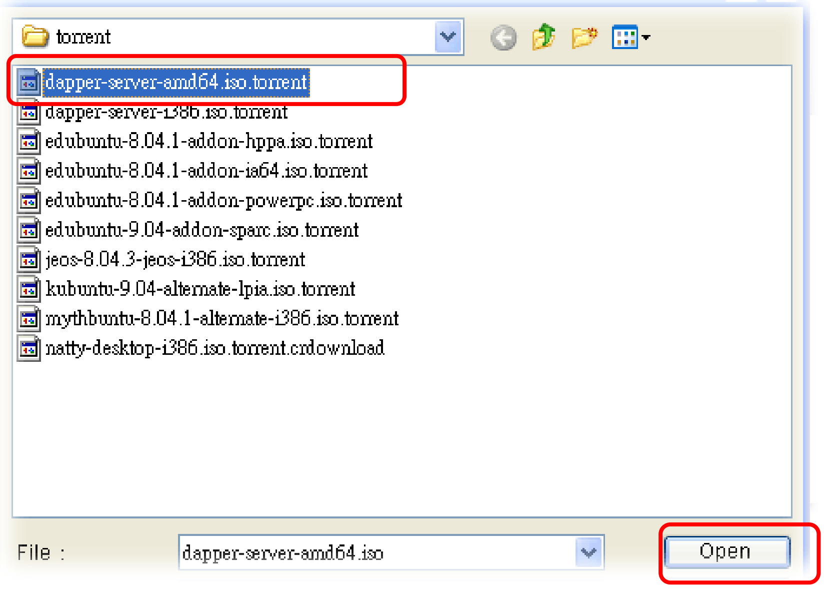
8. Click the link of **Open Web Client** to open another window.



9. Click **Open**. A pop up dialog will appear.

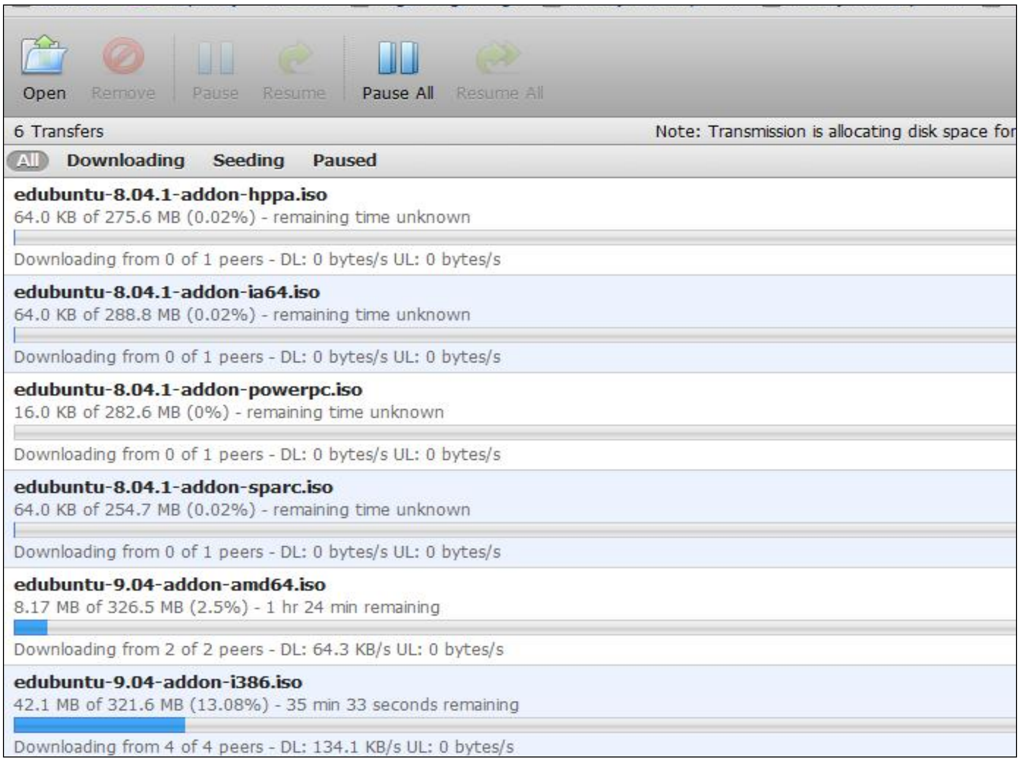


10. Click **Select File** to open the following dialog. Choose the seed of BT torrent file and click **Open**.


torrent
dapper-server-amd64.iso.torrent
dapper-server-i386.iso.torrent
edubuntu-8.04.1-addon-hppa.iso.torrent
edubuntu-8.04.1-addon-ia64.iso.torrent
edubuntu-8.04.1-addon-powerpc.iso.torrent
edubuntu-9.04-addon-sparc.iso.torrent
jeos-8.04.3-jeos-i386.iso.torrent
kubuntu-9.04-alternate-lpia.iso.torrent
mythbuntu-8.04.1-alternate-i386.iso.torrent
natty-desktop-i386.iso.torrent.crdownload
File :
dapper-server-amd64.iso
Open

Note: Before uploading torrent files to the router, please search from Internet and store the seed of the BT torrent on our hard disk first.

11. Next, the router will start to download the file to the USB disk. You can add new seed of torrent file one by one by clicking **Open** to let the router download them at one time.



6 Transfers

Note: Transmission is allocating disk space for

All Downloading Seeding Paused

edubuntu-8.04.1-addon-hppa.iso
64.0 KB of 275.6 MB (0.02%) - remaining time unknown
Downloading from 0 of 1 peers - DL: 0 bytes/s UL: 0 bytes/s

edubuntu-8.04.1-addon-ia64.iso
64.0 KB of 288.8 MB (0.02%) - remaining time unknown
Downloading from 0 of 1 peers - DL: 0 bytes/s UL: 0 bytes/s

edubuntu-8.04.1-addon-powerpc.iso
16.0 KB of 282.6 MB (0%) - remaining time unknown
Downloading from 0 of 1 peers - DL: 0 bytes/s UL: 0 bytes/s

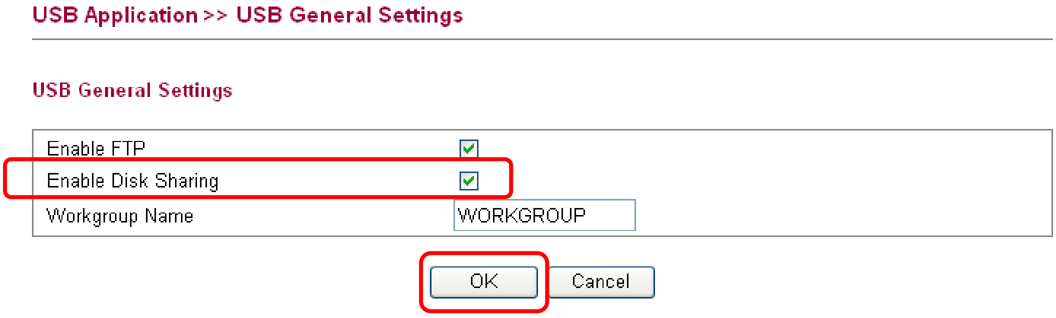
edubuntu-8.04.1-addon-sparc.iso
64.0 KB of 254.7 MB (0.02%) - remaining time unknown
Downloading from 0 of 1 peers - DL: 0 bytes/s UL: 0 bytes/s

edubuntu-9.04-addon-amd64.iso
8.17 MB of 326.5 MB (2.5%) - 1 hr 24 min remaining
Downloading from 2 of 2 peers - DL: 64.3 KB/s UL: 0 bytes/s

edubuntu-9.04-addon-i386.iso
42.1 MB of 321.6 MB (13.08%) - 35 min 33 seconds remaining
Downloading from 4 of 4 peers - DL: 134.1 KB/s UL: 0 bytes/s

Share the file after downloading completed

1. Access into Vigor1000 web configuration interface and open **USB Application** >> **USB General Settings**. Enable the **Disk Sharing** function by checking the box and click **OK**.

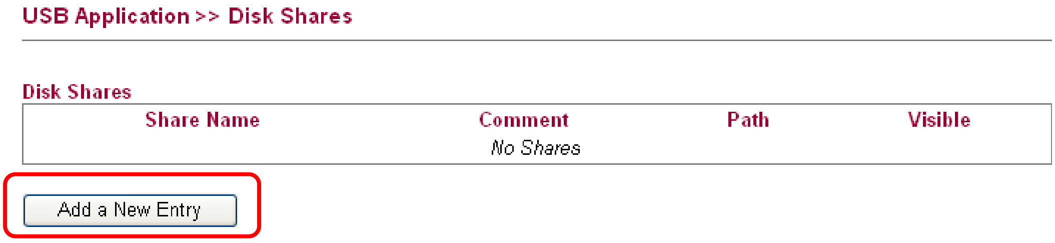


USB Application >> USB General Settings

USB General Settings

Enable FTP	☑
Enable Disk Sharing	☑
Workgroup Name	WORKGROUP

2. Open **USB Application** >> **Disk Shares**. Click **Add a New Entry.**

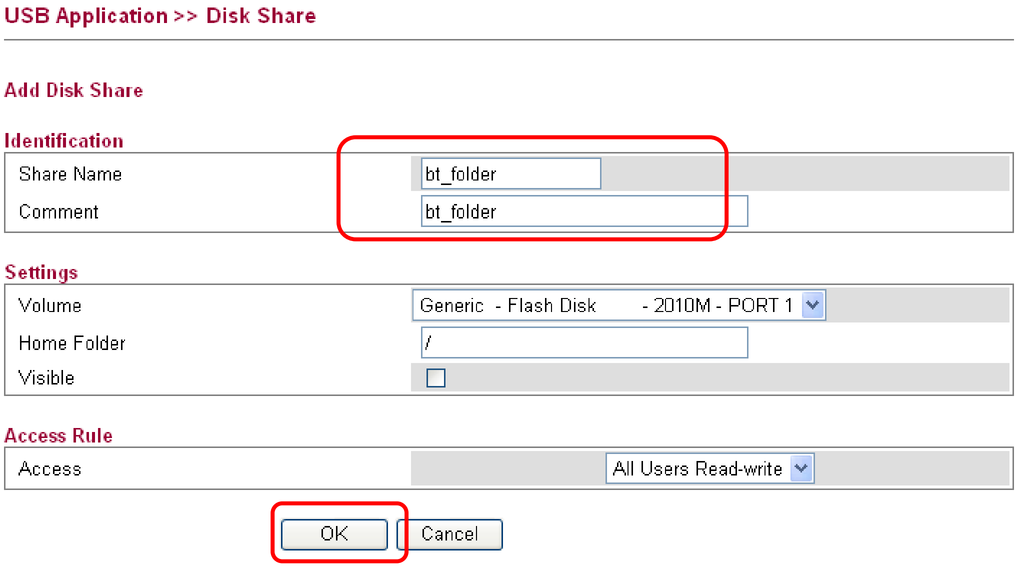


USB Application >> Disk Shares

Disk Shares

Share Name	Comment	Path	Visible
	No Shares		

3. In the following screen, add a new entry for the sharing folder/name. In this case, we give a name of **bt_folder** as **Share Nam**e for home folder ("/") . Click **OK**.



USB Application >> Disk Share

Add Disk Share

Identification

Share Name	bt_folder
Comment	bt_folder

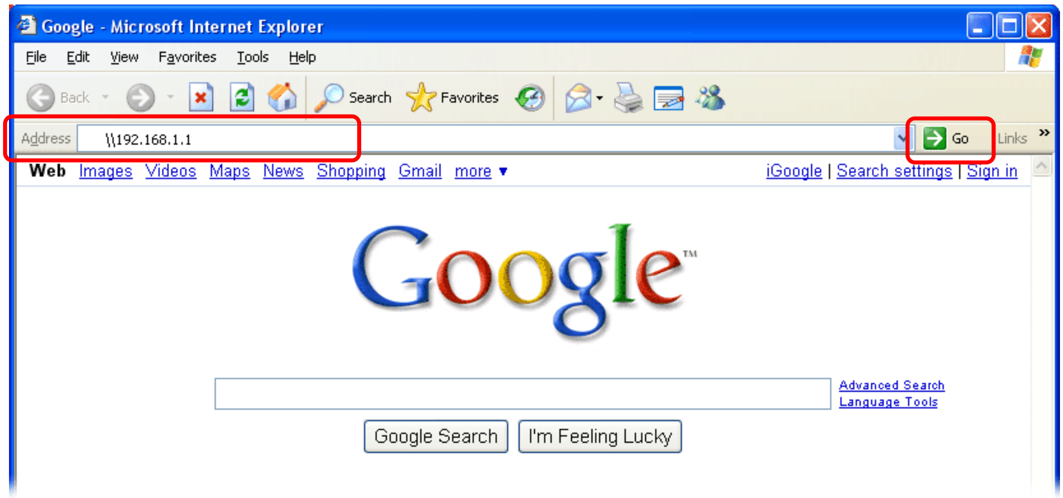
Settings

Volume	Generic - Flash Disk - 2010M - PORT 1
Home Folder	/
Visible	□

Access Rule

Access	All Users Read-write

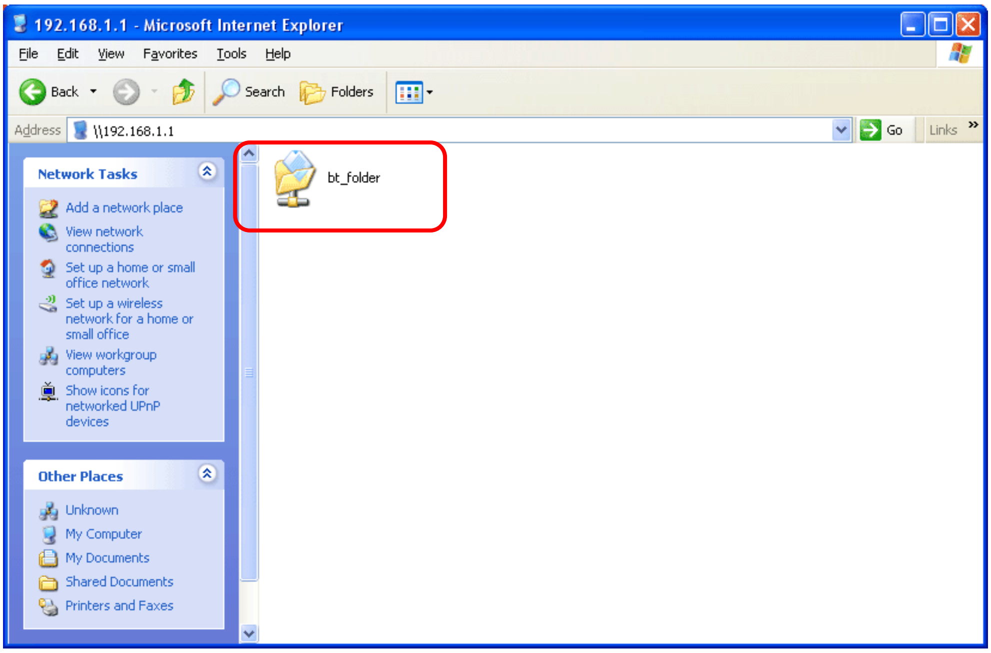
4. Now, **PCs in LAN** connected to Vigor1000 can open a browser from his / her computer. Simply type **"\\192.168.1.1**" in the field of **Address** and then click **Go**.



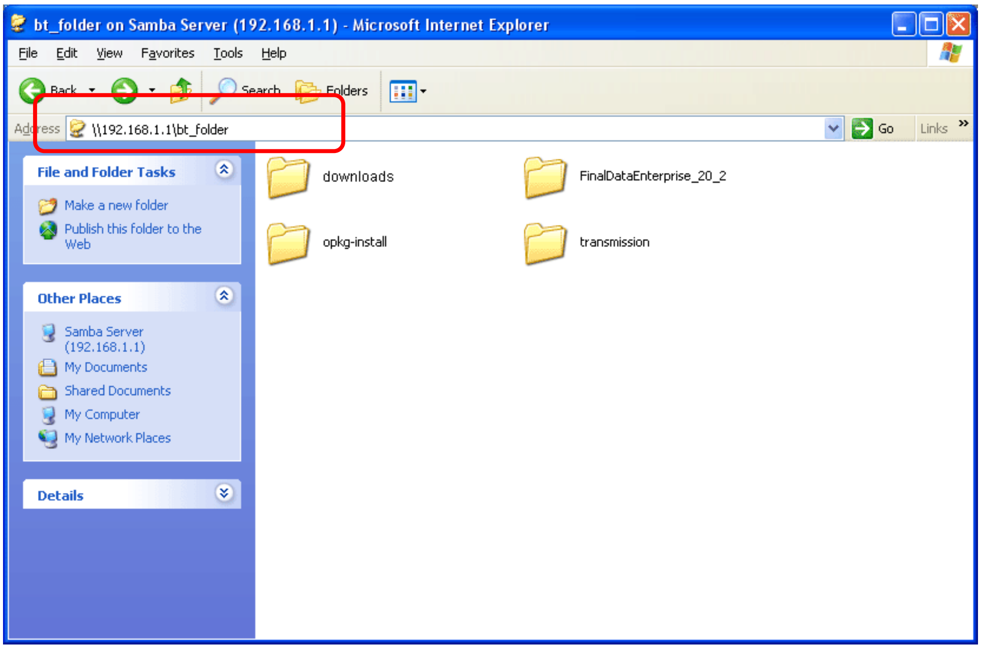
Address: \\192.168.1.1

Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Links
Web Images Videos Maps News Shopping Gmail more ▾
iGoogle | Search settings | Sign in
Google
Advanced Search
Language Tools
Google Search
I'm Feeling Lucky

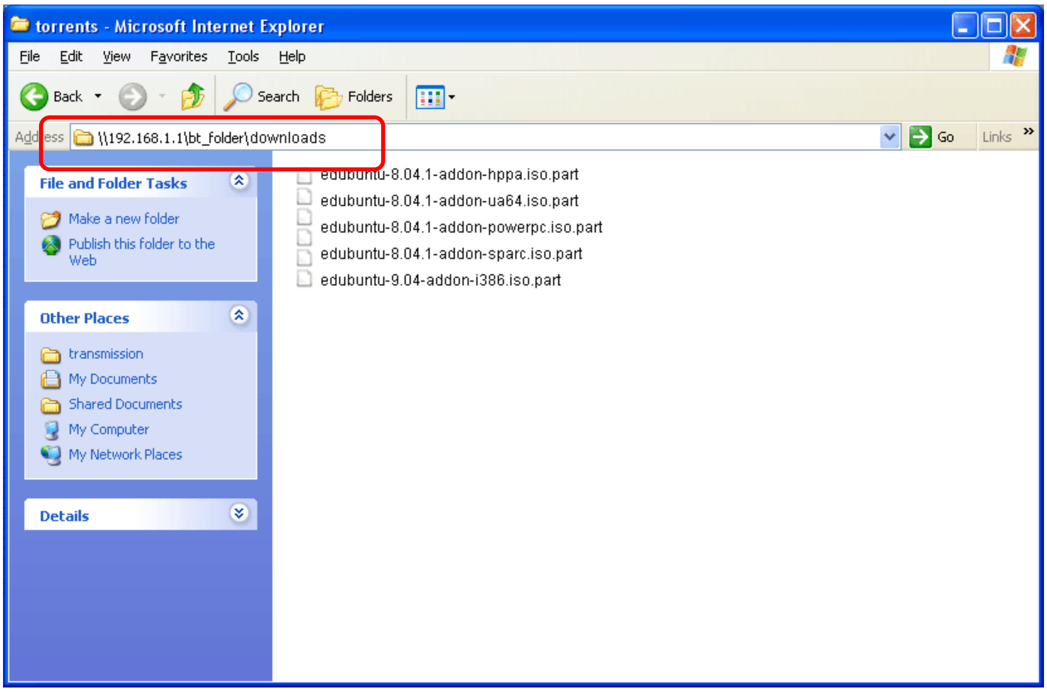
5. The sharing disk with the name of "**bt_folder**" created above will be shown as the following figure.



6. Double click **bt_folder** to view the files in the disk.



7. If you want to check the BT Torrent files downloaded from Internet to USB disk, access into **bt_folder>>downloads.**



edubuntu-8.04.1-addon-hppa.iso.part
edubuntu-8.04.1-addon-ua64.iso.part
edubuntu-8.04.1-addon-powerpc.iso.part
edubuntu-8.04.1-addon-sparc.iso.part
edubuntu-9.04-addon-i386.iso.part

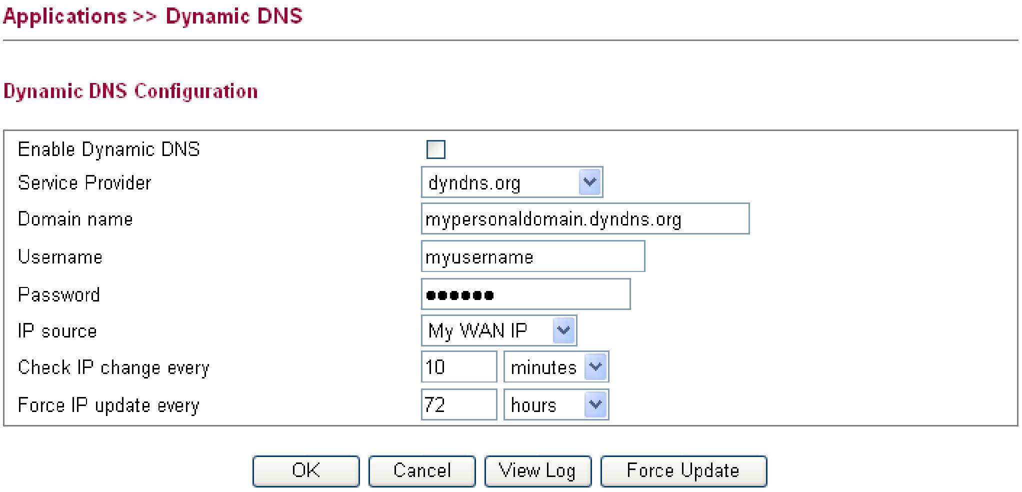
(**Note**: While the file is downloading, the file extension name will be “part”.)

3.6 How to configure Dynamic DNS Service on Vigor1000

DDNS stands for Dynamic DNS. Simply put, using this service gives a name to your IP. If you are hosting something on your line, people wouldn't have to bother typing your IP. They can just type in your domain name. It also helps when your ISP only provides dynamic IP address. Users won't need to discover what your new IP is, they can simply type your domain name. Vigor1000 supports dyndns.org, no-ip.org, chang-ip.com, zoneedit.com, and freedns.afraid.org. Here we are going to show you how to setup this function on Vigor1000.

Here is the way to configure well known free dynamic DNS service like dyndns.org, no-ip.org …etc.

1. Access into Vigor1000 web configurator.
2. Go to **Applications** >> **Dynamic DNS** and select one of the service provider in the list.



Applications >> Dynamic DNS

Dynamic DNS Configuration

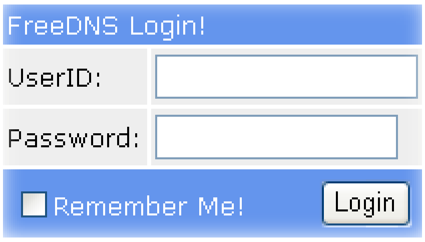
Enable Dynamic DNS	□
Service Provider	dyndns.org
Domain name	mypersonaldomain.dyndns.org
Username	myusername
Password	●●●●●●
IP source	My WAN IP
Check IP change every	10 minutes
Force IP update every	72 hours

Here we take **dyndns.org** as an example to setup the function.

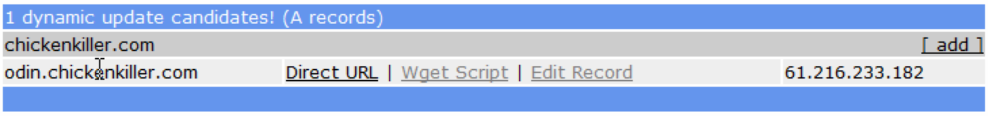
3. Input **Domain name**, **Username**, and **Password** which required by the DDNS provider.
4. Select the IP source as you need. If Vigor1000 is behind another NAT device, you should choose My Internet IP to discover a real public IP address for the DDNS service.

To configure **freedns.afraid.org** service is different than the other well know free DNS service providers. You have to login with your account and password on its website to copy a string which generated in the URL field and lead by a question mark. The next is the step by step to show you how to setup it on Vigor1000.

1. Go to http://freedns.afraid.org/dynamic/ and login with your normal username and password for the **FreeDNS** service.



2. Click **Direct URL** on the domain, you would like to set to your WAN IP address.

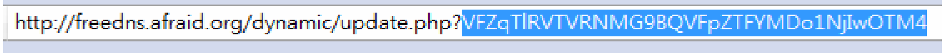


1 dynamic update candidates! (A records)

chickenkiller.com [add]

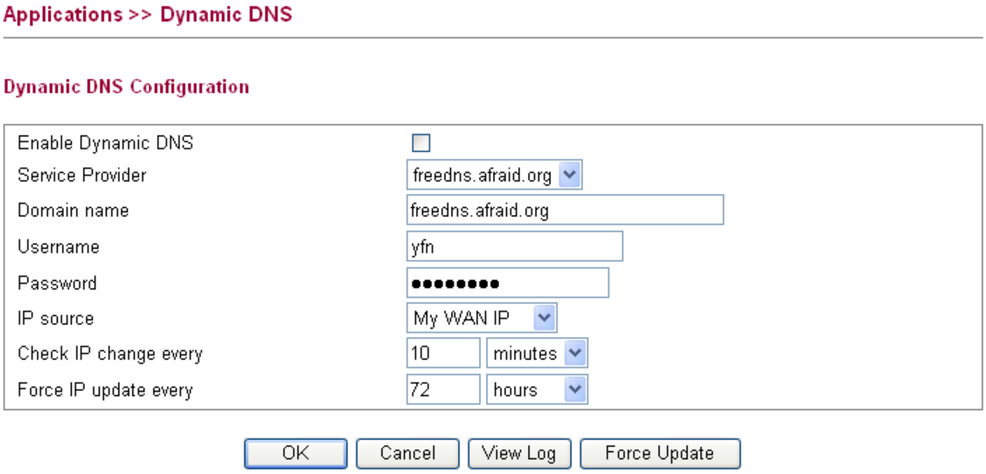
odin.chickenkiller.com Direct URL | Wget Script | Edit Record 61.216.233.182

3. Copy the character strings from the right of the **?** in the address bar.



http://freedns.afraid.org/dynamic/update.php?VFZqTlRVTVRNMG9BQVFpZTFYMDo1NjIwOTM4

4. Login to Vigor1000 by WUI, and go to **Application** >>**Dynamic DNS** page.



Applications >> Dynamic DNS

Dynamic DNS Configuration

Enable Dynamic DNS	□
Service Provider	freedns.afraid.org
Domain name	freedns.afraid.org
Username	yfn
Password	●●●●●●●●●
IP source	My WAN IP
Check IP change every	10 minutes
Force IP update every	72 hours

Select **freedns.afraid.org**, and fill in the username as you applied for the service.

5. Past the strings what you copied on step3 on password field.

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

Now, you can check the service by using `nslookup` command on your computer or check the syslog information on Vigor1000.

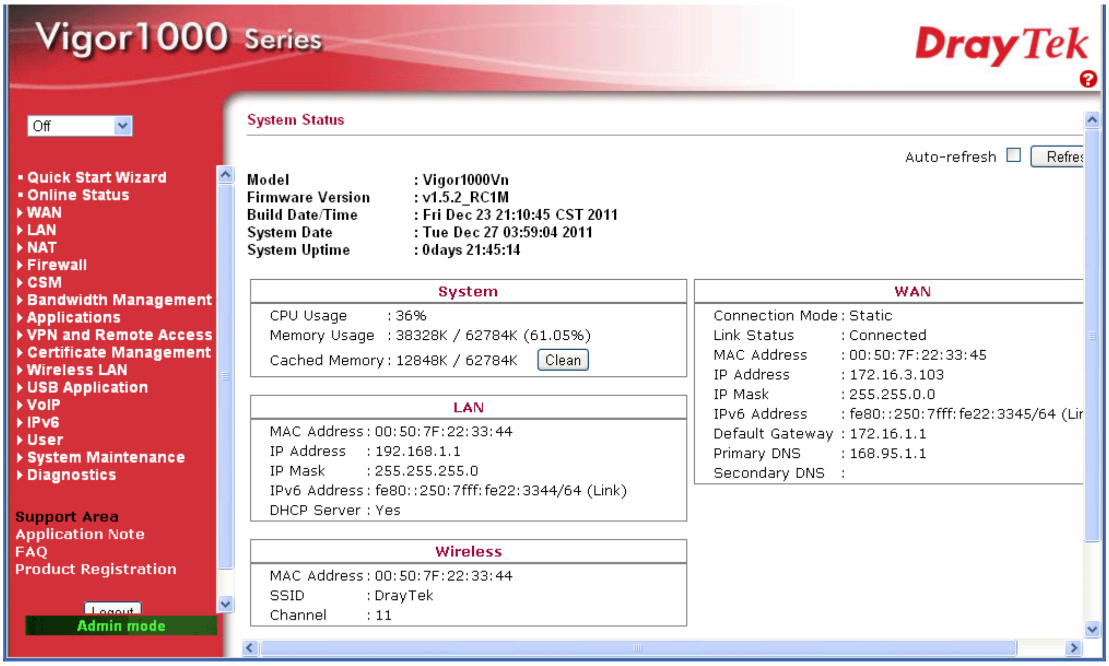
This page is left blank.

4 Web Configuration

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

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

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



System Status

Model : Vigor1000Vn
Firmware Version : v1.5.2_RC1M
Build Date/Time : Fri Dec 23 21:10:45 CST 2011
System Date : Tue Dec 27 03:59:04 2011
System Uptime : 0days 21:45:14

System
CPU Usage : 36%
Memory Usage : 38328K / 62784K (61.05%)
Cached Memory : 12848K / 62784K

LAN
MAC Address : 00:50:7F:22:33:44
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:7fff:fe22:3344/64 (Link)
DHCP Server : Yes

Wireless
MAC Address : 00:50:7F:22:33:44
SSID : DrayTek
Channel : 11

WAN
Connection Mode : Static
Link Status : Connected
MAC Address : 00:50:7F:22:33:45
IP Address : 172.16.3.103
IP Mask : 255.255.0.0
IPv6 Address : fe80::250:7fff:fe22:3345/64 (Lir
Default Gateway : 172.16.1.1
Primary DNS : 168.95.1.1
Secondary DNS :

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.

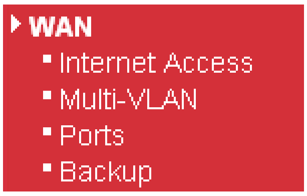
Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor router adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G 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/4G USB Modem allows you to receive 3G/4G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via wireless function of Vigor router, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor router.

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

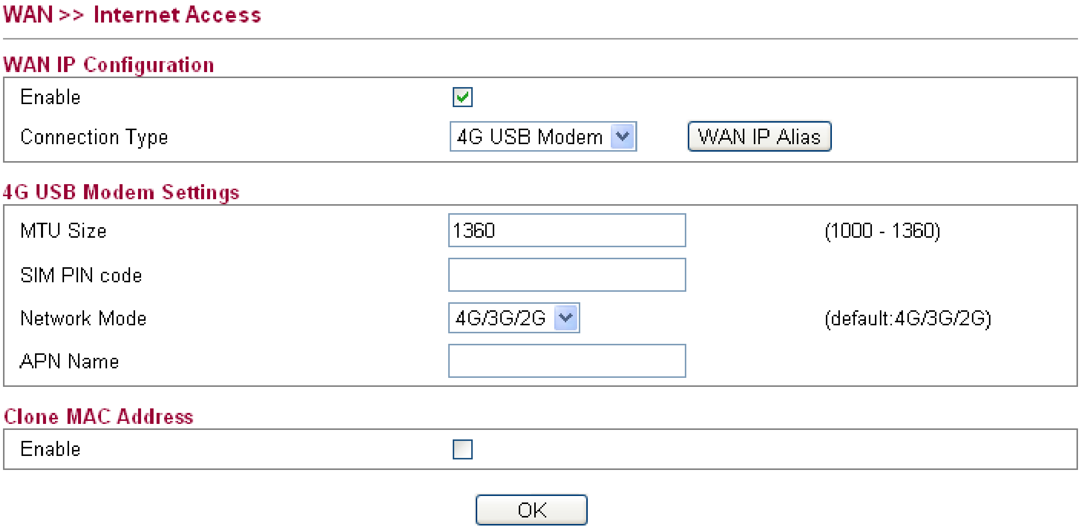
After connecting into the router, 3G/4G Modem will be regarded as the backup WAN port. Therefore, when WAN is not available, the router will use 3G/4G for supporting automatically. The supported 3G/4G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

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

Enable	☑	
Connection Type	4G USB Modem	WAN IP Alias

4G USB Modem Settings

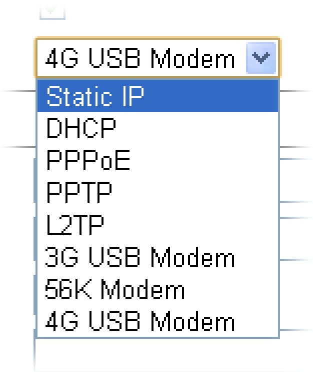
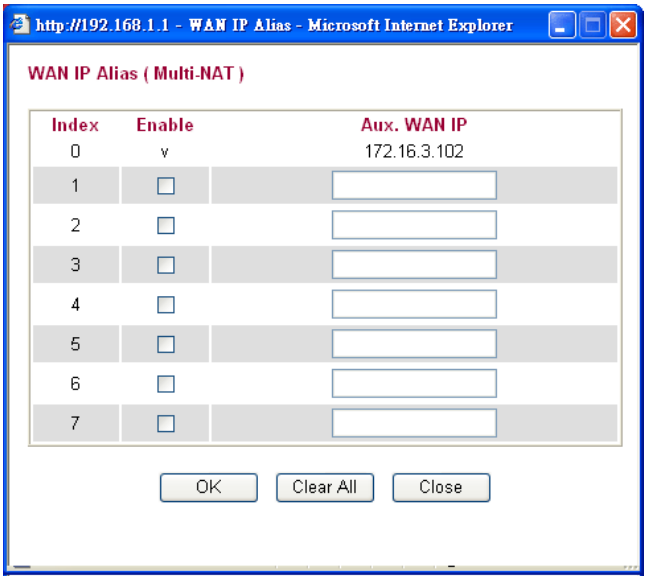
MTU Size	1360	(1000 - 1360)
SIM PIN code		
Network Mode	4G/3G/2G	(default:4G/3G/2G)
APN Name		

Clone MAC Address

Enable	□

OK

Available settings are explained as follows:

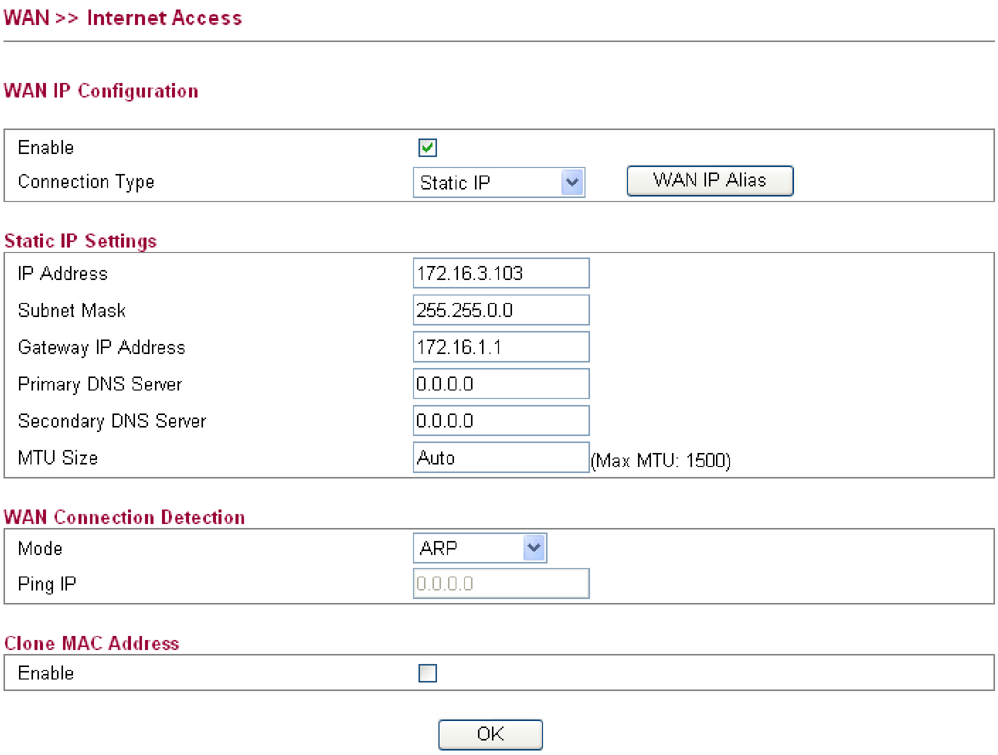
Item	Description
WAN IP Configuration	**Enable** - Check the box to enable the WAN IP configuration. **Connection Type** -the WAN modes. The corresponding page will be displayed.  4G USB Modem Static IP DHCP PPPoE PPTP L2TP 3G USB Modem 56K Modem 4G USB Modem **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Such function can be applied to each connection type.  http://192.168.1.1 - WAN IP Alias - Microsoft Internet Explorer WAN IP Alias (Multi-NAT) Index / Enable / Aux. WAN IP 0 / v / 172.16.3.102 1 / □ / 2 / □ / 3 / □ / 4 / □ / 5 / □ / 6 / □ / 7 / □ /

Below shows the configuration page for each connection type:

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

Enable	☑
Connection Type	Static IP

Static IP Settings

IP Address	172.16.3.103
Subnet Mask	255.255.0.0
Gateway IP Address	172.16.1.1
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
MTU Size	Auto (Max MTU: 1500)

WAN Connection Detection

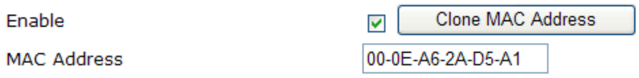
Mode	ARP
Ping IP	0.0.0.0

Clone MAC Address

Enable	□

Available settings are explained as follows:

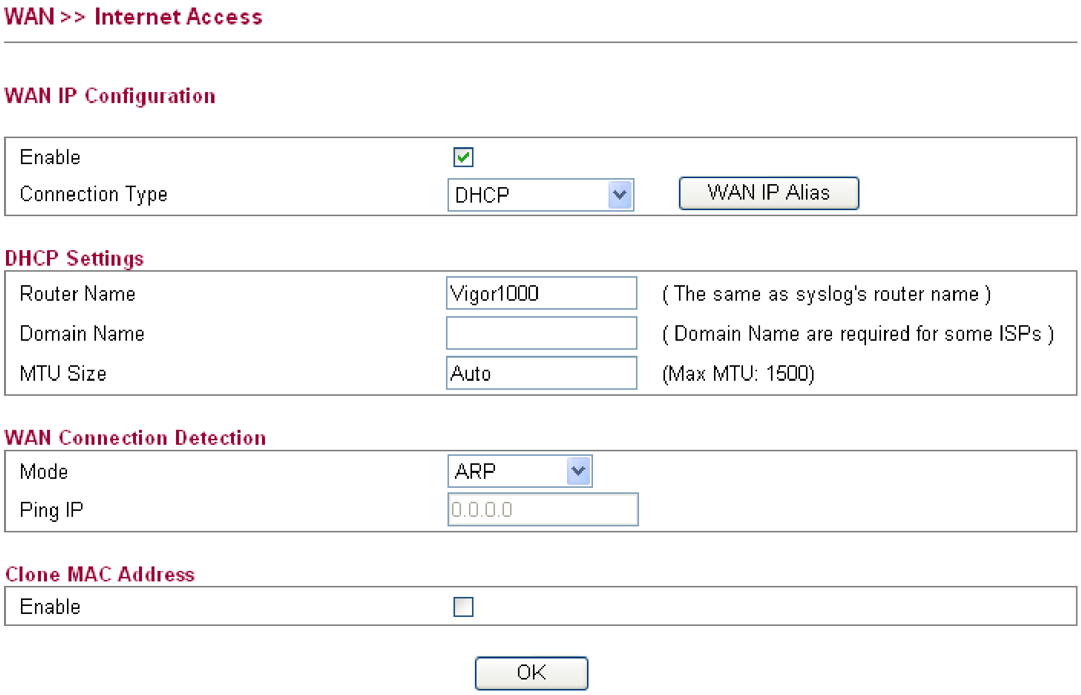
Item	Description
Static IP Settings	**IP Address** -Type the IP address. **Subnet Mask** -Type the subnet mask. **Gateway IP Address** - Type the gateway IP address. **Primary DNS Server** -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS 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. **MTU Size** - It means Max Transmit Unit for packet. The default setting will be specified by the system automatically.
WAN Connection Detection	**Mode** - Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** - If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.

Clone MAC Address	**Enable -** 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

Enable	☑	
Connection Type	DHCP	WAN IP Alias

DHCP Settings

Router Name	Vigor1000	(The same as syslog's router name)
Domain Name		(Domain Name are required for some ISPs)
MTU Size	Auto	(Max MTU: 1500)

WAN Connection Detection

Mode	ARP
Ping IP	0.0.0.0

Clone MAC Address

Enable	□

Available settings are explained as follows:

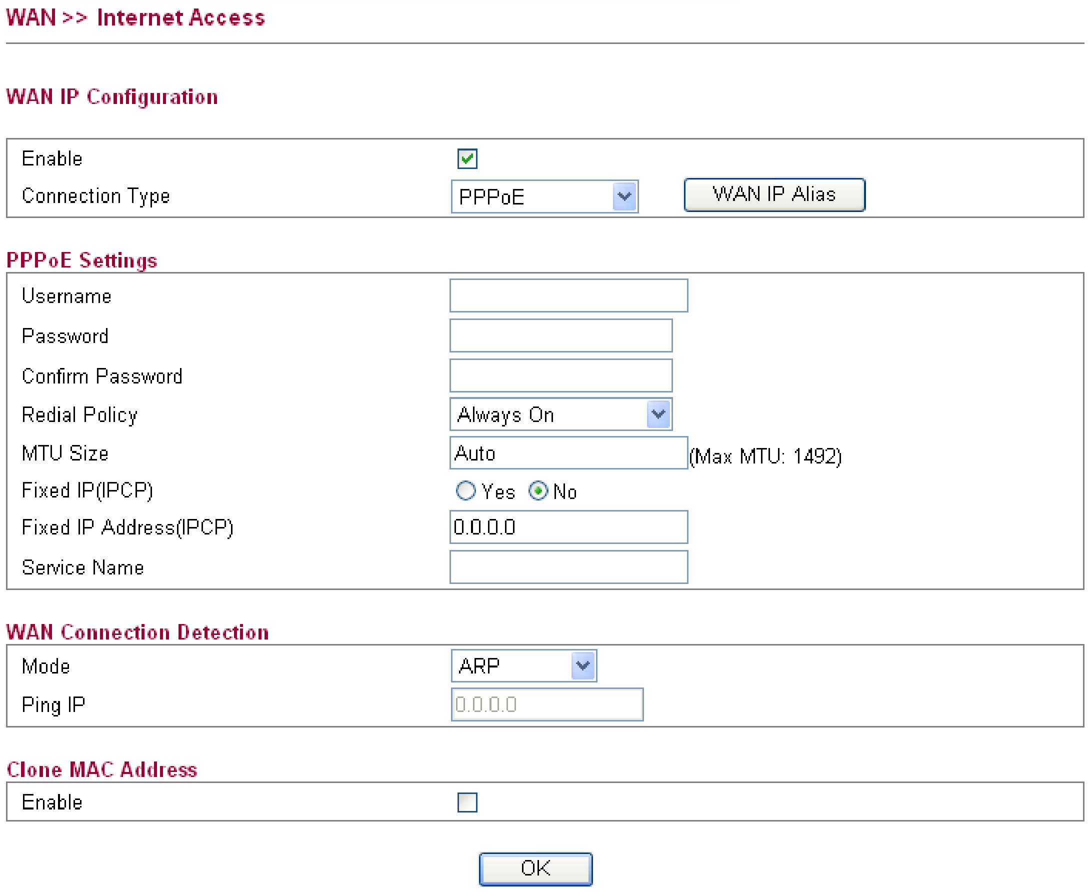
Item	Description
DHCP Settings	**Router Name**-Type in a name for the router. It must be the same as the name used in Syslog. The default setting is Vigor1000. **Domain Name**-Type the domain name (e.g., draytek) to fit the request of some ISPs. **MTU Size**-It means Max Transmit Unit for packet. The default setting will be specified by the system automatically.
WAN Connection Detection	**Mode -** Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP -** If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.

Clone MAC Address	**Enable -** 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

Enable	☑	
Connection Type	PPPoE	WAN IP Alias

PPPoE Settings

Username	
Password	
Confirm Password	
Redial Policy	Always On
MTU Size	Auto (Max MTU: 1492)
Fixed IP(IPCP)	○ Yes ● No
Fixed IP Address(IPCP)	0.0.0.0
Service Name	

WAN Connection Detection

Mode	ARP
Ping IP	0.0.0.0

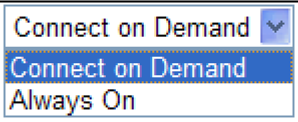
Clone MAC Address

Enable	□

OK

Available settings are explained as follows:

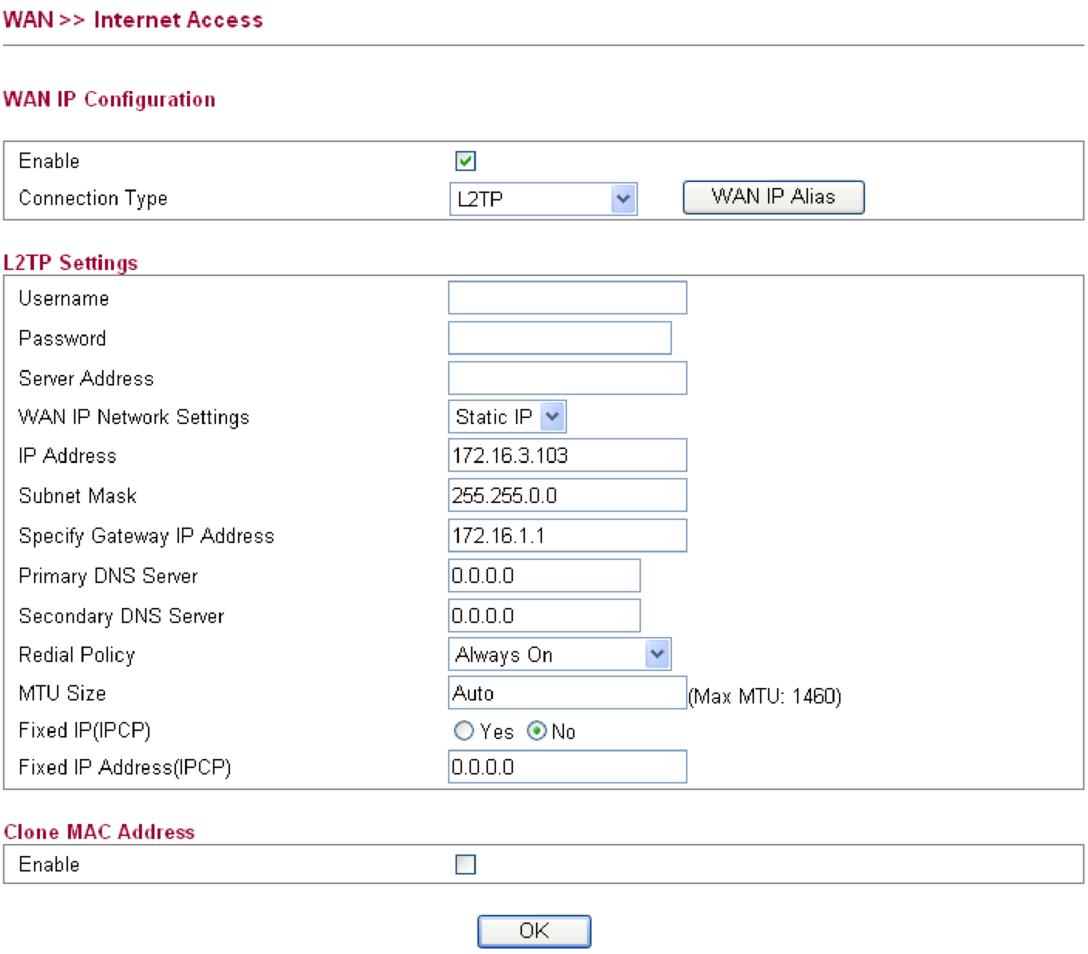
Item	Description
PPPoE Settings	**Username -** Type in the username provided by ISP in this field. **Password-** Type in the password provided by ISP in this field. **Confirm Password** – Type the password again for confirmation. **Redial Policy-** If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.

Item	Description
	 **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 will be specified by the system automatically. **Fixed IP (IPCP)-** Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function. **Fixed IP Address (IPCP)-** Type in a fixed IP address in the box if you click **Yes** for **Fixed IP(IPCP)**. **Service Name –** Some ISP might need such information for connection. Just contact to your dealer/ISP if it is required.
WAN Connection Detection	**Mode** - Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** - If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.
Clone MAC Address	**Enable** - 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

Enable	☑	
Connection Type	L2TP	WAN IP Alias

L2TP Settings

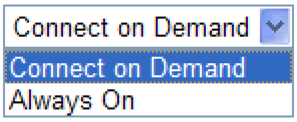
Username	
Password	
Server Address	
WAN IP Network Settings	Static IP
IP Address	172.16.3.103
Subnet Mask	255.255.0.0
Specify Gateway IP Address	172.16.1.1
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Redial Policy	Always On
MTU Size	Auto (Max MTU: 1460)
Fixed IP(IPCP)	○ Yes ● No
Fixed IP Address(IPCP)	0.0.0.0

Clone MAC Address

Enable	□

Available settings are explained as follows:

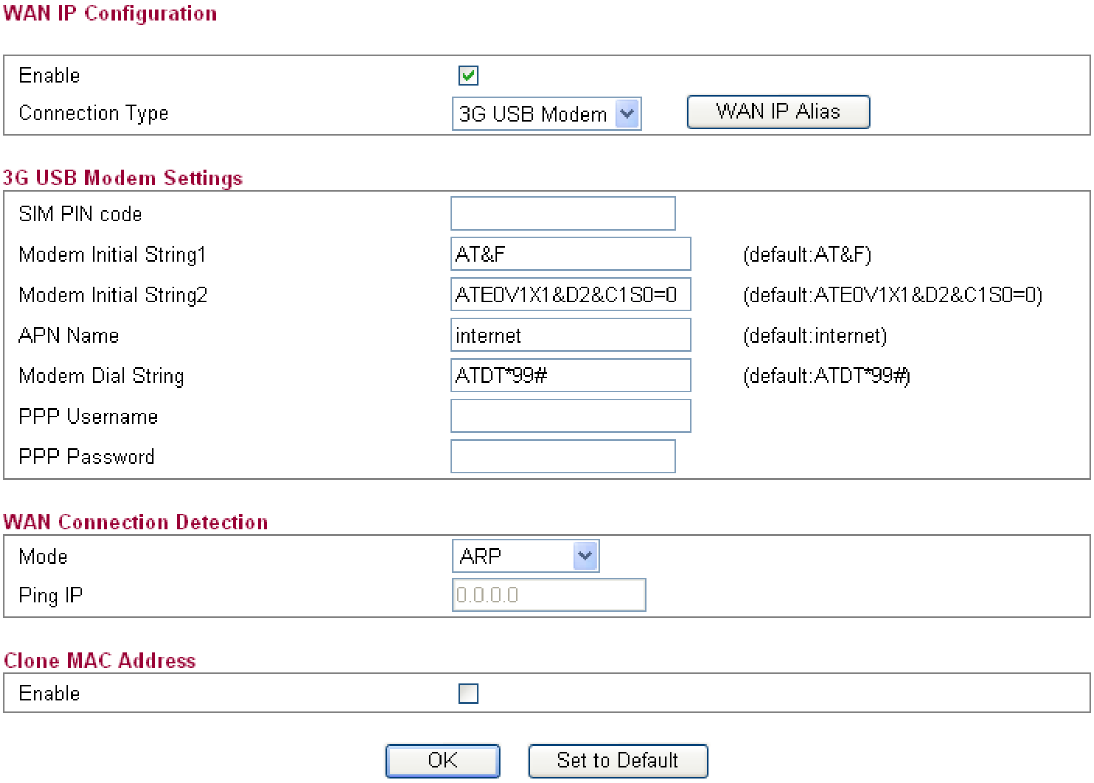
Item	Description
L2TP Settings	**Username** -Type in the username provided by ISP in this field. **Password**- Type in the password provided by ISP in this field. **Server Address**- Type in the IP address for PPTP /L2TP server. **WAN IP Network Settings**- You can choose Static IP or DHCP as WAN IP 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

Item	Description
	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 will be specified by the system automatically. **Fixed IP (IPCP)**-Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function **Fixed IP Address (IPCP)**-Type in a fixed IP address in the box if you click **Yes** for **Fixed IP(IPCP)**.
Clone MAC Address	**Enable** - 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 IP Configuration

Enable	☑	
Connection Type	3G USB Modem	WAN IP Alias

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		

WAN Connection Detection

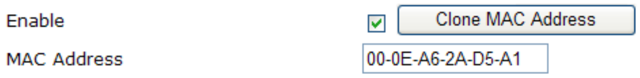
Mode	ARP
Ping IP	0.0.0.0

Clone MAC Address

Enable	□

OK Set to Default

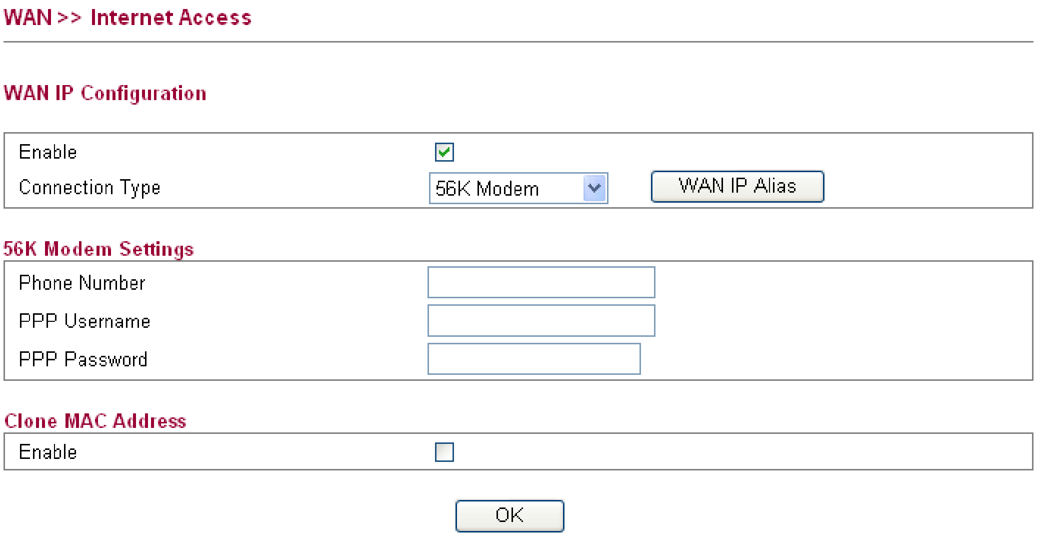
Available settings are explained as follows:

Item	Description
3G USB Modem Settings	**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	**Enable** - 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.

56K Modem

If your router connects to a 56K modem and you want to access Internet via 56K modem, choose 56K Modem as connection type and type the required information in this web page.



WAN >> Internet Access

WAN IP Configuration

Enable ☑

Connection Type: 56K Modem

56K Modem Settings

Phone Number

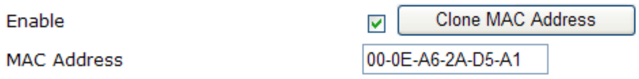
PPP Username

PPP Password

Clone MAC Address

Enable □

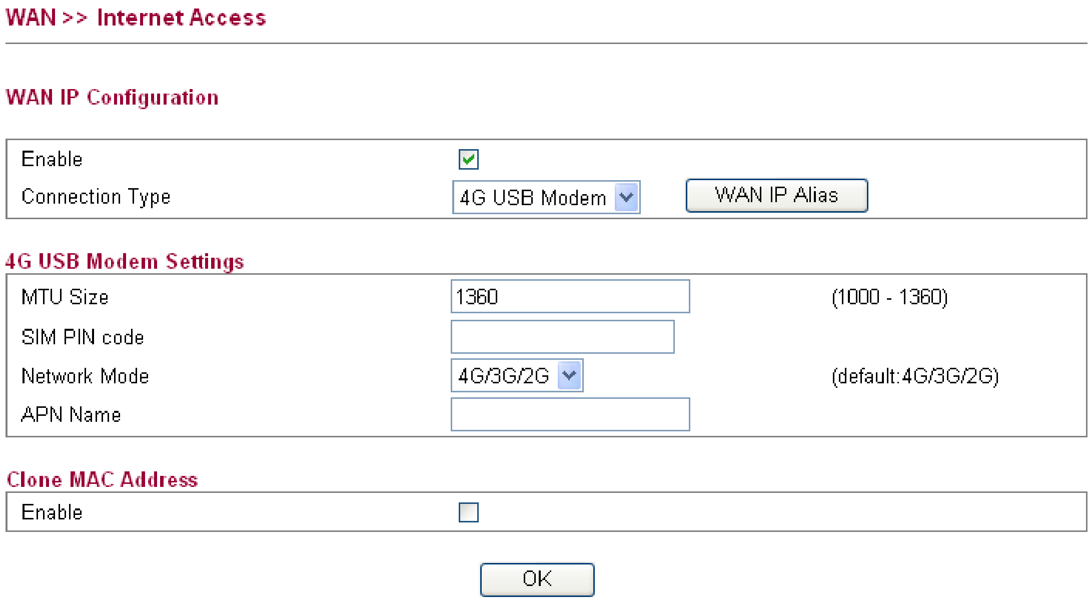
Available settings are explained as follows:

Item	Description
56k Modem Settings	**Phone Number**-Type the phone number offered by the ISP for dial-out connection. **PPP Username**-Type the PPP username (optional). **PPP Password**-Type the PPP password (optional).
Clone MAC Address	**Enable -** 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.

4G USB Modem

If your router connects to a 4G USB modem and you want to access Internet via the modem, choose 4G USB Modem as connection type and type the required information in this web page.



WAN >> Internet Access

WAN IP Configuration

Enable	☑	
Connection Type	4G USB Modem	WAN IP Alias

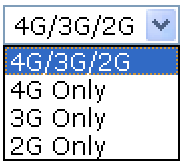
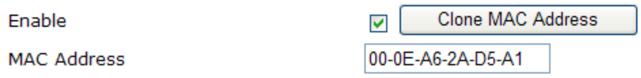
4G USB Modem Settings

MTU Size	1360	(1000 - 1360)
SIM PIN code		
Network Mode	4G/3G/2G	(default:4G/3G/2G)
APN Name		

Clone MAC Address

Enable	□

Available settings are explained as follows:

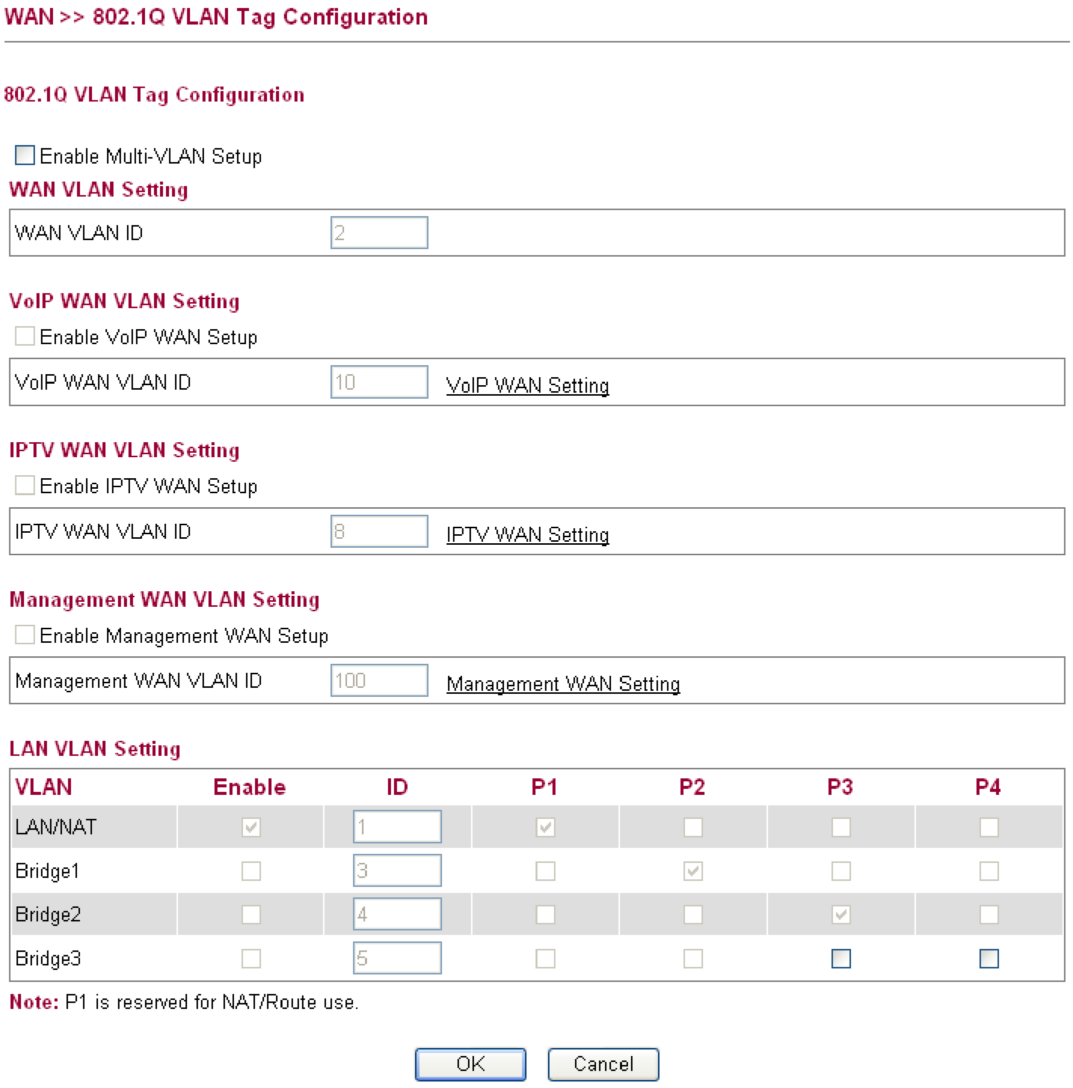
Item	Description
4G USB Modem Settings	**MTU Size**-It means Max Transmit Unit for packet. The default setting is 1360. **SIM PIN code**-Type PIN code of the SIM card that will be used to access Internet. **Network Mode**-Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.  **APN Name**-APN means Access Point Name which is provided and required by some ISPs.
Clone MAC Address	**Enable** - 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

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

4.1.2 Multi-VLAN

Vigor1000 series offers multi-VLAN function to make the data transmission with security. Data transmitting through the Ethernet port for connecting to Internet can be tagged with an ID number specified here for ensuring the security. In addition, each LAN port also can be tagged with an ID number in local network to reach the goal of protection.

If all the boxes are checked, it means that Internet connection and data transmission can be done via 4 VLAN groups.



WAN >> 802.1Q VLAN Tag Configuration

802.1Q VLAN Tag Configuration

□ Enable Multi-VLAN Setup

WAN VLAN Setting

WAN VLAN ID	2

VoIP WAN VLAN Setting

□ Enable VoIP WAN Setup

VoIP WAN VLAN ID	10	VoIP WAN Setting

IPTV WAN VLAN Setting

□ Enable IPTV WAN Setup

IPTV WAN VLAN ID	8	IPTV WAN Setting

Management WAN VLAN Setting

□ Enable Management WAN Setup

Management WAN VLAN ID	100	Management WAN Setting

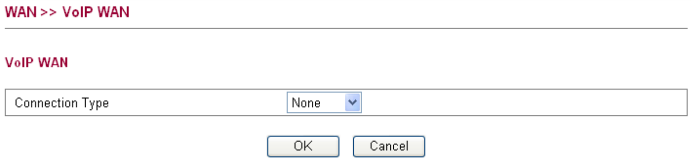
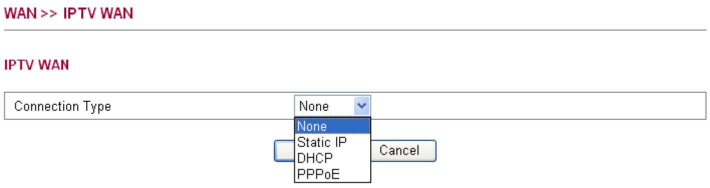
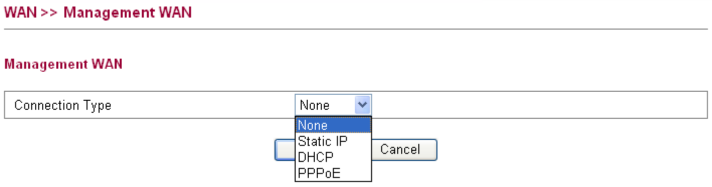
LAN VLAN Setting

VLAN	Enable	ID	P1	P2	P3	P4
LAN/NAT	☑	1	☑	□	□	□
Bridge1	□	3	□	☑	□	□
Bridge2	□	4	□	□	☑	□
Bridge3	□	5	□	□	□	□

Note: P1 is reserved for NAT/Route use.

Available settings are explained as follows:

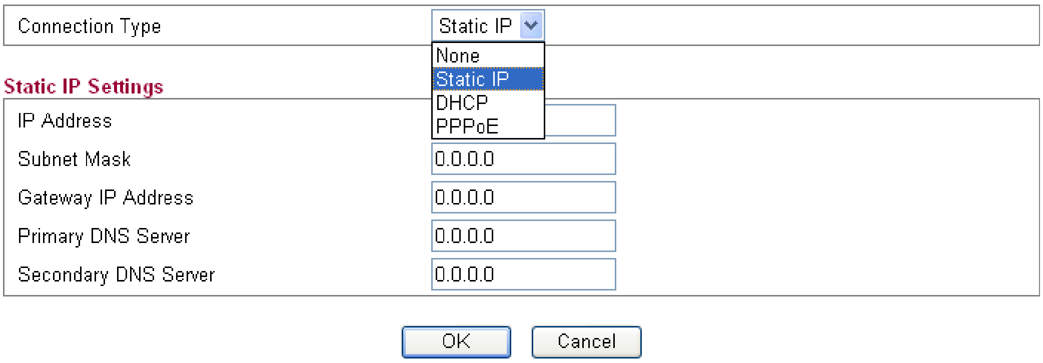
Item	Description
Enable Multi-VLAN Setup	Check the box to enable Multi-VLAN configuration.
WAN VLAN Setting	**WAN VLAN ID -** Data sent out through the WAN port will be tagged with VLAN ID number specified here. The range of ID number you can type is from 2 – 4096.

VoIP WAN VLAN Setting	**Enable VoIP WAN Setup** - Check the box to enable **VoIP WAN** configuration. **VoIP WAN VLAN ID-** Voice sent out through the WAN port will be tagged with VLAN ID number specified here. The range of ID number you can type is from 2 - 4096. **VoIP WAN Setting** – Click this link to open VoIP WAN setting.  WAN >> VoIP WAN VoIP WAN Connection Type: None
IPTV WAN VLAN Setting	**Enable IPTV WAN Setup-** Check the box to enable **IPTV WAN** configuration. **IPTV WAN VLAN ID-** IPTV signal sent out through the WAN port will be tagged with VLAN ID number specified here. The range of ID number you can type is from 2 - 4096. **IPTV WAN Setting** – Click this link to open IPTV WAN setting.  WAN >> IPTV WAN IPTV WAN Connection Type: None
Management WAN VLAN Setting	**Enable Management WAN Setup-** Check the box to enable **Management WAN** configuration. **Management WAN VLAN ID** - Data sent out through the WAN port will be tagged with VLAN ID number specified here. The range of ID number you can type is from 2 - 4096. **Management WAN Setting** – Click this link to open Management WAN setting.  WAN >> Management WAN Management WAN Connection Type: None
LAN VLAN Setting	**LAN/NAT-** Such value is constant and fixed. All the data will be transmitted by NAT through WAN port. **Bridge 1/2/3-** LAN port (P2-P4) selected here will ask a Public IP address from ISP for transmitting data from PC directly without NAT. The range of ID number you can type is from 2 – 4096. Each ID setting must be unique and different with WAN VLAN ID.

VoIP WAN Setting / IPTV WAN Setting / Management WAN Setting

VoIP WAN/IPTV WAN/Management WAN is the interface specified for the usage of VoIP/IPTV/Management. The settings will be changed based on the connection type selected.

