DrayTek

Vigor 2100 Series Broadband Router User's Guide

Version: 2.0

Date: 2007/03/30

Please visit www.draytek.com to get the newly updated manual at any time.

Copyright Information

Copyright Declarations

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Computer Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- Do not stack the routers.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor router via http://www.draytek.com. Alternatively, fill in the registration card and mail it to the address found on the reverse side of the card.

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:	Vigor2100 series Routers

DrayTek Corp. declares that Vigor2100 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 89/336/EEC 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 73/23/EEC by complying with the requirements set forth in EN60950.

The ***Vigor2100V/2100VG/2100G*** is designed for the WLAN 2.4GHz network throughput EC region, Switzerland, and the restrictions of France.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

Table of Contents

1 Preface

The Vigor2100 Series router includes Vigor2100G ,Vigor2100V and Vigor2100VG models.

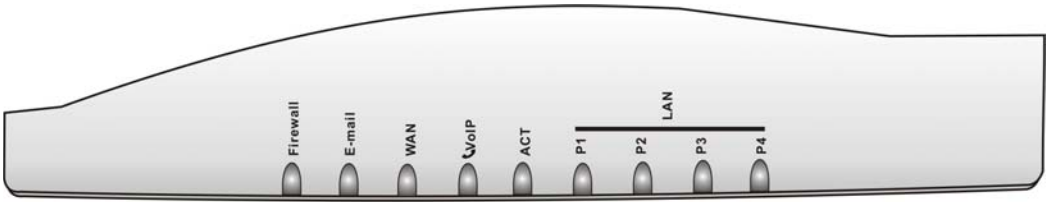
To secure your network, the Vigor2100 series provides an advanced firewall with advanced features, such as NAT with multi VPN pass-through, Stateful Packet Inspection (SPI) to offer network reliability by detecting and prohibiting malicious penetrating packets or DoS attacks, user-configurable web filtering for parental control against network abuse etc.

For G series model, it is embedded with an 802.11g compliant wireless module which provides wireless LAN access with data rate as much as (up to 54Mbps for Vigor2100G/VG).

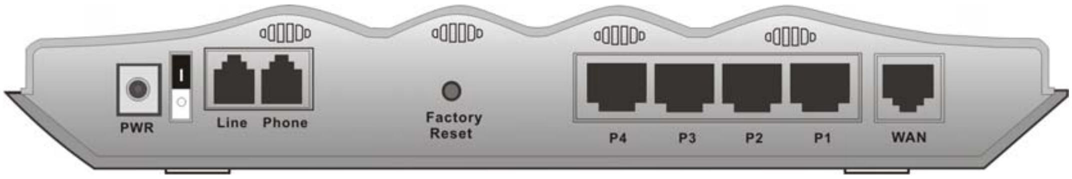
For V series model, with VoIP phone ports, it provides an Internet access solution for your LAN via shared web surfing and countless value-added features, such as Firewall, Security and VoIP. These are all in a reliable one-box solution. The V series model has a “Line” port on the rear panel for connecting to a PSTN (regular analogue) line. The Loop Through option can be used to set an alternate telephone number for your contact on the PSTN, which the Vigor2100V series will dial instead of the SIP account if you lose ADSL access or power to the Vigor2100V series. Hence, the PSTN line can act as a lifeline (backup mechanism) for VoIP calls. The lifeline mechanism is activated automatically but can also be manually configured.

1.1 LED Indicators and Connectors

1.1.1 Front and Rear View for Vigor2100V

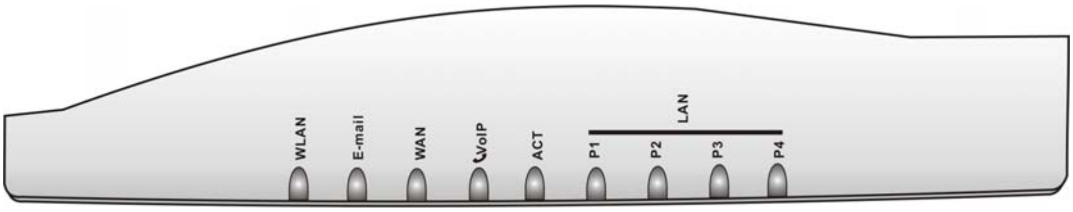


LED	Status	Explanation
Firewall	on	The firewall function is active.
	blinking	When encountering DoS attacks.
E-mail	blinking	When detecting one or more user-defined E-mails existing on mail server.
WAN	orange	A normal 10Mbps connection is through its corresponding port.
	green	A normal 100Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.
VoIP	green	Solid light when the handset of phone is picked up (off hooked).
		Blinking per 2 seconds when phone is connected through VoIP.
	orange	Solid light when phone call is via PSTN life line.
ACT (Activity)	on	The router is powered on and running properly.
LAN(P1 - P4)	orange	A normal 10Mbps connection is through its corresponding port.
	green	A normal 100Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.

