

# DrayTek

## Vigor2130 Series High Speed Gigabit Router



*Your reliable networking solutions partner*

# User's Guide

**V.1.0**

# **Vigor2130 Series High Speed Gigabit Router User's Guide**

**Version: 1.0**

**Date: 31/08/2009**

## Copyright Information

### Copyright Declarations

Copyright 2009 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

### Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista 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 by 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 to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

### Be a Registered Owner

Web registration is preferred. You can register your Vigor router via <http://www.draytek.com>.

### Firmware & Tools Updates

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

<http://www.draytek.com>

## European Community Declarations

Manufacturer: DrayTek Corp.  
Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303  
Product: Vigor2130 Series Router

DrayTek Corp. declares that Vigor2130 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

## Regulatory Information

### Federal Communication Commission Interference Statement

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

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

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

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.

Please visit <http://www.draytek.com/user/AboutRegulatory.php>



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

# Table of Contents

## 1

<b>Preface .....</b>	<b>1</b>
1.1 Web Configuration Buttons Explanation .....	1
1.2 LED Indicators and Connectors .....	2
1.2.1 For Vigor2130 .....	2
1.2.2 For Vigor2130n .....	4
1.2.3 For Vigor2130Vn .....	6
1.3 Hardware Installation .....	8
Stand Installation .....	9
1.4 Printer Installation .....	10

## 2

<b>Configuring Basic Settings .....</b>	<b>15</b>
2.1 Two-Level Management .....	15
2.2 Accessing Web Page .....	15
2.3 Changing Password .....	16
2.4 Quick Start Wizard .....	18
2.4.1 Setting up the Password .....	18
2.4.2 Setting up the Time Zone .....	19
2.4.3 Setting up the Internet Connection .....	19
2.4.4 Setting up the Wireless Connection .....	24
2.4.5 Save the Wizard Configuration .....	29
2.5 Online Status .....	29
2.6 Saving Configuration .....	30

## 3

<b>User Mode Operation .....</b>	<b>31</b>
3.1 WAN .....	31
3.1.1 Internet Access .....	33
3.1.2 Ports .....	39
3.1.3 3G Backup .....	40
3.2 LAN .....	41
3.2.1 General Setup .....	43
3.2.2 Ports .....	44
3.2.3 MAC Address Table .....	45
3.2.4 VLAN .....	46
3.2.5 Static Route .....	47
3.2.6 Bind IP to MAC .....	49
3.3 NAT .....	50
3.3.1 Hardware NAT .....	51
3.3.2 Open Ports .....	51

3.3.3 DMZ Host.....	53
3.4 Bandwidth Management .....	54
3.4.1 Session Limit .....	54
3.4.2 Bandwidth Limit .....	55
3.4.3 Port Rate Control .....	56
3.4.4 QoS Control List .....	57
3.4.5 Ports Priority .....	61
3.4.6 QoS Statistics .....	62
3.5 Applications .....	65
3.5.1 Dynamic DNS .....	65
3.5.2 Schedule .....	66
3.5.3 IGMP Snooping .....	67
3.5.4 IGMP Status .....	68
3.5.5 UPnP Configuration .....	68
3.6 Wireless LAN .....	70
3.6.1 Basic Concepts.....	70
3.6.2 General Setup.....	71
3.6.3 Access Control.....	76
3.6.4 Station List .....	77
3.6.5 Access Point Discovery .....	78
3.7 USB Application .....	78
3.7.1 USB General Settings.....	78
3.7.2 FTP User Management .....	79
3.7.3 Disk Status.....	80
3.7.4 Disk Shares .....	80
3.8 User.....	82
3.8.1 User Configuration.....	82
3.9 System Maintenance.....	83
3.9.1 System Status.....	83
3.9.2 User Password .....	85
3.9.3 Configuration Backup .....	85
3.9.4 Syslog / Mail Alert .....	87
3.9.5 Time and Date .....	89
3.9.6 Management.....	90
3.9.7 Reboot System .....	90
3.9.8 Firmware Upgrade .....	91

## 4

<b>Admin Mode Operation .....</b>	<b>93</b>
4.1 WAN .....	93
4.1.1 Internet Access .....	95
4.1.2 Ports.....	100
4.1.3 3G Backup .....	101
4.2 LAN .....	102
4.2.1 General Setup.....	104
4.2.2 Ports.....	105
4.2.3 MAC Address Table.....	107
4.2.4 VLAN.....	108
4.2.5 Static Route .....	109
4.2.6 Bind IP to MAC .....	111

4.3 NAT .....	112
4.3.1 Hardware NAT .....	113
4.3.2 Open Ports.....	113
4.3.3 DMZ Host.....	115
4.4 Firewall.....	116
4.4.1 DoS Defense .....	116
4.4.2 Ports Configuration .....	117
4.4.3 Rate Control Object .....	119
4.4.4 Access Control List .....	120
4.5 Bandwidth Management .....	136
4.5.1 Session Limit .....	137
4.5.2 Bandwidth Limit .....	138
4.5.3 Port Rate Control.....	139
4.5.4 QoS Control List .....	139
4.5.5 Ports Priority .....	144
4.5.6 QoS Statistics .....	145
4.6 Applications .....	148
4.6.1 Dynamic DNS .....	148
4.6.2 Schedule.....	149
4.6.3 IGMP Snooping .....	150
4.6.4 IGMP Status .....	151
4.6.5 UPnP Configuration.....	151
4.7 VPN and Remote Access.....	153
4.7.1 Remote Access Control.....	153
4.7.2 PPTP Remote Dial-in.....	154
4.7.3 IPsec Remote Dial-in .....	156
4.7.4 Remote Dial-in Status.....	158
4.7.5 LAN to LAN.....	159
4.8 Wireless LAN .....	161
4.8.1 Basic Concepts.....	161
4.8.2 General Setup.....	163
4.8.3 Access Control.....	167
4.8.4 Station List .....	168
4.8.5 Access Point Discovery .....	169
4.9 USB Application .....	169
4.9.1 USB General Settings.....	170
4.9.2 FTP User Management .....	170
4.9.3 Disk Status.....	171
4.9.4 Disk Shares .....	171
4.10 User.....	173
4.10.1 User Configuration.....	173
4.11 System Maintenance.....	175
4.11.1 System Status.....	175
4.11.2 System Password.....	176
4.11.3 User Password .....	176
4.11.4 Configuration Backup .....	177
4.11.5 Syslog/Mail Alert .....	178
4.11.6 Time and Date .....	180
4.11.7 Management.....	181
4.11.8 Reboot System .....	181
4.11.9 Firmware Upgrade .....	182

4.12 Diagnostics.....	183
4.12.1 Ping.....	183
4.12.2 Routing Table .....	184
4.12.3 System Log.....	185
4.12.4 Traffic Overview.....	185
4.12.5 Detailed Statistics .....	186
4.12.6 MAC Address Table.....	188
4.12.7 DHCP Table.....	190
4.12.8 Data Flow Monitor.....	191
4.12.9 Ports State .....	192

# 5

## **Trouble Shooting ..... 193**

5.1 Checking If the Hardware Status Is OK or Not.....	193
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not .....	194
5.3 Pinging the Router from Your Computer .....	196
5.4 Checking If the ISP Settings are OK or Not.....	197
5.5 Backing to Factory Default Setting If Necessary .....	199
5.6 Contacting Your Dealer .....	200



# 1

## Preface

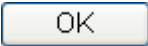
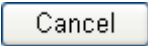
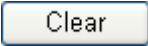



The Vigor2130 series are the routers with high speed in data transmission through WAN port and LAN ports. With hardware NAT acceleration, the rate of Vigor2130 series can be greater than 900Mbps almost.

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

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

### 1.1 Web Configuration Buttons Explanation

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

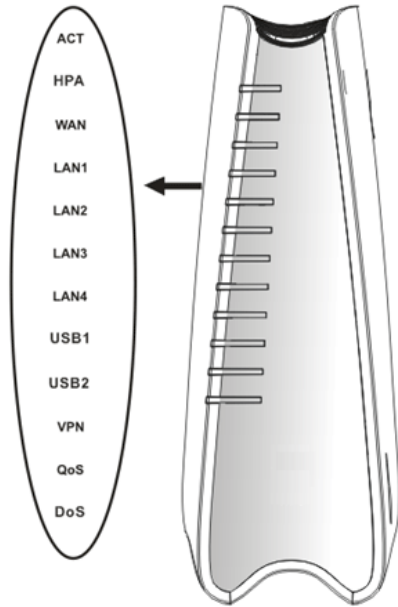
	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the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

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

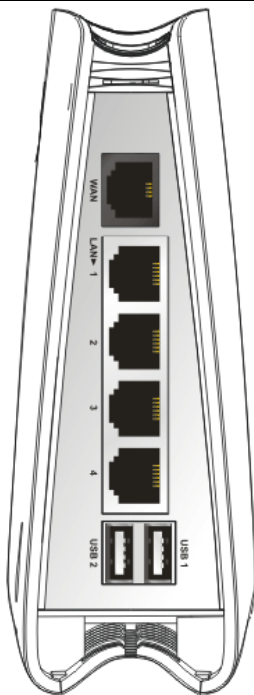
## 1.2 LED Indicators and Connectors

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

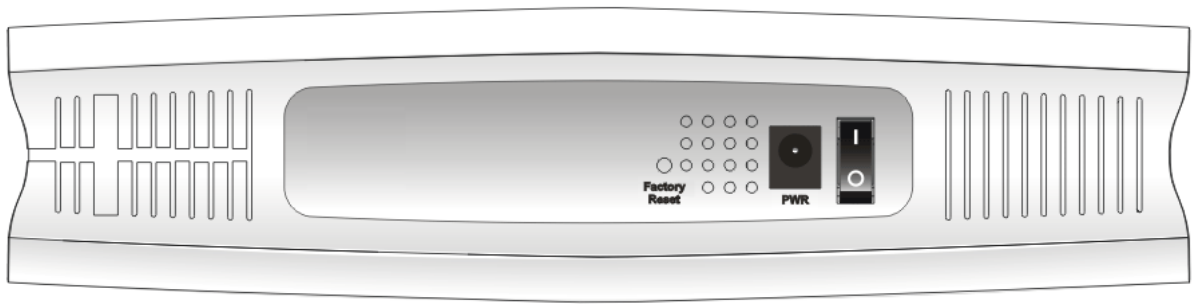
### 1.2.1 For Vigor2130



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

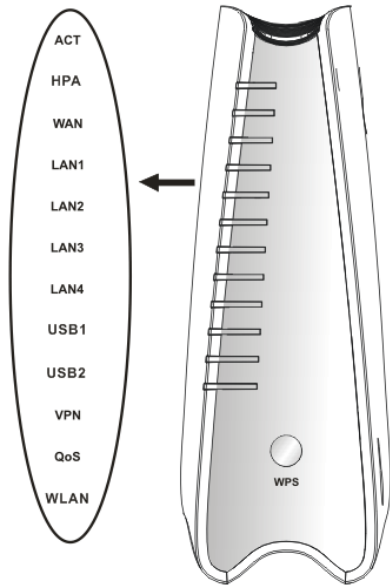


Interface	Description
WAN	Connector for accessing the Internet.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.

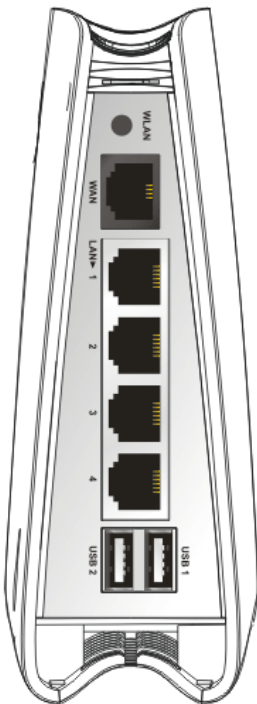


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.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

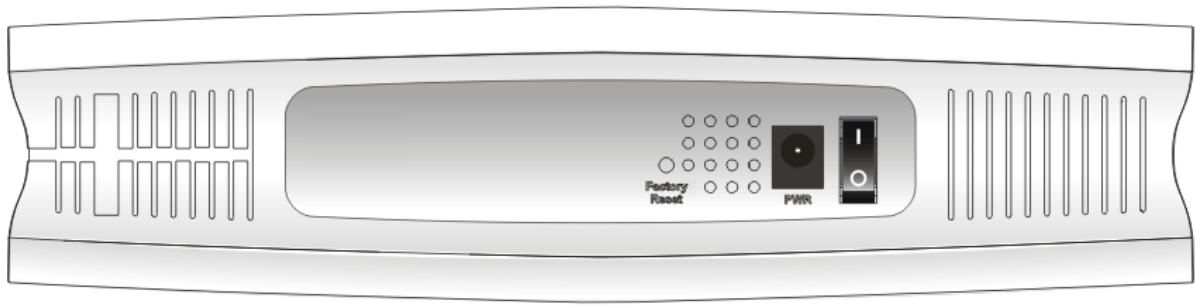
## 1.2.2 For Vigor2130n



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

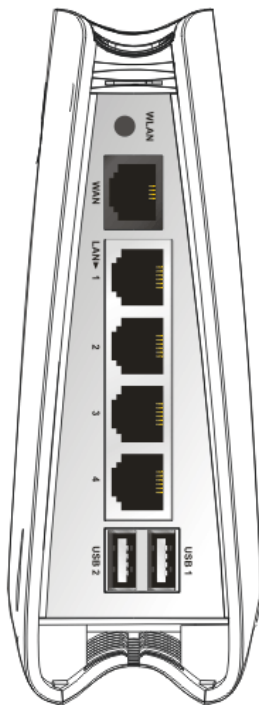
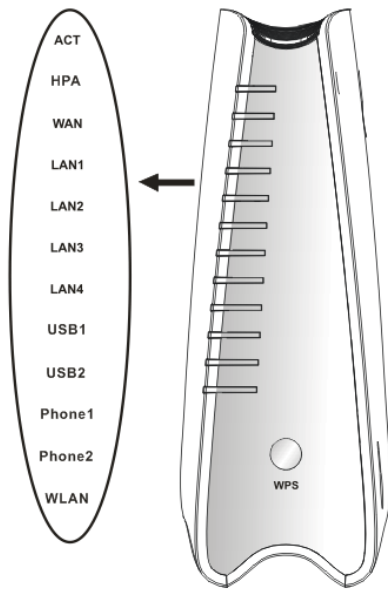


Interface	Description
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
WAN	Connector for accessing the Internet.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for USB storage (Pen Driver /Mobile HD) or printer.



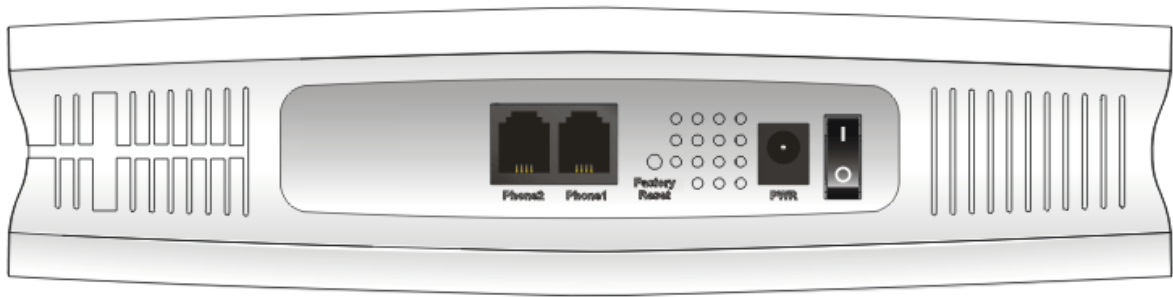
Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.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

### 1.2.3 For Vigor2130Vn



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

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

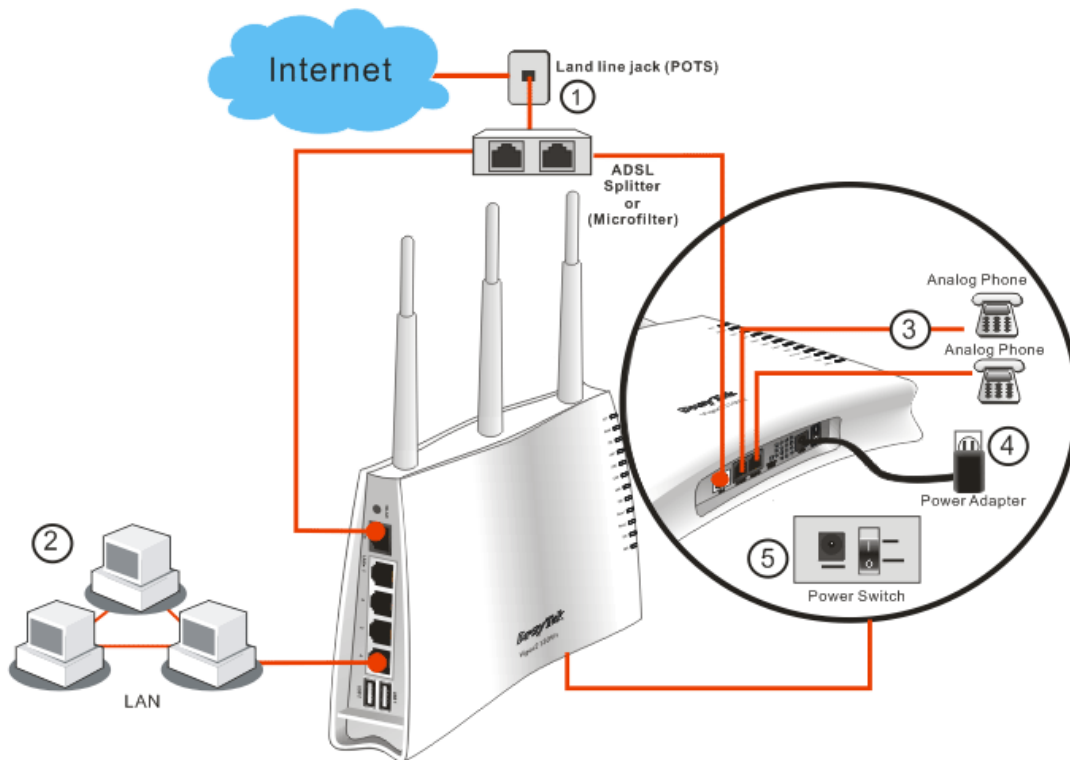


Interface	Description
Phone2/Phone1	Connector of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

## 1.3 Hardware Installation

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

1. Connect Line port to land line jack with a RJ-11 cable (Vn model).
2. Connect this device to a modem with an Ethernet cable.
3. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
4. Connect Phone port to a conventional analog telephone.
5. Connect detachable antennas to the router for Vigor2130 series (n model).
6. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
7. Power on the router.
8. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connections.



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

**Caution:**

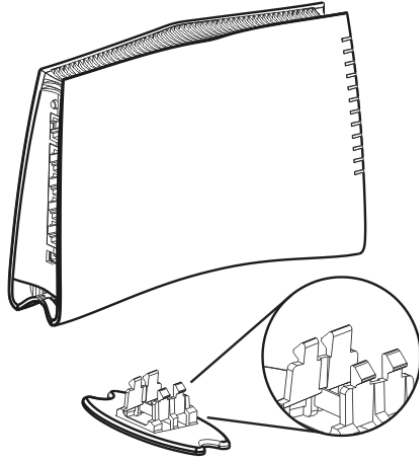
1. Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the land line jack. Such connection might damage your router.
2. When the power is shutdown, VoIP phone will be disconnected. However, a phone set connected to Phone 2 port can be used as the traditional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



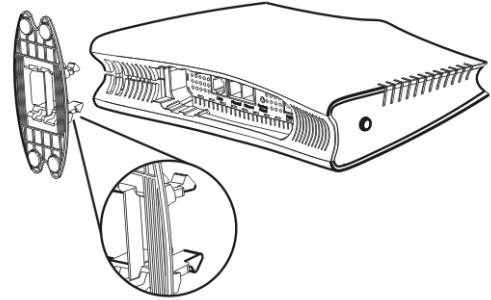
## Stand Installation

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

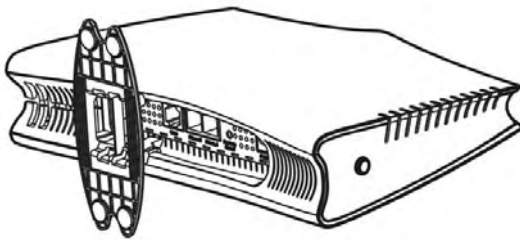
①



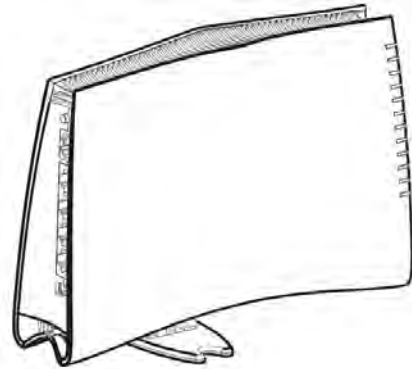
②



③

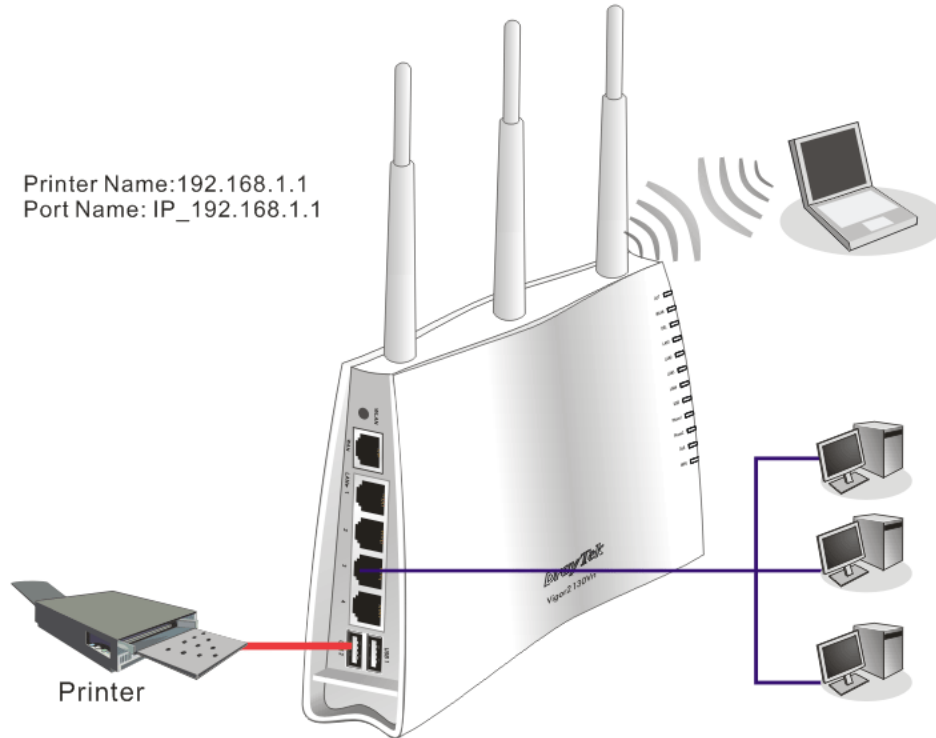


④



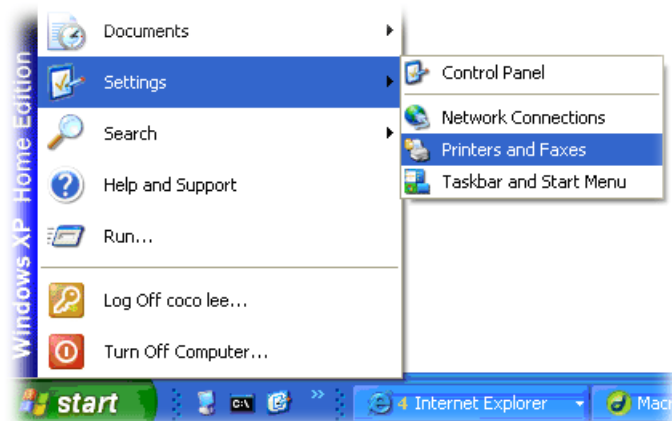
## 1.4 Printer Installation

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE/Vista, please visit [www.draytek.com](http://www.draytek.com).

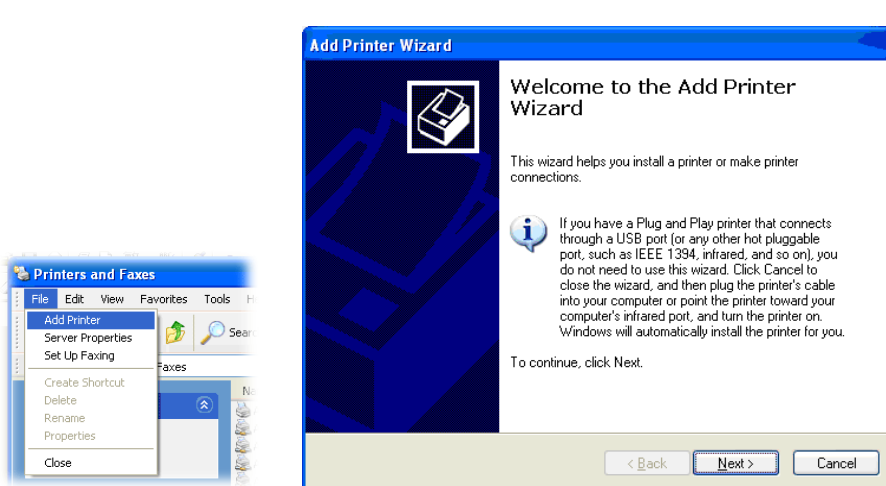


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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



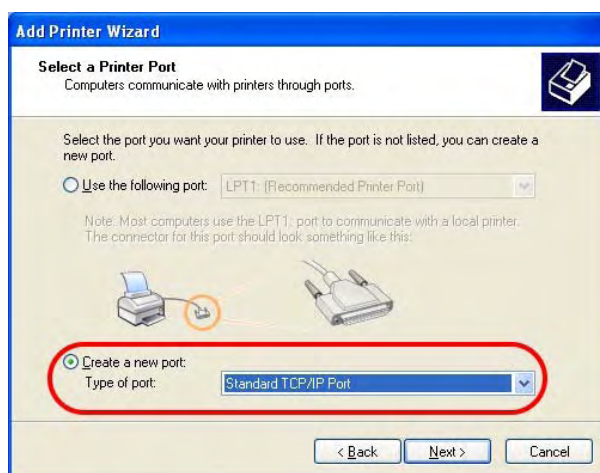
3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



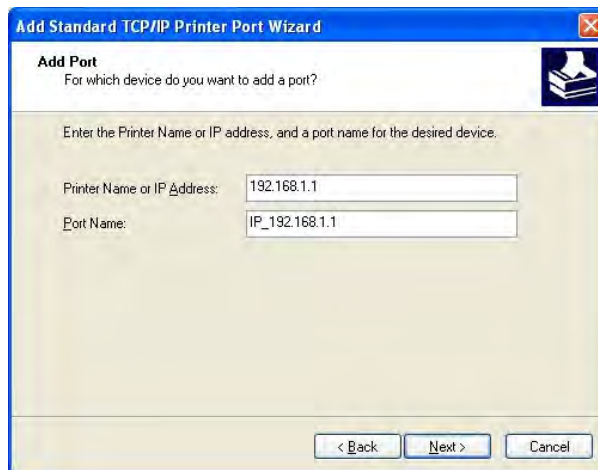
4. Click Local printer attached to this computer and click Next.



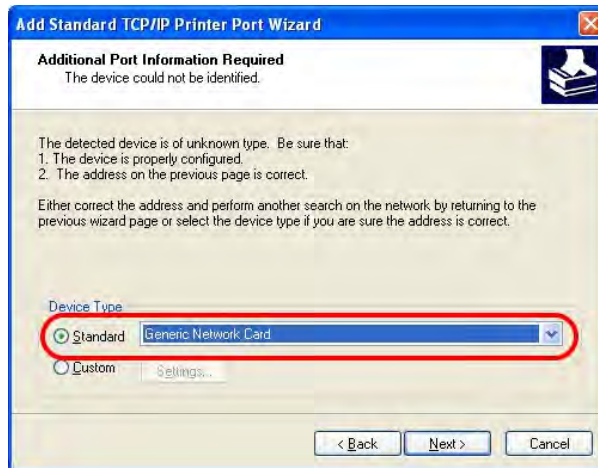
5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click Next.



- 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**.



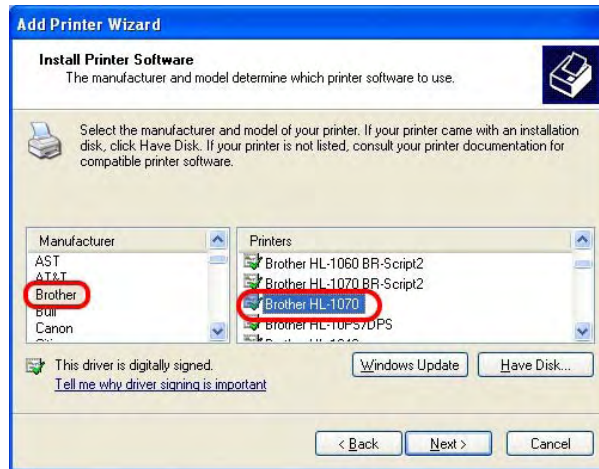
- Click **Standard** and choose **Generic Network Card**.



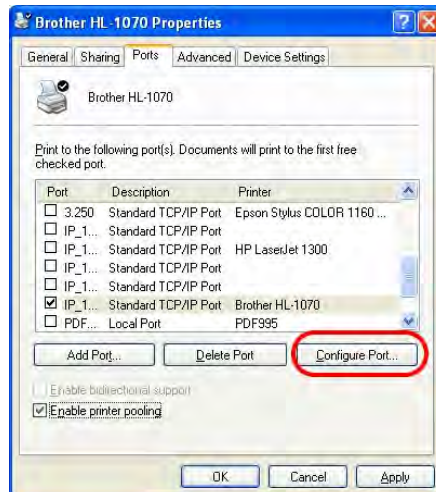
- Then, in the following dialog, click **Finish**.



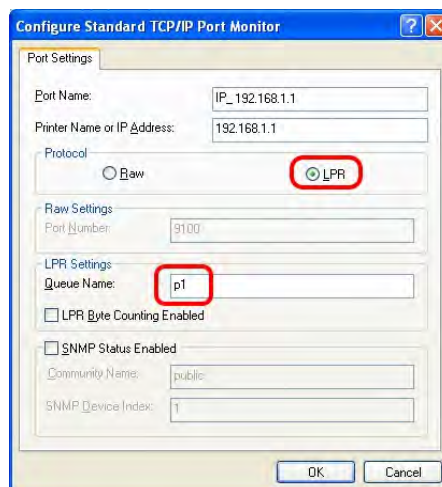
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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.