When **Static IP** is selected as connection type, you need to configure the following settings:



Connection Type: Static IP

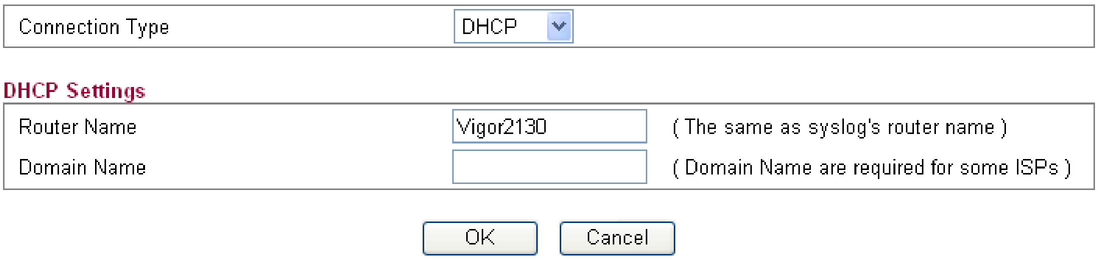
Static IP Settings

IP Address	
Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Available settings are explained as follows:

Item	Description
IP Address	Type the IP address obtained from ISP for the usage of VoIP.
Subnet Mask	Type the Subnet mask obtained from ISP for the usage of VoIP.
Gateway IP Address	Type the gateway IP address obtained from ISP for the usage of VoIP.
Primary DNS Server	Type the IP address of primary DNS server obtained from ISP for the usage of VoIP.
Secondary DNS Server	Type the IP address of secondary DNS server obtained from ISP for the usage of VoIP.

When **DHCP** is selected as connection type, you need to configure the following settings:



Connection Type: DHCP

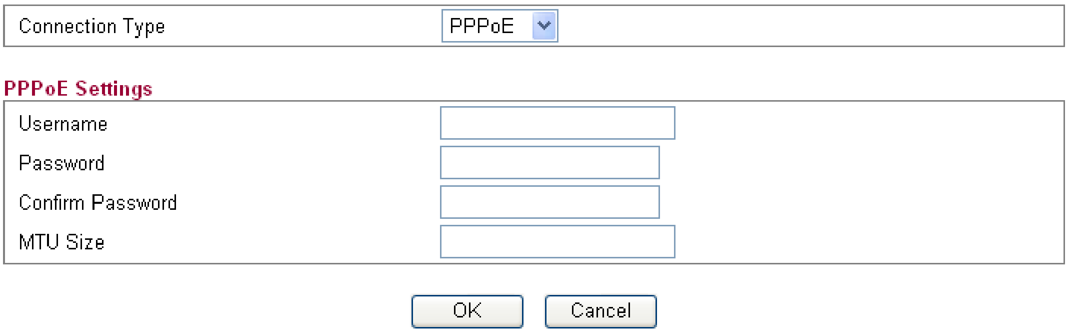
DHCP Settings

Router Name	Vigor2130	(The same as syslog's router name)
Domain Name		(Domain Name are required for some ISPs)

Available settings are explained as follows:

Item	Description
Router Name	Type the name of the router.
Domain Name	Type the domain name obtained from the ISP.

When **PPPoE** is selected as connection type, you need to configure the following settings:



Connection Type	PPPoE

PPPoE Settings

Username	
Password	
Confirm Password	
MTU Size	

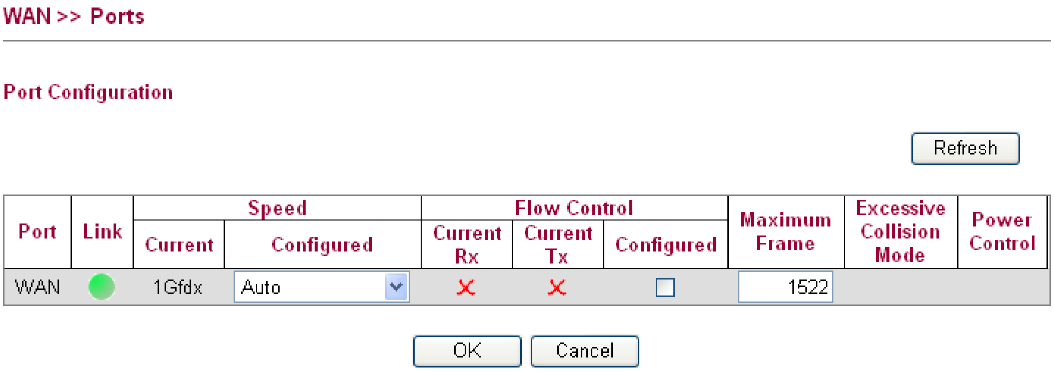
Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the ISP.
Password	Type the password obtained from the ISP.
Confirm Password	Type the password again for confirmation.
MTU Size	It means Max Transmit Unit for packet. The default setting will be specified by the system automatically. Therefore, keep this field in blank.

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

4.1.3 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.



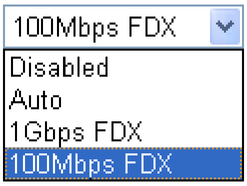
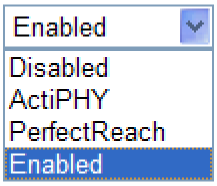
WAN >> Ports

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
WAN	●	1Gfdx	Auto	✗	✗	□	1522		

Available settings are explained as follows:

Item	Description
Port	It displays current network interface.
Link	It displays current connection status. Green light means the WAN connection is successful.
Speed 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**. 
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.

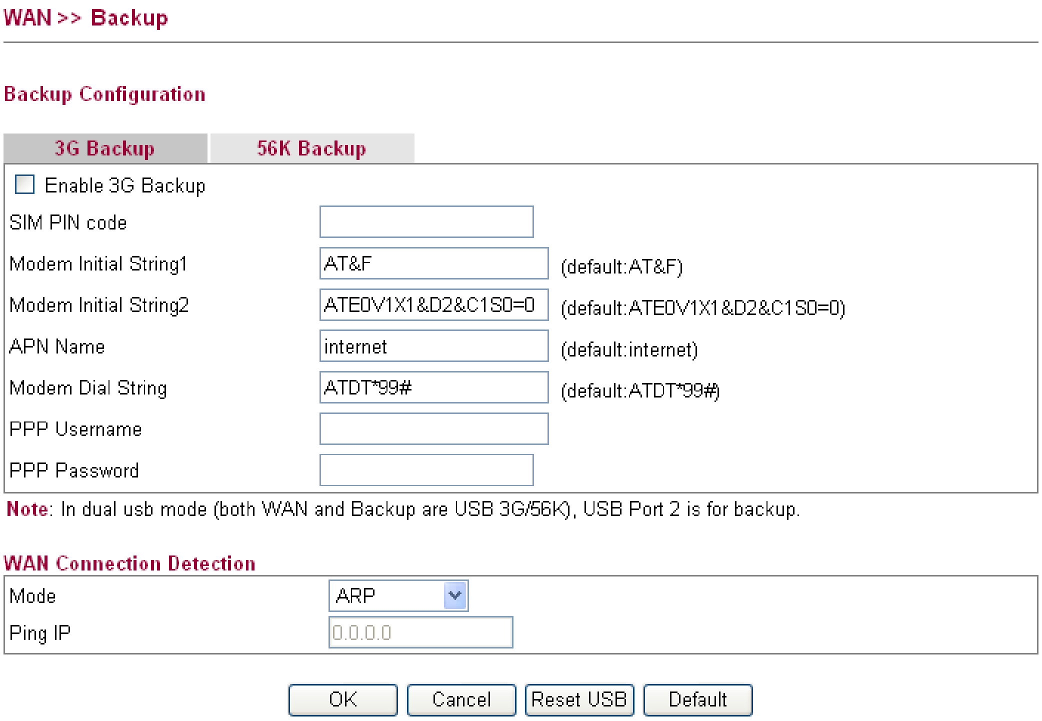
After finishing all the settings here, please click **OK** to activate them.

4.1.4 Backup

This page is used to setup 3G/56K backup function. If you enable 3G/56K backup, make sure your WAN connection type is not in 3G/56K mode. When the WAN connection is broken, router will try to keep the connection with 3G/56K mode. After WAN connection is recovered, router will disconnect the 3G/56K connection automatically.

If both USB ports connected with 3G modem and 56K modem, and both 3G Backup and 56K Backup modes are enabled, the system will determine which one (3G Backup or 56K Backup) will be selected as backup mode according to the detected physical connection automatically.

3G Backup



WAN >> Backup

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		

Note: In dual usb mode (both WAN and Backup are USB 3G/56K), USB Port 2 is for backup.

WAN Connection Detection

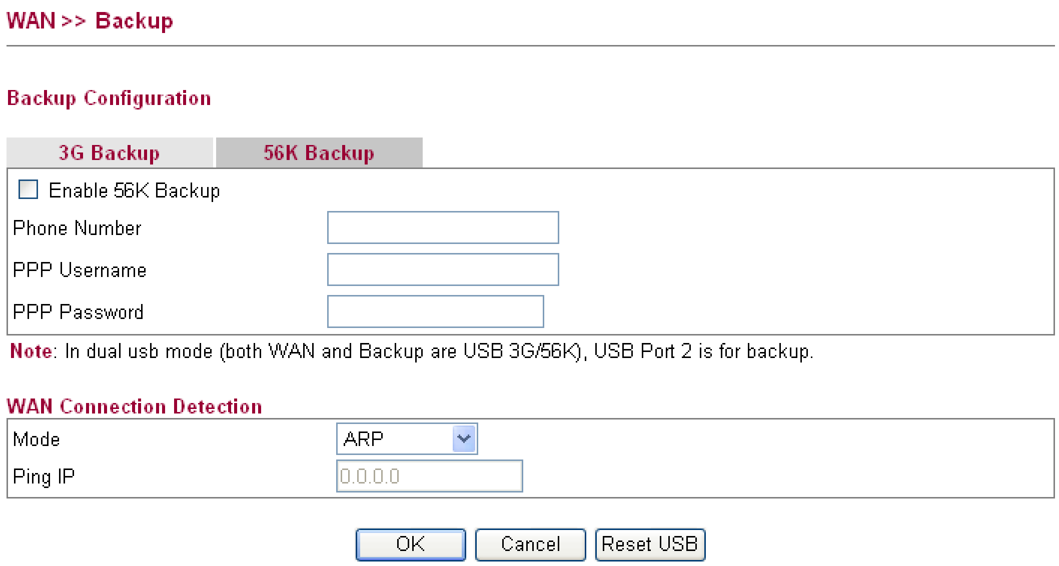
Mode	ARP
Ping IP	0.0.0.0

Available settings are explained as follows:

Item	Description
3G Backup	**Enable 3G Backup-** Check this box to enable such function. **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).
WAN Connection Detection	**Mode-** Such function allows you to verify whether network connection is alive or not through ARP or Ping Detect. Choose **ARP** or **Ping Detect** for the system to execute for WAN detection. **Ping IP-** If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.
Reset USB	Click this button to reset the USB port.
Default	Click this button for returning to the default settings.

56K Backup

When the WAN connection is broken, router will try to keep the connection with 56K mode if it is enabled. After WAN connection is recovered, router will disconnect the 56K connection automatically.



WAN >> Backup

Backup Configuration

☐ Enable 56K Backup

Phone Number

PPP Username

PPP Password

Note: In dual usb mode (both WAN and Backup are USB 3G/56K), USB Port 2 is for backup.

WAN Connection Detection

Mode: ARP

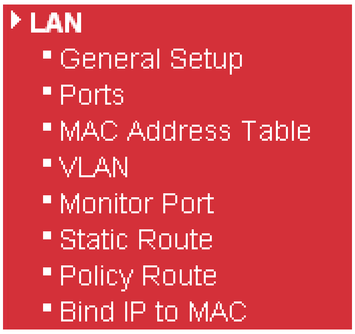
Ping IP: 0.0.0.0

Available settings are explained as follows:

Item	Description
56K Backup	**Enable 56K Backup-** Check this box to enable such function. **Phone Number-** Type the phone number offered by the ISP for dial-out connection. **PPP Username-** Type the PPP username (optional). **PPP Password-** Type the PPP password (optional).
WAN Connection Detection	**Mode-** Such function allows you to verify whether network connection is alive or not through ARP or Ping Detect. Choose **ARP** or **Ping Detect** for the system to execute for WAN detection. **Ping IP-** If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.
Reset USB	Click this button to reset the USB port.

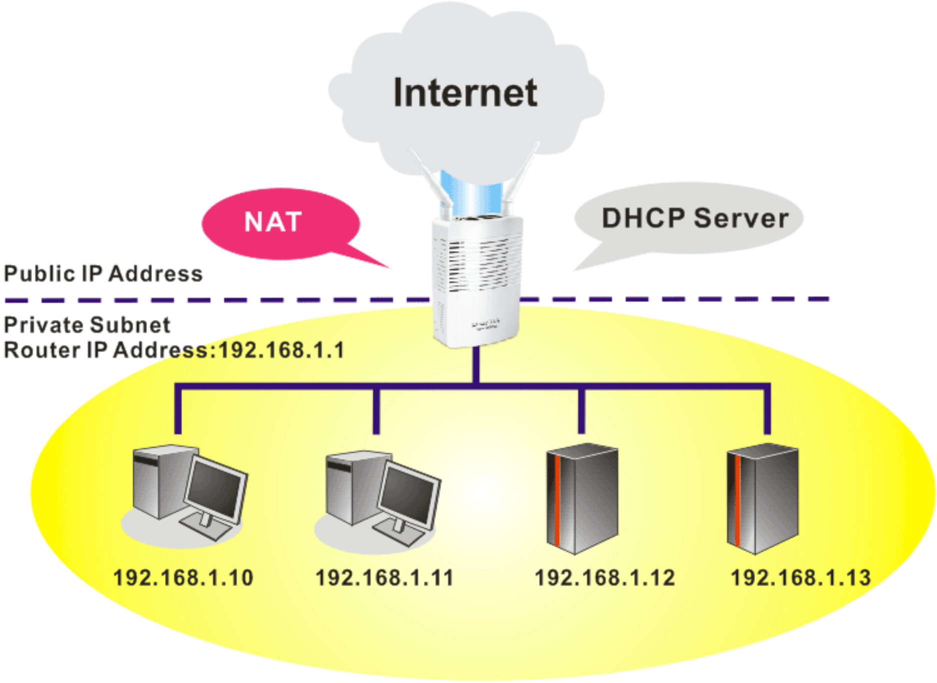
4.2 LAN

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.

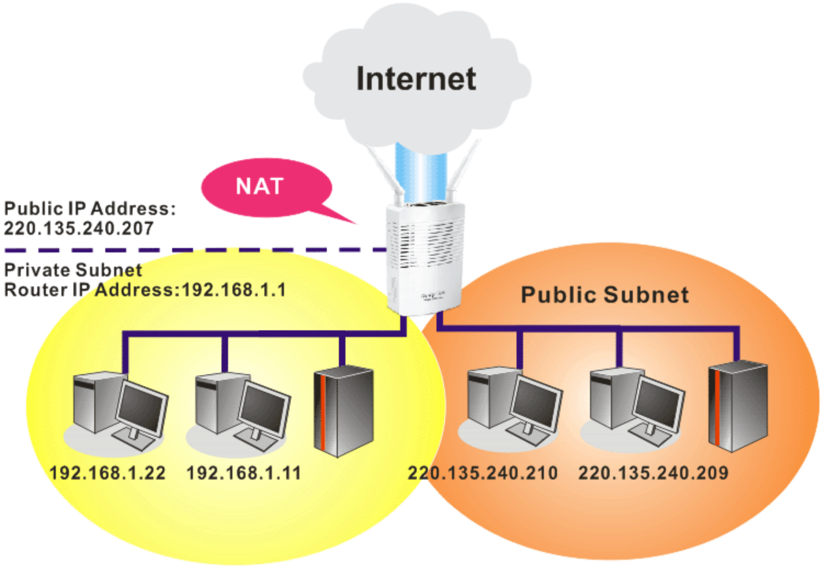


Basics of LAN

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)

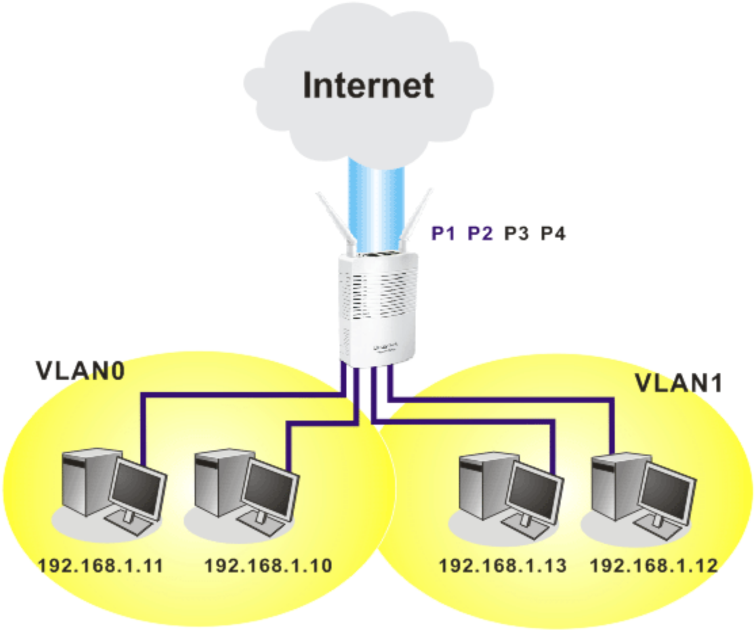
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

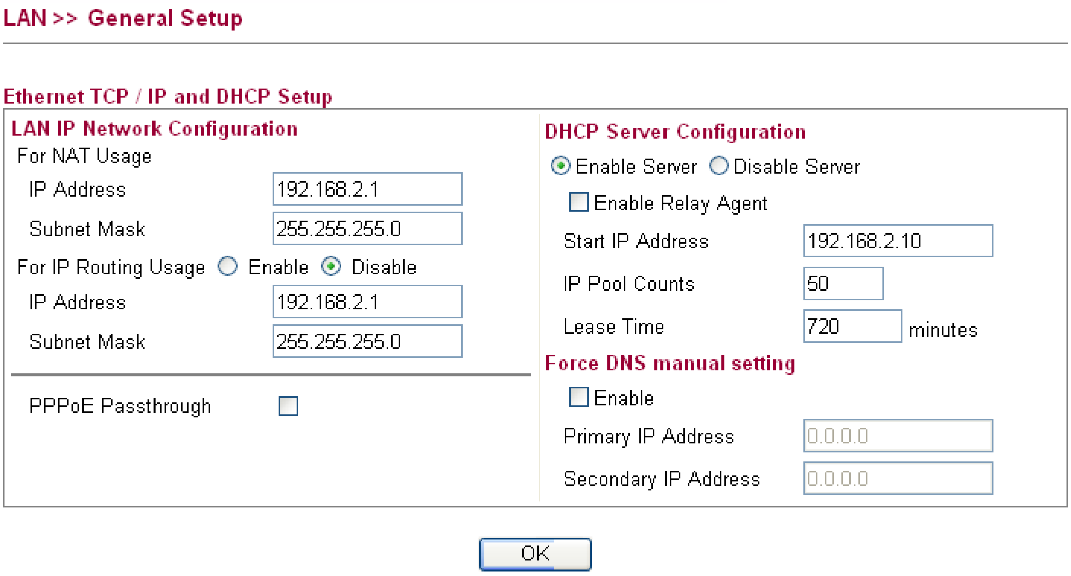
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



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

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

For IP Routing Usage ○ Enable ● Disable

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

PPPoE Passthrough □

DHCP Server Configuration

● Enable Server ○ Disable Server

□ Enable Relay Agent

Start IP Address: 192.168.2.10

IP Pool Counts: 50

Lease Time: 720 minutes

Force DNS manual setting

□ Enable

Primary IP Address: 0.0.0.0

Secondary IP Address: 0.0.0.0

Available settings are explained as follows:

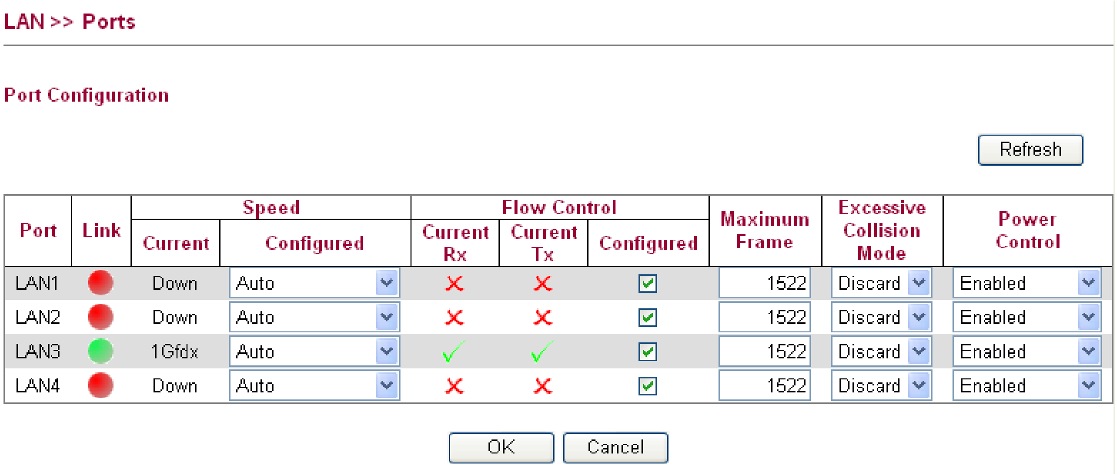
Item	Description
LAN IP Network Configuration	**For NAT Usage** **IP Address -** Type in private IP address for connecting to a local private network (Default: 192.168.1.1). **Subnet Mask-** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) **For IP Routing Usage** Click **Enable** to invoke this function. The default setting is **Disable**. **IP Address-** Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24) **Subnet Mask-** An address code that determines the size of the network. (Default: 255.255.255.0/ 24) **PPPoE Passthrough-** The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.

DHCP Server Configuration	**Enable Server -** 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. **Enable Relay Agent** – Check this box to enable such function. **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.
Force DNS manual setting	**Enable -** Force router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server). **Primary IP Address-** You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. **Secondary IP Address-** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status. If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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.

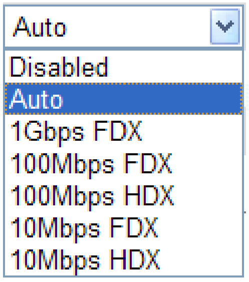


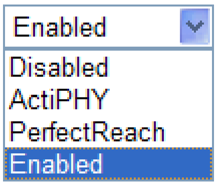
LAN >> Ports

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
LAN1	🔴	Down	Auto	✗	✗	☑	1522	Discard	Enabled
LAN2	🔴	Down	Auto	✗	✗	☑	1522	Discard	Enabled
LAN3	🟢	1Gfdx	Auto	✓	✓	☑	1522	Discard	Enabled
LAN4	🔴	Down	Auto	✗	✗	☑	1522	Discard	Enabled

Available settings are explained as follows:

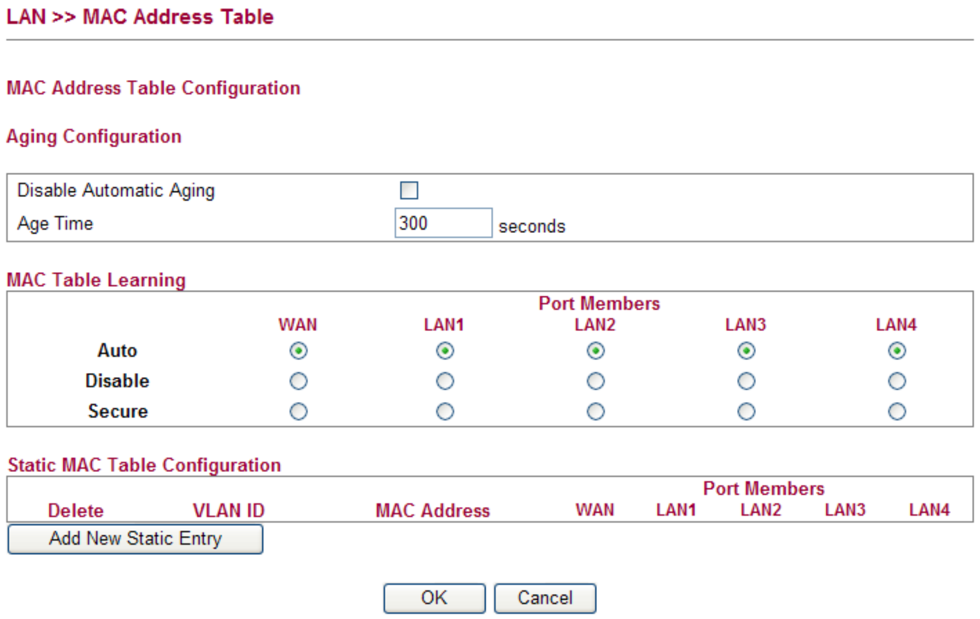
Item	Description
Port	It displays current network interface.
Link	It displays current connection status. Green light means the WAN connection is successful.
Speed Current	It displays current speed that the router uses.
Speed Configured	You can use the drop down list to choose the required speed for the 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.

4.2.3 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

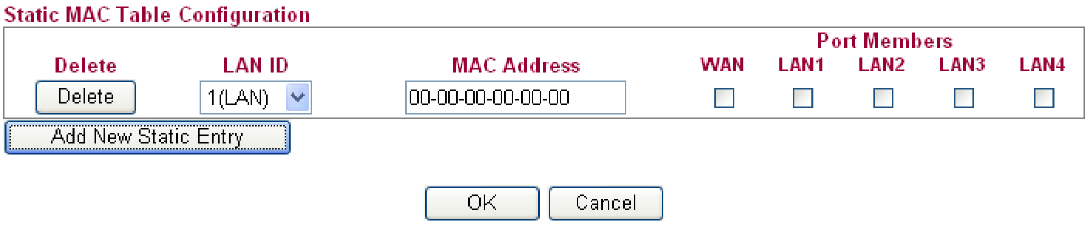
			Port Members				
Delete	VLAN ID	MAC Address	WAN	LAN1	LAN2	LAN3	LAN4

Available settings are explained as follows:

Item	Description
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. **LAN 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 a **VLAN ID** and type a new MAC address. Next, specify port member for this table. Finally, click OK to save the changes.

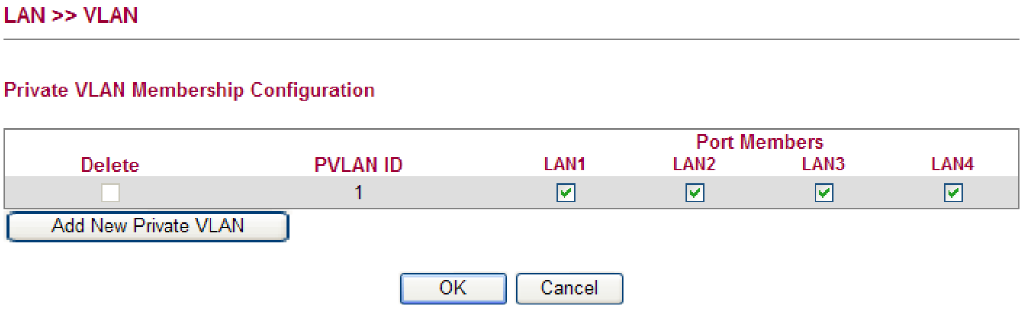


Static MAC Table Configuration

			Port Members				
Delete	LAN ID	MAC Address	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.



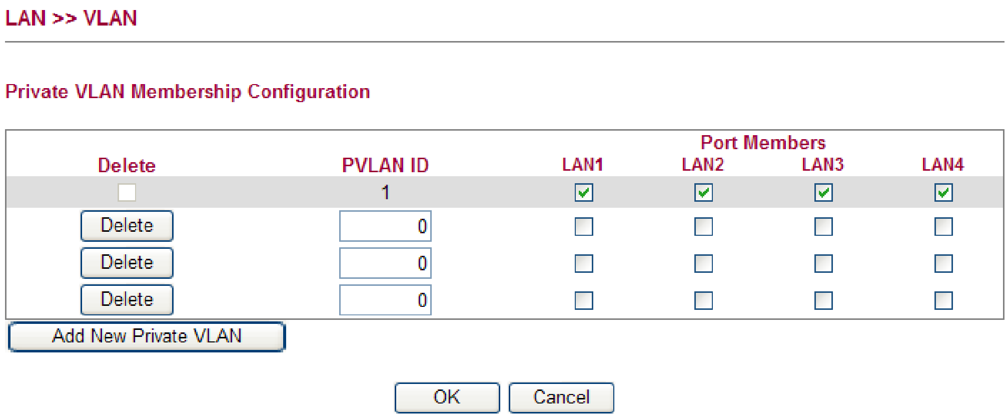
LAN >> VLAN

Private VLAN Membership Configuration

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

Available settings are explained as follows:

Item	Description
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

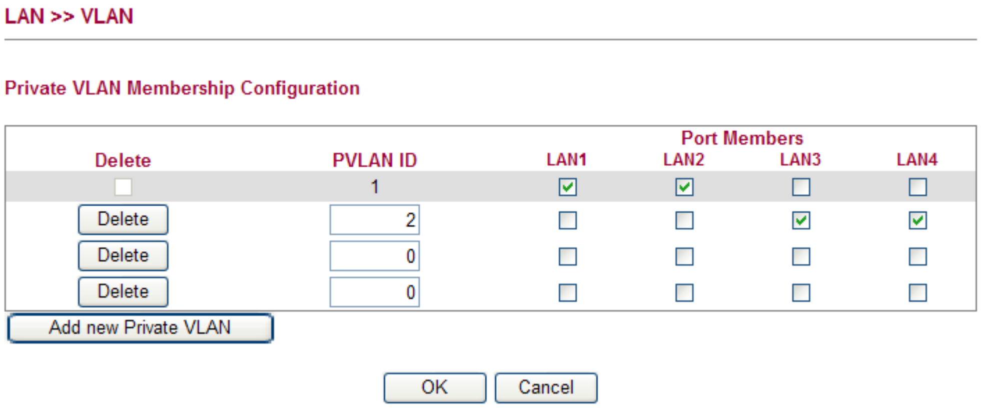
Private VLAN Membership Configuration

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

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

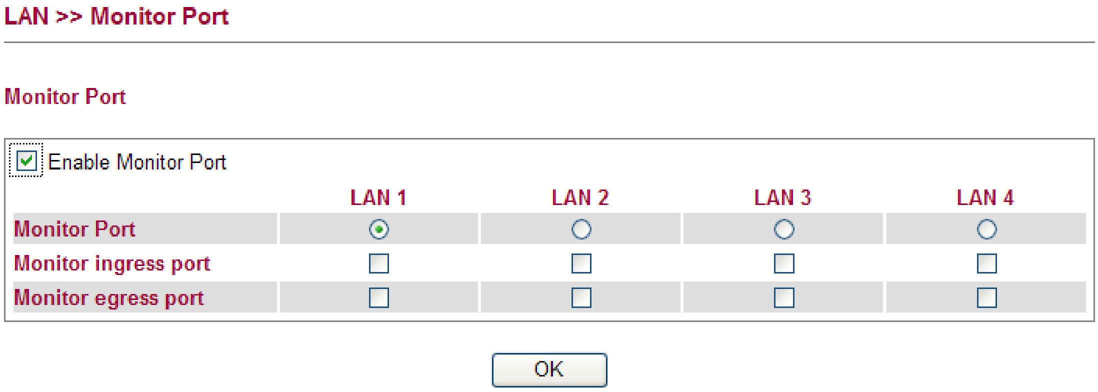
Private VLAN Membership Configuration

		Port Members			
Delete	PVLAN ID	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	□	□	□	□

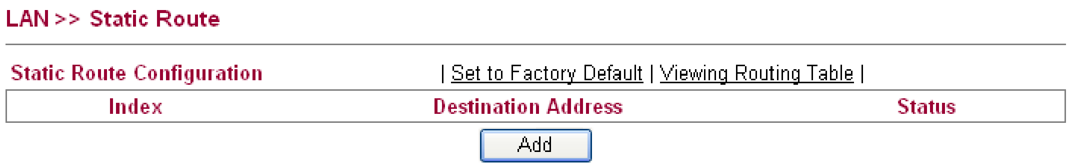
Available settings are explained as follows:

Item	Description

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 | Set to Factory Default | Viewing Routing Table |

Index	Destination Address	Status

Available settings are explained as follows:

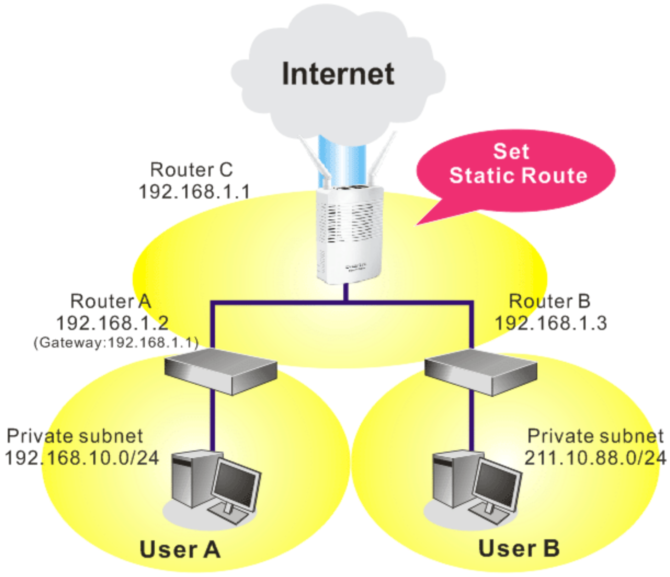
Item	Description
Set to Factory Default	Click this link to return to the factory default settings.
View Routing Table	Click this link to view the routing table.
Index	The number (1 to 10) under Index displays current static router.
Destination Address	Display the destination address of the static route.
Status	Display the status of the static route.
Add	Click it to add a new static route.

Add Static Routes to Private and Public Networks

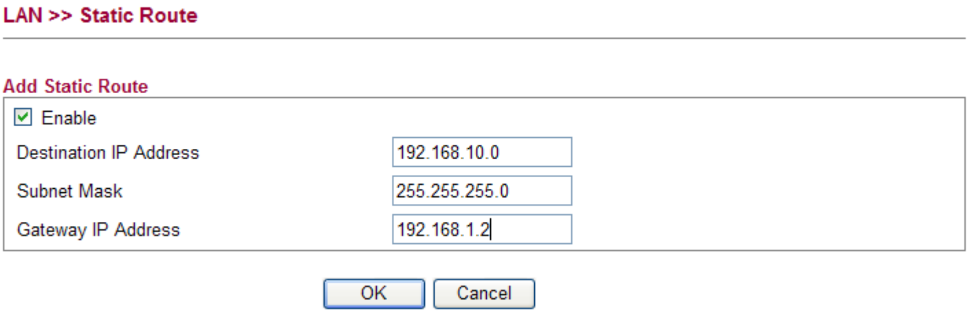
Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- 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.



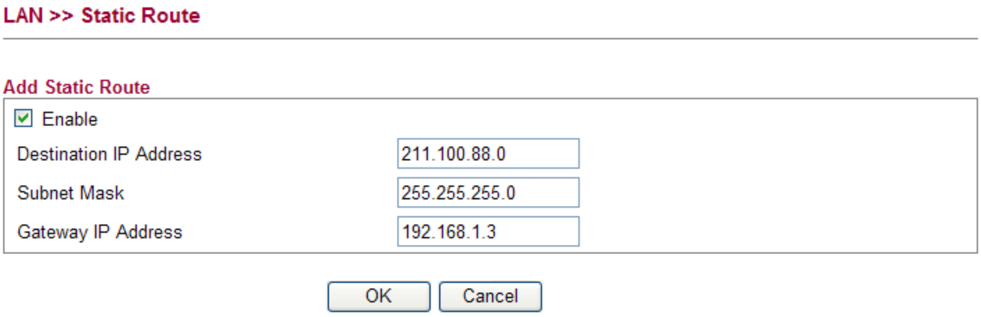
1. Click the **LAN - Static Route** and click **Add.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.


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

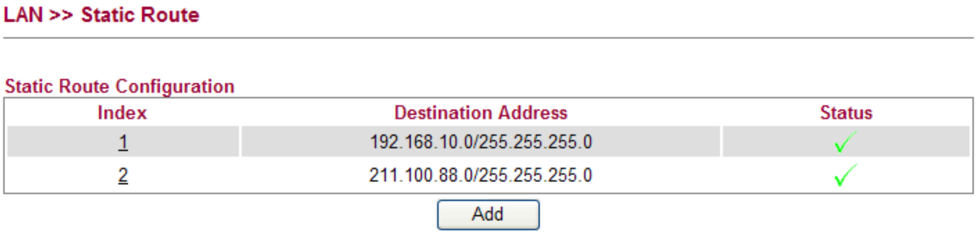
2. Return to **Static Route** page. Click **Add** again to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3.


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.

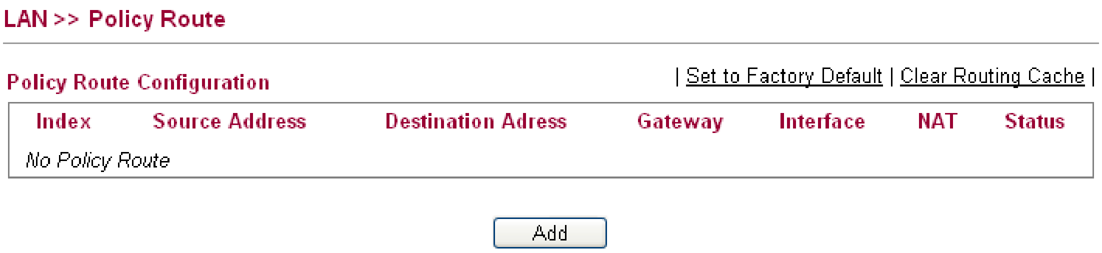

LAN >> Static Route

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 Policy Route

Such function allows you to determine the direction of data transmission from the specified source IP to the specified destination IP. In addition, the data can be sent to the specified gateway via the WAN or LAN interface.



LAN >> Policy Route

Policy Route Configuration

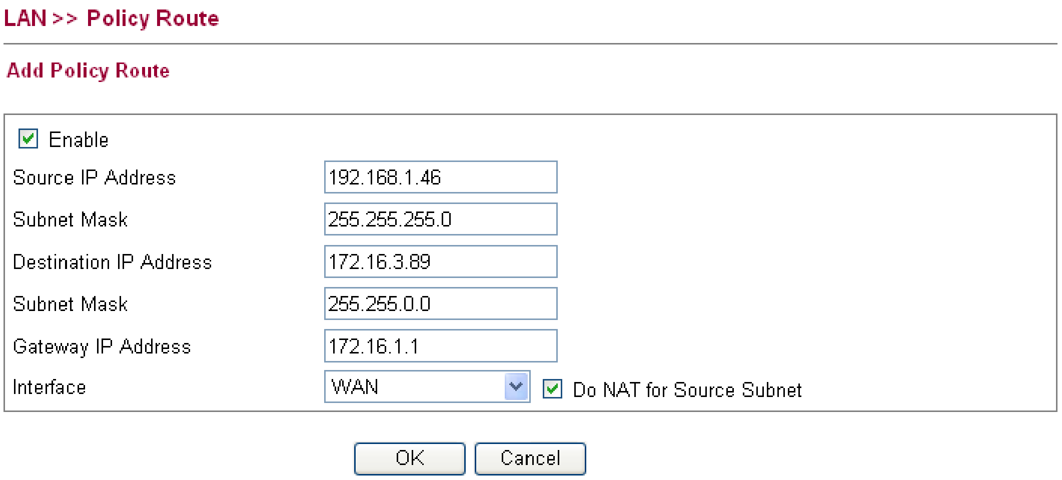
| Set to Factory Default | Clear Routing Cache |

Index	Source Address	Destination Adress	Gateway	Interface	NAT	Status
No Policy Route						

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click this link to return to the factory default settings.
Clear Routing Cache	Click this link to clear the routing cache data.
Index	The number (1 to 10) under Index displays current policy route.
Source Address	Display the source address of the policy route.
Destination Address	Display the destination address of the policy route.
Gateway	Display the IP address of the gateway.
Interface	Display the interface used for policy route.
NAT	Display if NAT for source subnet is enabled or not.
Status	Display the status of the policy route.
Add	Click it to add a new policy route.

Click **Add** to create a new policy route.



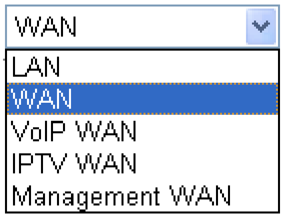
LAN >> Policy Route

Add Policy Route

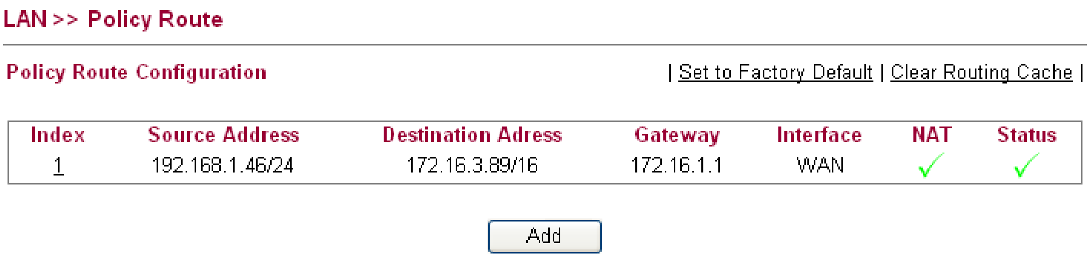
☑ Enable

Source IP Address	192.168.1.46
Subnet Mask	255.255.255.0
Destination IP Address	172.16.3.89
Subnet Mask	255.255.0.0
Gateway IP Address	172.16.1.1
Interface	WAN ☑ Do NAT for Source Subnet

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy route.
Source IP Address	Type the source address of the policy route.
Subnet Mask	Type the subnet mask for the source IP address.
Destination Address	Display the destination address of the policy route.
Subnet Mask	Type the subnet mask for the destination IP address.
Gateway IP Address	Display the IP address of the gateway.
Interface	Choose one of the options as the interface for such policy route. **Do NAT for Source Subnet** – This option is not available for LAN interface. If tt is enabled, the data from Source IP address will be transmitted into the WAN IP/VoIP WAN/IPTV WAN/Management WAN address of the router. 

Click **OK** to save the settings.



LAN >> Policy Route

Policy Route Configuration

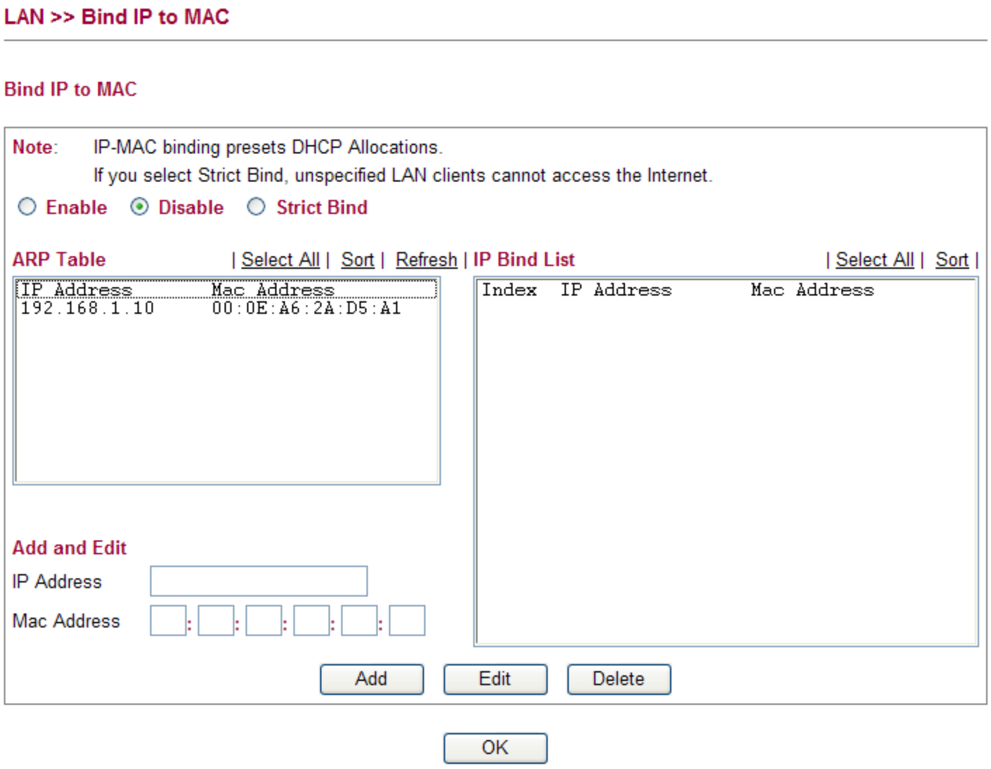
| Set to Factory Default | Clear Routing Cache |

Index	Source Address	Destination Adress	Gateway	Interface	NAT	Status
1	192.168.1.46/24	172.16.3.89/16	172.16.1.1	WAN	✓	✓

4.2.8 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

Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below. **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.
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.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**.

Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **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.

Click **OK** to save the settings.

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.

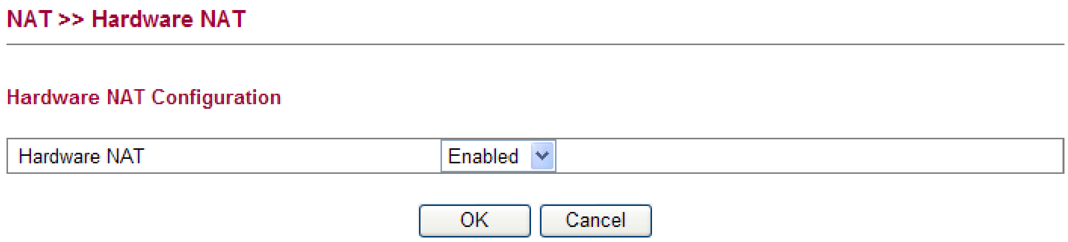
Below shows the menu items for NAT.

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

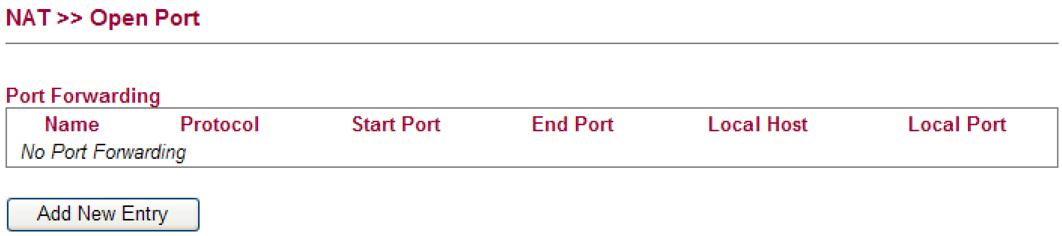
Hardware NAT Configuration

Hardware NAT	Enabled

Click **OK** to save the settings.

4.3.2 Open Ports

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



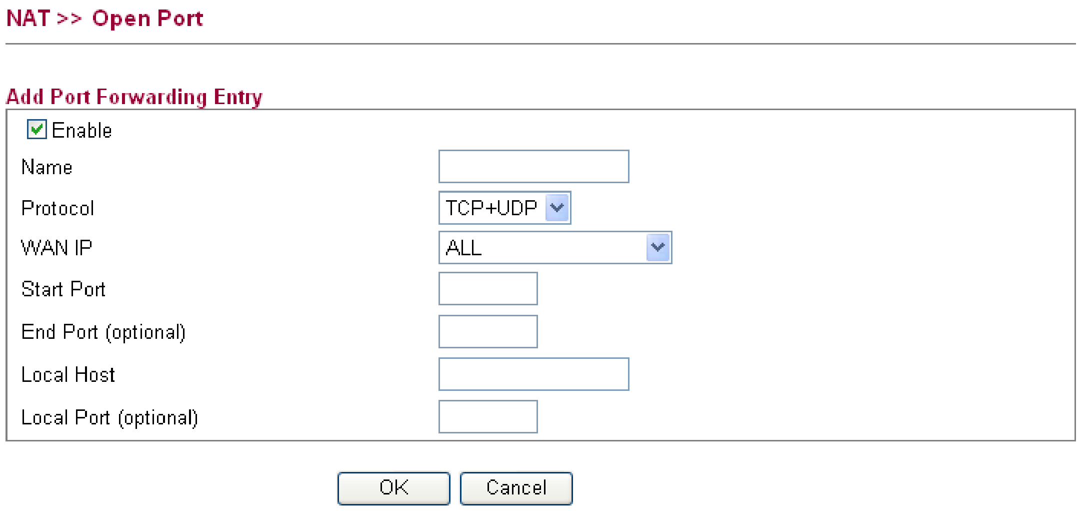
NAT >> Open Port

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**.



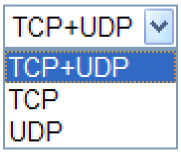
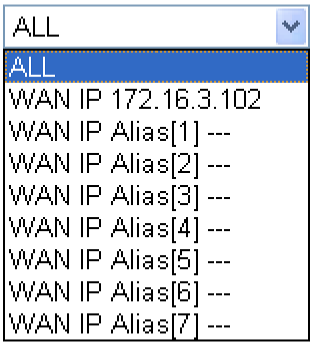
NAT >> Open Port

Add Port Forwarding Entry

☑ Enable	
Name	
Protocol	TCP+UDP
WAN IP	ALL
Start Port	
End Port (optional)	
Local Host	
Local Port (optional)	

Available settings are explained as follows:

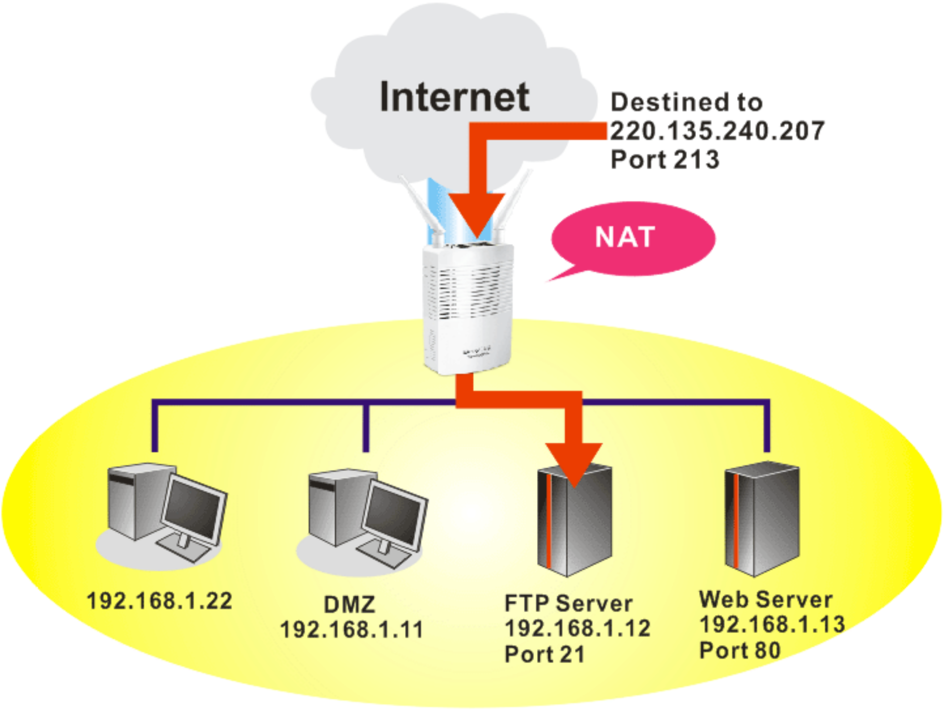
Item	**Description**
Enable	Check this box to enable this function.
Name	Specify the name for the defined network service.

Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**. 
WAN IP	Specify one WAN IP address to be used by such profile. The default setting is ALL, which mean such profile can be applied for all the WAN IP addresses.  ALL ALL WAN IP 172.16.3.102 WAN IP Alias[1] --- WAN IP Alias[2] --- WAN IP Alias[3] --- WAN IP Alias[4] --- WAN IP Alias[5] --- WAN IP Alias[6] --- WAN IP Alias[7] ---
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.

Click **OK** to save the settings.

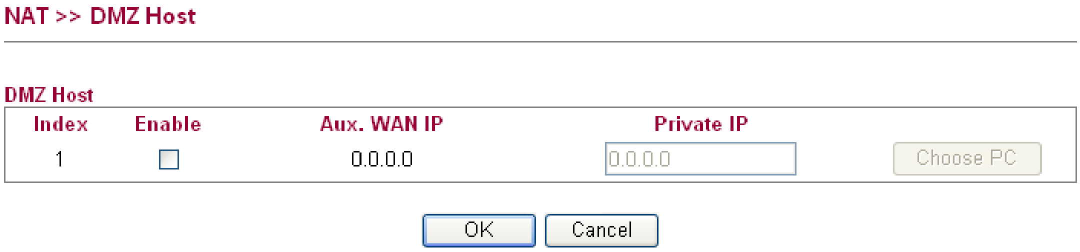
4.3.3 DMZ Host

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

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

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click **Choose PC** to specify a suitable one.
Choose PC	Bring a dialog for you to choose an IP address.

Click **OK** to save the settings.

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.

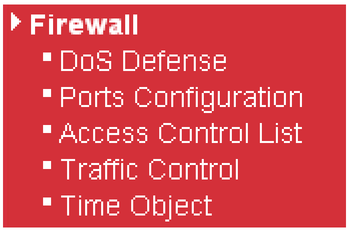
Denial of Service (DoS) Defense

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.

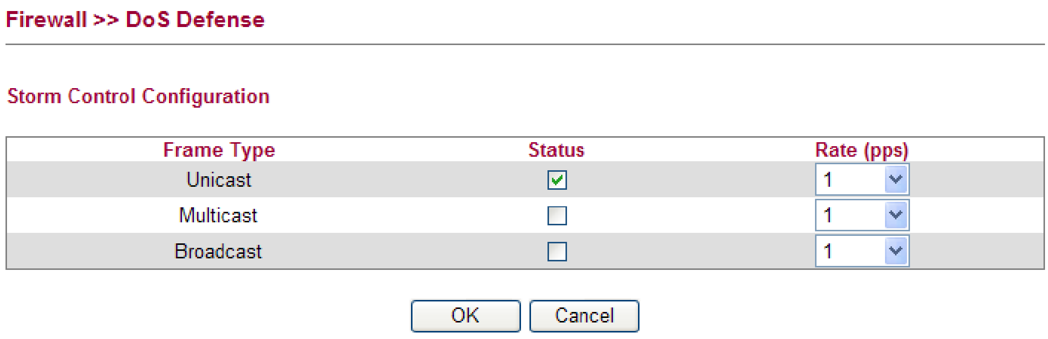
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

Below shows the menu items for Firewall.



4.4.1 DoS Defense

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



Firewall >> DoS Defense

Storm Control Configuration

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

Available settings are explained as follows:

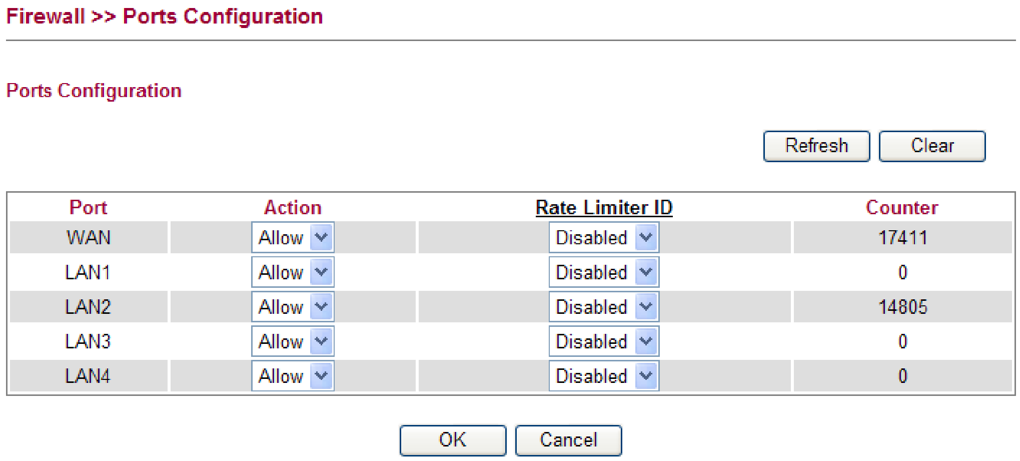
Item	Description

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.

Click **OK** to save the settings.

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).



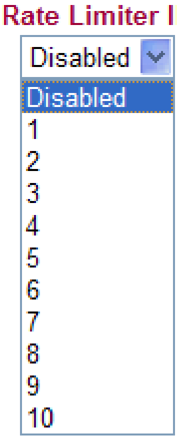
Firewall >> Ports Configuration

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

Available settings are explained as follows:

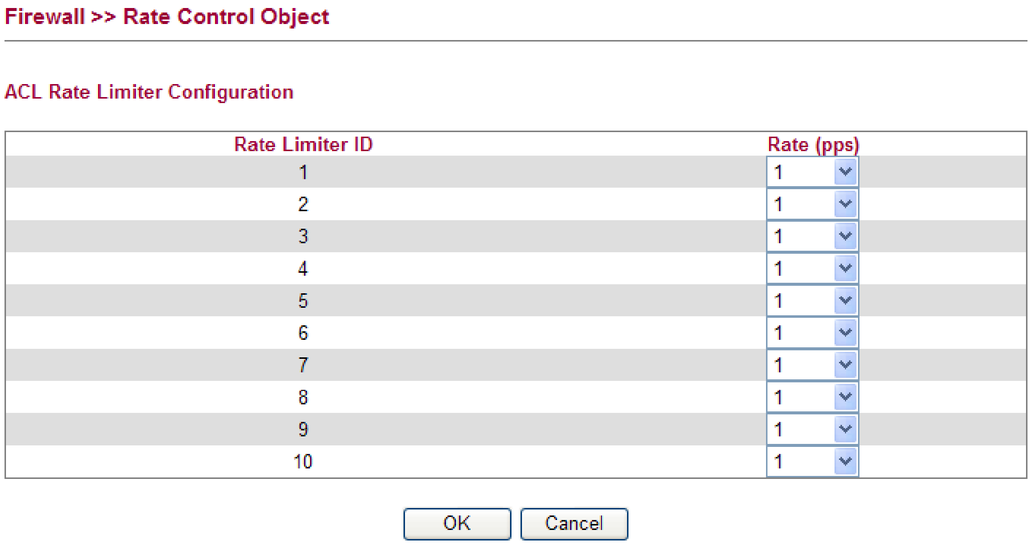
Item	Description
Port	There is one WAN port and 4 LAN ports in Vigor1000. Here each port will be configured with different ID, action, rate limiter ID, port copy and etc.
Action	Select whether forwarding is permitted ("Allow") or denied ("Deny"). The default value is "Allow". Action Allow Deny Allow

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**.  Rate Limiter ID Disabled Disabled 1 2 3 4 5 6 7 8 9 10
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.

Click **OK** to save the settings.

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.



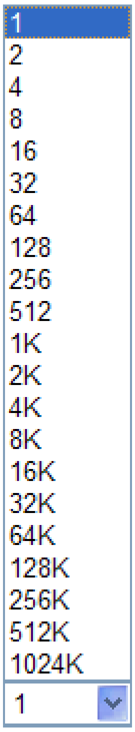
Firewall >> Rate Control Object

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

Available settings are explained as follows:

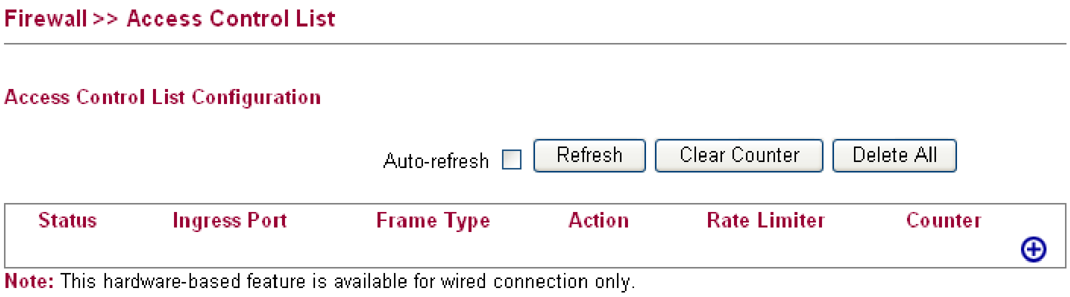
Item	Description
Rate Limiter ID	Rate limiter ID will be applied to WAN port and LAN port. Please specify a rate number for each ID. The default setting is “1”(packet per second).

Rate	Define the rate by choosing from the following drop down list.  1 2 4 8 16 32 64 128 256 512 1K 2K 4K 8K 16K 32K 64K 128K 256K 512K 1024K 1

Click **OK** to save the settings.

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

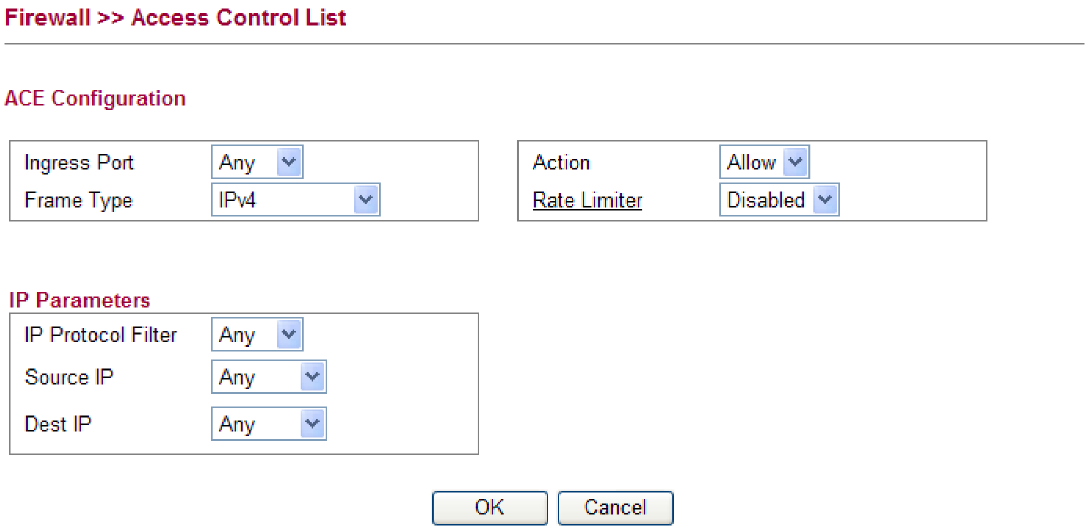
Auto-refresh □

Status	Ingress Port	Frame Type	Action	Rate Limiter	Counter
					⊕

Note: This hardware-based feature is available for wired connection only.

Adding a New Access Control Profile

Click ⊕ to add a new specific session limitation onto the list. Define which port the packet comes from.



Firewall >> Access Control List

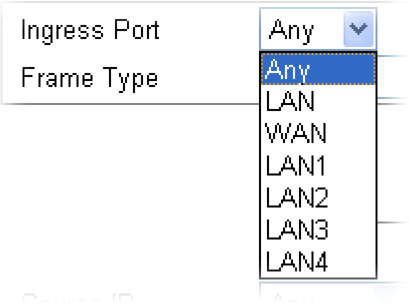
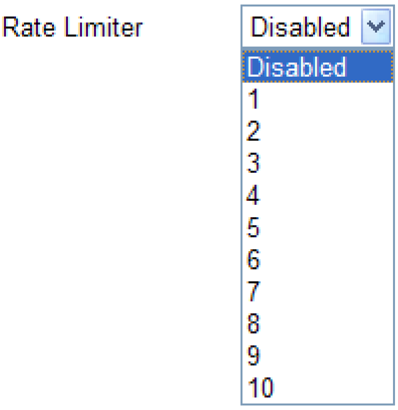
ACE Configuration

Ingress Port	Any
Frame Type	IPv4
Action	Allow
Rate Limiter	Disabled

IP Parameters

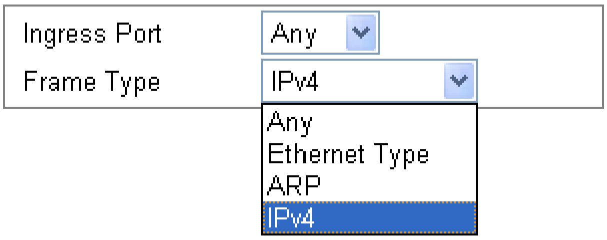
IP Protocol Filter	Any
Source IP	Any
Dest IP	Any

Available settings are explained as follows:

Item	Description
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 Any Frame Type **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

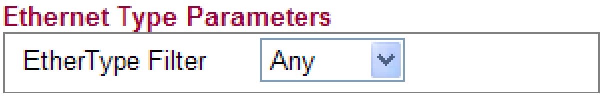
Frame Type selection will lead different options for configuration.



Ingress Port Any

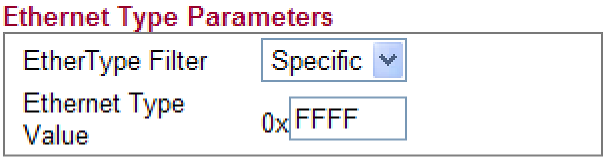
Frame Type IPv4

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

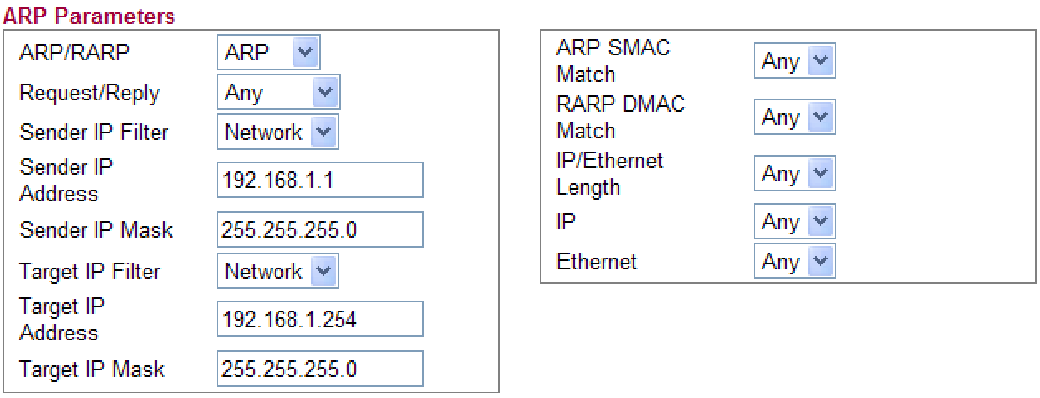


Ethernet Type Parameters

EtherType Filter	Any

Item	Description
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

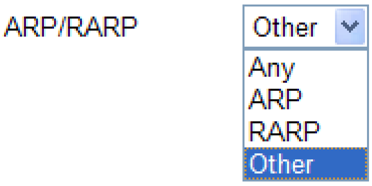
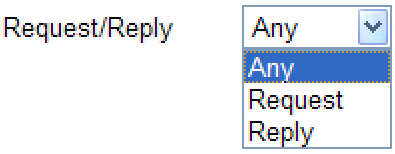
- Choose **ARP** as the Frame Type, you will get **ARP Parameters** option as the following:

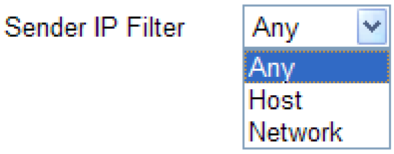
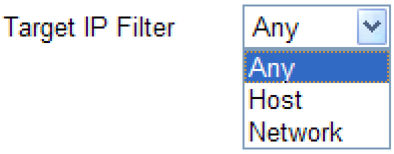
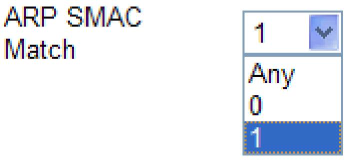


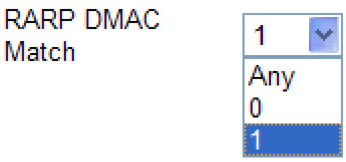
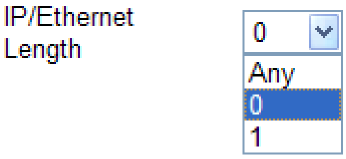
ARP Parameters

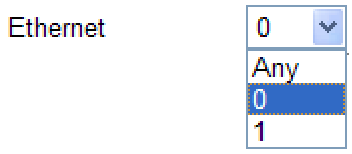
ARP/RARP	ARP
Request/Reply	Any
Sender IP Filter	Network
Sender IP Address	192.168.1.1
Sender IP Mask	255.255.255.0
Target IP Filter	Network
Target IP Address	192.168.1.254
Target IP Mask	255.255.255.0

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

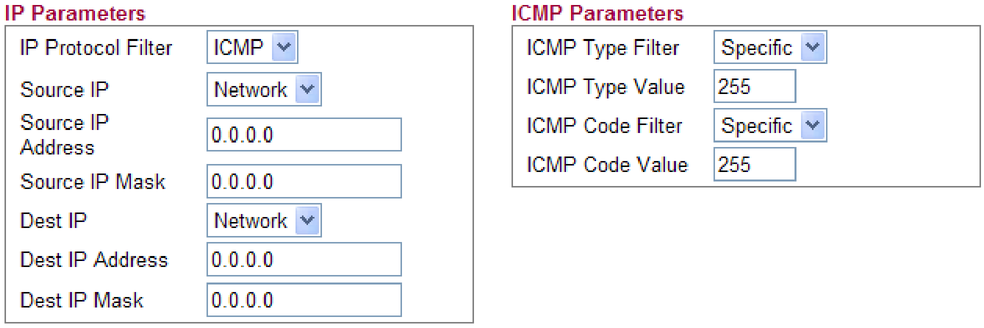
Item	Description
ARP/RARP	Choose the ARP/RARP that you want to filter.  ARP/RARP: Other Any ARP RARP Other
Request/Reply	Choose the request or replay that you want to filter.  Request/Reply: Any Any Request Reply

Sender IP Filter	Specify the sender IP filter for this ACE.  Sender IP Filter Any Any Host Network 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 Any Host Network 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 Any 0 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 Any 0 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 Any 0 1 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. IP: 0 Any 0 1 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.  Ethernet 0 Any 0 1 **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:

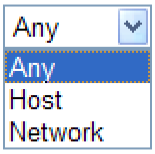


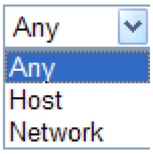
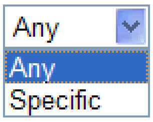
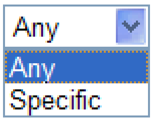
IP Parameters

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

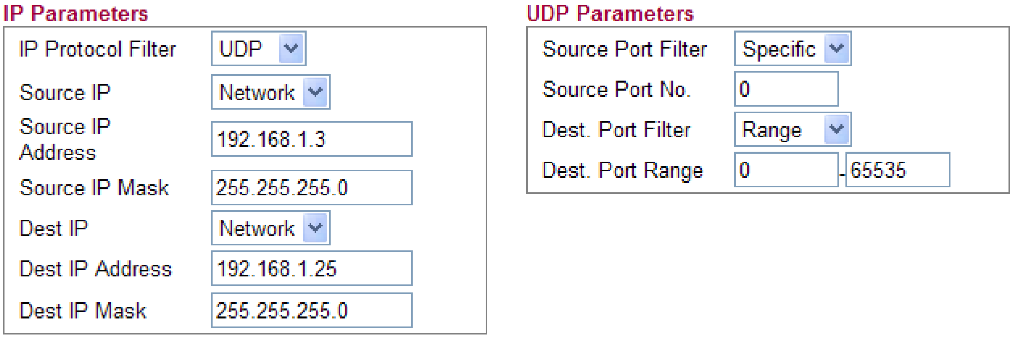
ICMP Parameters

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

Item	Description
IP Parameters	**Source IP**-Specify the Source IP filter for this ACE.  Any Any Host Network **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.