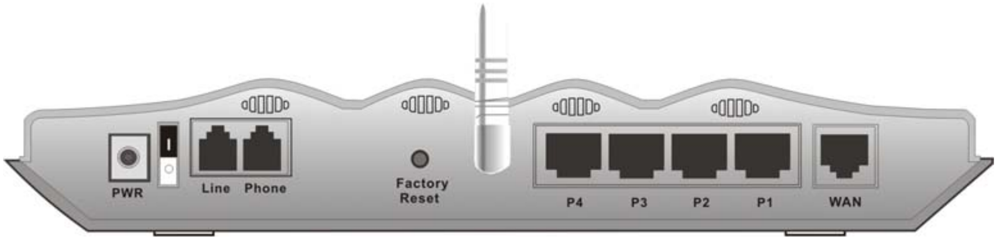


Interface	Description
PWR	Connect the included power adapter to the power outlet.
Line	Connect to the analog phone line for PSTN life line.
Phone	Connect to the analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1 - P4	Connect to the local network devices.
WAN	Connect the Cable/ADSL modem to access the Internet.

1.1.2 Front and Rear View for Vigor2100VG

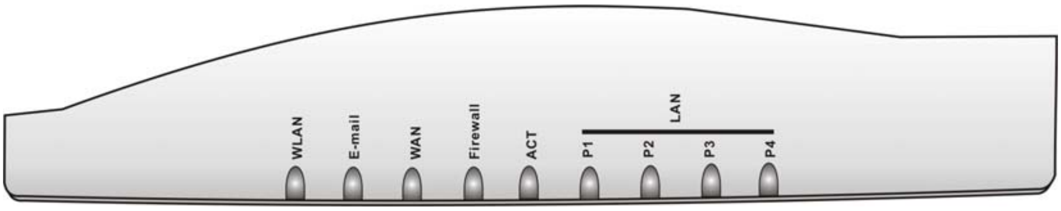


LED	Status	Explanation
WLAN	on	The Wireless LAN function is active.
	blinking	Data packets are transmitted over Wireless LAN.
E-mail	blinking	When detecting one or more user-defined e-mails existing on mail server.
WAN	orange	A normal 10Mbps connection is through its corresponding port.
	green	A normal 100Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.
VoIP	green	Solid light when the handset of phone is picked up (off hooked).
		Blinking per 2 seconds when phone is connected through VoIP.
	orange	Solid light when phone call is via PSTN life line.
ACT (Activity)	on	The router is powered on and running properly.
LAN(P1 - P4)	orange	A normal 10Mbps connection is through its corresponding port.
	green	A normal 100Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.

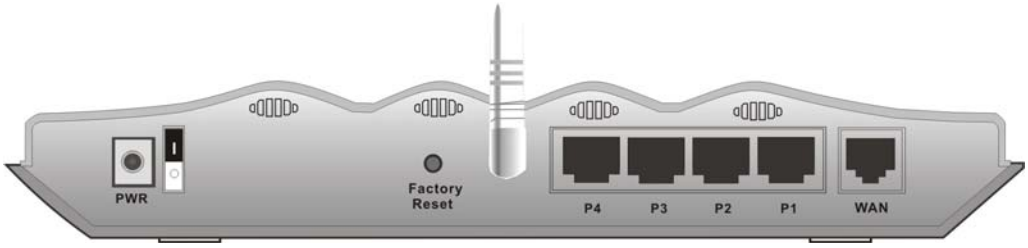


Interface	Description
PWR	Connect the included power adapter to the power outlet.
Line	Connect to the analog phone line for PSTN life line.
Phone	Connect to the analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1 - P4	Connect to the local network devices.
WAN	Connect the Cable/ADSL modem to access the Internet.

1.1.3 Front and Rear View for Vigor2100G



LED	Status	Explanation
WLAN	on	The Wireless LAN function is active.
	blinking	Data packets are transmitted over Wireless LAN.
E-mail	blinking	When detecting one or more user-defined e-mails existing on mail server.
WAN	orange	A normal 10Mbps connection is through its corresponding port.
	green	A normal 100Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.
Firewall	on	The firewall function is active.
	blinking	When encountering DoS attacks.
ACT (Activity)	on	The router is powered on and running properly.
LAN(P1 - P4)	orange	A normal 10Mbps connection is through its corresponding port.
	green	A normal 100Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.