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



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](http://www.draytek.com) to find out the printer list. Open **Support >FAQ**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.

The screenshot shows the DrayTek website's Support > FAQ page. The navigation bar includes links for About DrayTek, Products, Support, Partners, and Contact Us. The breadcrumb trail is Home > Support > FAQ. There are two main content areas: 'FAQ - Basic' and 'FAQ - Printer Server'. The 'FAQ - Basic' section contains 10 questions, with question 05 highlighted in orange. The 'FAQ - Printer Server' section contains 9 questions, with question 05 highlighted in orange. A sidebar on the right lists various FAQ categories, with 'Printer Server' highlighted in a dark red box.

Home > Support > **FAQ**

**FAQ - Basic**

01. What are the differences among these firmware file formats ?
02. How could I get the telnet command for routers ?
03. How can I backup/restore my configuration settings ?
04. How do I reset/clear the router's password ?
05. How to bring back my router to its default value ?
06. How do I tell the type of my Vigor Router is AnnexA or AnnexB? ( For ADSL model only )
07. Ways for firmware upgrade.
08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?
09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what should I do?
10. How to upgrade firmware of Vigor Router remotely ?

**FAQ - Printer Server**

01. How do I configure LPR printing on Windows2000/XP ?
02. How do I configure LPR printing on Windows98/Me ?
03. How do I configure LPR printing on Linux boxes ?
04. Why there are some strange print-out when I try to print my documents through Vigor210 4P / 2300's print server?
05. **What types of printers are compatible with Vigor router?**
06. What are the limitations in the USB Printer Port of Vigor Router ?
07. What is the printing buffer size of Vigor Router ?
08. How do I configure LPR printing on Mac OSX ?
09. How do I configure LPR printing on My Windows Vista ?

**FAQ**

- Basic
- Advanced
- VPN
- DHCP
- Wireless
- VoIP
- QoS
- ISDN
- Firewall / IP Filter
- Printer Server**
- USB ISDN TA
- USB

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



# 2

## Configuring Basic Settings

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

### 2.1 Two-Level Management

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

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

### 2.2 Accessing Web Page

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



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

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

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



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

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

## 2.3 Changing Password

No matter user mode operation or admin mode operation, please change the password for the original security of the router.

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password.
2. Please type “admin/admin” on Username/Password for admin mode. Otherwise, do not type any word (both username and password are Null for user mode) on the window and click **Login** on the window.
3. Now, the **Main Screen** will appear.

**Vigor2130 Series**  
High Speed Gigabit Router

DrayTek

Auto Logout ▾

- Quick Start Wizard
- Online Status
- ▶ WAN
- ▶ LAN
- ▶ NAT
- ▶ Firewall
- ▶ Bandwidth Management
- ▶ Applications
- ▶ VPN and Remote Access
- ▶ Wireless LAN
- ▶ USB Application
- ▶ User
- ▶ System Maintenance
- ▶ Diagnostics

Logout

All Rights Reserved.

Admin mode

System Status

Auto-refresh  Refresh

Model : Vigor2130  
Platform : VSC7501  
Bootloader Version : Dray-Boot 1.0.0E  
Firmware Version : v1.1.0\_RC6  
Build Date/Time : r753 Tue Aug 25 16:11:42 CST 2009  
Hardware NAT Version : 1.0.0.13  
System Date : Mon Aug 31 03:02:52 2009  
System Uptime : 3d 10:39:36

LAN	
MAC Address	: 00:50:7F:C7:7B:30
IP Address	: 192.168.1.1
IP Mask	: 255.255.255.0

WAN	
MAC Address	: 00:50:7F:C7:7B:31
IP Address	: 192.168.5.21
IP Mask	: 255.255.255.0
Default Gateway	: 192.168.5.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

Main screen for admin mode operation (full configuration)

**Vigor2130 Series**  
High Speed Gigabit Router

DrayTek

Auto Logout ▾

- Quick Start Wizard
- Online Status
- ▶ WAN
- ▶ LAN
- ▶ NAT
- ▶ Bandwidth Management
- ▶ Applications
- ▶ Wireless LAN
- ▶ USB Application
- ▶ User
- ▶ System Maintenance

Logout

All Rights Reserved.

User mode

System Status

Auto-refresh  Refresh

Model : Vigor2130  
Platform : VSC7501  
Bootloader Version : Dray-Boot 1.0.0E  
Firmware Version : v1.1.0\_RC6  
Build Date/Time : r753 Tue Aug 25 16:11:42 CST 2009  
Hardware NAT Version : 1.0.0.13  
System Date : Mon Aug 31 02:59:22 2009  
System Uptime : 3d 10:36:05

LAN	
MAC Address	: 00:50:7F:C7:7B:30
IP Address	: 192.168.1.1
IP Mask	: 255.255.255.0

WAN	
MAC Address	: 00:50:7F:C7:7B:31
IP Address	: 192.168.5.21
IP Mask	: 255.255.255.0
Default Gateway	: 192.168.5.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

Main screen for user mode operation (simple configuration)

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



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

**System Maintenance >> System Password**

---

**System Password**

New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Or

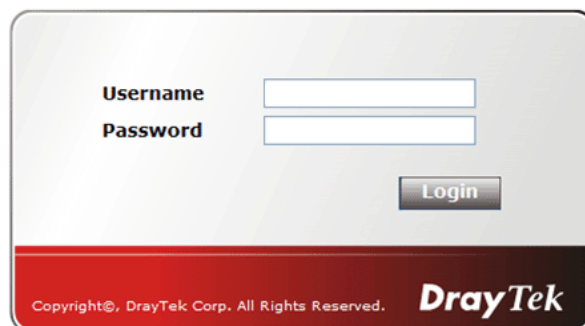
**System Maintenance >> User Password**

---

**User Password**

New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

5. Type **New Password** in New Password and Confirm New Password fields. Then click **OK** to continue.
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.



The image shows a login screen with a light gray background and a red footer. It features two input fields: 'Username' and 'Password'. Below the fields is a 'Login' button. The footer contains the text 'Copyright©, DrayTek Corp. All Rights Reserved.' and the 'DrayTek' logo.

## 2.4 Quick Start Wizard



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

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

### Quick Start Wizard

#### Welcome to the Quick Start Wizard!

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

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

< Back

Next >

Finish

Cancel

### 2.4.1 Setting up the Password

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

### Quick Start Wizard

#### User Password

Old Password

New Password

Confirm Password

< Back

Next >

Finish

Cancel

## 2.4.2 Setting up the Time Zone

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

Quick Start Wizard

### Time Configuration

Time Zone	Unknown
<b>NTP Servers</b>	
Delete	0.openwrt.pool.ntp.org
Delete	1.openwrt.pool.ntp.org
Delete	2.openwrt.pool.ntp.org
Delete	3.openwrt.pool.ntp.org
Add NTP server	

< Back   Next >   Finish   Cancel

## 2.4.3 Setting up the Internet Connection

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

Quick Start Wizard

### WAN IP Configuration

Connection Type	DHCP
Clone MAC Address	<input type="checkbox"/>
Enable	<input type="checkbox"/>

< Back   Next >   Finish   Cancel

## Static IP

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

### Quick Start Wizard

#### WAN IP Configuration

Connection Type	Static IP
<b>Static IP</b>	
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
<b>Clone MAC Address</b>	
Enable	<input type="checkbox"/>

< Back    Next >    Finish    Cancel

<b>IP Address</b>	Type the IP address.
<b>Subnet Mask</b>	Type the subnet mask.
<b>Gateway</b>	Type the gateway IP address.
<b>Primary DNS Server</b>	Type in the primary IP address for the router
<b>Secondary DNS Server</b>	Type in secondary IP address for necessity in the future.
<b>Enable</b>	The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.
<b>Clone MAC Address</b>	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	<input checked="" type="checkbox"/>	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.

The screenshot shows the 'Quick Start Wizard' interface. Under the 'WAN IP Configuration' section, the 'Connection Type' is set to 'DHCP'. Below this, there is a section for 'Clone MAC Address' with a checkbox labeled 'Enable' which is currently unchecked. At the bottom of the wizard, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

### 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.

This screenshot shows the configuration area for cloning a MAC address. The 'Enable' checkbox is checked with a green checkmark. To its right is a button labeled 'Clone MAC Address'. Below these, the 'MAC Address' field contains the value '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
<b>PPPoE</b>	
Username	<input type="text"/>
Password	<input type="text"/>
Redial Policy	Connect on Demand
Idle Time out	<input type="text"/>
MTU Size	<input type="text"/>
<b>Clone MAC Address</b>	
Enable	<input checked="" type="checkbox"/> <input type="button" value="Clone MAC Address"/>
MAC Address	<input type="text"/>

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

- Idle Time Out** Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds. The range is XX ~ XX.
- MTU Size** It means Max Transmit Unit for packet. The default setting is 1442.
- Enable** The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.
- Clone MAC Address** It is available when the box of Enable is checked. Click Clone PC Address. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/> <input type="button" value="Clone MAC Address"/>
MAC Address	<input type="text" value="00-0E-A6-2A-D5-A1"/>

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

## PPTP/L2TP

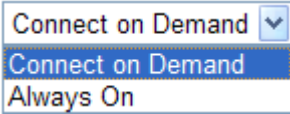
if you click PPTP/L2TP as the protocol, please manually enter the Username/Password provided by your ISP and all the required information.

### Quick Start Wizard

**WAN IP Configuration**

Connection Type	PPTP
<b>PPTP Settings</b>	
Username	<input type="text"/>
Password	<input type="text"/>
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	<input type="text"/>
MTU Size	<input type="text"/>
<b>Clone MAC Address</b>	
Enable	<input checked="" type="checkbox"/> Clone MAC Address
MAC Address	<input type="text"/>

< Back   Next >   Finish   Cancel

- User Name** Assign a specific valid user name provided by the ISP.
- Password** Assign a valid password provided by the ISP.
- Server Address** Specify the IP address of the PPTP server.
- WAN IP Network Settings** You can choose Static IP or DHCP as WAN IP network setting.
- IP Address** Type the IP address if you choose Static IP as the WAN IP network setting.
- Subnet Mask** Type the subnet mask if you chose Static IP as the WAN IP.
- Redial Policy** If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.
- 
- Idle Time Out** Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds. The range is XX ~ XX.
- MTU Size** It means Max Transmit Unit for packet. The default setting is 1442.
- Enable** The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.

### Clone MAC Address

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

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

## 2.4.4 Setting up the Wireless Connection

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

### Quick Start Wizard

#### Wireless System Configuration

Enable Wireless LAN	<input type="checkbox"/>
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
<b>Wireless Security Configuration</b>	
Encryption	None

< Back   Next >   Finish   Cancel

### Enable Wireless LAN

Check the box to enable the wireless function.

### SSID Broadcast

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

### SSID

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

### Wireless Mode

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

### Country Region Code

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

### Channel

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

### Encryption

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

None	▼
None	
WEP	
WPA-PSK	
WPA-RADIUS	
WPS	



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	<input type="checkbox"/>
SSID Broadcast	Show <input type="button" value="v"/>
SSID	DrayTek <input type="button" value="v"/>
Wireless Mode	Mixed (11b+11g+11n) <input type="button" value="v"/>
Country Region Code	0: channels 1-11 <input type="button" value="v"/>
Channel	Channel 11, 2462MHz <input type="button" value="v"/>
<b>Wireless Security Configuration</b>	
Encryption	WEP <input type="button" value="v"/>
<b>WEP Configuration</b>	
Default Key	Key1 <input type="button" value="v"/>
Key1	<input type="text"/>
Key2	<input type="text"/>
Key3	<input type="text"/>
Key4	<input type="text"/>
Authentication Mode	OPEN <input type="button" value="v"/>

**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	<input type="checkbox"/>
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
<b>Wireless Security Configuration</b>	
Encryption	WPA-PSK
<b>WPA-PSK Configuration</b>	
Type	WPA
WPA Algorithm	TKIP
WPA Pre-Shared Key	

< Back   Next >   Finish   Cancel

### Type

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

Auto(WPA or WPA2)
WPA
WPA2
Auto(WPA or WPA2)

### WPA Algorithm

Choose the WPA algorithm, TKIP, AES or Auto.

AES
TKIP
AES
Auto(TKIP or AES)

### 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	<input type="checkbox"/>
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz
<b>Wireless Security Configuration</b>	
Encryption	WPA-RADIUS
<b>WPA-RADIUS Configuration</b>	
Type	WPA
WPA Algorithm	TKIP
Server IP Address	0.0.0.0
Destination Port	1812
Shared Secret	radius_secret

< Back   Next >   Finish   Cancel

### Type

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

Auto(WPA or WPA2)
WPA
WPA2
Auto(WPA or WPA2)

### WPA Algorithm

Choose the WPA algorithm, TKIP, AES or Auto.

AES
TKIP
AES
Auto(TKIP or AES)

### Server IP Address

Enter the IP address of RADIUS server.

### Destination Port

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

## Shared Secret

The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

## WPS

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

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	<input type="checkbox"/>
SSID Broadcast	Show <input type="button" value="v"/>
SSID	DrayTek <input type="text"/>
Wireless Mode	Mixed (11b+11g+11n) <input type="button" value="v"/>
Country Region Code	0: channels 1-11 <input type="button" value="v"/>
Channel	Channel 11, 2462MHz <input type="button" value="v"/>
<b>Wireless Security Configuration</b>	
Encryption	WPS <input type="button" value="v"/>
<b>WPS Configuration</b>	
Configure via Push Button	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="Start PIN"/>

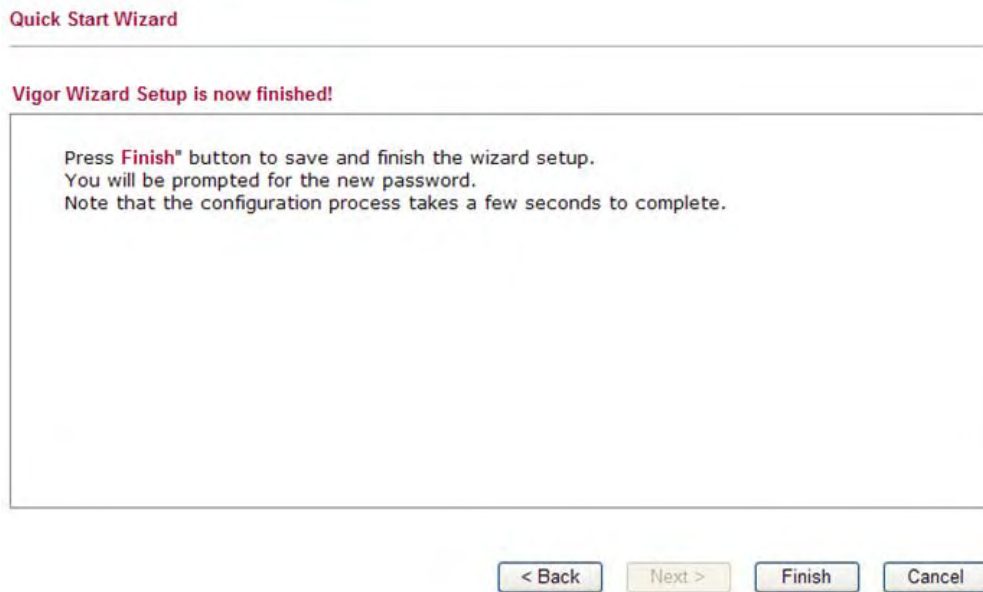
**Configure via Push Button** Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You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

**Configure via Client PinCode** Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

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

## 2.4.5 Save 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.



## 2.5 Online Status

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

### Online status for DHCP

**Online Status**

Auto-refresh  [Refresh](#)

System Status						System Uptime: 0d 03:15:19
<b>LAN Status</b>						
<b>IP Address</b>	<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>		
192.168.1.1	10991	11895	10669316	1696736		
<b>WAN Status</b>						<a href="#">&gt;&gt; Release</a>
<b>IP</b>	<b>GW IP</b>	<b>Mode</b>	<b>Up Time</b>			
192.168.5.21	192.168.5.1	DHCP	0d 03:14:45			
<b>Primary DNS</b>	<b>Secondary DNS</b>	<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>	
168.95.1.1		10253	20397	1640213	11506611	

Detailed explanation is shown below:

#### *LAN Status*

- IP Address** Displays the IP address of the LAN interface.
- TX Packets** Displays the total transmitted packets at the LAN interface.
- RX Packets** Displays the total number of received packets at the LAN interface.

#### *WAN Status*

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

<b>Name</b>	Displays the name set in WAN1/WAN web page.
<b>Mode</b>	Displays the type of WAN connection (e.g., PPPoE).
<b>Up Time</b>	Displays the total uptime of the interface.
<b>IP</b>	Displays the IP address of the WAN interface.
<b>GW IP</b>	Displays the IP address of the default gateway.
<b>TX Packets</b>	Displays the total transmitted packets at the WAN interface.
<b>TX Rate</b>	Displays the speed of transmitted octets at the WAN interface.
<b>RX Packets</b>	Displays the total number of received packets at the WAN interface.
<b>RX Rate</b>	Displays the speed of received octets at the WAN interface.

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

## 2.6 Saving Configuration

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

**Status: Ready**

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

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

# 3

## User Mode Operation

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

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

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

**Vigor2130 Series**  
High Speed Gigabit Router

DrayTek

Auto Logout ▾

- Quick Start Wizard
- Online Status
- WAN
- LAN
- NAT
- Bandwidth Management
- Applications
- Wireless LAN
- USB Application
- User
- System Maintenance

Logout

All Rights Reserved.

User mode

**System Status**

Auto-refresh  Refresh

Model : Vigor2130  
Platform : VSC7501  
Bootloader Version : Dray-Boot 1.0.0E  
Firmware Version : v1.1.0\_RC6  
Build Date/Time : r753 Tue Aug 25 16:11:42 CST 2009  
Hardware NAT Version : 1.0.0.13  
System Date : Mon Aug 31 02:59:22 2009  
System Uptime : 3d 10:36:05

LAN	
MAC Address	: 00:50:7F:C7:7B:30
IP Address	: 192.168.1.1
IP Mask	: 255.255.255.0

WAN	
MAC Address	: 00:50:7F:C7:7B:31
IP Address	: 192.168.5.21
IP Mask	: 255.255.255.0
Default Gateway	: 192.168.5.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

### 3.1 WAN

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

#### Basics of Internet Protocol (IP) Network

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

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

## What are Public IP Address and Private IP Address

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

## Get Your Public IP Address from ISP

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

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

## Network Connection by 3G USB Modem

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

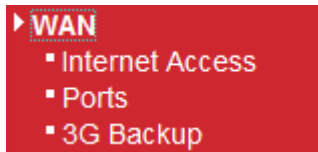


After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem also can be used as backup device. Therefore, when WAN is not available, the router will use 3.5G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



Modem will be listed on DrayTek web site. Please visit [www.draytek.com](http://www.draytek.com) for more detailed information.

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



### 3.1.1 Internet Access

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

WAN >> Internet Access

WAN IP Configuration

Connection Type	DHCP	▼
-----------------	------	---

DHCP Settings

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

Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK Cancel

### Static

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

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

WAN >> Internet Access

WAN IP Configuration

Connection Type	Static IP
<b>Static IP Settings</b>	
IP Address	172.16.3.229
Subnet Mask	255.255.0.0
Gateway IP Address	172.16.3.4
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
<b>Clone MAC Address</b>	
Enable	<input type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- IP Address** Type the IP address.
- Subnet Mask** Type the subnet mask.
- Gateway IP Address** Type the gateway IP address.
- Primary DNS Server** Type in the primary IP address for the router if you want to use **Static IP** mode.
- Secondary DNS Server** Type in secondary IP address for using in the future if necessary.
- Clone MAC Address** It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	<input type="button" value="Clone MAC Address"/>
MAC Address		<input type="text" value="00-0E-A6-2A-D5-A1"/>

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

## DHCP

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

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	DHCP
-----------------	------

#### DHCP Settings

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

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK Cancel

### Router Name

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

### Clone MAC Address

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

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

## PPPoE

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

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	PPPoE
-----------------	-------

#### PPPoE Settings

Username	<input type="text"/>
Password	<input type="text"/>
Redial Policy	Connect on Demand
Idle Time out	<input type="text"/>
MTU Size	<input type="text"/>

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

### Username

Type in the username provided by ISP in this field.

<b>Password</b>	Type in the password provided by ISP in this field.
<b>Redial Policy</b>	<p>If you want to connect to Internet all the time, you can choose <b>Always On</b>. Otherwise, choose <b>Connect on Demand</b>.</p> <div style="border: 1px solid black; padding: 2px;"> <span>Connect on Demand ▾</span>  <span>Connect on Demand</span>  <span>Always On</span> </div>
<b>Idle Time Out</b>	Set the timeout for breaking down the Internet after passing through the time without any action. When you choose <b>Connect on Demand</b> , you have to type value here.
<b>MTU Size</b>	It means Max Transmit Unit for packet. The default setting is 1442. Leave blank for default value.
<b>Enable/Disable</b>	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
<b>Clone MAC Address</b>	<p>It is available when the box of Enable is checked. Click <b>Clone MAC Address</b>. The result will be displayed in the field of MAC Address.</p> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="text-align: left;"> <p>Enable <input checked="" type="checkbox"/></p> <p>MAC Address</p> </div> <div style="text-align: right;"> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Clone MAC Address</div> <div style="border: 1px solid gray; padding: 2px; display: inline-block;">00-0E-A6-2A-D5-A1</div> </div> </div>

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

## PPTP/L2TP

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

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	PPTP
<b>PPTP Settings</b>	
Username	<input type="text"/>
Password	<input type="password"/>
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	<input type="text"/>
MTU Size	<input type="text"/>
<b>Clone MAC Address</b>	
Enable	<input type="checkbox"/>

OK Cancel

- 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.
- Redial Policy** If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand** and
- |                   |
|-------------------|
| 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. When you choose **Connect on Demand**, you have to type value here.
- MTU Size** It means Max Transmit Unit for packet. The default setting is 1442.
- Clone MAC Address** It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

### 3G USB Modem

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

#### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	3G USB Modem
-----------------	--------------

#### 3G USB Modem Settings

SIM PIN code	<input type="text"/>	
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	<input type="text"/>	
PPP Password	<input type="text"/>	

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
-----------------------------------	---------------------------------------

- SIM PIN code**                      Type PIN code of the SIM card that will be used to access Internet.
- Modem Initial String1/2**      Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
- APN Name**                              APN means Access Point Name which is provided and required by some ISPs.
- Modem Dial String**                  Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
- PPP Username**                        Type the PPP username (optional).
- PPP Password**                        Type the PPP password (optional).
- Clone MAC Address**                It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

### 3.1.2 Ports

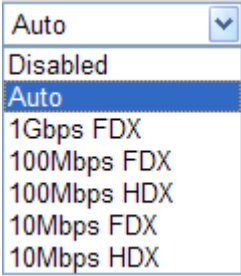
Ports page is used to change the setting for WAN port. You can set or reset the following items. All of them are described in detail below.

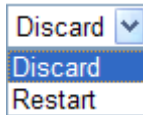
WAN >> Ports

Port Configuration

Port	Link	Current	Speed	Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
			Configured	Current Rx	Current Tx	Configured			
WAN	<span style="color: green;">●</span>	100fdx	Auto	✓	✓	<input checked="" type="checkbox"/>	1518	Discard	Disabled

- Port** It displays current network interface.
- Link** It displays current connection status. Green light means the WAN connection is successful.
- Current** It displays current speed that the router uses.
- Speed Configured** It can set the speed and duplex of the port. You can use the drop down list to choose the required speed for the router. If you have no idea in configuring speed, simple use the default setting, **Auto**.
 


- Flow Control** If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.  
 Current Rx: indicates whether pause frames on the port are obeyed.  
 Current Tx: indicates whether pause frames on the port are transmitted.
- Maximum Frame** This module offers 1518~9600 (Bytes) length to make the long packet for data transmission.
- Excessive Collision Mode** There are two modes for you to choose when excessive collision happened in half-duplex condition.

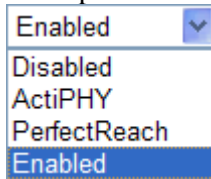


**Discard** - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

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

### Power Control

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



**Disabled:** All power savings mechanisms disabled.

**ActiPHY:** Link down power savings enabled.

**PerfectReach:** Link up power savings enabled.

**Enabled:** Both link up and link down power savings enabled.

### Refresh

Click this button to refresh the information for WAN port.

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

## 3.1.3 3G Backup

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

### WAN >> 3G backup

#### 3G Backup Configuration

<input type="checkbox"/> Enable 3G Backup		
SIM PIN code	<input type="text"/>	
Modem Initial String1	<input type="text" value="AT&amp;F"/>	(default:AT&F)
Modem Initial String2	<input type="text" value="ATE0V1X1&amp;D2&amp;C1S0=0"/>	(default:ATE0V1X1&D2&C1S0=0)
APN Name	<input type="text" value="internet"/>	(default:internet)
Modem Dial String	<input type="text" value="ATDT*99#"/>	(default:ATDT*99#)
PPP Username	<input type="text"/>	
PPP Password	<input type="text"/>	

OK Cancel

### SIM PIN code

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



<b>Modem Initial String1/2</b>	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
<b>APN Name</b>	APN means Access Point Name which is provided and required by some ISPs.
<b>Modem Dial String</b>	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
<b>PPP Username</b>	Type the PPP username (optional).
<b>PPP Password</b>	Type the PPP password (optional).
<b>Clone MAC Address</b>	It is available when the box of Enable is checked. Click <b>Clone MAC Address</b> . The result will be displayed in the field of MAC Address.

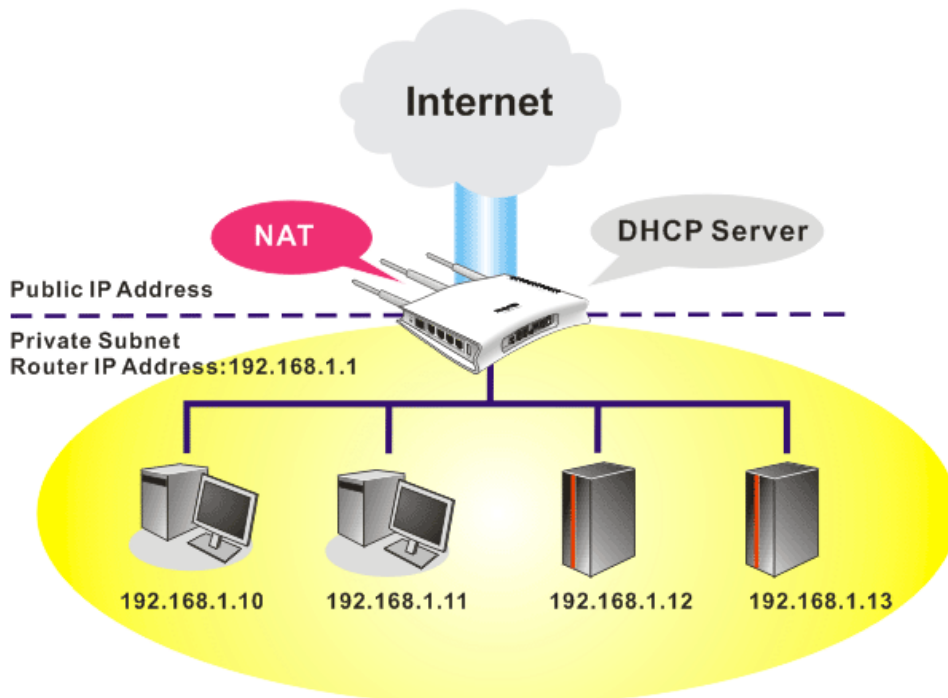
Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

## 3.2 LAN

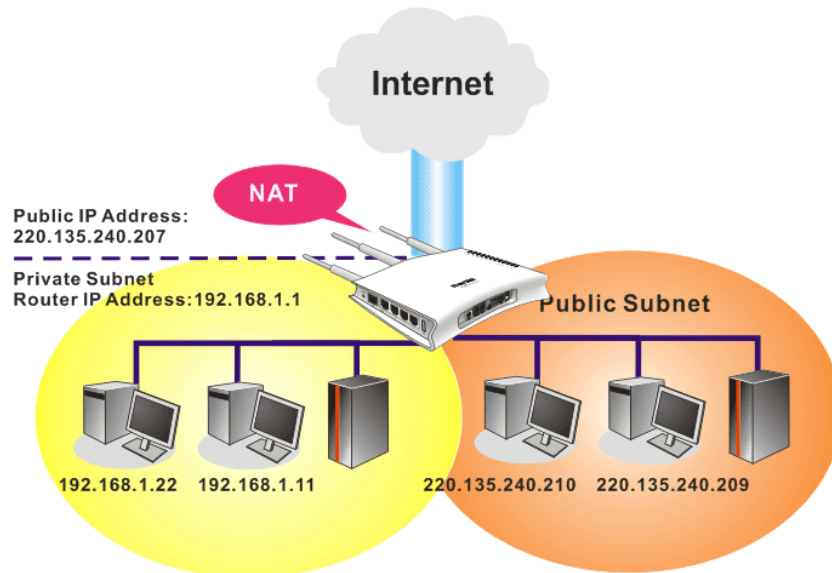
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

### Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



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

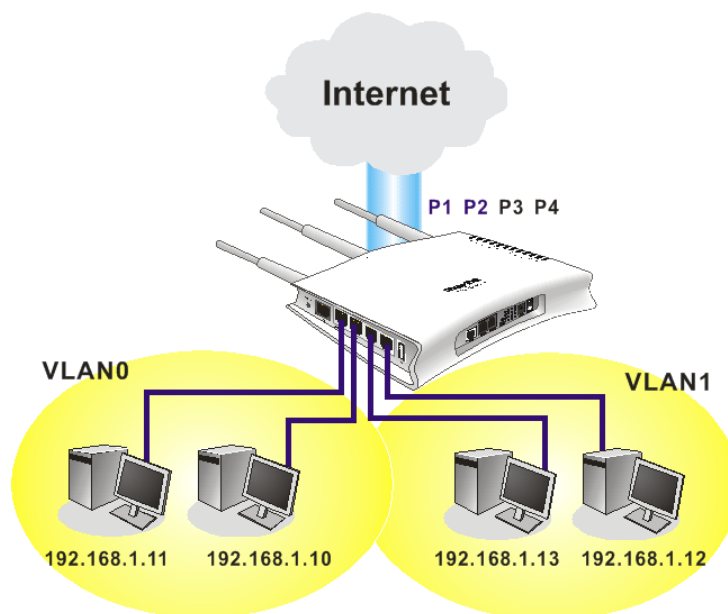


### What is Routing Information Protocol (RIP)

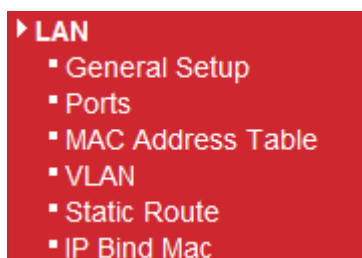
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### What are Virtual LANs and Rate Control

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



Below shows the LAN menu:



### 3.2.1 General Setup

This page provides you the general settings for LAN.