IP Parameters	**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 Parameters	**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:

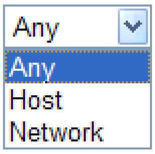
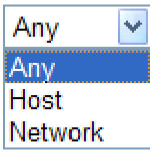


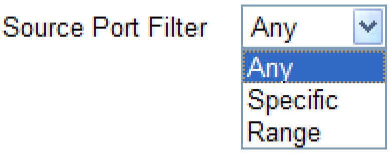
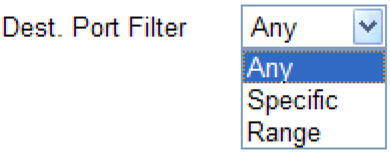
IP Parameters

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

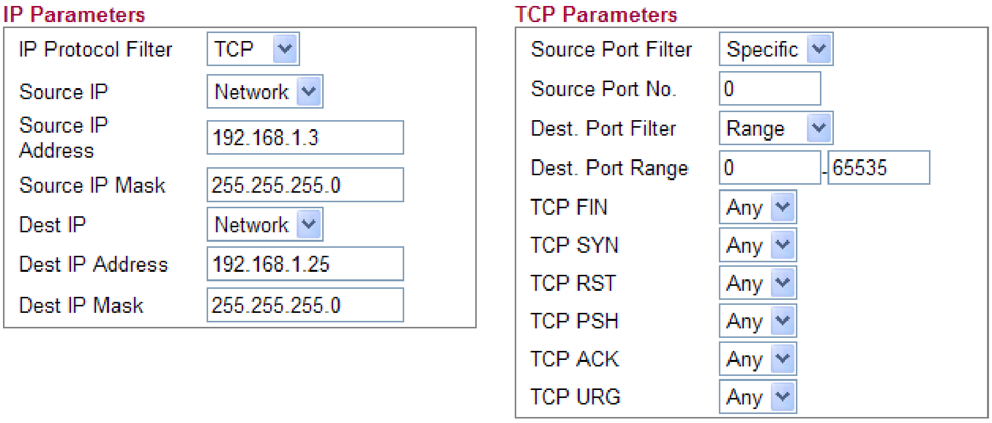
UDP Parameters

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

Item	Description
IP Parameters	**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.

UDP Parameters	**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:

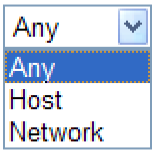
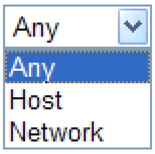


IP Parameters

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

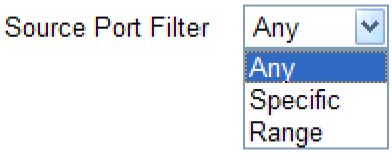
Item	Description
IP Parameters	**Source IP**-Specify the source IP filter for this ACE.  **Any:** No source IP filter is specified. **Host**: Source IP filter is set to Host. Specify the source IP address in the source IP Address field that appears. **Network:** Source IP filter is set to Network. Specify 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 SIP Mask here. This option is available only when you choose **Network** as source IP filter. **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.

IP Parameters

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.

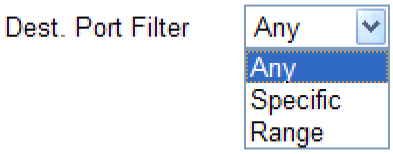
Specific: If you want to filter a specific TCP source filter with this ACE, you can enter a specific TCP source value. A field for entering a TCP source value appears.

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 Parameters

TCP FIN-Specify the TCP "No more data from sender" (FIN) value for this ACE.

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.

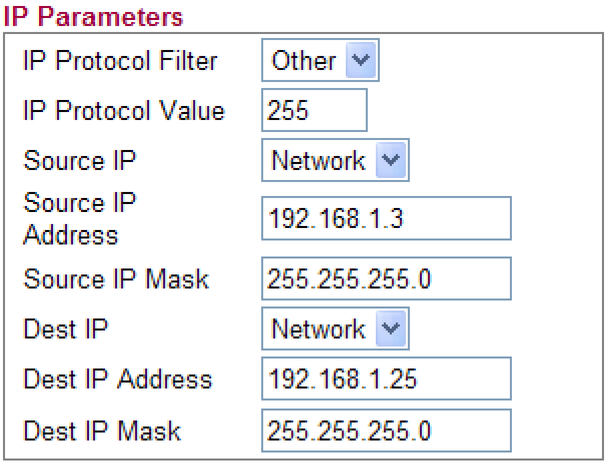
TCP ACK-Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

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.

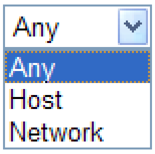
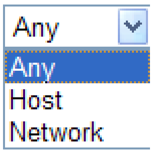
Any: Any value is allowed

- 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

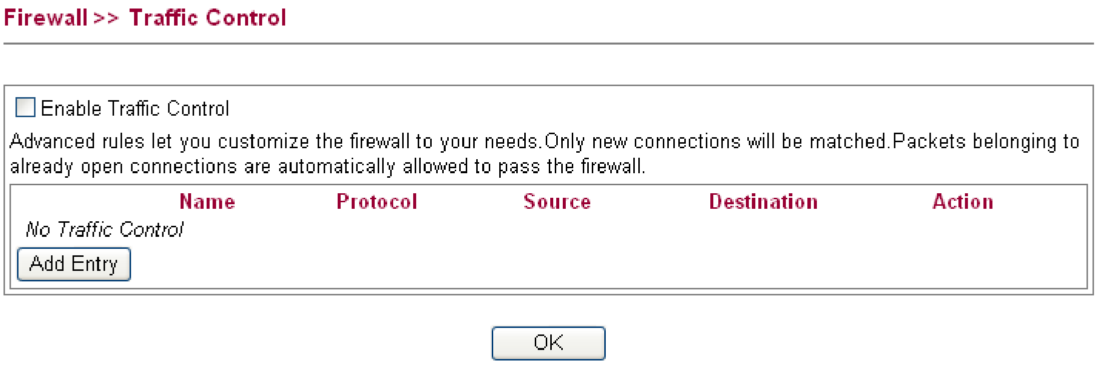
IP Protocol Filter	Other
IP Protocol Value	255
Source IP	Network
Source IP Address	192.168.1.3
Source IP Mask	255.255.255.0
Dest IP	Network
Dest IP Address	192.168.1.25
Dest IP Mask	255.255.255.0

Item	Description
IP Parameters	**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.

4.4.4 Traffic Control

There are some limitations that transmitting and receiving packets through WLAN or VPN tunnel cannot be controlled well in hardware. The function of Traffic Control is designed specifically to customize firewall rule for managing the traffic in and out.



Firewall >> Traffic Control

□ Enable Traffic Control

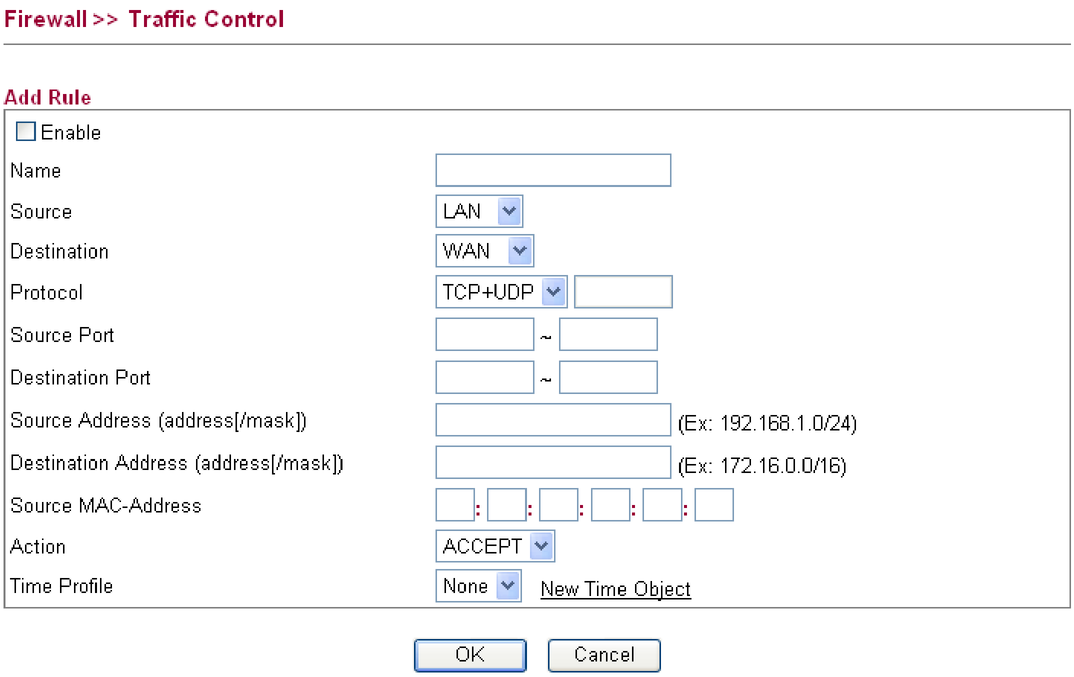
Advanced rules let you customize the firewall to your needs.Only new connections will be matched.Packets belonging to already open connections are automatically allowed to pass the firewall.

Name	Protocol	Source	Destination	Action
No Traffic Control				

Available settings are explained as follows:

Item	Description
Enable Traffic Control	Check the box to enable such function.
Add Entry	Click it add a new firewall rule.

You are allowed to add many firewall rules for your request. Simply click **Add Entry**, the following screen will be shown.



Firewall >> Traffic Control

Add Rule

☐ Enable

Name

Source: LAN

Destination: WAN

Protocol: TCP+UDP

Source Port ~

Destination Port ~

Source Address (address[/mask]) (Ex: 192.168.1.0/24)

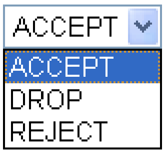
Destination Address (address[/mask]) (Ex: 172.16.0.0/16)

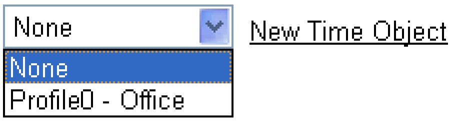
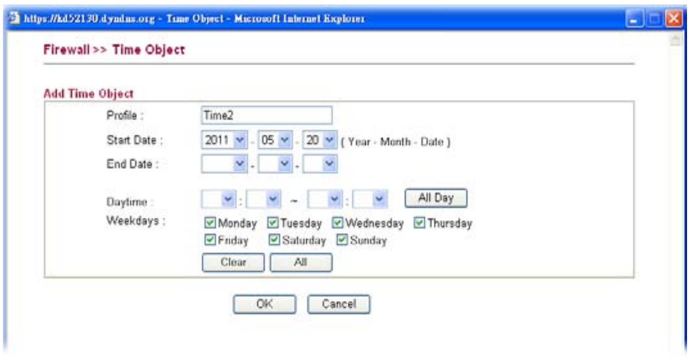
Source MAC-Address : : : : :

Action: ACCEPT

Time Profile: None New Time Object

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such rule.
Name	Type a name of the rule for identification.
Source	Specify the interface for the starting point.
Destination	Specify the interface for the ending point.
Protocol	Specify the protocol(s) which this filter rule will apply to.
Source Port / Destination Port	Type a fixed port number or a range of port number for such rule. Available value is 1 ~ 65535.
Source Address / Destination Address	Type WAN IP or LAN IP address based on the WAN or LAN interface specified in **Source** / **Destination** fields. Note that the format for this field must be "address[/mask]", e.g, 192.168.1.123 or 172.16.9.0/24.
Source MAC Address	Specify the MAC address for the packets.
Action	Choose the action to perform for the filtered packet. **Accept** – Packets matching with such rule can pass through the router. **Drop -** Packets matching with such rule will be discarded immediately. **Reject -** Packets matching with such rule cannot pass through the router and become packets with TCP reset or ICMP port unreachable packets. 

Time Profile	Specify a period for filtering the packets with web feature filter. Use the drop down list to choose the time setting, or click **New Time Object** to define a time period for you necessity.  None None Profile0 - Office New Time Object **New Time Object –** Such link allows you to create new time object for using by web feature filter. The method to configure the time object is that same as set in **Firewall>>Time Object**.  https://kd52130.dyndns.org - Time Object - Microsoft Internet Explorer Firewall >> Time Object Add Time Object Profile : Time2 Start Date : 2011 - 05 - 20 (Year - Month - Date) End Date : - - Daytime : : ~ : All Day Weekdays : ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday Clear All OK Cancel

Click **OK** to save the settings.

4.5 CSM

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

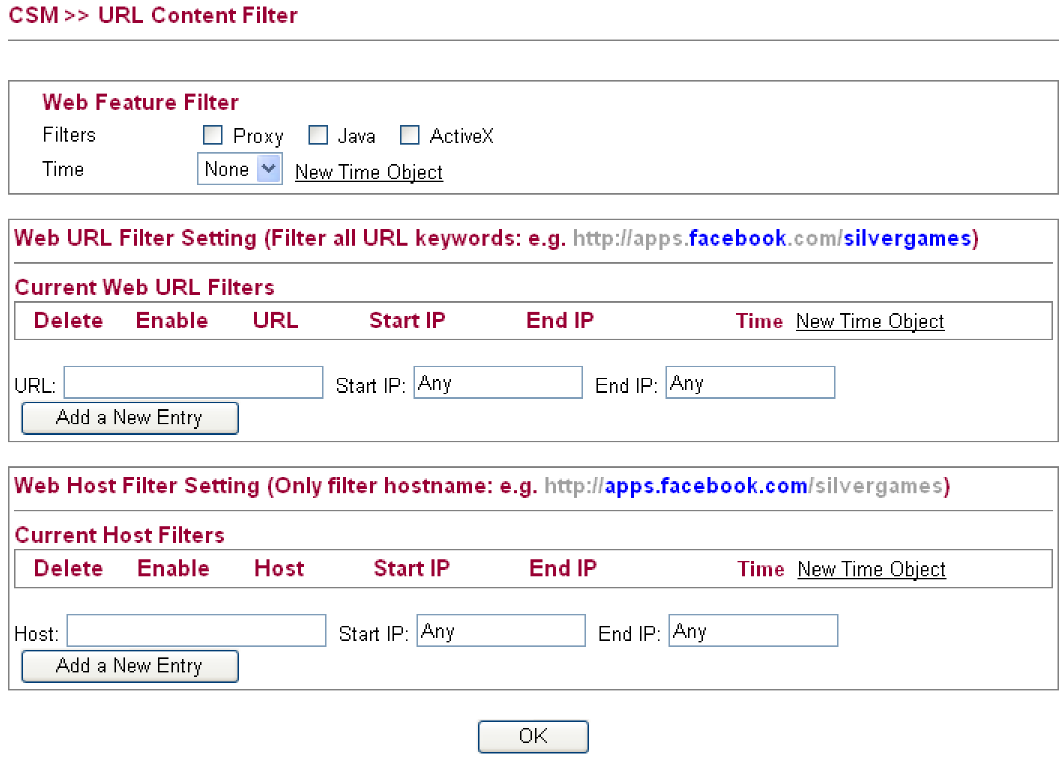
4.5.1 URL Content Filter

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

Vigor router also can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, Proxy, and so on.

In addition, Vigor router allows you to filter certain host specified with IP address.

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



CSM >> URL Content Filter

Web Feature Filter

Filters ☐ Proxy ☐ Java ☐ ActiveX

Time: None New Time Object

Web URL Filter Setting (Filter all URL keywords: e.g. http://apps.facebook.com/silvergames)

Current Web URL Filters

Delete	Enable	URL	Start IP	End IP	Time New Time Object

URL: Start IP: Any End IP: Any

Add a New Entry

Web Host Filter Setting (Only filter hostname: e.g. http://apps.facebook.com/silvergames)

Current Host Filters

Delete	Enable	Host	Start IP	End IP	Time New Time Object

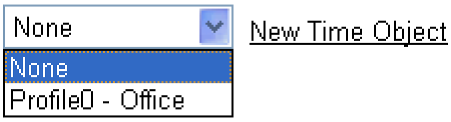
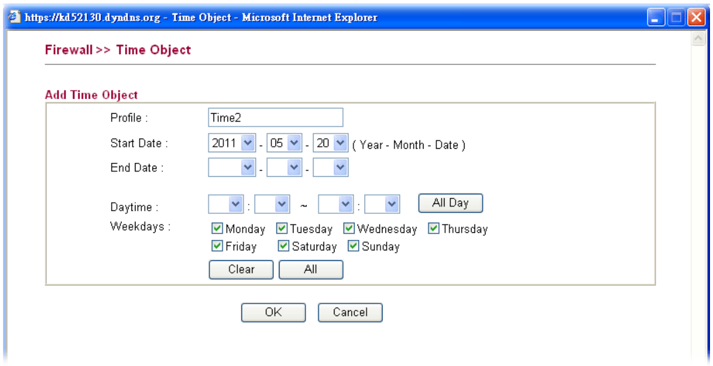
Host: Start IP: Any End IP: Any

Add a New Entry

OK

Available settings are explained as follows:

Item	Description
Web Feature Filter	If you do not check any box here, it means Vigor router will not prevent users from accidentally downloading malicious codes conceal in the executable objects from web pages. **Filters** – Choose any one of the items to be filtered by such router.

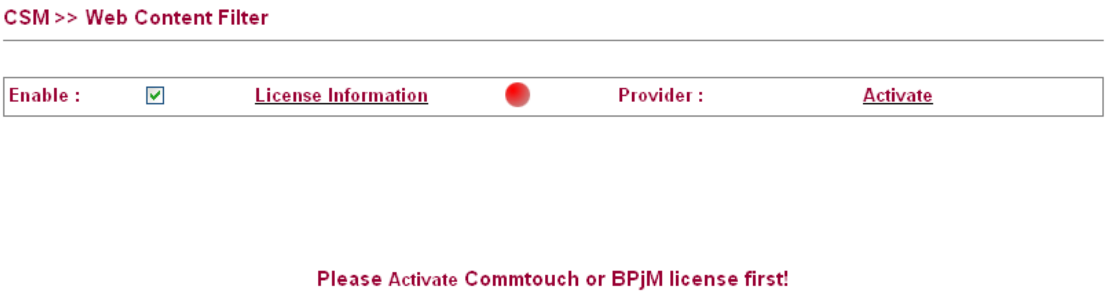
	Time –Specify a period for filtering the packets with web feature filter. Use the drop down list to choose the time setting, or click **New Time Object** to define a time period for you necessity.  **New Time Object –** Such link allows you to create new time object for using by web feature filter. The method to configure the time object is that same as set in **Firewall>>Time Object**.  https://kd52130.dyndns.org - Time Object - Microsoft Internet Explorer Firewall >> Time Object Add Time Object Profile : Time2 Start Date : 2011 - 05 - 20 (Year - Month - Date) End Date : - - Daytime : : ~ : All Day Weekdays : ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday
Web URL Filter Setting	Any URL that you want to filter by Vigor router, simply type the URL, Start IP and End IP in the specified fields and click **Add a New Entry.** The new added one will be displayed on the screen. After pressing **OK**, it will be filtered whenever you visit.
Web Host Filter Setting	Type the host name of URL for filtering. Type the host name of URL and type the Start IP and End IP and click **Add a New Entry**. The new one will be displayed on the screen. After pressing **OK**, it will be filtered whenever you visit.

4.5.2 Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Note: Be aware that Web Content Filter (WCF) is not a built-in service of Vigor router, but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer for detailed information.

Open **CSM>>Web Content Filter**. The following page will be displayed. Type the required information such as source IP address and subnet mask. Check the items that you want to filter. After finishing the general settings, please click **Activate** to activate Commtouch WCF mechanism by following the on-screen instructions.

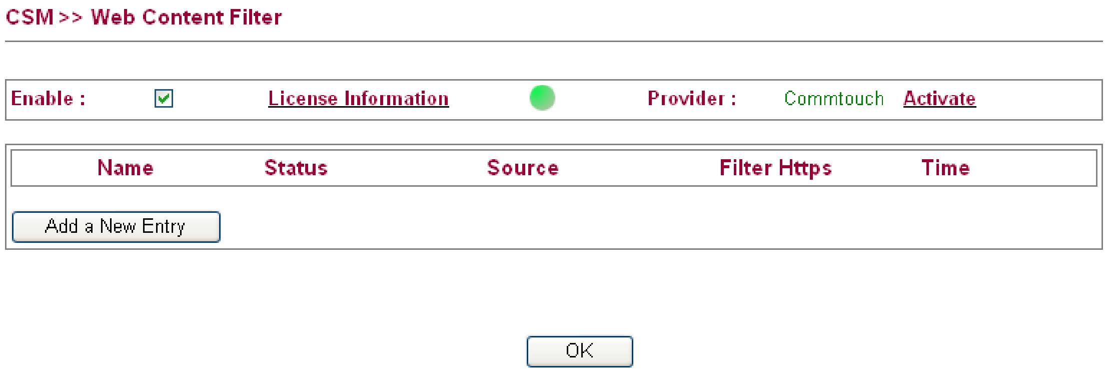


CSM >> Web Content Filter

Enable :	☑	License Information	●	Provider :	Activate

Please Activate Commtouch or BPjM license first!

If the WCF mechanism has been activated (green circle), you will see the following screen:



CSM >> Web Content Filter

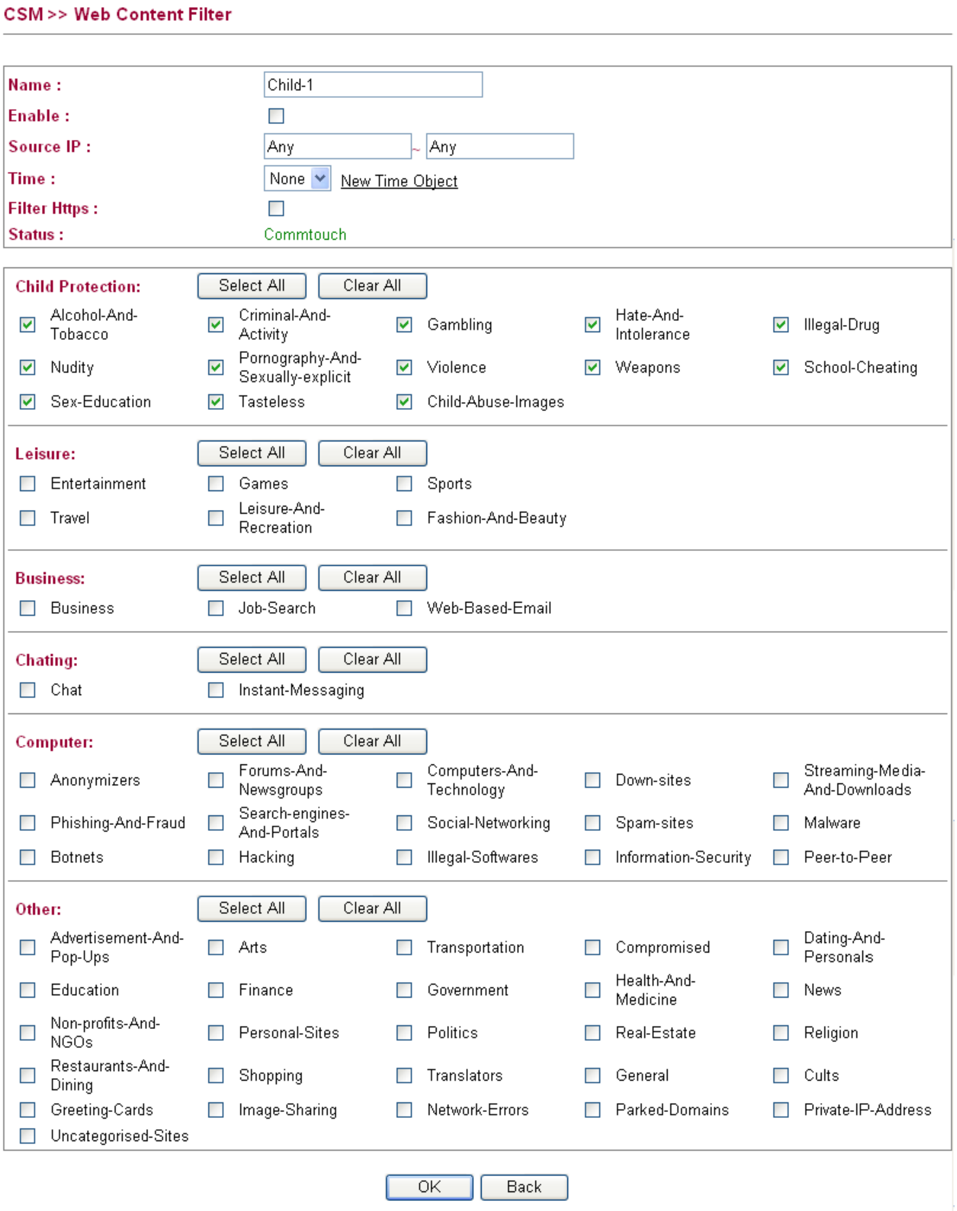
Enable :	☑	License Information	●	Provider :	Commtouch	Activate

Name	Status	Source	Filter Https	Time

Add a New Entry

OK

Now, you can click **Add a New Entry** to create a WCF profile which can be applied in **Firewall**.



CSM >> Web Content Filter

Name :	Child-1
Enable :	□
Source IP :	Any ~ Any
Time :	None ▾ New Time Object
Filter Https :	□
Status :	Commtouch

Child Protection: Select All | Clear All

☑ Alcohol-And-Tobacco	☑ Criminal-And-Activity	☑ Gambling	☑ Hate-And-Intolerance	☑ Illegal-Drug
☑ Nudity	☑ Pornography-And-Sexually-explicit	☑ Violence	☑ Weapons	☑ School-Cheating
☑ Sex-Education	☑ Tasteless	☑ Child-Abuse-Images		

Leisure: Select All | Clear All

□ Entertainment	□ Games	□ Sports
□ Travel	□ Leisure-And-Recreation	□ Fashion-And-Beauty

Business: Select All | Clear All

□ Business	□ Job-Search	□ Web-Based-Email

Chating: Select All | Clear All

□ Chat	□ Instant-Messaging

Computer: Select All | Clear All

□ Anonymizers	□ Forums-And-Newsgroups	□ Computers-And-Technology	□ Down-sites	□ Streaming-Media-And-Downloads
□ Phishing-And-Fraud	□ Search-engines-And-Portals	□ Social-Networking	□ Spam-sites	□ Malware
□ Botnets	□ Hacking	□ Illegal-Softwares	□ Information-Security	□ Peer-to-Peer

Other: Select All | Clear All

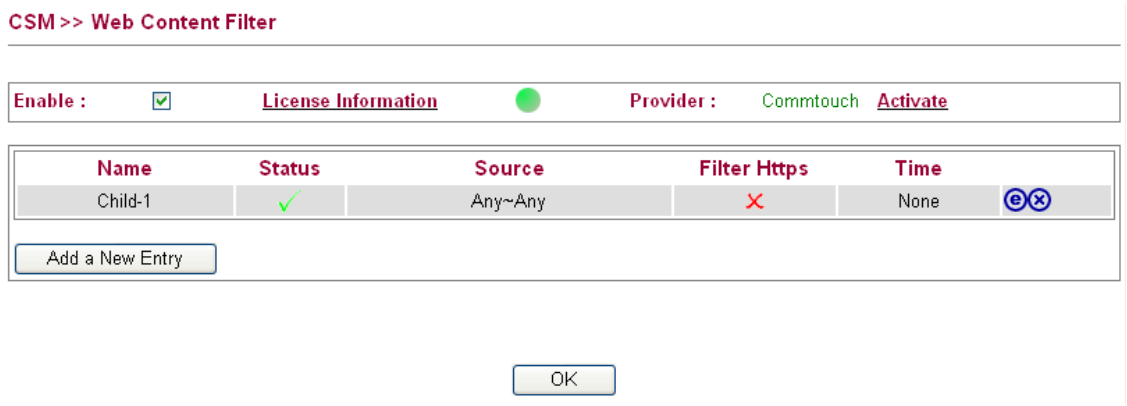
□ Advertisement-And-Pop-Ups	□ Arts	□ Transportation	□ Compromised	□ Dating-And-Personals
□ Education	□ Finance	□ Government	□ Health-And-Medicine	□ News
□ Non-profits-And-NGOs	□ Personal-Sites	□ Politics	□ Real-Estate	□ Religion
□ Restaurants-And-Dining	□ Shopping	□ Translators	□ General	□ Cults
□ Greeting-Cards	□ Image-Sharing	□ Network-Errors	□ Parked-Domains	□ Private-IP-Address
□ Uncategorised-Sites				

Available settings are explained as follows:

Item	Description
Name	Type a name for the profile.
Enable	Check the box to enable the web content filter.
Source IP	Type a range for the IP addresses (e.g, 192.168.1.12 ~ 192.168.1.20) of this profile.
Time	Use the drop down list to choose one of the time profiles. Such WCF profile will be activated on the time specified in the selected time profile. **New Time Object** – If there is no time profile created, you can click such link to access into the configuration page for setting a new one.
Filter Https	Check the box to filter the data transmitting via HTTPS.

Status	Display the service provider for current used WCF mechanism.
Child Protection / Leisure /Business / Chating / Computer / Other	Each category offers several items for you to choose. Click **Select All** to check all of the items under the selected category, or click **Clear All** to cancel the items selections.

After finished the configuration, click **OK** to save the settings and exit the page. The new added WCF profile will be displayed on the screen.



CSM >> Web Content Filter

Enable : ☑ License Information ● Provider : Commtouch Activate

Name	Status	Source	Filter Https	Time	
Child-1	✓	Any~Any	✗	None	ⓔ⊗

Add a New Entry

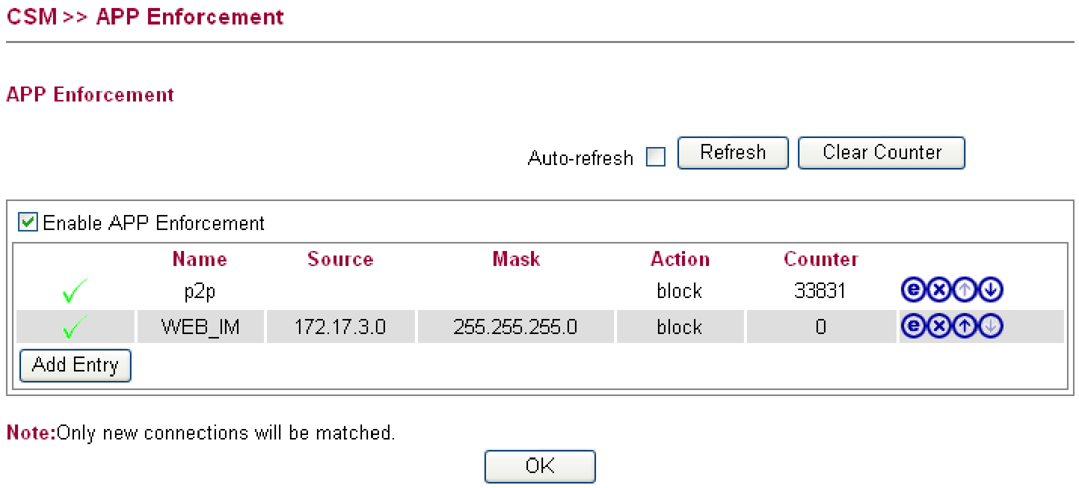
OK

To edit an existed profile, simply click the ⓔ button for the selected profile to modify it.

To delete and existed profile, simply click the ⊗ button of the selected profile to remove it.

4.5.3 APP Enforcement

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol application. This page allows you to set **32** profiles for different requirements.



CSM >> APP Enforcement

APP Enforcement

Auto-refresh □ Refresh Clear Counter

☑ Enable APP Enforcement

	Name	Source	Mask	Action	Counter	
✓	p2p			block	33831	ⓔ⊗↑↓
✓	WEB_IM	172.17.3.0	255.255.255.0	block	0	ⓔ⊗↑↓

Add Entry

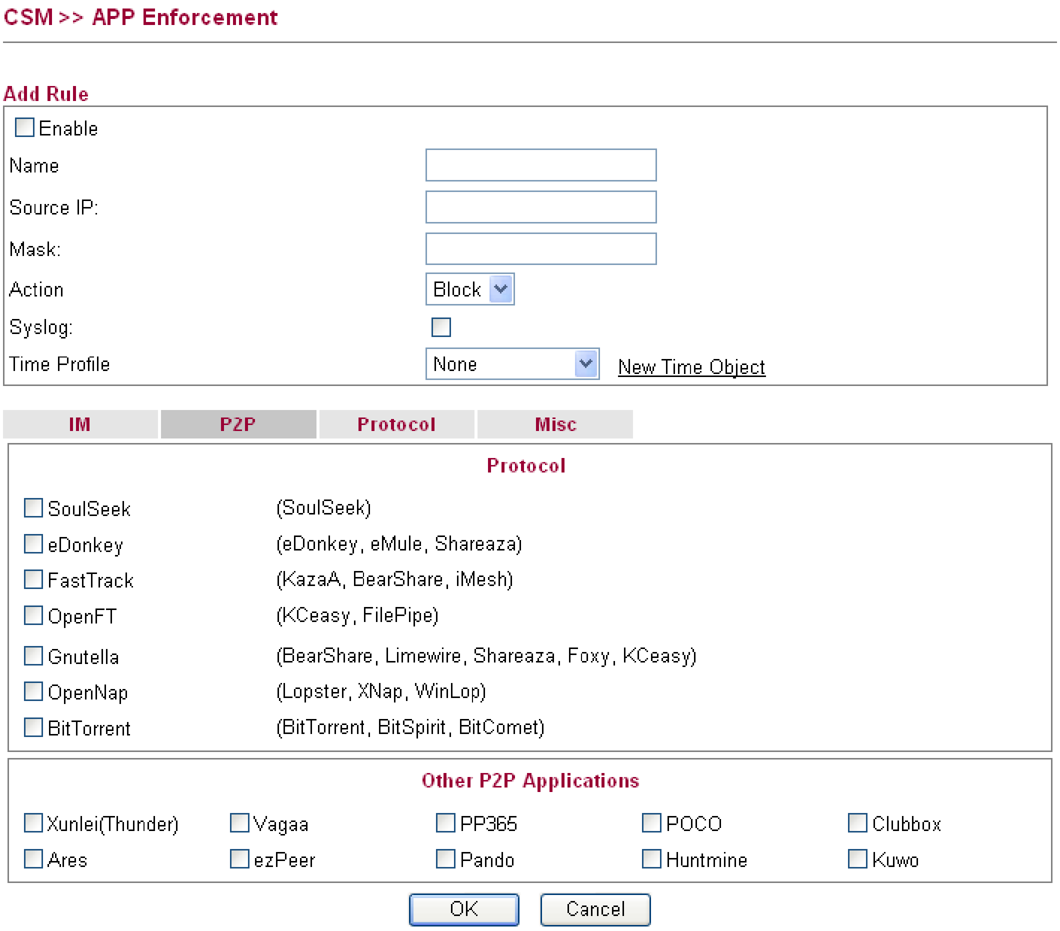
Note:Only new connections will be matched.

OK

Available settings are explained as follows:

Item	Description
Enable APP Enforcement	Check this box to enable such function. Only new network connection will be influenced by such rule.
Add Entry	Click it add a new blocking rule.

You are allowed to add many firewall rules for your request. Simply click **Add Entry**, the following screen will be shown. There are four tabs **IM, P2P, Protocol** and **Misc** displayed on this page. Each tab will bring out different items that you can choose to **disallow/allow** people using.



CSM >> APP Enforcement

Add Rule

□ Enable	
Name	
Source IP:	
Mask:	
Action	Block
Syslog:	□
Time Profile	None New Time Object

Protocol

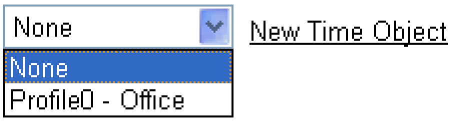
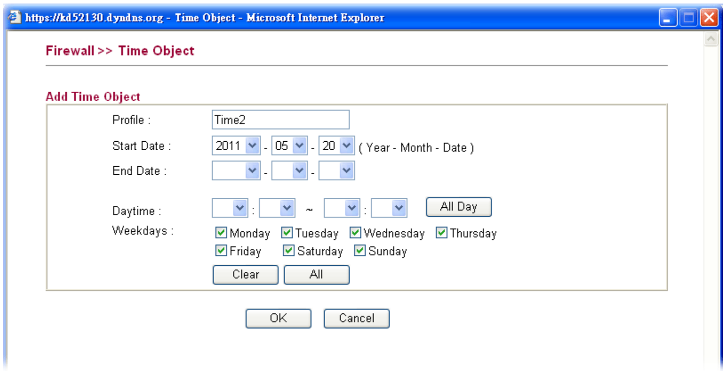
□ SoulSeek	(SoulSeek)
□ eDonkey	(eDonkey, eMule, Shareaza)
□ FastTrack	(KazaA, BearShare, iMesh)
□ OpenFT	(KCeasy, FilePipe)
□ Gnutella	(BearShare, Limewire, Shareaza, Foxy, KCeasy)
□ OpenNap	(Lopster, XNap, WinLop)
□ BitTorrent	(BitTorrent, BitSpirit, BitComet)

Other P2P Applications

□ Xunlei(Thunder)	□ Vagaa	□ PP365	□ POCO	□ Clubbox
□ Ares	□ ezPeer	□ Pando	□ Huntmine	□ Kuwo

Available settings are explained as follows:

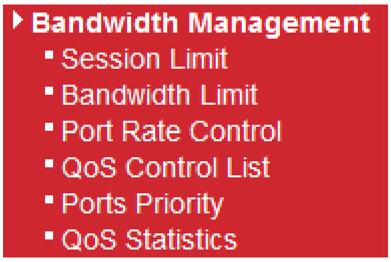
Item	Description
Enable	Check the box to enable such rule.
Name	Type a name of the rule for identification.
Source IP	Type IP address in LAN. Packets passing through such IP address will be filtered by the router.
Mask	Type the mask for the source IP.
Action	**Block** – Packets matching with such rule will be blocked by the router. **Pass** – Packets matching with such rule are allowed to pass through the router.
Syslog	Check this box to record the information on Syslog.

Time Profile	Specify a period for filtering the packets with web feature filter. Use the drop down list to choose the time setting, or click **New Time Object** to define a time period for you necessity.  **New Time Object –** Such link allows you to create new time object for using by web feature filter. The method to configure the time object is that same as set in **Firewall>>Time Object**.  https://kd52130.dyndns.org - Time Object - Microsoft Internet Explorer Firewall >> Time Object Add Time Object Profile : Time2 Start Date : 2011 - 05 - 20 (Year - Month - Date) End Date : - - Daytime : : ~ : Weekdays : ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Simply check the box(s) that you want to block and click **OK** to save the settings.

4.6 Bandwidth Management

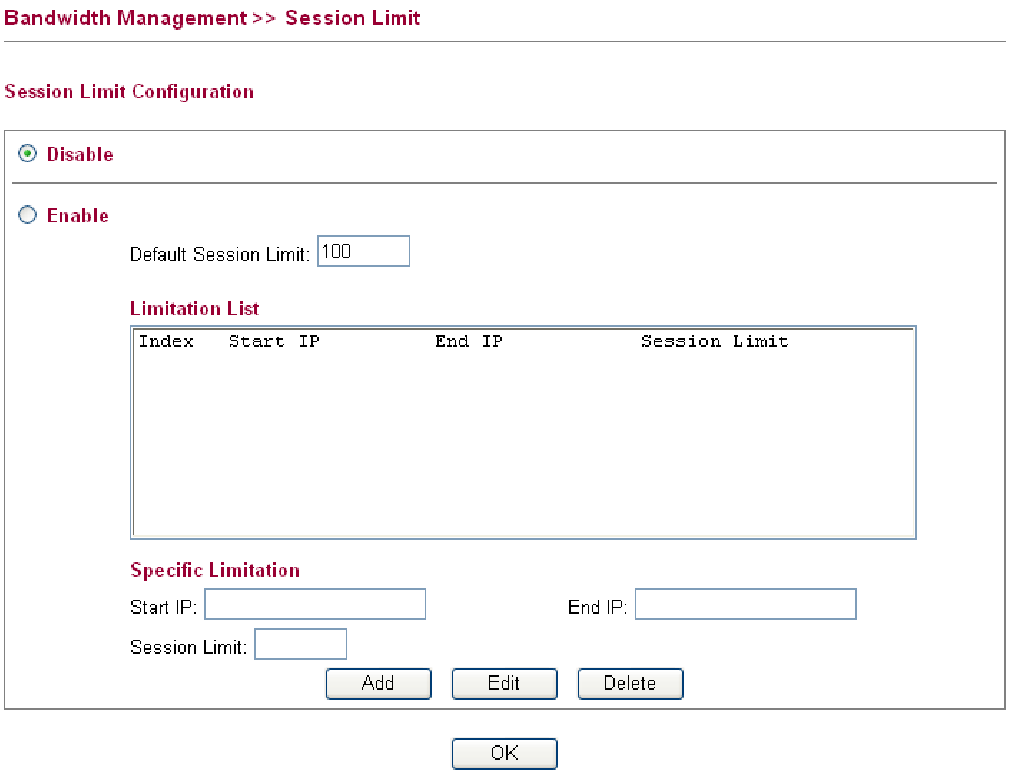
Below shows the menu items for Bandwidth Management.



4.6.1 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

● Disable

○ Enable

Default Session Limit: 100

Limitation List

```
Index   Start IP          End IP              Session Limit
```

Specific Limitation

Start IP: End IP:

Session Limit:

Available settings are explained as follows:

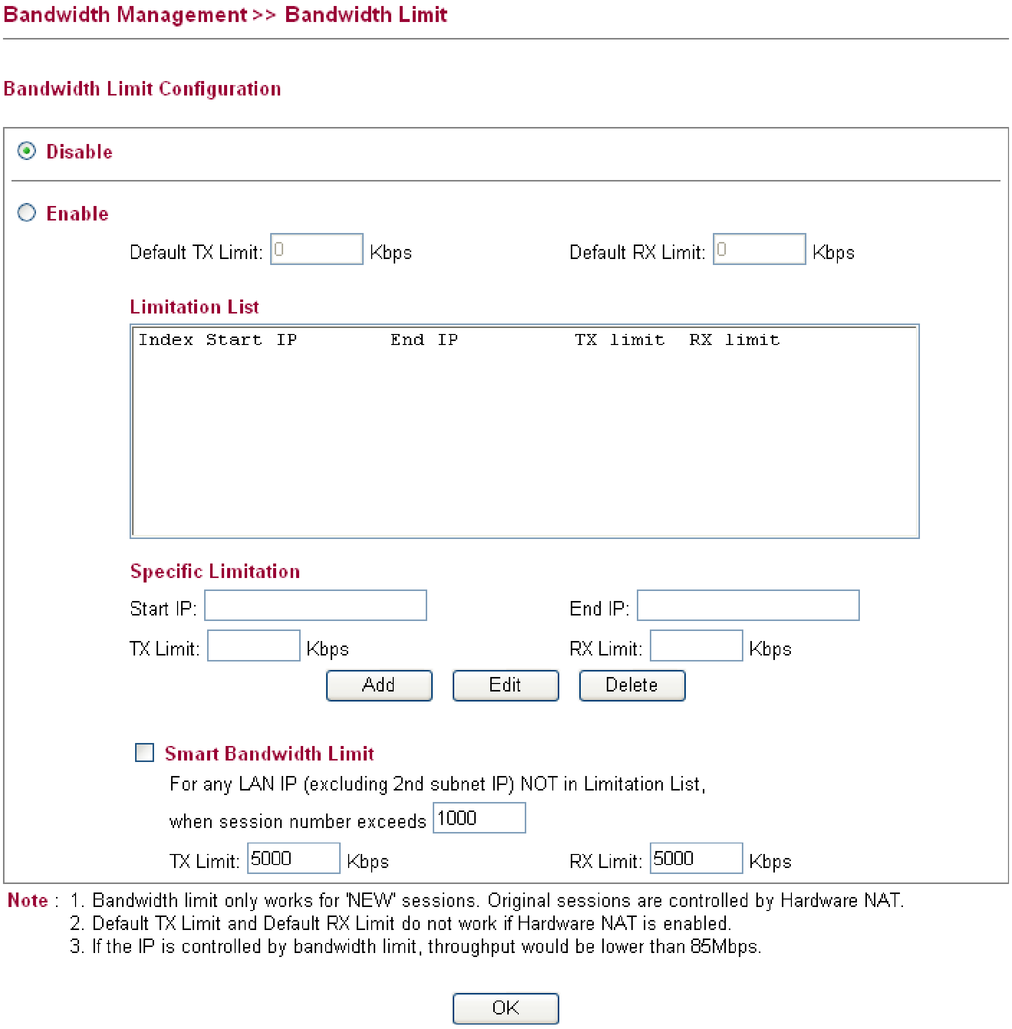
Item	Description
Enable	activate the function of limit session, simply click **Enable** and set the default session limit.
Disable	Click this button to close the function of limit session. **Default Sessions Limit-** Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP -** Defines the start LAN IP address for limit session. **End IP-** Defines the end LAN IP address for limit session. **Sessions Limit -** 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**.

4.6.2 Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

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



Bandwidth Management >> Bandwidth Limit

Bandwidth Limit Configuration

● Disable

○ Enable

Default TX Limit: 0 Kbps Default RX Limit: 0 Kbps

Limitation List

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

Specific Limitation

Start IP: End IP:

TX Limit: Kbps RX Limit: Kbps

□ Smart Bandwidth Limit

For any LAN IP (excluding 2nd subnet IP) NOT in Limitation List,

when session number exceeds 1000

TX Limit: 5000 Kbps RX Limit: 5000 Kbps

Note : 1. Bandwidth limit only works for 'NEW' sessions. Original sessions are controlled by Hardware NAT.
2. Default TX Limit and Default RX Limit do not work if Hardware NAT is enabled.
3. If the IP is controlled by bandwidth limit, throughput would be lower than 85Mbps.

Available settings are explained as follows:

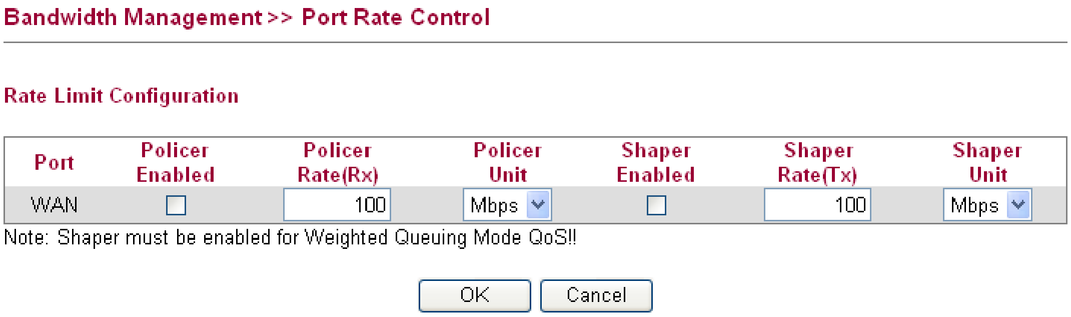
Item	Description
Disable	Disable this function.
Enable	To activate the function of limit bandwidth, simply click **Enable** and set the default or user-defined upstream and downstream limit. **Default TX Limit** - Define the limitation for the speed of the upstream as default setting. **Default RX Limit** - Define the limitation for the speed of the downstream as default setting.

Limitation List	**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.
Smart Bandwidth Limit	Check this box to configure the default limitation for bandwidth. **When session number exceeds –** type the value here as a threshold to apply the smart bandwidth limit. **TX limit** - Define the default speed of the upstream for each computer in LAN. **RX limit** - Define the default speed of the downstream for each computer in LAN.

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

4.6.3 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	□	100	Mbps	□	100	Mbps

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

Available settings are explained as follows:

Item	Description
Port	Represent LAN or WAN interface.
Policer Enabled	Check this box to enable policer function to limit the bandwidth of received frames.
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.

Click **OK** to save the settings.

4.6.4 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?

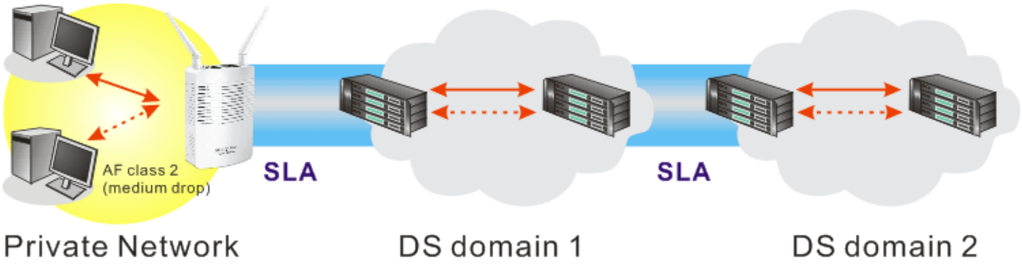
There are two components within Primary configuration of QoS deployment:

- 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.

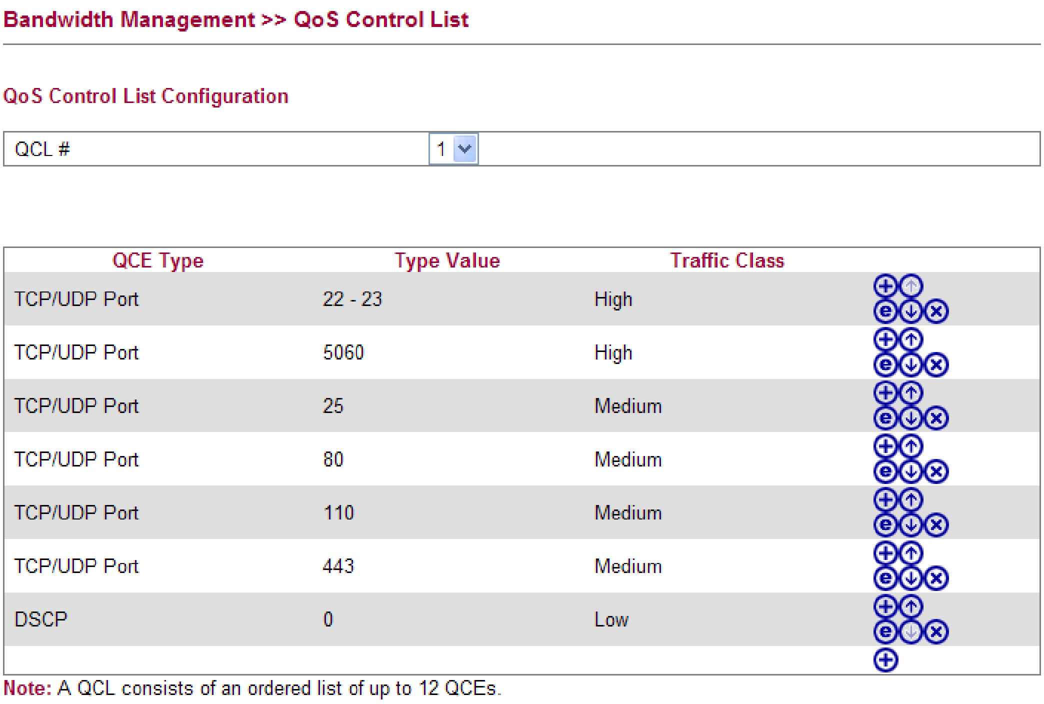
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes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

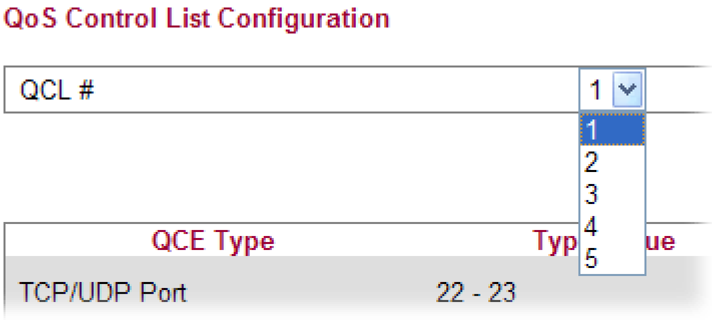
QCE Type	Type Value	Traffic Class
TCP/UDP Port	22 - 23	High
TCP/UDP Port	5060	High
TCP/UDP Port	25	Medium
TCP/UDP Port	80	Medium
TCP/UDP Port	110	Medium
TCP/UDP Port	443	Medium
DSCP	0	Low

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

Available settings are explained as follows:

Item	Description
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 (QCL) allows users to set up to **five** groups of QCL. Each QCL group can contain 12 QCE settings.



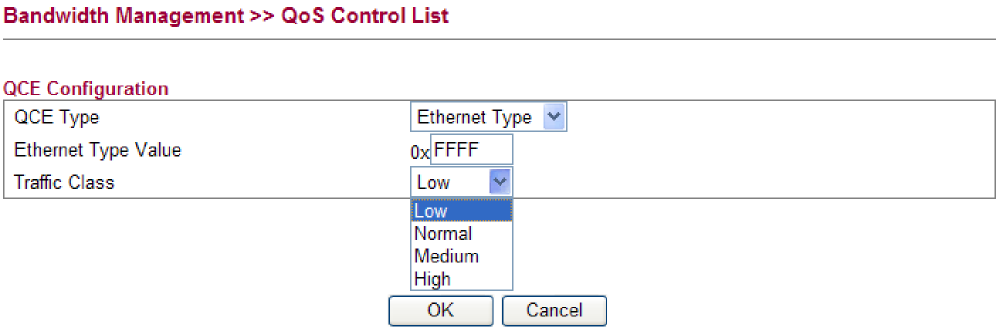
QoS Control List Configuration

QCL # 1

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

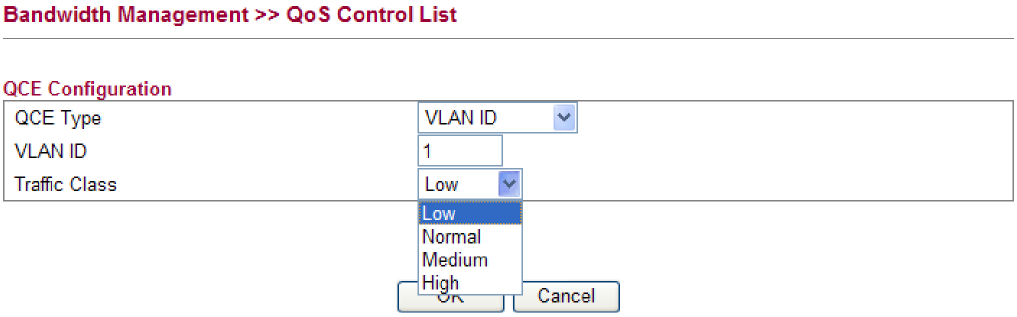
QCE Configuration

QCE Type	Ethernet Type
Ethernet Type Value	0x FFFF
Traffic Class	Low

Available settings are explained as follows:

Item	Description
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.

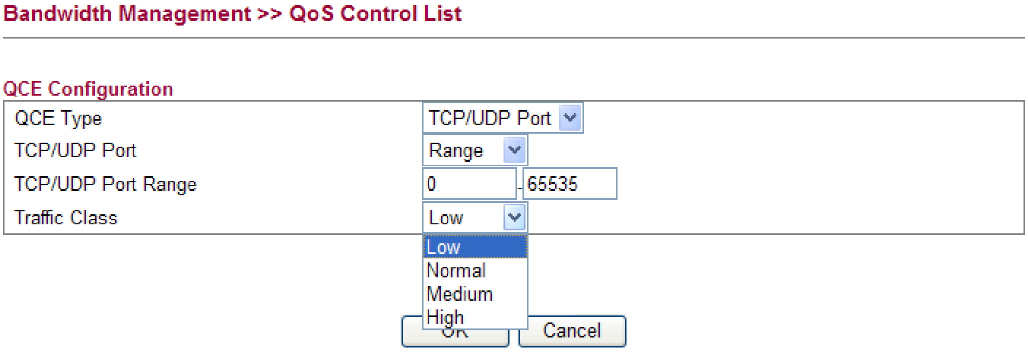


Bandwidth Management >> QoS Control List

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

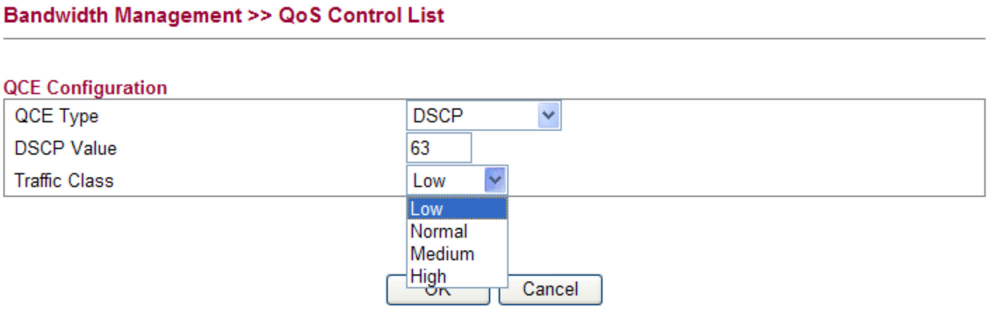
QCE Configuration

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

Available settings are explained as follows:

Item	Description
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.

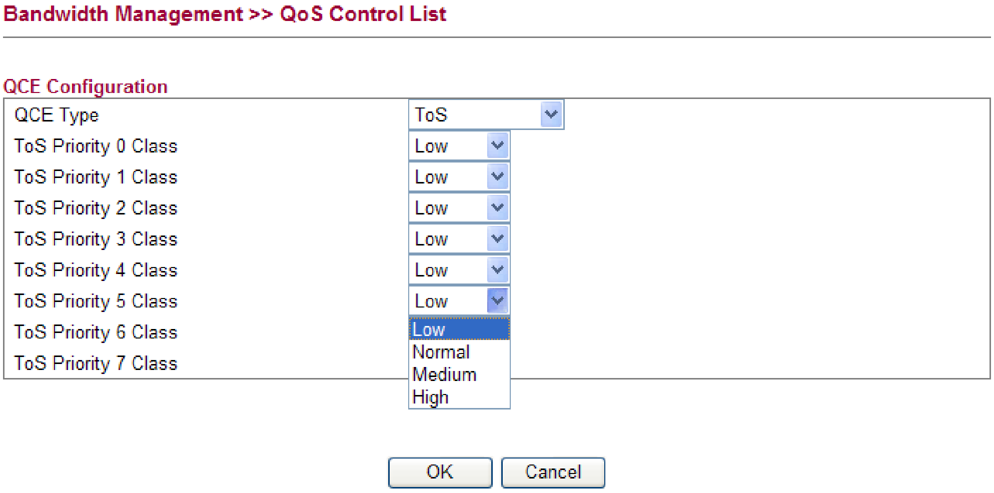


Bandwidth Management >> QoS Control List

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.

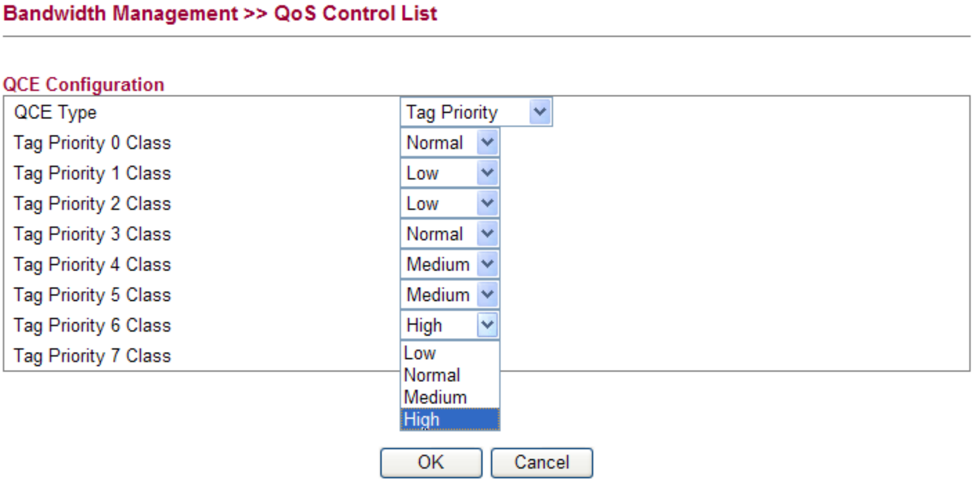


Bandwidth Management >> QoS Control List

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

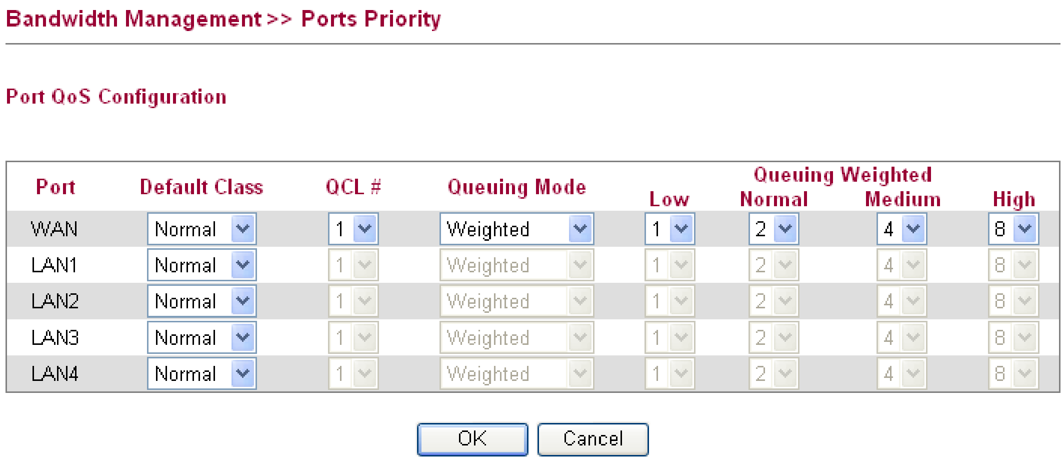
Click ⬇ and ⬆ to move a QCE up and down.

Deleting a QCE

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

4.6.5 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.

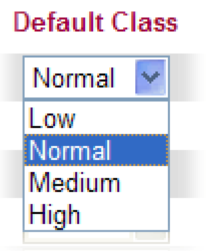


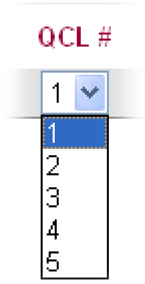
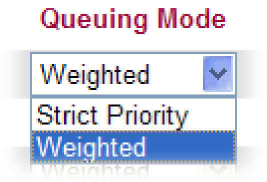
Bandwidth Management >> Ports Priority

Port QoS Configuration

Port	Default Class	QCL #	Queuing Mode	Queuing Weighted			
				Low	Normal	Medium	High
WAN	Normal	1	Weighted	1	2	4	8
LAN1	Normal	1	Weighted	1	2	4	8
LAN2	Normal	1	Weighted	1	2	4	8
LAN3	Normal	1	Weighted	1	2	4	8
LAN4	Normal	1	Weighted	1	2	4	8

Available settings are explained as follows:

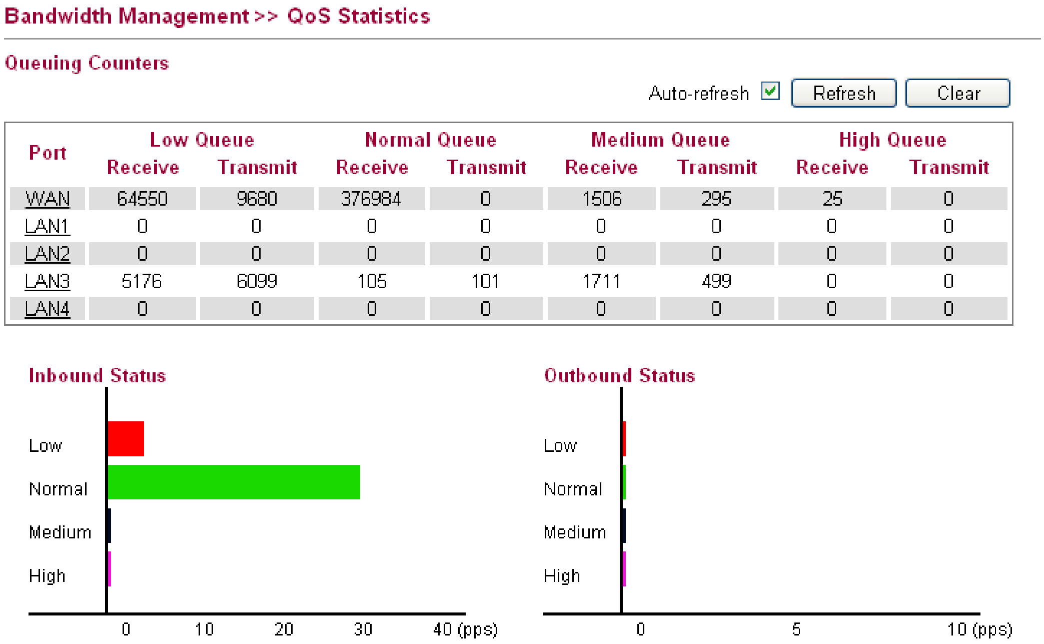
Item	Description
Port	Indicate the interface for the physical port, WAN port, LAN port and so on.
Default Class	Use the drop down list to choose the priority for each port.  Default Class Normal Low Normal Medium High

QCL (QoS Control List)	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.

Click **OK** to save the settings.