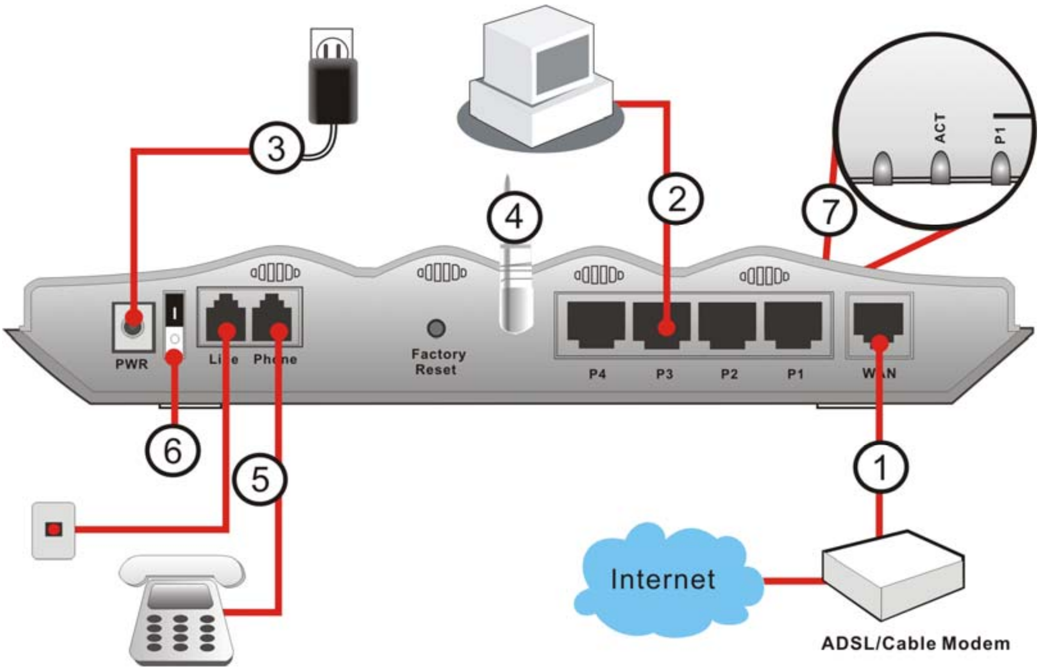
Interface	Description
PWR	Connect the included power adapter to the power outlet.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1 - P4	Connect to the local network devices.
WAN	Connect the Cable/ADSL modem to access the Internet.

1.2 Hardware Installation

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

1. Connect this device to a router with an Ethernet cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Connect detachable antennas to the router for Vigor2100 series (G model).
5. Connect Phone port to a conventional analog telephone, either corded or wireless (DECT), with a RJ-11 cable (V model) and connect Line port to land line jack with a RJ-11 cable (V model)
6. Power on the router.
7. 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: The Phone port can be connected to an analog phone only. Do not connect the Phone port to the telephone wall jack. This connection might damage your router.

This page is left blank.

2 Configuring Basic Settings

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

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

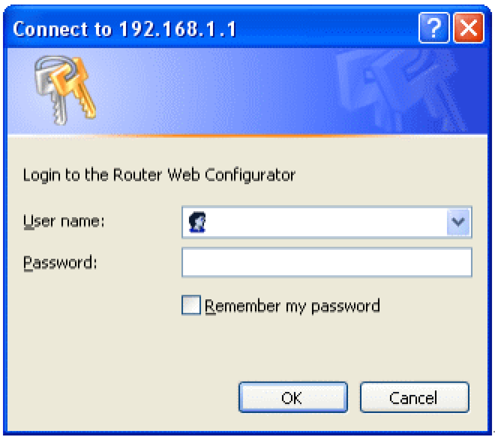
2.1 Changing Password

To change the password for this device, you have to access into the web browse with default password first.

1. Make sure your computer 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 this guide.

2. 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. Please type default values (both username and password are Null) on the window for the first time accessing and click **OK** for next screen.



Connect to 192.168.1.1

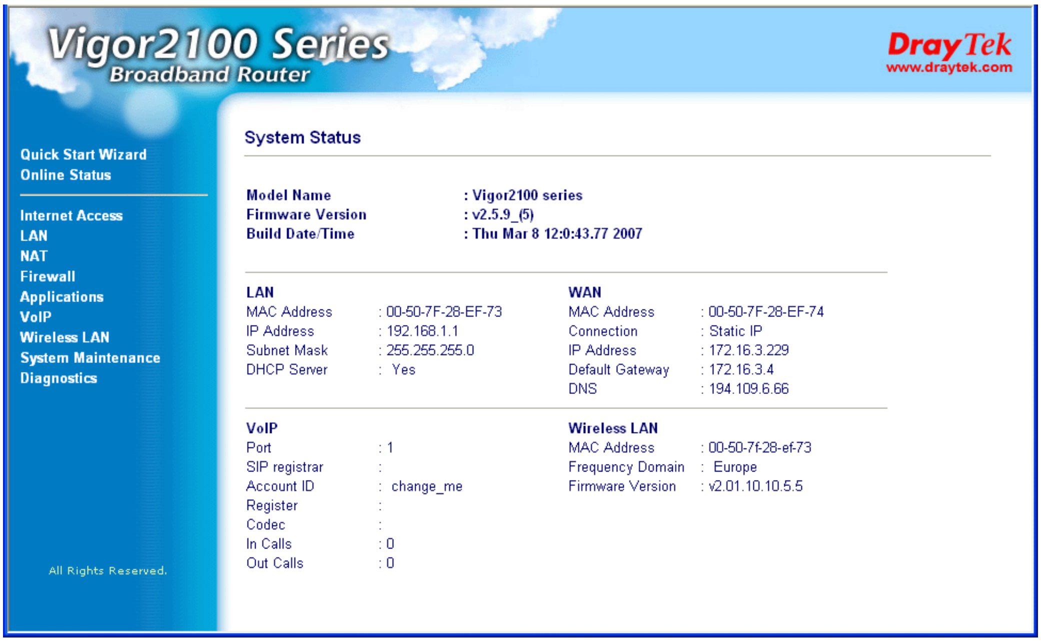
Login to the Router Web Configurator

User name:

Password:

□ Remember my password

3. Now, the **Main Screen** will pop up. The main screen will be changed slightly according to the model you have.



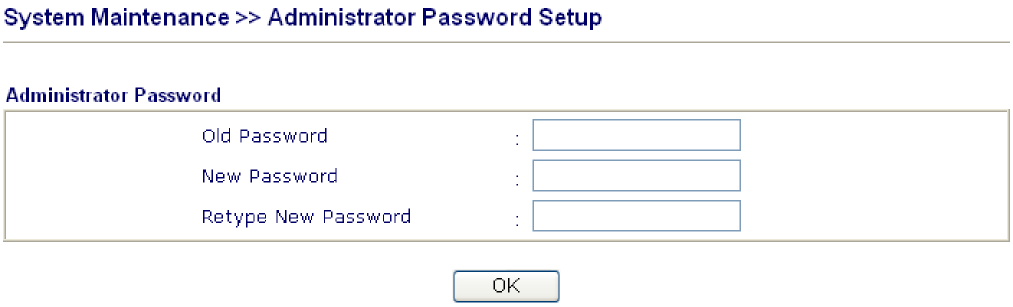
System Status

Model Name	: Vigor2100 series
Firmware Version	: v2.5.9_(5)
Build Date/Time	: Thu Mar 8 12:0:43.77 2007

LAN		WAN	
MAC Address	: 00-50-7F-28-EF-73	MAC Address	: 00-50-7F-28-EF-74
IP Address	: 192.168.1.1	Connection	: Static IP
Subnet Mask	: 255.255.255.0	IP Address	: 172.16.3.229
DHCP Server	: Yes	Default Gateway	: 172.16.3.4
		DNS	: 194.109.6.66

VoIP		Wireless LAN	
Port	: 1	MAC Address	: 00-50-7f-28-ef-73
SIP registrar	:	Frequency Domain	: Europe
Account ID	: change_me	Firmware Version	: v2.01.10.10.5.5
Register	:		
Codec	:		
In Calls	: 0		
Out Calls	: 0		

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



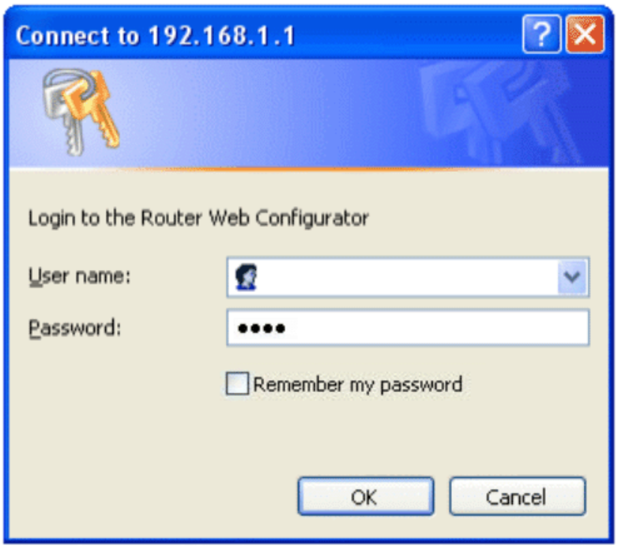
System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	:	
New Password	:	
Retype New Password	:	

5. Enter the login password (the default is blank) on the field of **Old Password**. Type a new one in the field of **New Password** and retype it on the field of **Retype New Password**. Then click **OK** to continue.

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



Connect to 192.168.1.1

Login to the Router Web Configurator

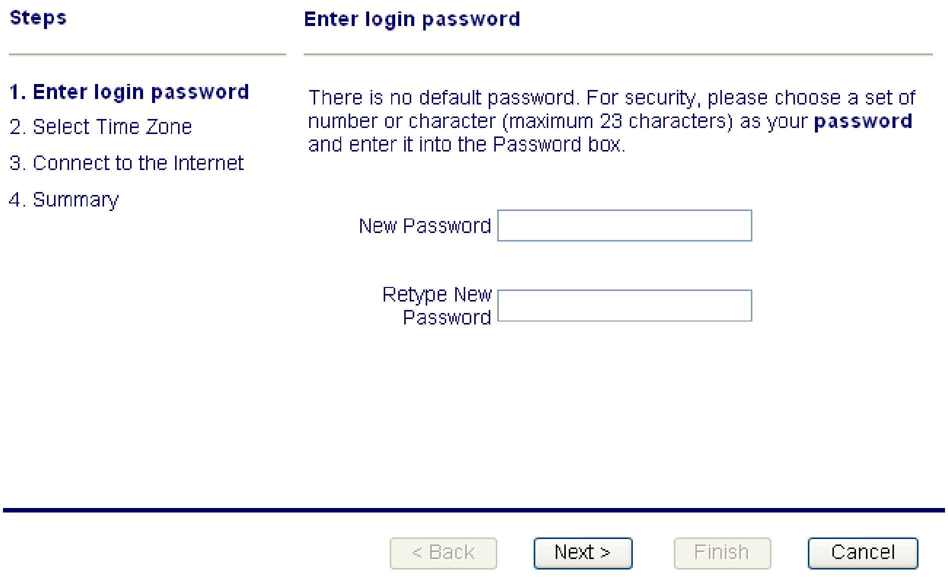
User name:

Password: ●●●●

□ Remember my password

2.2 Quick Start Wizard

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



Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. Summary

Enter login password

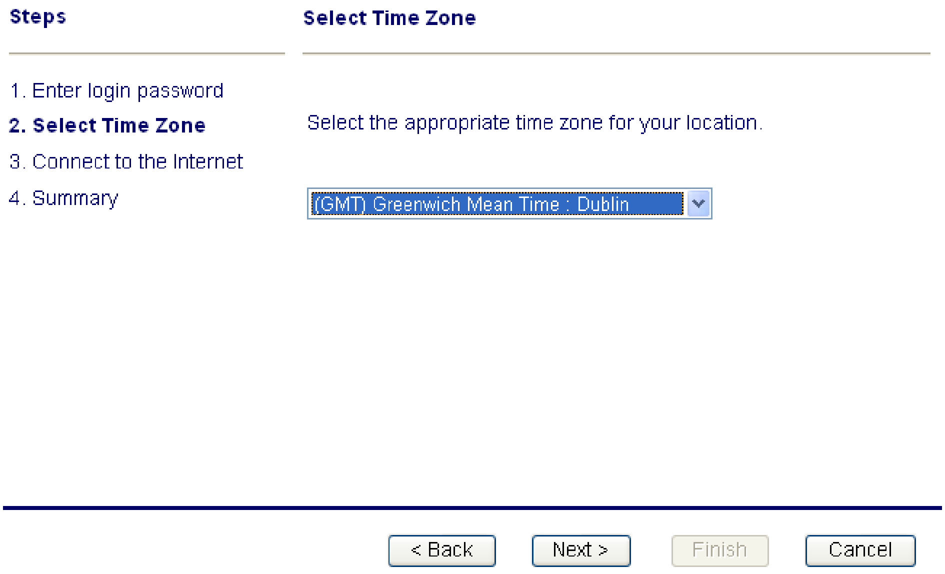
There is no default password. For security, please choose a set of number or character (maximum 23 characters) as your **password** and enter it into the Password box.

New Password

Retype New Password

2.2.1 Selecting Time Zone

Select the appropriate time zone for your location. Then click **Next** to continue.



Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. Summary

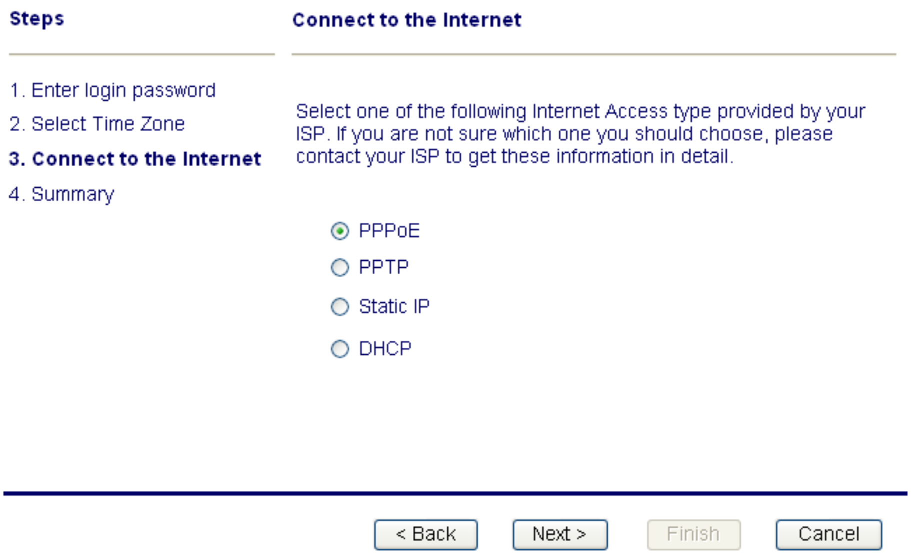
Select Time Zone

Select the appropriate time zone for your location.

(GMT) Greenwich Mean Time : Dublin

2.2.2 Selecting Internet Access Type

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPPTP, Static IP or DHCP**. The router supports the Ethernet WAN interface for Internet access.



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
4. Summary

Connect to the Internet

Select one of the following Internet Access type provided by your ISP. If you are not sure which one you should choose, please contact your ISP to get these information in detail.