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

**LAN >> General Setup**

#### LAN IP Network Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

#### DHCP Server Configuration

Enable DHCP	<input checked="" type="checkbox"/>
Start IP Address	192.168.1.10
IP Pool Counts	50
Lease Time	720 minutes

OK Cancel

- IP Address** Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
- Subnet Mask** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
- Enable DHCP** DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.  
You can configure the router to serve as a DHCP server for the 2nd subnet. Check the box to enable DHCP server setting.
- Start IP Address** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.
- IP Pool Counts** Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.
- Lease Time** It allows you to set the leased time for the specified PC.
- After finishing all the settings here, please click **OK** to activate them.

### 3.2.2 Ports

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

LAN >> Ports

Port Configuration

Refresh

Port	Link	Current	Speed	Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
			Configured	Current Rx	Current Tx	Configured			
LAN1	<span style="color:red">●</span>	Down	Auto	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1518	Discard	Disabled
LAN2	<span style="color:green">●</span>	100fdx	Auto	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1518	Discard	Disabled
LAN3	<span style="color:red">●</span>	Down	Auto	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1518	Discard	Disabled
LAN4	<span style="color:red">●</span>	Down	Auto	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1518	Discard	Disabled

OK Cancel

#### Port

It displays current network interface.

#### Link

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

#### Current

It displays current speed that the router uses.

#### Speed Configured

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

#### Flow Control

If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.

Current Rx: indicates whether pause frames on the port are obeyed.

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

#### Maximum Frame

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

#### Excessive Collision Mode

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

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

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

**Power Control**

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

**Disabled:** All power savings mechanisms disabled.

**ActiPHY:** Link down power savings enabled.

**PerfectReach:** Link up power savings enabled.

**Enabled:** Both link up and link down power savings enabled.

**Refresh**

Click this button to refresh the information for LAN ports.

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

### 3.2.3 MAC Address Table

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

**LAN >> MAC Address Table**

**MAC Address Table Configuration**

**Aging Configuration**

Disable Automatic Aging

Age Time  seconds

**MAC Table Learning**

	WAN	LAN1	Port Members			
			LAN2	LAN3	LAN4	
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Static MAC Table Configuration**

Delete	VLAN ID	MAC Address	WAN	Port Members			
				LAN1	LAN2	LAN3	LAN4
<input type="button" value="Add New Static Entry"/>							

- Disable Automatic Aging** Stop the MAC table aging timer, the learned MAC address will not age out automatically. The default setting is enabled. Check the box to disable this function if required.
- Age Time** Delete a MAC address idling for a period of time from the following MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.
- MAC Table Learning** List the port members which apply dynamic learning mechanism or not.  
**Auto** - Enable this port MAC address dynamic learning mechanism.  
**Disable** - Disable this port MAC address dynamic learning mechanism, only support static MAC address setting.  
**Secure** - Disable this port MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU.
- Static MAC Table Config..** Specify static MAC address with VLAN ID to apply aging configuration.  
**Delete** - Click the button to remove the VLAN setting.  
**VLAN ID** - Specify the interface for the port members.  
**MAC Address** - It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 - 40 - C7 - D6 - 00 - 02.  
**WAN/LAN1~4** - Check the port to apply this VLAN setting.

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

**Static MAC Table Configuration**

		VLAN ID	MAC Address	Port Members				
Delete				WAN	LAN1	LAN2	LAN3	LAN4
<input type="button" value="Delete"/>		1(LAN)	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Add new static entry"/>								

### 3.2.4 VLAN

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

**LAN >> VLAN**

**Private VLAN Membership Configuration**

Delete	PVLAN ID	LAN1	Port Members			
			LAN2	LAN3	LAN4	
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="button" value="Add New Private VLAN"/>						

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

## LAN >> VLAN

### Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members			
		LAN1	LAN2	LAN3	LAN4
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Private VLAN

OK Cancel

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

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

## LAN >> VLAN

### Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members			
		LAN1	LAN2	LAN3	LAN4
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Private VLAN

OK Cancel

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

## 3.2.5 Static Route

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

### LAN >> Static Route

#### Static Route Configuration

Index	Destination Address	Status
<p>Add</p>		

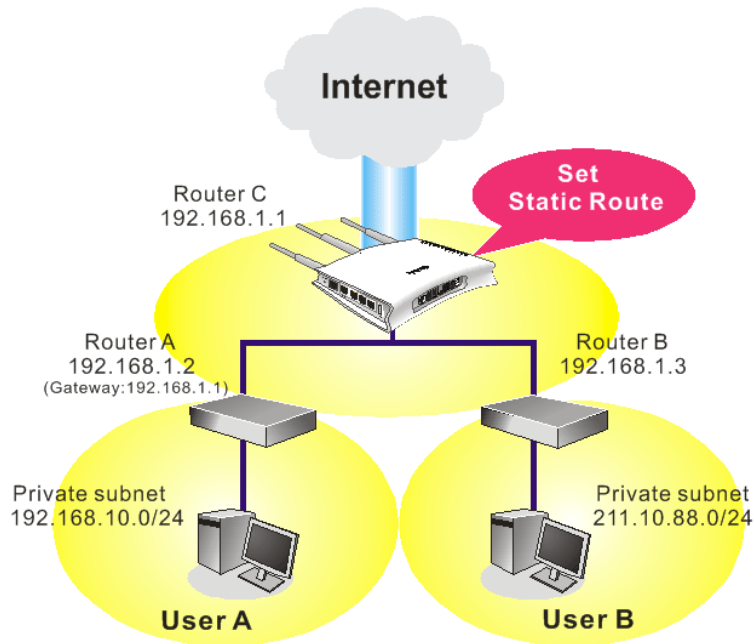
<b>Index</b>	The number (1 to 10) under Index displays current static router.
<b>Destination Address</b>	Display the destination address of the static route.
<b>Status</b>	Display the status of the static route.
<b>Add</b>	Add a new static route.

## 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	
<input checked="" type="checkbox"/> Enable	
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2

OK Cancel

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

Subnet Mask

Gateway IP Address

3. Verify current routing table.

LAN >> Static Route

Static Route Configuration

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

### 3.2.6 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 Bind List** | [Select All](#) | [Sort](#)

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

Index	IP Address	Mac Address
-------	------------	-------------

**Add and Edit**

IP Address

Mac Address

<b>Enable</b>	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
<b>Disable</b>	Click this radio button to disable this function. All the settings on this page will be invalid.
<b>Strict Bind</b>	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
<b>ARP Table</b>	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 <b>Add</b> below.
<b>Add and Edit</b>	<b>IP Address</b> – Type the IP address that will be used for the specified MAC address. <b>Mac Address</b> – Type the MAC address that is used to bind with the assigned IP address.
<b>Refresh</b>	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.
<b>IP Bind List</b>	It displays a list for the IP bind to MAC information.
<b>Add</b>	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in <b>Add and Edit</b> to the table of <b>IP Bind List</b> .
<b>Edit</b>	It allows you to edit and modify the selected IP address and MAC address that you create before.
<b>Remove</b>	You can remove any item listed in <b>IP Bind List</b> . Simply click and select the one, and click <b>Remove</b> . The selected item will be removed from the <b>IP Bind List</b> .

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

### 3.3 NAT

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

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

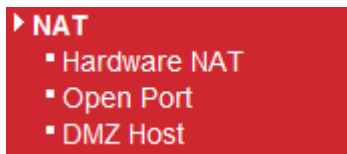
The benefit of the NAT includes:

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

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

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

Below shows the menu items for NAT.



### 3.3.1 Hardware NAT

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

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

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

**NAT >> Hardware NAT**

**Hardware NAT Configuration**

Hardware NAT	Enabled <input type="button" value="v"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### 3.3.2 Open Ports

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

**NAT >> Open Port**

**Port Forwarding**

Name	Protocol	Start Port	End Port	Local Host	Local Port
<i>No Port Forwarding</i>					

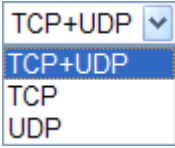
Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

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

## NAT >> Open Port

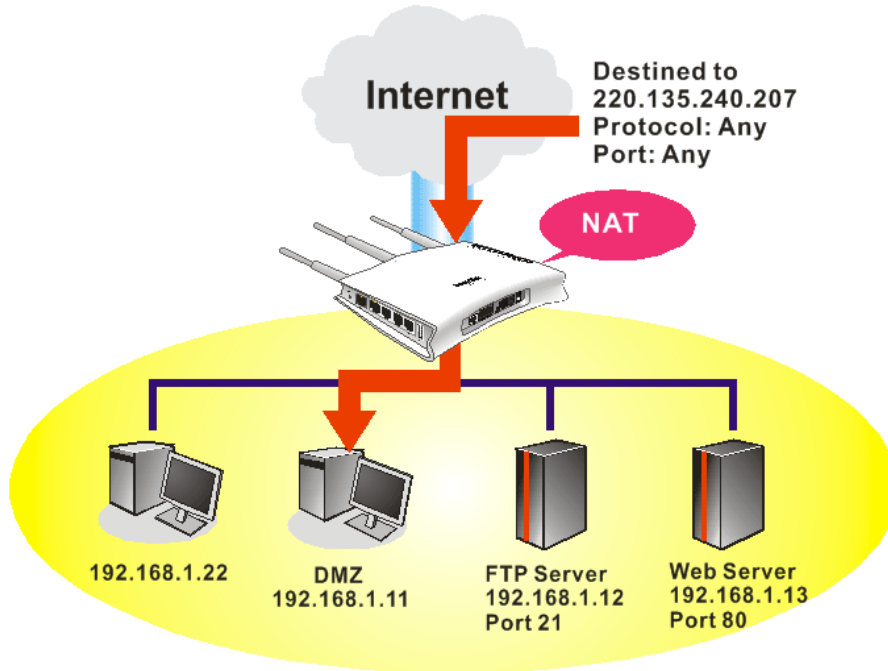
### Add Port Forwarding Entry

Name	<input type="text"/>
Protocol	TCP+UDP ▾
Start Port	<input type="text"/>
End Port (optional)	<input type="text"/>
Local Host	<input type="text"/>
Local Port (optional)	<input type="text"/>

- Name** Specify the name for the defined network service.
- Protocol** Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**.
- 
- Start Port** Specify the starting port number of the service offered by the local host.
- End Port (optional)** Specify the ending port number of the service offered by the local host.
- Local Host** Enter the private IP address of the local host.
- Local Port (optional)** If it is configured, the forwarded traffic is mapped to this port on the local host.

### 3.3.3 DMZ Host

Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



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

Click **DMZ Host** to open the following page:

NAT >> DMZ Host

DMZ Host

<b>Enable</b> <input checked="" type="checkbox"/>	<b>DMZ IP</b> <input type="text" value="0.0.0.0"/>
--	---

**Enable**

Check to enable the DMZ Host function.

**DMZ IP**

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

## 3.4 Bandwidth Management

Below shows the menu items for Bandwidth Management.



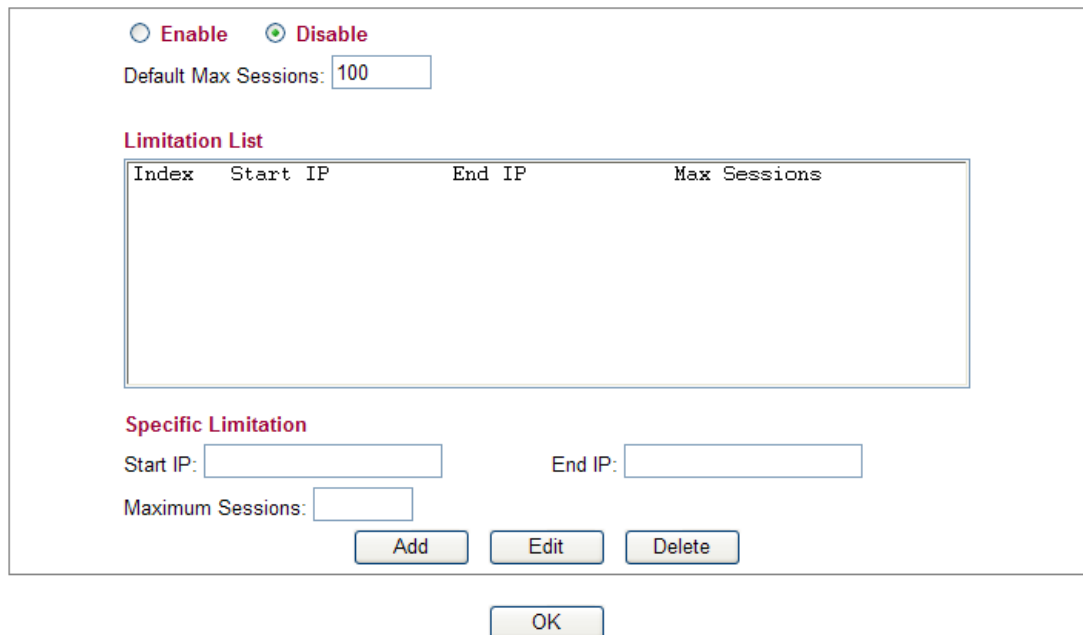
### 3.4.1 Session Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

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

**Bandwidth Management >> Session Limit**

#### Session Limit Configuration



The configuration page for Session Limit. At the top, there are two radio buttons: 'Enable' (unselected) and 'Disable' (selected). Below them is a text input field for 'Default Max Sessions' with the value '100'. A section titled 'Limitation List' contains a table with columns 'Index', 'Start IP', 'End IP', and 'Max Sessions'. Below the table is a 'Specific Limitation' section with input fields for 'Start IP', 'End IP', and 'Maximum Sessions'. At the bottom of this section are three buttons: 'Add', 'Edit', and 'Delete'. At the very bottom of the page is an 'OK' button.

To activate the function of limit session, simply click **Enable** and set the default session limit.

**Enable** Click this button to activate the function of limit session.

**Disable** Click this button to close the function of limit session.

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

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

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

- End IP** Defines the end LAN IP address for limit session.
- Maximum Sessions** Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
- Add** Adds the specific session limitation onto the list above.
- Edit** Allows you to edit the settings for the selected limitation.
- Delete** Remove the selected settings existing on the limitation list.

When you finish adding a new session limit, simply click **OK**. The following page will appear for you to check.

### 3.4.2 Bandwidth Limit

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

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

[Bandwidth Management >> Bandwidth Limit](#)

#### Bandwidth Limit Configuration

**Enable**     **Disable**

Default TX Limit:  Kbps      Default RX Limit:  Kbps

**Limitation List**

Index	Start IP	End IP	TX limit	RX limit

**Specific Limitation**

Start IP:       End IP:

TX Limit:  Kbps      RX Limit:  Kbps

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

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

- Enable** Click this button to activate the function of limit bandwidth.
- Disable** Click this button to close the function of limit bandwidth.
- Default TX limit** Define the default speed of the upstream for each computer in LAN.

<b>Default RX limit</b>	Define the default speed of the downstream for each computer in LAN.
<b>Limitation List</b>	Display a list of specific limitations that you set on this web page.
<b>Start IP</b>	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.
<b>End IP</b>	Define the end IP address for the specific limitation.
<b>TX Limit</b>	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.
<b>RX Limit</b>	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.
<b>Add</b>	Add the specific speed limitation onto the list above.
<b>Edit</b>	Allows you to edit the settings for the selected limitation.
<b>Delete</b>	Remove the selected settings existing on the limitation list.

When you finish adding a new bandwidth limit, simply click **OK**. The following page will appear for you to check.

### 3.4.3 Port Rate Control

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

#### Bandwidth Management >> Port Rate Control

##### Rate Limit Configuration

Port	Policer Enabled	Policer Rate(Rx)	Policer Unit	Shaper Enabled	Shaper Rate(Tx)	Shaper Unit
WAN	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	10	Mbps

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

OK Cancel

<b>Port</b>	Represent LAN or WAN interface.
<b>Policer Enabled</b>	Check this box to enable policer function.
<b>Policer Rate(Rx)</b>	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.
<b>Policer Unit</b>	Determine the unit (kbps/Mbps) for policer.
<b>Shaper Enabled</b>	Check this box to enable shaper function.



<b>Shaper Rate (Tx)</b>	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.
<b>Shaper Unit</b>	Determine the unit (kbps/Mbps) for shaper function.

### 3.4.4 QoS Control List

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

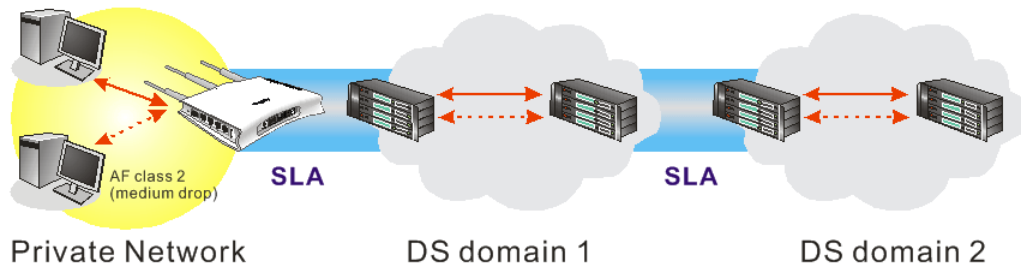
There are two components within Primary configuration of QoS deployment:

- **Classification:** Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- **Scheduling:** Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



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

In the **Bandwidth Management** menu, click **QoS Control List (QCL)** to open the web page.

**Bandwidth Management >> QoS Control List**

#### QoS Control List Configuration

QCL #

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

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

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

**Type Value** Display the value specified for the QCE.


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

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

## QoS Control List Configuration

QCL #	1
QCE Type	Type
TCP/UDP Port	22 - 23

### Adding a New QCE

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

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

[Bandwidth Management >> QoS Control List](#)

**QCE Configuration**

QCE Type	Ethernet Type
Ethernet Type Value	0xFFFF
Traffic Class	Low

Low  
Normal  
Medium  
High

OK Cancel

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

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

[Bandwidth Management >> QoS Control List](#)

**QCE Configuration**

QCE Type	VLAN ID
VLAN ID	1
Traffic Class	Low

Low  
Normal  
Medium  
High

OK Cancel

- 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

Low  
Normal  
Medium  
High  
OK Cancel

**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

Low  
Normal  
Medium  
High  
OK Cancel

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

**Bandwidth Management >> QoS Control List**

**QCE Configuration**

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

Low  
Normal  
Medium  
High  
OK Cancel

- 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	Low



Low  
Normal  
Medium  
High

OK Cancel

**Editing a QCE**

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

**Moving Up/Down a QCE**

Click  and  to move a QCE up and down.

**Deleting a QCE**

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

**3.4.5 Ports Priority**

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

**Bandwidth Management >> Ports Priority**

**Port QoS Configuration**

Port	Default Class	QCL #	Queuing Mode	Queue 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
WiFi1	Normal	1	Weighted	1	2	4	8

OK Cancel

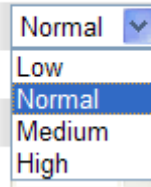
**Port**

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

### Default Class

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

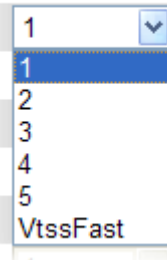
#### Default Class



### QCL

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

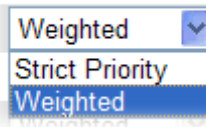
#### QCL #



### Queuing Mode

Use the drop down list to choose suitable mode.

#### Queuing Mode



### Queue Weighted

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

## 3.4.6 QoS Statistics

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

### 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
<a href="#">WAN</a>	58350	61843	69518	0	76195	63030	22	12
<a href="#">LAN1</a>	0	0	0	0	0	0	0	0
<a href="#">LAN2</a>	57361	7575	1953	61191	66042	75655	21	0
<a href="#">LAN3</a>	0	0	0	0	0	0	0	0
<a href="#">LAN4</a>	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

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		

<b>Rx Packets</b>	Display the counting number of the packet received.
<b>Rx Octets</b>	Display the total received bytes.
<b>Rx Unicast</b>	Display the counting number of the received unicast packet.
<b>Rx Broadcast</b>	Display the counting number of the received broadcast packet.
<b>Rx Pause</b>	Display the counting number of the received pause packet.
<b>RX 64 Bytes</b>	Display the number of 64-byte frames in good and bad packets received.
<b>RX 65-127 Bytes</b>	Display the number of 65 ~ 127-byte frames in good and bad packets received.
<b>RX 128-255 Bytes</b>	Display the number of 128 ~ 255-byte frames in good and bad packets received.
<b>RX 256-511 Bytes</b>	Display the number of 256 ~ 511-byte frames in good and bad packets received.
<b>RX 512-1023 Bytes</b>	Display the number of 512 ~ 1023-byte frames in good and bad packets received.
<b>RX 1024- 1526 Bytes</b>	Display the number of 1024-1522-byte frames in good and bad packets received.
<b>RX 1527 Bytes</b>	Display the number of 1527-byte frames in good and bad packets received.

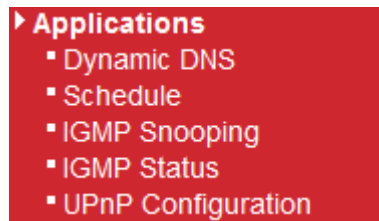
<b>Rx Low</b>	Display the low queue counter of the packet received.
<b>Rx Normal</b>	Display the normal queue counter of the packet received.
<b>Rx Medium</b>	Display the medium queue counter of the packet received.
<b>Rx High</b>	Display the high queue counter of the packet received.
<b>Rx Drops</b>	Display the number of frames dropped due to the lack of receiving buffer.
<b>Rx CRC/Alignment</b>	Display the number of Alignment errors packets received.
<b>Rx Undersize</b>	Display the number of short frames (<64 Bytes) with valid CRC.
<b>Rx Oversize</b>	Display the number of long frames (according to max_length register) with valid CRC.
<b>Rx Fragments</b>	Display the number of short frames (< 64 bytes) with invalid CRC.
<b>Rx Jabber</b>	Display the number of long frames (according to max_length register) with invalid CRC.
<b>Rx Filtered</b>	Display the filtered number of the packet received.
<b>Tx Packets</b>	Display the counting number of the packet transmitted.
<b>Tx Octets</b>	Display the total transmitted bytes.
<b>Tx Unicast</b>	Display the show the counting number of the transmitted unicast packet.
<b>Tx Multicast</b>	Display the show the counting number of the transmitted multicast packet.
<b>Tx Broadcast</b>	Display the counting number of the transmitted broadcast packet.
<b>Tx Pause</b>	Show the counting number of the transmitted pause packet.
<b>Tx 64 Bytes</b>	Display the number of 64-byte frames in good and bad packets transmitted.
<b>Tx 65-127 Bytes</b>	Display the number of 65 ~ 127-byte frames in good and bad packets transmitted.
<b>Tx 128-255 Bytes</b>	Display the number of 128 ~ 255-byte frames in good and bad packets transmitted.
<b>Tx 256-511 Bytes</b>	Display the number of 256 ~ 511-byte frames in good and bad packets transmitted.
<b>Tx 512-1023 Bytes</b>	Display the number of 512 ~ 1023-byte frames in good and bad packets transmitted.
<b>Tx 1024- 1526 Bytes</b>	Display the number of 1024 ~ 1522-byt frames in good and bad packets transmitted.
<b>Tx 1527 Bytes:</b>	Display the number of 1527-byte frames in good and bad packets transmitted.
<b>Tx Low</b>	Display the low queue counter of the packet transmitted.
<b>Tx Normal</b>	Display the normal queue counter of the packet transmitted.
<b>Tx Medium</b>	Display the medium queue counter of the packet received.



<b>Tx High</b>	Display the high queue counter of the packet received.
<b>Tx Drops</b>	Display the number of frames dropped due to excessive collision, late collision, or frame aging.
<b>Tx lat/Exc.Coll.</b>	Display the number of Frames late collision or excessive collision Error, which switch transmitted

## 3.5 Applications

Below shows the menu items for Applications.



### 3.5.1 Dynamic DNS

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

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

[Applications >> Dynamic DNS](#)

#### Dynamic DNS Configuration

Enable Dynamic DNS	<input type="checkbox"/>
DynDNS Service	dyndns.org
Hostname	mypersonaldomain.dyndn:
Username	myusername
Password	mypassword
Check IP change every	10 minutes
Force IP update every	72 hours

<b>Enable Dynamic DNS</b>	Check this box to enable the current account.
<b>DynDNS Service</b>	Select the service provider for the DDNS account.
<b>Hostname</b>	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
<b>Username</b>	Type in the login name that you set for applying domain.

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

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

### 3.5.2 Schedule

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

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

#### Applications >> Schedule

Schedule Configuration		
Index	Setting	Status
<input type="button" value="Add"/>		

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

#### Applications >> Schedule

**Add Schedule**

Enable

Start Date:  -  -  ( Year - Month - Date )

Start Time:  :  ( Hour : Minute )

Action:  ▾

Acts:  ▾

Weekday:  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

<b>Enable</b>	Check to enable the schedule.
<b>Start Date</b>	Specify the starting date of the schedule.
<b>Start Time</b>	Specify the starting time of the schedule.
<b>Action</b>	Specify which action Call Schedule should apply during the period of the schedule. <b>Force On</b> -Force the connection to be always on. <b>Force Down</b> -Force the connection to be always down. <b>Enable Dial-On-Demand</b> -Specify the connection to be dial-on-demand and the value of idle timeout should be

specified in **Idle Timeout** field.

**Disable Dial-On-Demand** -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

**Acts**

Specify how often the schedule will be applied

**Once** -The schedule will be applied just once

**Routine** or **Weekdays** -Specify which days in one week should perform the schedule.

### 3.5.3 IGMP Snooping

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

#### Applications >> IGMP Snooping

##### IGMP Snooping Configuration

General Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input type="checkbox"/>

Port	Fast Leave
LAN1	<input type="checkbox"/>
LAN2	<input type="checkbox"/>
LAN3	<input type="checkbox"/>
LAN4	<input type="checkbox"/>

**Snooping Enabled**

Check the box to enable this function.

**Unregistered IPMC...**

Check the box to enable unregistered IPMC traffic flooding

**Fast Leave**

Check the box to Fast Leave on the LAN port.

### 3.5.4 IGMP Status

This page display current IGMP snooping status.

[Applications >> IGMP Status](#)

#### IGMP Snooping Status

Auto-refresh

#### Statistics

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

#### IGMP Groups

Groups	Port Members
No IGMP groups	2 3 4

- V1~3 Reports Receive**      Display the number of Received V1 – V3 Reports.
- V2 Leave Receive**      Display the number of Received V2 Leave.
- Groups**      Display current IGMP groups. Maximum number of group for each VLAN can be set is 128.
- Port Members**      Display the LAN ports in this group.
- Refresh**      Click this button to refresh the page immediately.
- Clear**      Click this button to clear the settings on this page.

### 3.5.5 UPnP Configuration

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

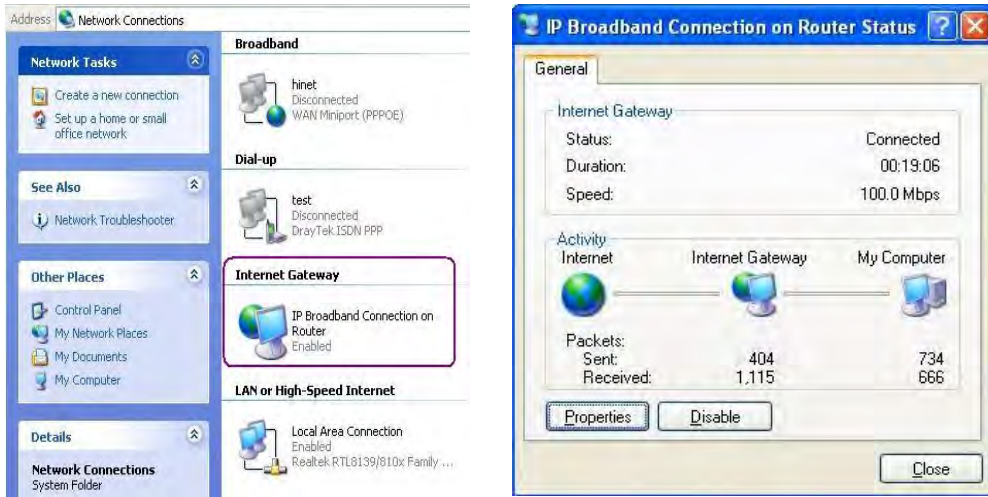
[Applications >> UPnP Configuration](#)

#### UPnP Configuration

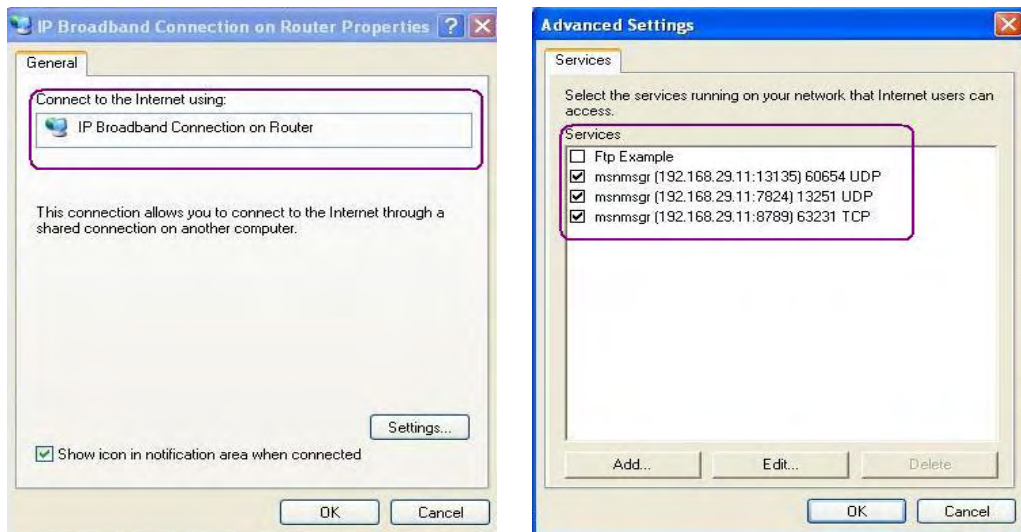
Enable UPnP	<input checked="" type="checkbox"/>
Download Speed	<input type="text" value="1024"/> kbps
Upload Speed	<input type="text" value="512"/> kbps

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

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



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.



The reminder as regards concern about Firewall and UPnP

**Can't work with Firewall Software**  
 Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

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

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

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

## 3.6 Wireless LAN

This function is used for “n” models.