4.6.6 QoS Statistics

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



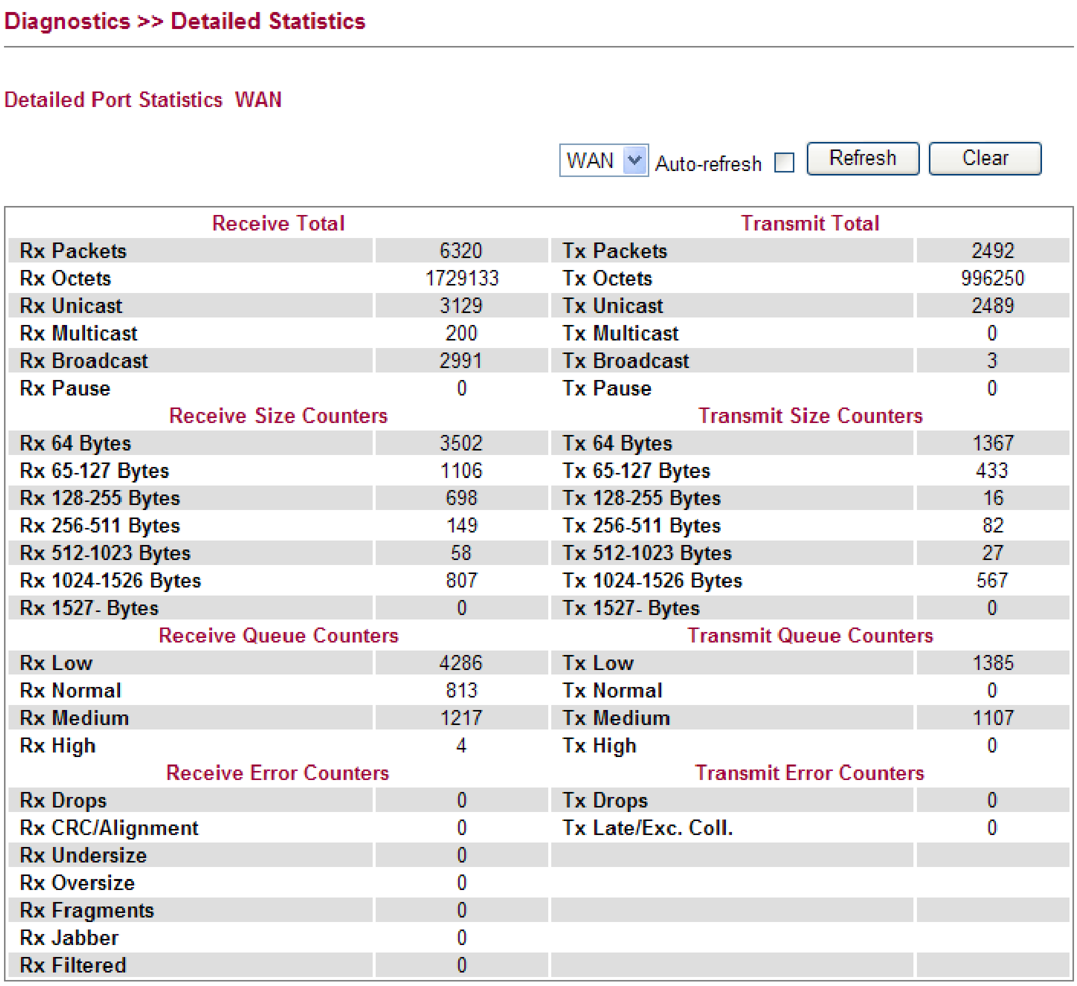
Bandwidth Management >> QoS Statistics

Queuing Counters

Auto-refresh ☑ Refresh Clear

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
WAN	64550	9680	376984	0	1506	295	25	0
LAN1	0	0	0	0	0	0	0	0
LAN2	0	0	0	0	0	0	0	0
LAN3	5176	6099	105	101	1711	499	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		

Available settings are explained as follows:

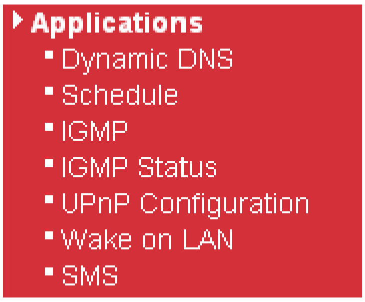
Item	Description
WAN/LAN	Choose WAN or LAN to display the corresponding statistics.
Auto-refresh	Check it to enable auto-refresh function.
Refresh	Click it to reload the page.
Clear	Click it to clear the counters for all ports.
Receive Total	**Rx Packets -** Display the counting number of the packet 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.
Receive Size Counters	**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.
Receive Queue Counters	**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.
Receive Error Counters	**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.
Transmit Total	**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.
Transmit Size Counters	**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.
Transmit Queue Counters	**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.
Transmit Error Counters	**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.

4.7 Applications

Below shows the menu items for Applications.

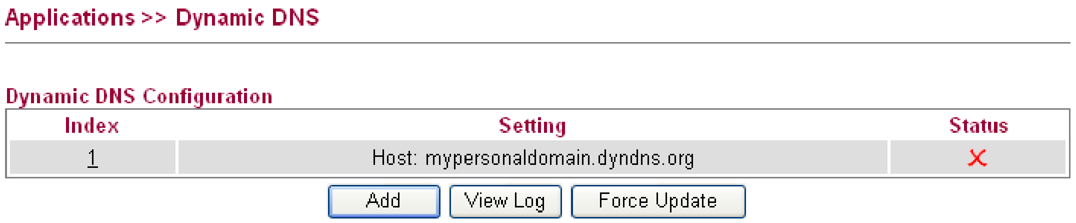


4.7.1 Dynamic DNS

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

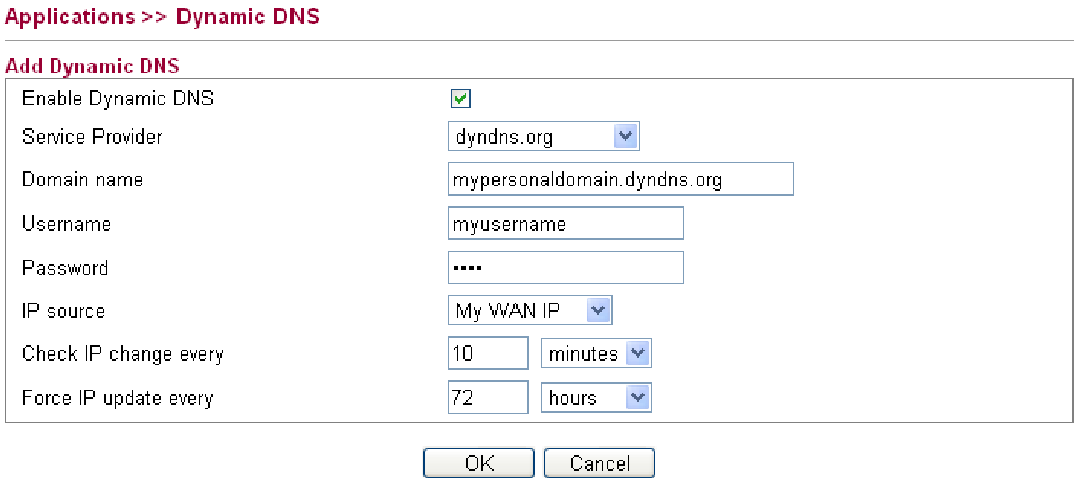
Dynamic DNS Configuration

Index	Setting	Status
1	Host: mypersonaldomain.dyndns.org	✗

Each item can be explained as follows

Item	Description
Index	Display the DDNS profile link.
Setting	Display a brief description for the profile.
Status	Display the status (disabled or enabled) of the profile.
Add	Allow you to add a new profile.
View Log	Allow you to view the log of the DDNS profile.
Force Update	Click this button to update the DDNS immediately.

To create a new DDNS profile, simply click **Add**. The following page will appear.

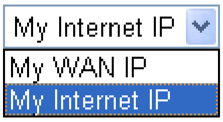

Applications >> Dynamic DNS

Add Dynamic DNS

Enable Dynamic DNS	☑
Service Provider	dyndns.org
Domain name	mypersonaldomain.dyndns.org
Username	myusername
Password	••••
IP source	My WAN IP
Check IP change every	10 minutes
Force IP update every	72 hours

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS	Check this box to enable the current account.
Service Provider	Select the service provider for the DDNS account.
Domain name	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.

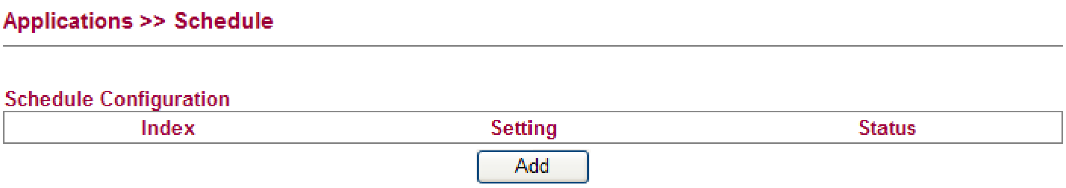
IP Source	Determine the IP source for DDNS server. **My WAN IP** – Use IP configured for WAN interface for DDNS server. **My Internet IP** – Use true IP for DDNS server.  My Internet IP My WAN IP My Internet IP
Check IP change every	Set the interval for checking the information.
Force IP update every	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.

4.7.2 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.

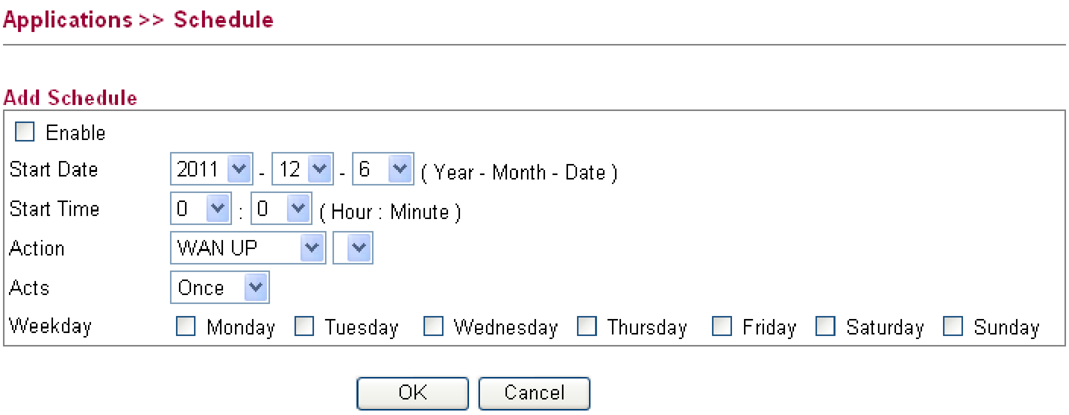


Applications >> Schedule

Schedule Configuration

Index	Setting	Status

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

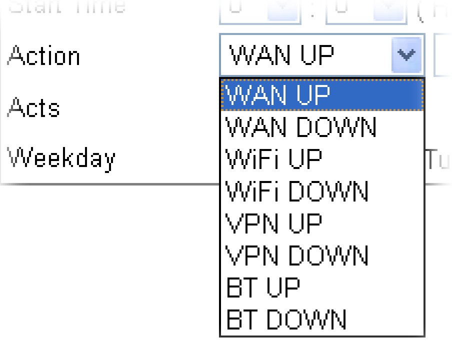


Applications >> Schedule

Add Schedule

□ Enable	
Start Date	2011 - 12 - 6 (Year - Month - Date)
Start Time	0 : 0 (Hour : Minute)
Action	WAN UP
Acts	Once
Weekday	□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

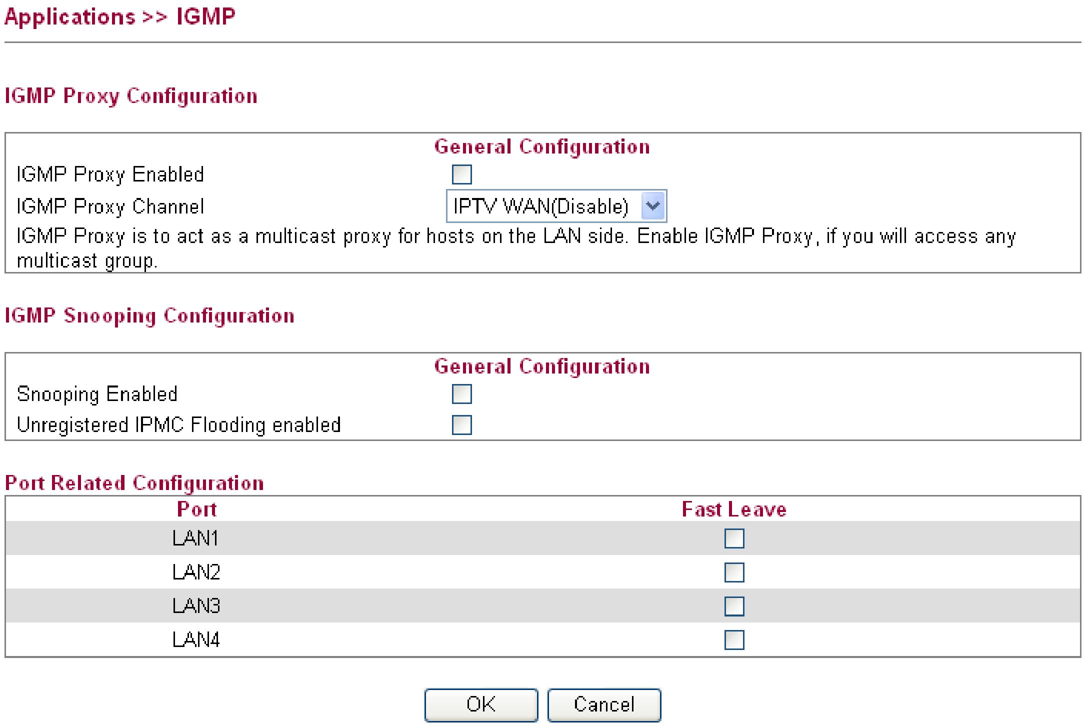
Available settings are explained as follows:

Item	Description
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.  Start Time Action Acts Weekday WAN UP WAN UP WAN DOWN WiFi UP WiFi DOWN VPN UP VPN DOWN BT UP BT DOWN Tu **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. **BT UP/DOWN** - BT 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.

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

4.7.3 IGMP

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

IGMP Proxy Configuration

General Configuration	
IGMP Proxy Enabled	□
IGMP Proxy Channel	IPTV WAN(Disable)

IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group.

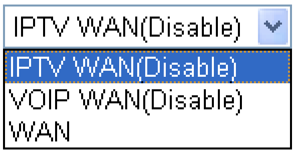
IGMP Snooping Configuration

General Configuration	
Snooping Enabled	□
Unregistered IPMC Flooding enabled	□

Port Related Configuration

Port	Fast Leave
LAN1	□
LAN2	□
LAN3	□
LAN4	□

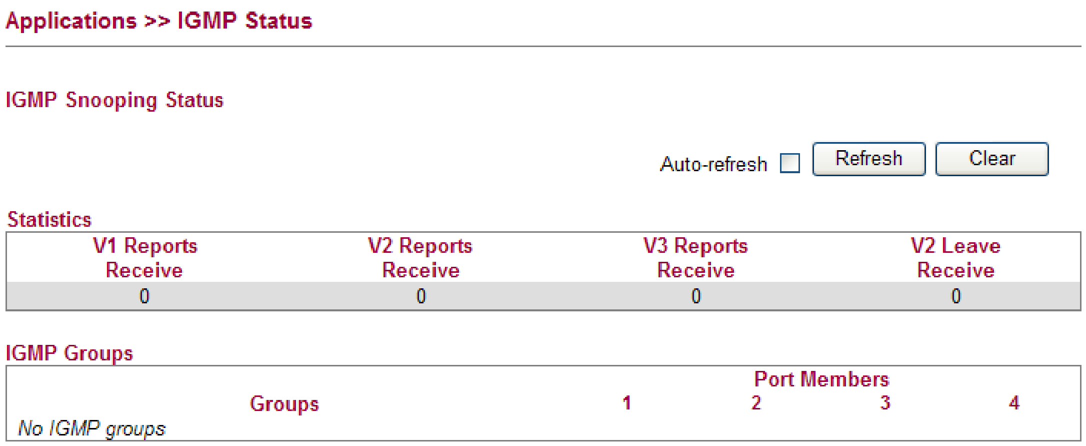
Available settings are explained as follows:

Item	Description
IGMP Proxy Configuration	**IGMP Proxy Enabled -** Check the box to enable this function. The IGMP proxy can act as a multicast proxy for hosts on LAN sides. If you enable such function, you can access any multicast group whenever you want. **IGMP Proxy Channel** – Use the drop down list to choose the proxy channel. (Disable) means that channel has not been enabled. Go to **WAN>>Multi-VALN** to enable IPTV WAN/VoIP WAN first before choosing the corresponding options.  IPTV WAN(Disable) IPTV WAN(Disable) VOIP WAN(Disable) WAN
IGMP Snooping Configuration	**Snooping Enabled -** Check the box to enable this function. **Unregistered IPMC Flooding enabled -** Check the box to enable unregistered IPMC traffic flooding.
Port Related Configuration	Check the box to make the LAN port supporting IGMP Fast Leave. **Fast Leave -** Check the box to fast leave from the LAN port.

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

4.7.4 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

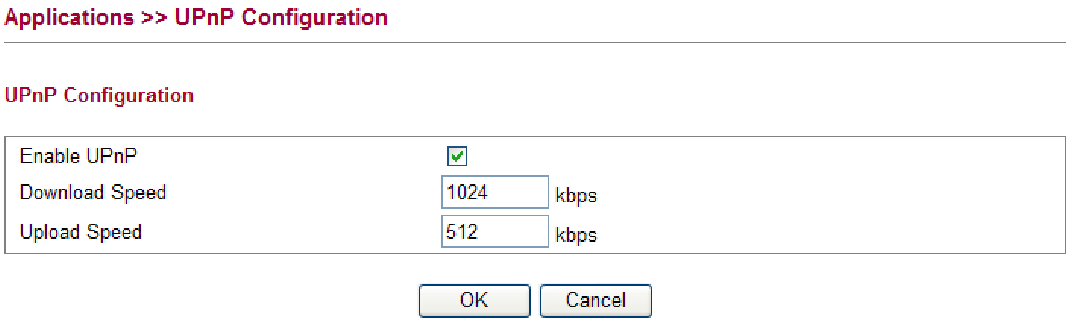
Groups	Port Members 1	2	3	4
No IGMP groups				

Available settings are explained as follows:

Item	Description
Auto-refresh	Check it to enable auto-refresh function.
Refresh	Click this button to refresh the page immediately.
Clear	Click this button to clear the settings on this page.
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.

4.7.5 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

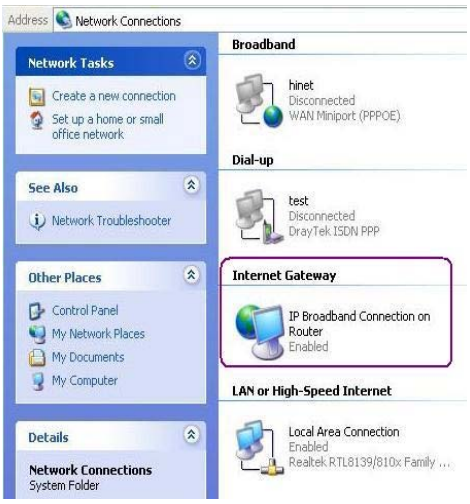
UPnP Configuration

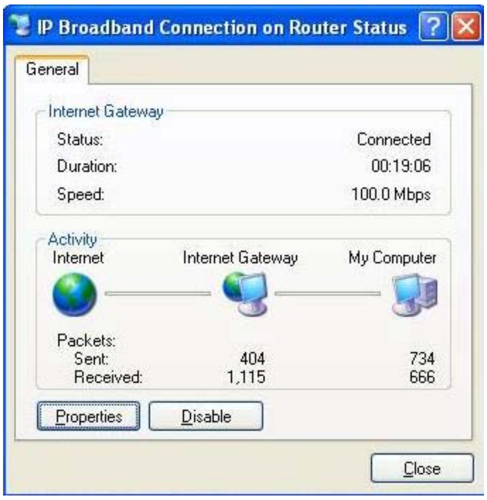
Enable UPnP	☑
Download Speed	1024 kbps
Upload Speed	512 kbps

Available settings are explained as follows:

Item	Description
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.




IP Broadband Connection on Router Status

General

Internet Gateway

Status: Connected

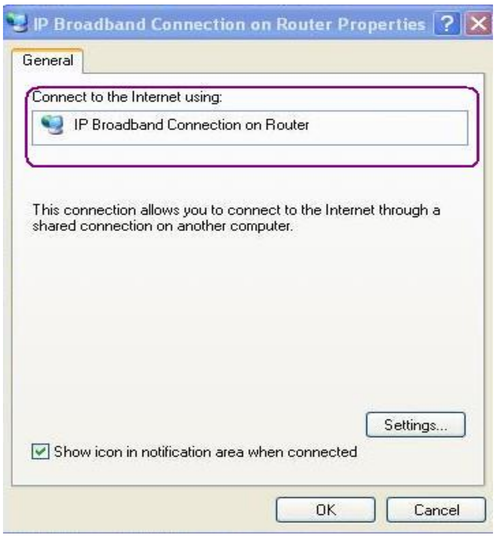
Duration: 00:19:06

Speed: 100.0 Mbps

Activity

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

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



IP Broadband Connection on Router Properties

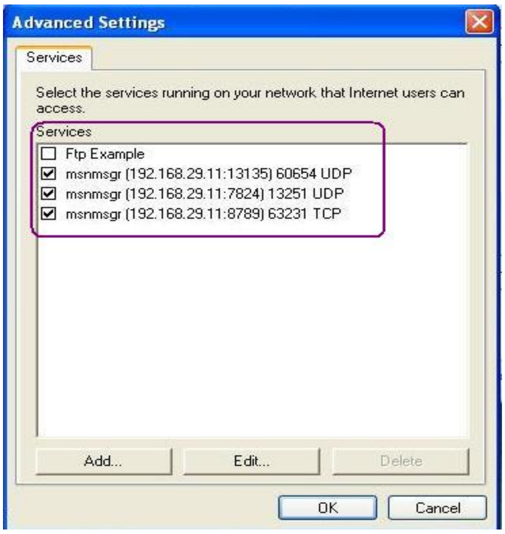
General

Connect to the Internet using:

IP Broadband Connection on Router

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

☑ Show icon in notification area when connected



Advanced Settings

Services

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

Services

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

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

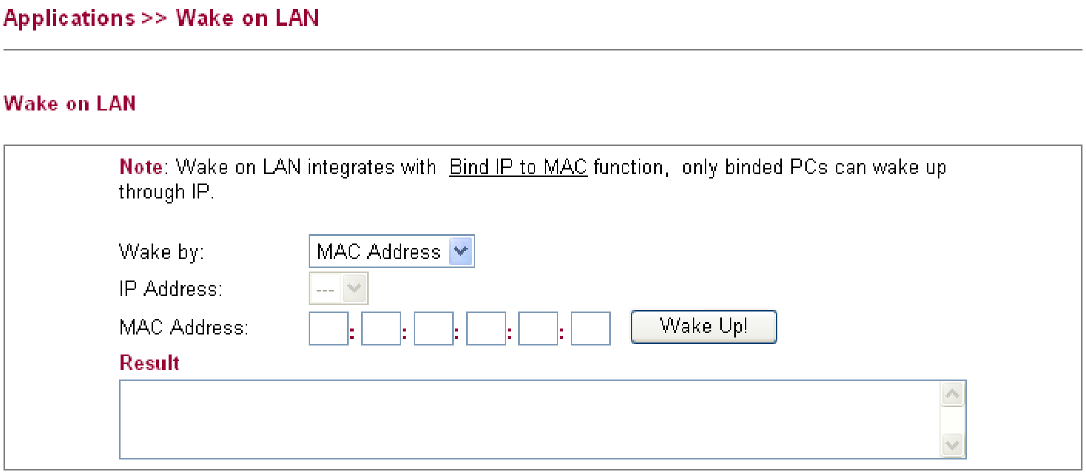
- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

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

4.7.6 Wake On LAN

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

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



Applications >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.

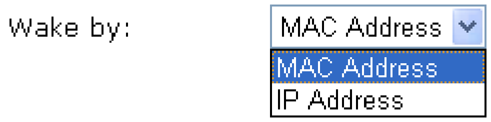
Wake by: MAC Address

IP Address: ---

MAC Address: __ : __ : __ : __ : __ : __

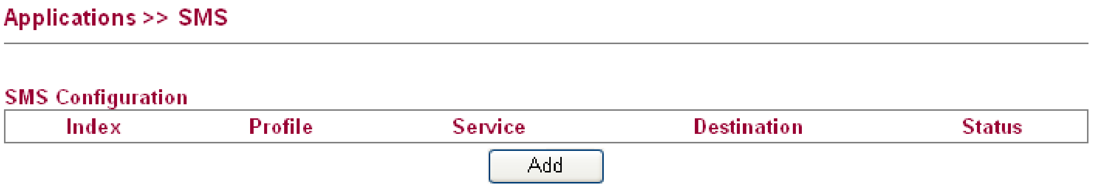
Result

Available settings are explained as follows:

Item	Description
Wake by	Two types provide for you to wake up the bond IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.  Wake by: MAC Address
IP Address	The IP addresses that have been configured in **LAN>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the bond PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

4.7.7 SMS

The router will send a SMS to the user for notification when something special happens. It can assist the user to know the abnormal situation of network connection.



Applications >> SMS

SMS Configuration

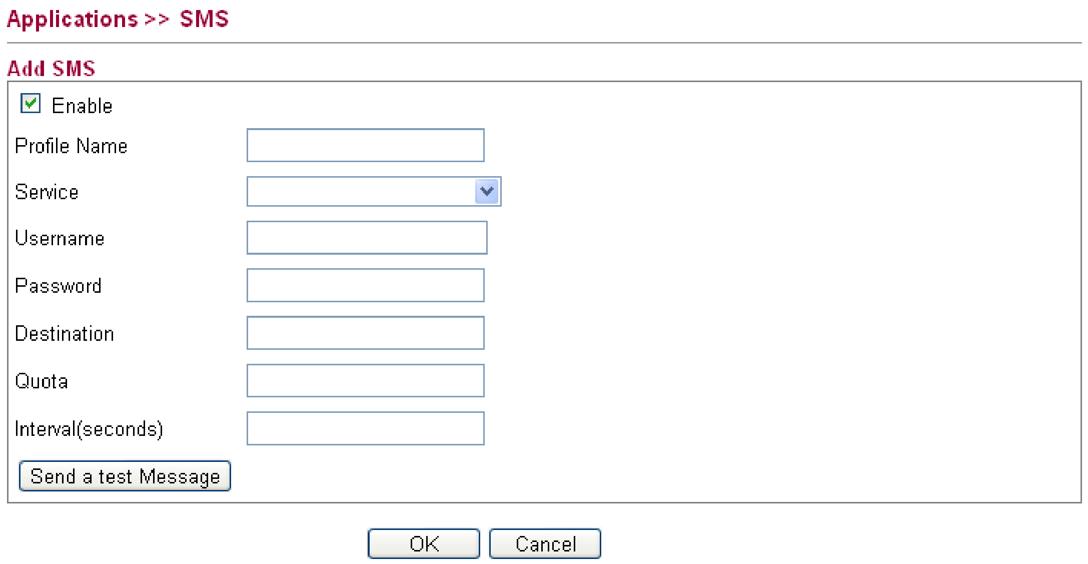
Index	Profile	Service	Destination	Status

Each item is explained as follows:

Item	Description
Index	Display the queue number of the profile.

Profile	Display the name of the profile.
Service	Display the Service Provider which supports SMS.
Destination	Display the telephone number of the user who will receive the SMS.
Status	Display if such service is enabled or disabled.
Add	It allows you to create a new profile.

Click **Add** to create a new SMS profile.



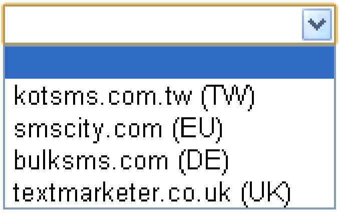
Applications >> SMS

Add SMS

☑ Enable

Profile Name	
Service	
Username	
Password	
Destination	
Quota	
Interval(seconds)	

Available settings are explained as follows:

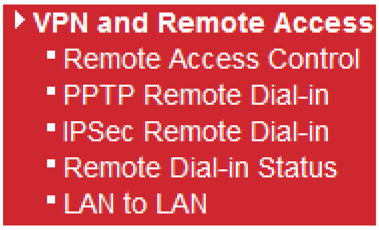
Item	Description
Enable	Check the box to enable this profile.
Profile Name	Type the name of the profile.
Service	Use the drop down list to choose the **Service Provider** that you apply for SMS  kotsms.com.tw (TW) smscity.com (EU) bulksms.com (DE) textmarketer.co.uk (UK)
Username	Type the account name which will be used for sending SMS.
Password	Type the password which will be used for sending SMS.
Destination	Type the telephone number of the user who will receive the SMS.
Quota	Type the total number of the messages that the router will send out in this field. The system will reduce the amount for each SMS sent out till out of the quota. Usually, SMS

	service should be charged. Such function can save the money of the user to avoid money waste. If there is no need to configure quota, simply type 0 in this field. Then, there is no limit for the amount of SMS sent.
Interval (seconds)	Type the shortest time interval for the system to send SMS. For example, it is set with 60 (seconds). If WAN1 disconnects for three times within 60 seconds, the system will send the SMS notification just for once.
Send a test message	Click this button to send one SMS to somebody just for test.

4.8 VPN and Remote Access

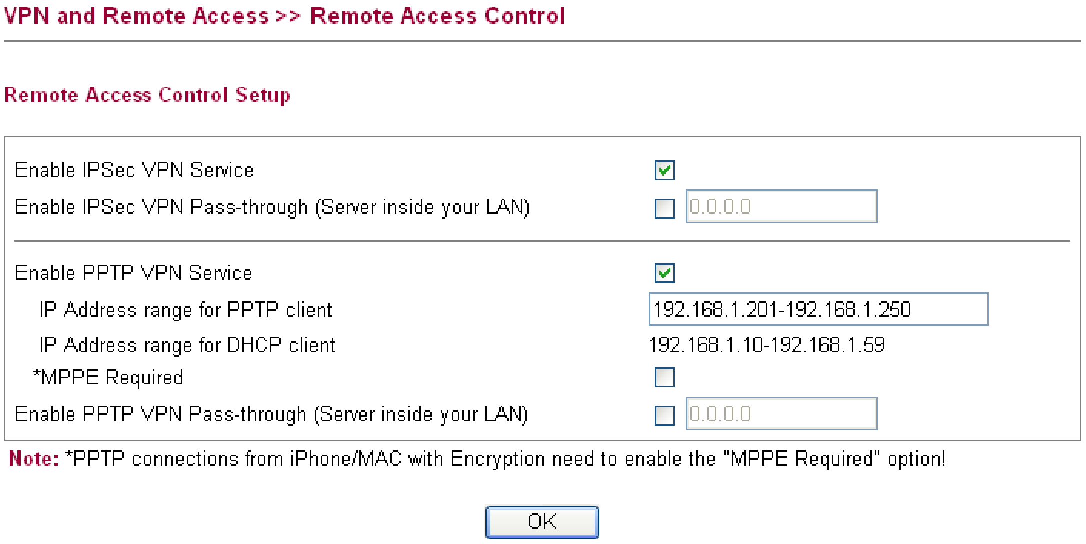
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



4.8.1 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

Enable IPSec VPN Service	☑
Enable IPSec VPN Pass-through (Server inside your LAN)	□ 0.0.0.0
Enable PPTP VPN Service	☑
IP Address range for PPTP client	192.168.1.201-192.168.1.250
IP Address range for DHCP client	192.168.1.10-192.168.1.59
*MPPE Required	□
Enable PPTP VPN Pass-through (Server inside your LAN)	□ 0.0.0.0

Note: *PPTP connections from iPhone/MAC with Encryption need to enable the "MPPE Required" option!

Available settings are explained as follows:

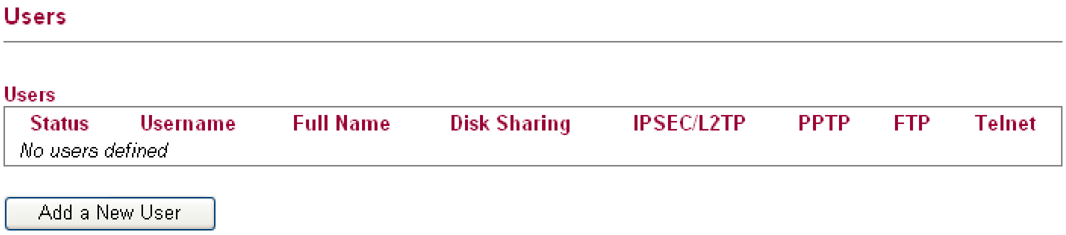
Item	Description

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 (Server inside your LAN)	If this checkbox is checked, the system 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.
	IP Address range for PPTP client – Specify an IP address pool for the local private network that will be assigned to PPTP clients. Note the values given here should not be the same as **IP address range for DHCP Client**. **IP Address range for DHCP client** – Display the range of IP address assigned by DHCP server. **MPPE** – Check this box to encrypt data transmission via PPTP connection.
Enable PPTP VPN Pass-through (Server inside your LAN)	If this checkbox is checked, the system firewall will pass VPN (PPTP) remote access from WAN side to a VPN server in the LAN. Type the IP address of the VPN server in the field next to the checkbox.

4.8.2 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

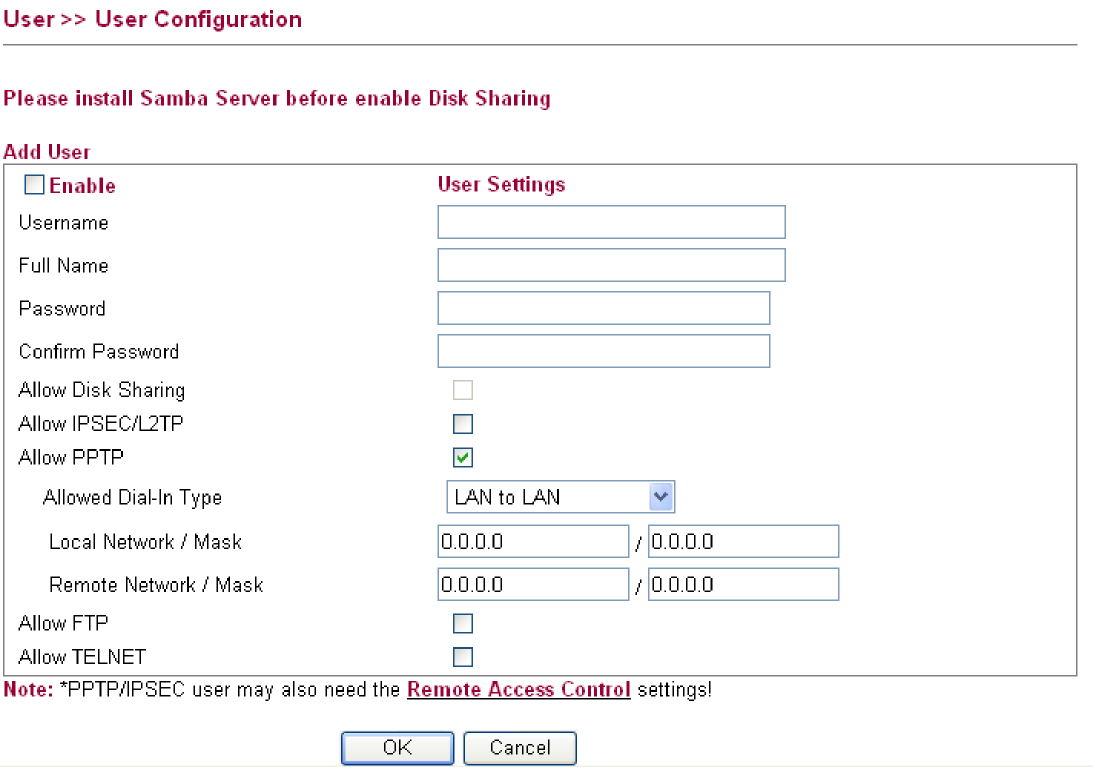
Users

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

Note: This page is similar to the page under **User>>User Configuration.**

Adding a New User

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



User >> User Configuration

Please install Samba Server before enable Disk Sharing

Add User

□ Enable	User Settings
Username	
Full Name	
Password	
Confirm Password	
Allow Disk Sharing	□
Allow IPSEC/L2TP	□
Allow PPTP	☑
Allowed Dial-In Type	LAN to LAN
Local Network / Mask	0.0.0.0 / 0.0.0.0
Remote Network / Mask	0.0.0.0 / 0.0.0.0
Allow FTP	□
Allow TELNET	□

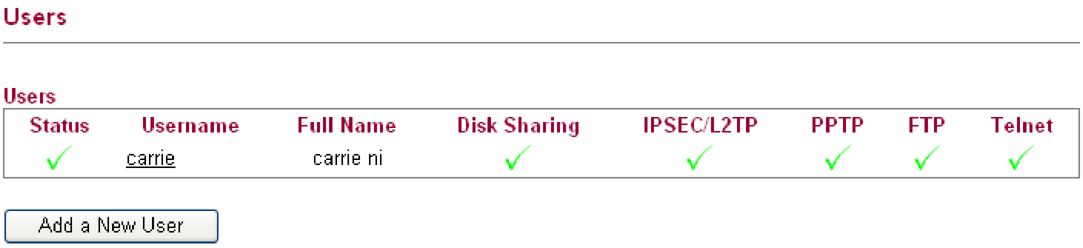
Note: *PPTP/IPSEC user may also need the Remote Access Control settings!

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such user profile.
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**.** When such user profile needs to have PPTP LAN to LAN connection, the following items must be adjusted. **Allowed Dial-In Type** – Specify which dial-in type will be used for PPTP connection. **Assign Static IP Address** – If you choose Remote Dial-in Client as Allowed Dial-In type, you can assign a fixed IP address. **Local Network/Mask** – If you choose LAN to LAN as Allowed Dial-In Type, you have to type the IP address as

	local network / mask. **Remote Network/Mask** – If you choose LAN to LAN as Allowed Dial-In Type, you have to type the IP address as remote network /mask.
Allow FTP	Check this box to let the remote user connecting to FTP server via this router.
Allow TELNET	Check this box to let the remote user to adjust the settings of router by TELNET.

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



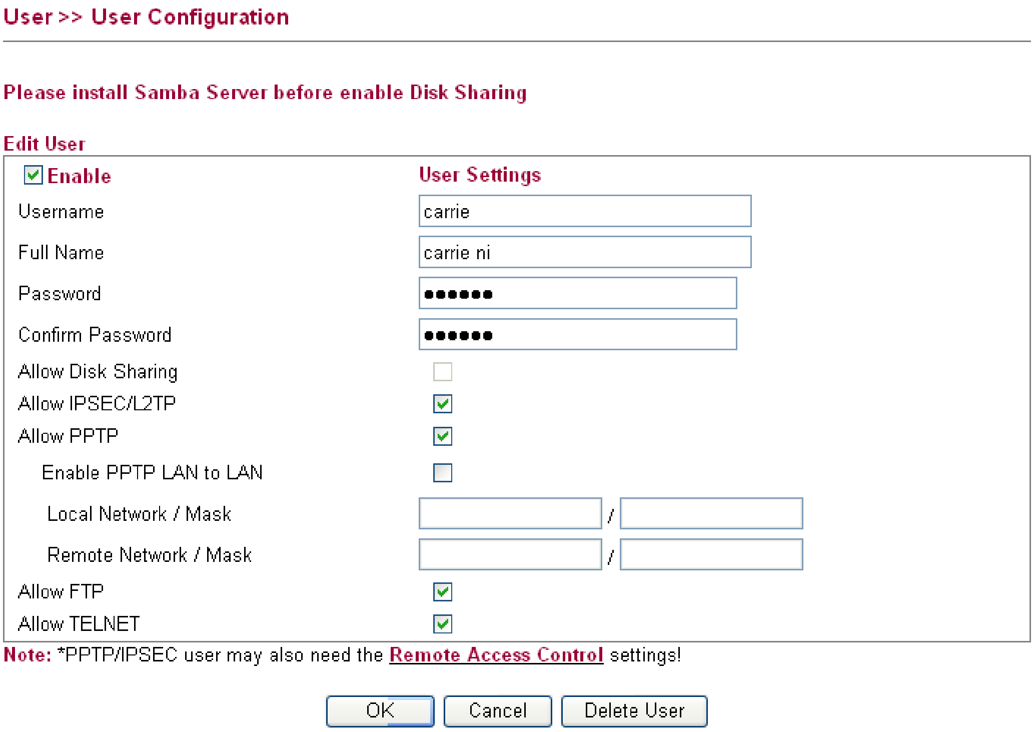
Users

Users

Status	Username	Full Name	Disk Sharing	IPSEC/L2TP	PPTP	FTP	Telnet
✓	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 >> User Configuration

Please install Samba Server before enable Disk Sharing

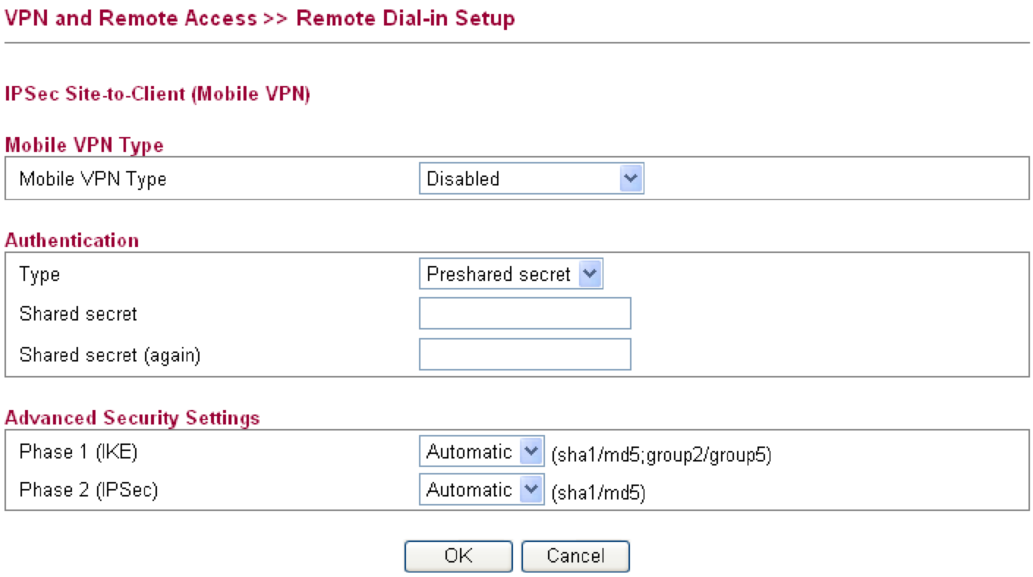
Edit User

☑ Enable	User Settings
Username	carrie
Full Name	carrie ni
Password	••••••
Confirm Password	••••••
Allow Disk Sharing	□
Allow IPSEC/L2TP	☑
Allow PPTP	☑
Enable PPTP LAN to LAN	□
Local Network / Mask	/
Remote Network / Mask	/
Allow FTP	☑
Allow TELNET	☑

Note: *PPTP/IPSEC user may also need the Remote Access Control settings!

4.8.3 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

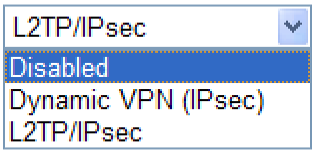
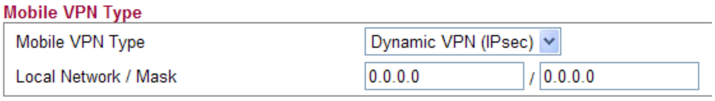
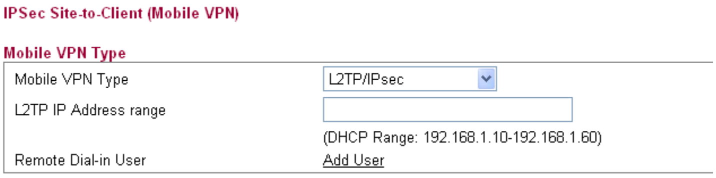
Authentication

Type	Preshared secret
Shared secret	
Shared secret (again)	

Advanced Security Settings

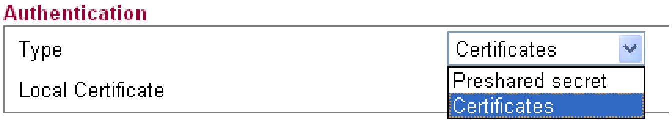
Phase 1 (IKE)	Automatic (sha1/md5;group2/group5)
Phase 2 (IPSec)	Automatic (sha1/md5)

Available settings are explained as follows:

Item	Description
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.  L2TP/IPsec Disabled Dynamic VPN (IPsec) L2TP/IPsec **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.  IPSec Site-to-Client (Mobile VPN) Mobile VPN Type Mobile VPN Type: L2TP/IPsec L2TP IP Address range: (DHCP Range: 192.168.1.10-192.168.1.60) Remote Dial-in User: Add User

Authentication

Type – There are two types for you to choose for authentication.

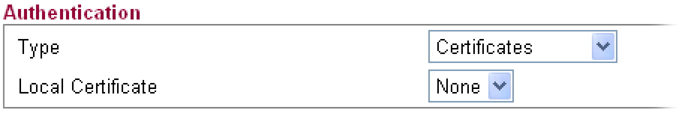


Authentication

Type: Certificates

Local Certificate

If you choose **Certificate** as the **Type**, you have to specify one of the local certificates.

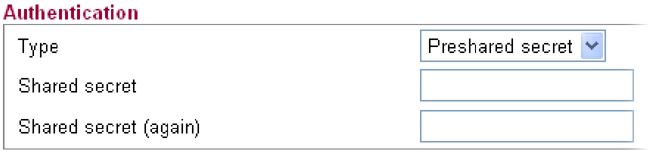


Authentication

Type: Certificates

Local Certificate: None

If you choose **Pre-Shared Secret** as the **Type**, you have to type and confirm the shared secret. IPSec remote dial-in clients will use the given secret.



Authentication

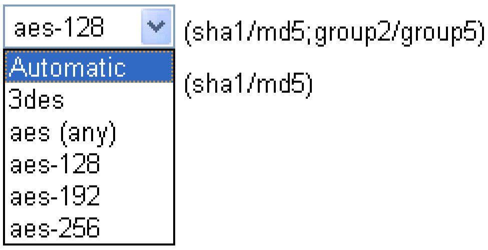
Type: Preshared secret

Shared secret

Shared secret (again)

Advanced Settings

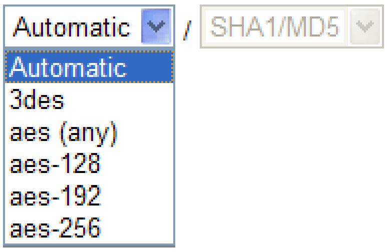
Phase 1 (IKE) - Negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its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



aes-128 (sha1/md5;group2/group5)

(sha1/md5)

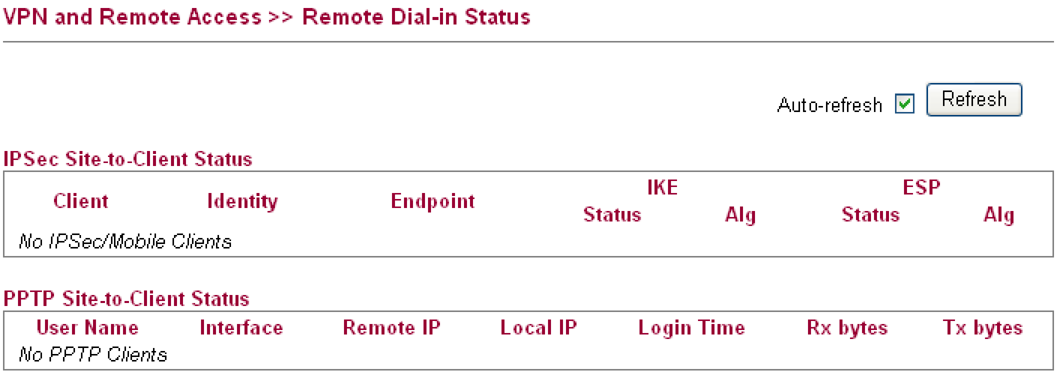
Phase 2 (IPSec) - Negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.



Automatic / SHA1/MD5

4.8.4 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 Status	IKE Alg	ESP Status	ESP Alg
No IPSec/Mobile Clients						

PPTP Site-to-Client Status

User Name	Interface	Remote IP	Local IP	Login Time	Rx bytes	Tx bytes
No PPTP Clients						

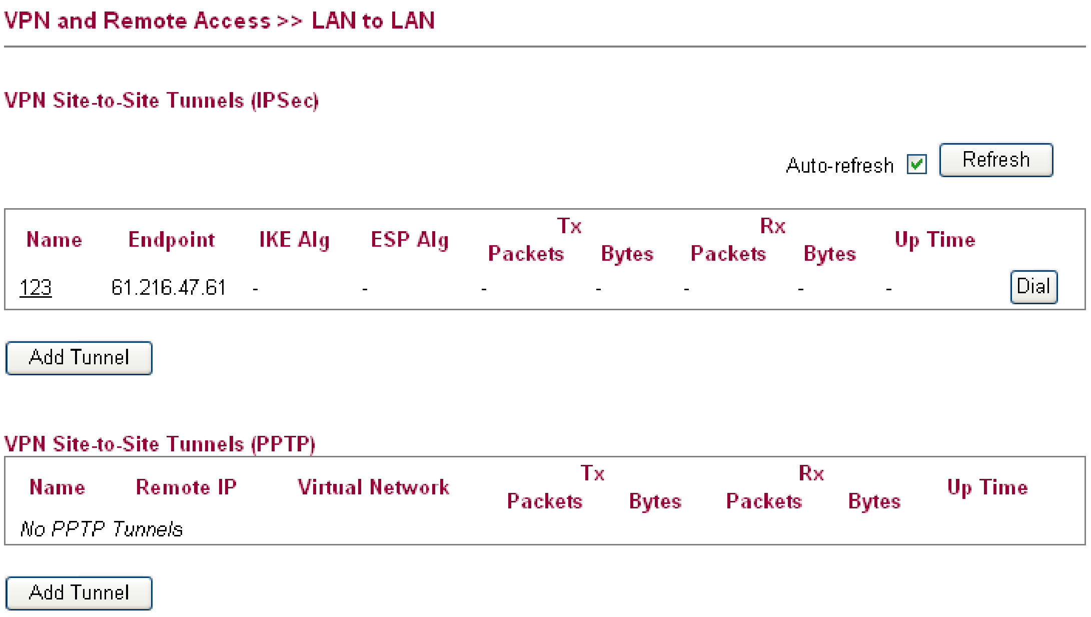
Available settings are explained as follows:

Item	Description
Auto-refresh	Check this box to make the system refresh this page automatically.
Refresh	Click this button to refresh the page immediately.
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.
Local IP	Display the given local IP address of a 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.

4.8.5 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 peer ID, connection type and corresponding security methods, etc.

The router supports two VPN tunnels for IPSec and PPTP by providing 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 Alg	ESP Alg	Tx		Rx		Up Time	
				Packets	Bytes	Packets	Bytes		
123	61.216.47.61	-	-	-	-	-	-	-	Dial

Add Tunnel

VPN Site-to-Site Tunnels (PPTP)

Name	Remote IP	Virtual Network	Tx		Rx		Up Time
			Packets	Bytes	Packets	Bytes	
No PPTP Tunnels							

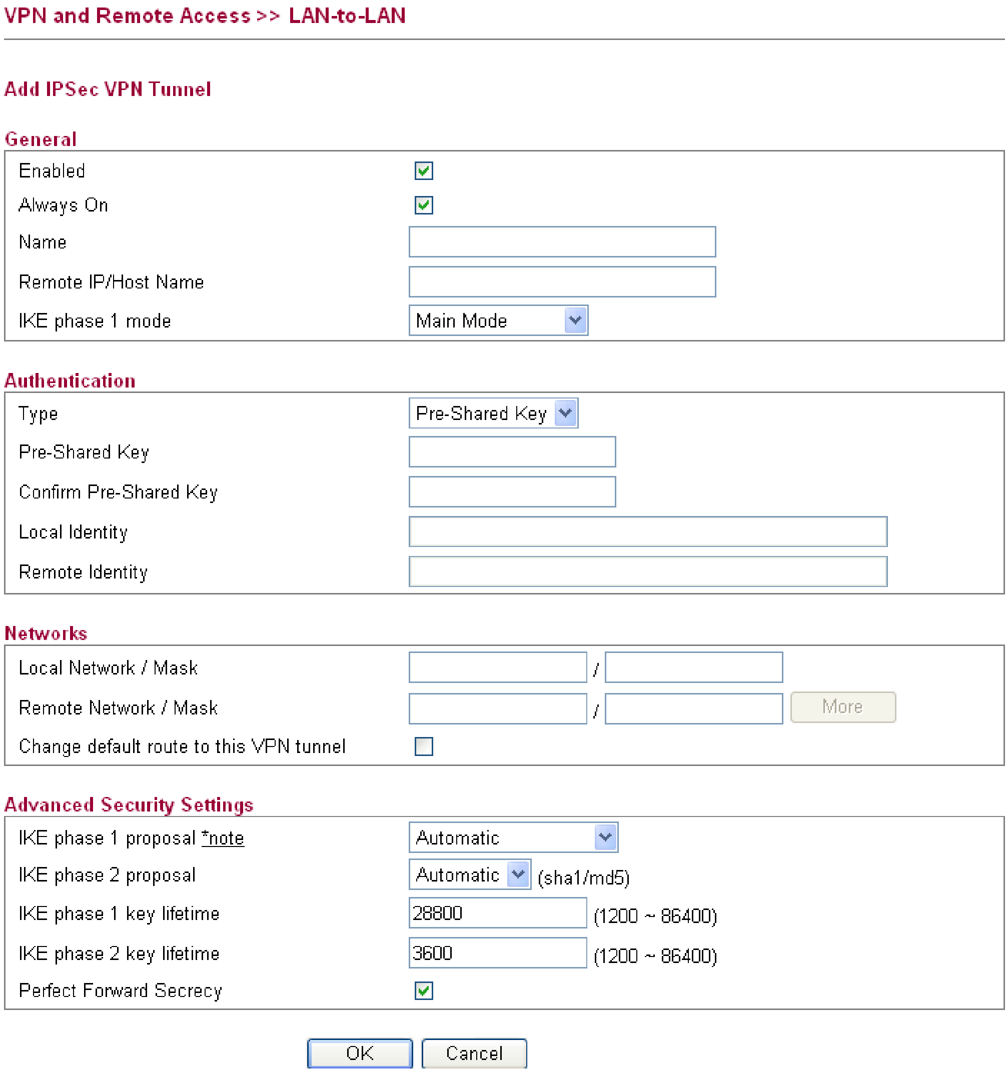
Add Tunnel

Available settings are explained as follows:

Item	Description
Auto-refresh	Check this box to make the system refresh this page automatically.
Refresh	Click this button to refresh the page immediately.
Name	Indicate the name of the LAN-to-LAN profile.
Endpoint	Display the IP address of the VPN client.
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 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.
Tx Packets / Tx Bytes	Display the data transmission packets / bytes through VPN tunnel (by IPSec or PPTP).
Rx Packets / Rx Bytes	Display the data receiving packets / bytes through VPN tunnel (by IPSec or PPTP).
Up Time	Display the duration time of the IPSec / PPTP connection.
Add Tunnel	Click it to add a new VPN tunnel via IPSec / PPTP protocol.

Adding a VPN Tunnel for IPSec

Click **Add Tunnel** to open the following page.



VPN and Remote Access >> LAN-to-LAN

Add IPSec VPN Tunnel

General

Enabled	☑
Always On	☑
Name	
Remote IP/Host Name	
IKE phase 1 mode	Main Mode

Authentication

Type	Pre-Shared Key
Pre-Shared Key	
Confirm Pre-Shared Key	
Local Identity	
Remote Identity	

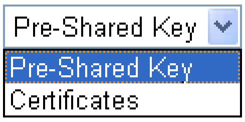
Networks

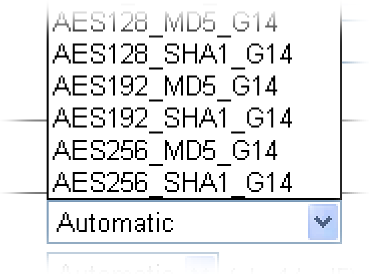
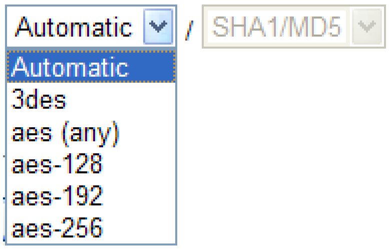
Local Network / Mask	/
Remote Network / Mask	/ More
Change default route to this VPN tunnel	□

Advanced Security Settings

IKE phase 1 proposal *note	Automatic
IKE phase 2 proposal	Automatic (sha1/md5)
IKE phase 1 key lifetime	28800 (1200 ~ 86400)
IKE phase 2 key lifetime	3600 (1200 ~ 86400)
Perfect Forward Secrecy	☑

Available settings are explained as follows:

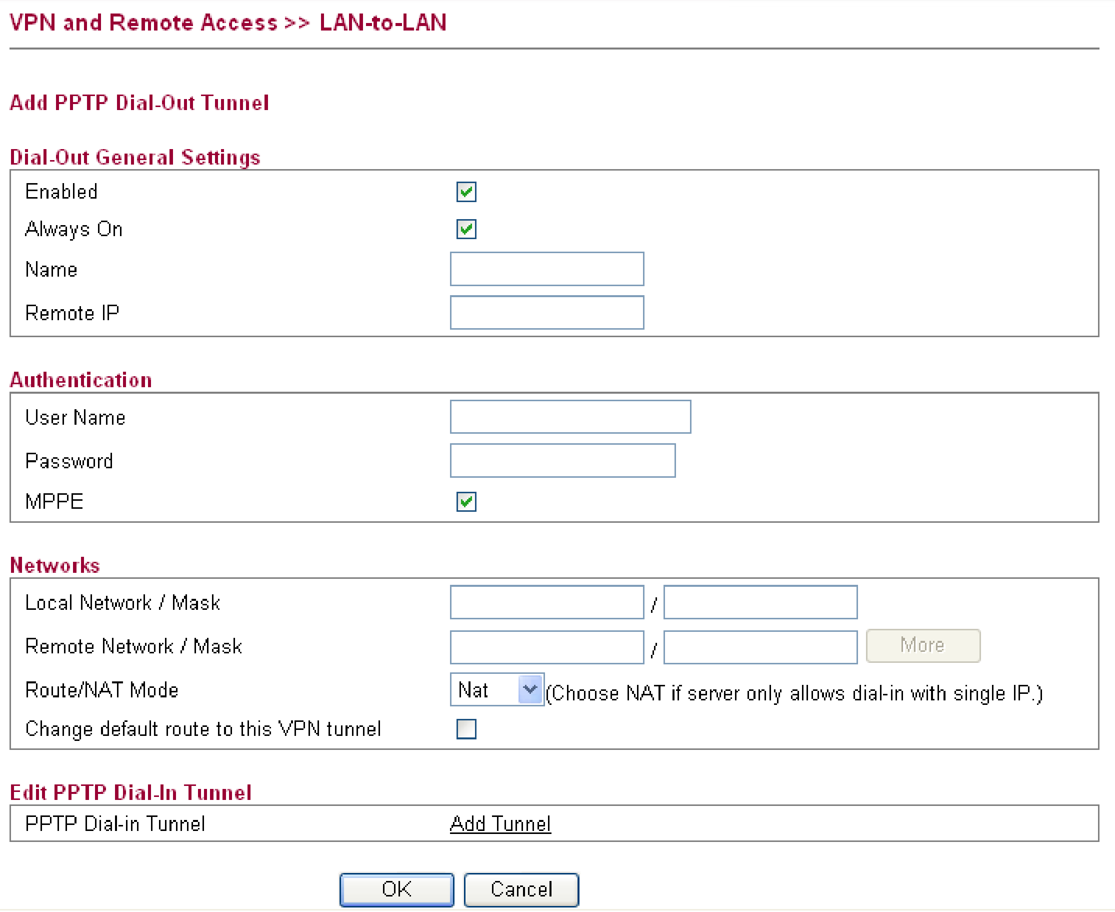
Item	Description
General	**Enabled** - Check here to activate this tunnel. **Always On** - Check this box to make the WAN connection being activated always. **Name** - Specify a name for this tunnel. **Remote IP/Host Name** - Enter the IP address/FQDN of the remote host that located at the other-end 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
Authentication	**Type** - There are two types for you to choose for authentication.  **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 Certificate** - If you choose **Certificate** as the **Type**, you have to specify one of the local certificates.
Network	**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. **Change default route to this VPN tunnel –** Check the

	box to change the default route to this configured VPN tunnel.
Advanced Security Settings	**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.  AES128_MD5_G14 AES128_SHA1_G14 AES192_MD5_G14 AES192_SHA1_G14 AES256_MD5_G14 AES256_SHA1_G14 Automatic **IKE Phase 2 proposal** - Propose the local available algorithms to the VPN peers, and get its feedback to find a match.  Automatic / SHA1/MD5 Automatic 3des aes (any) aes-128 aes-192 aes-256 **IKE phase 1 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. **Perfect Forward Secrecy** - The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

Click **OK** to save the settings.

Adding a VPN Tunnel for PPTP

Click **Add Tunnel** to open the following page.



VPN and Remote Access >> LAN-to-LAN

Add PPTP Dial-Out Tunnel

Dial-Out General Settings

Enabled	☑
Always On	☑
Name	
Remote IP	

Authentication

User Name	
Password	
MPPE	☑

Networks

Local Network / Mask	/
Remote Network / Mask	/ More
Route/NAT Mode	Nat (Choose NAT if server only allows dial-in with single IP.)
Change default route to this VPN tunnel	□

Edit PPTP Dial-In Tunnel

PPTP Dial-in Tunnel	Add Tunnel

Available settings are explained as follows:

Item	Description
Dial-Out General Setting	**Enabled -** Check here to activate this tunnel. **Always On -** Check this box to make the WAN connection being activated always. **Name** - Specify a name for this tunnel. **Remote IP** - Enter the IP address/name of the remote host that located at the other-end of the VPN tunnel.
Authentication	**User Name** - Type a name for this tunnel for authentication. **Password** - Type a password for this tunnel for authentication. **MPPE** - Check this box to enable the function of MPPE for such tunnel.
Networks	**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. **Route/NAT Mode** - If the remote network only allows you to dial in with single IP, please choose NAT Mode, otherwise please choose Route Mode. **Change default route to this VPN tunnel** - Check this box to change the default route into such VPN tunnel.
Edit PPTP Dial-in Tunnel	**PPTP Dial-In Tunnel** - If it is required, click **Add Tunnel** link to access into **VPN and Remote Access>>PPTP Remote Dial-in** page for adding other dial-in tunnel. Refer to the section 4.8.2 for detailed information.

Click **OK** to save the settings.

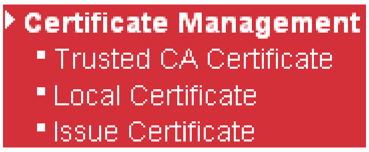
4.9 Certificate Management

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

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

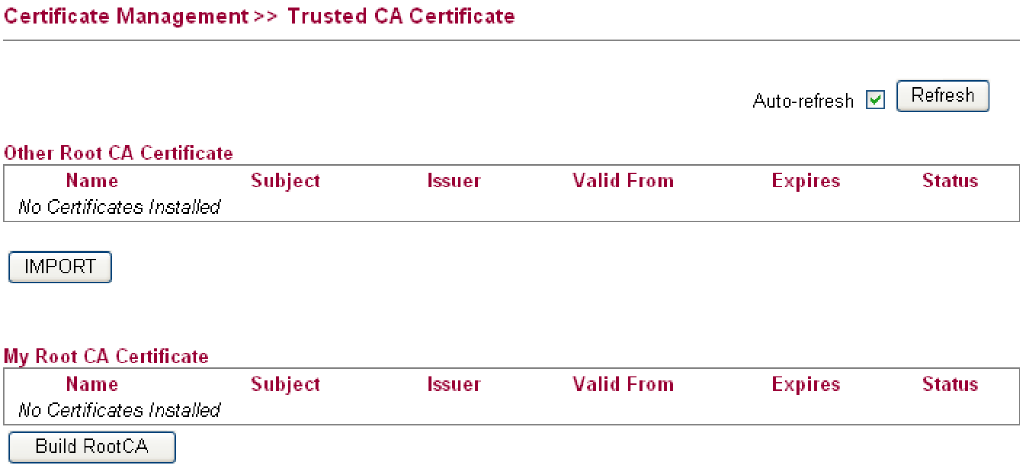


4.9.1 Trusted CA Certificate

The CA (certification authority) certificate specified in this page is the issuer of the certificates for both clients requesting for network connection.

It allows you to import the third-party certificate authenticated by other certification authority (CA), or build My RootCA to be used as a CA for signing the local certicate.

Just create a new Trust CA Certificate first.



Certificate Management >> Trusted CA Certificate

Auto-refresh ☑ Refresh

Other Root CA Certificate

Name	Subject	Issuer	Valid From	Expires	Status
No Certificates Installed					

IMPORT

My Root CA Certificate

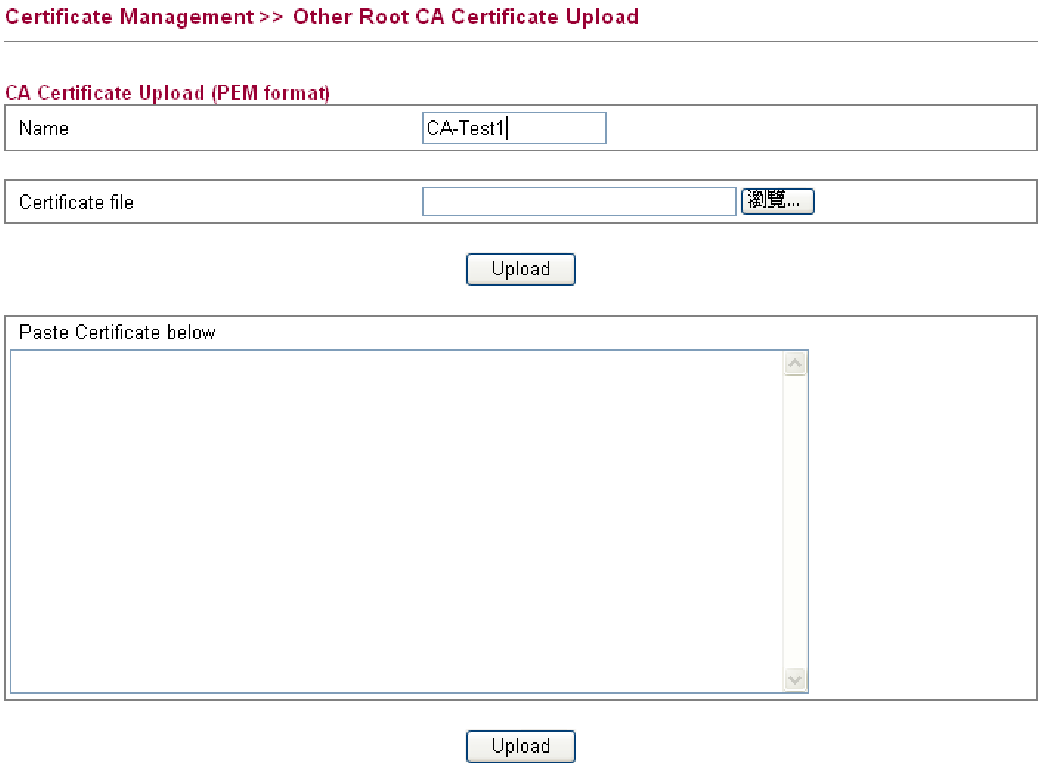
Name	Subject	Issuer	Valid From	Expires	Status
No Certificates Installed					

Build RootCA

Available settings are explained as follows:

Item	Description
Other Root CA Certificate	You can **import** several Root CA certificates to meet different requests. **Name** – Display the name of the certificate. **Subject –** Display a brief description for the content of the certificate. **Issuer** - Display the name of the issuer**.** **Valid From** - Display the starting time for the valid Root CA. **Expires** - Display the ending time for the valid Root CA. **Status** - Display if such certificate is active or not. **IMPORT** - Allow to import existed certificate from other CA.
My Root CA Certificate	You can create **one** Root CA certificates to meet different requests. **Name** – Display the name of the certificate. **Subject –** Display a brief description for the content of the certificate. **Issuer** - Display the name of the issuer**.** **Valid From** - Display the starting time for the valid Root CA. **Expires** - Display the ending time for the valid Root CA. **Status** - Display if such certificate is **Active** or not. **Build RootCA** - Allow to build user-defined Root CA certificate.

You can import other Root CA certificates made by others and ***upload to Vigor router*** as CA. Simply click **IMPORT** to access into the following page.



Certificate Management >> Other Root CA Certificate Upload

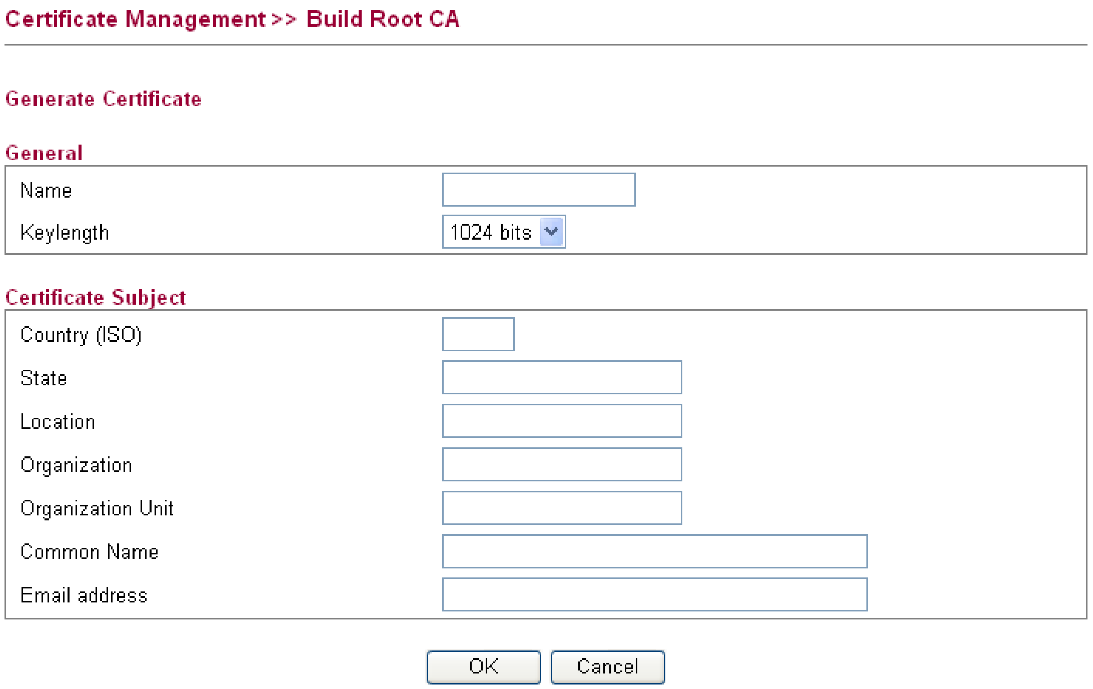
CA Certificate Upload (PEM format)

Name: CA-Test1

Available settings are explained as follows:

Item	**Description**
Name	Type a new name for such certificate.
Certificate file	Use the **Browse.**. button to specify the file. **Upload** - After choosing the certificate file above, click this button to upload onto the router.
Paste Certificate below	You many paste the information of the certificate from other files. After pasting the data in this field, simply click Upload below. The related data will be uploaded onto the router. **Upload** – After pasting the information, click it to upload the CA data coming from the third-party to Vigor router.