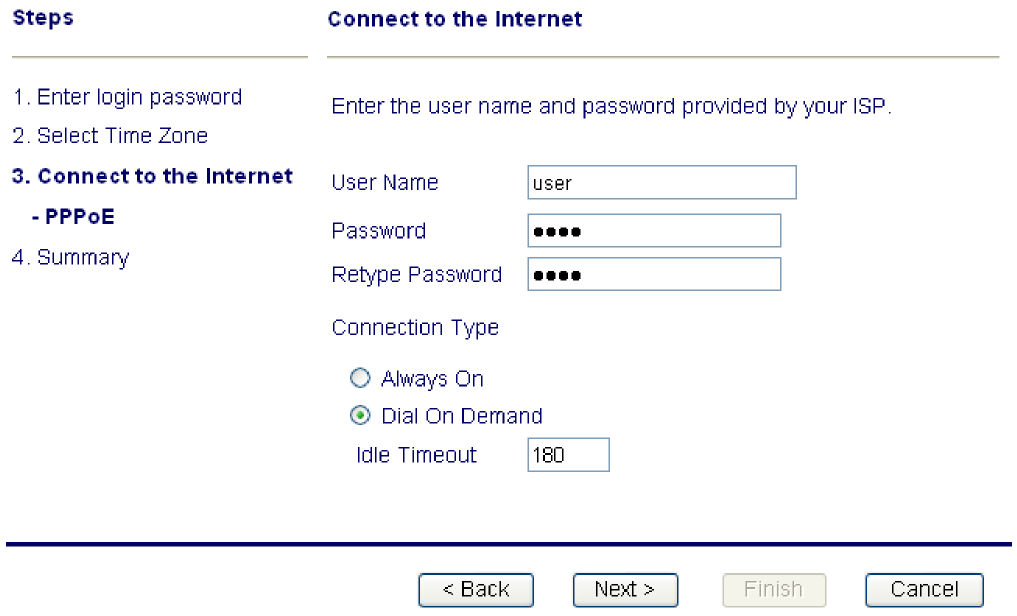
● PPPoE
○ PPTP
○ Static IP
○ DHCP

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:



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
   - PPPoE
4. Summary

Connect to the Internet

Enter the user name and password provided by your ISP.

User Name: user
Password: ●●●●
Retype Password: ●●●●

Connection Type

○ Always On
● Dial On Demand

Idle Timeout: 180

ISP Name Assign a specific name for ISP requirement.

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

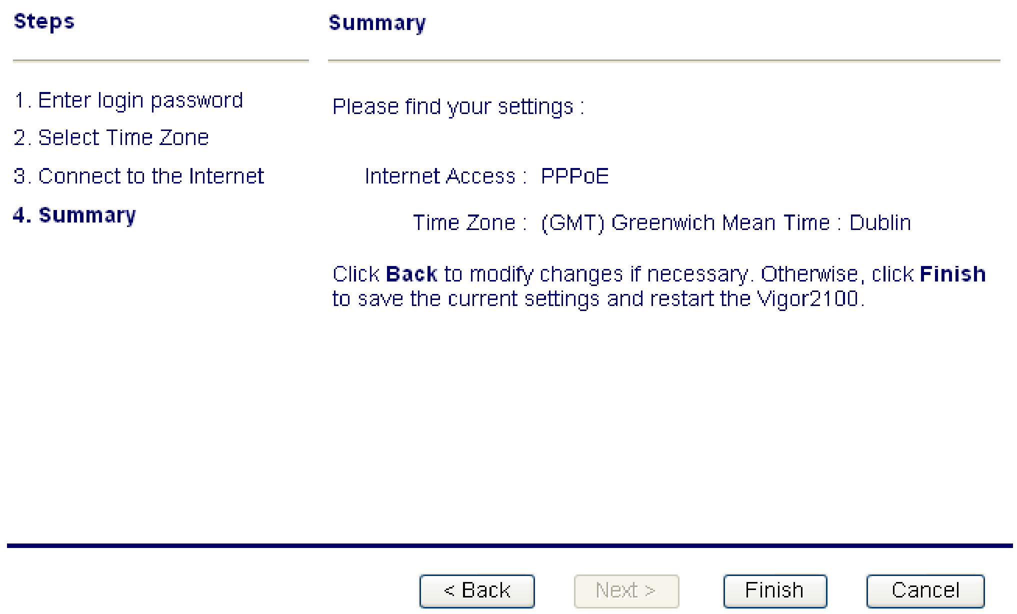
Password Assign a valid password provided by the ISP.

Retype Password Retype the password.

Always On Check this box to allow the router connecting to Internet forever.

Dial On Demand **Idle Timeout -** Type in the value (unit is second) as the idle timeout of the connection. When the time is expired, the internet connection will be dropped immediately.

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



Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. **Summary**

Summary

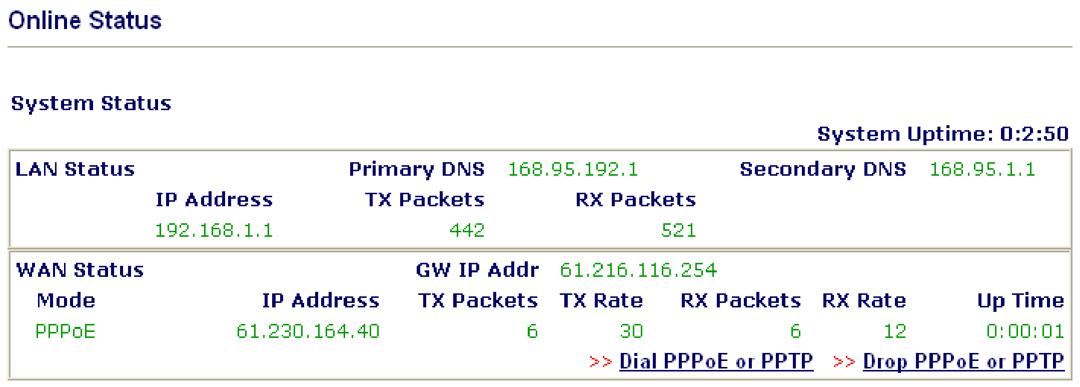
Please find your settings :

Internet Access : PPPoE

Time Zone : (GMT) Greenwich Mean Time : Dublin

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2100.