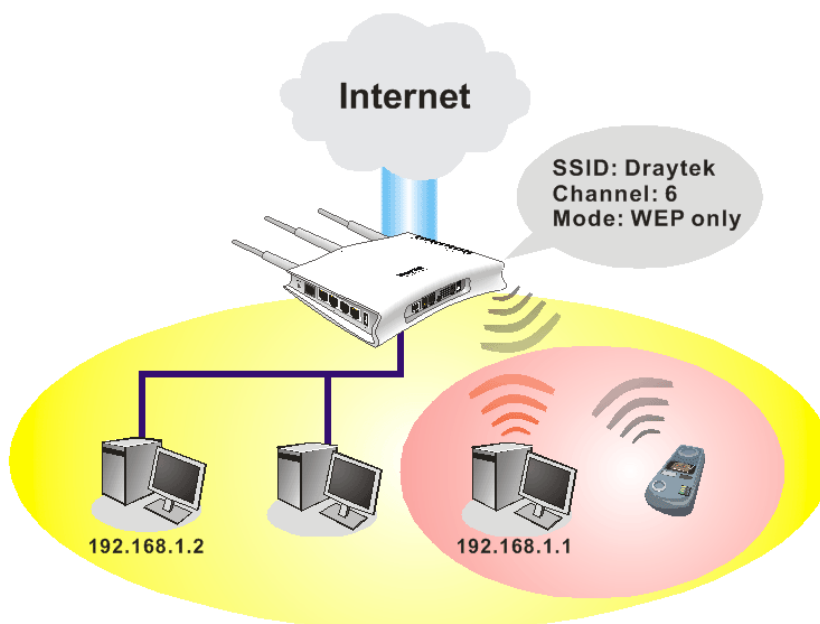
### 3.6.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor “n” model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a lot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.

**Note:** \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



## Security Overview

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

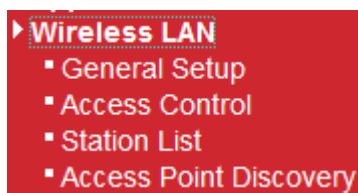
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Below shows the menu items for Wireless LAN.



### 3.6.2 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

Please refer to the following figure for more information.

#### Wireless LAN >> General Setup

##### General Setting

Enable Wireless LAN	<input checked="" type="checkbox"/>
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz

##### Wireless Security Configuration

Encryption	None
------------	------

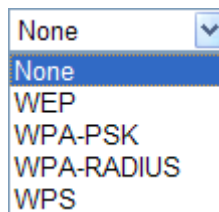
OK Cancel

#### Enable Wireless LAN

Check the box to enable the wireless function.



<b>SSID Broadcast</b>	Choose <b>Show</b> to make the SSID being seen by wireless clients. Choose <b>Hide</b> to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.
<b>SSID</b>	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.
<b>Wireless Mode</b>	Choose the wireless mode for this router. At present, only 802.11B/B/N mix is available.
<b>Country Region Code</b>	It represents different country region code. Use the drop down list to choose the one that fit the usage of regulations locally.
<b>Channel</b>	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 <b>Auto</b> to let system determine for you.
<b>Encryption</b>	Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.



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

## Wireless Security Configuration

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

- **None**  
The encryption mechanism is turned off.
- **WEP**  
Accepts only WEP clients and the encryption key should be entered in WEP Key.



### Wireless Security Configuration

Encryption	WEP
------------	-----

### WEP Configuration

Default Key	Key1
Key1	
Key2	
Key3	
Key4	
Authentication Mode	OPEN

OK Cancel

### 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	

OK Cancel

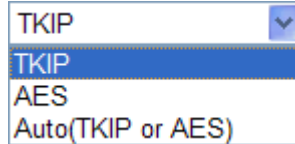
### WPA Mode

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.



**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 ▼

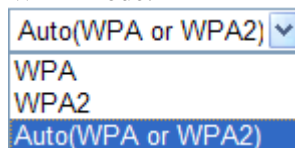
**WPA-RADIUS Configuration**

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

OK      Cancel

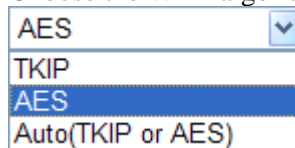
**Type**

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 <input type="button" value="v"/>
------------	--------------------------------------

### WPS Configuration

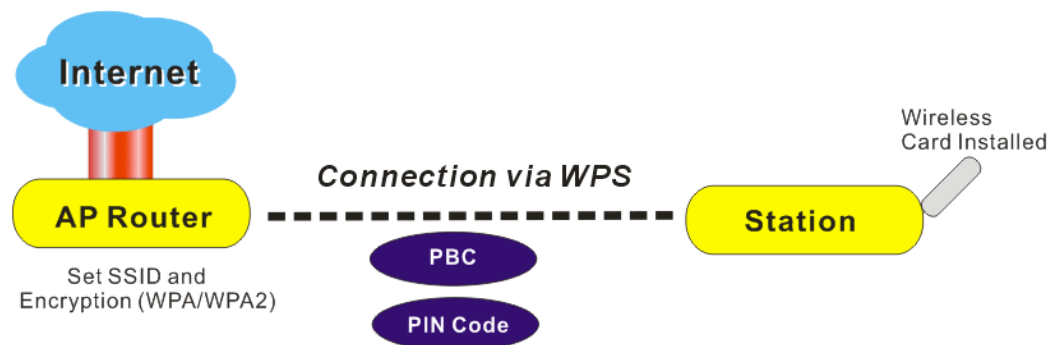
Configure via Push Button	<input type="button" value="Start PBC"/>	
Configure via Client PinCode	<input type="text"/>	<input type="button" value="Start PIN"/>

<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
-----------------------------------	---------------------------------------

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

**Configure via Client PinCode** Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

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

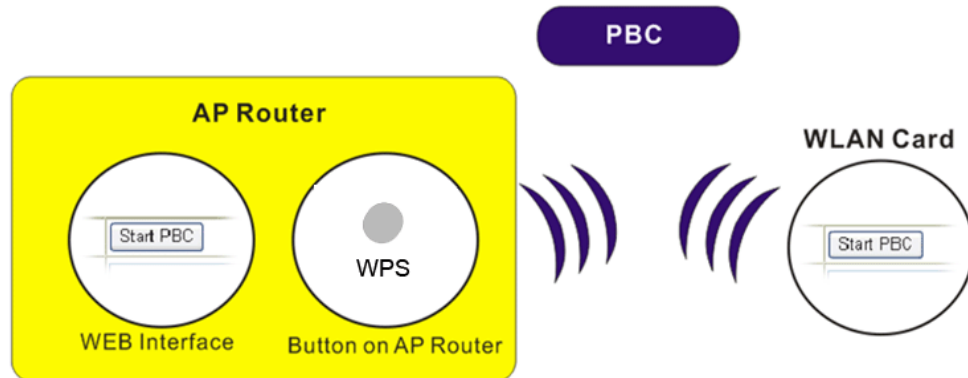


**Note:** Such function is available for the wireless station with WPS supported.

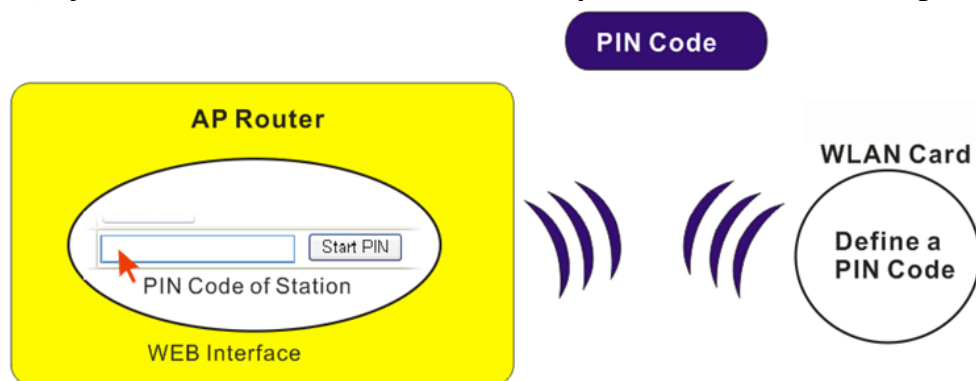
There are two methods to do network connection through WPS between AP and Stations: pressing the **Start PBC** button or using **PIN Code**.

On the side of Vigor 2130 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side

of a station with network card installed, press **Start PBC** button of network card.



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



### 3.6.3 Access Control

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

**Wireless LAN >> Access Control**

**Wireless MAC Address Filter Configuration**

Filter Type	Deny List
<b>Delete</b>	<b>MAC Address</b>
Add a New Entry	
OK	Cancel

#### Filter Type

Choose the rule for the MAC addresses displayed in this page.

**Allow List** – all the MAC address of wireless clients listed here are allowed to do wireless connection.

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

**Add a New Entry**

Add a new MAC address into the list.

**Delete**

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

Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type Deny List

Delete Delete MAC Address 00:20:00:05:30:12  
Add a New Entry

OK Cancel

**Cancel**

Give up the configuration.

**OK**

Click it to save the configuration.

### 3.6.4 Station List

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

Wireless LAN >> Station List

Station List

Auto-refresh  Refresh

Index	IP Address	MAC Address	Connected Time
No Station			

**Index**

Display the number of the connecting client.

**IP Address**

Display the WAN IP address for the connecting client.

**MAC Address**

Display the MAC Address for the connecting client.

**Connected Time**

Display the connection time for the connecting client.

**Auto-refresh**

Check this box to force the system refreshing the table automatically.

**Refresh**

Click this button to refresh current page.

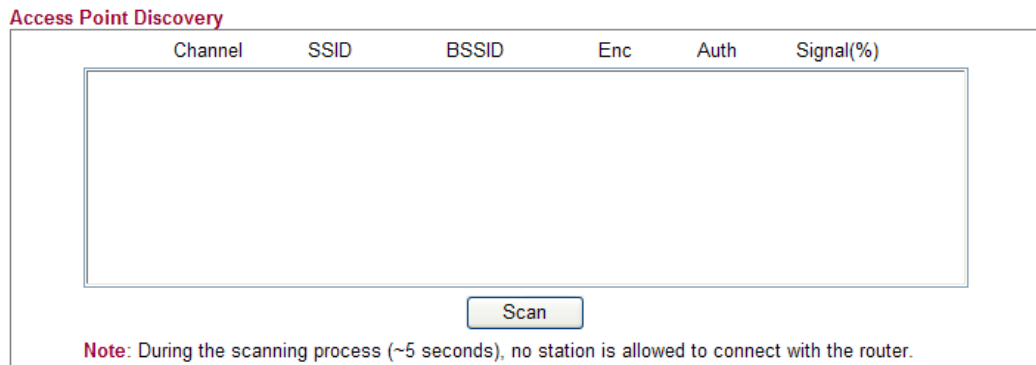
### 3.6.5 Access Point Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage.

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

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

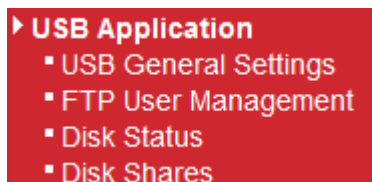
#### Wireless LAN >> Access Point Discovery



<b>Channel</b>	Display the channel for the scanned AP.
<b>SSID</b>	Display the SSID of the scanned AP.
<b>BSSID</b>	Display the MAC address of the scanned AP.
<b>Enc</b>	Display the encryption type of the scanned AP.
<b>Auth</b>	Display the authentication method of the scanned AP.
<b>Signal</b>	Display the strength (in percentage) of the signal of the scanned AP.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button.

## 3.7 USB Application

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



### 3.7.1 USB General Settings

At present, the Vigor router can support USB diskette with versions of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure

the memory format for the USB diskette is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

**USB Application >> USB General Settings**

**USB General Settings**

Enable FTP	<input type="checkbox"/>
Enable Disk Sharing	<input type="checkbox"/>
Workgroup Name	<input type="text" value="WORKGROUP"/>

- Enable FTP**                      Check this box to enable FTP connection.
- Enable Disk Sharing**        Check this box to enable Samba file sharing.
- Workgroup Name**              Type the name for FTP users for accessing into FTP server (USB diskette). Be aware that users cannot access into USB diskette in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage diskette.

### 3.7.2 FTP User Management

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

**USB Application >> FTP User Management**

**FTP User Management**

User Name	Volume	Path	Access Rights
<a href="#">carrie</a>	--	--	Read-only

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

**USB Application >> FTP User Setting**

**FTP User Configuration**

User Name	<input type="text" value="carrie"/>
Volume	<input type="text" value="USB2.0 - Mobile Disk (1) - 1967M - PORT 1"/>
Home Folder	<input type="text" value="/"/>
Access Rule	<input type="text" value="Read-only"/>

- User Name**                      It displays the username that user uses to login to the FTP server.
- Volume**                          Select the proper volume for the connected USB diskette.
- Home Folder**                  It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB diskette. In addition, if the user types “/”

here, he/she can access into all of the disk folders and files in USB diskette.

**Note:** When write protect status for the USB diskette is **ON**, you cannot type any new folder name in this field. Only “/” can be used in such case.

**Access Rule**

Select the access right for the USB diskette.

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

### 3.7.3 Disk Status

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

**USB Application >> Disk Status**

**Disk Status**

Safely Remove Disk	Manufacturer	Model	Size	Status
<input type="checkbox"/>	USB2.0	Mobile Disk	1968M	In use

**Safely Remove Disk**

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

**Manufacturer**

Display the manufacturer of the disk.

**Model**

Display the model of the disk.

**Size**

Display the storage space of the diskette(s).

**Status**

Display current usage status of the diskette(s)

**Update**

Click this button to refresh the disk status.

### 3.7.4 Disk Shares

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

**USB Application >> Disk Shares**

**Disk Shares**

Share Name	Comment	Path	Visible
No Shares			

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



## USB Application >> Disk Share

### Add Disk Share

#### Identification

Share Name	<input type="text"/>
Comment	<input type="text"/>

#### Settings

Volume	USB2.0 - Mobile Disk (1) - 1967M - PORT 1 ▾
Path	<input type="text" value="/"/>
Visible	<input type="checkbox"/>

#### Access Rights

Access	All Users Read-only ▾
--------	-----------------------

- Share Name** Type a name to be used as shared folder name in Samba service. The name must not contain spaces or special characters.
- Comment** Type the brief description for the disk sharing. The words here will be seen in Network Neighborhood on Windows client computers
- Volume** Select the proper volume for the connected USB diskette.
- Path** It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB diskette. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB diskette.  
**Note:** When write protect status for the USB diskette is **ON**, you cannot type any new folder name in this field. Only “/” can be used in such case.
- Visible** Check this box to make the shared folder to be seen in Network Neighborhood on Windows of clients in local network.
- Access Rights** Specify the access right and apply to all the wireless clients that want to connect to the attached USB diskette.

All Users Read-only ▾
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.

## 3.8 User

### 3.8.1 User Configuration

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

#### Users

##### Users

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

Add a New User

### Adding a New User

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

#### User Configuration

##### Add User

User Settings	
Username	<input type="text" value="carrie"/>
Full Name	<input type="text" value="carrie ni"/>
Password	<input type="password" value="••••••••"/>
Confirm Password	<input type="password" value="••••••••"/>
Allow Disk Sharing	<input checked="" type="checkbox"/>
Allow IPSEC/L2TP	<input checked="" type="checkbox"/>
Allow PPTP	<input checked="" type="checkbox"/>
Allow FTP	<input checked="" type="checkbox"/>

OK

Cancel

<b>Username</b>	Type a name for this user.
<b>Full Name</b>	Type full name for this user.
<b>Password</b>	Type the password for this user.
<b>Password (again)</b>	Type the password again for confirmation.
<b>Allow Disk Sharing</b>	Check this box to enable Samba file sharing.
<b>Allow IPSEC/L2TP</b>	Check this box to let the user connect via IPSEC/L2TP.
<b>Allow PPTP</b>	Check this box to let the user connect via PPTP.
<b>Allow FTP</b>	Check this box to let the user connect to FTP server.

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

## Users

### Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
<a href="#">carrie</a>	carrie ni	✓	✓	✓	✓

Add a New User

## Editing/Deleting User Settings

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

### User Configuration

#### Edit User

User Settings	
Username	<input type="text" value="carrie"/>
Full Name	<input type="text" value="carrie ni"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="••••"/>
Allow Disk Sharing	<input type="checkbox"/>
Allow IPSEC/L2TP	<input type="checkbox"/>
Allow PPTP	<input type="checkbox"/>
Allow FTP	<input type="checkbox"/>

OK

Cancel

Delete User

## 3.9 System Maintenance

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

Below shows the menu items for System Maintenance.

- ▶ **System Maintenance**
  - System Status
  - User Password
  - Configuration Backup
  - Syslog / Mail Alert
  - Time and Date
  - Management
  - Reboot System
  - Firmware Upgrade

### 3.9.1 System Status

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

## System Status

Auto-refresh  Refresh

Model : Vigor2130  
Platform : VSC7501  
Bootloader Version : Dray-Boot 1.0.0E  
Firmware Version : v1.1.0\_RC2  
Build Date/Time : r527 Mon Jun 8 19:31:53 CST 2009  
Hardware NAT Version : 1.0.0.13  
System Date : Tue Jun 16 17:06:18 2009  
System Uptime : 0d 07:20:28

LAN	
MAC Address	: 00:50:7F:C7:7B:30
IP Address	: 192.168.1.1
IP Mask	: 255.255.255.0

WAN	
MAC Address	: 00:50:7F:C7:7B:31
IP Address	: 192.168.5.30
IP Mask	: 255.255.255.0
Default Gateway	: 192.168.5.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

Wireless	
MAC Address	: 00:21:85:F7:44:D1
Device Type	: rt2880
SSID	: DrayTek
Channel	: 11

USB1	
Manufacturer	: USB2.0
Model	: Mobile Disk
Size	: 1968M
Status	: In use

<b>Model Name</b>	Display the model name of the router.
<b>Platform</b>	Display the hardware type that this device is built upon.
<b>Bootloader Version</b>	Display the bootloader version of the router.
<b>Firmware Version</b>	Display the firmware version of the router.
<b>Build Date/Time</b>	Display the date and time of the current firmware build.
<b>Hardware NAT Version</b>	Display the hardware acceleration NAT version.
<b>System Date</b>	Display current time and date for the system server.
<b>System Uptime</b>	Display the connection time for the system server.
<b>LAN-----</b>	
<b>MAC Address</b>	Display the MAC address of the LAN Interface.
<b>IP Address</b>	Display the IP address of the LAN interface.
<b>IP Mask</b>	Display the subnet mask address of the LAN interface.
<b>WAN-----</b>	
<b>MAC Address</b>	Display the MAC address of the WAN Interface.
<b>IP Address</b>	Display the IP address of the WAN interface.
<b>IP Mask</b>	Display the subnet mask address of the WAN interface.
<b>Default Gateway</b>	Display the gateway address of the WAN interface.
<b>Primary DNS</b>	Display the specified primary DNS setting.
<b>Secondary DNS</b>	Display the specified secondary DNS setting.
<b>Wireless LAN-----</b>	

<b>MAC Address</b>	Display the MAC address of the wireless LAN.
<b>Device Type</b>	Display the device type used for wireless LAN.
<b>SSID</b>	Display the SSID of the router.
<b>Channel</b>	Display the channel that wireless LAN used.
<b>Manufacturer</b>	Display the manufacturer of the disk.
<b>Model</b>	Display the model of the disk.
<b>Size</b>	Display the storage size of the USB diskette.
<b>Status</b>	Display current status of the USB diskette.

### 3.9.2 User Password

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

#### System Maintenance >> User Password

##### User Password

New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

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

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

### 3.9.3 Configuration Backup

#### Backup the Configuration

Follow the steps below to backup your configuration.

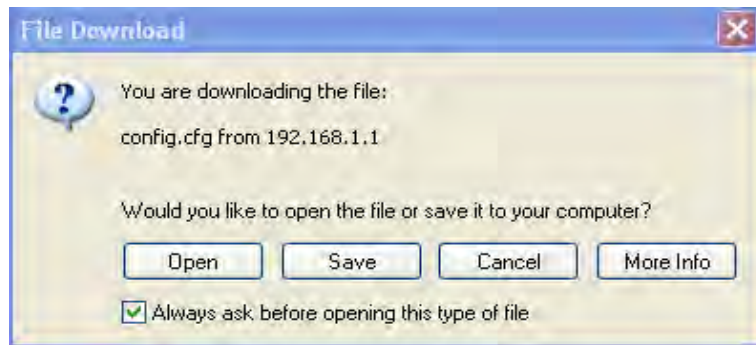
1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

#### System Maintenance >> Configuration Backup

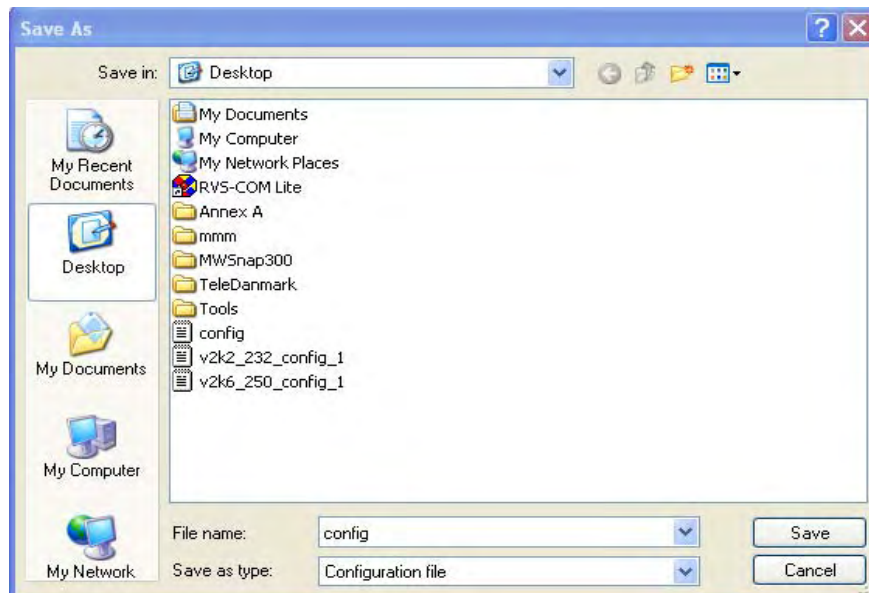
##### Configuration Backup / Restoration

<b>Backup</b>	
Click Backup to download current running configurations as a file.	
<input type="button" value="Backup"/>	
<b>Restoration</b>	
Select a configuration file.	
<input type="text"/>	<input type="button" value="Browse.."/>
Click Restore to upload the file.	
<input type="button" value="Restore"/>	

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



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

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

**Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

## Restore Configuration

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

## System Maintenance >> Configuration Backup

### Configuration Backup / Restoration

#### Backup

Click Backup to download current running configurations as a file.

Backup

#### Restoration

Select a configuration file.

Browse..

Click Restore to upload the file.

Restore

2. Click **Browse** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

## 3.9.4 Syslog / Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

### System Maintenance >> Syslog / Mail Alert Setup

#### Syslog Access Setup

Enable	<input type="checkbox"/>
Router Name	<input type="text" value="Vigor2130"/>
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="514"/>
Log Level	All <input type="button" value="v"/>

#### Mail Alert Setup

Enable	<input type="checkbox"/>
SMTP Server	<input type="text"/>
Mail To	<input type="text"/>
Mail From	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Enable E-Mail Alert:	
<input checked="" type="checkbox"/> User Login	

OK

Cancel

**Enable (Syslog Access...)**

Check the box to activate function of syslog.

**Router Name**

Type a name of this device.

**Server IP Address**

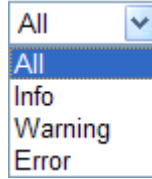
The IP address of the Syslog server.

**Destination Port**

Type a port for the Syslog protocol.

**Log Level**

Choose the severity level for the system log entry.



**Enable (Mail Alert...)**

Check the box to activate function of mail alert.

**Send a test e-mail**

Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.

**SMTP Server**

The IP address of the SMTP server.

**Mail To**

Assign a mail address for sending mails out.

**Mail From**

Assign a path for receiving the mail from outside.

**User Name**

Type the user name for authentication.

**Password**

Type the password for authentication.

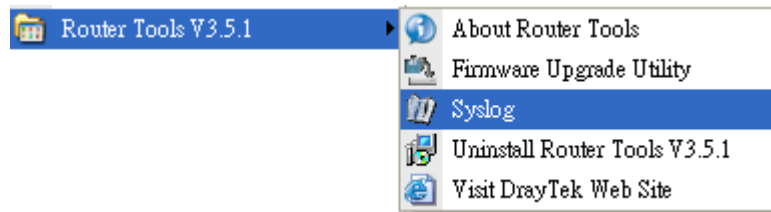
**Enable E-mail Alert**

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

Click **OK** to save these settings.

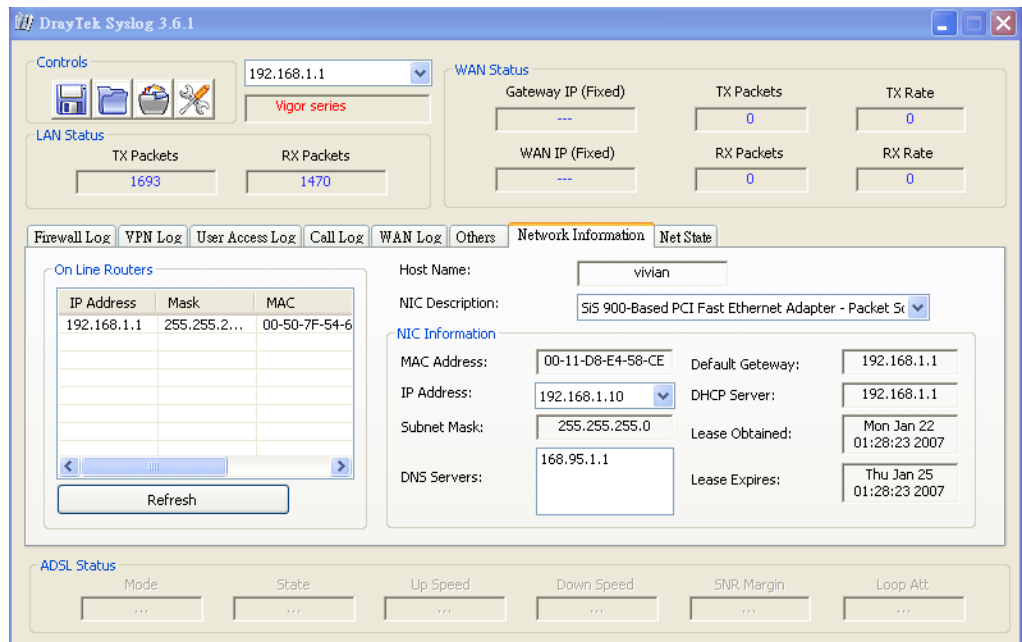
For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.





### 3.9.5 Time and Date

It allows you to specify where the time of the router should be inquired from.

**System Maintenance >> Time and Date**

#### Time Configuration

**Time Zone**

Unknown ▼

---

**NTP Servers**

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

Add NTP server

#### Time Zone

Select the time zone where the router is located.

#### Add NTP server

Click the button to add a new NTP server.

#### Delete

Click this button to remove an NTP server.

Click **OK** to save these settings.

### 3.9.6 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

**System Maintenance >> Remote Management**

#### Management Access Control

Enable HTTP	<input type="checkbox"/>	80	<b>SNMP Setup</b>	Enable SNMP	<input type="checkbox"/>	161
Enable HTTPS	<input type="checkbox"/>	443	Manager Host IP	<input type="text"/>		
Enable SSH	<input type="checkbox"/>	22				
Enable ICMP Ping	<input type="checkbox"/>					
Enable FTP	<input type="checkbox"/>					

Access List	IP	Subnet Mask
List		
1	<input type="text"/>	255.255.255.255 / 32
2	<input type="text"/>	255.255.255.255 / 32
3	<input type="text"/>	255.255.255.255 / 32

**Enable HTTP/HTTPS/SSH/ICMP Ping/FTP/SNMP** Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.

**Manager Host IP** – Type the IP address for the host to perform the remote management.

#### Access List

You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.

**List IP** - Indicate an IP address allowed to login to the router.

**Subnet Mask** - Represent a subnet mask allowed to login to the router.

### 3.9.7 Reboot System

The Web Configurator may be used to restart your router for using current configuration. Click **Reboot System** from **System Maintenance** to open the following page.

## System Maintenance >> Reboot System

---

### Reboot System

**Do You want to reboot your router ?**

Using current configuration  
 Using factory default configuration

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

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

### 3.9.8 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is [www.draytek.com](http://www.draytek.com) (or local DrayTek's web site) and FTP site is [ftp.draytek.com](http://ftp.draytek.com).

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

#### System Maintenance >> Firmware Upgrade

---

#### Firmware Update

Current Firmware Version: v1.1.0\_RC2

Select a firmware file.

Click Upgrade to upload the file.

For the detailed information about firmware update, please go to Chapter 5.



# 4

## Admin Mode Operation

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

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

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

The screenshot displays the 'System Status' page of a DrayTek Vigor2130 Series High Speed Gigabit Router. The page is divided into several sections:

- System Status:** Lists key system information:
  - Model : Vigor2130
  - Platform : VSC7501
  - Bootloader Version : Dray-Boot 1.0.0E
  - Firmware Version : v1.1.0\_RC6
  - Build Date/Time : r753 Tue Aug 25 16:11:42 CST 2009
  - Hardware NAT Version : 1.0.0.13
  - System Date : Mon Aug 31 03:02:52 2009
  - System Uptime : 3d 10:39:36
- LAN Network Settings:**

LAN	
MAC Address	: 00:50:7F:C7:7B:30
IP Address	: 192.168.1.1
IP Mask	: 255.255.255.0
- WAN Network Settings:**

WAN	
MAC Address	: 00:50:7F:C7:7B:31
IP Address	: 192.168.5.21
IP Mask	: 255.255.255.0
Default Gateway	: 192.168.5.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

The interface also features a navigation menu on the left with options like 'Quick Start Wizard', 'Online Status', 'WAN', 'LAN', 'NAT', 'Firewall', 'Bandwidth Management', 'Applications', 'VPN and Remote Access', 'Wireless LAN', 'USB Application', 'User', 'System Maintenance', and 'Diagnostics'. A 'Logout' button is located at the bottom left, and the text 'Admin mode' is displayed in a green box at the bottom center.

### 4.1 WAN

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

#### Basics of Internet Protocol (IP) Network

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

**From 10.0.0.0 to 10.255.255.255**

**From 172.16.0.0 to 172.31.255.255**

**From 192.168.0.0 to 192.168.255.255**

## What are Public IP Address and Private IP Address

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

## Get Your Public IP Address from ISP

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

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

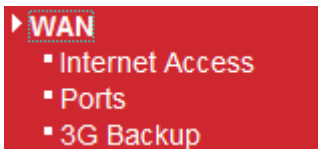
## Network Connection by 3G USB Modem

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



After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem also can be used as backup device. Therefore, when WAN is not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit [www.draytek.com](http://www.draytek.com) for more detailed information.