If you want to create your Root CA certificate for the router adopting for issuing local certificate and certificate request from the remote client, simply click **Build RootCA** to access into the following page.



Certificate Management >> Build Root CA

Generate Certificate

General

Name	
Keylength	1024 bits

Certificate Subject

Country (ISO)	
State	
Location	
Organization	
Organization Unit	
Common Name	
Email address	

Available settings are explained as follows:

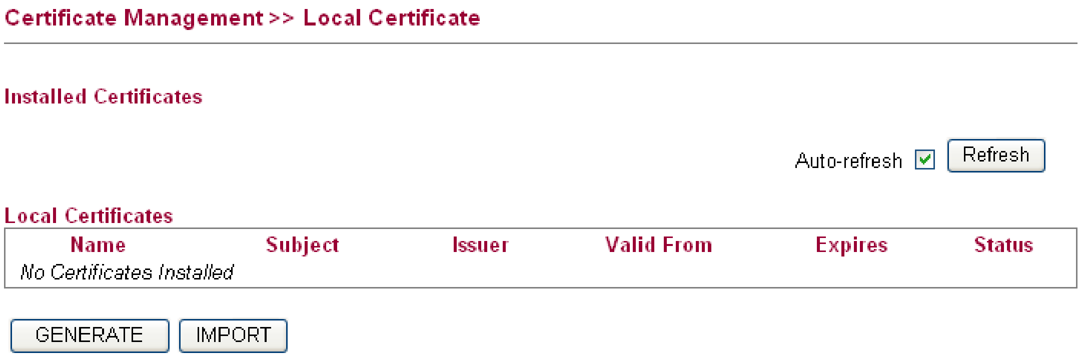
Item	Description
General	**Name** - Type a new name for such certificate. **Keylength** - Specify the length of the certificate.
Certificate Subject	**Country (ISO)** - Type the abbreviation of your country in this field. **State** - Type the state that you live. **Location** - Give a brief description your location. **Organization** - Type the name of your company. **Organization Unit** - Type the department or unit for your company. **Common Name** - Type a common name for such certificate. **Email address** - Type an email address for the system to send any information for you.

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

4.9.2 Local Certificate

This page displays the certificate which will be authenticated for network connection. Note that it must be issued by Trusted CA Certificate first.

You have to generate a local certificate to be signed by trusted CA (no matter My Root CA or other Root CA). After that, import the signed certificate to this page.



Certificate Management >> Local Certificate

Installed Certificates

Auto-refresh ☑ Refresh

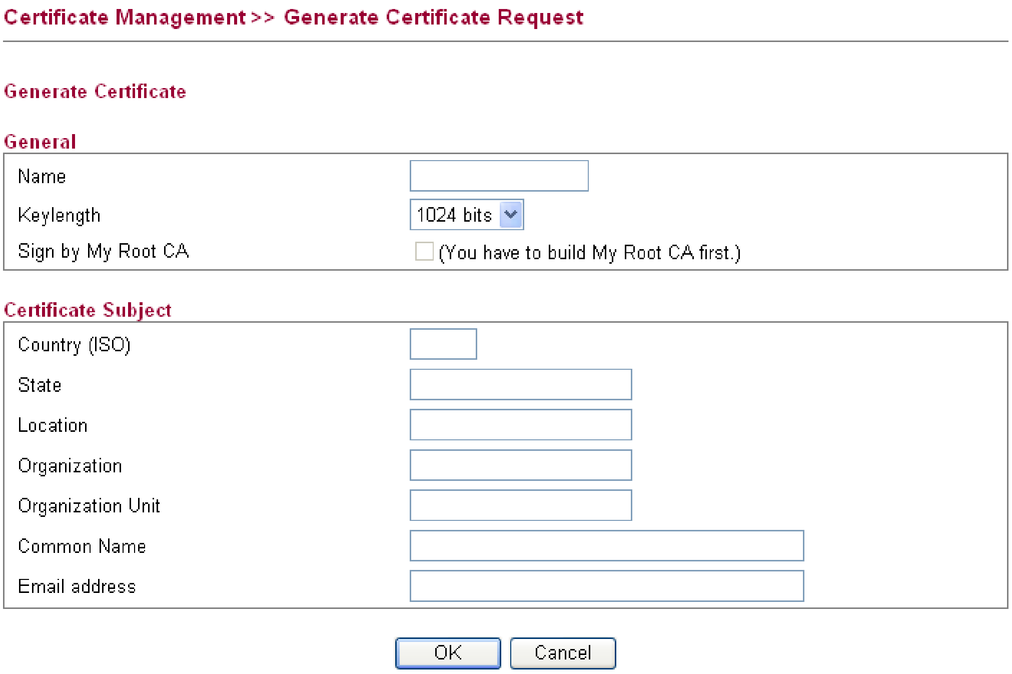
Local Certificates

Name	Subject	Issuer	Valid From	Expires	Status
No Certificates Installed					

Available settings are explained as follows:

Item	Description
Auto-refresh	Click the button to refresh current page automatically.
Refresh	Click the button to refresh current page whenever you want.
Name	Display the name of the certificate.
Subject	Display the subject information.
Issuer	Display the name of the issuer**.**
Valid From	Display the starting time for the valid Root CA.
Expires	Display the ending time for the valid Root CA.
Status	Display if such certificate is **Active** (illegal and available certificate) or **Requesting** (needed to be signed by CA).
GENERATE	Allows you to create a new local certificate and local certificate request. Later, it can be issued by Trusted CA. Next, import the issued information in this page to be the local certificate for network connection.
IMPORT	Allows you to import a certificate which has been issued by Trusted CA Certificate.

Click **GENERATE** to open the following page:



Certificate Management >> Generate Certificate Request

Generate Certificate

General

Name	
Keylength	1024 bits
Sign by My Root CA	□ (You have to build My Root CA first.)

Certificate Subject

Country (ISO)	
State	
Location	
Organization	
Organization Unit	
Common Name	
Email address	

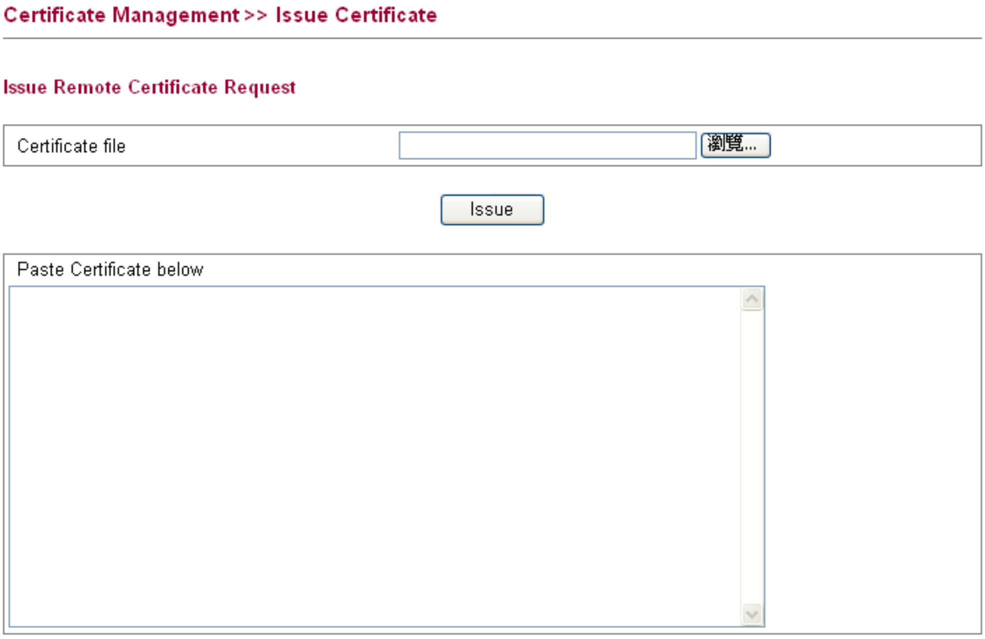
Available settings are explained as follows:

Item	Description
General	**Name** - Type a new name for such certificate. **Keylength** - Specify the length of the certificate. **Sign by My Root CA** – If you have created a Root CA for yourself, the check box will be available for you to activate. If you do not check the box, then such local certificate might be signed by other Root CA in default.
Certificate Subject	**Country (ISO)** - Type the abbreviation of your country in this field. **State** - Type the state that you live. **Location** - Give a brief description your location. **Organization** - Type the name of your company. **Organization Unit** - Type the department or unit for your company. **Common Name** - Type a common name. **Email address** - Type an email address for the system to send any information for you.

Click **OK** to save the settings and return to previous page.

4.9.3 Issue Certificate

Vigor router can be used as a Root CA to authenticate and issue the certificates request coming from other clients.



Certificate Management >> Issue Certificate

Issue Remote Certificate Request

vailable settings are explained as follows:

Item	Description
Certificate file	Use the **Browse.**. button to specify the file. **Issue -** After choosing the certificate file above, click this button to issue the certificate.
Paste Certificate below	You many paste the information of the certificate from other files. After pasting the data in this field, simply click **Issue** above.

4.10 Wireless LAN

This function is used for "n" models.

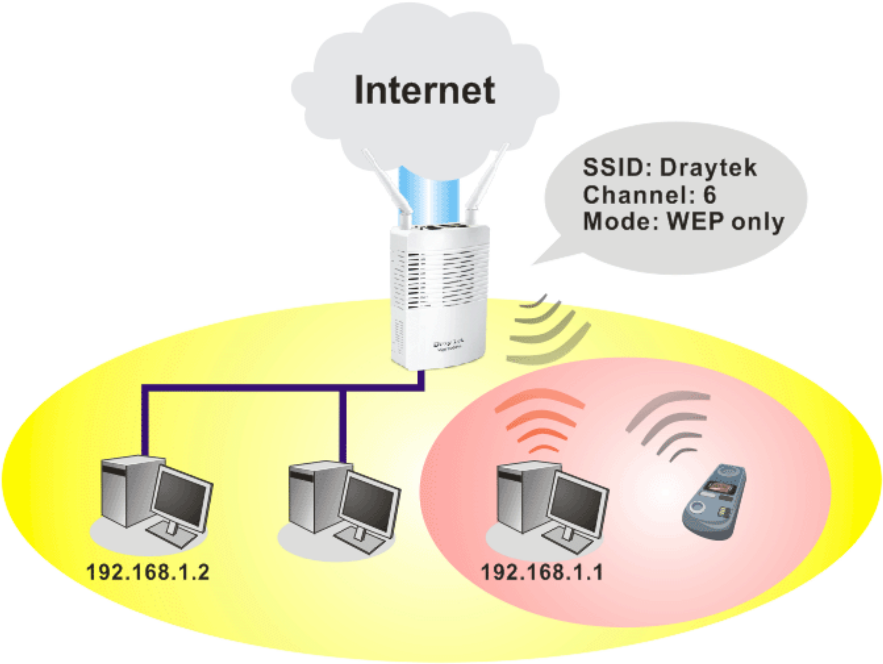
4.10.1 Basic Concepts

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.

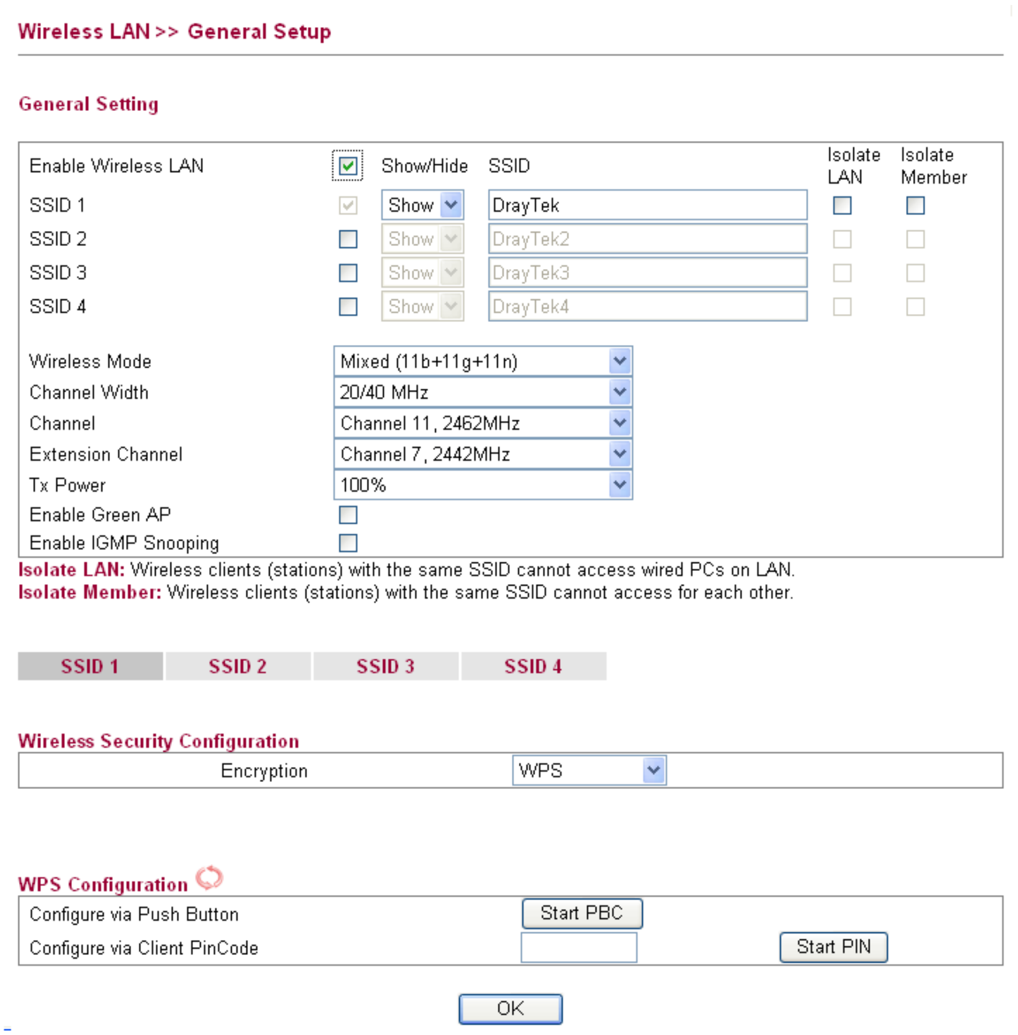
Below shows the menu items for Wireless LAN.

Wireless LAN
- General Setup
- Access Control
- Station List
- Access Point Discovery
- WMM Configuration
- WDS

4.10.2 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	☑	Show/Hide	SSID	Isolate LAN	Isolate Member
SSID 1	☑	Show	DrayTek	□	□
SSID 2	□	Show	DrayTek2	□	□
SSID 3	□	Show	DrayTek3	□	□
SSID 4	□	Show	DrayTek4	□	□

Wireless Mode	Mixed (11b+11g+11n)
Channel Width	20/40 MHz
Channel	Channel 11, 2462MHz
Extension Channel	Channel 7, 2442MHz
Tx Power	100%
Enable Green AP	□
Enable IGMP Snooping	□

Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

Wireless Security Configuration

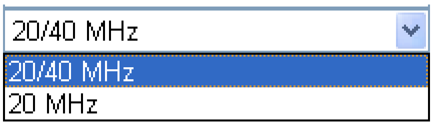
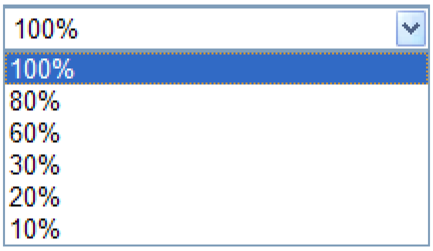
Encryption	WPS

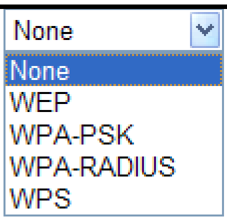
WPS Configuration

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

Available settings are explained as follows:

Item	Description
General Setting	**Enable Wireless LAN -** Check the box to enable the wireless function. **Show/Hide-** Choose **Show** to make the SSID being seen by wireless clients. Choose **Hide** to prevent from wireless sniffing and make it

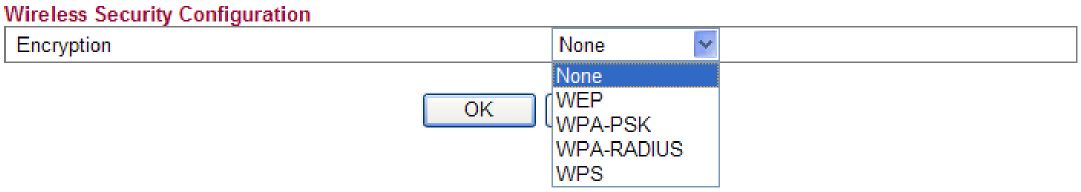
	harder for unauthorized clients or STAs to join your wireless LAN. **SSID-** It means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it. **Isolate LAN-** Check this box to make the wireless clients (stations) not accessing the PC with wired connection. **Isolate Member-** Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. **Wireless Mode-** Choose the wireless mode for this router. At present, only 802.11B/B/N mix is available. **Channel Width-20/40 –** the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transmission. **20 -** the router will use 20Mhz for data transmitting and receiving between the AP and the stations.  **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. **Extension Channel-** Such channel will be brought out automatically when you determine the **Channel** selection. It can help to extend the bandwidth for wireless connection. Such value can be modified manually. **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. **Enable IGMP Snooping-** Check it to enable IGMP snooping for WLAN client.
Wireless Security Configuration	**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.

Click **OK** to save the settings.

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

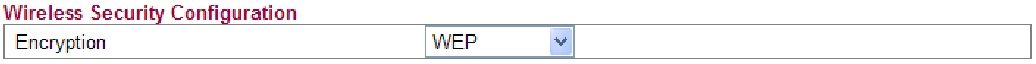
Encryption: None

- **None**

  The encryption mechanism is turned off.

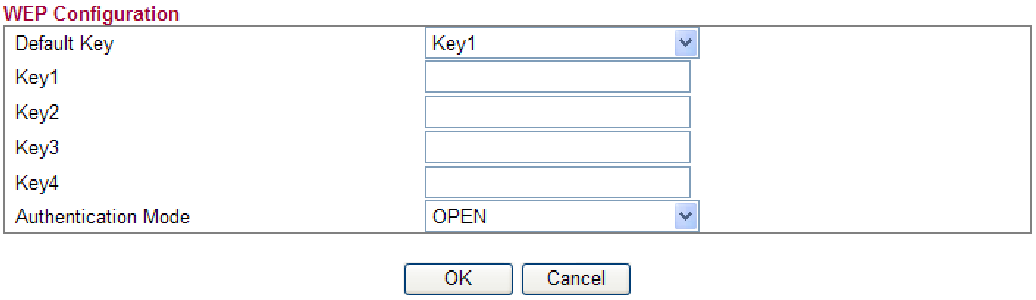
- **WEP**

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



Wireless Security Configuration

Encryption: WEP



WEP Configuration

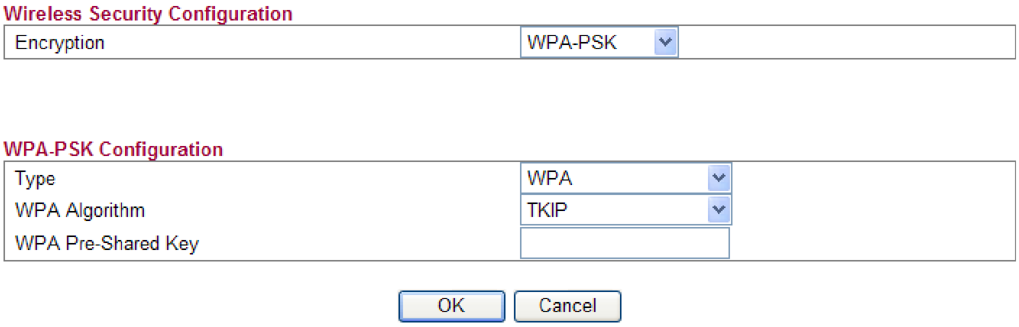
Default Key	Key1
Key1	
Key2	
Key3	
Key4	
Authentication Mode	OPEN

Available settings are explained as follows:

Item	Description
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.



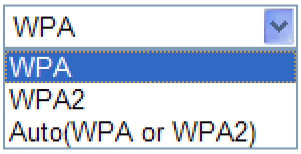
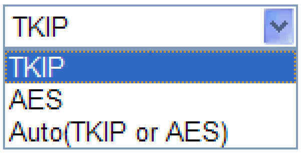
Wireless Security Configuration

Encryption	WPA-PSK

WPA-PSK Configuration

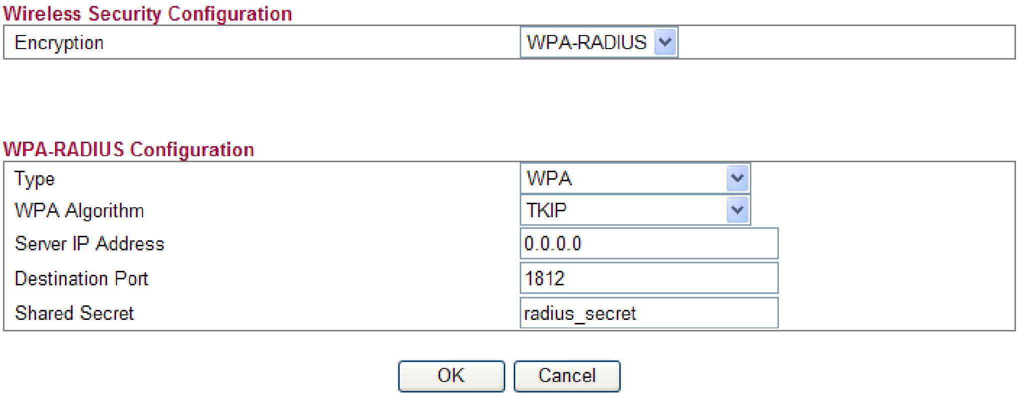
Type	WPA
WPA Algorithm	TKIP
WPA Pre-Shared Key	

Available settings are explained as follows:

Item	Description
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

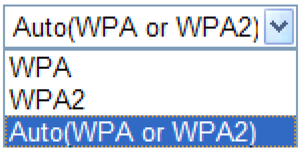
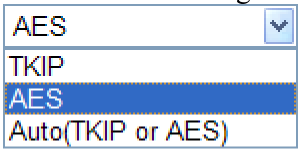
Encryption	WPA-RADIUS

WPA-RADIUS Configuration

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

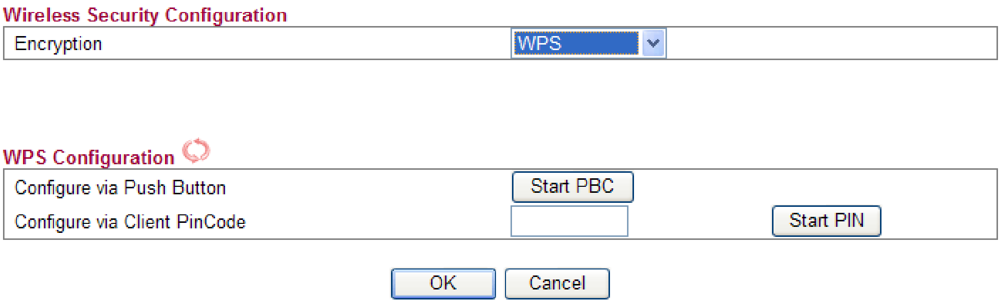
Available settings are explained as follows:

Item	Description
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

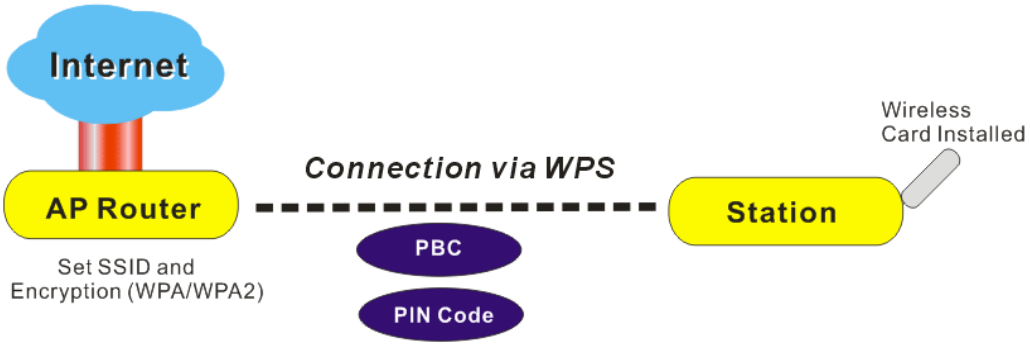
Configure via Push Button

Configure via Client PinCode

Available settings are explained as follows:

Item	Description
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.

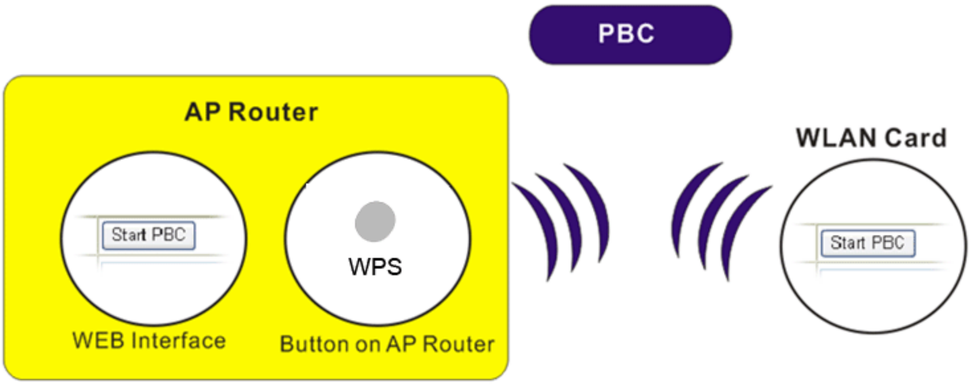
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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



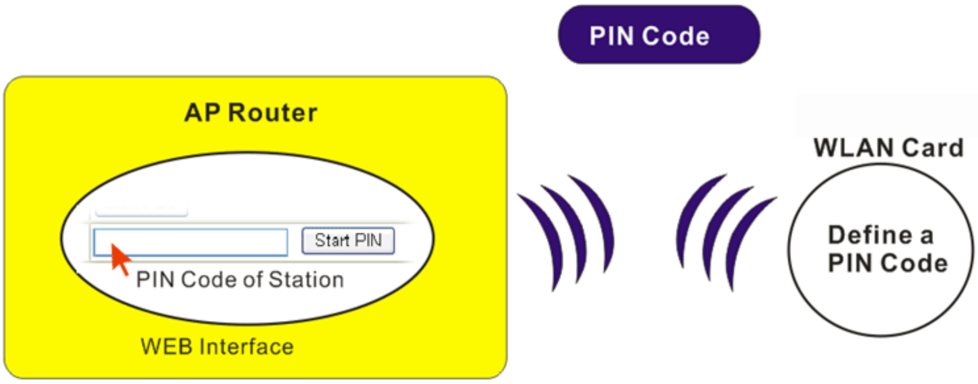
Note: Such function is available for the wireless station with WPS supported.

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 Vigor1000 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.

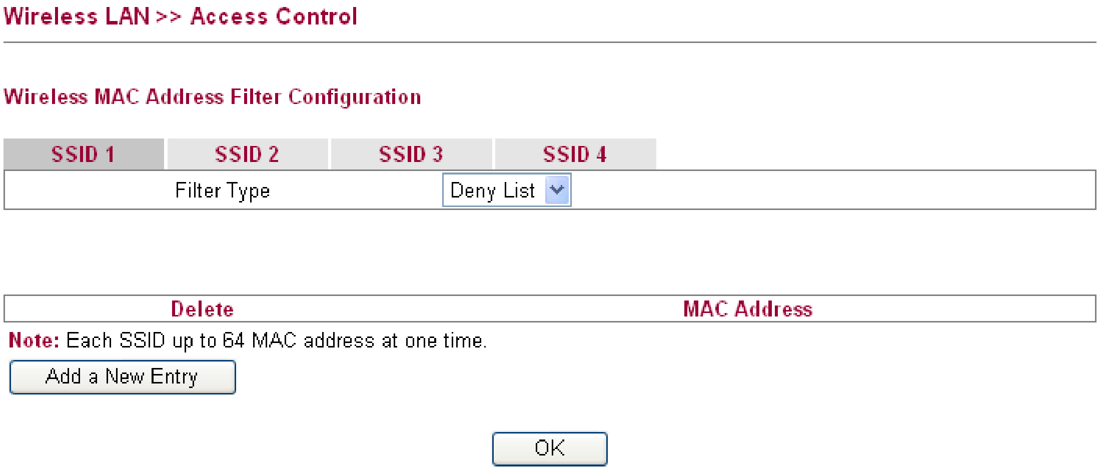


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



4.10.3 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

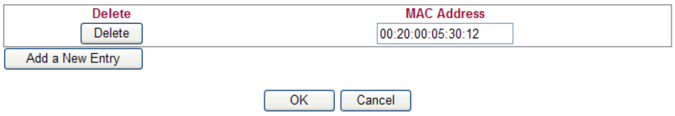
SSID 1 | SSID 2 | SSID 3 | SSID 4

Filter Type: Deny List

Delete	MAC Address

Note: Each SSID up to 64 MAC address at one time.

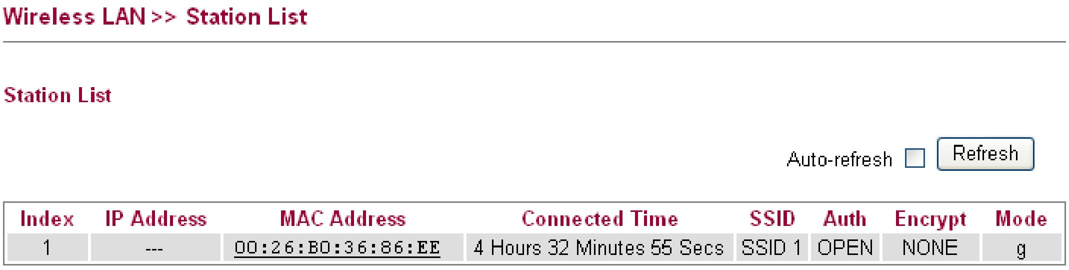
Available settings are explained as follows:

Item	Description
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.  Delete: Delete — MAC Address: 00:20:00:05:30:12 Add a New Entry — OK — Cancel

Click **OK** to save the configuration.

4.10.4 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	SSID	Auth	Encrypt	Mode
1	---	00:26:B0:36:86:EE	4 Hours 32 Minutes 55 Secs	SSID 1	OPEN	NONE	g

Available settings are explained as follows:

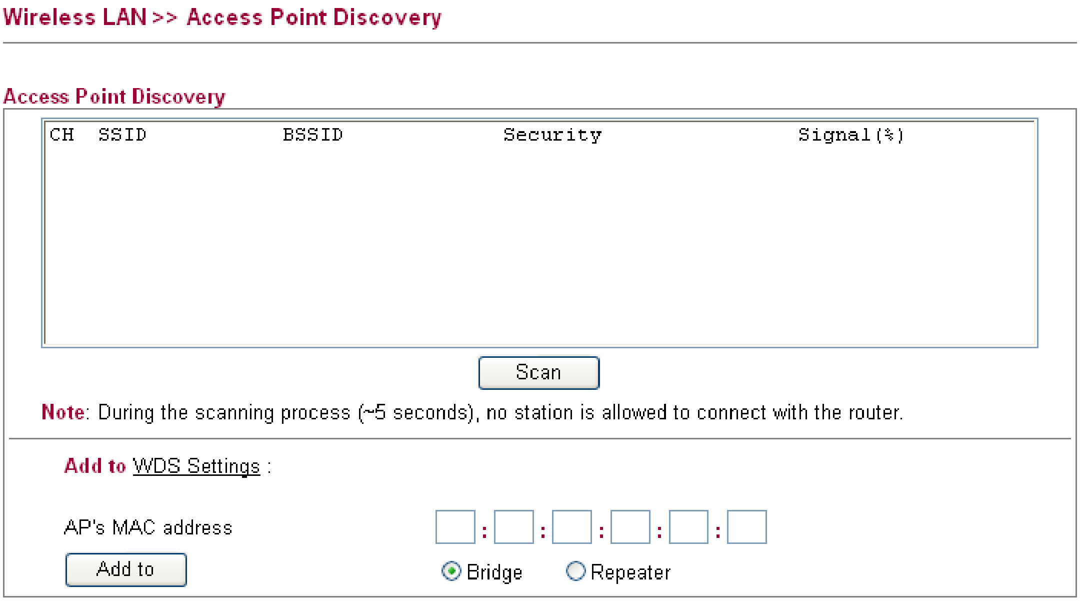
Item	Description
Auto-refresh	Check this box to force the system refreshing the table automatically**.**
Refresh	Click this button to refresh current page.
Index	Display the number of the connected station.
IP Address	Display the WAN IP address for the connected station.
MAC Address	Display the MAC Address for the connected station.
Connected Time	Display the connection time for the connected station.
SSID	Display the SSID of the connected station.
Auth	Display the authentication of the connected station.
Encrypt	Display the encryption type adapted by the connected station.
Mode	Display the connection mode used by the connected station.

4.10.5 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.

Add to WDS Settings :

AP's MAC address □ : □ : □ : □ : □ : □

● Bridge ○ Repeater

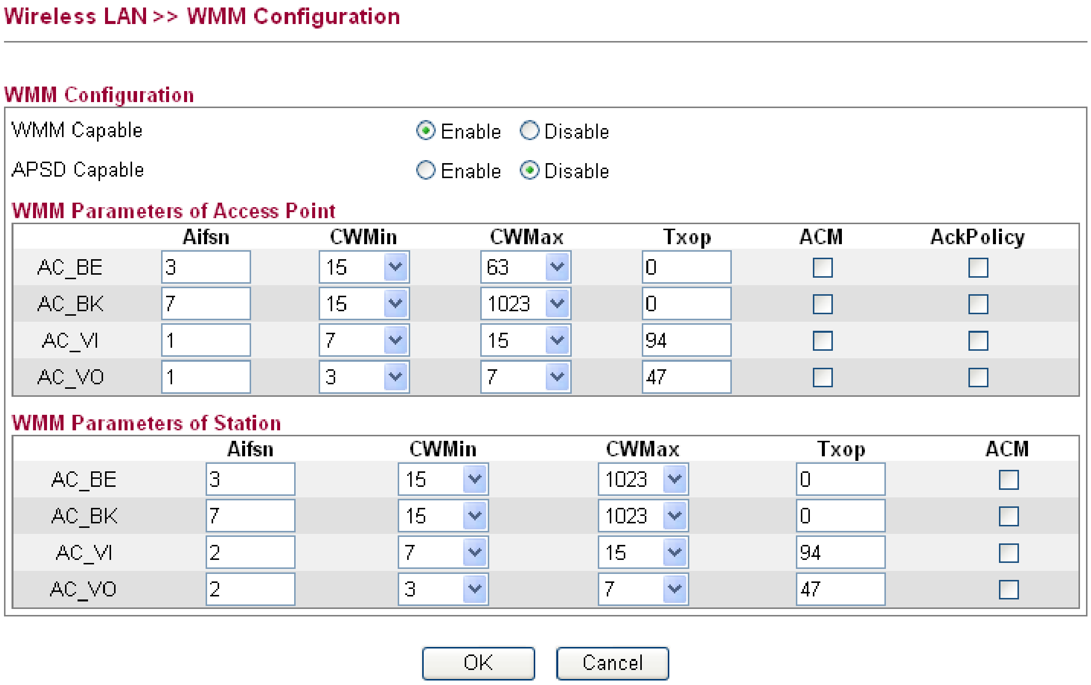
Available settings are explained as follows:

Item	Description
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.
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added on WDS settings page.

4.10.6 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.



Wireless LAN >> WMM Configuration

WMM Configuration

WMM Capable ● Enable ○ Disable

APSD Capable ○ Enable ● Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

Available settings are explained as follows:

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable	The default setting is **Disable**.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO

	categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. **Note:** Vigor1000 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	**"**Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

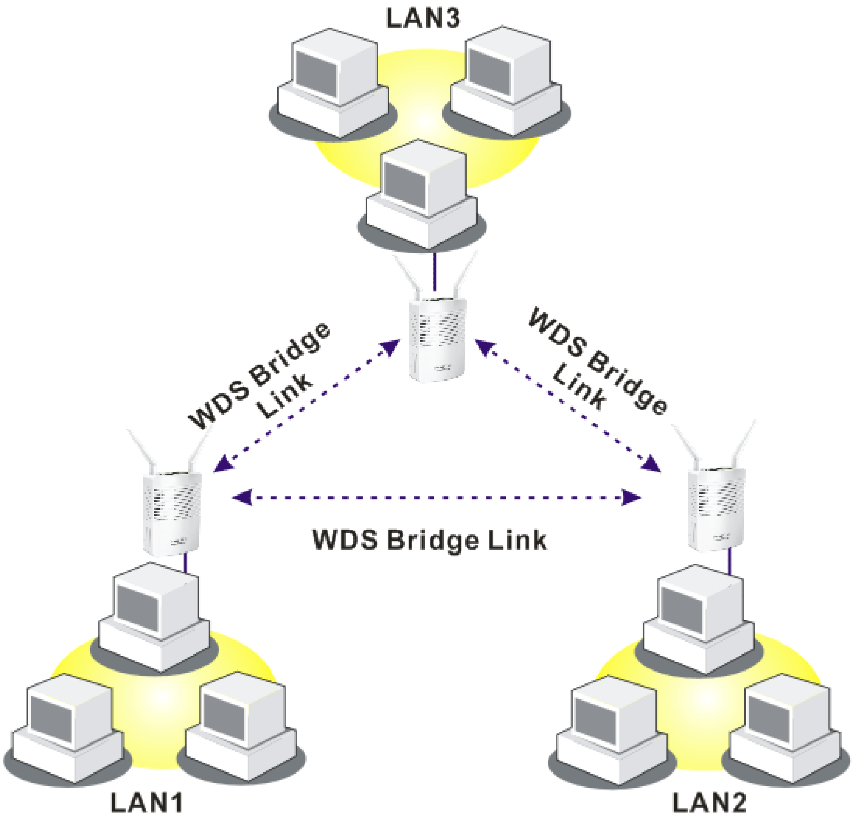
Click **OK** to save the settings.

4.10.7 WDS

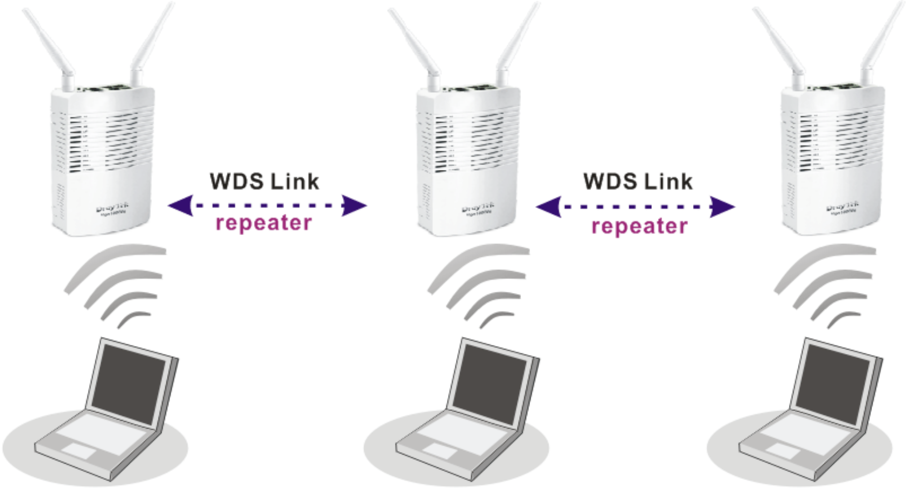
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:



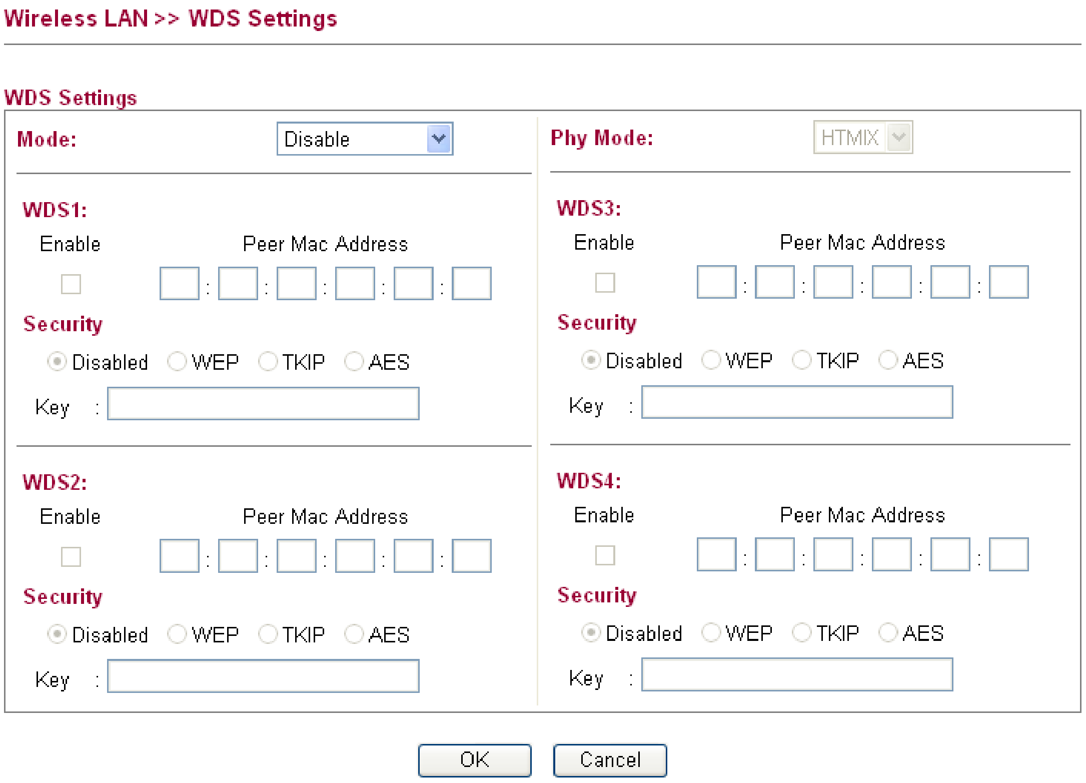
The application for the WDS-Repeater mode is depicted as below:



In **Bridge** mode, the router will connect to up to four Vigor1000 which use the same mode, and all wired Ethernet clients of every Vigor1000 will be connected together. You can use this mode to connect a network to other networks which is physically isolated. Please note that when you set to this mode, Vigor1000 will not accept regular wireless clients anymore.

In **Repeater** mode, the router will connect to up to four Vigor1000 which use the same mode, and all wired Ethernet clients of every Vigor1000 will be connected together. You can use this mode to connect a network to other networks which is physically isolated. When you use this mode, this access point is still able to accept wireless clients.

Click **WDS** from **Wireless LAN** menu. The following page will be shown.



Wireless LAN >> WDS Settings

WDS Settings

Mode: Disable

Phy Mode: HTMIX

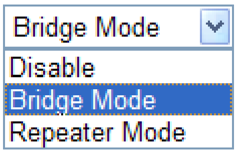
WDS1:
Enable □ Peer Mac Address □ : □ : □ : □ : □ : □
Security ● Disabled ○ WEP ○ TKIP ○ AES
Key :

WDS2:
Enable □ Peer Mac Address □ : □ : □ : □ : □ : □
Security ● Disabled ○ WEP ○ TKIP ○ AES
Key :

WDS3:
Enable □ Peer Mac Address □ : □ : □ : □ : □ : □
Security ● Disabled ○ WEP ○ TKIP ○ AES
Key :

WDS4:
Enable □ Peer Mac Address □ : □ : □ : □ : □ : □
Security ● Disabled ○ WEP ○ TKIP ○ AES
Key :

Available settings are explained as follows:

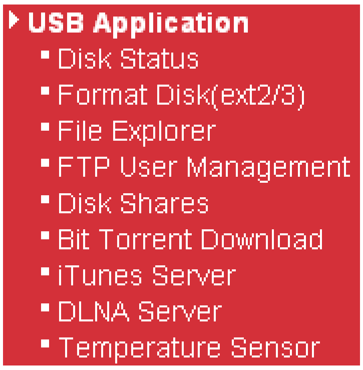
Item	Description
Mode	Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge Mode** is designed to fulfill the first type of application. **Repeater Mode** is for the second one.  Bridge Mode Disable Bridge Mode Repeater Mode
Security	There are four types for security, **Disabled**, **WEP**, **TKIP** and **Key** or **Peer Mac Address** field valid or not. Choose one of the types for the router. Please disable the unused link to get better performance. **Key-** Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by "0x". **Peer Mac Address-** Four peer MAC addresses are allowed

	to be entered in this page at one time.
Phy Mode	There are three types of transmission rates developed by different techniques for **Phy Mode**. Data will be transmitted via communication channel. **CCK** – If 802.11b wireless mode is used, please choose such type as the Phy Mode. **OFDM** – If 802.11g wireless mode is used, please choose such type as the Phy Mode. **HTMIX** – If 802.11b/g/n wireless mode is used, please choose such type as the Phy Mode. Both clients (local and remote) must use the same Phy Mode to have the same transmission rate.

Click **OK** to save the settings.

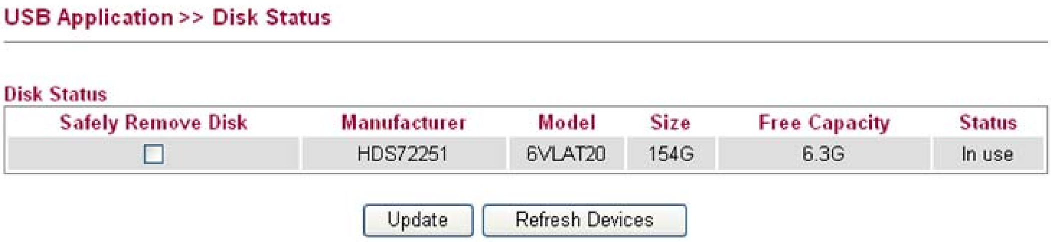
4.11 USB Application

USB storage disk can be regarded as an FTP server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk. 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 storage disk) through Vigor router.



4.11.1 Disk Status

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



USB Application >> Disk Status

Disk Status

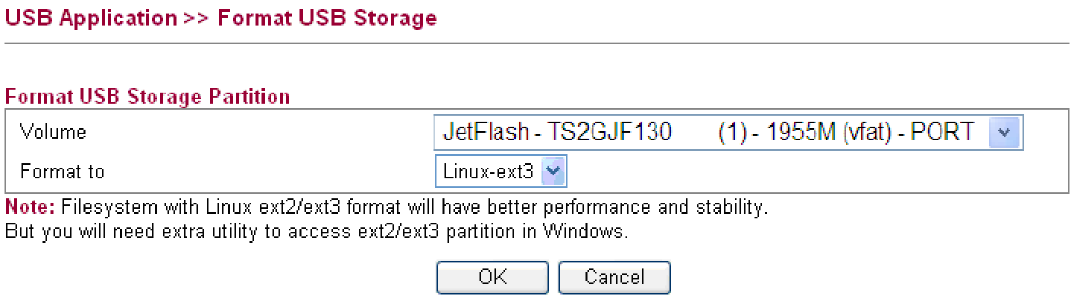
Safely Remove Disk	Manufacturer	Model	Size	Free Capacity	Status
□	HDS72251	6VLAT20	154G	6.3G	In use

Available settings are explained as follows:

Item	Description
Safely Remove Disk	Check this box and then you can remove the USB disk safely.
Manufacturer	Display the manufacturer of the disk.
Model	Display the type of the disk.
Size	Display the storage space of the disk.
Free Capacity	Display the free disk space of the disk.
Status	Display current usage status of the disk
Update	Check the box of **Safely Remove Disk,** then click this button to update the disk status.
Refresh Devices	Click this button to refresh the disk status.

4.11.2 Format Disk (ext2/3)

Under Linux environment, USB disk can be formatted in ext2 or ext3 to have good stability and efficiency for data transmitting.



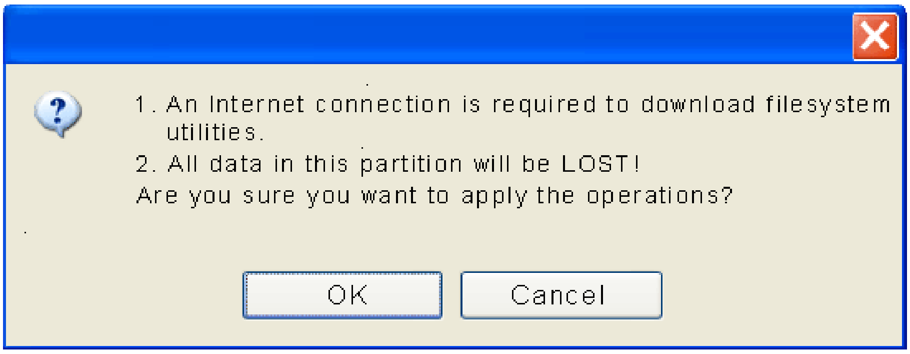
USB Application >> Format USB Storage

Format USB Storage Partition

Volume	JetFlash - TS2GJF130 (1) - 1955M (vfat) - PORT
Format to	Linux-ext3

Note: Filesystem with Linux ext2/ext3 format will have better performance and stability.
But you will need extra utility to access ext2/ext3 partition in Windows.

After clicking **OK**, the following confirmation dialog will appear.

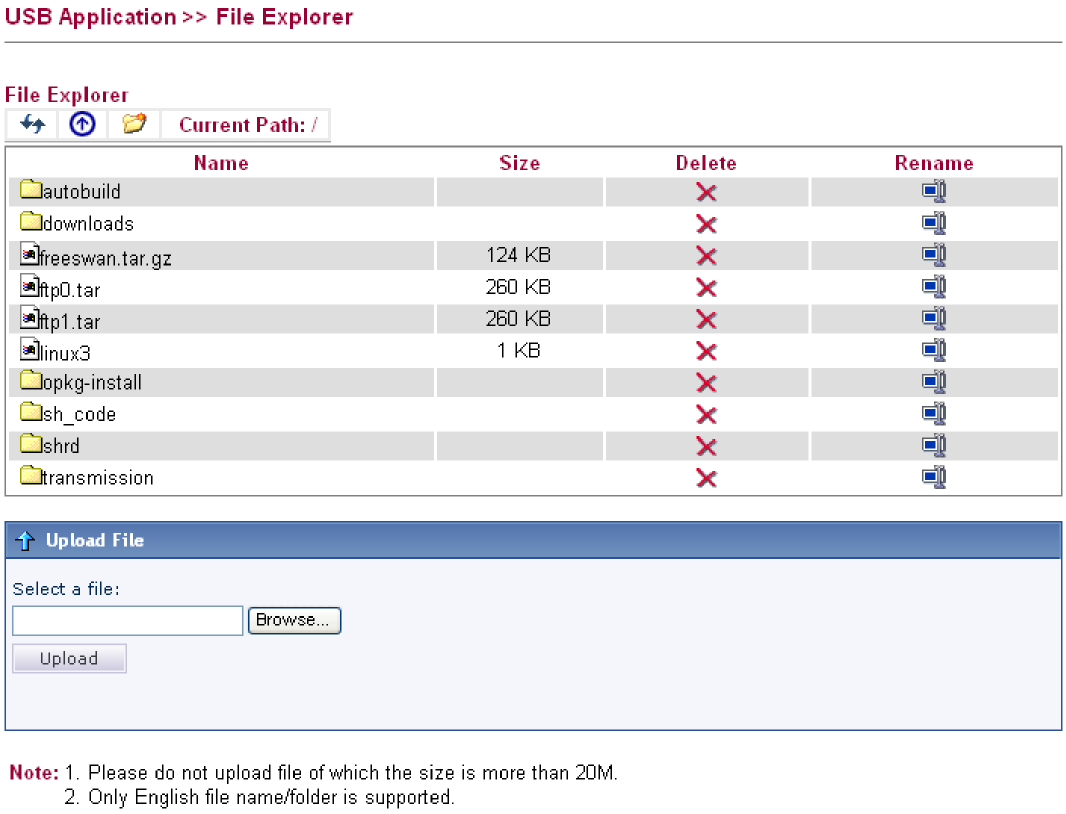


1. An Internet connection is required to download filesystem utilities.
2. All data in this partition will be LOST!
Are you sure you want to apply the operations?

Simply click **OK** to continue the procedure.

4.11.3 File Explorer

To review the content of USB diskette via USB port of the router, please open USB Application Explorer to browse the files.



USB Application >> File Explorer

File Explorer

Name	Size	Delete	Rename
autobuild		✕	✎
downloads		✕	✎
freeswan.tar.gz	124 KB	✕	✎
ftp0.tar	260 KB	✕	✎
ftp1.tar	260 KB	✕	✎
linux3	1 KB	✕	✎
opkg-install		✕	✎
sh_code		✕	✎
shrd		✕	✎
transmission		✕	✎

Upload File

Select a file:

Note: 1. Please do not upload file of which the size is more than 20M.
2. Only English file name/folder is supported.

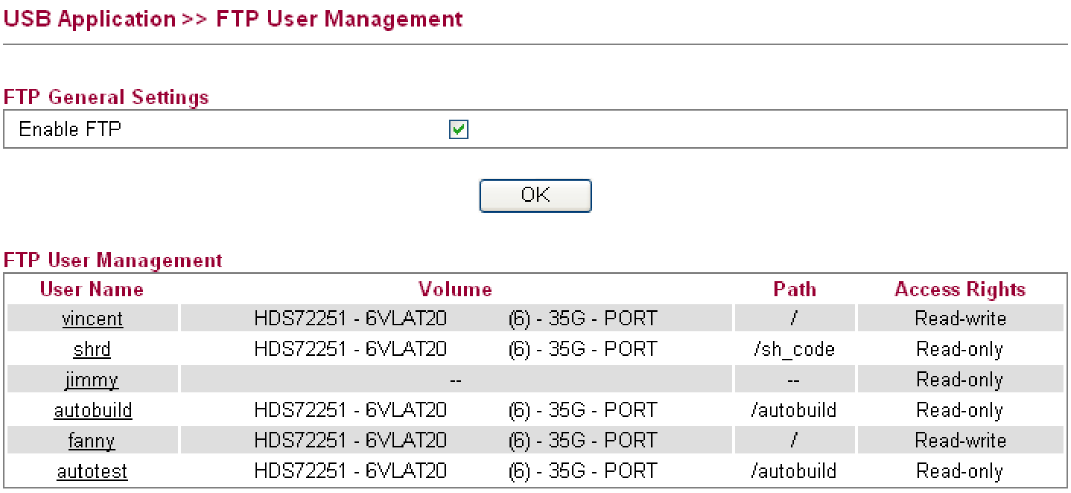
Available settings are explained as follows:

Item	Description
Refresh	Click this icon to refresh files list.
Back	Click this icon to return to the upper directory.
Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB diskette. The uploaded file in the USB diskette can be shared for other user through FTP.

4.11.4 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 disk and configure settings in **User>>User Configuration** first. Otherwise, an error message will appear to warn you.

At present, the Vigor router can support USB storage disk with versions of FAT16/32 and NTFS only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16/32 or NTFS.



USB Application >> FTP User Management

FTP General Settings

Enable FTP ☑

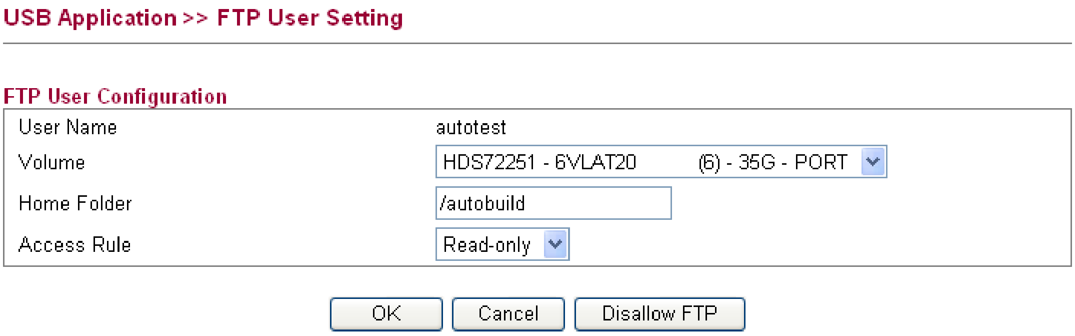
FTP User Management

User Name	Volume	Path	Access Rights
vincent	HDS72251 - 6VLAT20 (6) - 35G - PORT	/	Read-write
shrd	HDS72251 - 6VLAT20 (6) - 35G - PORT	/sh_code	Read-only
jimmy	--	--	Read-only
autobuild	HDS72251 - 6VLAT20 (6) - 35G - PORT	/autobuild	Read-only
fanny	HDS72251 - 6VLAT20 (6) - 35G - PORT	/	Read-write
autotest	HDS72251 - 6VLAT20 (6) - 35G - PORT	/autobuild	Read-only

Available settings are explained as follows:

Item	Description
Enable FTP	Check this box to enable FTP connection.
User Name	It displays the username that user uses to login to the FTP server.
Volume	It displays the proper volume for the connected USB disk.
Path	It displays the directory name for the connected USB disk.
Access Rights	It displays the access right for the connected USB disk.

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



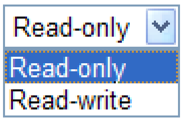
USB Application >> FTP User Setting

FTP User Configuration

User Name	autotest
Volume	HDS72251 - 6VLAT20 (6) - 35G - PORT
Home Folder	/autobuild
Access Rule	Read-only

Available settings are explained as follows:

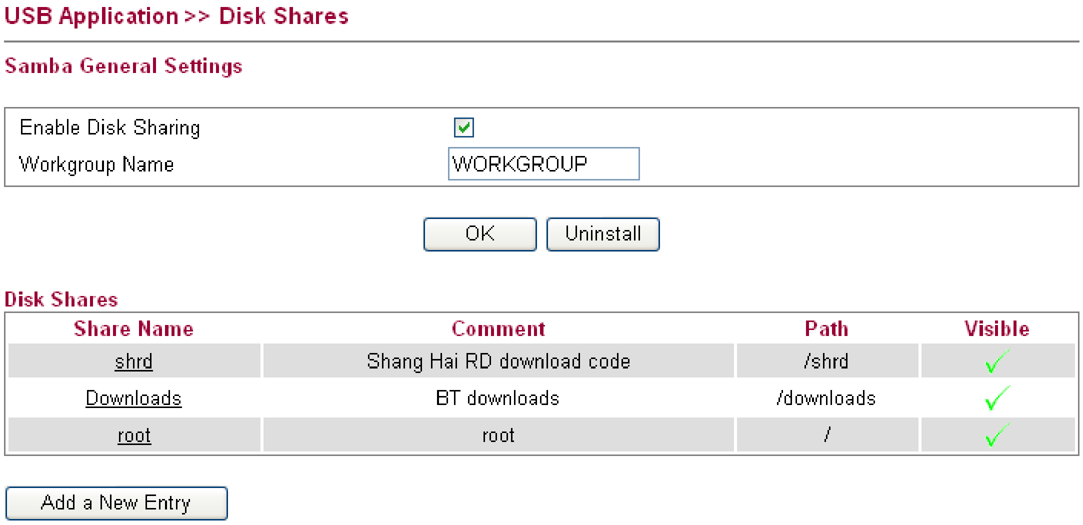
Item	Description
Volume	Select the proper volume for the connected USB disk.

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 disk.
	 Read-only Read-only Read-write
Disallow FTP	Disconnect the FTP service for the select ed user.

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

4.11.5 Disk Shares

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



USB Application >> Disk Shares

Samba General Settings

Enable Disk Sharing	☑
Workgroup Name	WORKGROUP

Disk Shares

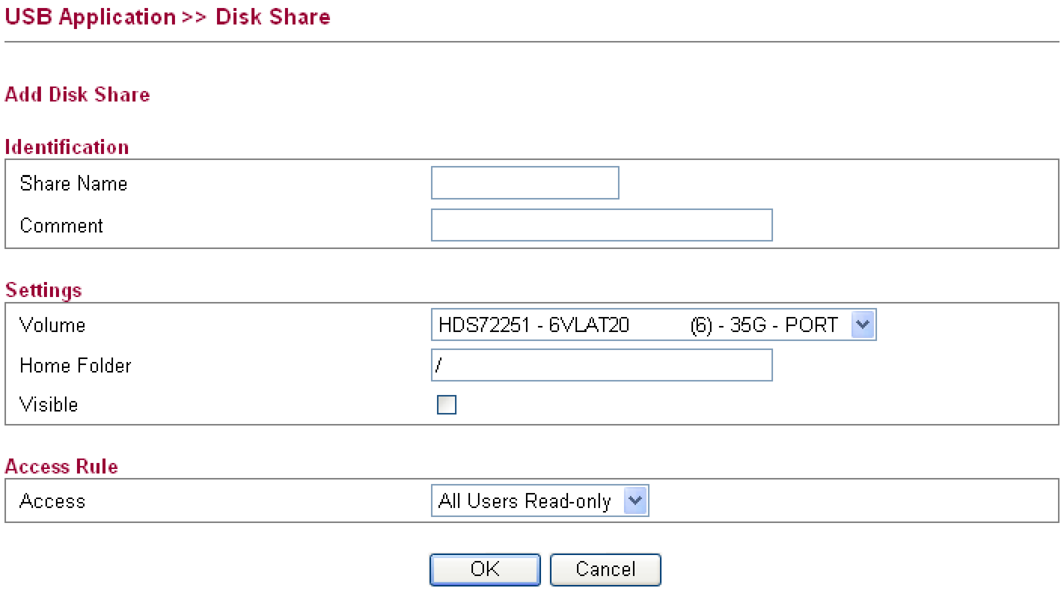
Share Name	Comment	Path	Visible
shrd	Shang Hai RD download code	/shrd	✓
Downloads	BT downloads	/downloads	✓
root	root	/	✓

Available settings are explained as follows:

Item	Description
Enable Disk Sharing	Check this box to share the information on USB storage disk.
Workgroup Name	It provides easy sharing of files, printers and other network resources for the computers collected under such group on LAN.
Share Name	It displays the name to be known by other computers in local network.
Comment	It displays the description for the disk sharing.
Path	It displays the directory name for the connected USB disk.

Visible	It displays the status of the connected USB disk.

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

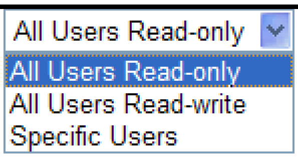
Volume	HDS72251 - 6VLAT20 (6) - 35G - PORT
Home Folder	/
Visible	□

Access Rule

Access	All Users Read-only

Available settings are explained as follows:

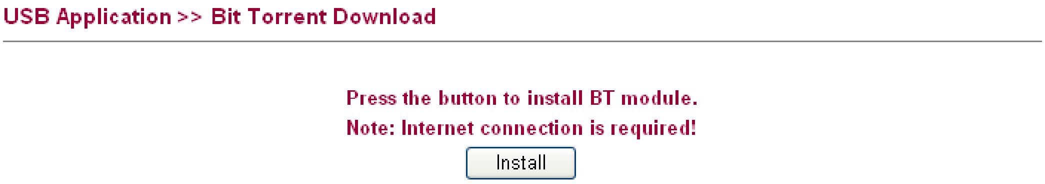
Item	Description
Share Name	Type a name to be known by other computers in local network. The name must not contain spaces or special characters.
Comment	Type the brief description for the disk sharing. The words here will be seen in Network Neighborhood on Windows client computers.
Volume	Select the proper volume for the connected USB disk.
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 disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB disk. **Note:** When write protect status for the USB disk 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	Specify the access right and apply to all the wireless clients that want to connect to the attached USB disk.

	 All Users Read-only All Users Read-only All Users Read-write Specific Users **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.

4.11.6 Bit Torrent Download

There are many seeds of BT Torrents in Internet for users to download preferred video file, image file and so on. In general, the downloaded files would be stored in the computer. However, if the computer is shut down, the file downloading also will be terminated. Here, Vigor router provides a function to download the BT Torrent file into USB storage device. The downloading job will not be terminated even if the computer is powered off, for the file is downloaded and transferred from the router to the USB storage device directly.

Click **USB Application >>Bit Torrent Download**.

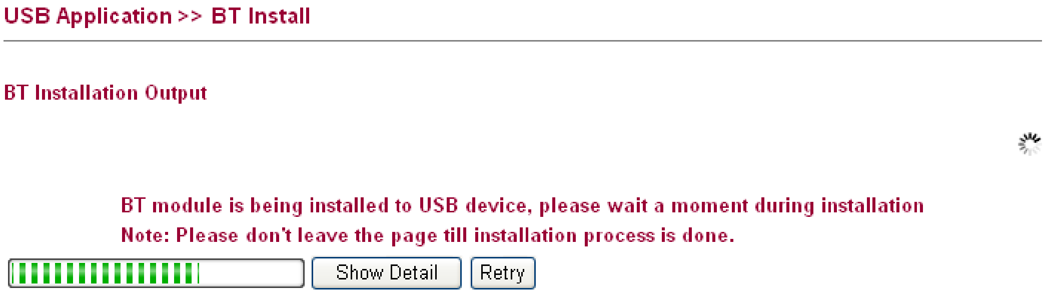


USB Application >> Bit Torrent Download

Press the button to install BT module.

Note: Internet connection is required!

Click **Install** to install the BT module for the router and the USB storage device.



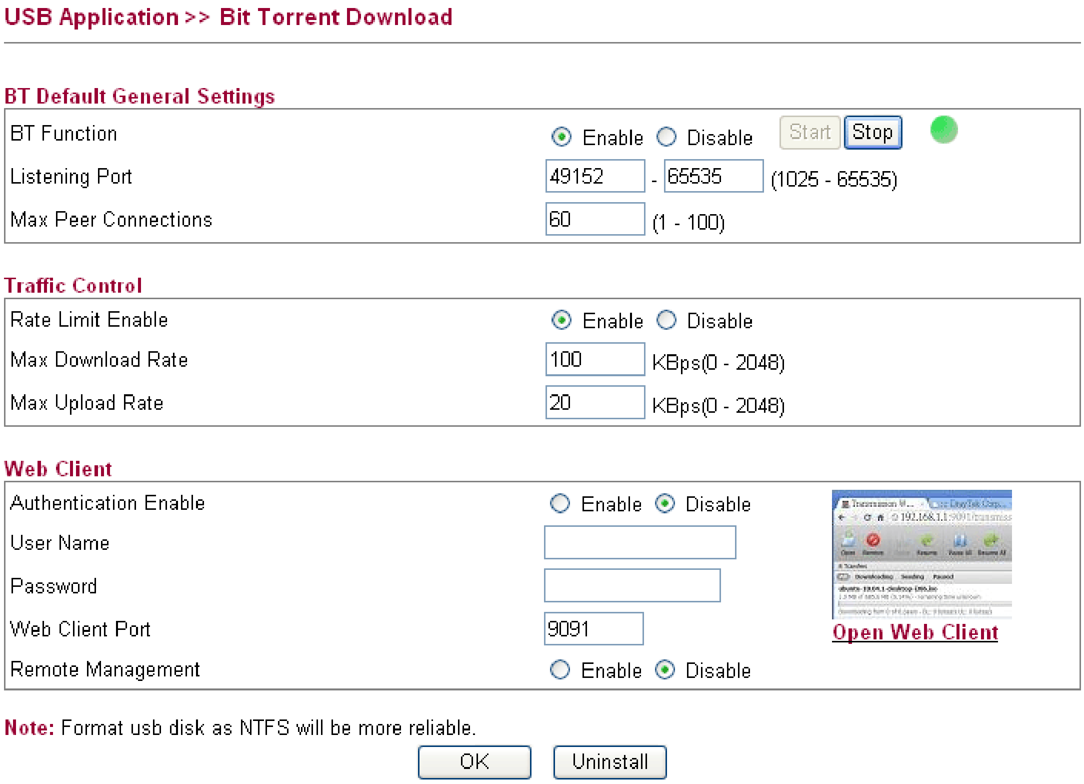
USB Application >> BT Install

BT Installation Output

BT module is being installed to USB device, please wait a moment during installation

Note: Please don't leave the page till installation process is done.