Click **Finish.** The online status of this protocol will be shown as below.



Online Status

System Status

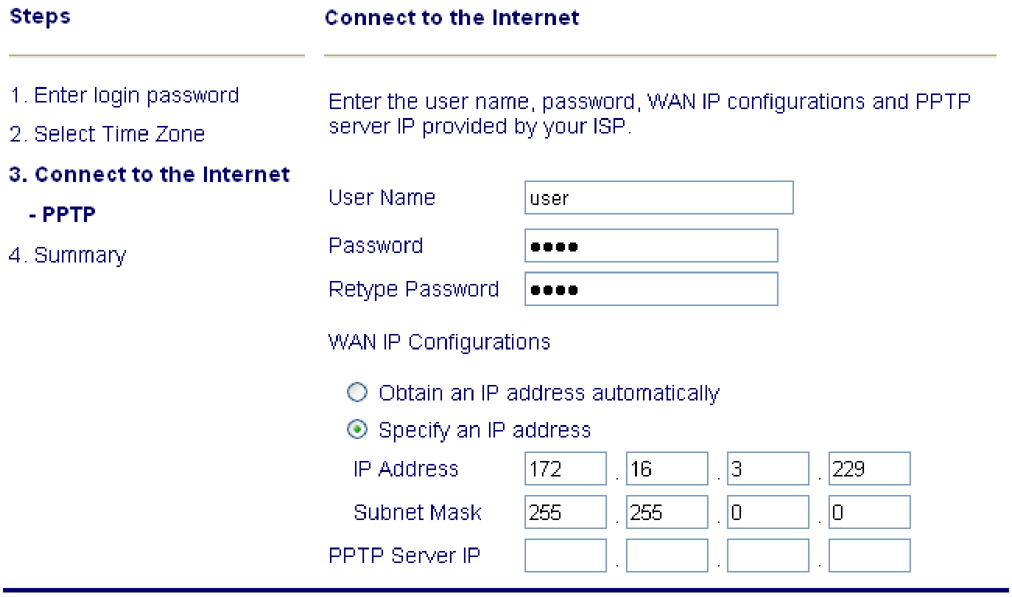
System Uptime: 0:2:50

LAN Status		Primary DNS	168.95.192.1	Secondary DNS	168.95.1.1
	IP Address	TX Packets	RX Packets		
	192.168.1.1	442	521		

WAN Status		GW IP Addr	61.216.116.254			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.164.40	6	30	6	12	0:00:01

PPTP

For PPTP connection, please click **PPTP** as the protocol.



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
   - PPTP
4. Summary

Connect to the Internet

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

User Name: user

Password: ●●●●

Retype Password: ●●●●

WAN IP Configurations

○ Obtain an IP address automatically

● Specify an IP address

IP Address: 172 . 16 . 3 . 229

Subnet Mask: 255 . 255 . 0 . 0

PPTP Server IP: . . .

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

Password Assign a valid password provided by the ISP.

Retype Password Retype the password.

Obtain an IP address automatically Click this selection to get the IP address from the router automatically.

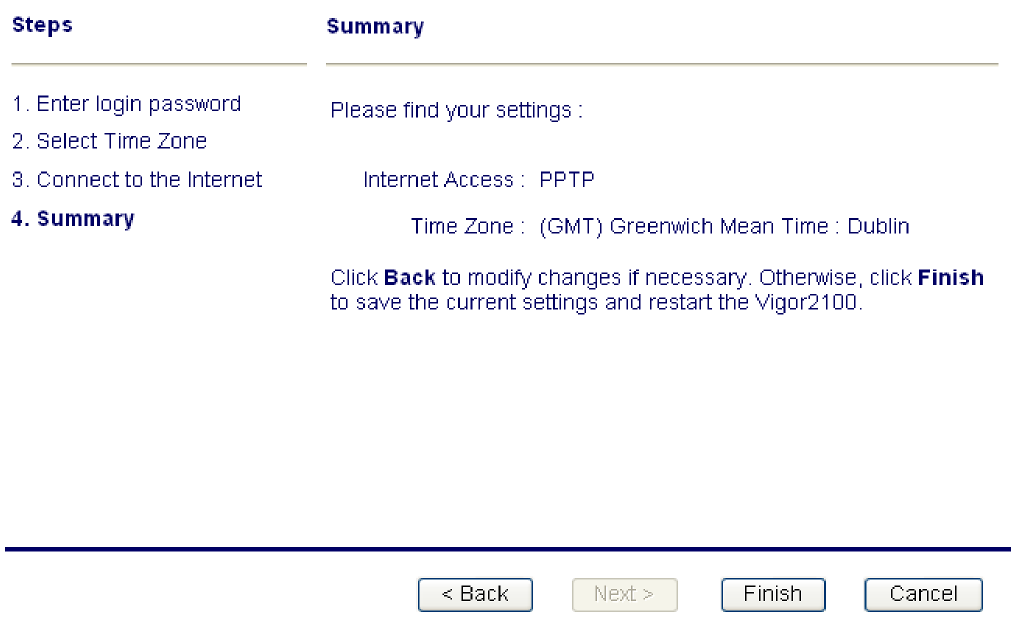
Specify an IP address Click this selection to specify an IP address and subnet mask manually.