Below shows the menu items for WAN.



### 4.1.1 Internet Access

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

**WAN >> Internet Access**

---

**WAN IP Configuration**

Connection Type: DHCP

**DHCP Settings**

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

**Clone MAC Address**

Enable:

OK Cancel

### Static

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

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

**WAN >> Internet Access**

---

**WAN IP Configuration**

Connection Type: Static IP

**Static IP Settings**

IP Address: 172.16.3.229

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.3.4

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

**Clone MAC Address**

Enable:

OK Cancel

**IP Address** Type the IP address.

**Subnet Mask** Type the subnet mask.

- Gateway IP Address**            Type the gateway IP address.
- Primary DNS Server**            Type in the primary IP address for the router if you want to use **Static IP** mode.
- Secondary DNS Server**        Type in secondary IP address for using in the future if necessary.
- Clone MAC Address**            It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

## DHCP

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

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	DHCP <span style="font-size: small;">▼</span>
-----------------	---

#### DHCP Settings

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

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK	Cancel
----	--------

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

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

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

## PPPoE

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



## WAN >> Internet Access

### WAN IP Configuration

Connection Type	PPPoE
-----------------	-------

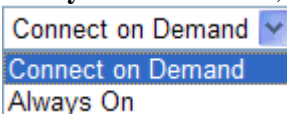
### PPPoE Settings

Username	<input type="text"/>
Password	<input type="text"/>
Redial Policy	Connect on Demand
Idle Time out	<input type="text"/>
MTU Size	<input type="text"/>

### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK Cancel

- Username** Type in the username provided by ISP in this field.
- Password** Type in the password provided by ISP in this field.
- Redial Policy** If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.
- 
- Idle Time Out** Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand**, you have to type value here.
- MTU Size** It means Max Transmit Unit for packet. The default setting is 1442.
- Enable/Disable** Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
- Clone MAC Address** It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

## PPTP/L2TP

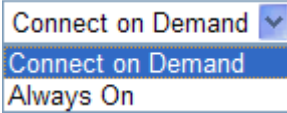
To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Connection Type** drop down menu. The following web page will be shown.

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	PPTP
<b>PPTP Settings</b>	
Username	<input type="text"/>
Password	<input type="password"/>
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Redial Policy	Connect on Demand
Idle Time out	<input type="text"/>
MTU Size	<input type="text"/>
<b>Clone MAC Address</b>	
Enable	<input type="checkbox"/>

OK Cancel

<b>Username</b>	Type in the username provided by ISP in this field.
<b>Password</b>	Type in the password provided by ISP in this field.
<b>Server Address</b>	Type in the IP address for PPTP /L2TP server.
<b>WAN IP Network Settings</b>	You can choose Static IP or DHCP as WAN IP network setting.
<b>IP Address</b>	Type the IP address if you choose Static IP as the WAN IP network setting.
<b>Subnet Mask</b>	Type the subnet mask if you chose Static IP as the WAN IP.
<b>Redial Policy</b>	If you want to connect to Internet all the time, you can choose <b>Always On</b> . Otherwise, choose <b>Connect on Demand</b> and 
<b>Idle Time Out</b>	Set the timeout for breaking down the Internet after passing through the time without any action. When you choose <b>Connect on Demand</b> , you have to type value here.
<b>MTU Size</b>	It means Max Transmit Unit for packet. The default setting is 1442.
<b>Clone MAC Address</b>	It is available when the box of Enable is checked. Click <b>Clone MAC Address</b> . The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

### 3G USB Modem

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

#### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	3G USB Modem
-----------------	--------------

#### 3G USB Modem Settings

SIM PIN code	<input type="text"/>	
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	<input type="text"/>	
PPP Password	<input type="text"/>	

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK	Cancel
----	--------

- SIM PIN code** Type PIN code of the SIM card that will be used to access Internet.
- Modem Initial String1/2** Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
- APN Name** APN means Access Point Name which is provided and required by some ISPs.
- Modem Dial String** Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
- PPP Username** Type the PPP username (optional).
- PPP Password** Type the PPP password (optional).
- Clone MAC Address** It is available when the box of Enable is checked. Click **Clone MAC Address**. The result will be displayed in the field of MAC Address.

Enable	<input checked="" type="checkbox"/>	Clone MAC Address
MAC Address		00-0E-A6-2A-D5-A1

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

## 4.1.2 Ports

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

WAN >> Ports

Port Configuration

Port	Link	Current	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
			Configured	Current Rx	Current Tx	Configured				
WAN	●	100fdx	Auto	✓	✓	<input checked="" type="checkbox"/>	1518	Discard	Disabled	

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

### Port

It displays current network interface.

### Link

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

### Current

It displays current speed that the router uses.

### Speed Configured

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

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

### Flow Control

If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.

Current Rx: indicates whether pause frames on the port are obeyed.

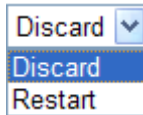
Current Tx: indicates whether pause frames on the port are transmitted.

### Maximum Frame

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

### Excessive Collision Mode

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

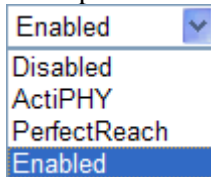


**Discard** - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

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

### Power Control

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



**Disabled:** All power savings mechanisms disabled.

**ActiPHY:** Link down power savings enabled.

**PerfectReach:** Link up power savings enabled.

**Enabled:** Both link up and link down power savings enabled.

### Refresh

Click this button to refresh the information for WAN port.

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

## 4.1.3 3G Backup

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

### WAN >> 3G backup

#### 3G Backup Configuration

<input type="checkbox"/> Enable 3G Backup		
SIM PIN code	<input type="text"/>	
Modem Initial String1	<input type="text" value="AT&amp;F"/>	(default:AT&F)
Modem Initial String2	<input type="text" value="ATE0V1X1&amp;D2&amp;C1S0=0"/>	(default:ATE0V1X1&D2&C1S0=0)
APN Name	<input type="text" value="internet"/>	(default:internet)
Modem Dial String	<input type="text" value="ATDT*99#"/>	(default:ATDT*99#)
PPP Username	<input type="text"/>	
PPP Password	<input type="text"/>	



### SIM PIN code

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

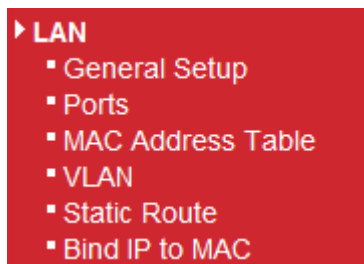
<b>Modem Initial String1/2</b>	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
<b>APN Name</b>	APN means Access Point Name which is provided and required by some ISPs.
<b>Modem Dial String</b>	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
<b>PPP Username</b>	Type the PPP username (optional).
<b>PPP Password</b>	Type the PPP password (optional).
<b>Clone MAC Address</b>	It is available when the box of Enable is checked. Click <b>Clone MAC Address</b> . The result will be displayed in the field of MAC Address.

Enable  Clone MAC Address

MAC Address

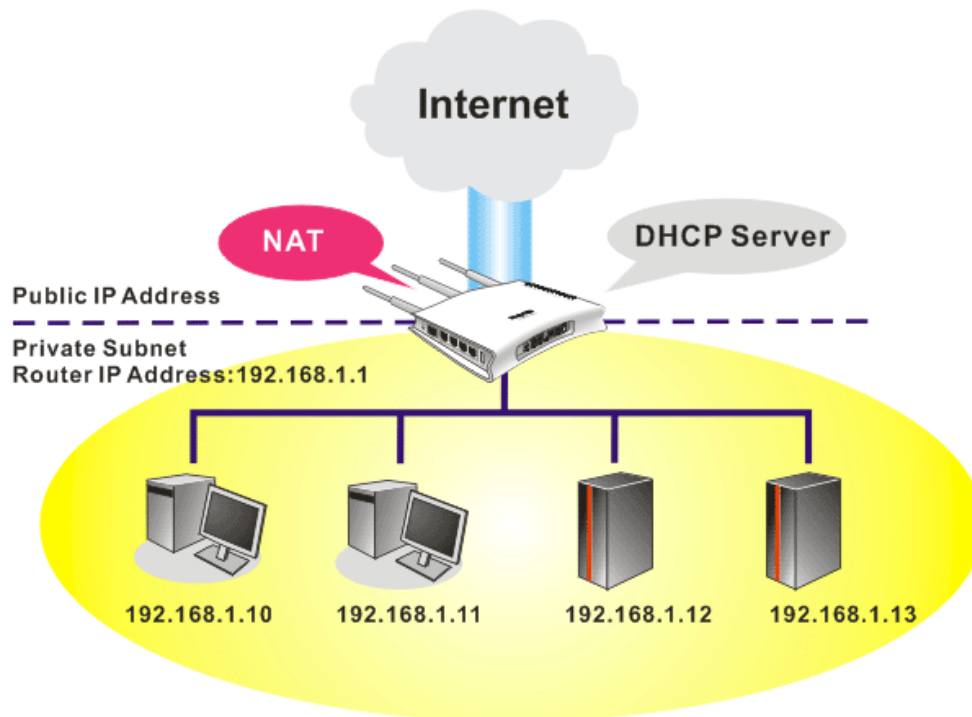
## 4.2 LAN

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

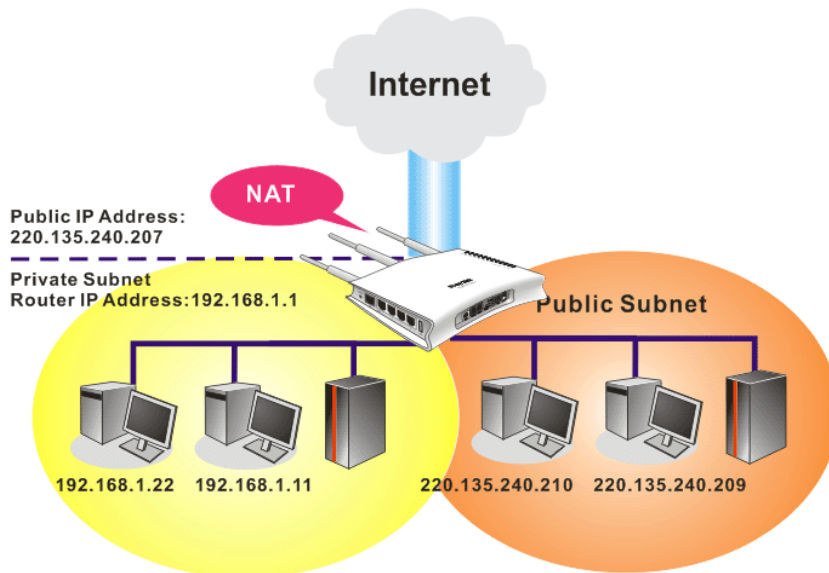


### Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



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



## What is Routing Information Protocol (RIP)

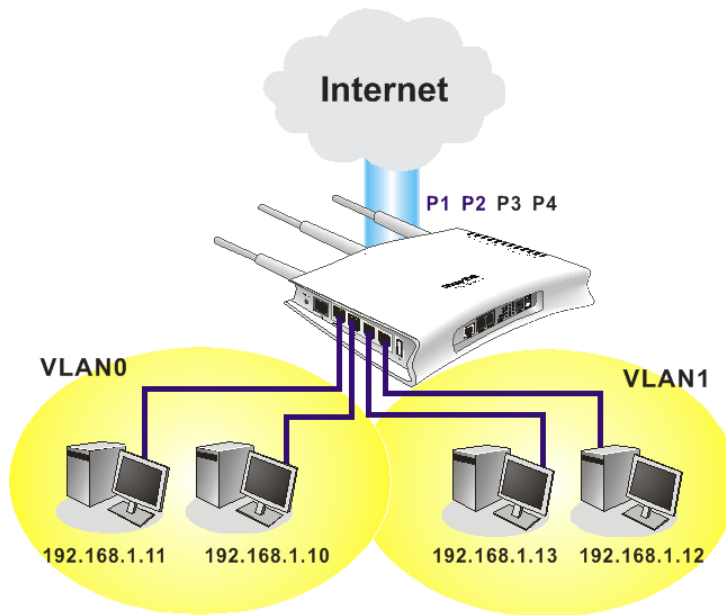
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

## What is Static Route

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

### What are Virtual LANs and Rate Control

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



### 4.2.1 General Setup

This page provides you the general settings for LAN.

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

**LAN >> General Setup**

#### LAN IP Network Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

#### DHCP Server Configuration

Enable DHCP	<input checked="" type="checkbox"/>
Start IP Address	192.168.1.10
IP Pool Counts	50
Lease Time	720 minutes

OK Cancel

#### IP Address

Type in private IP address for connecting to a local private network (Default: 192.168.1.1).

#### Subnet Mask

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

#### Enable DHCP

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network



so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

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

**Start IP Address**

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

**IP Pool Counts**

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

**Lease Time**

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

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

### 4.2.2 Ports

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

LAN >> Ports

Port Configuration

Refresh

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

OK Cancel

**Port**

It displays current network interface.

**Link**

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

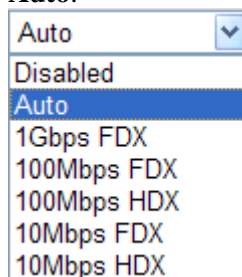
**Current**

It displays current speed that the router uses.

**Speed Configured**

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

**Auto.**



**Flow Control**

If flow control is enabled by checking **Configured** box, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. If not, there will be no flow control in the port. It drops the packet if too much to handle.

Current Rx: indicates whether pause frames on the port are obeyed.

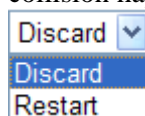
Current Tx: indicates whether pause frames on the port are transmitted.

**Maximum Frame**

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

**Excessive Collision Mode**

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

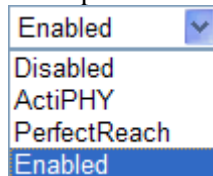


**Discard** - It determines whether the MAC drops frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

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

**Power Control**

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



**Disabled:** All power savings mechanisms disabled.

**ActiPHY:** Link down power savings enabled.

**PerfectReach:** Link up power savings enabled.

**Enabled:** Both link up and link down power savings enabled.

**Refresh**

Click this button to refresh the information for LAN ports.

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

### 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	<input type="checkbox"/>
Age Time	<input type="text" value="300"/> seconds

##### MAC Table Learning

	WAN	LAN1	Port Members LAN2	LAN3	LAN4
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

##### Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members WAN	LAN1	LAN2	LAN3	LAN4
<input type="button" value="Add New Static Entry"/>							

#### Disable Automatic Aging

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

#### Age Time

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

#### MAC Table Learning

List the port members which apply dynamic learning mechanism or not.

**Auto** - Enable this port MAC address dynamic learning mechanism.

**Disable** - Disable this port MAC address dynamic learning mechanism, only support static MAC address setting.

**Secure** - Disable this port MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU.

#### Static MAC Table Config..

Specify static MAC address with VLAN ID to apply aging configuration.

**Delete** - Click the button to remove the VLAN setting.

**VLAN ID** - Specify the interface for the port members.

**MAC Address** - It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 - 40 - C7 - D6 - 00 - 02.

**WAN/LAN1~4** - Check the port to apply this VLAN setting.

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

### Static MAC Table Configuration

Delete	VLAN ID	MAC Address	WAN	Port Members			
Delete	1(LAN)	00-00-00-00-00-00	<input type="checkbox"/>	LAN1	LAN2	LAN3	LAN4
<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add new static entry

OK Cancel

## 4.2.4 VLAN

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

LAN >> VLAN

### Private VLAN Membership Configuration

Delete	PVLAN ID	LAN1	Port Members			
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	LAN2	LAN3	LAN4	
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Add New Private VLAN

OK Cancel

#### Add New Private VLAN

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

LAN >> VLAN

### Private VLAN Membership Configuration

Delete	PVLAN ID	LAN1	Port Members			
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	LAN2	LAN3	LAN4	
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Add New Private VLAN

OK Cancel

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

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

## LAN >> VLAN

### Private VLAN Membership Configuration

Delete	PVLAN ID	LAN1	Port Members			LAN4
<input type="checkbox"/>			LAN2	LAN3		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="button" value="Delete"/>	<input type="text" value="2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="button" value="Delete"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="button" value="Delete"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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

## 4.2.5 Static Route

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

### LAN >> Static Route

#### Static Route Configuration

Index	Destination Address	Status
<input type="button" value="Add"/>		

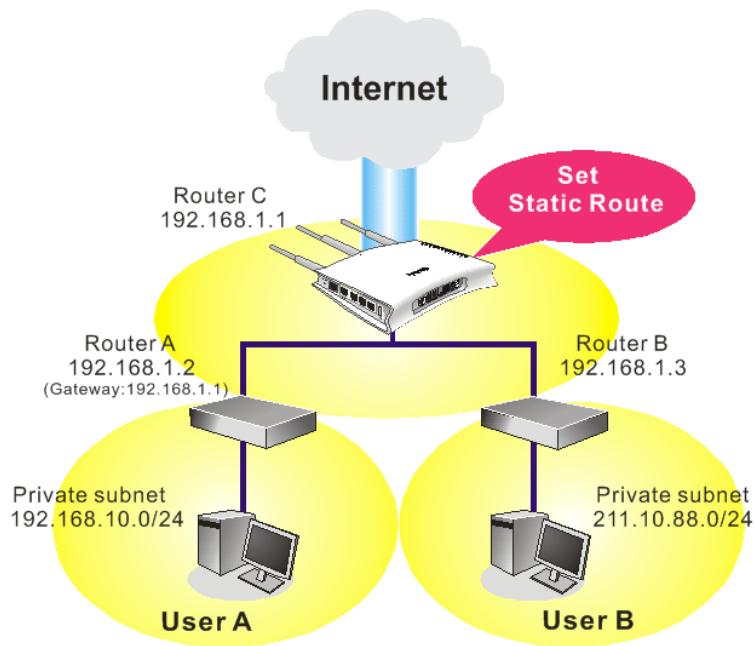
<b>Index</b>	The number (1 to 10) under Index displays current static router.
<b>Destination Address</b>	Display the destination address of the static route.
<b>Status</b>	Display the status of the static route.
<b>Add</b>	To add a new static route.

### 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**

<input checked="" type="checkbox"/> Enable	
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2

OK Cancel

- 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**

<input checked="" type="checkbox"/> Enable	
Destination IP Address	<input type="text" value="211.100.88.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway IP Address	<input type="text" value="192.168.1.3"/>

- 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	✓

## 4.2.6 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 Bind List** | [Select All](#) | [Sort](#)

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

Index	IP Address	Mac Address
-------	------------	-------------

**Add and Edit**

IP Address

Mac Address

<b>Enable</b>	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
<b>Disable</b>	Click this radio button to disable this function. All the settings on this page will be invalid.
<b>Strict Bind</b>	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
<b>ARP Table</b>	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 <b>Add</b> below.
<b>Add and Edit</b>	<b>IP Address</b> – Type the IP address that will be used for the specified MAC address. <b>Mac Address</b> – Type the MAC address that is used to bind with the assigned IP address.
<b>Refresh</b>	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.
<b>IP Bind List</b>	It displays a list for the IP bind to MAC information.
<b>Add</b>	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in <b>Add and Edit</b> to the table of <b>IP Bind List</b> .
<b>Edit</b>	It allows you to edit and modify the selected IP address and MAC address that you create before.
<b>Remove</b>	You can remove any item listed in <b>IP Bind List</b> . Simply click and select the one, and click <b>Remove</b> . The selected item will be removed from the <b>IP Bind List</b> .

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

## 4.3 NAT

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

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

The benefit of the NAT includes:

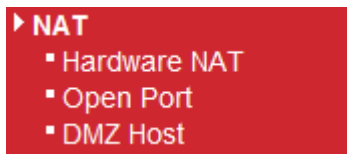
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.



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

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

Below shows the menu items for NAT.



### 4.3.1 Hardware NAT

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

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

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

#### NAT >> Hardware NAT

##### Hardware NAT Configuration

Hardware NAT Enabled ▾

### 4.3.2 Open Ports

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

#### NAT >> Open Port

##### Port Forwarding

Name	Protocol	Start Port	End Port	Local Host	Local Port
<i>No Port Forwarding</i>					

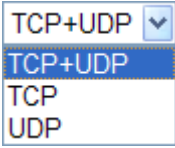
Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

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

## NAT >> Open Port

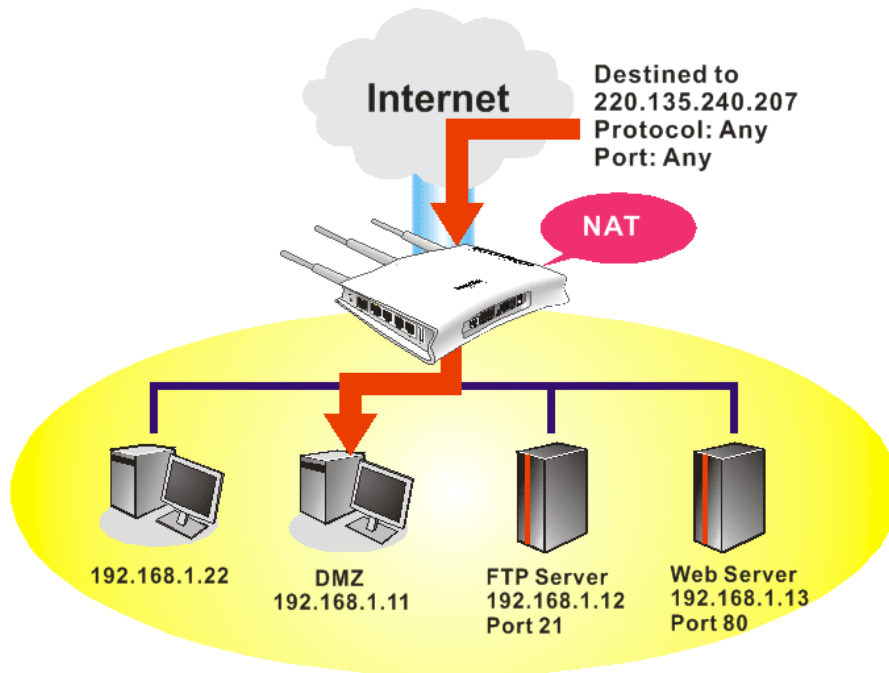
### Add Port Forwarding Entry

Name	<input type="text"/>
Protocol	TCP+UDP ▾
Start Port	<input type="text"/>
End Port (optional)	<input type="text"/>
Local Host	<input type="text"/>
Local Port (optional)	<input type="text"/>

- Name** Specify the name for the defined network service.
- Protocol** Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**.
- 
- Start Port** Specify the starting port number of the service offered by the local host.
- End Port (optional)** Specify the ending port number of the service offered by the local host.
- Local Host** Enter the private IP address of the local host.
- Local Port (optional)** If it is configured, the forwarded traffic is mapped to this port on the local host.

### 4.3.3 DMZ Host

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



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

Click **DMZ Host** to open the following page:

NAT >> DMZ Host

DMZ Host

Enable	DMZ IP
<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>

OK Cancel

**Enable**

Check to enable the DMZ Host function.

**DMZ IP**

Enter the private IP address of the DMZ host, or click Choose

## 4.4 Firewall

### Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

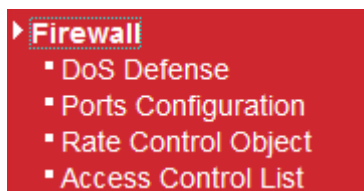
### Denial of Service (DoS) Defense

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

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

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

Below shows the menu items for Firewall.



#### 4.4.1 DoS Defense

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

Firewall >> DoS Defense

##### Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	<input checked="" type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

OK Cancel

##### Frame Type

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

##### Status

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

##### Rate

The unit is packet per second (pps). Use the drop down list to set the rate for data transmission. The rate is  $2^n$ , where n is

equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

## 4.4.2 Ports Configuration

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

Firewall >> Ports Configuration

ACL Ports Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Counter
WAN	1	Permit	Disabled	Disabled	70125
LAN1	1	Permit	Disabled	Disabled	0
LAN2	1	Permit	Disabled	Disabled	41520
LAN3	1	Permit	Disabled	Disabled	0
LAN4	1	Permit	Disabled	Disabled	0

OK Cancel

### Port

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

### Policy ID

Select a policy to apply to this port. The range for values is from 1 to 8. The default value is 1.

Policy ID

1

1

2

3

4

5

6

7

8

### Action

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

Action

Permit

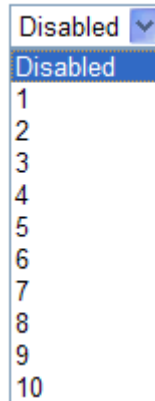
Deny

Permit

### Rate Limited 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

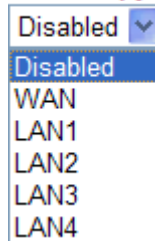


A dropdown menu with a blue border. The top bar is blue with the text "Disabled" and a downward arrow. The menu is open, showing a list of options: "Disabled" (highlighted in blue), "1", "2", "3", "4", "5", "6", "7", "8", "9", and "10".

### Port Copy

Select which port the frames are copied to for the purpose of monitoring. Available settings include **Disabled**, and 1 to 10. The default value is **Disabled**.

#### Port Copy



A dropdown menu with a blue border. The top bar is blue with the text "Disabled" and a downward arrow. The menu is open, showing a list of options: "Disabled" (highlighted in blue), "WAN", "LAN1", "LAN2", "LAN3", and "LAN4".

### 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.

### 4.4.3 Rate Control Object

Configure the rate limiter for the ACL (Access Control List) of the router.

**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

OK Cancel

#### Rate Limited 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

## 4.4.4 Access Control List

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

**Firewall >> Access Control List**

---


### Access Control List Configuration

Auto-refresh  Refresh Clear Remove All

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counter

+

### Adding a New Access Control Profile

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

**Firewall >> Access Control List**

---

### ACE Configuration

Ingress Port	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Copy	Disabled
Counter	0

### MAC Parameters

DMAC Filter	Any
-------------	-----

### VLAN Parameters

VLAN ID Filter	Any
Tag Priority	Any

OK Cancel

Define which port the packet from. Policy ID is defined in Ports Configuration Page which can group more than 1 port.

### ACE Configuration

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



Ingress Port

Policy 8 ▾  
 Any  
 Policy 1  
 Policy 2  
 Policy 3  
 Policy 4  
 Policy 5  
 Policy 6  
 Policy 7  
**Policy 8**  
 WAN  
 LAN1  
 LAN2  
 LAN3  
 LAN4

**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 ▾  
 Deny  
**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**.

Rate Limiter

Disabled ▾  
**Disabled**  
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8  
 9  
 10

**Port Copy** - Select which port the frames are copied to for the purpose of monitoring. Available settings include **Disabled**, and 1 to 10. The default value is **Disabled**.

Port Copy

Disabled ▾  
**Disabled**  
 WAN  
 LAN1  
 LAN2  
 LAN3  
 LAN4

**Counter** - The counter indicates the number of times the ACE was hit by a frame

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

## MAC Parameter

Specify the destination MAC filter for this ACE.

### MAC Parameters

DMAC Filter	Any ▾
	Any
	MC
	BC
	UC

**Any:** No DMAC filter is specified. (DMAC filter status is "don't-care".)

**MC:** Frame must be multicast.

**BC:** Frame must be broadcast.

**UC:** Frame must be unicast.

## VLAN Parameter

Specify the VLAN ID filter for this ACE.

### VLAN Parameters

VLAN ID Filter	Specific ▾
VLAN ID	1
Tag Priority	Any ▾

**VLAN ID Filter** - Specify the VLAN ID filter for this ACE. If you choose **Any**, no VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) If you want to filter a specific VLAN ID with this ACE, choose **Specific**. A field for entering a VLAN ID number appears.

**VLAN ID** - If you choose Specific, you have to type VLAN ID number manually. The allowed range is 1 to 4095.

**Tag Priority** - Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is from 0 to 7. The value **Any** means that no tag priority is specified (tag priority is "don't-care").

Tag Priority	1 ▾
	0
	1
	2
	3
	4
	5
	6
	7
	Any

## Detailed Explanation for Frame Type

Frame Type selection will lead different options for configuration.

Ingress Port	Policy 1 <input type="button" value="v"/>
Frame Type	ARP <input type="button" value="v"/> Any Ethernet Type <b>ARP</b> IPv4

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

### Ethernet Type Parameters

EtherType Filter	Any <input type="button" value="v"/>
------------------	--------------------------------------

### 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 <input type="button" value="v"/>
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 <input type="button" value="v"/>
Request/Reply	Any <input type="button" value="v"/>
Sender IP Filter	Network <input type="button" value="v"/>
Sender IP Address	192.168.1.1
Sender IP Mask	255.255.255.0
Target IP Filter	Network <input type="button" value="v"/>
Target IP Address	192.168.1.254
Target IP Mask	255.255.255.0

ARP SMAC Match	Any <input type="button" value="v"/>
RARP DMAC Match	Any <input type="button" value="v"/>
IP/Ethernet Length	Any <input type="button" value="v"/>
IP	Any <input type="button" value="v"/>
Ethernet	Any <input type="button" value="v"/>

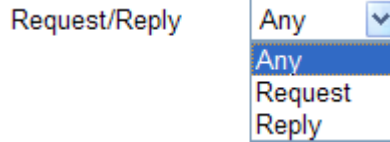
### ARP/RARP

Choose the ARP/RARP that you want to filter.

ARP/RARP	Other <input type="button" value="v"/> Any ARP RARP <b>Other</b>
----------	--

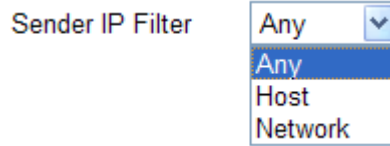
**Request/Reply**

Choose the request or replay that you want to filter.



**Sender IP Filter**

Specify the sender IP filter for this ACE.



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 field.  
Choose **Network** to filter the packets within the network defined in **Sender IP Address** and **Sender IP Mask** fields.

**Sender IP Address**

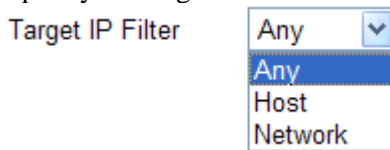
Type the Sender IP Address here. This option is available when you choose **Host** or **Network** as Sender IP Filter.

**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.



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 field.  
Choose **Network** to filter the packets within the network defined in **Target IP Address** and **Target IP Mask** fields.