When the module installation is finished, you will see the following screen:



USB Application >> Bit Torrent Download

BT Default General Settings

BT Function	● Enable ○ Disable Start Stop
Listening Port	49152 - 65535 (1025 - 65535)
Max Peer Connections	60 (1 - 100)

Traffic Control

Rate Limit Enable	● Enable ○ Disable
Max Download Rate	100 KBps(0 - 2048)
Max Upload Rate	20 KBps(0 - 2048)

Web Client

Authentication Enable	○ Enable ● Disable
User Name	
Password	
Web Client Port	9091
Remote Management	○ Enable ● Disable

Note: Format usb disk as NTFS will be more reliable.

Available settings are explained as follows:

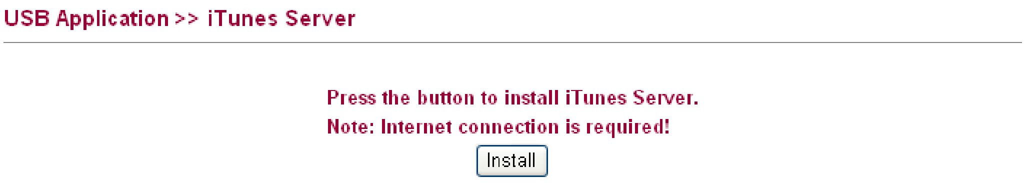
Item	Description
BT Function	**Enable** – Click it to enable BT download function after powering your computer. **Disable** – Click it to disable BT download function after powering your computer **Start** – Start the BT download process. **Stop** – Stop the BT download process.
Listening Port	Type the port number to listen for incoming peer connection.
Max Peer Connections	Type a number of the peers that can connect to the router at one time.
Rate Limit Enable	Transmission rate can be limited by clicking **Enable**. If it is enabled, please specify the maximum rate for download and upload respectively.
Max Download Rate	Type the maximum rate for data downloading per second. The range is 0 – 2048KB.
Max Upload Rate	Type the maximum rate for data uploading per second. The range is 0 – 2048KB.
Authentication Enable	**Enable** – Click it to enable authentication function. Each wireless clients or PC in LAN must type the username and password for authentication to the remote control services. **Disable** – Click it to disable authentication function.
User Name	Type a name for authentication.

Password	Type a password for authentication.
Web Client Port	Type a port number for accessing Open Web Client.
Remote Management	**Enable** – Click it to enable remote control for BT torrent download. **Disable** – Click it to disable remote management function.
OK	Save the settings.
Uninstall	Cancel the module installation settings and exit the dialog.

For the detailed information of BT Torrent application, please refer to Chapter 5.

4.11.7 iTunes Server

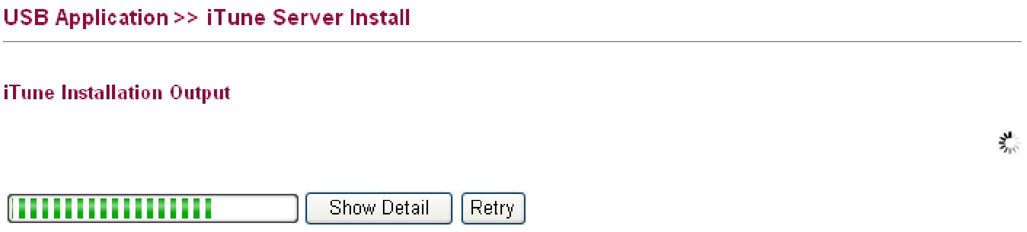
iTunes server is one of the most popular programs for managing media content on a computer. Vigor router provides a function to support iTunes service that users can play music files (e.g., mp3) from the USB storage device on Vigor router directly.



USB Application >> iTunes Server

Press the button to install iTunes Server.
Note: Internet connection is required!

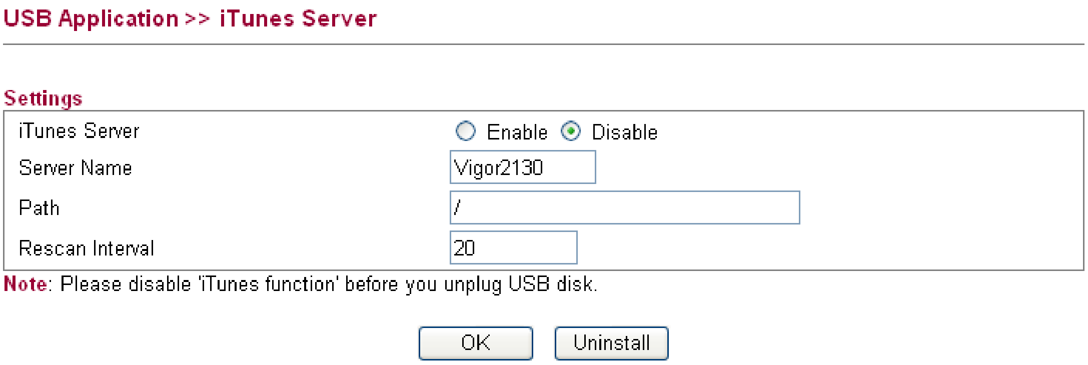
Click **Install** to install the iTunes Server for the router and the USB storage device.



USB Application >> iTune Server Install

iTune Installation Output

When the server installation is finished, you will see the following screen:



USB Application >> iTunes Server

Settings

iTunes Server	○ Enable ● Disable
Server Name	Vigor2130
Path	/
Rescan Interval	20

Note: Please disable 'iTunes function' before you unplug USB disk.

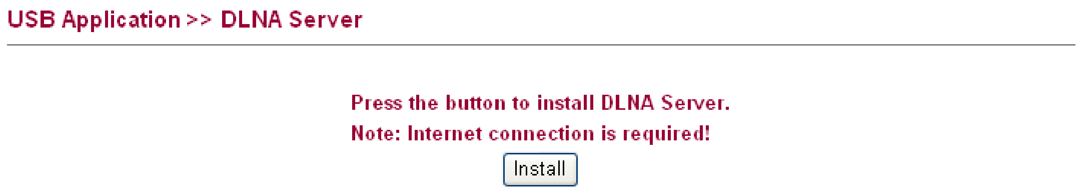
Available settings are explained as follows:

Item	Description
iTunes Server	**Enable** – Click it to enable iTunes Server function.

	Disable – Click it to disable iTunes Server function.
Server Name	The default name is the router name. You can change it if needed.
Path	After storing the media files in the USB storage device, please specify a path for the files to be accessed for iTunes service. “/” is the symbol for the top folder of USB storage.
Rescan Interval	The USB storage disk will be scanned by iTunes Server again based on the time interval set here. The unit is second.
OK	Save the settings.
Uninstall	Cancel the module installation settings and exit the dialog.

4.11.8 DLNA server

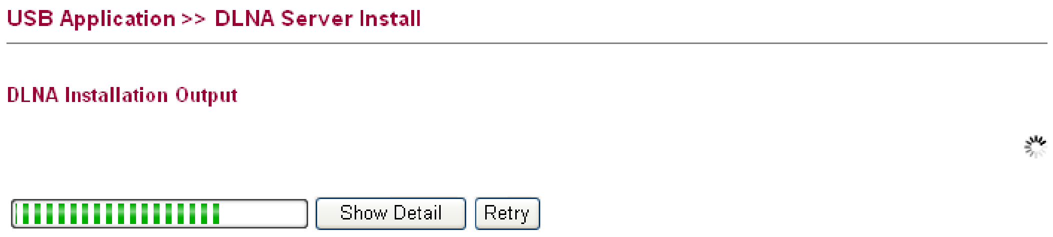
DLNA (Digital Living Network Alliance) is a framework which personal computer, HDD video recorder, television and other digital devices can share each other data through network connection. The DLNA devices are divided into two functions. One is server side which transmits images, music and video, and the other is client side which receives data only. Some devices support both functions. Vigor1000 can install server program onto the connected USB storage device. Clients with equipments supporting DLNA can play the files stored in the USB storage device connected to Vigor1000 through the network.



USB Application >> DLNA Server

Press the button to install DLNA Server.
Note: Internet connection is required!

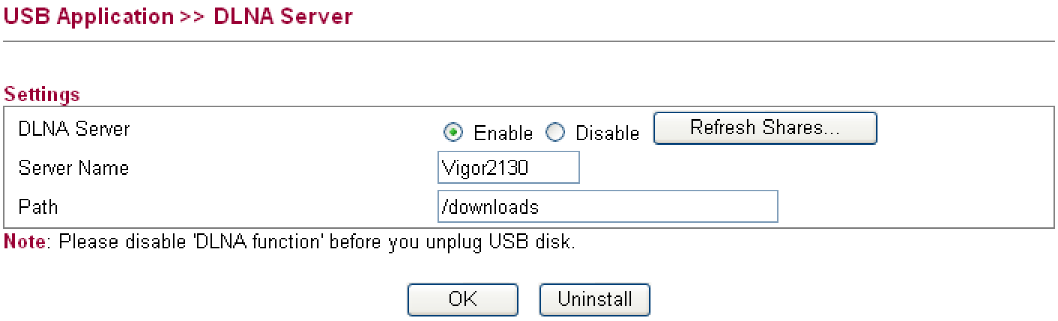
Click **Install** to install the DLNA Server for the router and the USB storage device.



USB Application >> DLNA Server Install

DLNA Installation Output

When the server installation is finished, you will see the following screen:



USB Application >> DLNA Server

Settings

DLNA Server	● Enable ○ Disable [Refresh Shares...]
Server Name	Vigor2130
Path	/downloads

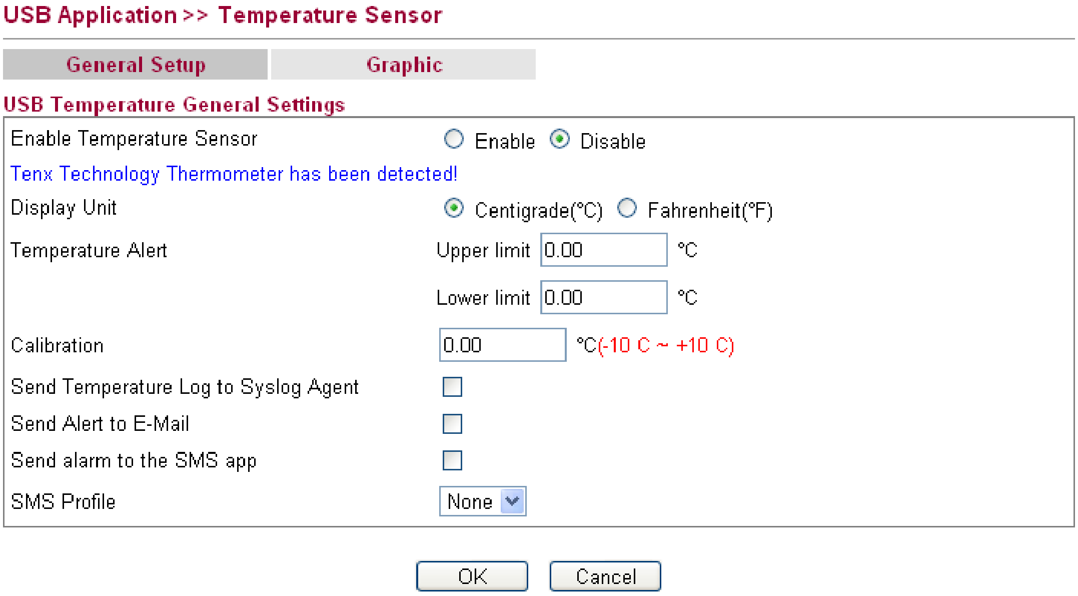
Note: Please disable 'DLNA function' before you unplug USB disk.

Available settings are explained as follows:

Item	Description
DLNA Server	**Enable** – Click it to enable DLNA Server function. **Disable** – Click it to disable DLNA Server function.
Server Name	The default name is the router name. You can change it if needed.
Path	After storing the files in the USB storage device, please specify a path for the files to be accessed for DLNA service. "/" is the symbol for the top folder of USB storage.
OK	Save the settings.
Uninstall	Cancel the module installation settings and exit the dialog.

4.11.9 Temperature Sensor

A USB Thermometer can be attached to Vigor router to monitor the environmental temperature. If the temperature is higher the upper limit or lower than the lower limit, an alert would be sent out for notification.



USB Application >> Temperature Sensor

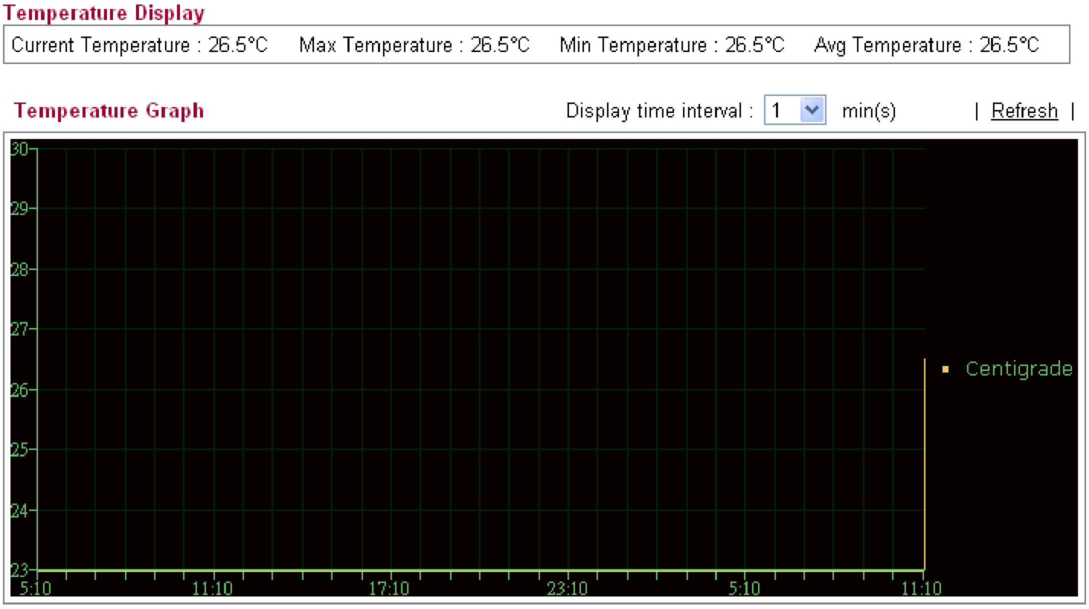
USB Temperature General Settings

Enable Temperature Sensor	○ Enable ● Disable
Tenx Technology Thermometer has been detected!	
Display Unit	● Centigrade(°C) ○ Fahrenheit(°F)
Temperature Alert	Upper limit 0.00 °C
	Lower limit 0.00 °C
Calibration	0.00 °C(-10 C ~ +10 C)
Send Temperature Log to Syslog Agent	□
Send Alert to E-Mail	□
Send alarm to the SMS app	□
SMS Profile	None

Available settings are explained as follows:

Item	Description
Enable Temperature Sensor	**Enable** – Enable the function of temperature sensor. **Disable** – Disable the function.
Display Unit	Choose the display unit of the temperature. There are two types for you to choose.
Temperature Alert	Type the upper limit and lower limit for the system to send out temperature alert.
Calibration	Type a value used for correcting the temperature error.
Send Temperature Log to Syslog Agent	Check the box to enable this function. The temperature log will be recorded on Syslog.
Send Alert to E-Mail.	Check the box to enable this function. The alert will be sent to the e-mail address that you offer on the page of **System Maintenance>>Syslog / Mail Alert Setup**.
Send alarm to the SMS app	Check the box to enable this function.
SMS Profile	Use the drop down list to choose a SMS profile for sending the alarm.
OK	Save the settings.
Cancel	Cancel the settings.

Below shows an example of temperature graph:



Temperature Display

Current Temperature : 26.5°C　Max Temperature : 26.5°C　Min Temperature : 26.5°C　Avg Temperature : 26.5°C

Temperature Graph　Display time interval : 1 min(s)　| Refresh |

Current temperature, maximum temperature, minimum temperature and average temperature will be displayed on the screen.

4.12 VoIP

Note: This function is used for "V" models.

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, "SIP Address". The standard format of SIP URI is

sip: user:password @ host: port

Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN/ISDN network.

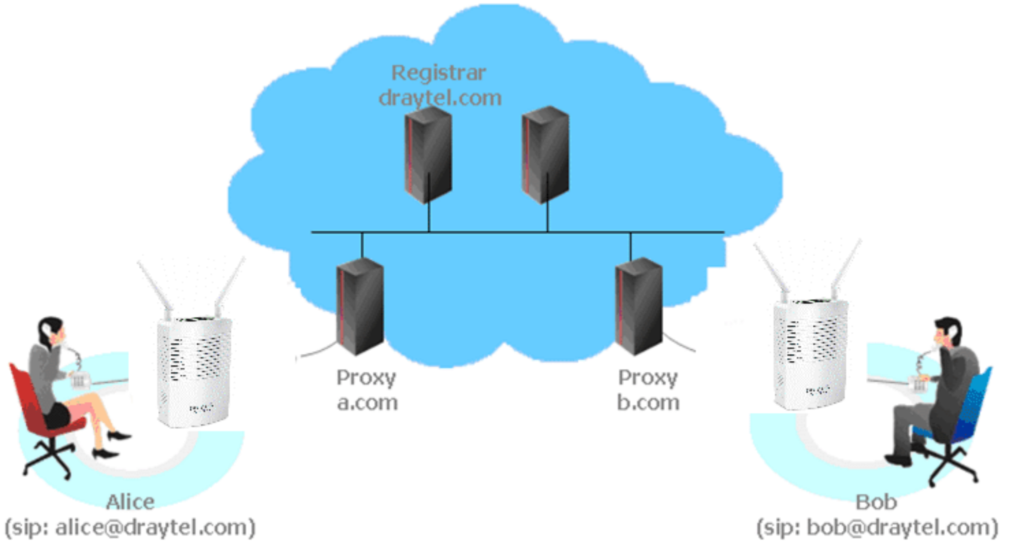
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

Usually there will be two types of calling scenario, as illustrated below:

Calling via SIP Servers

First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.

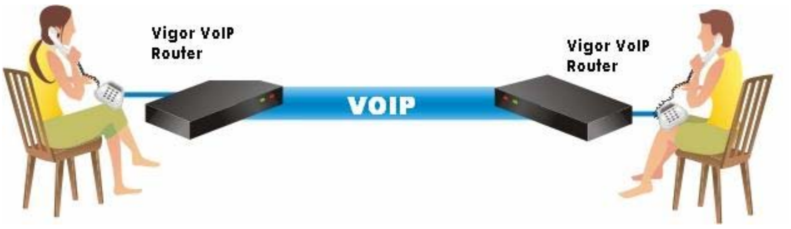
If you both register to the same SIP Registrar, then it will be illustrated as below:



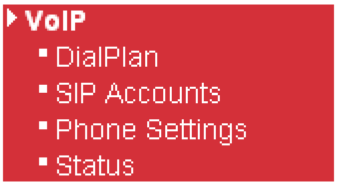
The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar.

Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.

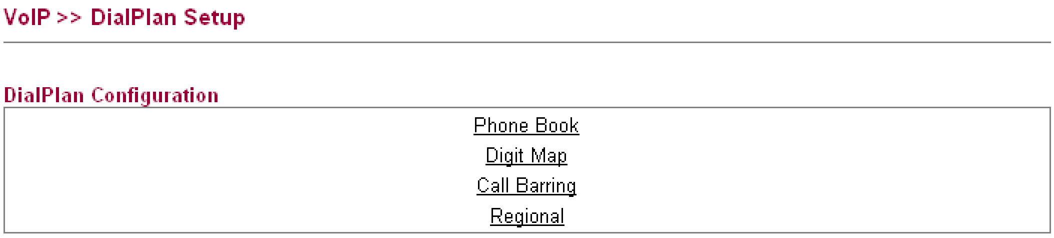


Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.



4.12.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book**, **Digit Map, Call Barring and Regional** links on the page to access into next pages for dialplan settings.



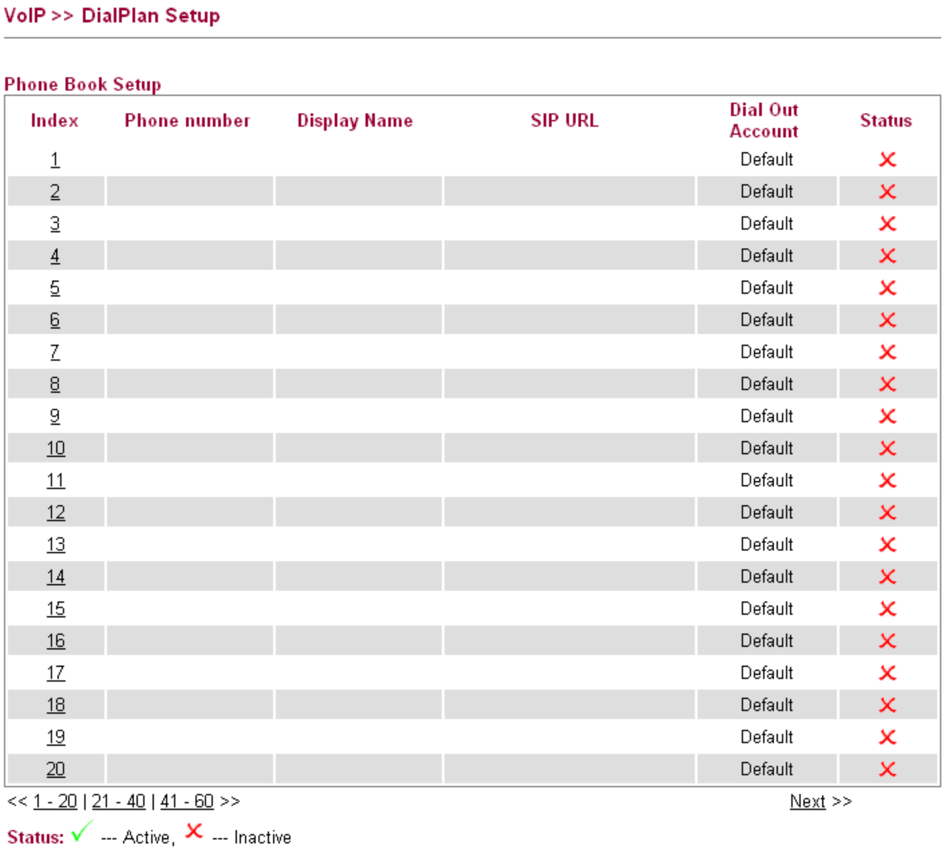
VoIP >> DialPlan Setup

DialPlan Configuration

Phone Book
Digit Map
Call Barring
Regional

4.12.1.1 Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor2820V for setting the phone book.



VoIP >> DialPlan Setup

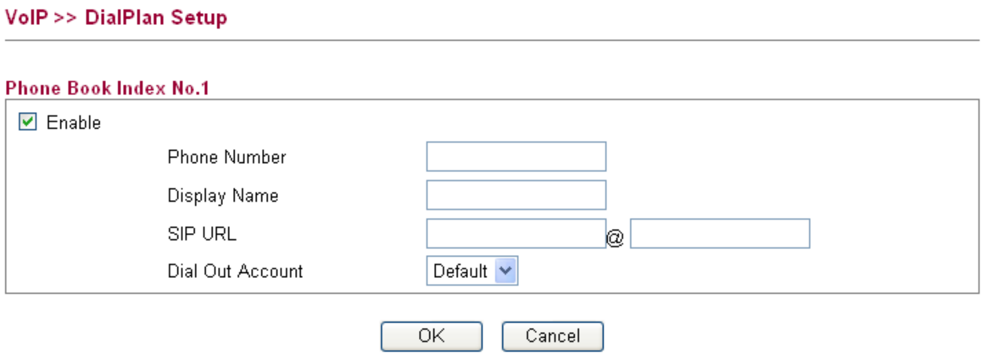
Phone Book Setup

Index	Phone number	Display Name	SIP URL	Dial Out Account	Status
1				Default	✗
2				Default	✗
3				Default	✗
4				Default	✗
5				Default	✗
6				Default	✗
7				Default	✗
8				Default	✗
9				Default	✗
10				Default	✗
11				Default	✗
12				Default	✗
13				Default	✗
14				Default	✗
15				Default	✗
16				Default	✗
17				Default	✗
18				Default	✗
19				Default	✗
20				Default	✗

<< 1 - 20 | 21 - 40 | 41 - 60 >>   Next >>

Status: ✓ --- Active, ✗ --- Inactive

Click any index number to display the dial plan setup page.



VoIP >> DialPlan Setup

Phone Book Index No.1

☑ Enable	
Phone Number	
Display Name	
SIP URL	@
Dial Out Account	Default

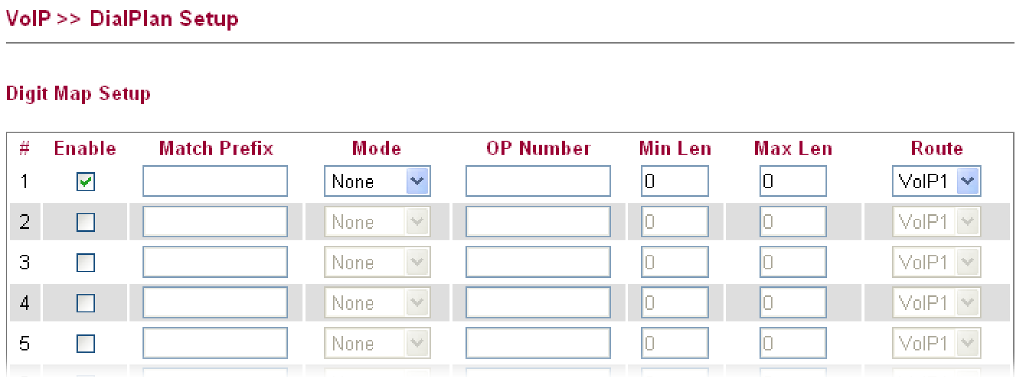
OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP account.
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.

4.12.1.2 Digit Map

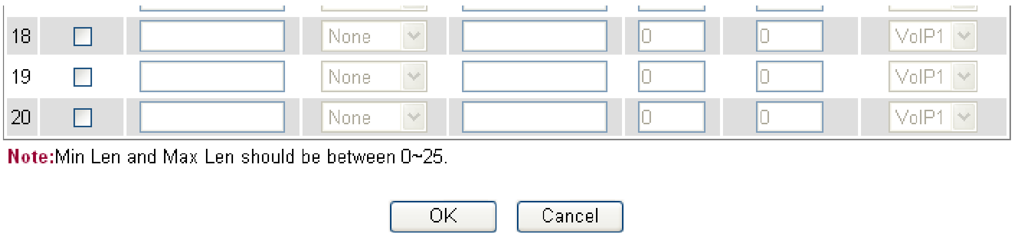
For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.



VoIP >> DialPlan Setup

Digit Map Setup

#	Enable	Match Prefix	Mode	OP Number	Min Len	Max Len	Route
1	☑		None		0	0	VoIP1
2	☐		None		0	0	VoIP1
3	☐		None		0	0	VoIP1
4	☐		None		0	0	VoIP1
5	☐		None		0	0	VoIP1



18	□		None		0	0	VoIP1
19	□		None		0	0	VoIP1
20	□		None		0	0	VoIP1

Note:Min Len and Max Len should be between 0~25.

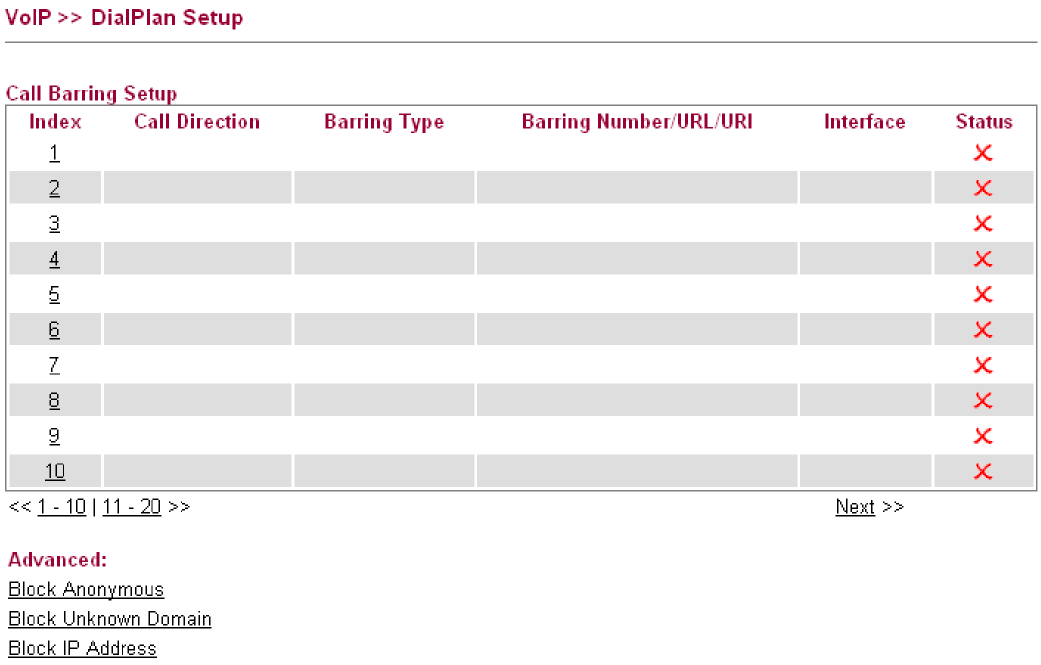
Available settings are explained as follows:

Item	Description
Enable	Check this box to invoke this setting.
Match Prefix	The phone number set here is used to add, strip, or replace the OP number.
Mode	**None** - No action. **Add** - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface. **Strip** - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of *886* will be deleted completely for the prefix number is set with *886*. **Replace** - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of “031111111” will be changed to “88631111111” and sent to SIP server.
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dial number for applying the prefix number settings.
Route	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP

	account first to make this interface available. This item will be changed according to the port settings configured in **VoIP>> Phone Settings**.

4.12.1.3 Call Barring

Call barring is used to block phone calls coming from the one that is not welcomed.



VoIP >> DialPlan Setup

Call Barring Setup

Index	Call Direction	Barring Type	Barring Number/URL/URI	Interface	Status
1					✗
2					✗
3					✗
4					✗
5					✗
6					✗
7					✗
8					✗
9					✗
10					✗

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

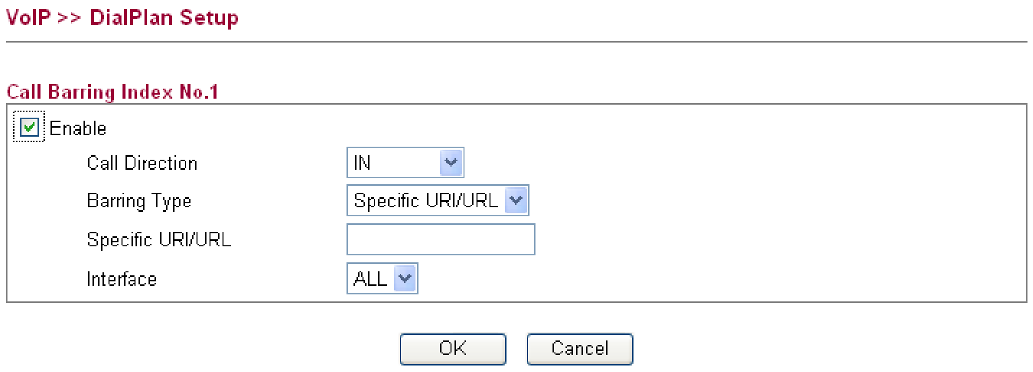
Advanced:

Block Anonymous

Block Unknown Domain

Block IP Address

Click any index number to display the dial plan setup page.



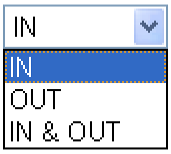
VoIP >> DialPlan Setup

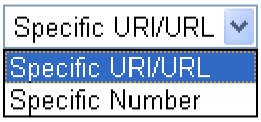
Call Barring Index No.1

☑ Enable

Call Direction	IN
Barring Type	Specific URI/URL
Specific URI/URL	
Interface	ALL

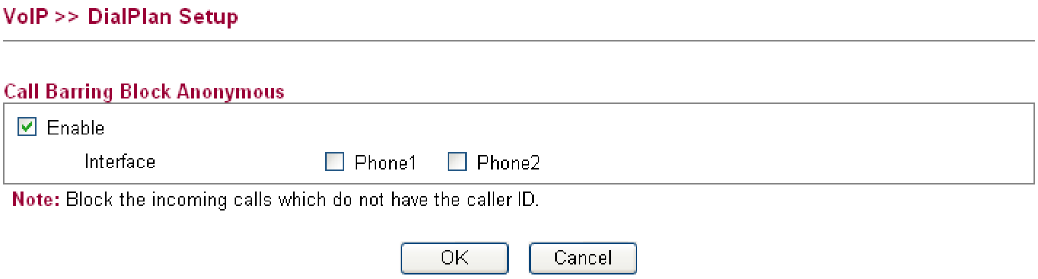
Available settings are explained as follows:

Item	Description
Enable	Click this to enable this entry.
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.  IN IN OUT IN & OUT

Barring Type	Determine the type of the VoIP phone call, URI/URL or number. 
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.
Interface	**All** means all the phone calls will be blocked with such mechanism.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

For **Block Anonymous –** this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.



VoIP >> DialPlan Setup

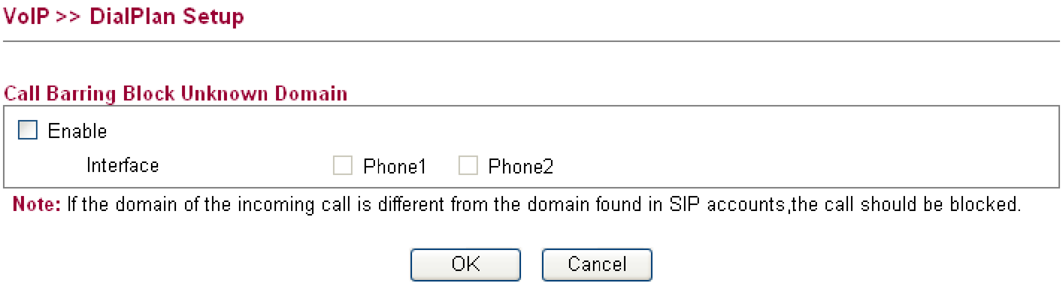
Call Barring Block Anonymous

☑ Enable

Interface ☐ Phone1 ☐ Phone2

Note: Block the incoming calls which do not have the caller ID.

For **Block Unknown Domain –** this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.



VoIP >> DialPlan Setup

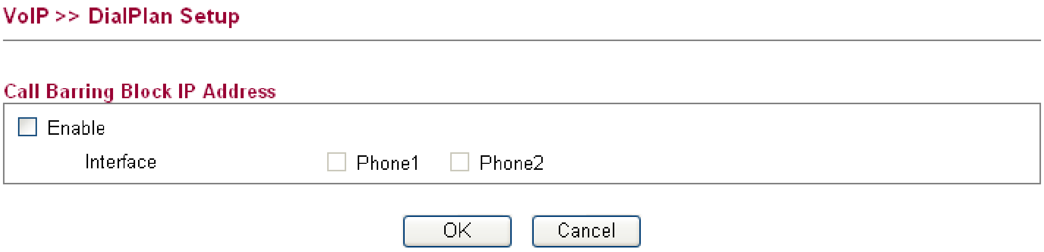
Call Barring Block Unknown Domain

☐ Enable

Interface ☐ Phone1 ☐ Phone2

Note: If the domain of the incoming call is different from the domain found in SIP accounts,the call should be blocked.

For **Block IP Address –** this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.



VoIP >> DialPlan Setup

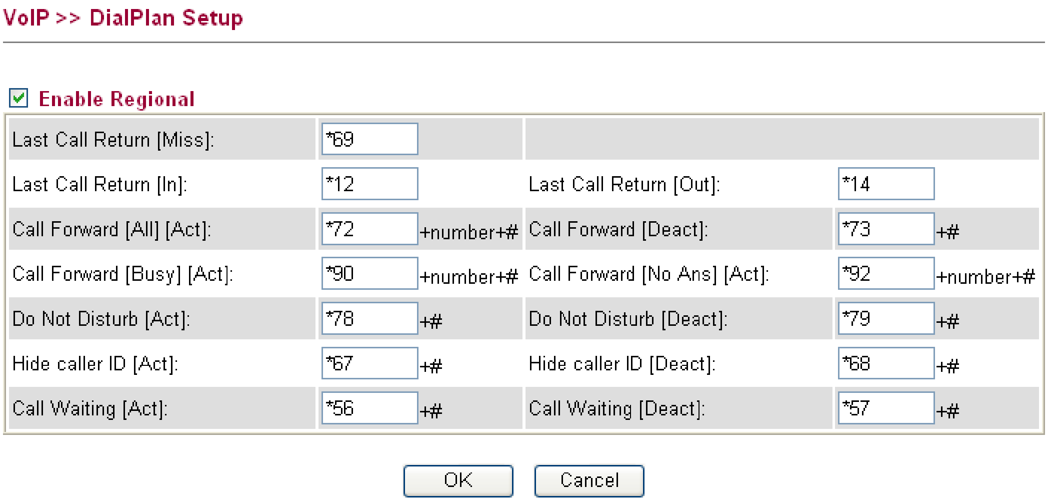
Call Barring Block IP Address

☐ Enable

Interface ☐ Phone1 ☐ Phone2

4.12.1.4 Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You ***can change*** the number based on the region that the router is placed.



VoIP >> DialPlan Setup

☑ Enable Regional

Last Call Return [Miss]:	*69		
Last Call Return [In]:	*12	Last Call Return [Out]:	*14
Call Forward [All] [Act]:	*72 +number+#	Call Forward [Deact]:	*73 +#
Call Forward [Busy] [Act]:	*90 +number+#	Call Forward [No Ans] [Act]:	*92 +number+#
Do Not Disturb [Act]:	*78 +#	Do Not Disturb [Deact]:	*79 +#
Hide caller ID [Act]:	*67 +#	Hide caller ID [Deact]:	*68 +#
Call Waiting [Act]:	*56 +#	Call Waiting [Deact]:	*57 +#

Available settings are explained as follows:

Item	Description
Enable Regional	Check this box to enable this function.
Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know w
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote

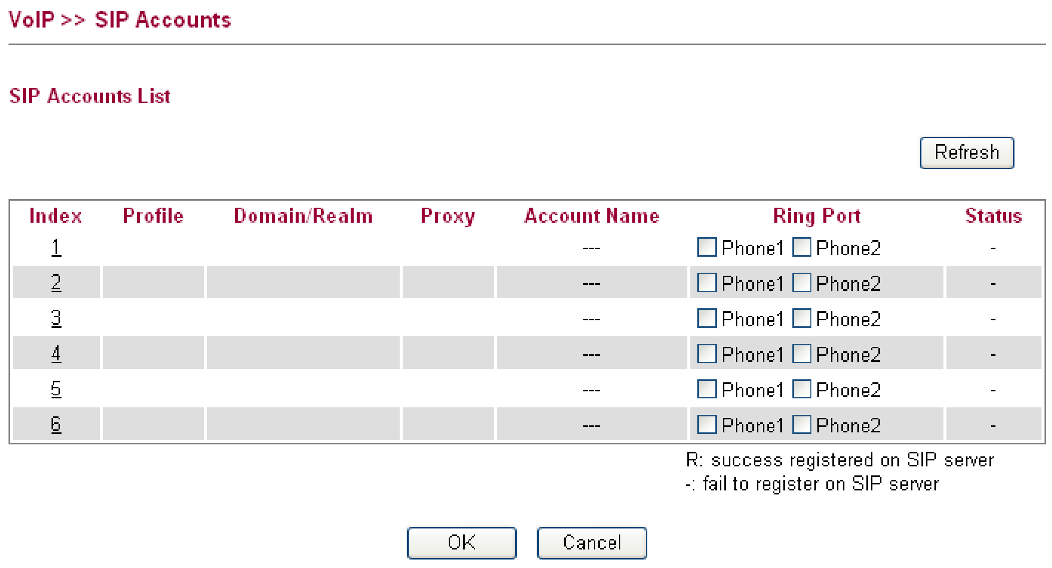
	end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.

4.12.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

Note: Selection items for **Ring Port** will differ according to the router you have.



VoIP >> SIP Accounts

SIP Accounts List

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1				---	□ Phone1 □ Phone2	-
2				---	□ Phone1 □ Phone2	-
3				---	□ Phone1 □ Phone2	-
4				---	□ Phone1 □ Phone2	-
5				---	□ Phone1 □ Phone2	-
6				---	□ Phone1 □ Phone2	-

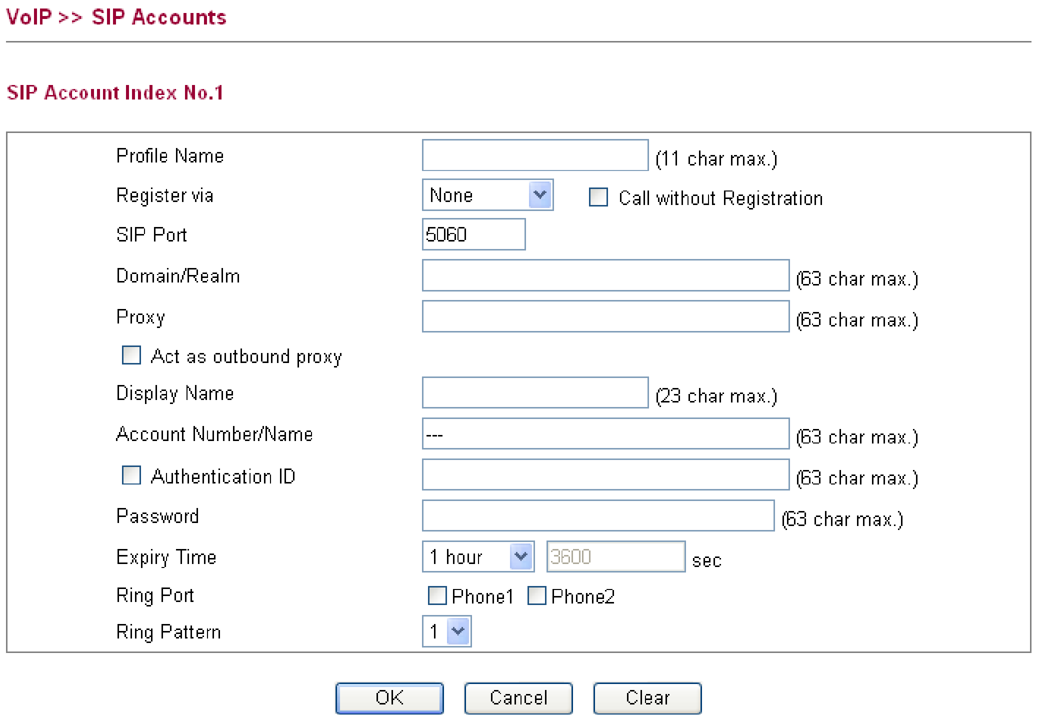
R: success registered on SIP server
-: fail to register on SIP server

Available settings are explained as follows:

Item	Description
Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @..
Ring Port	Specify which port will ring when receiving a phone call.

Status	Show the status for the corresponding SIP account. **R** means such account is registered on SIP server successfully. **–** means the account is failed to register on SIP server.

Click any index number to access into the following page.

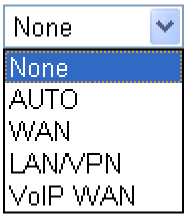


VoIP >> SIP Accounts

SIP Account Index No.1

Profile Name	(11 char max.)
Register via	None ☐ Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
☐ Act as outbound proxy	
Display Name	(23 char max.)
Account Number/Name	--- (63 char max.)
☐ Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 3600 sec
Ring Port	☐ Phone1 ☐ Phone2
Ring Pattern	1

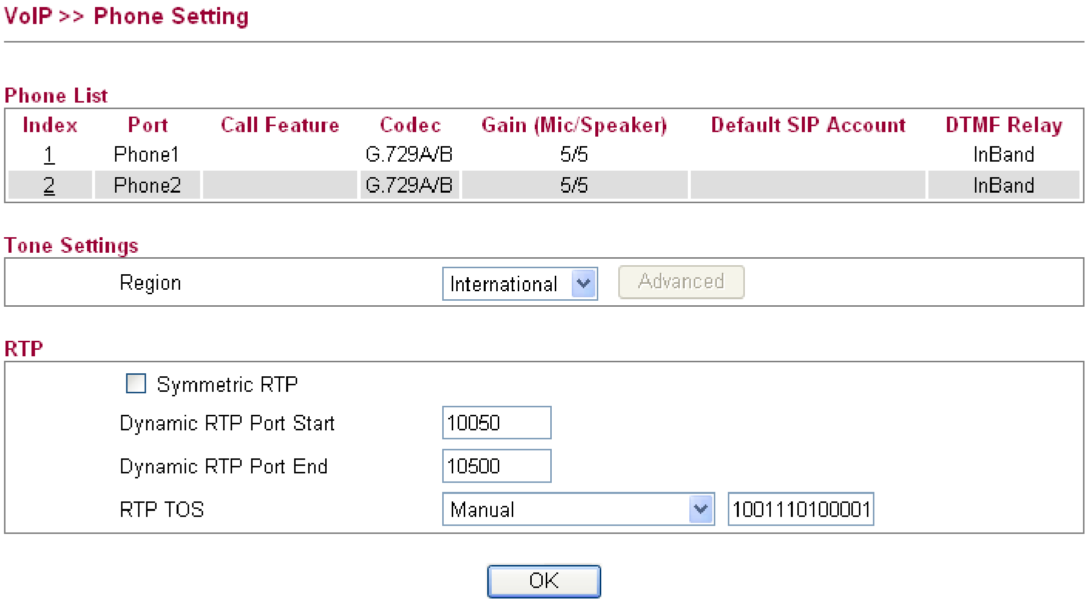
Available settings are explained as follows:

Item	Description
Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.
Register via	If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of **Call without Registration**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call. 
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is **5060.** Your peer

	must set the same value in his/her Registrar.
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type **:port number** after the domain name to specify that port as the destination of data transmission (e.g., **nat.draytel.org:5065**)
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.
Display Name	The caller-ID that you want to be displayed on your friend's screen.
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.
Password	The password provided to you when you registered with a SIP service.
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.
Ring Pattern	Choose a ring tone type for the VoIP phone call.

4.12.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.



VoIP >> Phone Setting

Phone List

Index	Port	Call Feature	Codec	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1		G.729A/B	5/5		InBand
2	Phone2		G.729A/B	5/5		InBand

Tone Settings

Region: International

RTP

□ Symmetric RTP

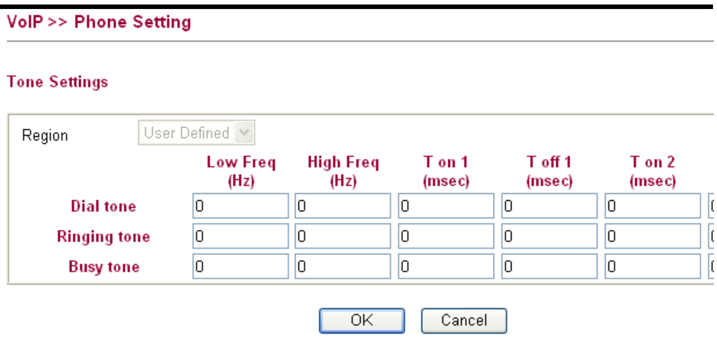
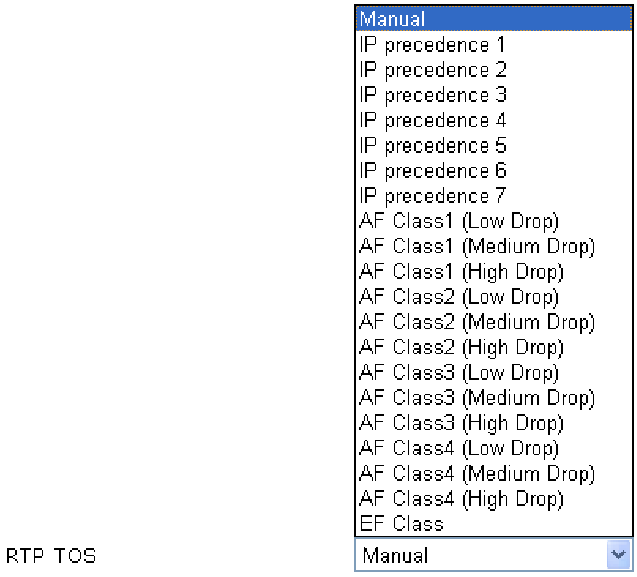
Dynamic RTP Port Start: 10050

Dynamic RTP Port End: 10500

RTP TOS: Manual 1001110100001

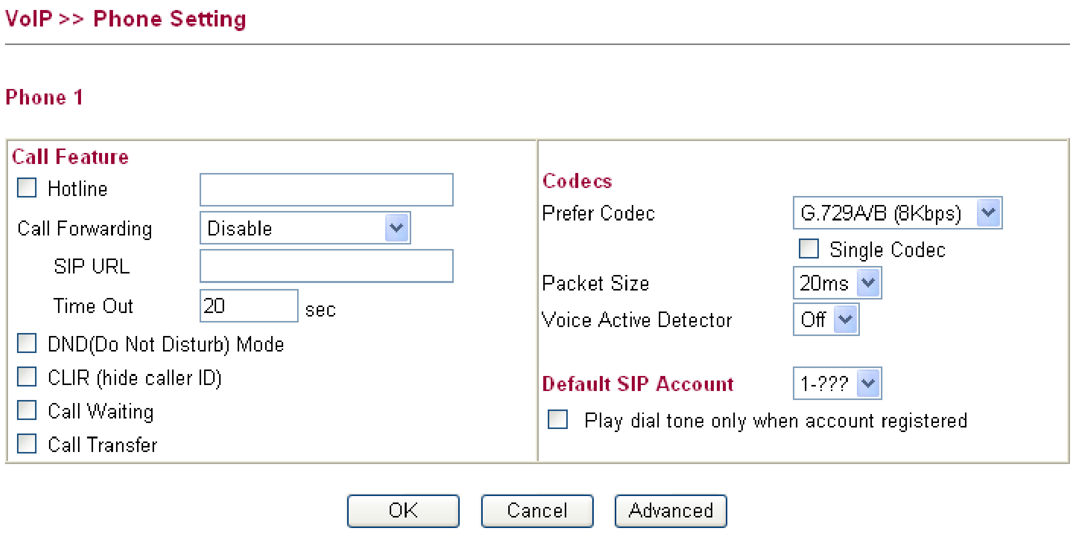
Available settings are explained as follows:

Item	Description
Phone List	**Port –** there are two phone ports provided here for you to configure. **Phone1/Phone2** allows you to set general settings for PSTN phones. **Call Feature** – A brief description for call feature will be shown in this field for your reference. **Codec** – Display the codec used for such phone entry. **Gain** - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index. **Default SIP Account** – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port. **DTMF Relay** – Display DTMF mode that configured in the advanced settings page of Phone Index.
Tone Settings	**Region –** Select the proper region which you are located. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone. If you choose **User Defined**, the Advanced button will be available for you to click to set the detailed configuration. **Advanced** setting allows you to adjust tone settings manually if you choose **User Defined**. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

	 VoIP >> Phone Setting Tone Settings Region: User Defined Columns: Low Freq (Hz), High Freq (Hz), T on 1 (msec), T off 1 (msec), T on 2 (msec) Dial tone: 0, 0, 0, 0, 0 Ringing tone: 0, 0, 0, 0, 0 Busy tone: 0, 0, 0, 0, 0 OK Cancel Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.
RTP	**Symmetric RTP** – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem. **Dynamic RTP Port Start** - Specifies the start port for RTP stream. The default value is 10050. **Dynamic RTP Port End** - Specifies the end port for RTP stream. The default value is 15000. **RTP TOS** – It decides the level of VoIP package. Use the drop down list to choose any one of them.  Manual IP precedence 1 IP precedence 2 IP precedence 3 IP precedence 4 IP precedence 5 IP precedence 6 IP precedence 7 AF Class1 (Low Drop) AF Class1 (Medium Drop) AF Class1 (High Drop) AF Class2 (Low Drop) AF Class2 (Medium Drop) AF Class2 (High Drop) AF Class3 (Low Drop) AF Class3 (Medium Drop) AF Class3 (High Drop) AF Class4 (Low Drop) AF Class4 (Medium Drop) AF Class4 (High Drop) EF Class RTP TOS: Manual

Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.



VoIP >> Phone Setting

Phone 1

Call Feature

□ Hotline

Call Forwarding: Disable

SIP URL

Time Out: 20 sec

□ DND(Do Not Disturb) Mode

□ CLIR (hide caller ID)

□ Call Waiting

□ Call Transfer

Codecs

Prefer Codec: G.729A/B (8Kbps)

□ Single Codec

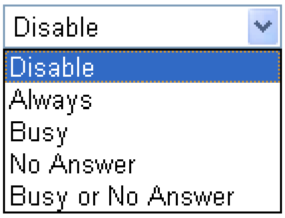
Packet Size: 20ms

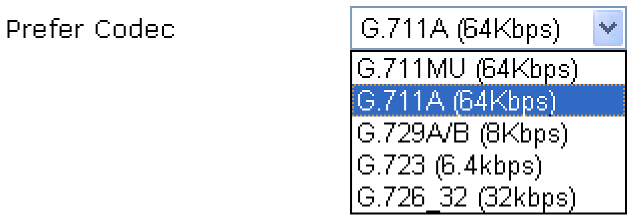
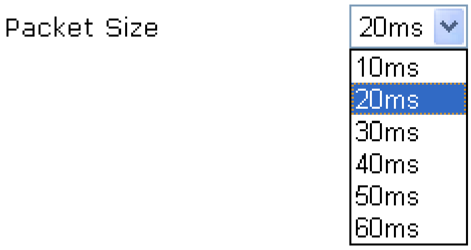
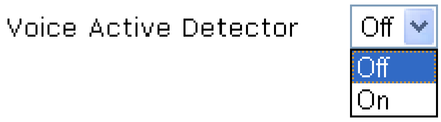
Voice Active Detector: Off

Default SIP Account: 1-???

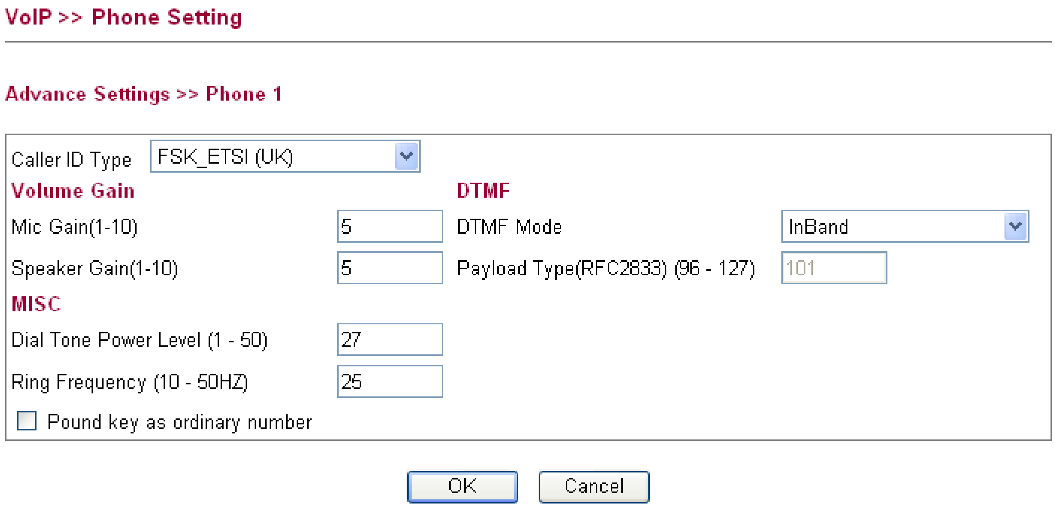
□ Play dial tone only when account registered

Available settings are explained as follows:

Item	Description
Call Feature	**Hotline-** Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set. **Call Forwarding-** There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No Answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.  Disable Disable Always Busy No Answer Busy or No Answer **SIP URL** – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. **Time Out** – Set the time out for the call forwarding. The default setting is 30 sec. **DND (Do Not Disturb) mode-** Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone. **CLIR (hide caller ID)-** Check this box to hide the caller ID on the display panel of the phone set. **Call Waiting-** Check this box to invoke this function. A

	notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call. **Call Transfer-** Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.
Codecs	**Prefer Codec-** Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.  Prefer Codec G.711A (64Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps) If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. **Single Codec** – If the box is checked, only the selected Codec will be applied. **Packet Size-** The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.  Packet Size 20ms 10ms 20ms 30ms 40ms 50ms 60ms **Voice Active Detection-** This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.  Voice Active Detector Off Off On
Default SIP Account	You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting. **Play dial tone only when account registered -** Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong settings might cause inconvenience for users.



VoIP >> Phone Setting

Advance Settings >> Phone 1

Caller ID Type: FSK_ETSI (UK)

Volume Gain

Mic Gain(1-10): 5

Speaker Gain(1-10): 5

MISC

Dial Tone Power Level (1 - 50): 27

Ring Frequency (10 - 50HZ): 25

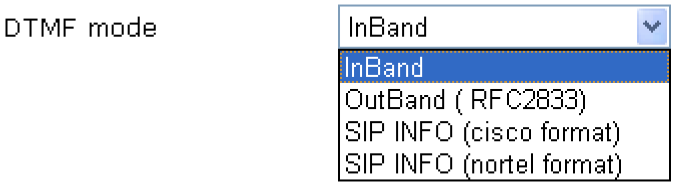
□ Pound key as ordinary number

DTMF

DTMF Mode: InBand

Payload Type(RFC2833) (96 - 127): 101

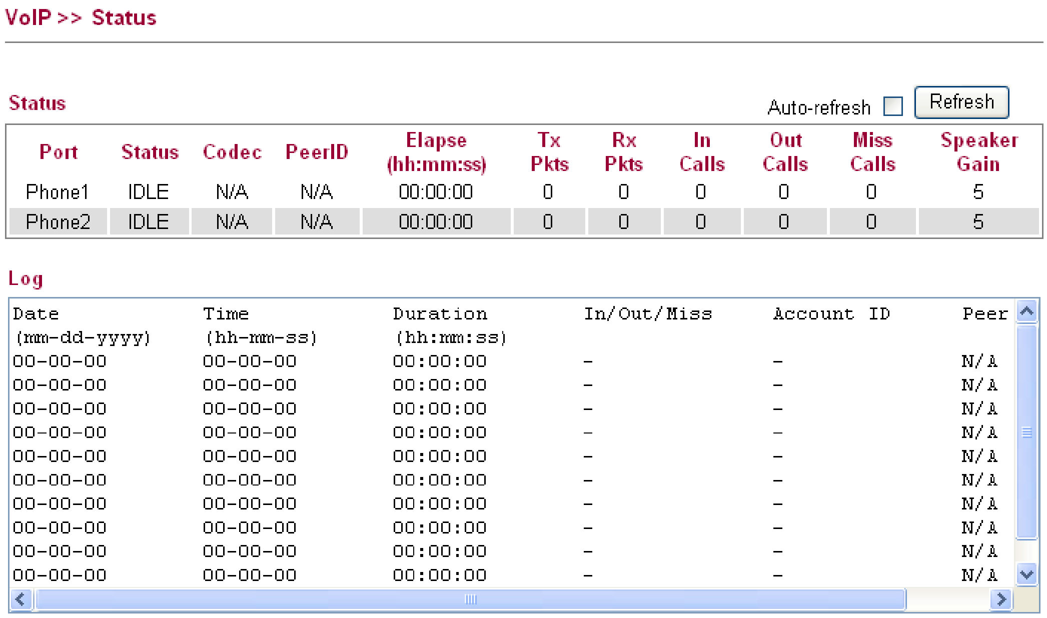
Available settings are explained as follows:

Item	Description
Caller ID Type	Choose one of the selections as caller ID type.
Volume Gain	**Mic Gain (1-10)/Speaker Gain (1-10)** - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.
MISC	**Dial Tone Power Level** - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. **Ring Frequency** - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting. **Pound key as ordinary number –** Check this box to make "#" key can be sent out as a number.
DTMF	**DTMF Mode –** There are four DTMF modes for you to choose.  DTMF mode: InBand InBand OutBand (RFC2833) SIP INFO (cisco format) SIP INFO (nortel format) ***InBand*** - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone ***OutBand*** - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function

	is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. ***SIP INFO***- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message. **Payload Type (rfc2833) -** Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

4.12.4 Status

From this page, you can find codec, connection and other important call status for each port.



VoIP >> Status

Status

Auto-refresh □ Refresh

Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	In Calls	Out Calls	Miss Calls	Speaker Gain
Phone1	IDLE	N/A	N/A	00:00:00	0	0	0	0	0	5
Phone2	IDLE	N/A	N/A	00:00:00	0	0	0	0	0	5

Log

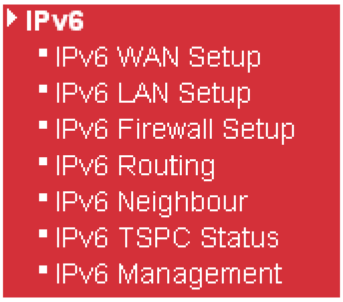
```
Date          Time          Duration      In/Out/Miss    Account ID     Peer
(mm-dd-yyyy)  (hh-mm-ss)    (hh:mm:ss)
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
00-00-00      00-00-00      00:00:00      -              -              N/A
```

Each item is explained as follows:

Item	Description
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click it to reload the page.
Port	It shows the VoIP connection status. **IDLE** - Indicates that the VoIP function is idle. **HANG_UP** - Indicates that the connection is not established (busy tone). **CONNECTING** - Indicates that the user is calling out. **WAIT_ANS** - Indicates that a connection is launched and waiting for remote user's answer. **ALERTING** - Indicates that a call is coming. **ACTIVE**-Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be

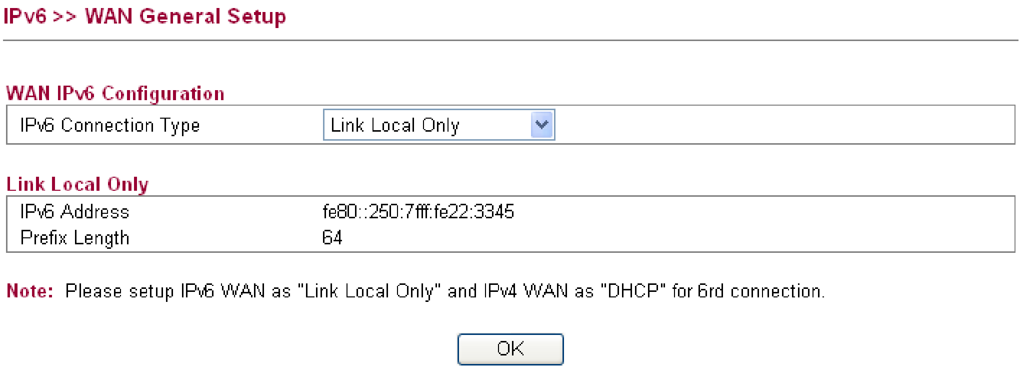
	IP or Domain).
Elapse	The format is represented as hours:minutes:seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.
Rx Pkts	Total number of received voice packets during this connection session.
Rx Losts	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

4.13 IPv6



4.13.1 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

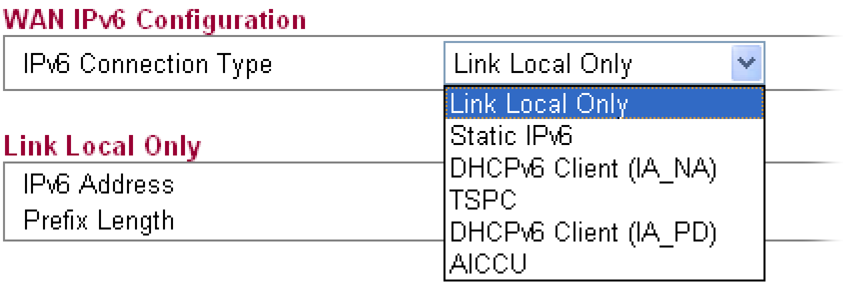
IPv6 Connection Type	Link Local Only

Link Local Only

IPv6 Address	fe80::250:7fff:fe22:3345
Prefix Length	64

Note: Please setup IPv6 WAN as "Link Local Only" and IPv4 WAN as "DHCP" for 6rd connection.

There are six IPv6 Connection Types for you to choose.



WAN IPv6 Configuration

IPv6 Connection Type: Link Local Only

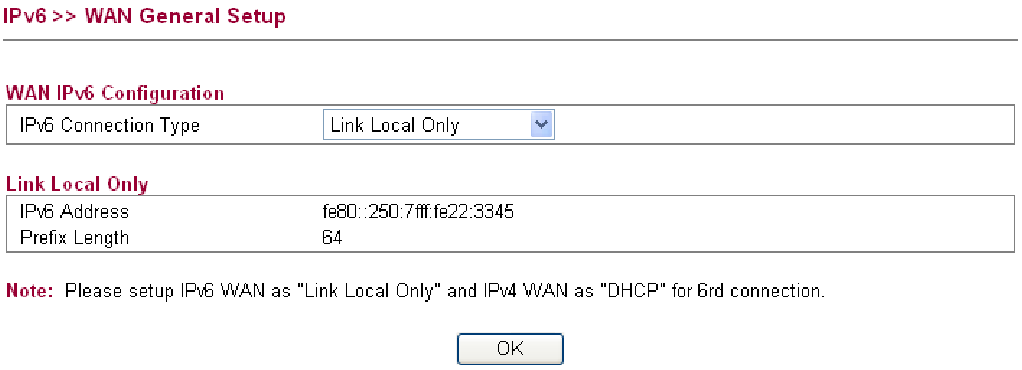
Link Local Only

IPv6 Address

Prefix Length

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:fe22:3345
Prefix Length	64

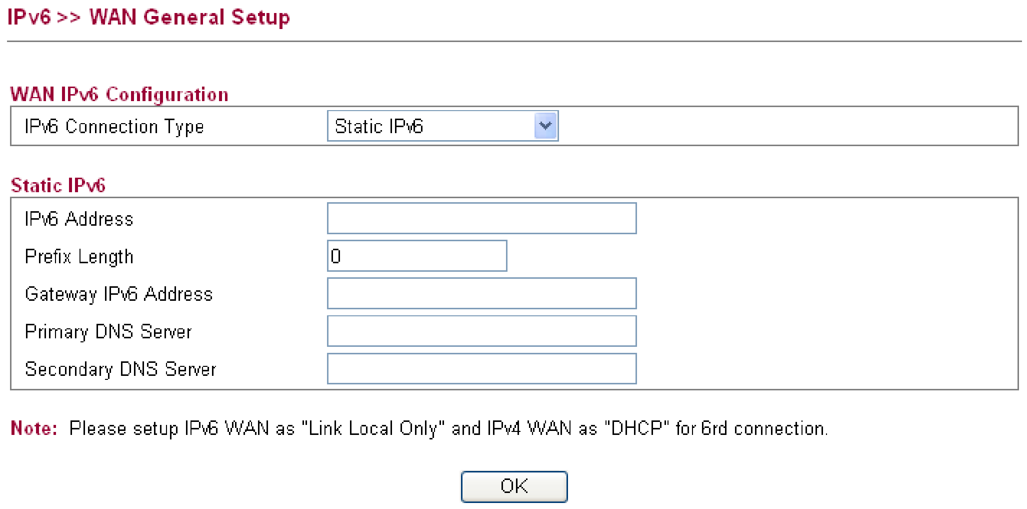
Note: Please setup IPv6 WAN as "Link Local Only" and IPv4 WAN as "DHCP" for 6rd connection.

Available settings are explained as follows:

Item	Description
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	

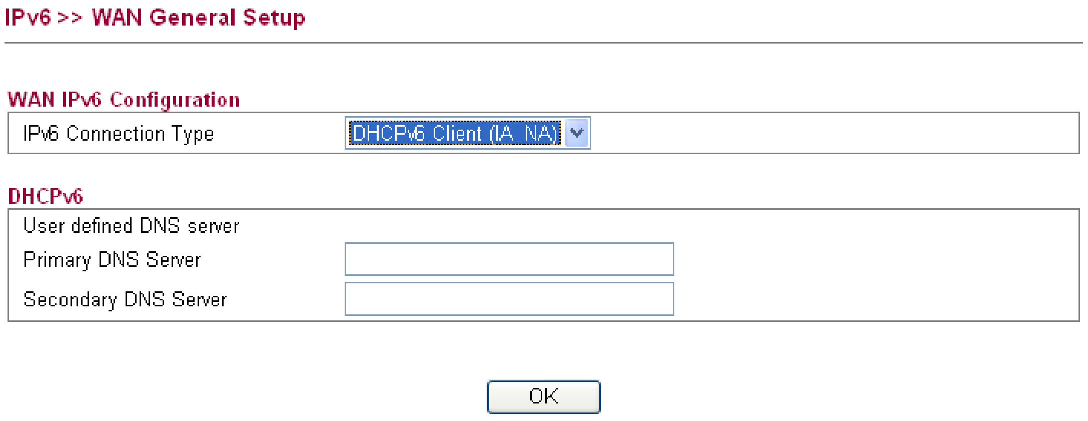
Note: Please setup IPv6 WAN as "Link Local Only" and IPv4 WAN as "DHCP" for 6rd connection.

Available settings are explained as follows:

Item	Description
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 (IA_NA)

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



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type	DHCPv6 Client (IA_NA)

DHCPv6

User defined DNS server	
Primary DNS Server	
Secondary DNS Server	

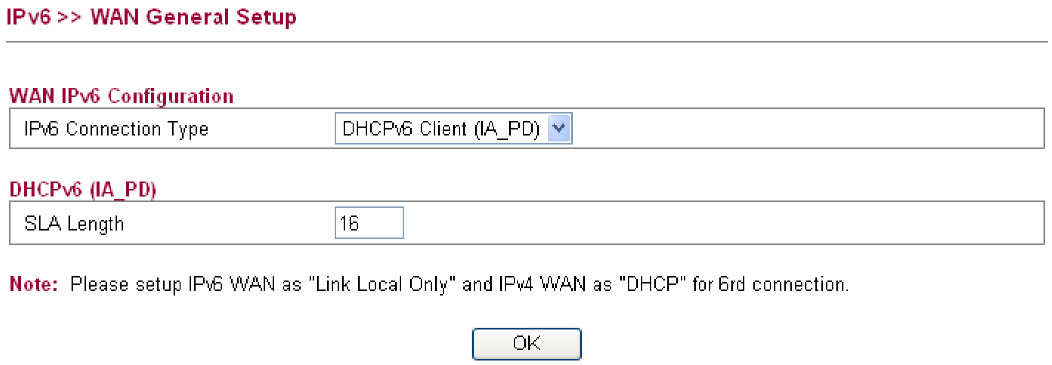
Available settings are explained as follows:

Item	Description
Primary DNS Server	Type primary DNS Server address here.

Secondary DNS Server	Type secondary DNS Server address here

DHCPv6 Client (IA_PD)

DHCPv6 client mode would use IA_PA option of DHCPv6 protocol to obtain IPv6 prefix from server.



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type: DHCPv6 Client (IA_PD)

DHCPv6 (IA_PD)

SLA Length: 16

Note: Please setup IPv6 WAN as "Link Local Only" and IPv4 WAN as "DHCP" for 6rd connection.

Available settings are explained as follows:

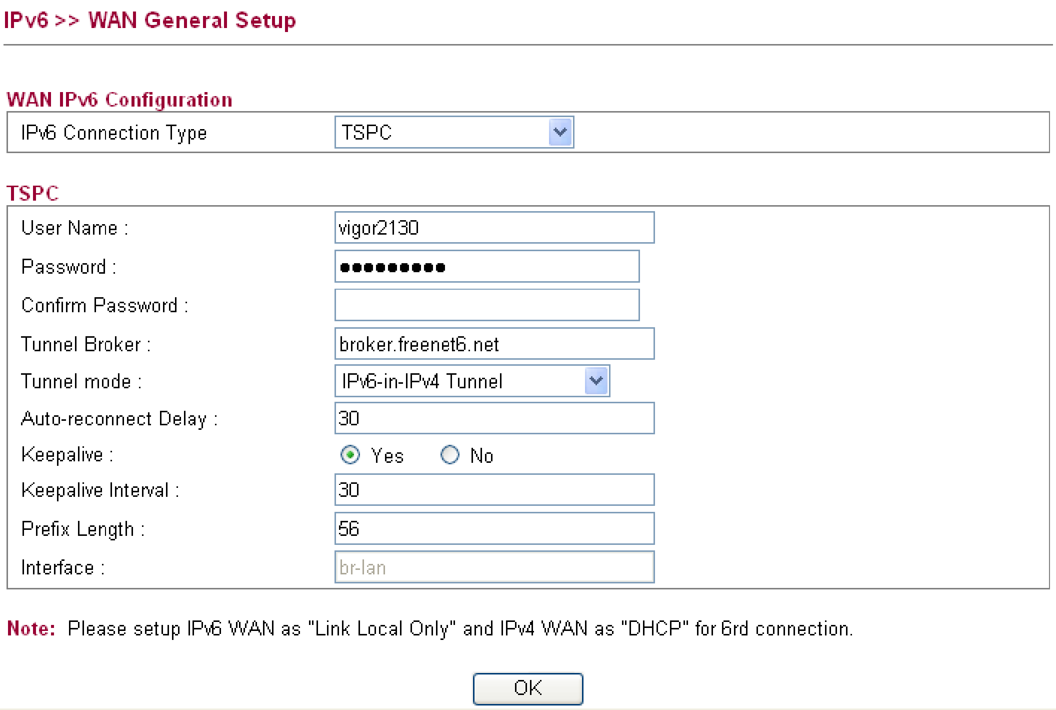
Item	Description
SLA Length	It is used by an individual organization to create its own local addressing hierarchy and to identify subnets.

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 the Internet.



IPv6 >> WAN General Setup

WAN IPv6 Configuration

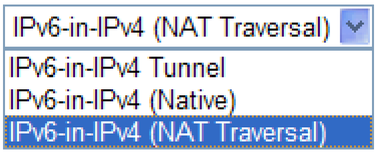
IPv6 Connection Type	TSPC

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
Prefix Length :	56
Interface :	br-lan

Note: Please setup IPv6 WAN as "Link Local Only" and IPv4 WAN as "DHCP" for 6rd connection.

Available settings are explained as follows:

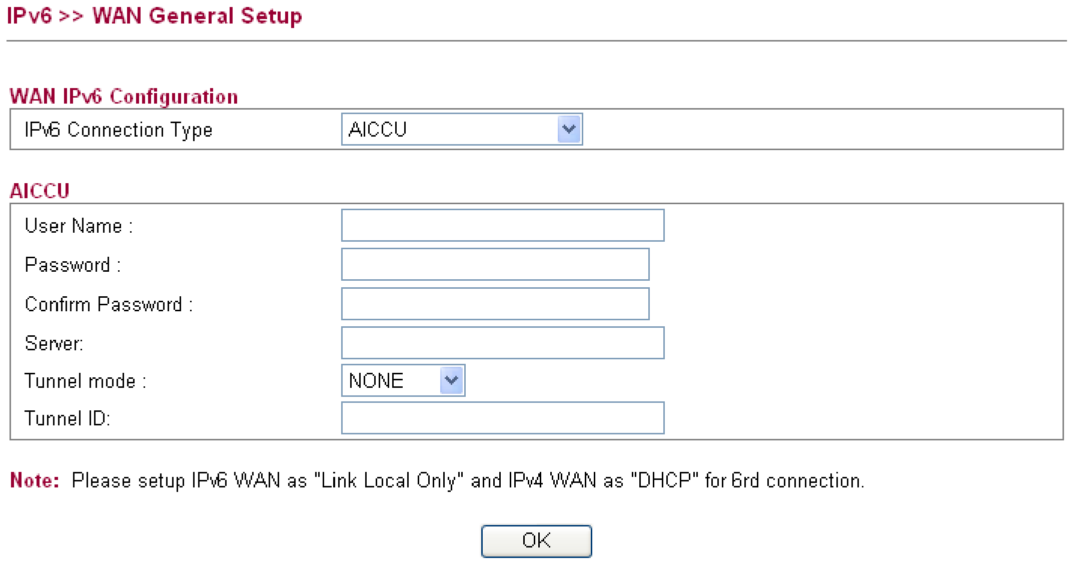
Item	Description
User Name	Type the name obtained from the broker. “Vigor1000” is a default username applied from http://go6.net/4105/register.asp. It is suggested for you to apply another username and password.
Password	Type the password assigned with the user name.
Confirm Password	Type the password 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 chose 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).  IPv6-in-IPv4 (NAT Traversal) IPv6-in-IPv4 Tunnel IPv6-in-IPv4 (Native) IPv6-in-IPv4 (NAT Traversal)
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.
Prefix Length	Type the required prefix length for the client network.
Interface	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 interface.

AICCU

It stands for **Automatic IPv6 Connectivity Client Utility** which can be used for NAT-Traversal and gets IPv6 connectivity easily.

This page defines the AICCU connection types for LAN interface.



IPv6 >> WAN General Setup

WAN IPv6 Configuration

IPv6 Connection Type: AICCU

AICCU

User Name :

Password :

Confirm Password :

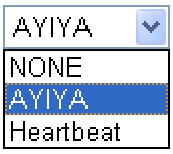
Server:

Tunnel mode : NONE

Tunnel ID:

Note: Please setup IPv6 WAN as "Link Local Only" and IPv4 WAN as "DHCP" for 6rd connection.

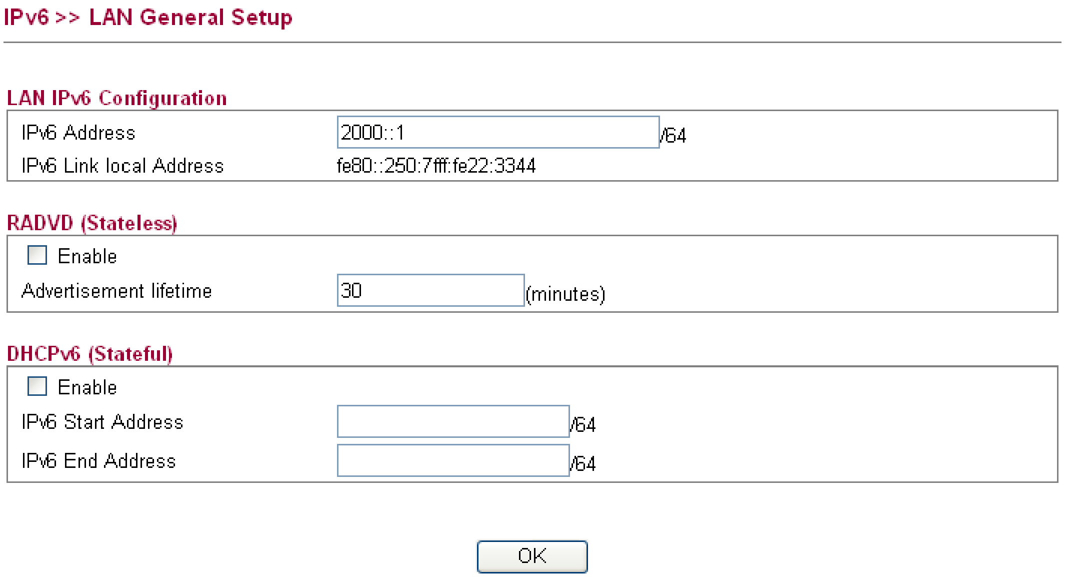
Available settings are explained as follows:

Item	Description
User Name	Type the name obtained from the service provider. It is suggested for you to apply another username and password from other ISP, such as http://www.sixxs.net/.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Server	Type the default server address, tic.sixxs.net.
Tunnel mode	Choose one of the tunnel modes
	 AYIYA NONE AYIYA Heartbeat **AYIYA** – allows tunnels to be created even behind

	firewalls and NAT's. **Heartbeat** – sends a packet to the PoP (Point of Presence, serving IPv6 in IPv4 tunnel), then enables the tunnel on the PoP side.
Tunnel ID	Each account applied by the user from AICCU service provider supports 2 or more services for IPv4 to IPv6/IPv6 to IPv4 with different tunnel IDs. Simply type tunnel ID characters obtained from AICCU service provider for IPv6 connection. For the default setting, simply use the word “any”. For more details, please refer to http://www.sixxs.net/tools/aiccu/ 。

4.13.2 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::250:7fff:fe22:3344

RADVD (Stateless)

□ Enable

Advertisement lifetime: 30 (minutes)

DHCPv6 (Stateful)

□ Enable

IPv6 Start Address: /64

IPv6 End Address: /64

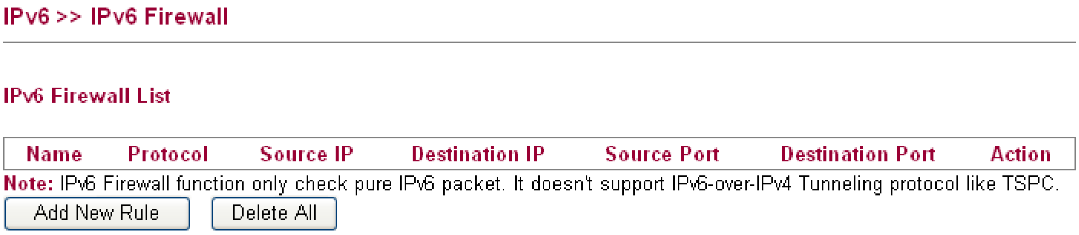
Available settings are explained as follows:

Item	Description
LAN IPv6 Configuration	**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.
RADVD (Stateless)	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 auto-configuration. **Enable -** Check this box to enable RADVD function for IPv6 connection. **Advertisement lifetime -** The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
DHCPv6 (Stateful)	**IPv6 Start Address/IPv6 End Address -** Type the start and end address for IPv6 server.

4.13.3 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

Note: IPv6 Firewall function only check pure IPv6 packet. It doesn't support IPv6-over-IPv4 Tunneling protocol like TSPC.

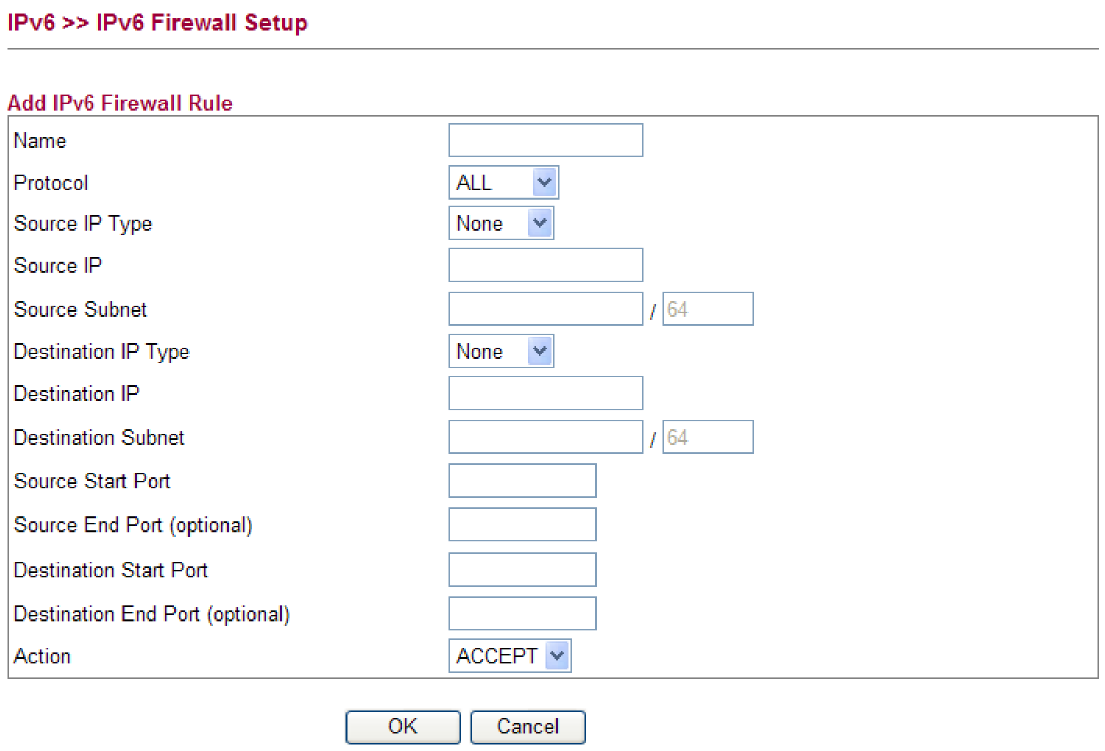
Each item is explained as follows:

Item	Description
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.

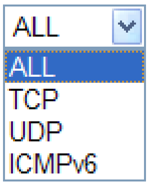
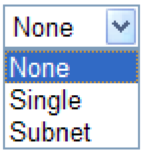
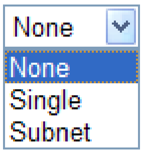


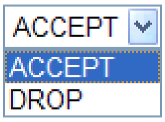
IPv6 >> IPv6 Firewall Setup

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

Available settings are explained as follows:

Item	Description
Name	Type a name for the rule.
Protocol	Specify a protocol for this rule.  ALL ALL TCP UDP ICMPv6
Source IP Type	Determine the IP type as the source.  None None Single Subnet
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.  None None Single Subnet
Destination IP	Type the IP address here if you choose **Single** as **Destination IP Type**.

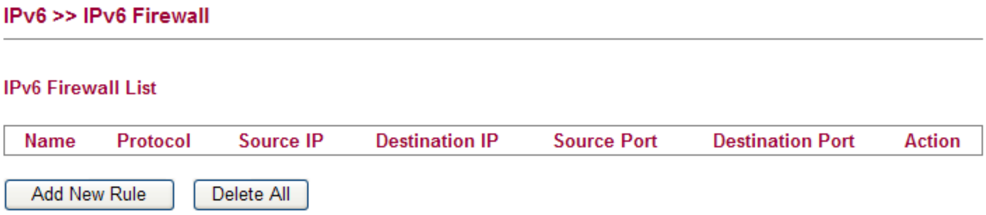
Item	Description
Destination Subnet	Type the subnet mask here if you choose **Subnet** as **Destination IP Type**.
Source Start Port	Type a value as the source start port. Such value will be available only TCP/UDP is selected as the protocol.
Source End Port (optional)	Type a value as the source end 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 ACCEPT DROP **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**.

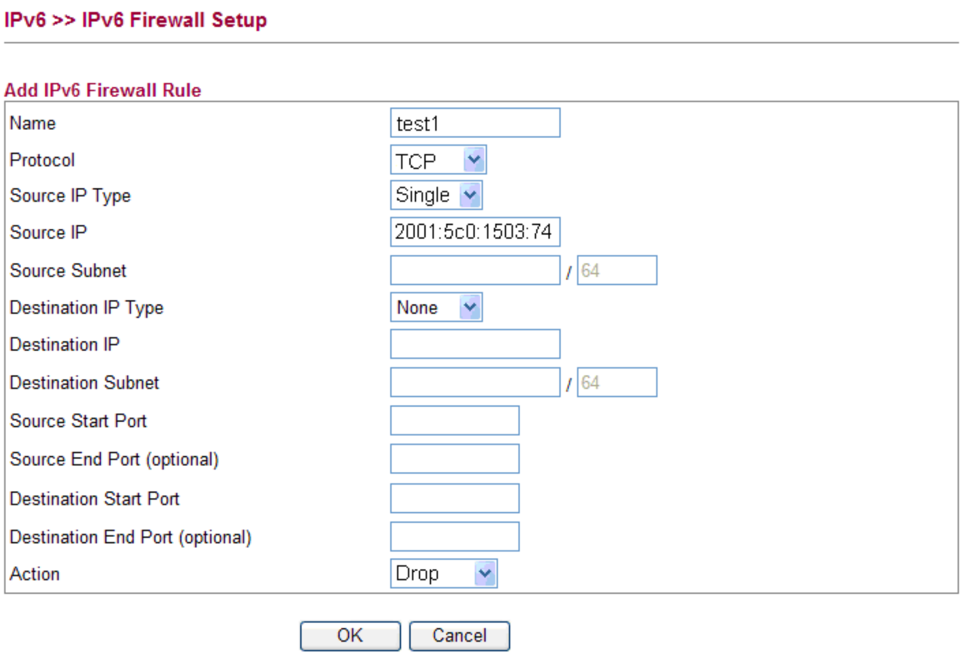


IPv6 >> IPv6 Firewall

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

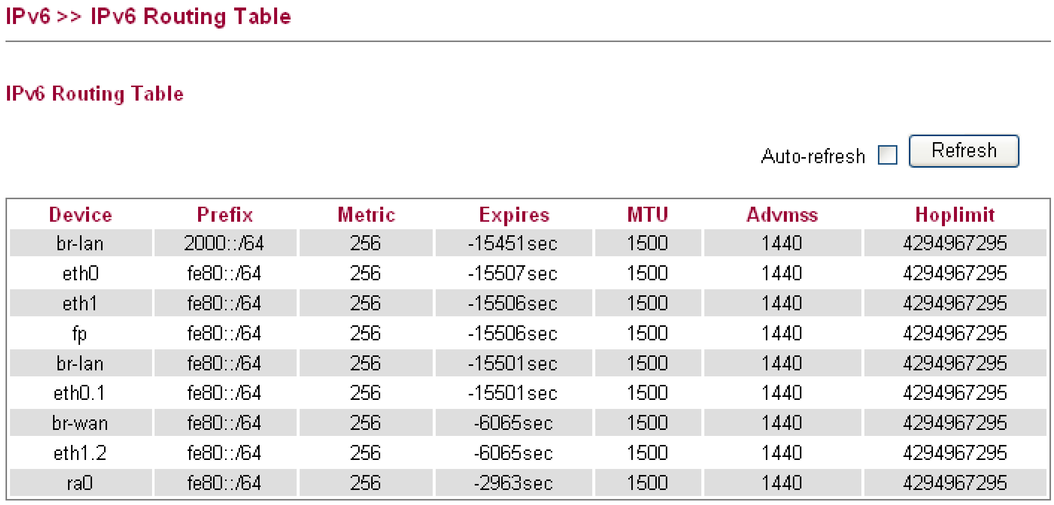
Name	test1
Protocol	TCP
Source IP Type	Single
Source IP	2001:5c0:1503:74
Source Subnet	/ 64
Destination IP Type	None
Destination IP	
Destination Subnet	/ 64
Source Start Port	
Source End Port (optional)	
Destination Start Port	
Destination End Port (optional)	
Action	Drop

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

4.13.4 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
br-lan	2000::/64	256	-15451sec	1500	1440	4294967295
eth0	fe80::/64	256	-15507sec	1500	1440	4294967295
eth1	fe80::/64	256	-15506sec	1500	1440	4294967295
fp	fe80::/64	256	-15506sec	1500	1440	4294967295
br-lan	fe80::/64	256	-15501sec	1500	1440	4294967295
eth0.1	fe80::/64	256	-15501sec	1500	1440	4294967295
br-wan	fe80::/64	256	-6065sec	1500	1440	4294967295
eth1.2	fe80::/64	256	-6065sec	1500	1440	4294967295
ra0	fe80::/64	256	-2963sec	1500	1440	4294967295

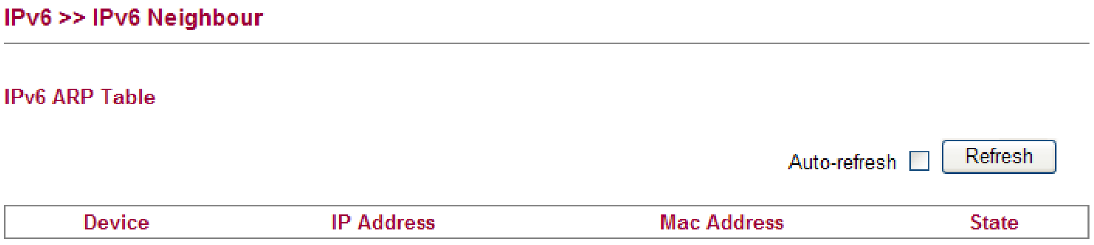
Each item is explained as follows:

Item	Description
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).

Item	Description
	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.
Refresh	Click it to reload the page.

4.13.5 IPv6 Neighbour

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



Device	IP Address	Mac Address	State

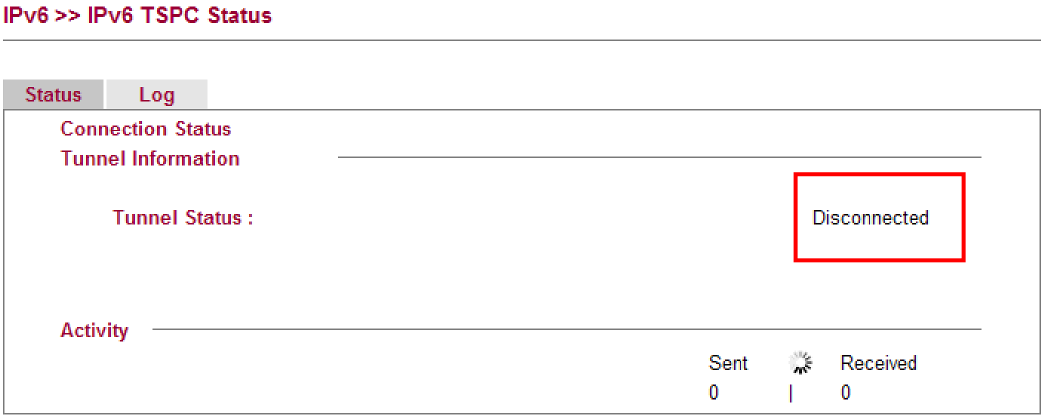
Each item is explained as follows:

Item	Description
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.
Refresh	Click it to reload the page.

4.13.6 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

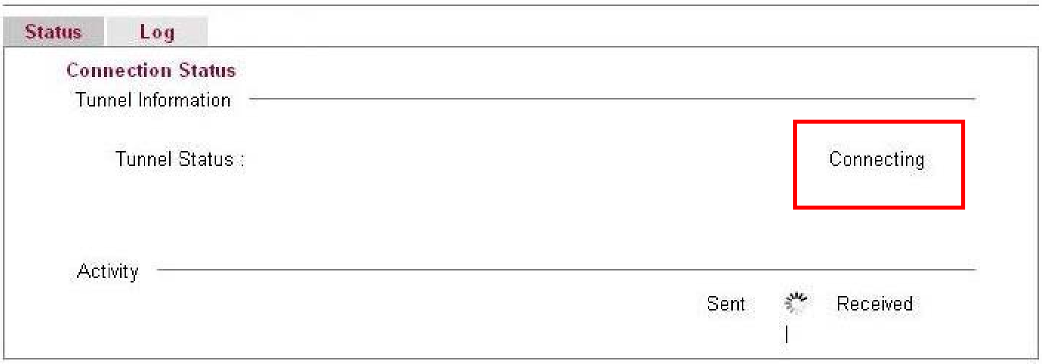
Tunnel Information

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

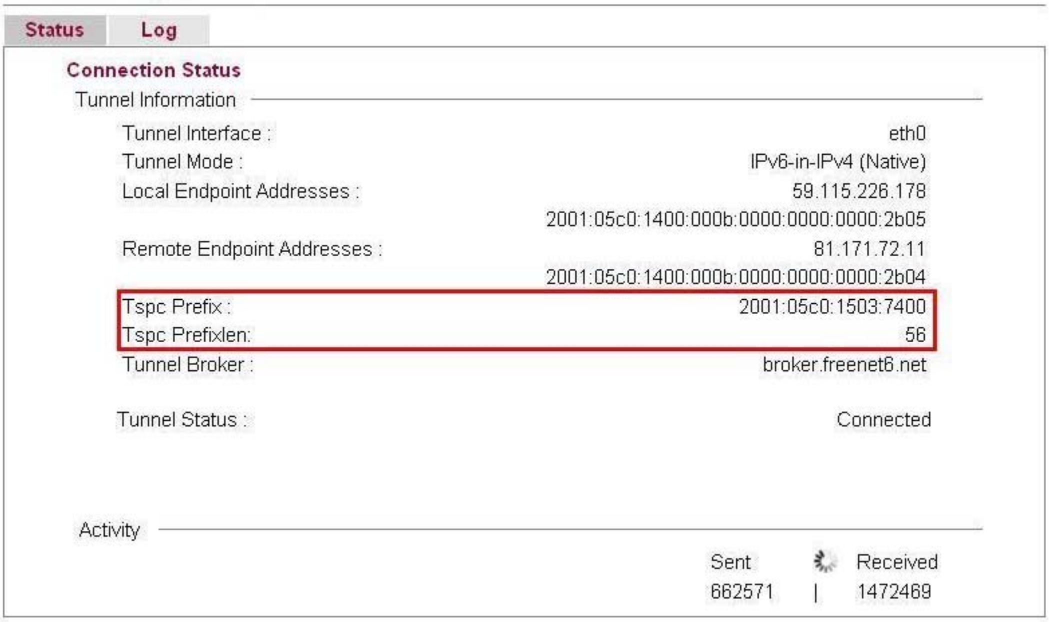
Tunnel Information

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

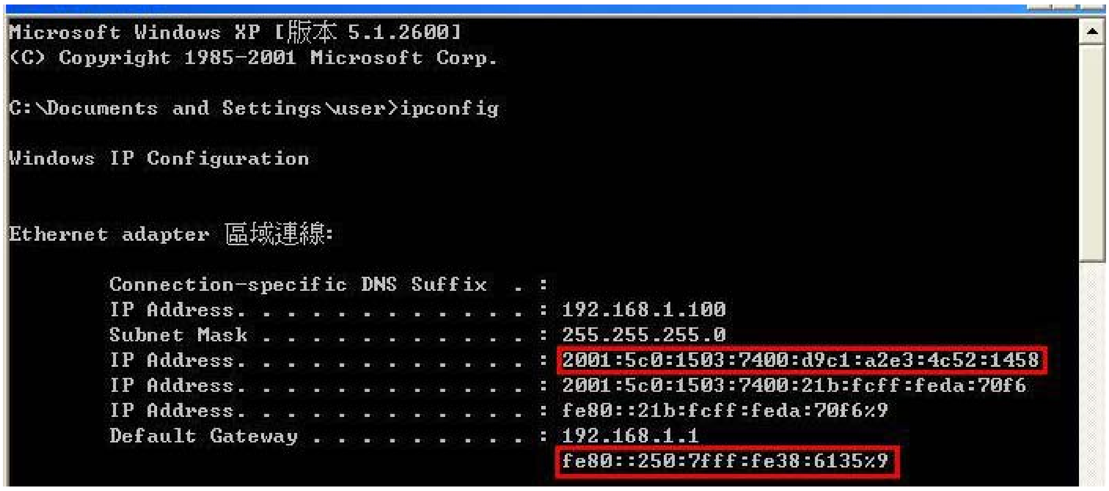
Activity

Sent		Received
662571	|	1472469

Each item is explained as follows:

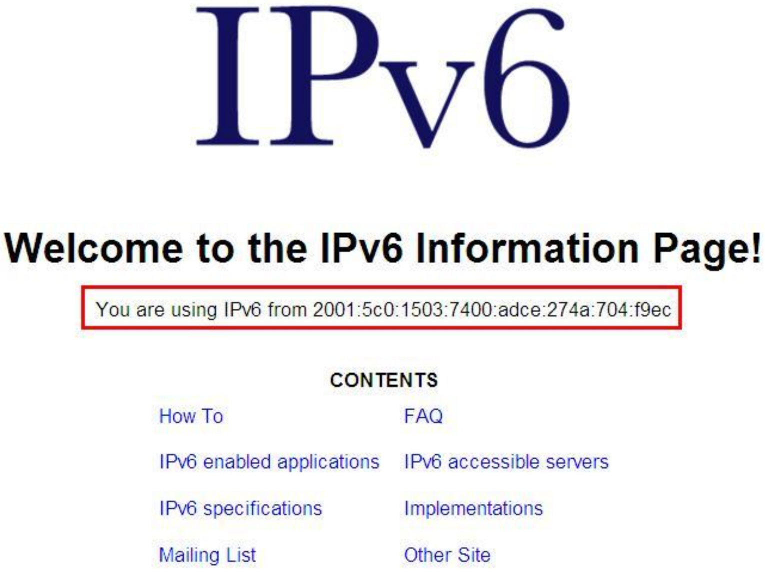
Item	Description
Connection Status	It will bring out different pages to represent IPv6 disconnection, connecting and connected.
Tunnel Information	Display interface name (used to send TSPC prefix), tunnel mode, local endpoint addresses, remote endpoint address, TSPC Prfix, TSPC Prefixlen (prefix length), 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!

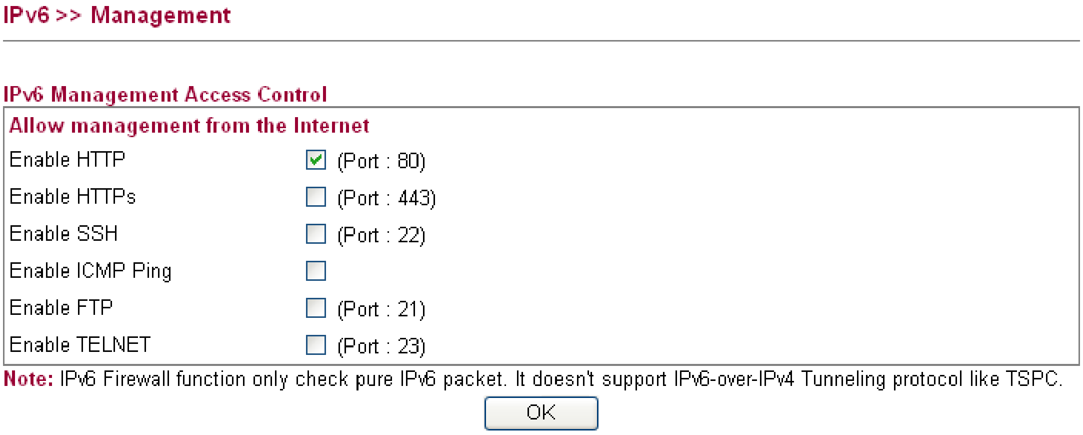
You are using IPv6 from 2001:5c0:1503:7400:adce:274a:704:f9ec

CONTENTS

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

4.13.7 IPv6 Management

This page allows you to manage the settings for IPv6 access control including settings of HTTP, HTTPs, SSH, FTP and TELNET by using IPv6 protocol. Check the box and type the port number respectively to enable the remote management of services.



IPv6 >> Management

IPv6 Management Access Control

Allow management from the Internet

Enable HTTP	☑ (Port : 80)
Enable HTTPs	□ (Port : 443)
Enable SSH	□ (Port : 22)
Enable ICMP Ping	□
Enable FTP	□ (Port : 21)
Enable TELNET	□ (Port : 23)

Note: IPv6 Firewall function only check pure IPv6 packet. It doesn't support IPv6-over-IPv4 Tunneling protocol like TSPC.

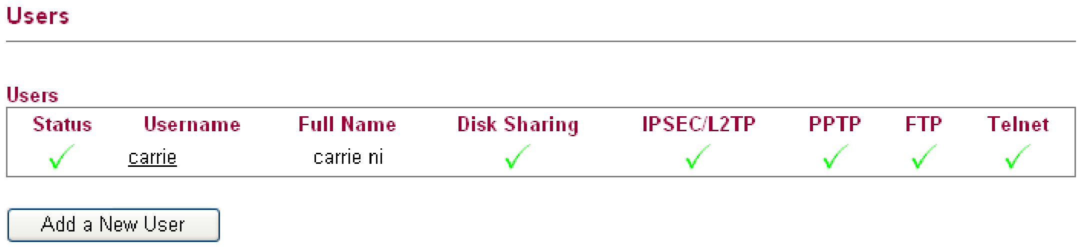
Available settings are explained as follows:

Item	Description
Allow management from the Internet	**Enable HTTP/HTTPS/SSH/ICMP Ping/FTP/TELNET** -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 the service.

4.14 User

4.14.1 User Configuration

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



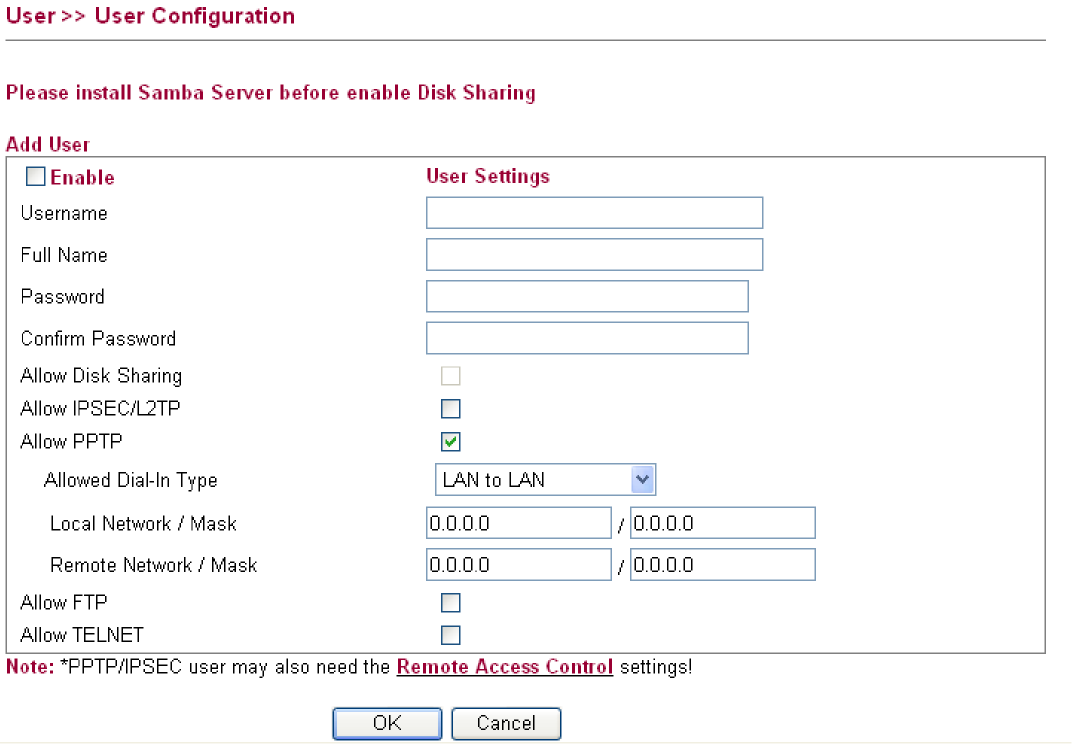
Users

Users

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

Adding a New User

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



User >> User Configuration

Please install Samba Server before enable Disk Sharing

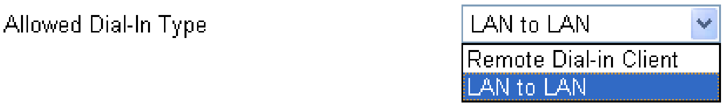
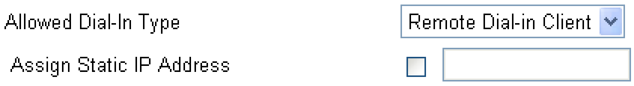
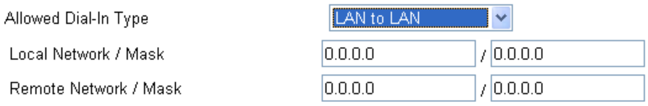
Add User

☐ Enable	User Settings
Username	
Full Name	
Password	
Confirm Password	
Allow Disk Sharing	☐
Allow IPSEC/L2TP	☐
Allow PPTP	☑
Allowed Dial-In Type	LAN to LAN
Local Network / Mask	0.0.0.0 / 0.0.0.0
Remote Network / Mask	0.0.0.0 / 0.0.0.0
Allow FTP	☐
Allow TELNET	☐

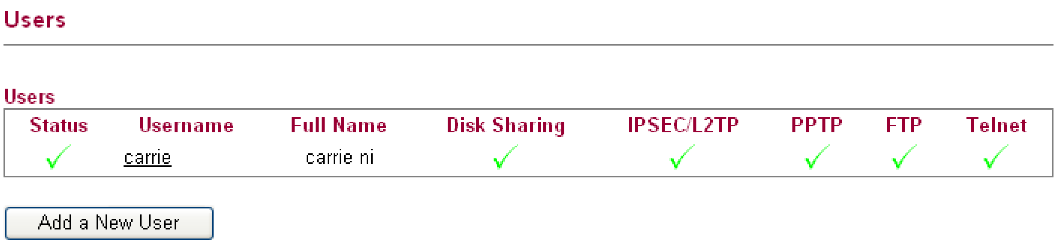
Note: *PPTP/IPSEC user may also need the Remote Access Control settings!

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such user profile.
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.

Item	Description
Allow Disk Sharing	Check this box to have the remote user share the disk information. Before enable this function, please install Samba Server first.
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**.**  Allowed Dial-In Type: LAN to LAN ● **Allowed Dial-In Type** ***Remote Dial-in Client***  Allowed Dial-In Type: Remote Dial-in Client Assign Static IP Address: □ **Assign Static IP Address –** Check the box and type the IP address. ● ***LAN to LAN***  Allowed Dial-In Type: LAN to LAN Local Network / Mask: 0.0.0.0 / 0.0.0.0 Remote Network / Mask: 0.0.0.0 / 0.0.0.0 When such user profile needs to have PPTP LAN to LAN connection, the following three items must be adjusted. **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.
Allow FTP	Check this box to let the remote user connecting to FTP server via this router.
Allow TELNET	Check this box to let the remote user to adjust the settings of router by TELNET.

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



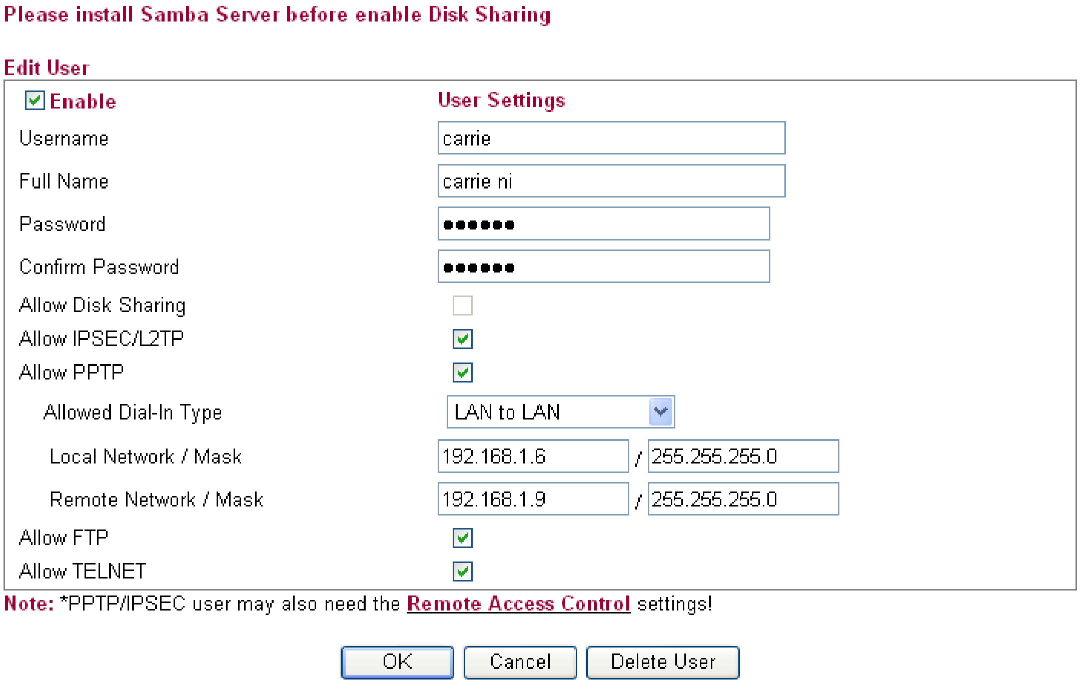
Users

Users

Status	Username	Full Name	Disk Sharing	IPSEC/L2TP	PPTP	FTP	Telnet
✓	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**.



Please install Samba Server before enable Disk Sharing

Edit User

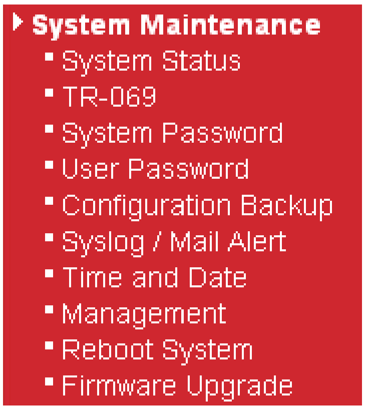
☑ Enable	User Settings
Username	carrie
Full Name	carrie ni
Password	••••••
Confirm Password	••••••
Allow Disk Sharing	□
Allow IPSEC/L2TP	☑
Allow PPTP	☑
Allowed Dial-In Type	LAN to LAN
Local Network / Mask	192.168.1.6 / 255.255.255.0
Remote Network / Mask	192.168.1.9 / 255.255.255.0
Allow FTP	☑
Allow TELNET	☑

Note: *PPTP/IPSEC user may also need the Remote Access Control settings!

4.15 System Maintenance

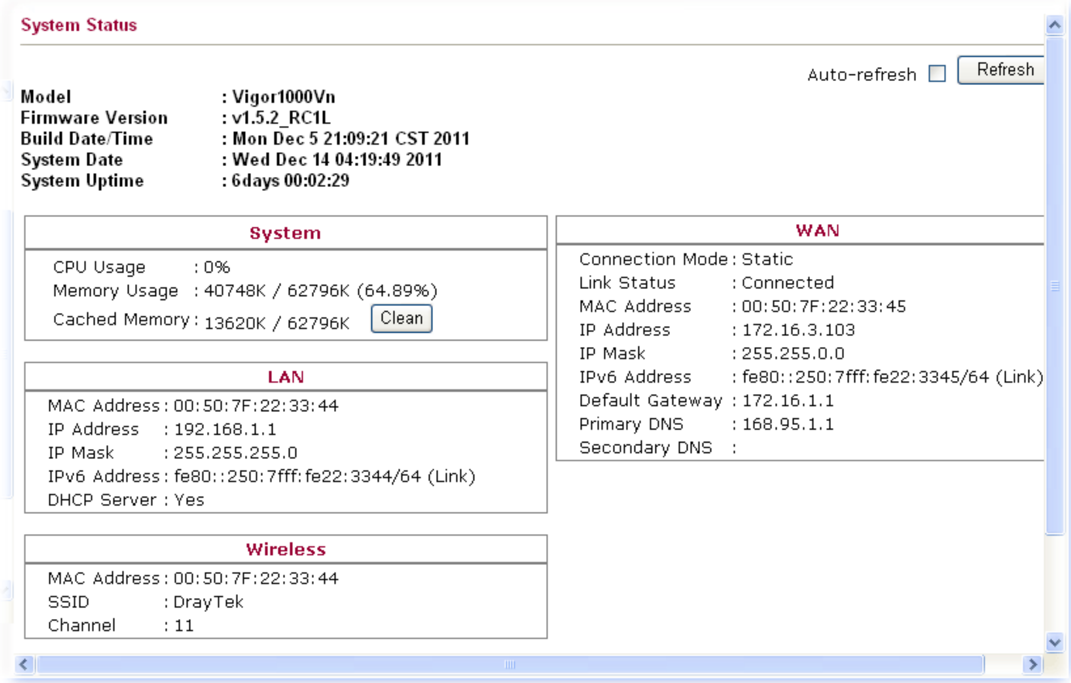
For the system setup, there are several items that you have to know the way of configuration: TR-069, System Password, User Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.15.1 System Status

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



System Status

Auto-refresh □ Refresh

Model : Vigor1000Vn
Firmware Version : v1.5.2_RC1L
Build Date/Time : Mon Dec 5 21:09:21 CST 2011
System Date : Wed Dec 14 04:19:49 2011
System Uptime : 6days 00:02:29

System

CPU Usage : 0%
Memory Usage : 40748K / 62796K (64.89%)
Cached Memory : 13620K / 62796K Clean

LAN

MAC Address : 00:50:7F:22:33:44
IP Address : 192.168.1.1
IP Mask : 255.255.255.0
IPv6 Address : fe80::250:7fff:fe22:3344/64 (Link)
DHCP Server : Yes

Wireless

MAC Address : 00:50:7F:22:33:44
SSID : DrayTek
Channel : 11

WAN

Connection Mode : Static
Link Status : Connected
MAC Address : 00:50:7F:22:33:45
IP Address : 172.16.3.103
IP Mask : 255.255.0.0
IPv6 Address : fe80::250:7fff:fe22:3345/64 (Link)
Default Gateway : 172.16.1.1
Primary DNS : 168.95.1.1
Secondary DNS :

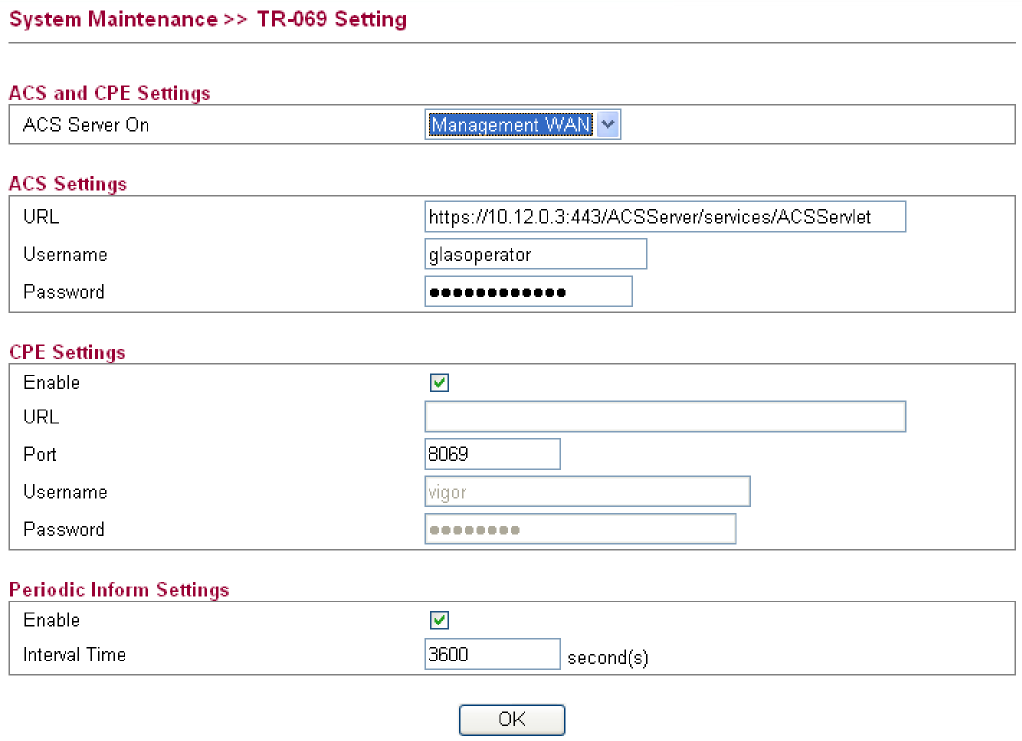
Each item is explained as follows:

Item	Description
Model	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware built.
System Date	Display current time and date for the system server.
System Uptime	Display the connection time for the system server.
System	**CPU Usage** - Display the percentage of the CPU usage of your system. **Memory Usage** - Display the size of the memory usage and the percentage. **Cached Memory** – Display the used cached memory and the remaining memory.
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. **IPv6 Address** - Display the link local IPv6 address of the LAN interface. **DHCP Server** - Display if the DHCP server is active or not.

Wireless	**MAC Address** - Display the MAC address of the wireless LAN. **SSID** - Display the SSID of the router. **Channel** Display the channel that wireless LAN used.
WAN	**Connection Mode** - Display current connection type used. **Link Status** - Display the connection status. **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.

4.15.2 TR-069

Vigor router with TR-069 is available for matching with VigorACS server. Such page provides VigorACS and CPE settings under TR-069 protocol. All the settings configured here is for CPE to be controlled and managed with VigorACS server. Users need to type URL, username and password for the VigorACS server that such device will be connected. However URL, username and password under CPE client are fixed that users cannot change it. The default CPE username and password are "vigor" and "password". You will need it when you configure VigorACS server.



System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server On	Management WAN

ACS Settings

URL	https://10.12.0.3:443/ACSServer/services/ACSServlet
Username	glasoperator
Password	●●●●●●●●●●●●●

CPE Settings

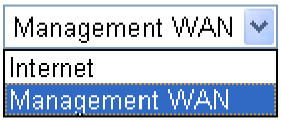
Enable	☑
URL	
Port	8069
Username	vigor
Password	●●●●●●●●

Periodic Inform Settings

Enable	☑
Interval Time	3600 second(s)

OK

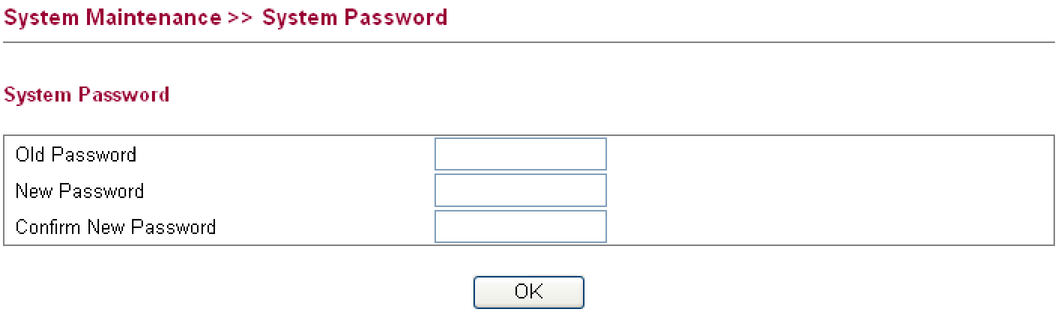
Available settings are explained as follows:

Item	Description
ACS and CEP Settings	**ACS Server On –** Choose the interface for the router connecting to ACS server.  Management WAN Internet Management WAN
ACS Settings	Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to VigorACS user's manual for detailed information. **URL** - Type the URL for VigorACS server. If the connected CPE needs to be authenticated, please set URL as the following and type username and password for VigorACS server: ***http://{IP address of VigorACS}:8080/ACSServer/services/ACSServlet*** If the connected CPE does not need to be authenticated please set URL as the following: ***http://{IP address of***

Item	Description
	VigorACS}:8080/ACSServer/services/UnAuthACSServlet **Username/Password -** Type username and password for ACS Server for authentication. For example, if you want to use such CPE with VigorACS, you can type as the following: **Username*: acs*** **Password*: password***
CPE Settings	Such information is useful for Auto Configuration Server. **Enable** – Check the box to allow the CPE Client to connect with Auto Configuration Server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **Username** – Type a name for VigorACS to access into Vigor router's web configurator. **Password** –Type a password for VigorACS to access into Vigor router's web configurator.
Periodic Inform Settings	**Enable –** Check the box for the system to send inform message to ACS server periodically (with the time set in the box of interval time). **Interval Time -** Please set interval time or schedule time for the router to send notification to CPE. Or uncheck **Enable** to close the mechanism of notification.

4.15.3 System Password

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



System Maintenance >> System Password

System Password

Old Password	
New Password	
Confirm New Password	

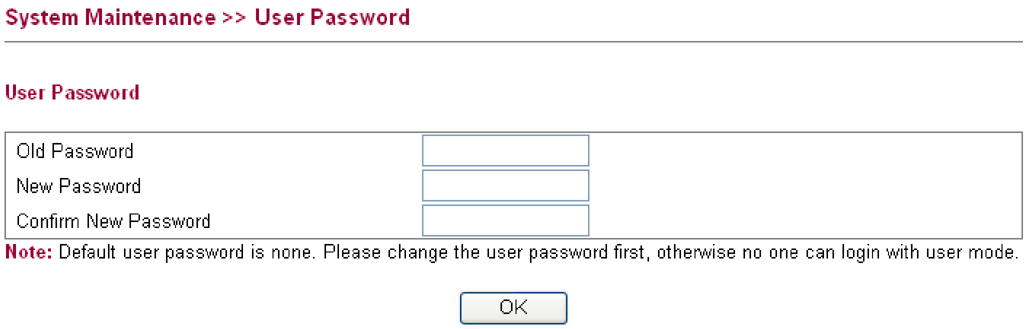
Available settings are explained as follows

Item	Description
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.

4.15.4 User Password

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



System Maintenance >> User Password

User Password

Old Password	
New Password	
Confirm New Password	

Note: Default user password is none. Please change the user password first, otherwise no one can login with user mode.

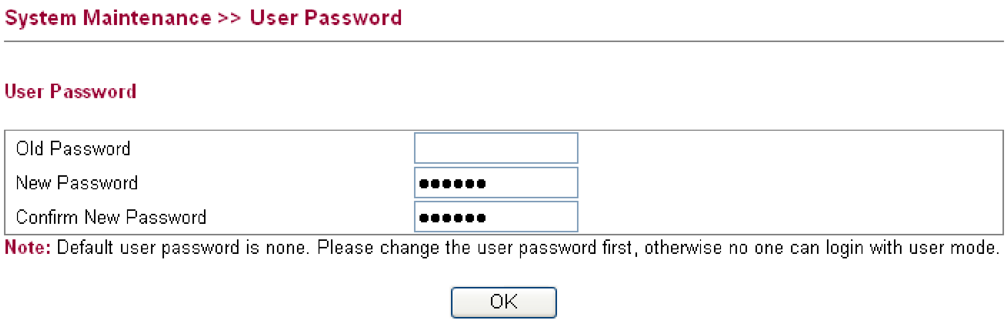
Available settings are explained as follows

Item	Description
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.

Below shows an example for accessing into User Operation with User Password.

1. Type a new password in the field of New Password and click **OK**.



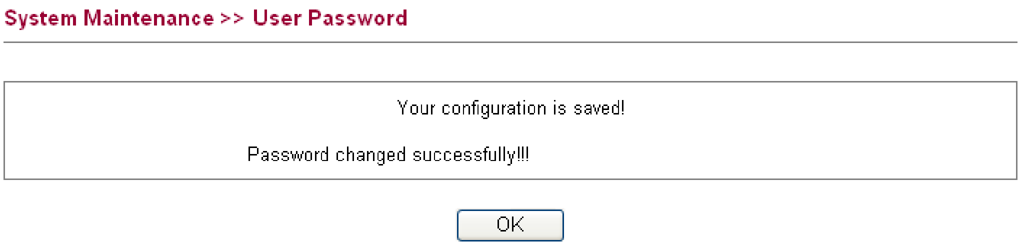
System Maintenance >> User Password

User Password

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

Note: Default user password is none. Please change the user password first, otherwise no one can login with user mode.

2. The following screen will appear. Simply click **OK**.

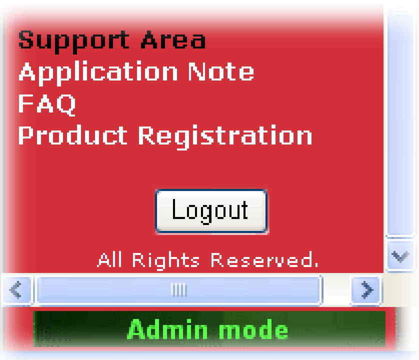


System Maintenance >> User Password

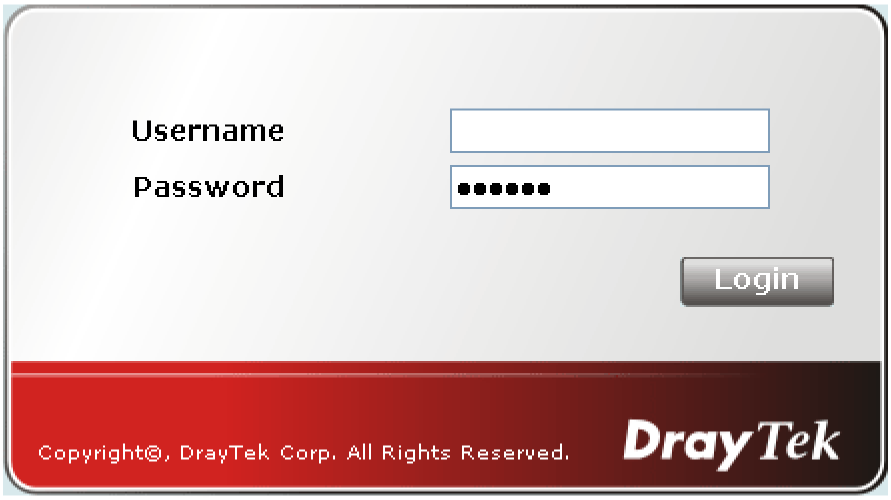
Your configuration is saved!

Password changed successfully!!!

3. Log out Vigor1000 Web Configurator.

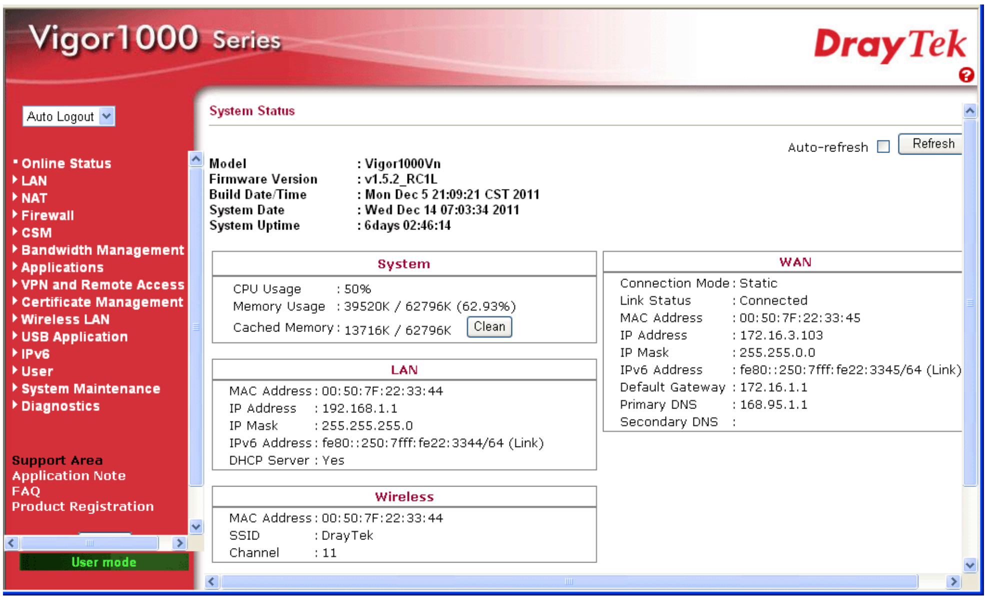


4. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.


Username

Password ●●●●●●

5. The main screen with User Mode will be shown as follows.



System Status

Auto-refresh □

```
Model               : Vigor1000Vn
Firmware Version    : v1.5.2_RC1L
Build Date/Time     : Mon Dec 5 21:09:21 CST 2011
System Date         : Wed Dec 14 07:03:34 2011
System Uptime       : 6days 02:46:14
```

System

```
CPU Usage      : 50%
Memory Usage   : 39520K / 62796K (62.93%)
Cached Memory  : 13716K / 62796K
```

LAN

```
MAC Address  : 00:50:7F:22:33:44
IP Address   : 192.168.1.1
IP Mask      : 255.255.255.0
IPv6 Address : fe80::250:7fff:fe22:3344/64 (Link)
DHCP Server  : Yes
```

Wireless

```
MAC Address : 00:50:7F:22:33:44
SSID        : DrayTek
Channel     : 11
```

WAN

```
Connection Mode : Static
Link Status     : Connected
MAC Address     : 00:50:7F:22:33:45
IP Address      : 172.16.3.103
IP Mask         : 255.255.0.0
IPv6 Address    : fe80::250:7fff:fe22:3345/64 (Link)
Default Gateway : 172.16.1.1
Primary DNS     : 168.95.1.1
Secondary DNS   :
```

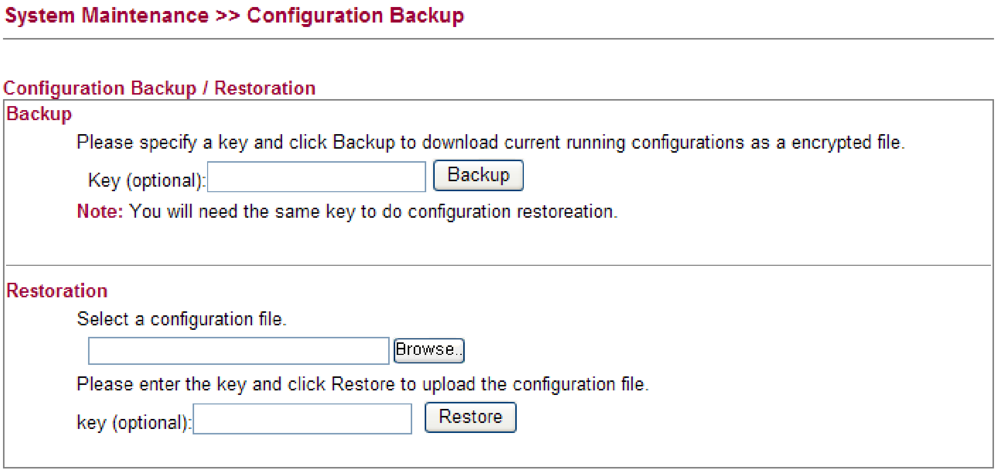
Settings to be configured in User Mode will be less than settings in Admin Mode.

4.15.5 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.

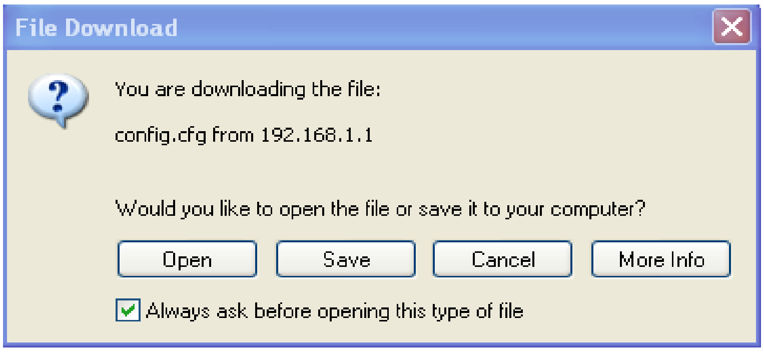
Restoration

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.



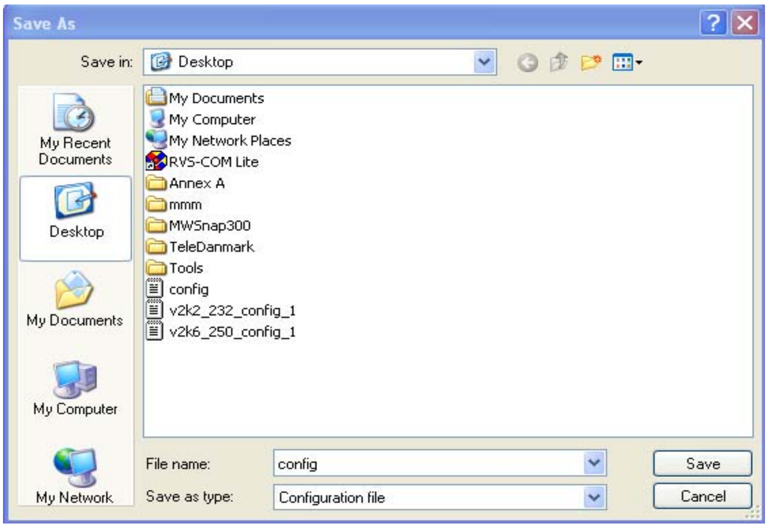
You are downloading the file:

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.



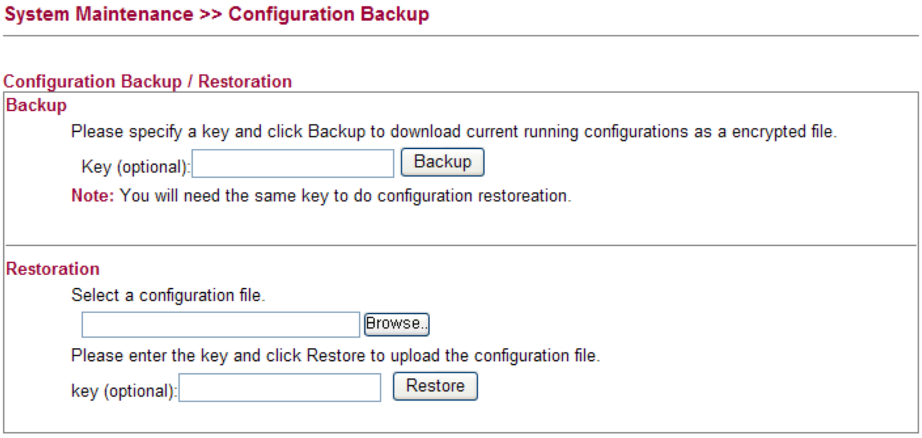
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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):

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):

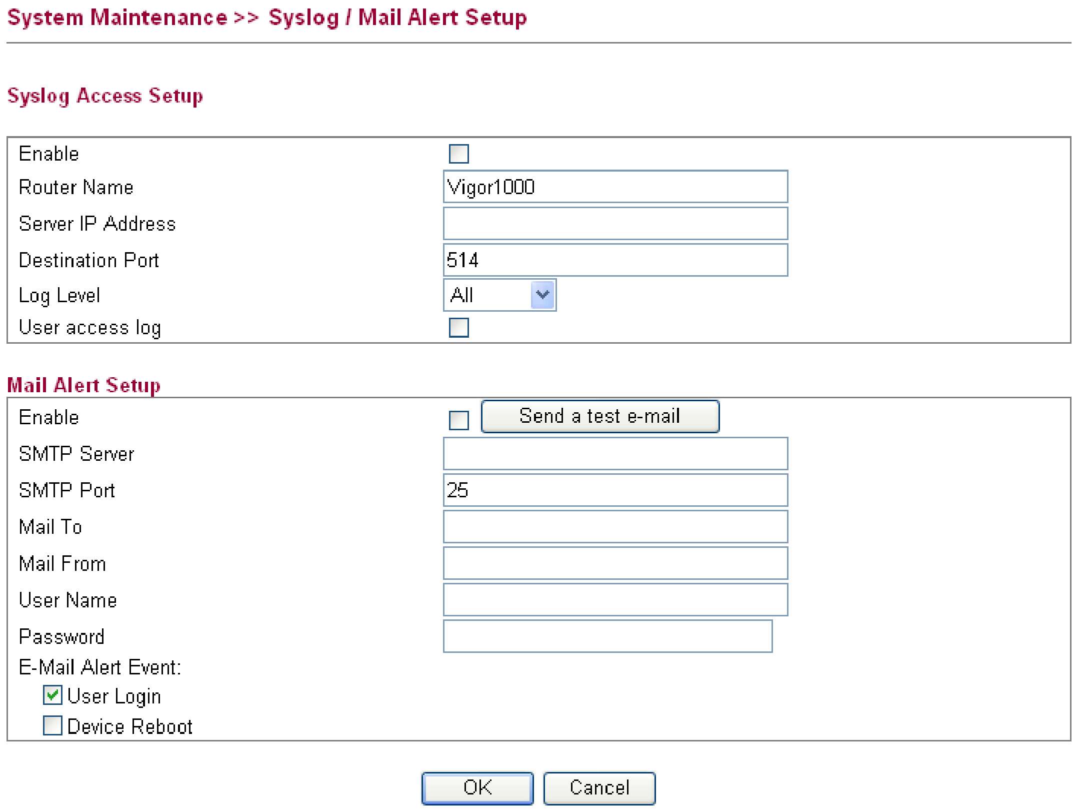
2. Click **Browse** button to choose the correct configuration file for uploading to the router.