**Target IP Address**

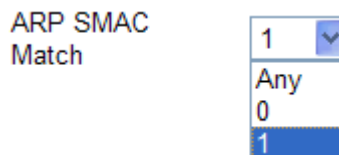
Type the Target IP Address here. This option is available when you choose **Host** or **Network** as Target IP Filter.

**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.



**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 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		ICMP Parameters	
IP Protocol Filter	ICMP	ICMP Type Filter	Specific
IP TTL	Any	ICMP Type Value	255
IP Fragment	Any	ICMP Code Filter	Specific
IP Option	Any	ICMP Code Value	Any
SIP Filter	Network		Specific
SIP Address	192.168.1.1		
SIP Mask	255.255.255.0		
DIP Filter	Network		
DIP Address	192.168.1.254		
DIP Mask	255.255.255.0		

### IP TTL

Specify the Time-to-Live settings for this ACE.

IP TTL	Non-zero
IP Fragment	Any
IP Option	Non-zero
	Zero

**Zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

**Non-zero:** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

**Any:** Any value is allowed.

### IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

IP Fragment	Any
	Any
	Yes
	No

**No:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

**Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

**Any:** Any value is allowed.

### IP Option

Specify the options flag setting for this ACE.

IP Option	Yes
	Any
	Yes
	No

**No:** IPv4 frames where the options flag is set must not be able to match this entry.

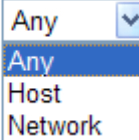
**Yes:** IPv4 frames where the options flag is set must be able

to match this entry.

**Any:** Any value is allowed.

### SIP Filter

Specify the source IP filter for this ACE.

SIP Filter 

**Any:** No source IP filter is specified.

**Host:** Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

**Network:** Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

### SIP Address

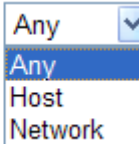
Type the SIP Address here. This option is available when you choose **Host** or **Network** as source SIP Filter.

### SIP Mask

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

### DIP Filter

Specify the destination IP filter for this ACE.

DIP Filter 

**Any:** No destination IP filter is specified.

**Host:** Destination IP filter is set to Host. Specify the destination IP address in the DIP 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 DIP Mask fields that appear.

### DIP Address

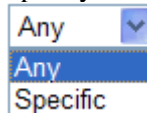
Type the DIP Address here. This option is available when you choose **Host** or **Network** as destination DIP Filter.

### DIP Mask

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

### ICMP Type Filter

Specify the ICMP filter for this ACE.



**Any:** No ICMP filter is specified.

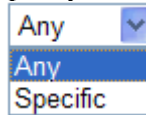
**Specific:** If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

### 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").

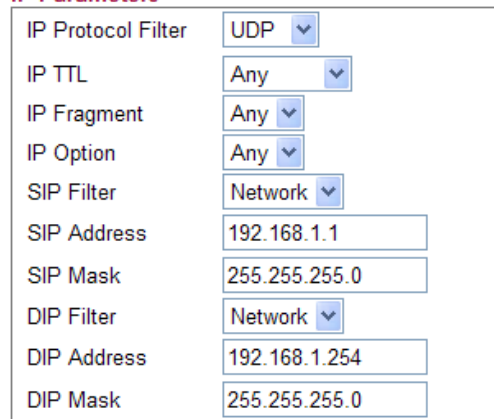
**Specific:** If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

### ICMP Code Value

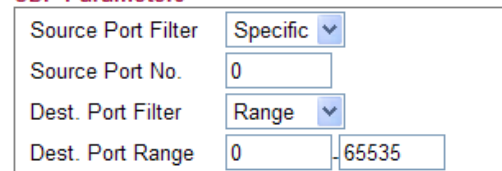
If you choose Specific as ICMP Code Filter, you have to type the ICMP Type Value manually. The allowed range is 0 to 255. A frame meeting this ACE matches this ICMP value.

- 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

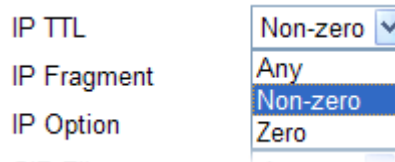


#### UDP Parameters



### IP TTL

Specify the Time-to-Live settings for this ACE.



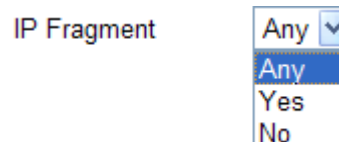
**Zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

**Non-zero:** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

**Any:** Any value is allowed.

### IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.



**No:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.



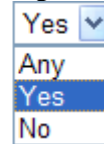
**Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

**Any:** Any value is allowed.

### IP Option

Specify the options flag setting for this ACE.

IP Option



A dropdown menu with a blue arrow icon on the right. The menu is open, showing four options: 'Yes' (top), 'Any', 'Yes' (highlighted in blue), and 'No' (bottom).

**No:** IPv4 frames where the options flag is set must not be able to match this entry.

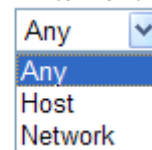
**Yes:** IPv4 frames where the options flag is set must be able to match this entry.

**Any:** Any value is allowed.

### SIP Filter

Specify the source IP filter for this ACE.

SIP Filter



A dropdown menu with a blue arrow icon on the right. The menu is open, showing four options: 'Any' (top), 'Any' (highlighted in blue), 'Host', and 'Network' (bottom).

**Any:** No source IP filter is specified.

**Host:** Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

**Network:** Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

### SIP Address

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

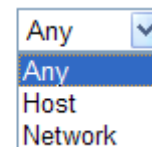
### SIP Mask

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

### DIP Filter

Specify the destination IP filter for this ACE.

DIP Filter



A dropdown menu with a blue arrow icon on the right. The menu is open, showing four options: 'Any' (top), 'Any' (highlighted in blue), 'Host', and 'Network' (bottom).

**Any:** No destination IP filter is specified.

**Host:** Destination IP filter is set to Host. Specify the destination IP address in the DIP 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 DIP Mask fields that appear.

### DIP Address

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

### DIP Mask

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

### Source Port Filter

Specify the UDP port source filter for this ACE.

Source Port Filter 

**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.

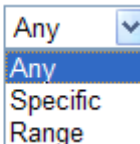
Type the value if you choose **Specific** as the Source Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this UDP source value.

### 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.

Dest. Port Filter 

**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
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Network
SIP Address	192.168.1.1
SIP Mask	255.255.255.0
DIP Filter	Network
DIP Address	192.168.1.254
DIP 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

### IP TTL

Specify the Time-to-Live settings for this ACE.

IP TTL	Non-zero
IP Fragment	Any
IP Option	Non-zero

**Zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

**Non-zero:** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

**Any:** Any value is allowed.

### IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

IP Fragment	Any
-------------	-----

**No:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

**Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

**Any:** Any value is allowed.

### IP Option

Specify the options flag setting for this ACE.

IP Option	Yes
-----------	-----

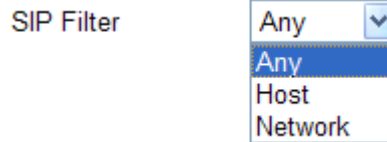
**No:** IPv4 frames where the options flag is set must not be able to match this entry.

**Yes:** IPv4 frames where the options flag is set must be able to match this entry.

**Any:** Any value is allowed.

### SIP Filter

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 SIP Address field that appears.

**Network:** Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

### SIP Address

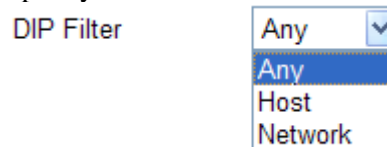
Type the SIP Address here. This option is available when you choose **Host** or **Network** as source SIP Filter.

### SIP Mask

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

### DIP 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 DIP 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 DIP Mask fields that appear.

### DIP Address

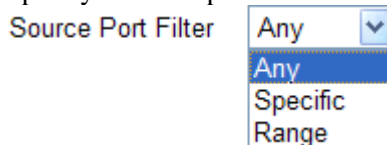
Type the DIP Address here. This option is available when you choose **Host** or **Network** as destination DIP Filter.

### DIP Mask

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

### Source Port Filter

Specify the TCP port source filter for this ACE.



**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.

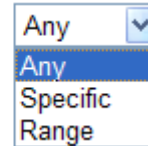
### Source Port Range

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



A dropdown menu with a blue arrow on the right. The current selection is 'Any'. The menu is open, showing three options: 'Any' (highlighted in blue), 'Specific', and 'Range'.

**Any:** No TCP destination filter is specified.

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

**Range:** If you want to filter a specific TCP destination range filter with this ACE, you can enter a specific TCP destination range value. A field for entering a TCP destination port range appears.

### Dest. Port No.

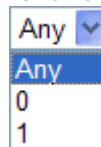
Type the value if you choose **Specific** as the Dest. Port Filter. The allowed range is 0 to 65535. A frame meeting this ACE matches this TCP source value.

### Dest. Port Range

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

### TCP FIN

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



A dropdown menu with a blue arrow on the right. The current selection is 'Any'. The menu is open, showing three options: 'Any' (highlighted in blue), '0', and '1'.

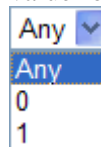
**0:** TCP frames where the FIN field is set must not be able to match this entry.

**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.



A dropdown menu with a blue arrow on the right. The current selection is 'Any'. The menu is open, showing three options: 'Any' (highlighted in blue), '0', and '1'.

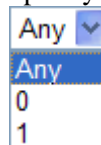
**0:** TCP frames where the SYN field is set must not be able to match this entry.

**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.



A dropdown menu with a blue arrow on the right. The current selection is 'Any'. The menu is open, showing three options: 'Any' (highlighted in blue), '0', and '1'.

**0:** TCP frames where the RST field is set must not be able to match this entry.

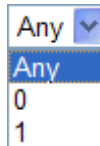
**1:** TCP frames where the RST field is set must be able to

match this entry.

**Any:** Any value is allowed.

### TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.



A dropdown menu with a blue border and a downward arrow on the right. The selected option is 'Any', which is highlighted in blue. Below it, the options '0' and '1' are visible in black text.

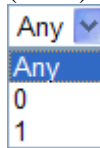
**0:** TCP frames where the PSH field is set must not be able to match this entry.

**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.



A dropdown menu with a blue border and a downward arrow on the right. The selected option is 'Any', which is highlighted in blue. Below it, the options '0' and '1' are visible in black text.

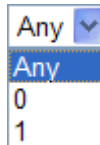
**0:** TCP frames where the ACK field is set must not be able to match this entry.

**1:** TCP frames where the ACK field is set must be able to match this entry.

**Any:** Any value is allowed

### TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.



A dropdown menu with a blue border and a downward arrow on the right. The selected option is 'Any', which is highlighted in blue. Below it, the options '0' and '1' are visible in black text.

**0:** TCP frames where the URG field is set must not be able to match this entry.

**1:** TCP frames where the URG field is set must be able to match this entry.

**Any:** Any value is allowed.

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

### IP Parameters

IP Protocol Filter	Other
IP Protocol Value	255
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Network
SIP Address	192.168.1.1
SIP Mask	255.255.255.0
DIP Filter	Network
DIP Address	192.168.1.254
DIP Mask	255.255.255.0

#### IP Protocol Value

When "Other" is selected for the IP protocol filter, you can enter a specific value here. The range is 0 to 255. The default value is "255". A frame meeting this ACE matches this IP protocol value.

#### IP TTL

Specify the Time-to-Live settings for this ACE.

IP TTL	Non-zero
IP Fragment	Any
IP Option	Non-zero

**Zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

**Non-zero:** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

**Any:** Any value is allowed.

#### IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

IP Fragment	Any
-------------	-----

**No:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

**Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

**Any:** Any value is allowed.

#### IP Option

Specify the options flag setting for this ACE.

IP Option	Yes
-----------	-----

**No:** IPv4 frames where the options flag is set must not be

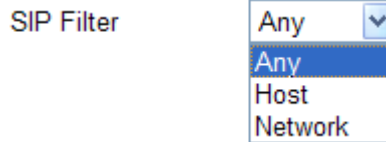
able to match this entry.

**Yes:** IPv4 frames where the options flag is set must be able to match this entry.

**Any:** Any value is allowed.

### SIP Filter

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 SIP Address field that appears.

**Network:** Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

### SIP Address

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

### SIP Mask

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

### DIP 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 DIP 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 DIP Mask fields that appear.

### DIP Address

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

### DIP Mask

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

## 4.5 Bandwidth Management

Below shows the menu items for Bandwidth Management.





## 4.5.1 Session Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

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

**Bandwidth Management >> Session Limit**

### Session Limit Configuration

Enable  Disable

Default Max Sessions:

**Limitation List**

Index	Start IP	End IP	Max Sessions
-------	----------	--------	--------------

**Specific Limitation**

Start IP:  End IP:

Maximum Sessions:

To activate the function of limit session, simply click **Enable** and set the default session limit.

**Enable**

Click this button to activate the function of limit session.

**Disable**

Click this button to close the function of limit session.

**Default Max Sessions**

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

**Limitation List**

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

**Start IP**

Defines the start LAN IP address for limit session.

**End IP**

Defines the end LAN IP address for limit session.

**Maximum Sessions**

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

**Add**

Adds the specific session limitation onto the list above.

**Edit**

Allows you to edit the settings for the selected limitation.

**Delete**

Remove the selected settings existing on the limitation list.

When you finish adding a new session limit, simply click **OK**. The following page will appear for you to check.

## 4.5.2 Bandwidth Limit

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

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

**Bandwidth Management >> Bandwidth Limit**

### Bandwidth Limit Configuration

Enable  Disable

Default TX Limit:  Kbps      Default RX Limit:  Kbps

**Limitation List**

Index	Start IP	End IP	TX limit	RX limit
-------	----------	--------	----------	----------

**Specific Limitation**

Start IP:       End IP:

TX Limit:  Kbps      RX Limit:  Kbps

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

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

**Enable**      Click this button to activate the function of limit bandwidth.

**Disable**      Click this button to close the function of limit bandwidth.

**Default TX limit**      Define the default speed of the upstream for each computer in LAN.

**Default RX limit**      Define the default speed of the downstream for each computer in LAN.

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

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

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

**TX Limit**      Define the limitation for the speed of the upstream to be applied as specific limitation. If you do not set the limit in this field, the

system will use the default speed for the specific limitation you set for each index.

- RX Limit** Define the limitation for the speed of the downstream to be applied as specific limitation. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
- Add** Add the specific speed limitation onto the list above.
- Edit** Allows you to edit the settings for the selected limitation.
- Delete** Remove the selected settings existing on the limitation list.

When you finish adding a new bandwidth limit, simply click **OK**. The following page will appear for you to check.

### 4.5.3 Port Rate Control

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

#### Bandwidth Management >> Port Rate Control

##### Rate Limit Configuration

Port	Policer Enabled	Policer Rate(Rx)	Policer Unit	Shaper Enabled	Shaper Rate(Tx)	Shaper Unit
WAN	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	10	Mbps

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

OK Cancel

- Port** Represent LAN or WAN interface.
- Policer Enabled** Check this box to enable policer function.
- Policer Rate(Rx)** Type the number for policer function. The default value is 500. It is restricted to 500-1000000 when the Policer Unit is set in kbps, and it is restricted to 1-1000 when the Policer Unit is set in Mbps.
- Policer Unit** Determine the unit (kbps/Mbps) for policer.
- Shaper Enabled** Check this box to enable shaper function.
- Shaper Rate (Tx)** Type the number for shaper function. The default value is 500. It is restricted to 500-1000000 when the Shaper Unit is set in kbps, and it is restricted to 1-1000 when the Shaper Unit is set in Mbps.
- Shaper Unit** Determine the unit (kbps/Mbps) for shaper function.

### 4.5.4 QoS Control List

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If

other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

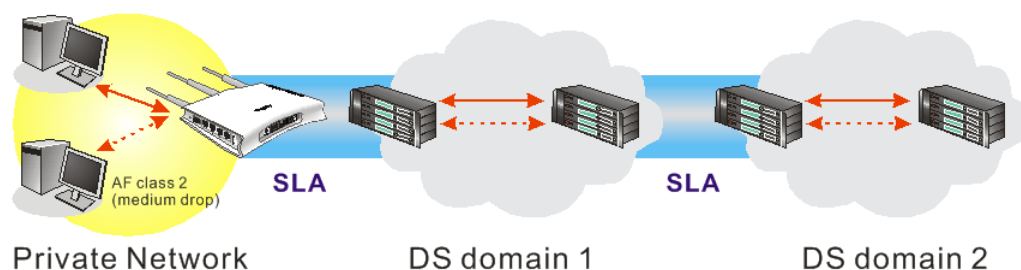
There are two components within Primary configuration of QoS deployment:

- **Classification:** Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- **Scheduling:** Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



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

In the **Bandwidth Management** menu, click **QoS Control List** to open the web page.

## Bandwidth Management >> QoS Control List

### QoS Control List Configuration

QCL #

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

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

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

**Type Value** Display the value specified for the QCE.

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

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

### QoS Control List Configuration

QCL #

QCE Type	Type Value
TCP/UDP Port	22 - 23

### Adding a New QCE

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

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

## Bandwidth Management >> QoS Control List

### QCE Configuration

QCE Type	Ethernet Type
Ethernet Type Value	0xFFFF
Traffic Class	Low

Low  
Normal  
Medium  
High

OK Cancel

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

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

## Bandwidth Management >> QoS Control List

### QCE Configuration

QCE Type	VLAN ID
VLAN ID	1
Traffic Class	Low

Low  
Normal  
Medium  
High

OK Cancel

- 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

Low  
Normal  
Medium  
High

OK Cancel

**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

Low  
Normal  
Medium  
High

OK Cancel

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

**Bandwidth Management >> QoS Control List**

**QCE Configuration**

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

Low  
Normal  
Medium  
High

OK Cancel

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

**Bandwidth Management >> QoS Control List**


**QCE Configuration**

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



Low  
Normal  
Medium  
High

OK Cancel

## Editing a QCE

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

## Moving Up/Down a QCE

Click  and  to move a QCE up and down.

## Deleting a QCE

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

## 4.5.5 Ports Priority

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

[Bandwidth Management >> Ports Priority](#)

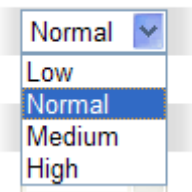
### Port QoS Configuration

Port	Default Class	QCL #	Queuing Mode	Queue 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
WiFi1	Normal	1	Weighted	1	2	4	8

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

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

### Default Class

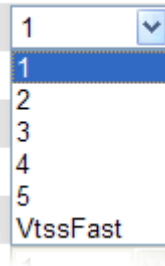




## QCL

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

**QCL #**

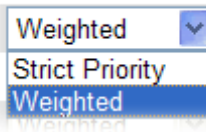


1  
1  
2  
3  
4  
5  
VtssFast

## Queuing Mode

Use the drop down list to choose suitable mode.

**Queuing Mode**



Weighted  
Strict Priority  
Weighted

## Queue Weighted

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

## 4.5.6 QoS Statistics

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

### Bandwidth Management >> QoS Statistics

#### Queuing Counters

Auto-refresh  Refresh Clear

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
<a href="#">WAN</a>	58350	61843	69518	0	76195	63030	22	12
<a href="#">LAN1</a>	0	0	0	0	0	0	0	0
<a href="#">LAN2</a>	57361	7575	1953	61191	66042	75655	21	0
<a href="#">LAN3</a>	0	0	0	0	0	0	0	0
<a href="#">LAN4</a>	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

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		

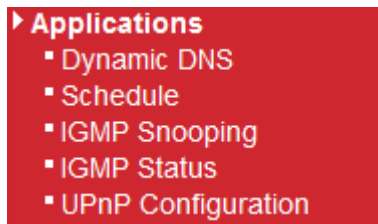
<b>Rx Packets</b>	Display the counting number of the packet received.
<b>Rx Octets</b>	Display the total received bytes.
<b>Rx Unicast</b>	Display the counting number of the received unicast packet.
<b>Rx Broadcast</b>	Display the counting number of the received broadcast packet.
<b>Rx Pause</b>	Display the counting number of the received pause packet.
<b>RX 64 Bytes</b>	Display the number of 64-byte frames in good and bad packets received.
<b>RX 65-127 Bytes</b>	Display the number of 65 ~ 127-byte frames in good and bad packets received.
<b>RX 128-255 Bytes</b>	Display the number of 128 ~ 255-byte frames in good and bad packets received.
<b>RX 256-511 Bytes</b>	Display the number of 256 ~ 511-byte frames in good and bad packets received.
<b>RX 512-1023 Bytes</b>	Display the number of 512 ~ 1023-byte frames in good and bad packets received.
<b>RX 1024- 1526 Bytes</b>	Display the number of 1024-1522-byte frames in good and bad packets received.
<b>RX 1527 Bytes</b>	Display the number of 1527-byte frames in good and bad packets received.

<b>Rx Low</b>	Display the low queue counter of the packet received.
<b>Rx Normal</b>	Display the normal queue counter of the packet received.
<b>Rx Medium</b>	Display the medium queue counter of the packet received.
<b>Rx High</b>	Display the high queue counter of the packet received.
<b>Rx Drops</b>	Display the number of frames dropped due to the lack of receiving buffer.
<b>Rx CRC/Alignment</b>	Display the number of Alignment errors packets received.
<b>Rx Undersize</b>	Display the number of short frames (<64 Bytes) with valid CRC.
<b>Rx Oversize</b>	Display the number of long frames (according to max_length register) with valid CRC.
<b>Rx Fragments</b>	Display the number of short frames (< 64 bytes) with invalid CRC.
<b>Rx Jabber</b>	Display the number of long frames (according to max_length register) with invalid CRC.
<b>Rx Filtered</b>	Display the filtered number of the packet received.
<b>Tx Packets</b>	Display the the counting number of the packet transmitted.
<b>Tx Octets</b>	Display the total transmitted bytes.
<b>Tx Unicast</b>	Display the show the counting number of the transmitted unicast packet.
<b>Tx Multicast</b>	Display the show the counting number of the transmitted multicast packet.
<b>Tx Broadcast</b>	Display the counting number of the transmitted broadcast packet.
<b>Tx Pause</b>	Show the counting number of the transmitted pause packet.
<b>Tx 64 Bytes</b>	Display the number of 64-byte frames in good and bad packets transmitted.
<b>Tx 65-127 Bytes</b>	Display the number of 65 ~ 127-byte frames in good and bad packets transmitted.
<b>Tx 128-255 Bytes</b>	Display the number of 128 ~ 255-byte frames in good and bad packets transmitted.
<b>Tx 256-511 Bytes</b>	Display the number of 256 ~ 511-byte frames in good and bad packets transmitted.
<b>Tx 512-1023 Bytes</b>	Display the number of 512 ~ 1023-byte frames in good and bad packets transmitted.
<b>Tx 1024- 1526 Bytes</b>	Display the number of 1024 ~ 1522-byt frames in good and bad packets transmitted.
<b>Tx 1527 Bytes:</b>	Display the number of 1527-byte frames in good and bad packets transmitted.
<b>Tx Low</b>	Display the low queue counter of the packet transmitted.
<b>Tx Normal</b>	Display the normal queue counter of the packet transmitted.
<b>Tx Medium</b>	Display the medium queue counter of the packet received.

<b>Tx High</b>	Display the high queue counter of the packet received.
<b>Tx Drops</b>	Display the number of frames dropped due to excessive collision, late collision, or frame aging.
<b>Tx lat/Exc.Coll.</b>	Display the number of Frames late collision or excessive collision Error, which switch transmitted.

## 4.6 Applications

Below shows the menu items for Applications.



### 4.6.1 Dynamic DNS

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

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

[Applications >> Dynamic DNS](#)

#### Dynamic DNS Configuration

Enable Dynamic DNS	<input type="checkbox"/>
DynDNS Service	dyndns.org
Hostname	mypersonaldomain.dyndn:
Username	myusername
Password	mypassword
Check IP change every	10 minutes
Force IP update every	72 hours

OK Cancel

<b>Enable Dynamic DNS</b>	Check this box to enable the current account.
<b>DynDNS Service</b>	Select the service provider for the DDNS account.
<b>Hostname</b>	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
<b>Username</b>	Type in the login name that you set for applying domain.

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

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

## 4.6.2 Schedule

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

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

### Applications >> Schedule

Schedule Configuration		
Index	Setting	Status
<input type="button" value="Add"/>		

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

### Applications >> Schedule

#### Add Schedule

<input checked="" type="checkbox"/> Enable		
Start Date	<input type="text"/> - <input type="text"/> - <input type="text"/> ( Year - Month - Date )	
Start Time	<input type="text"/> : <input type="text"/> ( Hour : Minute )	
Action	<input type="text" value="WAN UP"/> ▾	
Acts	<input type="text" value="Once"/> ▾	
Weekday	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

<b>Enable</b>	Check to enable the schedule.
<b>Start Date</b>	Specify the starting date of the schedule.
<b>Start Time</b>	Specify the starting time of the schedule.
<b>Action</b>	Specify which action Call Schedule should apply during the period of the schedule. <b>Force On</b> -Force the connection to be always on. <b>Force Down</b> -Force the connection to be always down. <b>Enable Dial-On-Demand</b> -Specify the connection to be dial-on-demand and the value of idle timeout should be

specified in **Idle Timeout** field.

**Disable Dial-On-Demand** -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

**Acts**

Specify how often the schedule will be applied

**Once** -The schedule will be applied just once

**Routine /Weekday** -Specify which days in one week should perform the schedule.

### 4.6.3 IGMP Snooping

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

**Applications >> IGMP Snooping**

**IGMP Snooping Configuration**

General Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input type="checkbox"/>

Port Related Configuration	
Port	Fast Leave
LAN1	<input type="checkbox"/>
LAN2	<input type="checkbox"/>
LAN3	<input type="checkbox"/>
LAN4	<input type="checkbox"/>

**Snooping Enabled**

Check the box to enable this function.

**Unregistered IPMC...**

Check the box to enable unregistered IPMC traffic flooding

**Fast Leave**

Check the box to Fast Leave on the LAN port.

## 4.6.4 IGMP Status

This page display current IGMP status.

[Applications >> IGMP Status](#)

### IGMP Snooping Status

Auto-refresh

#### Statistics

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

#### IGMP Groups

Groups	Port Members
No IGMP groups	2 3 4

#### V1~3 Reports Receive

Display the number of Received V1 – V3 Reports.

#### V2 Leave Receive

Display the number of Received V2 Leave.

#### Groups

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

#### Port Members

Display the LAN ports in this group.

#### Refresh

Click this button to refresh the page immediately.

#### Clear

Click this button to clear the settings on this page.

## 4.6.5 UPnP Configuration

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

[Applications >> UPnP Configuration](#)

### UPnP Configuration

Enable UPnP	<input checked="" type="checkbox"/>
Download Speed	<input type="text" value="1024"/> kbps
Upload Speed	<input type="text" value="512"/> kbps

#### Enable UPnP

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



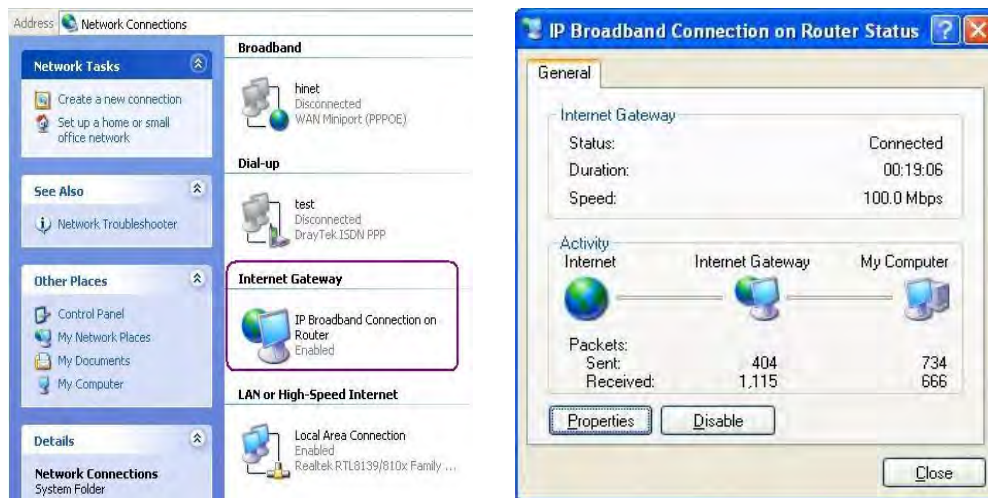
## Download Speed

Enter the maximum sustained WAN download speed in kilobits/second. Such information can be requested by UPnP clients.

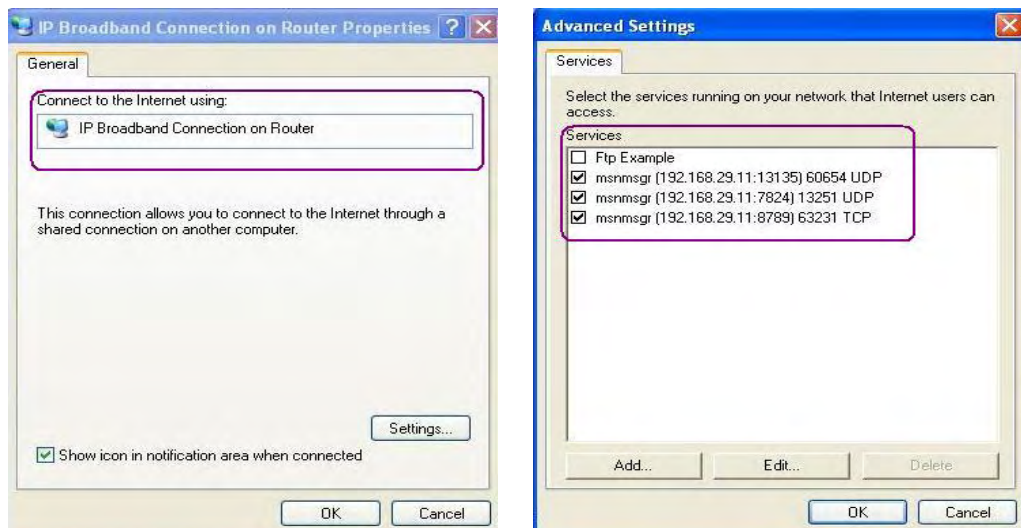
## Upload Speed

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.



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.



The reminder as regards concern about Firewall and UPnP  
**Can't work with Firewall Software**



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

#### Security Considerations

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

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

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

## 4.7 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.

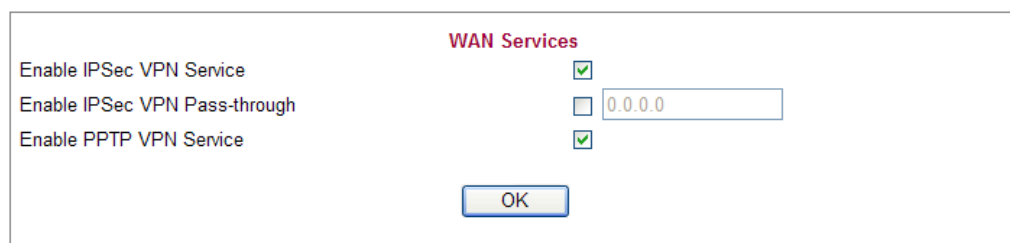


### 4.7.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should enable IPSec VPN Pass-through and specify an IP address to allow VPN tunnel pass through.

[VPN and Remote Access >> Remote Access Control](#)

Remote Access Control Setup



#### Enable IPSec VPN Service

If this checkbox is checked, the system firewall will allow VPN (IPSec) remote access from WAN side to the router.

#### Enable IPSec VPN Pass-through

If this checkbox is checked, the system firewall will allow VPN (IPSec) remote access from WAN side to a VPN device on the LAN. Type the IP address of the VPN device in the field next to the checkbox.

### Enable PPTP VPN Service

If this checkbox is checked, the system firewall will allow VPN (PPTP) remote access from WAN side to the router.

## 4.7.2 PPTP Remote Dial-in

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection.

The router provides access accounts for dial-in users.

### Users

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

Add a New User

### Adding a New User

Click **Add new user** to open the following page.

### User Configuration

#### Add User

User Settings	
Username	<input type="text" value="carrie"/>
Full Name	<input type="text" value="carrie ni"/>
Password	<input type="password" value="••••••"/>
Confirm Password	<input type="password" value="••••••"/>
Allow Disk Sharing	<input checked="" type="checkbox"/>
Allow IPSEC/L2TP	<input checked="" type="checkbox"/>
Allow PPTP	<input checked="" type="checkbox"/>
Allow FTP	<input checked="" type="checkbox"/>

OK

Cancel

Delete User

#### Username

Type a name for this user.

#### Full Name

Type full name for this user.

#### Password

Type the password for this user.

#### Password (again)

Type the password again for confirmation.

#### Allow Disk Sharing

Check this box to have the remote user share the disk information.

#### Allow IPSEC/L2TP

Check this box to let the remote user connecting to this device through IPSEC/L2TP.

#### Allow PPTP

Check this box to let the remote user connecting to this device through PPTP.

#### Allow FTP

Check this box to let the remote user connecting to FTP server via this router.

#### Delete User

Remove settings on current page and delete the user. This button is not available for new configuration by pressing **Add a New User**.

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

### Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
<a href="#">carrie</a>	carrie ni	✓	✓	✓	✓

### Editing/Deleting User Settings

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

### User Configuration

#### Edit User

User Settings	
Username	<input type="text" value="carrie"/>
Full Name	<input type="text" value="carrie ni"/>
Password	<input type="password" value="••••••"/>
Confirm Password	<input type="password" value="••••••"/>
Allow Disk Sharing	<input checked="" type="checkbox"/>
Allow IPSEC/L2TP	<input checked="" type="checkbox"/>
Allow PPTP	<input checked="" type="checkbox"/>
Allow FTP	<input checked="" type="checkbox"/>

### 4.7.3 IPSec Remote Dial-in

This page allows you to configure IPSec Site-to-Client settings.

#### VPN and Remote Access >> Remote Dial-in Setup

##### IPSec Site-to-Client (Mobile VPN)

###### Mobile VPN Type

Mobile VPN Type	Disabled
-----------------	----------

###### Authentication

Type	Preshared secret
Shared secret	
Shared secret (again)	

###### Identities

Local Identity	
----------------	--

###### Advanced Settings

Phase 1 (IKE) Encryption	Automatic
Phase 2 (IPSec) Encryption	Automatic

OK Cancel

#### 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.

###### Mobile VPN Type

Mobile VPN Type	L2TP/IPsec
L2TP IP Address range	
DHCP IP Address range	192.168.1.10-192.168.1.60

## Authentication

**Type** - Determine the authentication method for remote dial-in user.

### Authentication

Type	Preshared secret ▼
------	--------------------

### Authentication

Type	Certificates ▼
------	----------------

**Preshared secret** – If you choose this one, you have to type the shared secret manually and specify local identity. When using Preshared secret, *all* clients share the same secret.

**Certificates** - If you choose this one, you have to choose local certificate from the **Local Certificate** drop down list and type in local identity. Then, use **Add Identity** to specify remote identity for this service.

## Identities

### Identities

Local Certificate	None ▼
Local Identity	<input type="text"/>
Remote Identities	<input type="button" value="Add Identity"/>

**Local Certificate** - Used to authenticate the local part of the VPN tunnel (while using certificate-based authentication).

**Local Identity** - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode. It can also be a DNS name or an email address.

**Remote Identities** - Define the identities of allowed clients.

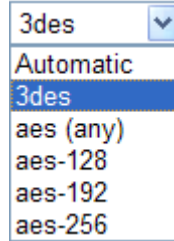
## Advanced Settings

**Phase 1 (IKE) Encryption** - 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.

3des ▼
Automatic
3des
aes (any)
aes-128
aes-192
aes-256

**Phase 2 (IPSec) Encryption** - 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.



#### 4.7.4 Remote Dial-in Status

You can find the summary table of all dial-in user status.

[VPN and Remote Access >> Remote Dial-in Status](#)

Auto-refresh

---

**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	TTY	Remote IP	Login Time	Rx bytes	Tx bytes
No PPTP Clients					

- Client** Display the name of the VPN IPSec/Mobile client.
- Identity** Display the remote ID of the VPN client.
- Endpoint** Display the IP address of the VPN client.
- IKE Status** Display the status of the phase 1 ISAKMP key exchange.
- IKE Alg** Display the encryption and authentication algorithm used during phase 1 of the VPN connection Establishment. The algorithm is used during exchange of key exchange.
- ESP Status** Display the status of the phase 2 IPSec ESP key exchange.
- ESP Alg** Display the encryption and authentication algorithm used during phase 2 of the VPN connection Establishment. This algorithm is used for transporting data, and the choice will affect the performance of the VPN tunnel.
- User Name** Display the dial-in user account.
- TTY** Display the connection name assigned by the router.
- Remote IP** Display IP address of remote client.
- Login Time** Display the system time that the user logs in.
- Rx bytes** Display the data total received for such client.
- Tx bytes** Display the data total transmitted for such client.
- Auto-refresh** Check this box to make the system refresh this page automatically.

## Refresh

Click this button to refresh the page immediately.

### 4.7.5 LAN to LAN

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

The router supports 2 VPN tunnels simultaneously and provides up to 2 profiles. The following figure shows the summary table.

#### VPN and Remote Access >> LAN to LAN

##### VPN Site-to-Site Tunnels (IPSec)

Auto-refresh

Name	Endpoint	IKE Status	IKE Alg	ESP Status	ESP Alg
No VPN tunnels					

<b>Name</b>	Indicate the name of the LAN-to-LAN profile.
<b>Endpoint</b>	Display the IP address of the VPN client.
<b>IKE Status</b>	Display the status of the phase 1 ISAKMP key exchange.
<b>IKE Alg</b>	Display the encryption and authentication algorithm used during phase 1 of the VPN connection Establishment. The algorithm is used during exchange of key exchange.
<b>ESP Status</b>	Display the status of the phase 2 IPSec ESP key exchange.
<b>ESP Alg</b>	Display the encryption and authentication algorithm used during phase 2 of the VPN connection Establishment. This algorithm is used for transporting data, and the choice will affect the performance of the VPN tunnel.

#### Adding a VPN Tunnel

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

Add VPN Tunnel

General

Enabled	<input checked="" type="checkbox"/>
Name	<input type="text"/>
Remote IP	<input type="text"/>

Authentication

Type	Pre-Shared Key ▾
Pre-Shared Key	<input type="text"/>
Confirm Pre-Shared Key	<input type="text"/>
Local Identity	<input type="text"/>
Remote Identity	<input type="text"/>

Networks

Local Network / Mask	<input type="text"/> / <input type="text"/>
Remote Network / Mask	<input type="text"/> / <input type="text"/>

Advanced Settings

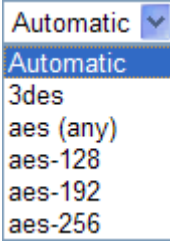
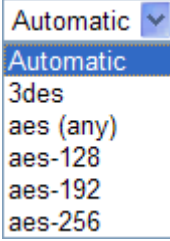
IKE phase 1 proposal	Automatic ▾
IKE phase 2 proposal	Automatic ▾
Perfect Forward Secrecy	<input checked="" type="checkbox"/>

OK Cancel

- Enabled** Check here to activate this tunnel.
- Name** Specify a name for this tunnel.
- Remote IP** Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
- Type** This group of fields is applicable for IPSec Tunnels. Different type will bring out different requirement of information.  

<b>Authentication</b>	
Type	Certificates ▾
Local Certificate	Preshared key
Local Identity	Certificates
Remote Identity	<input type="text"/>
- Pre-Shared Key** Such field will be applicable when Preshared 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 Preshared key is selected as the Type for the authentication. Input 1-63 characters as pre-shared key again to confirm it.
- Local Certificate** Such field will be applicable when Certificates is selected as the Type for the authentication.
- 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.



<b>Local Network / Mask</b>	Traffic between this subnet and the subnet specified in Remote Network / Mask will travel through the VPN tunnel.
<b>Remote Network / Mask</b>	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.
<b>IKE Phase 1 proposal</b>	To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. 
<b>IKE Phase 2 proposal</b>	To propose the local available algorithms to the VPN peers, and get its feedback to find a match. 
<b>Perfect Forward Secrecy</b>	The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

## 4.8 Wireless LAN

This function is used for “n” models.

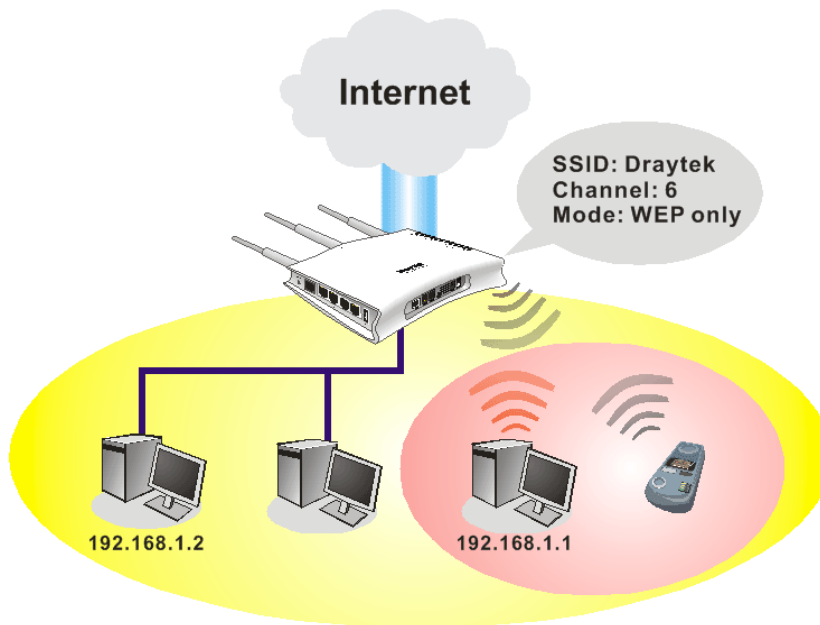
### 4.8.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor “n” model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.

**Note:** \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



## Security Overview

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

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

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Below shows the menu items for Wireless LAN.



## 4.8.2 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

Please refer to the following figure for more information.

**Wireless LAN >> General Setup**

---

**General Setting**

Enable Wireless LAN	<input checked="" type="checkbox"/>
SSID Broadcast	Show
SSID	DrayTek
Wireless Mode	Mixed (11b+11g+11n)
Country Region Code	0: channels 1-11
Channel	Channel 11, 2462MHz

**Wireless Security Configuration**

Encryption	None
------------	------

OK Cancel

### Enable Wireless LAN

Check the box to enable the wireless function.

### SSID Broadcast

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

### SSID

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

### Wireless Mode

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

### Country Region Code

It represents different country region code. Use the drop down list to choose the one that fit the usage of regulations locally.

### Channel

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

### Encryption

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

None

None

WEP

WPA-PSK

WPA-RADIUS

WPS

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

## Wireless Security Configuration

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

**Wireless Security Configuration**

Encryption

- None
- WEP
- WPA-PSK
- WPA-RADIUS
- WPS

- **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 Configuration**

Default Key

Key1

Key2

Key3

Key4

Authentication Mode

**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	

OK Cancel

### 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 Preshared 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

OK Cancel

### Type

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

Auto(WPA or WPA2)
WPA
WPA2
Auto(WPA or WPA2)

**WPA Algorithm**

Choose the WPA algorithm, TKIP, AES or Auto.

**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.

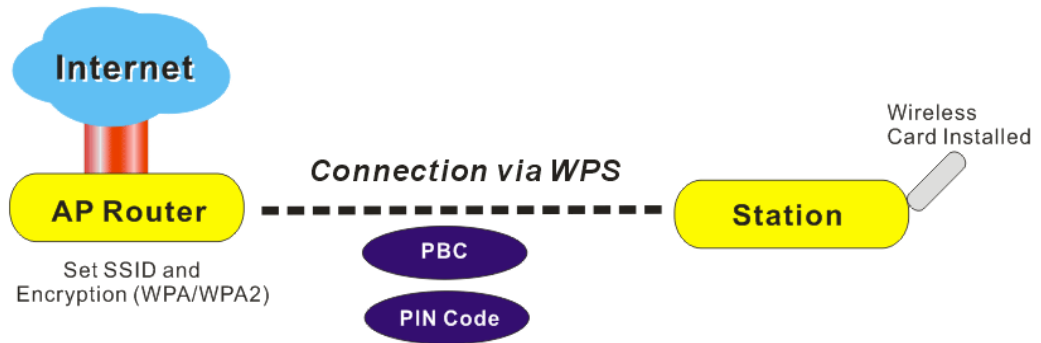
**Configure via Push Button**

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

**Configure via Client PinCode**

Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

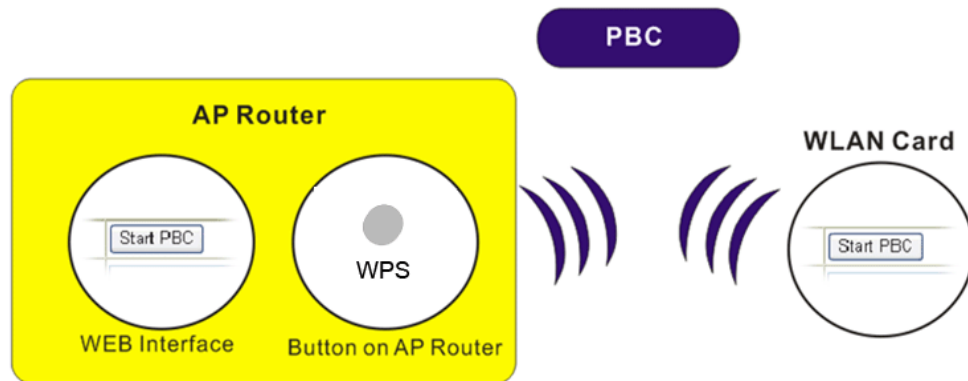
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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



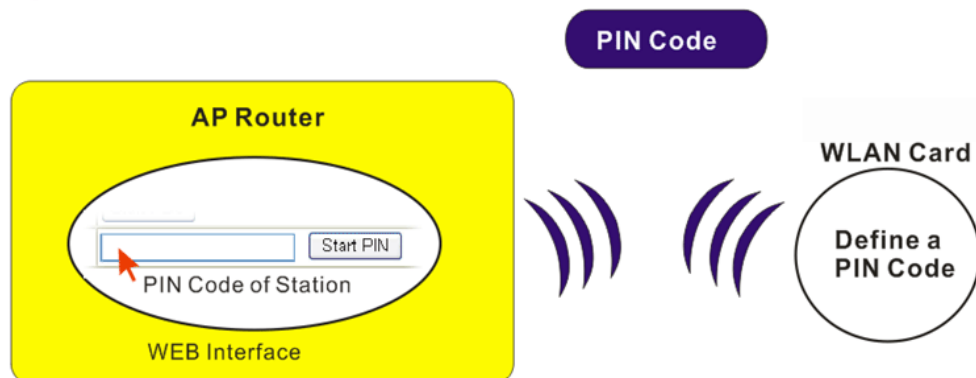
**Note:** Such function is available for the wireless station with WPS supported.

There are two methods to do network connection through WPS between AP and Stations: pressing the **Start PBC** button or using **PIN Code**.

On the side of Vigor 2130 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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



### 4.8.3 Access Control

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

Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type Deny List ▾

---

**Delete** **MAC Address**

Add a New Entry

**Filter Type**

Choose the rule for the MAC addresses displayed in this page.

**Allow List** – all the MAC address of wireless clients listed here are allowed to do wireless connection.

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

**Add a New Entry**

Add a new MAC address into the list.

**Delete**

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

Wireless LAN >> Access Control

Wireless MAC Address Filter Configuration

Filter Type Deny List ▾

---

**Delete** **MAC Address**

Delete 00:20:00:05:30:12

Add a New Entry

**Cancel**

Give up the configuration.

**OK**

Click it to save the configuration.

### 4.8.4 Station List

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

Wireless LAN >> Station List

Station List

Auto-refresh

Index	IP Address	MAC Address	Connected Time
No Station			

**Index**

Display the number of the connecting client.

**IP Address**

Display the WAN IP address for the connecting client.

**MAC Address**

Display the MAC Address for the connecting client.



<b>Connected Time</b>	Display the connection time for the connecting client.
<b>Auto-refresh</b>	Check this box to force the system refreshing the table automatically.
<b>Refresh</b>	Click this button to refresh current page.

## 4.8.5 Access Point Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage.

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

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

### Wireless LAN >> Access Point Discovery

**Access Point Discovery**

Channel	SSID	BSSID	Enc	Auth	Signal(%)

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

<b>Channel</b>	Display the channel for the scanned AP.
<b>SSID</b>	Display the SSID of the scanned AP.
<b>BSSID</b>	Display the MAC address of the scanned AP.
<b>Enc</b>	Display the encryption type of the scanned AP.
<b>Auth</b>	Display the authentication method of the scanned AP.
<b>Signal</b>	Display the strength (in percentage) of the signal of the scanned AP.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button.

## 4.9 USB Application

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

- ▶ **USB Application**
  - USB General Settings
  - FTP User Management
  - Disk Status
  - Disk Shares

## 4.9.1 USB General Settings

This page will determine the number of concurrent FTP connection and default charset for FTP server. At present, the Vigor router can support USB diskette with versions of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure the memory format for the USB diskette is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

### USB Application >> USB General Settings

#### USB General Settings

Enable FTP	<input type="checkbox"/>
Enable Disk Sharing	<input type="checkbox"/>
Workgroup Name	<input type="text" value="WORKGROUP"/>

- Enable FTP** Check this box to enable FTP connection.
- Enable Disk Sharing** Check this box to share the information on USB disk.
- Workgroup Name** Type the name for FTP users for accessing into FTP server (USB diskette). Be aware that users cannot access into USB diskette in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage diskette.

## 4.9.2 FTP User Management

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

### USB Application >> FTP User Management

#### FTP User Management

User Name	Volume	Path	Access Rights
<a href="#">carrie</a>	--	--	Read-only

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

### USB Application >> FTP User Setting

#### FTP User Configuration

User Name	<input type="text" value="carrie"/>
Volume	<input type="text" value="USB2.0 - Mobile Disk (1) - 1967M - PORT 1"/>
Home Folder	<input type="text" value="/"/>
Access Rule	<input type="text" value="Read-only"/>

- User Name** It displays the username that user uses to login to the FTP server.
- Volume** Select the proper volume for the connected USB diskette.

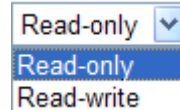
### Home Folder

It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB diskette. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB diskette.

**Note:** When write protect status for the USB diskette is **ON**, you cannot type any new folder name in this field. Only “/” can be used in such case.

### Access Rule

Select the access right for the USB diskette.



A dropdown menu with a blue border and a downward arrow. The current selection is 'Read-only'. The menu is open, showing 'Read-only' and 'Read-write' as options.

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

## 4.9.3 Disk Status

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

### USB Application >> Disk Status

#### Disk Status

Safely Remove Disk	Manufacturer	Model	Size	Status
<input type="checkbox"/>	USB2.0	Mobile Disk	1968M	In use

Update

### S Safely Remove Disk

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

### Manufacturer

Display the manufacturer of the disk.

### Model

Display the type of the disk.

### Size

Display the storage space of the diskette(s).

### Status

Display current usage status of the diskette(s)

### Update

Click this button to refresh the disk status.

## 4.9.4 Disk Shares

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

### USB Application >> Disk Shares

#### Disk Shares

Share Name	Comment	Path	Visible
	No Shares		

Add a New Entry

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	<input type="text"/>
Comment	<input type="text"/>

**Settings**

Volume	USB2.0 - Mobile Disk (1) - 1967M - PORT 1 ▾
Path	<input type="text" value="/"/>
Visible	<input type="checkbox"/>

**Access Rights**

Access	All Users Read-only ▾
--------	-----------------------

OK Cancel

- Share Name** Type a name to be known by other computers in local network. The name must not contain spaces or special characters.
- Comment** Type the brief description for the disk sharing. The words here will be seen in Network Neighborhood on Windows client computers
- Volume** Select the proper volume for the connected USB diskette.
- Path** It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB diskette. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB diskette.  
**Note:** When write protect status for the USB diskette is **ON**, you cannot type any new folder name in this field. Only “/” can be used in such case.
- Visible** Check this box to make this USB diskette to be seen in Network Neighborhood on Windows of clients in local network.
- Access Rights** Specify the access right and apply to all the wireless clients that want to connect to the attached USB diskette.

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

## 4.10 User

### 4.10.1 User Configuration

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

#### Users

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

Add a New User

### Adding a New User

Click **Add new user** to open the following page.

#### User Configuration

##### Add User

User Settings	
Username	<input type="text" value="carrie"/>
Full Name	<input type="text" value="carrie ni"/>
Password	<input type="password" value="••••••••"/>
Confirm Password	<input type="password" value="••••••••"/>
Allow Disk Sharing	<input checked="" type="checkbox"/>
Allow IPSEC/L2TP	<input checked="" type="checkbox"/>
Allow PPTP	<input checked="" type="checkbox"/>
Allow FTP	<input checked="" type="checkbox"/>

OK

Cancel

<b>Username</b>	Type a name for this user.
<b>Full Name</b>	Type full name for this user.
<b>Password</b>	Type the password for this user.
<b>Password (again)</b>	Type the password again for confirmation.
<b>Allow Disk Sharing</b>	Check this box to have the remote user share the disk information.
<b>Allow IPSEC/L2TP</b>	Check this box to let the remote user connecting to this device through IPSEC/L2TP.
<b>Allow PPTP</b>	Check this box to let the remote user connecting to this device through PPTP.
<b>Allow FTP</b>	Check this box to let the remote user connecting to FTP server via this router.
<b>Delete User</b>	Remove settings on current page and delete the user. This button is not available for new configuration by pressing <b>Add a New User</b> .

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

### Users

#### Users

Username	Full Name	Allow Disk Sharing	Allow IPSEC/L2TP	Allow PPTP	Allow FTP
<a href="#">carrie</a>	carrie ni	✓	✓	✓	✓

Add a New User

### Editing/Deleting User Settings

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

### User Configuration

#### Edit User

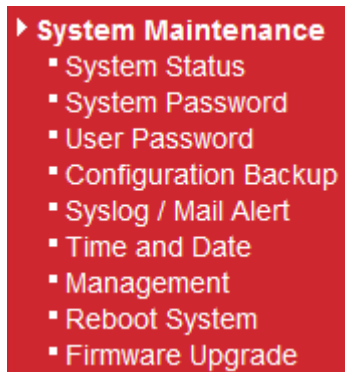
User Settings	
Username	<input type="text" value="carrie"/>
Full Name	<input type="text" value="carrie ni"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="••••"/>
Allow Disk Sharing	<input type="checkbox"/>
Allow IPSEC/L2TP	<input type="checkbox"/>
Allow PPTP	<input type="checkbox"/>
Allow FTP	<input type="checkbox"/>

OK Cancel Delete User

## 4.11 System Maintenance

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

Below shows the menu items for System Maintenance.



### 4.11.1 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

Model	: Vigor2130
Platform	: VSC7501
Bootloader Version	: Dray-Boot 1.0.0E
Firmware Version	: v1.1.0_RC6
Build Date/Time	: r753 Tue Aug 25 16:11:42 CST 2009
Hardware NAT Version	: 1.0.0.13
System Date	: Mon Aug 31 03:02:52 2009
System Uptime	: 3d 10:39:36

LAN
MAC Address : 00:50:7F:C7:7B:30
IP Address : 192.168.1.1
IP Mask : 255.255.255.0

WAN
MAC Address : 00:50:7F:C7:7B:31
IP Address : 192.168.5.21
IP Mask : 255.255.255.0
Default Gateway : 192.168.5.1
Primary DNS : 168.95.1.1
Secondary DNS :

<b>Model Name</b>	Display the model name of the router.
<b>Platform</b>	Display the hardware type that this device is built upon.
<b>Bootloader Version</b>	Display the bootloader version of the router.
<b>Firmware Version</b>	Display the firmware version of the router.
<b>Build Date/Time</b>	Display the date and time of the current firmware build.
<b>Hardware NAT Version</b>	Display the hardware acceleration NAT version.
<b>System Date</b>	Display current time and date for the system server.
<b>System Uptime</b>	Display the connection time for the system server.

**LAN-----**

<b>MAC Address</b>	Display the MAC address of the LAN Interface.
<b>IP Address</b>	Display the IP address of the LAN interface.
<b>IP Mask</b>	Display the subnet mask address of the LAN interface.

**WAN-----**

<b>MAC Address</b>	Display the MAC address of the WAN Interface.
<b>IP Address</b>	Display the IP address of the WAN interface.
<b>IP Mask</b>	Display the subnet mask address of the WAN interface.
<b>Default Gateway</b>	Display the gateway address of the WAN interface.
<b>Primary DNS</b>	Display the specified primary DNS setting.
<b>Secondary DNS</b>	Display the specified secondary DNS setting.

**Wireless LAN-----**

<b>MAC Address</b>	Display the MAC address of the wireless LAN.
<b>Device Type</b>	Display the device type used for wireless LAN.
<b>SSID</b>	Display the SSID of the router.
<b>Channel</b>	Display the channel that wireless LAN used.
<b>Manufacturer</b>	Display the manufacturer of the disk.
<b>Model</b>	Display the type of the disk.
<b>Size</b>	Display the storage size of the USB diskette.
<b>Status</b>	Display current status of the USB diskette.

### 4.11.2 System Password

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

[System Maintenance >> System Password](#)

**System Password**

New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

<b>Old Password</b>	Type in the old password. The factory default setting for password is blank.
<b>New Password</b>	Type in new password in this field.
<b>Confirm Password</b>	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.

### 4.11.3 User Password

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



## System Maintenance >> User Password

### User Password

New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

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

**New Password** Type in new password in this field.

**Confirm Password** Type in the new password again.

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

## 4.11.4 Configuration Backup

### Backup the Configuration

Follow the steps below to backup your configuration.

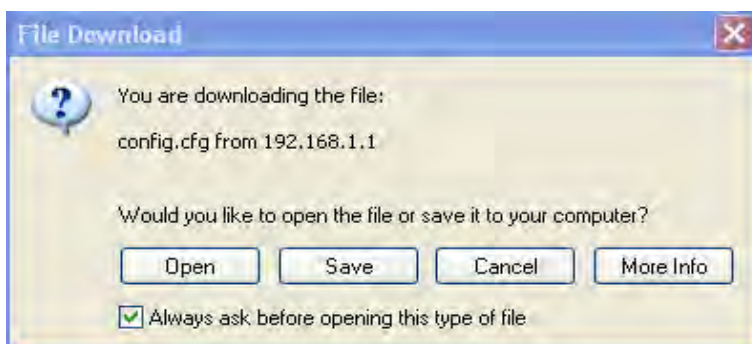
1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

### System Maintenance >> Configuration Backup

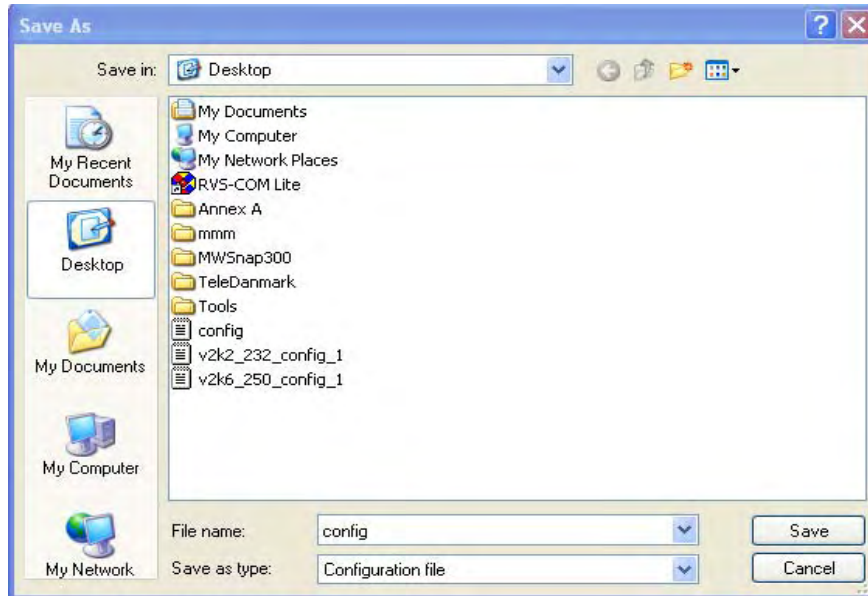
#### Configuration Backup / Restoration

<b>Backup</b>
Click Backup to download current running configurations as a file.
<input type="button" value="Backup"/>
<b>Restoration</b>
Select a configuration file.
<input type="text"/> <input type="button" value="Browse.."/>
Click Restore to upload the file.
<input type="button" value="Restore"/>

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



- In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



- 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

- Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

### System Maintenance >> Configuration Backup

**Configuration Backup / Restoration**

**Backup**

Click Backup to download current running configurations as a file.

---

**Restoration**

Select a configuration file.

Click Restore to upload the file.

- Click **Browse** button to choose the correct configuration file for uploading to the router.
- Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

### 4.11.5 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

Syslog Access Setup

Enable	<input type="checkbox"/>
Router Name	Vigor2130
Server IP Address	
Destination Port	514
Log Level	All

Mail Alert Setup

Enable	<input type="checkbox"/>
SMTP Server	
Mail To	
Mail From	
User Name	
Password	
Enable E-Mail Alert:	
<input checked="" type="checkbox"/> User Login	

OK Cancel

**Enable (Syslog Access...)**

Check “**Enable**” to activate function of syslog.