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**.

4.15.6 Syslog/Mail Alert

SysLog function is provided for users to monitor the 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	Vigor1000
Server IP Address	
Destination Port	514
Log Level	All
User access log	□

Mail Alert Setup

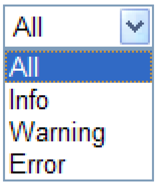
Enable	□ Send a test e-mail
SMTP Server	
SMTP Port	25
Mail To	
Mail From	
User Name	
Password	

E-Mail Alert Event:

☑ User Login

□ Device Reboot

Available settings are explained as follows

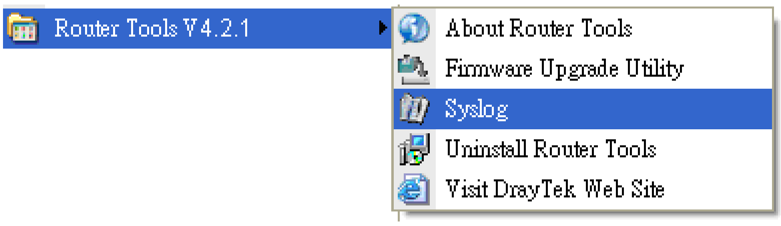
Item	Description
Syslog Access Setup	**Enable (Syslog Access…) -** Check "**Enable**" to activate the function of Syslog. **Router Name -** Assign a name of this device. **Server IP Address -** The IP address of the Syslog server. **Destination Port -** Assign a port for the Syslog protocol. **Log Level -** Choose the severity level for the system log entry.  **User Access Log -** Check this box to record the user logging information.
Mail Alert Setup	**Enable -** Check "**Enable**" to activate function of mail alert. **Send a Test e-mail** – Click this button to let the system

	send a test e-mail to the specified e-mail address. **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. **E-mail Alert Event** - 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.

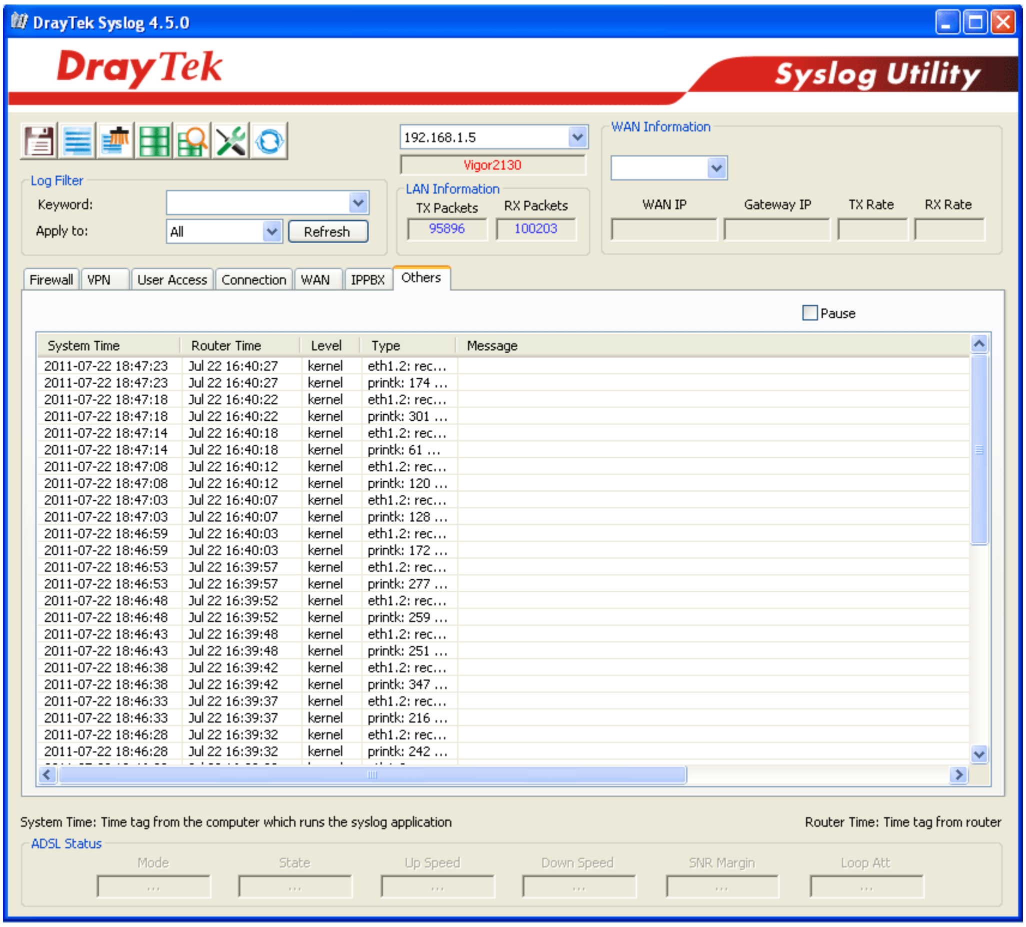
Click **OK** to save these settings.

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.



192.168.1.5

Vigor2130

Log Filter

Keyword:

Apply to: All

LAN Information

TX Packets	RX Packets
95896	100203

WAN Information

WAN IP	Gateway IP	TX Rate	RX Rate

□ Pause

System Time	Router Time	Level	Type	Message
2011-07-22 18:47:23	Jul 22 16:40:27	kernel	eth1.2: rec…	
2011-07-22 18:47:23	Jul 22 16:40:27	kernel	printk: 174 …	
2011-07-22 18:47:18	Jul 22 16:40:22	kernel	eth1.2: rec…	
2011-07-22 18:47:18	Jul 22 16:40:22	kernel	printk: 301 …	
2011-07-22 18:47:14	Jul 22 16:40:18	kernel	eth1.2: rec…	
2011-07-22 18:47:14	Jul 22 16:40:18	kernel	printk: 61 …	
2011-07-22 18:47:08	Jul 22 16:40:12	kernel	eth1.2: rec…	
2011-07-22 18:47:08	Jul 22 16:40:12	kernel	printk: 120 …	
2011-07-22 18:47:03	Jul 22 16:40:07	kernel	eth1.2: rec…	
2011-07-22 18:47:03	Jul 22 16:40:07	kernel	printk: 128 …	
2011-07-22 18:46:59	Jul 22 16:40:03	kernel	eth1.2: rec…	
2011-07-22 18:46:59	Jul 22 16:40:03	kernel	printk: 172 …	
2011-07-22 18:46:53	Jul 22 16:39:57	kernel	eth1.2: rec…	
2011-07-22 18:46:53	Jul 22 16:39:57	kernel	printk: 277 …	
2011-07-22 18:46:48	Jul 22 16:39:52	kernel	eth1.2: rec…	
2011-07-22 18:46:48	Jul 22 16:39:52	kernel	printk: 259 …	
2011-07-22 18:46:43	Jul 22 16:39:48	kernel	eth1.2: rec…	
2011-07-22 18:46:43	Jul 22 16:39:48	kernel	printk: 251 …	
2011-07-22 18:46:38	Jul 22 16:39:42	kernel	eth1.2: rec…	
2011-07-22 18:46:38	Jul 22 16:39:42	kernel	printk: 347 …	
2011-07-22 18:46:33	Jul 22 16:39:37	kernel	eth1.2: rec…	
2011-07-22 18:46:33	Jul 22 16:39:37	kernel	printk: 216 …	
2011-07-22 18:46:28	Jul 22 16:39:32	kernel	eth1.2: rec…	
2011-07-22 18:46:28	Jul 22 16:39:32	kernel	printk: 242 …	

System Time: Time tag from the computer which runs the syslog application

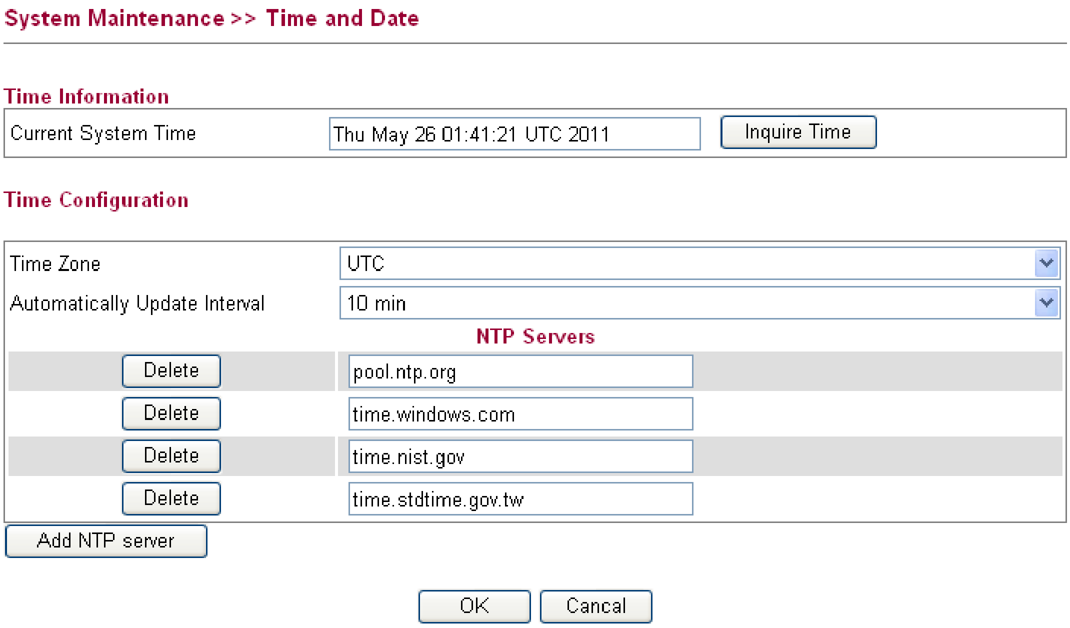
Router Time: Time tag from router

ADSL Status

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

4.15.7 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: Thu May 26 01:41:21 UTC 2011

Time Configuration

Time Zone: UTC

Automatically Update Interval: 10 min

NTP Servers

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

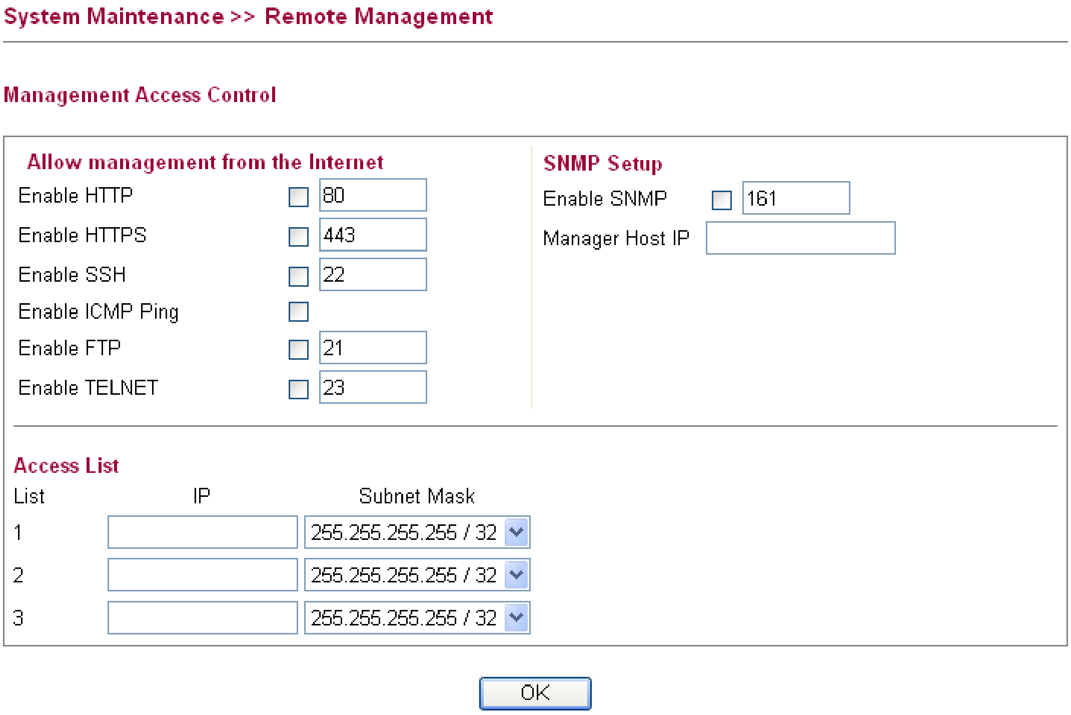
Available settings are explained as follows

Item	Description
Time Information	**Current System Time** - Display current time in the box. Click **Inquire Time** to get the current time.
Time Configuration	**Time Zone** - Select the time zone where the router is located. **Automatically Update Interval** - Specify a time interval for the router to update current time. **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.

4.15.8 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

Allow management from the Internet

Enable HTTP	□	80
Enable HTTPS	□	443
Enable SSH	□	22
Enable ICMP Ping	□	
Enable FTP	□	21
Enable TELNET	□	23

SNMP Setup

Enable SNMP □ 161

Manager Host IP

Access List

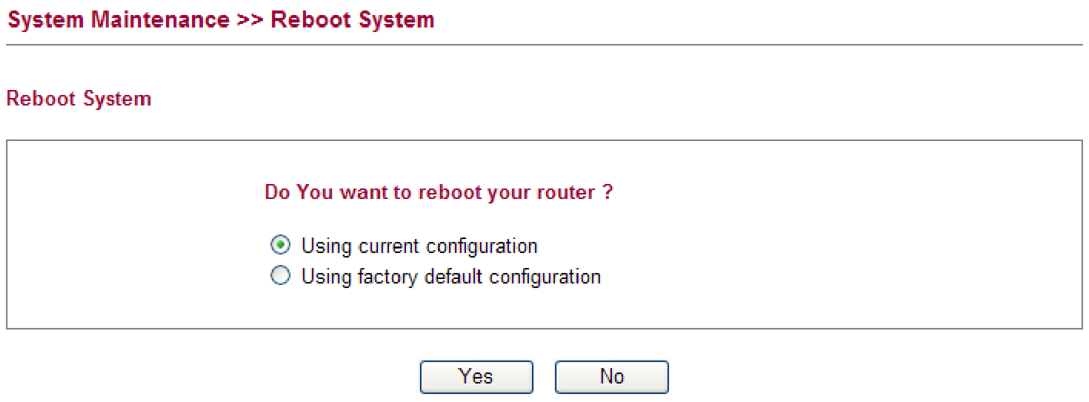
List	IP	Subnet Mask
1		255.255.255.255 / 32
2		255.255.255.255 / 32
3		255.255.255.255 / 32

Available settings are explained as follows

Item	Description
Allow management from the Internet	**Enable HTTP/HTTPS/SSH/ICMP Ping/FTP/TELNET -** Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Enable SNMP	Check it to enable such service. **Manager Host IP** – Set one host as the manager to execute SNMP function. Type the IP address to specify the certain host.
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.

4.15.9 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.

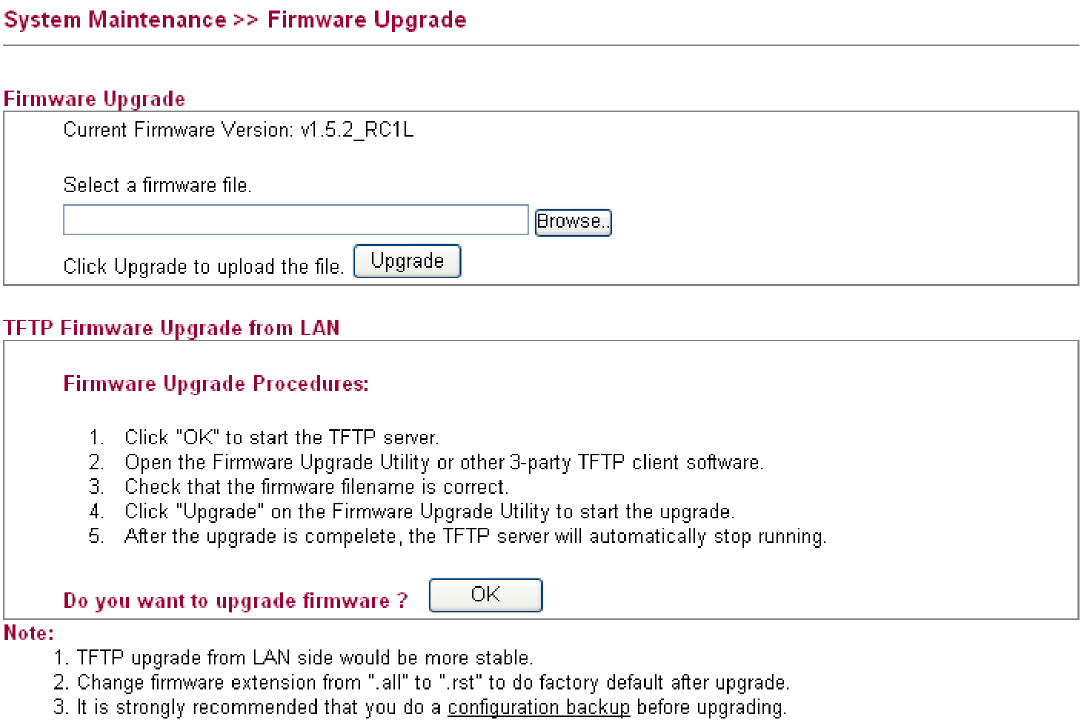
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

4.15.10 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: v1.5.2_RC1L

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Firmware Upgrade Procedures:

1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is compelete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ?

Note:

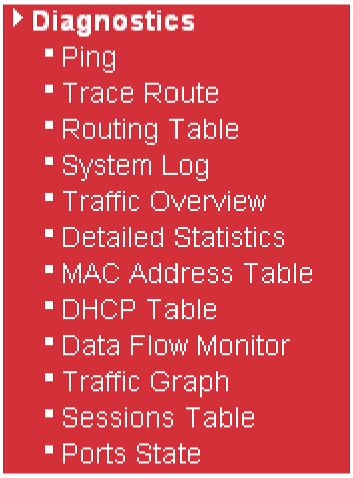
1. TFTP upgrade from LAN side would be more stable.
2. Change firmware extension from ".all" to ".rst" to do factory default after upgrade.
3. It is strongly recommended that you do a configuration backup before upgrading.

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

4.16 Diagnostics

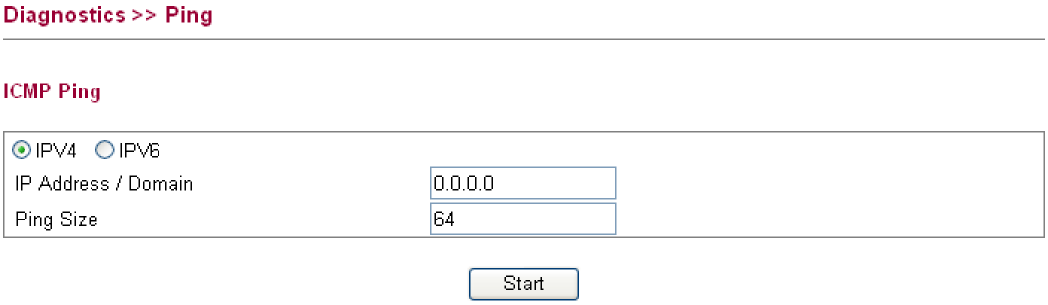
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



4.16.1 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

● IPV4 ○ IPV6

IP Address / Domain: 0.0.0.0

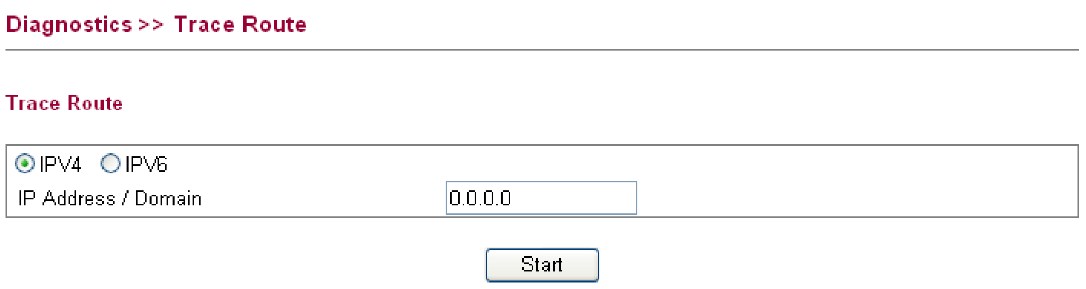
Ping Size: 64

Available settings are explained as follows

Item	Description
IPv4 / IPv6	Click IPv4 or IPv6 for performing the ICMP Ping function.
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.

4.16.2 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.



Diagnostics >> Trace Route

Trace Route

● IPV4 ○ IPV6

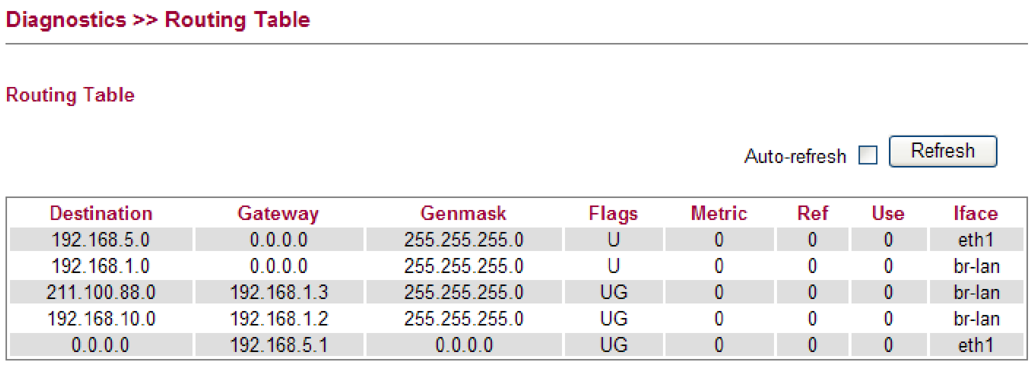
IP Address / Domain: 0.0.0.0

Available settings are explained as follows

Item	Description
IPv4 / IPv6	Click IPv4 or IPv6 for performing the ICMP Ping function.
IP Address / Domain	Type in the IP address /domain of the Host/IP that you want to trace.
Start	Click this button to start the route tracing work. The result will be displayed on the screen.

4.16.3 Routing Table

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



Diagnostics >> Routing Table

Routing Table

Auto-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

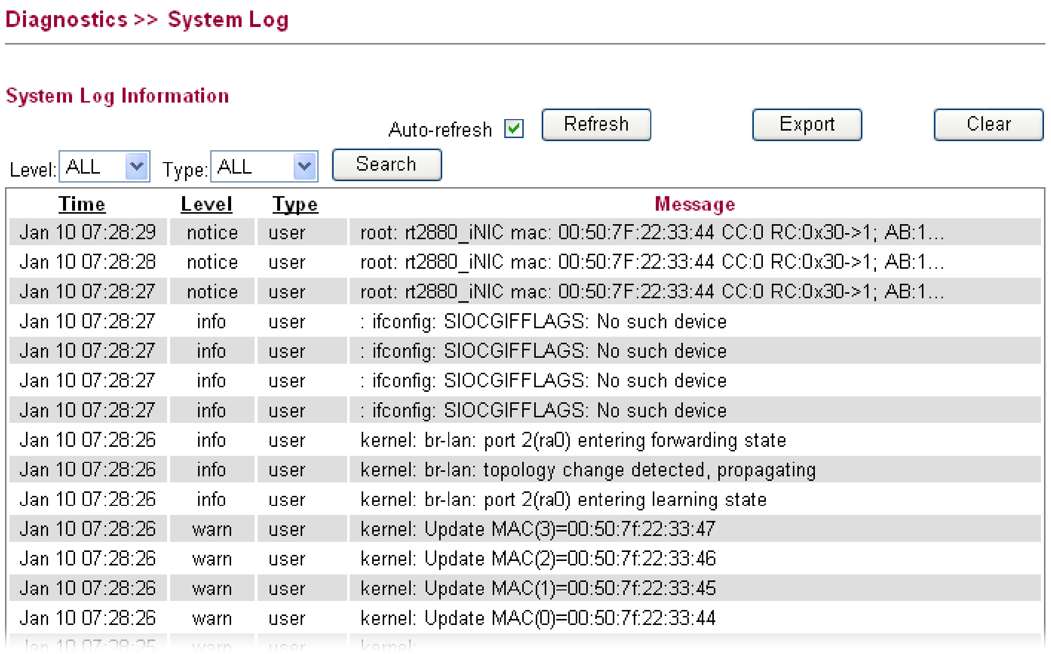
Each item is explained as follows:

Item	Description
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.

4.16.4 System Log

Click **Diagnostics** and click **System Log** to open the web page.



Diagnostics >> System Log

System Log Information

Auto-refresh ☑ Refresh Export Clear

Level: ALL Type: ALL Search

Time	Level	Type	Message
Jan 10 07:28:29	notice	user	root: rt2880_iNIC mac: 00:50:7F:22:33:44 CC:0 RC:0x30->1; AB:1...
Jan 10 07:28:28	notice	user	root: rt2880_iNIC mac: 00:50:7F:22:33:44 CC:0 RC:0x30->1; AB:1...
Jan 10 07:28:27	notice	user	root: rt2880_iNIC mac: 00:50:7F:22:33:44 CC:0 RC:0x30->1; AB:1...
Jan 10 07:28:27	info	user	: ifconfig: SIOCGIFFLAGS: No such device
Jan 10 07:28:27	info	user	: ifconfig: SIOCGIFFLAGS: No such device
Jan 10 07:28:27	info	user	: ifconfig: SIOCGIFFLAGS: No such device
Jan 10 07:28:27	info	user	: ifconfig: SIOCGIFFLAGS: No such device
Jan 10 07:28:26	info	user	kernel: br-lan: port 2(ra0) entering forwarding state
Jan 10 07:28:26	info	user	kernel: br-lan: topology change detected, propagating
Jan 10 07:28:26	info	user	kernel: br-lan: port 2(ra0) entering learning state
Jan 10 07:28:26	warn	user	kernel: Update MAC(3)=00:50:7f:22:33:47
Jan 10 07:28:26	warn	user	kernel: Update MAC(2)=00:50:7f:22:33:46
Jan 10 07:28:26	warn	user	kernel: Update MAC(1)=00:50:7f:22:33:45
Jan 10 07:28:26	warn	user	kernel: Update MAC(0)=00:50:7f:22:33:44
Jan 10 07:28:25	warn	user	kernel:

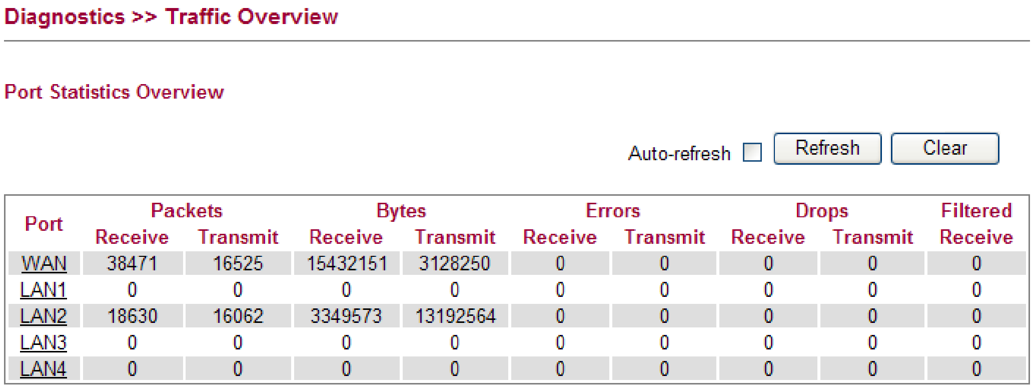
Available settings are explained as follows:

Item	Description
Auto-refresh	Check it to enable auto-refresh function.
Refresh	Click it to reload the page.

Export	Click it to export the log as a text file.
Clear	Click it to clear the information.
Time	Display the time of the system log entry.
Level	Display the severity level of the system log entry. You can specify the level from the drop down list to display the log just for the selected level.
Type	Display the type or subsystem of the system log entry. You can specify the type from the drop down list to display the log just for the selected type.
Message	Display a short description of the system log entry.

4.16.5 Traffic Overview

This page offers an overview of general traffic statistics for all connecting ports.



Diagnostics >> Traffic Overview

Port Statistics Overview

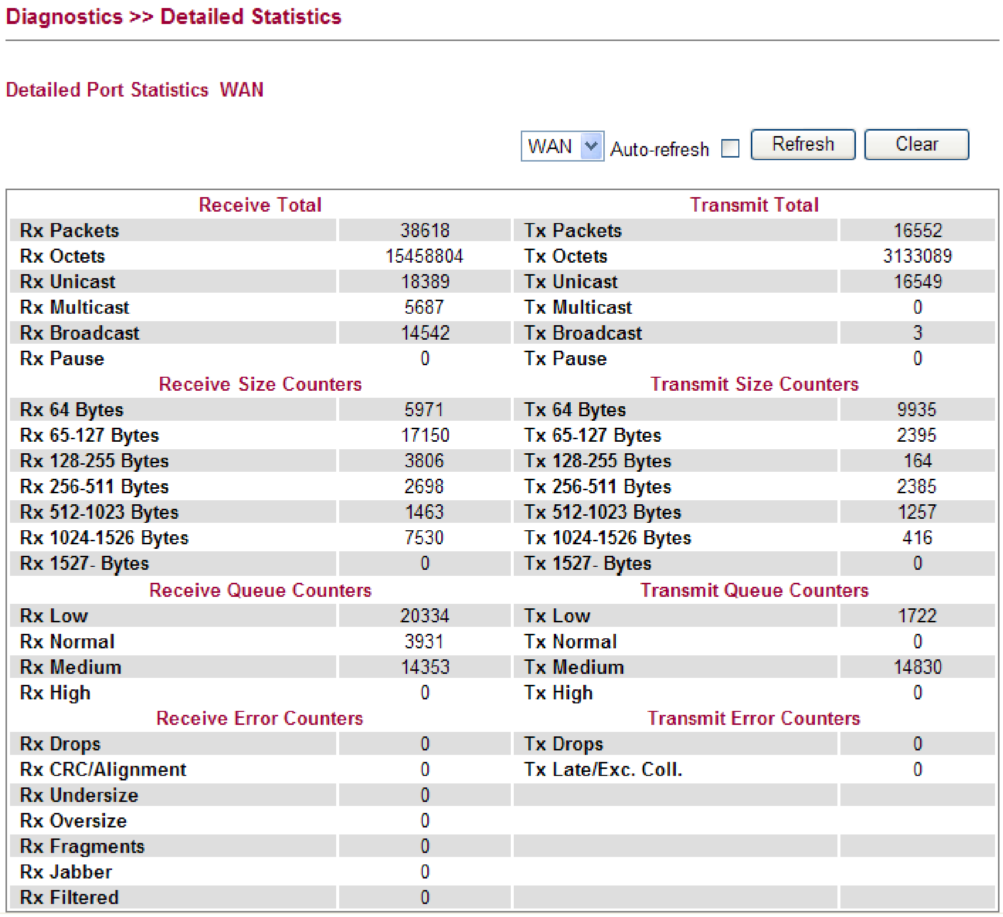
Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
WAN	38471	16525	15432151	3128250	0	0	0	0	0
LAN1	0	0	0	0	0	0	0	0	0
LAN2	18630	16062	3349573	13192564	0	0	0	0	0
LAN3	0	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0	0

Each item is explained as follows:

Item	**Description**
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.

4.16.6 Detailed Statistics

This page display detailed statistics for WAN/LAN interface.



Diagnostics >> Detailed Statistics

Detailed Port Statistics WAN

WAN Auto-refresh □ Refresh Clear

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		

Each item is explained as follows:

Item	Description
WAN/LAN	Choose WAN or LAN to display the corresponding statistics.
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.
Receive Total	**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.

Receive Size Counters	**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.
Receive Queue Counters	**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.
Receive Error Counters	**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.
Transmit Total	**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.

Transmit Size Counters	**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.
Transmit Queue Counters	**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.
Transmit Error Counters	**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.

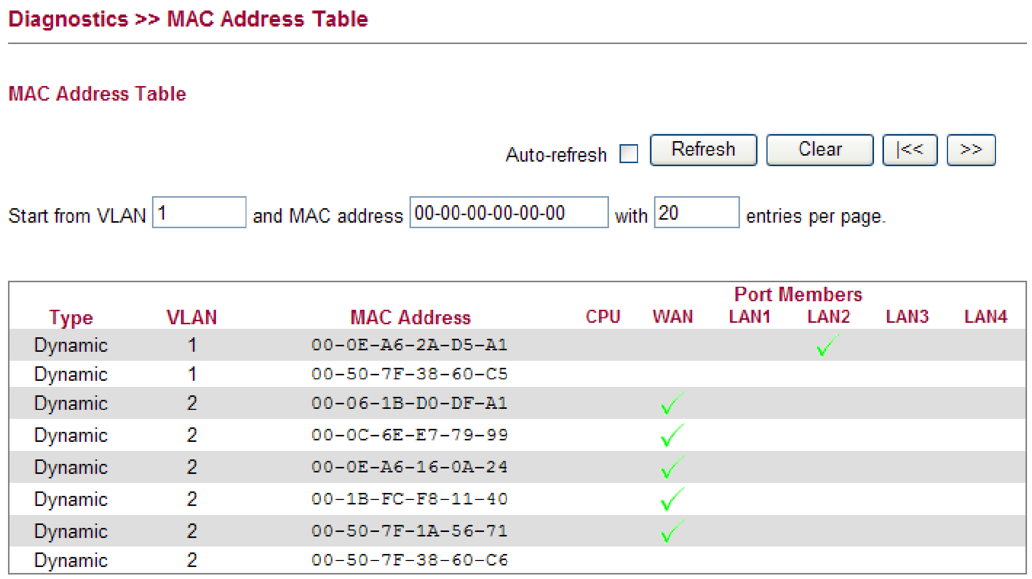
4.16.7 MAC Address Table

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						

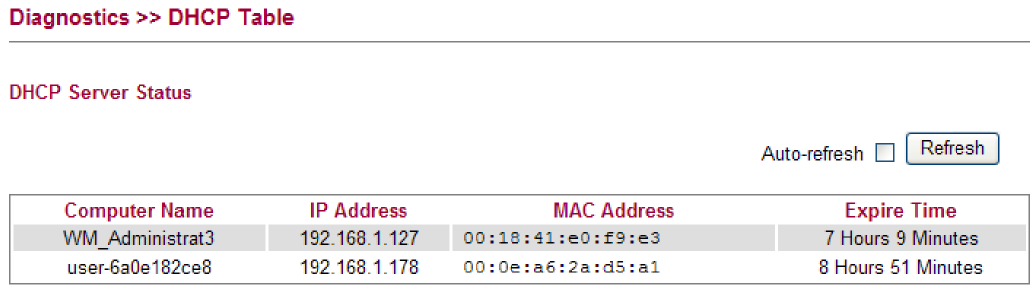
Each item is explained as follows:

Item	Description
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.
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.

4.16.8 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

Auto-refresh □ Refresh

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

Each item is explained as follows:

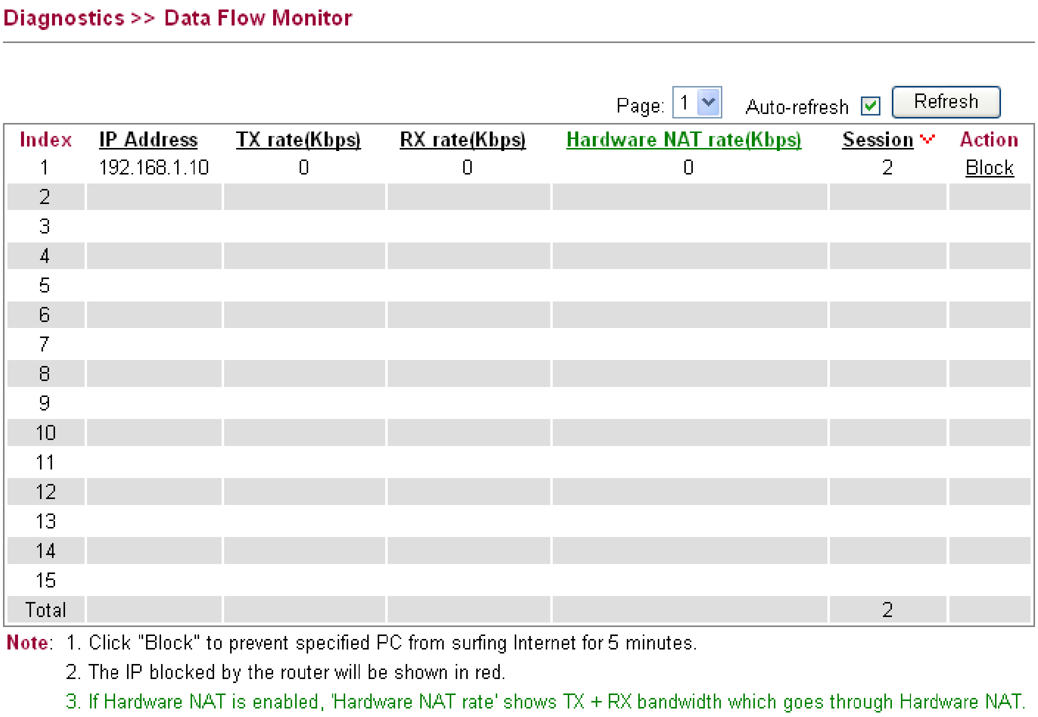
Item	Description
Auto-refresh	Check it to enable auto-refresh function.

Refresh	Click it to reload the page.
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.

4.16.9 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before 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

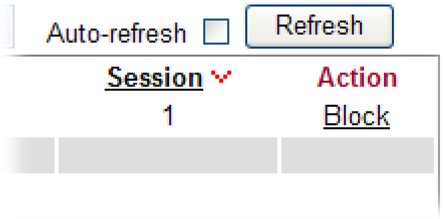
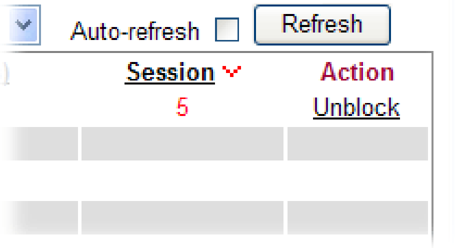
Page: 1 Auto-refresh ☑ Refresh

Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Hardware NAT rate(Kbps)	Session	Action
1	192.168.1.10	0	0	0	2	Block
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Total					2	

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.
3. If Hardware NAT is enabled, 'Hardware NAT rate' shows TX + RX bandwidth which goes through Hardware NAT.

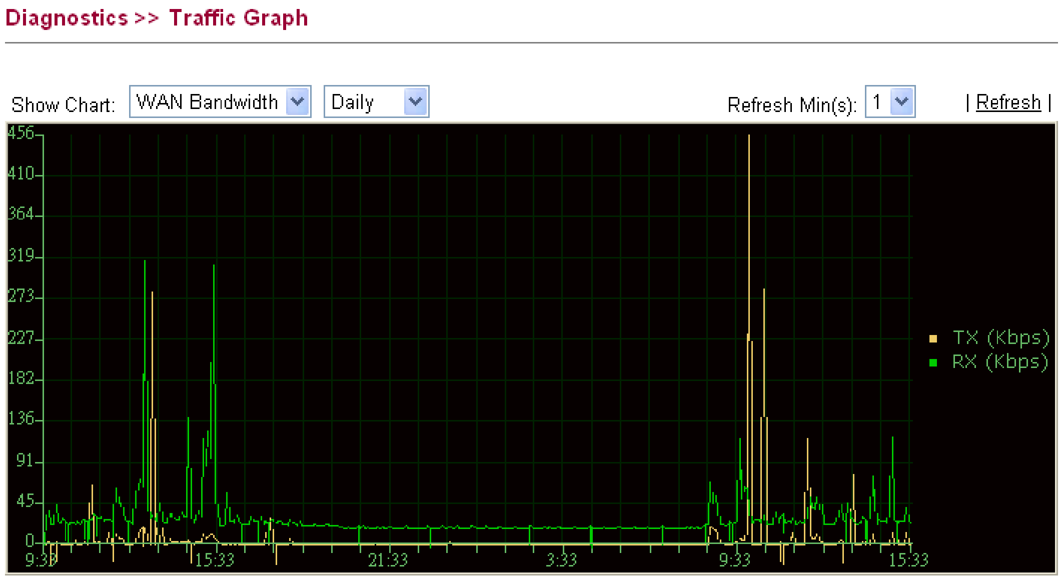
Each item is explained as follows:

Item	Description
Page	Allow to choose the page to be displayed on this screen.
Auto-refresh	Check it to enable auto-refresh function.
Refresh	Click it to reload the page.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.

TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Hardware NAT rate	Display the data processing rate of the monitored device if hardware NAT is enabled.
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.  Auto-refresh □ Refresh Session Action 5 Unblock

4.16.10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



Diagnostics >> Traffic Graph

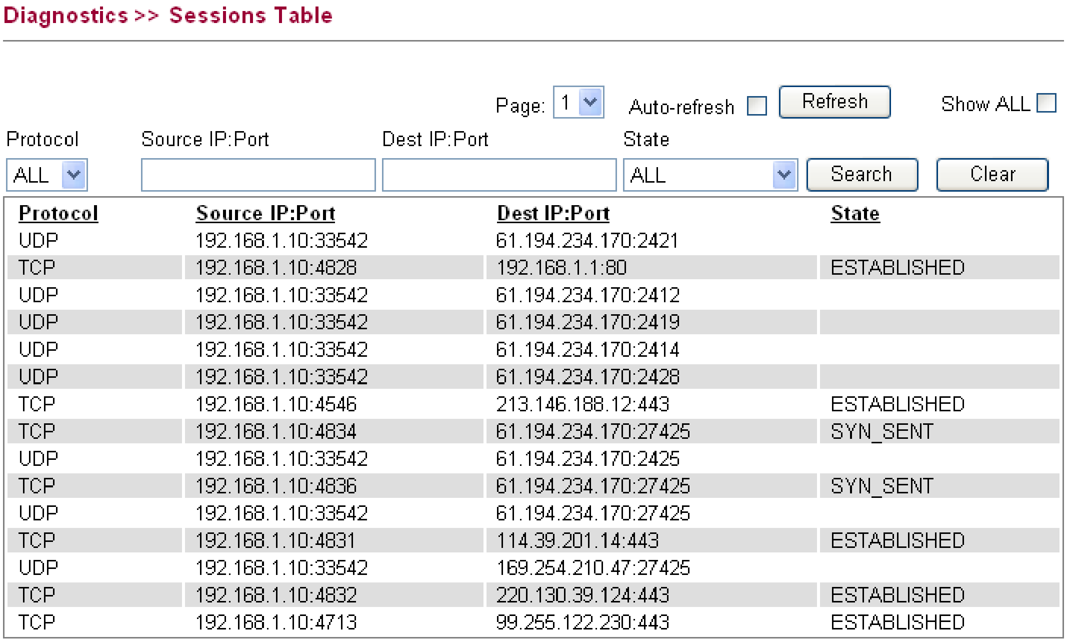
Show Chart: WAN Bandwidth Daily Refresh Min(s): 1 | Refresh |

The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

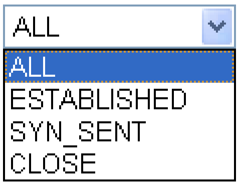
4.16.11 Sessions Table

Click **Diagnostics** and click **Sessions Table** to open the list page. This page displays the session information for UDP and/or TCP. Also, you can specify the IP range to observe the corresponding information for your necessity.



Protocol	Source IP:Port	Dest IP:Port	State
UDP	192.168.1.10:33542	61.194.234.170:2421	
TCP	192.168.1.10:4828	192.168.1.1:80	ESTABLISHED
UDP	192.168.1.10:33542	61.194.234.170:2412	
UDP	192.168.1.10:33542	61.194.234.170:2419	
UDP	192.168.1.10:33542	61.194.234.170:2414	
UDP	192.168.1.10:33542	61.194.234.170:2428	
TCP	192.168.1.10:4546	213.146.188.12:443	ESTABLISHED
TCP	192.168.1.10:4834	61.194.234.170:27425	SYN_SENT
UDP	192.168.1.10:33542	61.194.234.170:2425	
TCP	192.168.1.10:4836	61.194.234.170:27425	SYN_SENT
UDP	192.168.1.10:33542	61.194.234.170:27425	
TCP	192.168.1.10:4831	114.39.201.14:443	ESTABLISHED
UDP	192.168.1.10:33542	169.254.210.47:27425	
TCP	192.168.1.10:4832	220.130.39.124:443	ESTABLISHED
TCP	192.168.1.10:4713	99.255.122.230:443	ESTABLISHED

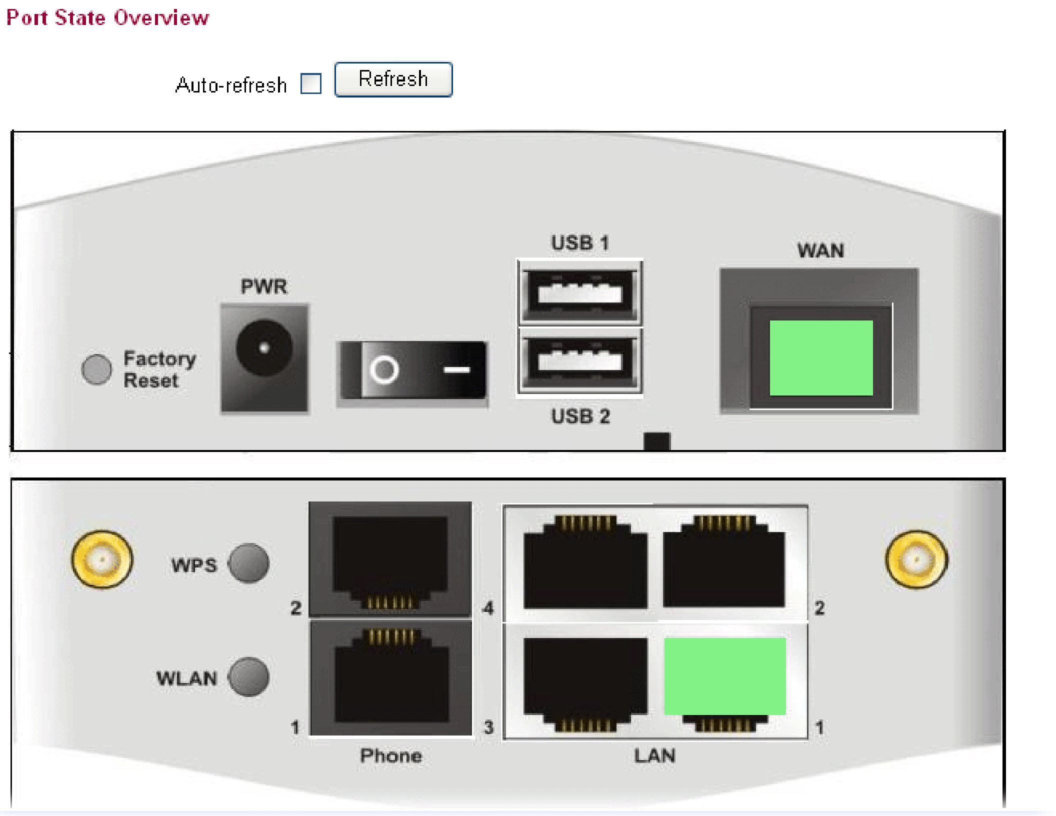
Each item is explained as follows:

Item	Description
Page	Allow to choose the page to be displayed on this screen.
Auto-refresh	Check it to enable auto-refresh function.
Refresh	Click it to reload the page.
Shall ALL	Check this box to display all of the data via UDP and TCP.
Protocol	Choose one of the protocols to be displayed the corresponding information in this page.
Source IP: Port / **Dest IP: Port**	You can check a range of certain devices by specifying the source and destination IP address (es) with the port number.
State	Display the sessions based on the state chosen here. 

Search	Click this button to search the information based on the conditions specified.
Clear	Clear all of the information displayed in this page.

4.16.12 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.



Port State Overview

Auto-refresh □ Refresh

Each item is explained as follows:

Item	Description
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.

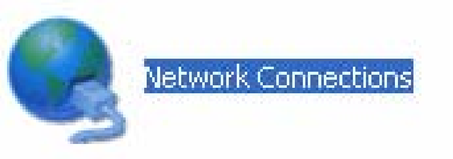
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

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.

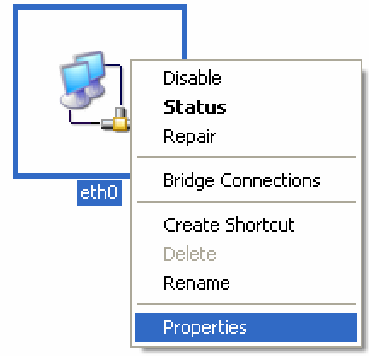
For Windows

> 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**.

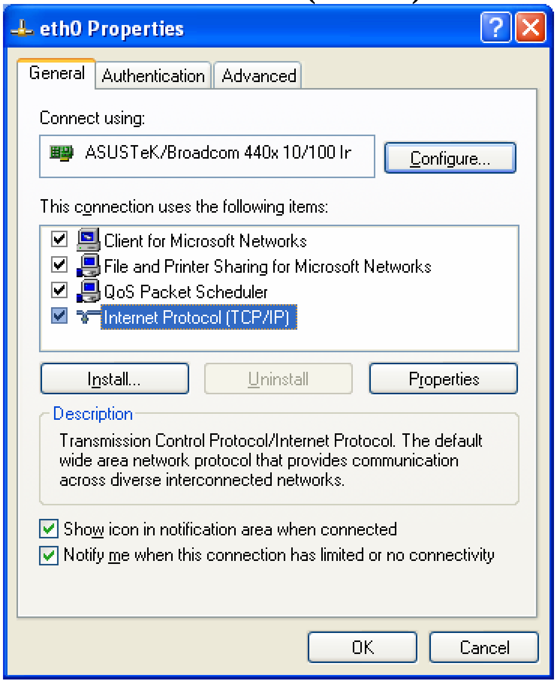
1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on **Local Area Connection** and click on **Properties**.



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



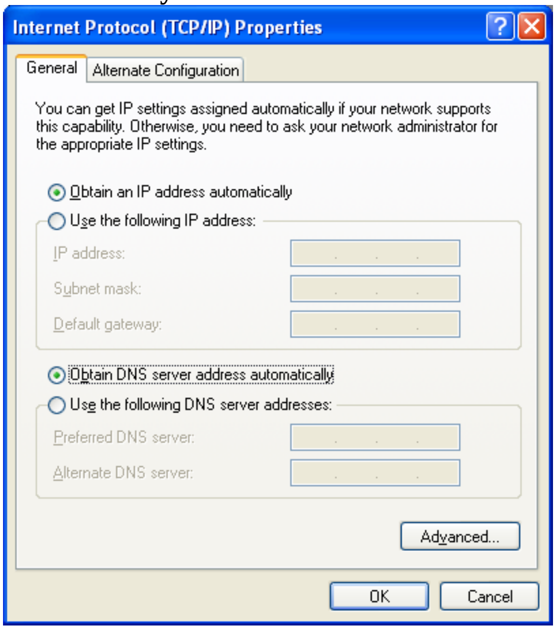
Connect using:
ASUSTeK/Broadcom 440x 10/100 Ir

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



Internet Protocol (TCP/IP) Properties

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

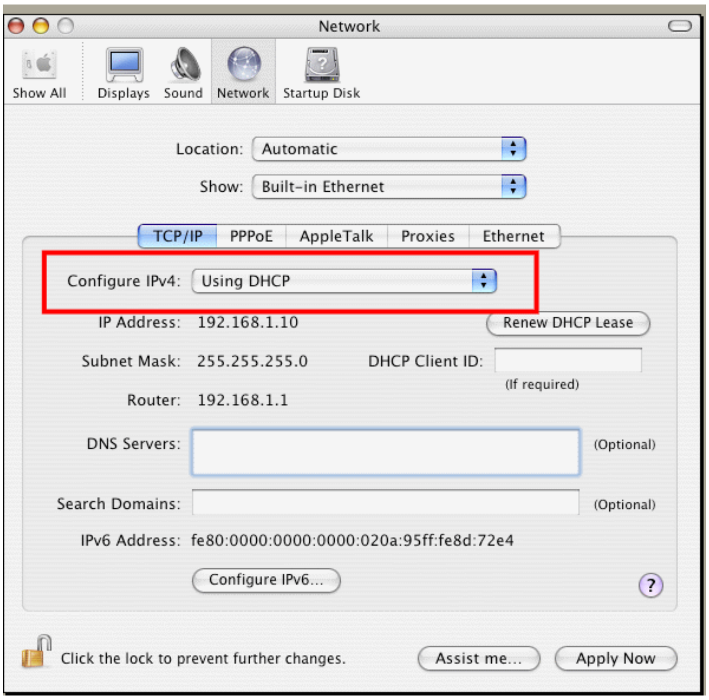
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



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

Router: 192.168.1.1

DHCP Client ID: (If required)

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

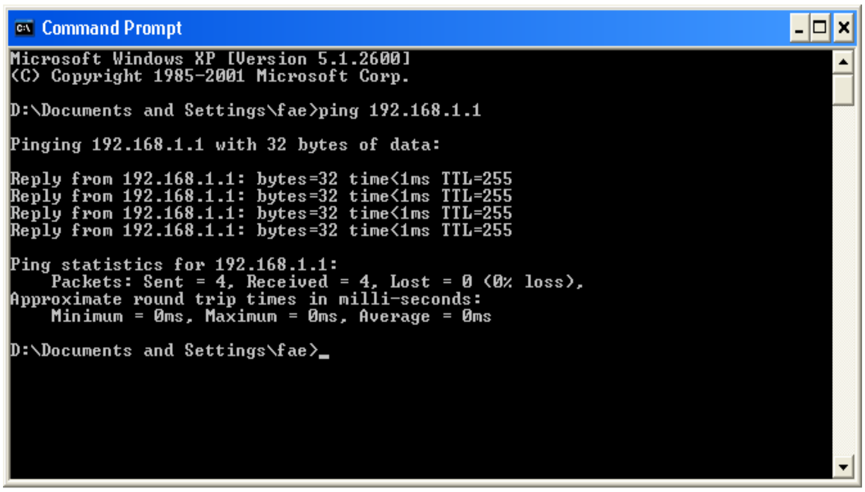
5.3 Pinging the Router from Your Computer

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/Vista). The DOS command dialog will appear.

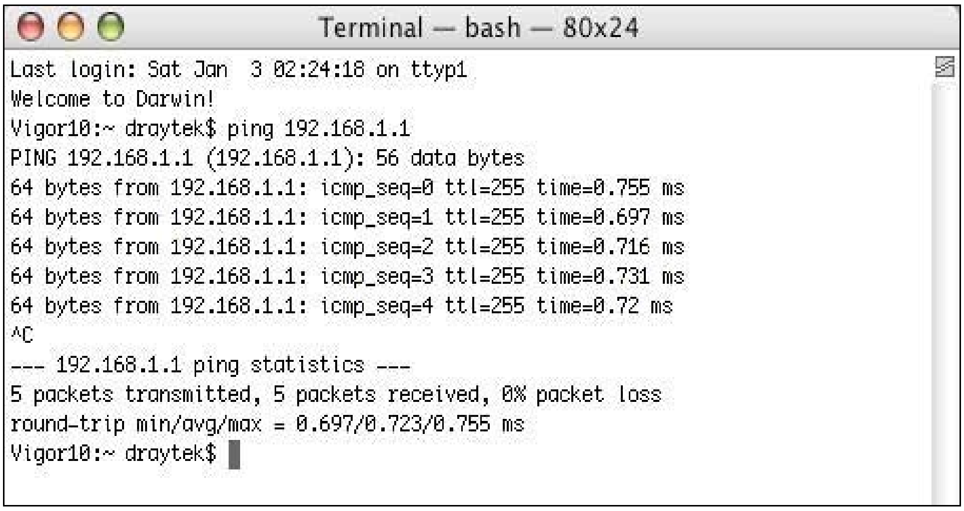


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

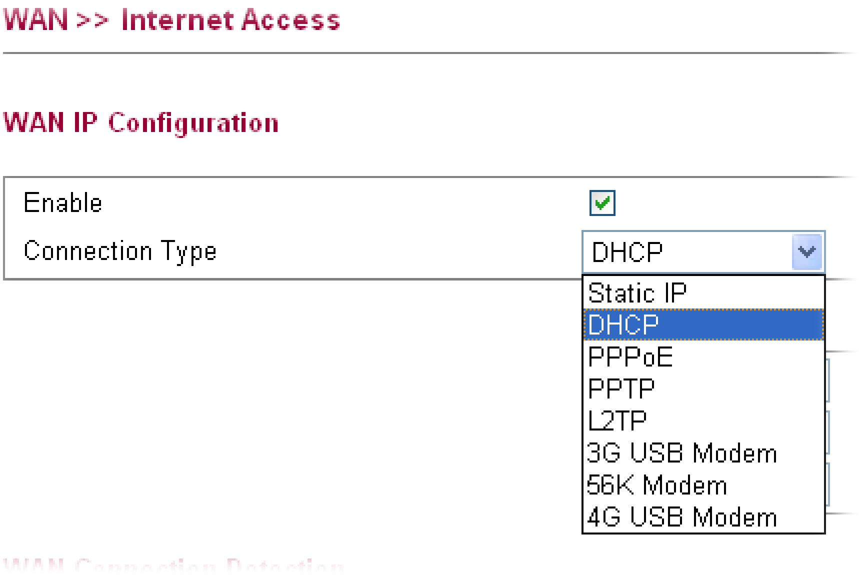


Terminal — bash — 80x24

```
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/3G USB Modem for reviewing the settings that you configured previously.



WAN >> Internet Access

WAN IP Configuration

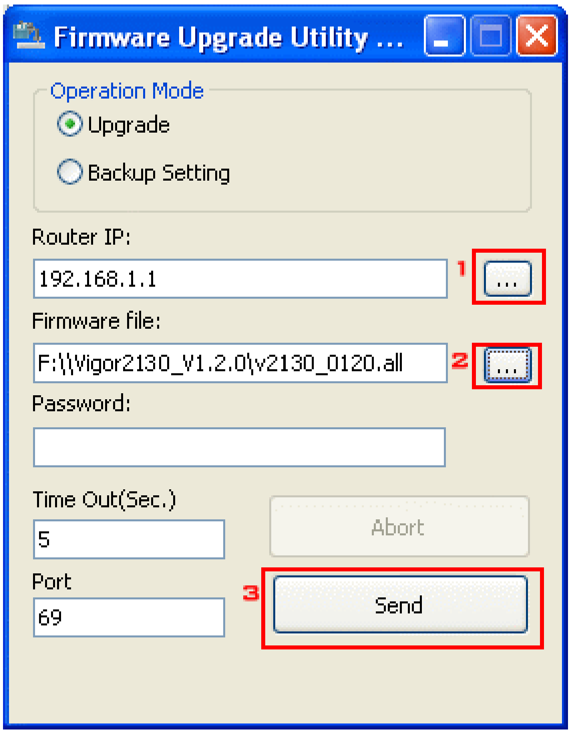
Enable	☑
Connection Type	DHCP

5.5 Forcing Vigor Router into TFTP Mode for Performing the Firmware Upgrade

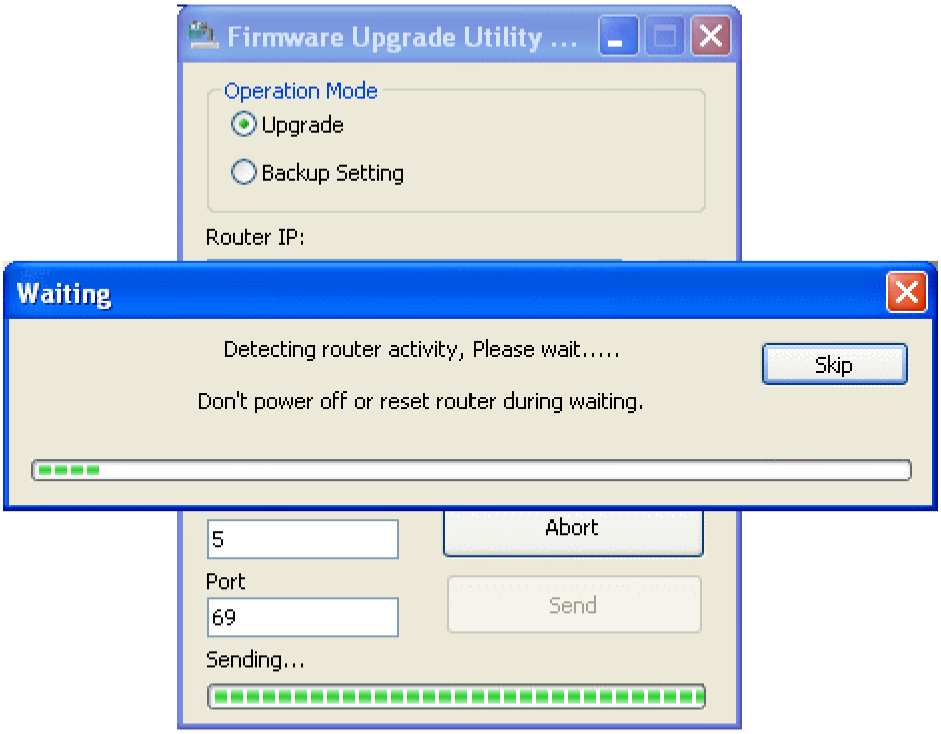
1. Press and hold the **Factory Reset** button. The system will power off and power on the Vigor Router.
2. Release the **Factory Reset** button when the ACT LED and its neighbor LED blink simultaneously.

   There are different LED blinking methods in describing TFTP mode status: Vigor1000: 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**.



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.

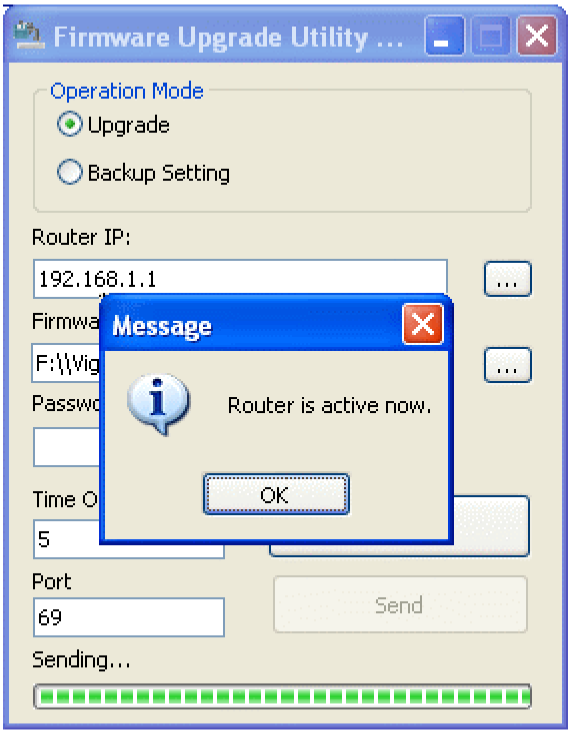
5

Port

69

Sending...

12. When the firmware upgrade is successful, the following window will pop up.



Firmware Upgrade Utility ...

Operation Mode

● Upgrade

○ Backup Setting

Router IP:

192.168.1.1

Firmwa

F:\\Vig

Passwo

Time O

5

Port

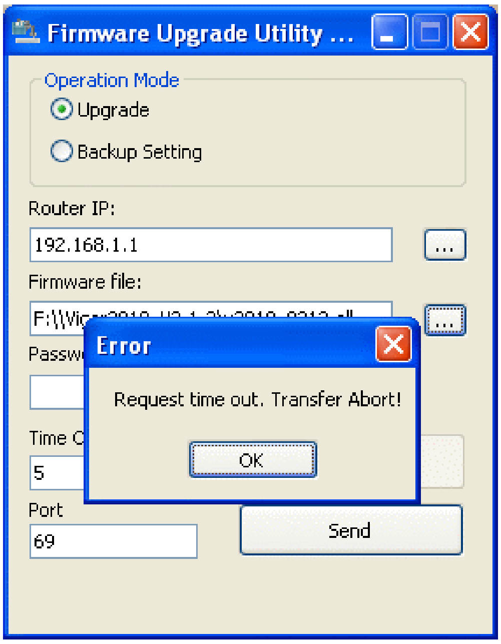
69

Sending...

Message

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.

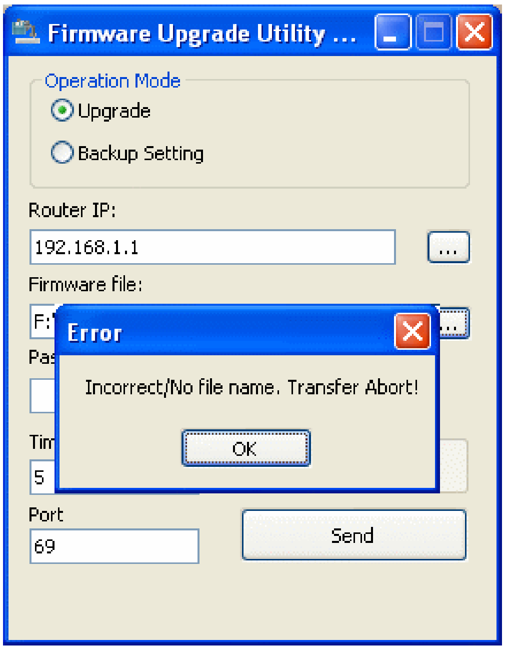


Router IP: 192.168.1.1

Time O: 5

Port: 69

Request time out. Transfer Abort!



Router IP: 192.168.1.1

Tim: 5

Port: 69

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

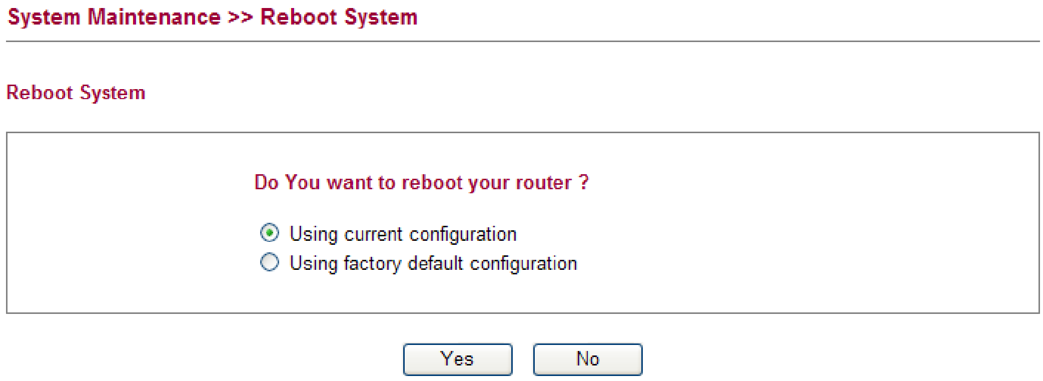
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

> **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

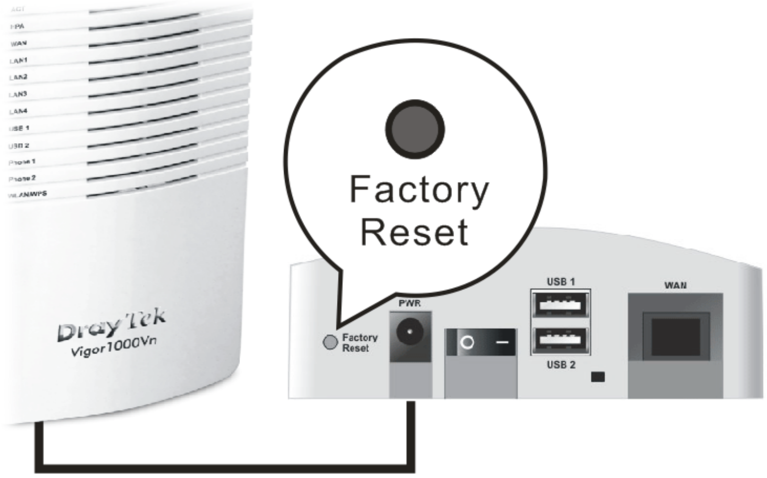
Reboot System

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.