**Router Name**

Assign a name of this device.

**Server IP Address**

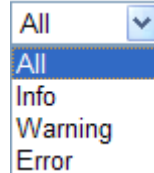
The IP address of the Syslog server.

**Destination Port**

Assign a port for the Syslog protocol.

**Log Level**

Choose the severity level for the system log entry.



**Enable (Mail Alert...)**

Check “**Enable**” to activate function of mail alert.

**SMTP Server**

The IP address of the SMTP server.

**Mail To**

Assign a mail address for sending mails out.

**Mail From**

Assign a path for receiving the mail from outside.

**User Name**

Type the user name for authentication.

**Password**

Type the password for authentication.

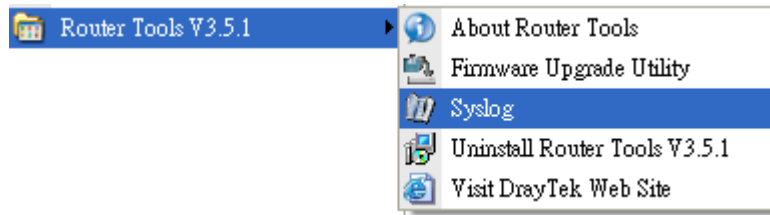
**Enable E-mail Alert**

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

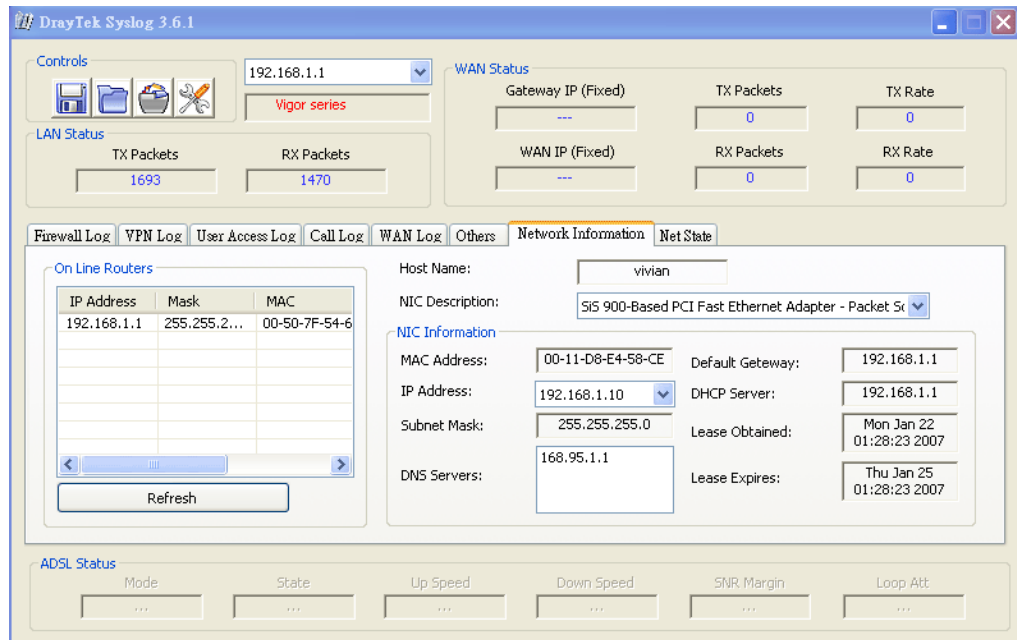
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

4. Just set your monitor PC’s IP address in the field of Server IP Address
5. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



- From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

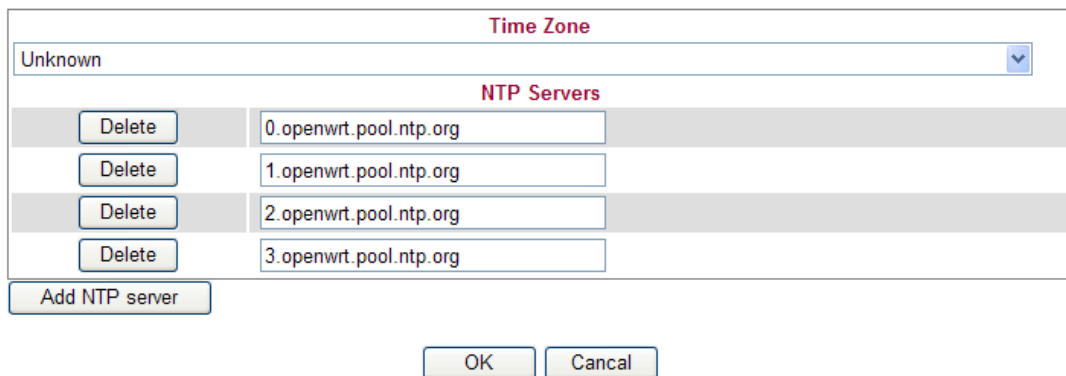


### 4.11.6 Time and Date

It allows you to specify where the time of the router should be inquired from.

**System Maintenance >> Time and Date**

#### Time Configuration



#### Time Zone

Select the time zone where the router is located.

#### Add NTP server

Click the button to add a new NTP server.

**Delete**

Click this button to remove an NTP server.

Click **OK** to save these settings.

### 4.11.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

#### System Maintenance >> Remote Management

##### Management Access Control

Enable HTTP	<input type="checkbox"/>	80	<b>SNMP Setup</b>	Enable SNMP	<input type="checkbox"/>	161
Enable HTTPS	<input type="checkbox"/>	443	Manager Host IP	<input type="text"/>		
Enable SSH	<input type="checkbox"/>	22				
Enable ICMP Ping	<input type="checkbox"/>					
Enable FTP	<input type="checkbox"/>					
<b>Access List</b>						
List		IP		Subnet Mask		
1		<input type="text"/>		255.255.255.255 / 32	▼	
2		<input type="text"/>		255.255.255.255 / 32	▼	
3		<input type="text"/>		255.255.255.255 / 32	▼	
<input type="button" value="OK"/>						

**Enable HTTP/HTTPS/SSH/ICMP Ping/FTP/SNMP** Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.

**Manager Host IP** – Type the IP address for the host to perform the remote management.

##### Access List

You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.

**List IP** - Indicate an IP address allowed to login to the router.

**Subnet Mask** - Represent a subnet mask allowed to login to the router.

### 4.11.8 Reboot System

The Web Configurator may be used to restart your router for using current configuration. Click **Reboot System** from **System Maintenance** to open the following page.

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.

### 4.11.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is [www.draytek.com](http://www.draytek.com) (or local DrayTek's web site) and FTP site is [ftp.draytek.com](ftp://ftp.draytek.com).

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

Firmware Update

Current Firmware Version: v1.1.0\_RC4

Select a firmware file.

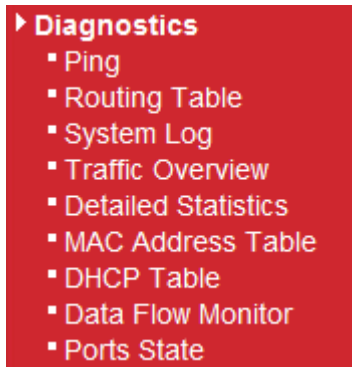
Click Upgrade to upload the file.

For the detailed information about firmware update, please go to Chapter 5.

## 4.12 Diagnostics

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

Below shows the menu items for Diagnostics.



### 4.12.1 Ping

Click **Diagnostics** and click **Ping** to open the web page. It is used to troubleshoot IP connection for your router.

**Diagnostics >> Ping**

**ICMP Ping**

IP Address	<input type="text" value="0.0.0.0"/>
Ping Size	<input type="text" value="64"/>

**IP Address**

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

**Ping Size**

Type in the payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

**Start**

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

## 4.12.2 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

<b>Destination</b>	Display the IP address for destination network or destination host.
<b>Gateway</b>	Display the gateway address or "*" if none set.
<b>Genmask</b>	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.
<b>Flags</b>	Different codes represent different routing status. <b>U</b> - route is up. <b>H</b> - target is a host <b>G</b> - use gateway <b>R</b> - reinstate route for dynamic routing <b>D</b> - dynamically installed by daemon or redirect <b>M</b> - modified from routing daemon or redirect <b>A</b> - installed by addrconf <b>C</b> - cache entry <b>!</b> - reject route
<b>Metric</b>	Display the distance to the target (usually counted in hops).
<b>Ref</b>	Display number of references to this route. (Not used in the Linux kernel.)
<b>Use</b>	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).
<b>Iface</b>	Display interface to which packets for this route will be sent.
<b>Refresh</b>	Click it to reload the page.



### 4.12.3 System Log

Click **Diagnostics** and click **System Log** to open the web page.

**Diagnostics >> System Log**

**System Log Information**

Auto-refresh  Reverse

Time	Level	Type	Message
May 7 07:58:15	info	user	: 2009-05-07 07:58:15: (server.c.1258) NOTE: a request for /config_ip.htm? ifname=wan timed out after writing 144 bytes. We waited 360 seconds. If this a problem increase server.max-write-idle
May 7 07:40:32	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:40:32	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:40:29	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:40:29	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:30:35	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:30:35	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:30:32	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:30:32	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:18:37	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-6a0e182ce8
May 7 07:18:37	info	daemon	dnsmasq[2538]: DHCPINFORM(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1
May 7 07:18:34	info	daemon	dnsmasq[2538]: DHCPACK(br-lan) 192.168.1.178 00:0e:a6:2a:d5:a1 user-

- Time** Display the time of the system log entry.
- Level** Display the severity level of the system log entry.
- Type** Display the type or subsystem of the system log entry.
- Message** Display a short description of the system log entry.
- Auto-refresh** Check it to enable auto-refresh function.
- Reverse** Check it to have newest log entries presented first.
- Refresh** Click it to reload the page.

### 4.12.4 Traffic Overview

This page offers an overview of general traffic statistics for all connecting ports.

**Diagnostics >> Traffic Overview**

**Port Statistics Overview**

Auto-refresh

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

<b>Port</b>	Display the interface that data transmission passing through.
<b>Packets</b>	Display the packet sizes for data transmission in receiving and sending.
<b>Bytes</b>	Display the number of received and transmitted bytes per port.
<b>Errors</b>	Display the number of the error occurred in data receiving and data sending.
<b>Drops</b>	Display the number of the data lost in receiving and sending.
<b>Filtered</b>	Display the number of received frames filtered by the forwarding process.
<b>Auto-refresh</b>	Check it to enable auto-refresh function.
<b>Refresh</b>	Click it to reload the page.
<b>Clear</b>	Click it to clear the counters for all ports.

### 4.12.5 Detailed Statistics

This page display detailed statistics for WAN/LAN interface.

[Diagnostics >> Detailed Statistics](#)

Detailed Port Statistics WAN

WAN  Auto-refresh

Receive Total		Transmit Total	
Rx Packets	38618	Tx Packets	16552
Rx Octets	15458804	Tx Octets	3133089
Rx Unicast	18389	Tx Unicast	16549
Rx Multicast	5687	Tx Multicast	0
Rx Broadcast	14542	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	5971	Tx 64 Bytes	9935
Rx 65-127 Bytes	17150	Tx 65-127 Bytes	2395
Rx 128-255 Bytes	3806	Tx 128-255 Bytes	164
Rx 256-511 Bytes	2698	Tx 256-511 Bytes	2385
Rx 512-1023 Bytes	1463	Tx 512-1023 Bytes	1257
Rx 1024-1526 Bytes	7530	Tx 1024-1526 Bytes	416
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	20334	Tx Low	1722
Rx Normal	3931	Tx Normal	0
Rx Medium	14353	Tx Medium	14830
Rx High	0	Tx High	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

**Rx Packets** Display the counting number of the packet received.

**Rx Octets** Display the total received bytes.

<b>Rx Unicast</b>	Display the counting number of the received unicast packet.
<b>Rx Broadcast</b>	Display the counting number of the received broadcast packet.
<b>Rx Pause</b>	Display the counting number of the received pause packet.
<b>RX 64 Bytes</b>	Display the number of 64-byte frames in good and bad packets received.
<b>RX 65-127 Bytes</b>	Display the number of 65 ~ 127-byte frames in good and bad packets received.
<b>RX 128-255 Bytes</b>	Display the number of 128 ~ 255-byte frames in good and bad packets received.
<b>RX 256-511 Bytes</b>	Display the number of 256 ~ 511-byte frames in good and bad packets received.
<b>RX 512-1023 Bytes</b>	Display the number of 512 ~ 1023-byte frames in good and bad packets received.
<b>RX 1024- 1526 Bytes</b>	Display the number of 1024-1522-byte frames in good and bad packets received.
<b>RX 1527 Bytes</b>	Display the number of 1527-byte frames in good and bad packets received.
<b>Rx Low</b>	Display the low queue counter of the packet received.
<b>Rx Normal</b>	Display the normal queue counter of the packet received.
<b>Rx Medium</b>	Display the medium queue counter of the packet received.
<b>Rx High</b>	Display the high queue counter of the packet received.
<b>Rx Drops</b>	Display the number of frames dropped due to the lack of receiving buffer.
<b>Rx CRC/Alignment</b>	Display the number of Alignment errors packets received.
<b>Rx Undersize</b>	Display the number of short frames (<64 Bytes) with valid CRC.
<b>Rx Oversize</b>	Display the number of long frames (according to max_length register) with valid CRC.
<b>Rx Fragments</b>	Display the number of short frames (< 64 bytes) with invalid CRC.
<b>Rx Jabber</b>	Display the number of long frames (according to max_length register) with invalid CRC.
<b>Rx Filtered</b>	Display the filtered number of the packet received.
<b>Tx Packets</b>	Display the counting number of the packet transmitted.
<b>Tx Octets</b>	Display the total transmitted bytes.
<b>Tx Unicast</b>	Display the show the counting number of the transmitted unicast packet.
<b>Tx Multicast</b>	Display the show the counting number of the transmitted multicast packet.
<b>Tx Broadcast</b>	Display the counting number of the transmitted broadcast packet.

<b>Tx Pause</b>	Show the counting number of the transmitted pause packet.
<b>Tx 64 Bytes</b>	Display the number of 64-byte frames in good and bad packets transmitted.
<b>Tx 65-127 Bytes</b>	Display the number of 65 ~ 127-byte frames in good and bad packets transmitted.
<b>Tx 128-255 Bytes</b>	Display the number of 128 ~ 255-byte frames in good and bad packets transmitted.
<b>Tx 256-511 Bytes</b>	Display the number of 256 ~ 511-byte frames in good and bad packets transmitted.
<b>Tx 512-1023 Bytes</b>	Display the number of 512 ~ 1023-byte frames in good and bad packets transmitted.
<b>Tx 1024- 1526 Bytes</b>	Display the number of 1024 ~ 1522-byt frames in good and bad packets transmitted.
<b>Tx 1527 Bytes:</b>	Display the number of 1527-byte frames in good and bad packets transmitted.
<b>Tx Low</b>	Display the low queue counter of the packet transmitted.
<b>Tx Normal</b>	Display the normal queue counter of the packet transmitted.
<b>Tx Medium</b>	Display the medium queue counter of the packet received.
<b>Tx High</b>	Display the high queue counter of the packet received.
<b>Tx Drops</b>	Display the number of frames dropped due to excessive collision, late collision, or frame aging.
<b>Tx lat/Exc.Coll.</b>	Display the number of Frames late collision or excessive collision Error, which switch transmitted
<b>Auto-refresh</b>	Check it to enable auto-refresh function.
<b>Refresh</b>	Click it to reload the page.
<b>Clear</b>	Click it to clear the counters for all ports.

#### 4.12.6 MAC Address Table

The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The **Start from MAC address** and **VLAN** input fields allow the user to select the starting point in the MAC Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The button >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table, use the << button to start over.

## Diagnostics >> MAC Address Table

### MAC Address Table

Auto-refresh  Refresh Clear |<< >>

Start from VLAN  and MAC address  with  entries per page.

Type	VLAN	MAC Address	CPU	WAN	Port Members			
					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						

<b>Type</b>	Indicate whether the entry is a static or dynamic entry.
<b>VLAN</b>	Display the VLAN ID of that entry.
<b>MAC Address</b>	Display the MAC address of that entry.
<b>Port Members</b>	Display the port of that entry.
<b>Auto-refresh</b>	Check it to enable auto-refresh function.
<b>Refresh</b>	Click it to reload the page.
<b>Clear</b>	Click it to clear the whole table.

## 4.12.7 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

[Diagnostics >> DHCP Table](#)

DHCP Server Status

Auto-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

<b>Computer Name</b>	It displays the name of the computer accepted the assigned IP address by this router.
<b>IP Address</b>	It displays the IP address assigned by this router for specified PC.
<b>MAC Address</b>	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
<b>Expire Time</b>	It displays the leased time of the specified PC.
<b>Auto-refresh</b>	Check it to enable auto-refresh function.
<b>Refresh</b>	Click it to reload the page.

## 4.12.8 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.

[Diagnostics >> Data Flow Monitor](#)

Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Session	Action
1	192.168.1.10	HNAT	HNAT	1	<a href="#">Block</a>
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Total				3	

- Note:**
1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
  2. The IP blocked by the router will be shown in red.

**Auto-refresh**

Check it to enable auto-refresh function.

**Refresh**

Click this link to refresh this page manually.

**Index**

Display the number of the data flow.

**IP Address**

Display the IP address of the monitored device.

**TX rate (kbps)**

Display the transmission speed of the monitored device. If "HNAT" is shown, that means the transmission is through Hardware NAT can't be computed.

**RX rate (kbps)**

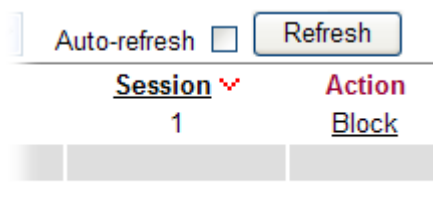
Display the receiving speed of the monitored device. If "HNAT" is shown, that means the transmission is through Hardware NAT can't be computed.

**Sessions**

Display the session number that you specified in Limit Session web page.

**Action**

**Block** - can prevent specified PC accessing into Internet within 5 minutes.



**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

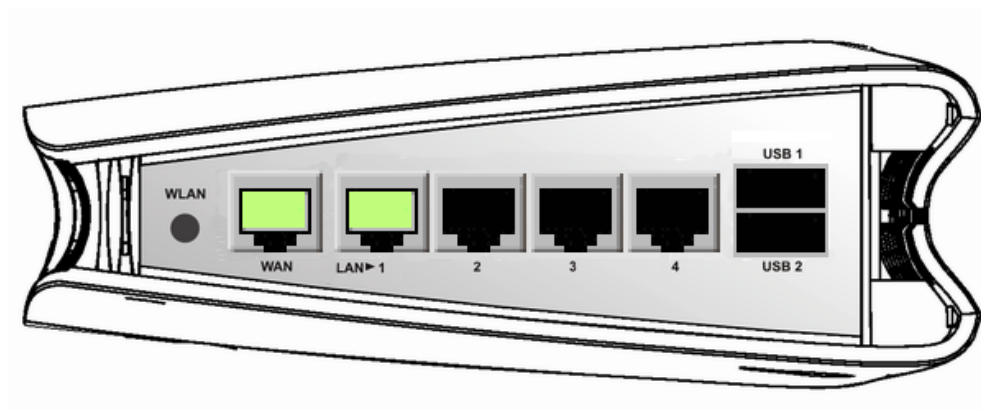
Session	Action
5	Unblock

### 4.12.9 Ports State

Click **Diagnostics** and click **Ports State** to open the list page. There are for LAN ports and one WAN port in your router. Through this page, you can know which port is using and you can get the detailed statistics for each port by moving and clicking the mouse on the connected one.

#### Port State Overview

Auto-refresh  Refresh



**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.



# 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.

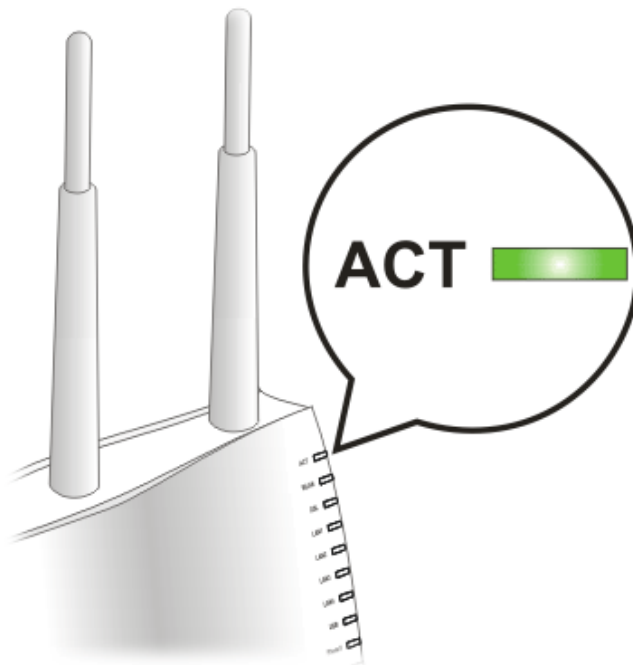
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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 still failed, please do the steps listed below to make sure the network connection settings is OK.

### For Windows

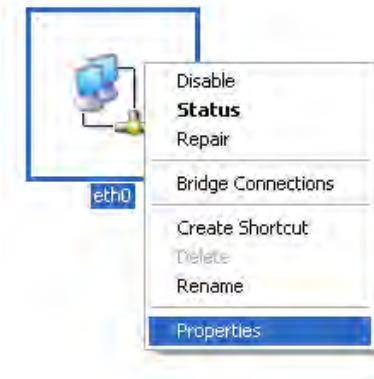


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in [www.draytek.com](http://www.draytek.com).

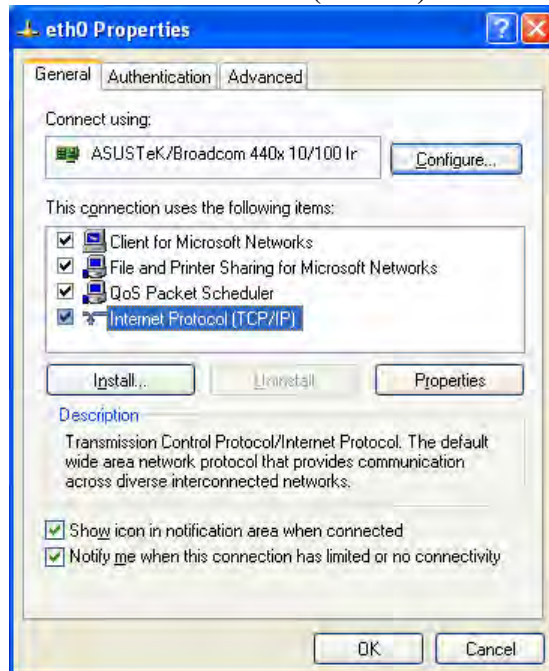
1. Go to **Control Panel** and then double-click on **Network Connections**.



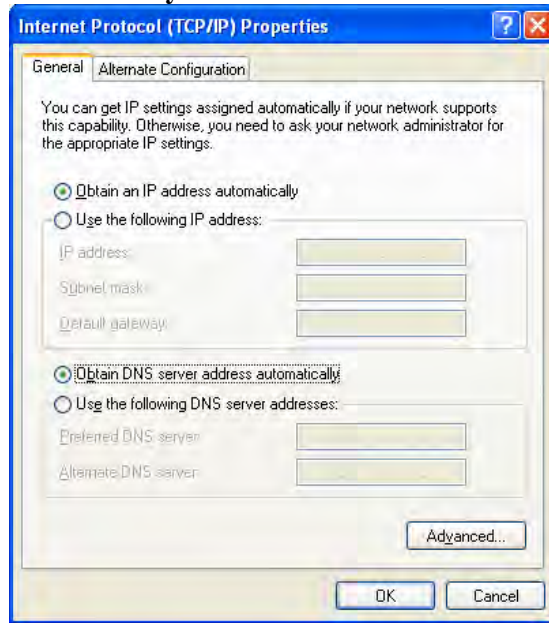
2. Right-click on **Local Area Connection** and click on **Properties**.



3. Select **Internet Protocol (TCP/IP)** and then click **Properties**.

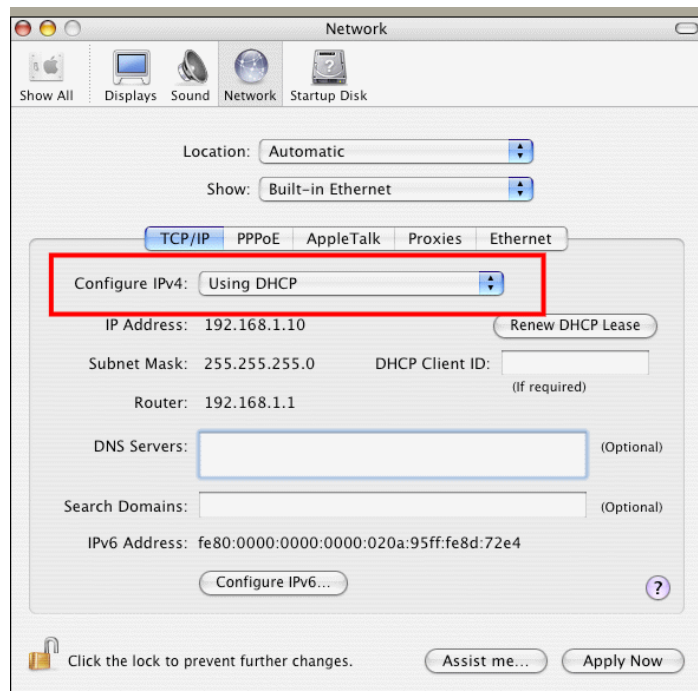


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



### For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



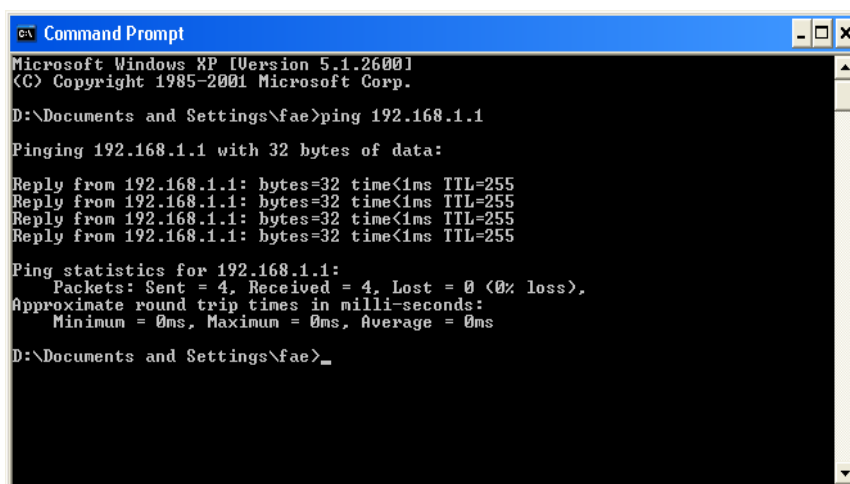
## 5.3 Pinging the Router from Your Computer

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 4.2)

Please follow the steps below to ping the router correctly.

### For Windows

1. Open the **Command Prompt** window (from **Start menu**> **Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



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

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of “**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

### For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “**64 bytes from 192.168.1.1: icmp\_seq=0 ttl=255 time=xxxx ms**” will appear.

```

Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

```

## 5.4 Checking If the ISP Settings are OK or Not

Open **WAN>>Internet Access** page and then check whether the ISP settings are set correctly. Use the Connection Type drop down list to choose Static IP/DHCP/PPPoE/PPTP/L2TP for reviewing the settings that you configured previously.



### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	DHCP	
<ul style="list-style-type: none"> <li>Static IP</li> <li style="background-color: #0070C0; color: white;">DHCP</li> <li>PPPoE</li> <li>PPTP</li> <li>L2TP</li> <li>3G USB Modem</li> </ul>		
<b>DHCP Settings</b>		
Router Name		( The same as syslog's router name )
<b>Clone MAC Address</b>		
Enable	<input type="checkbox"/>	

## For Static Users

1. Choose **Static IP** as the connection type.

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	Static IP
-----------------	-----------

#### Static IP Settings

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

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK Cancel

2. Check if **IP Address**, **IP Mask** and **IP Router** are set correctly (must identify with the values from your ISP).

## For PPPoE Users

1. Choose **PPPoE** as the connection type.

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	PPPoE
-----------------	-------

#### PPPoE Settings

Username	2130
Password	••••
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	
Default Route	<input type="checkbox"/>

#### Clone MAC Address

Enable	<input type="checkbox"/>
--------	--------------------------

OK Cancel

2. Check if **Username** and **Password** are set correctly (must identify with the values from your ISP).

## For PPTP/L2TP Users

1. Choose **PPTP/L2TP** as the connection type.

### WAN >> Internet Access

#### WAN IP Configuration

Connection Type	PPTP
<b>PPTP Settings</b>	
Username	2130
Password	••••
Server Address	0.0.0.0
WAN IP Network Settings	Static IP
IP Address	192.168.1.5
Subnet Mask	255.255.0.0
Redial Policy	Connect on Demand
Idle Time out	
MTU Size	
Default Route	<input type="checkbox"/>
<b>Clone MAC Address</b>	
Enable	<input type="checkbox"/>

2. Check if **Username, Password, IP address, Subnet Mask** are entered with correct values that you **get from your ISP**.

## 5.5 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 lose 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.

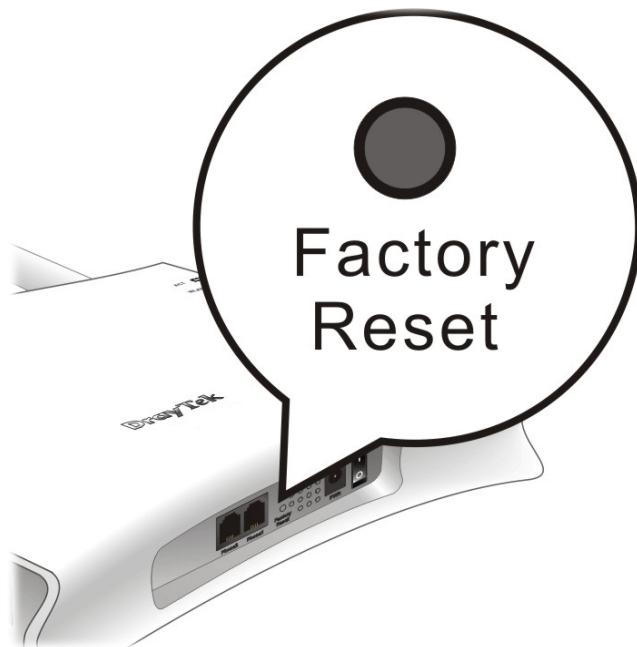
### Reboot System

**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.

## 5.6 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](mailto:support@draytek.com).