IP Address Type a specific IP address for PPTP connection mode that obtained from ISP.

Subnet Mask Type the subnet mask.

PPTP Server IP Specify the IP address of the PPTP Server.

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



Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. **Summary**

Summary

Please find your settings :

Internet Access : PPTP

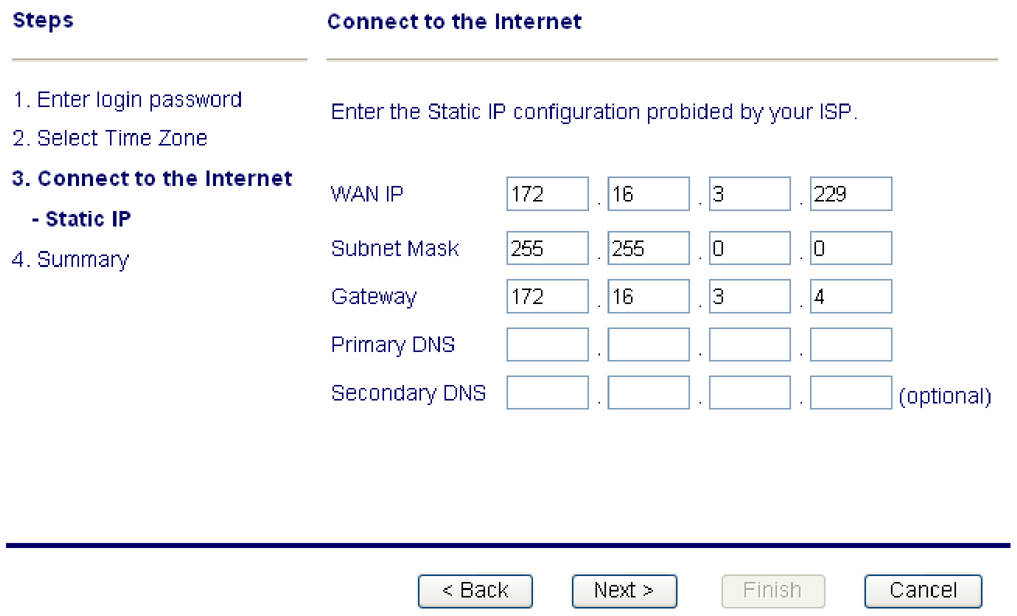
Time Zone : (GMT) Greenwich Mean Time : Dublin

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2100.

Click **Finish.**

Static IP

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



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
   - **Static IP**
4. Summary

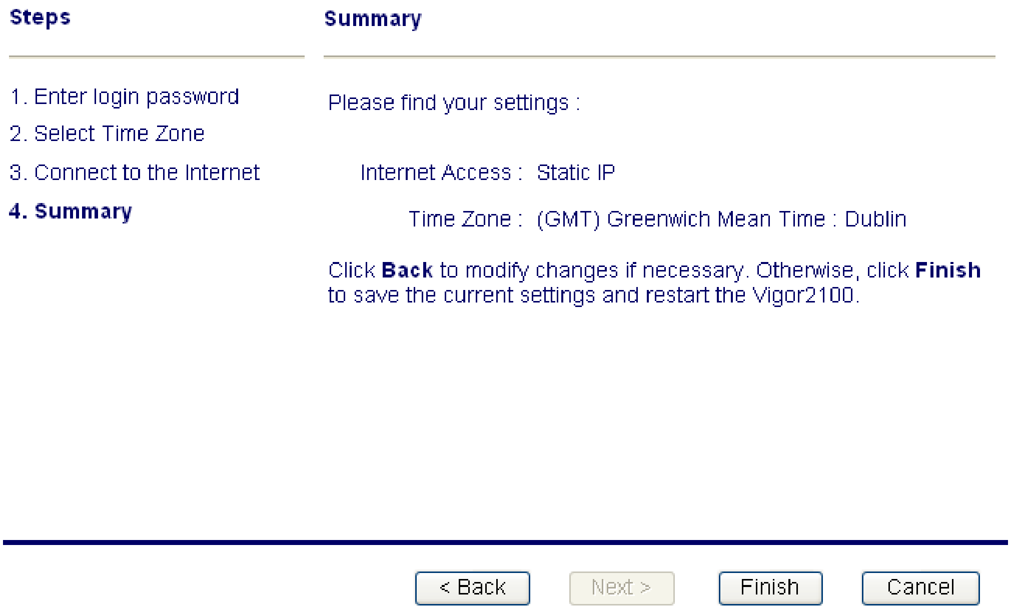
Connect to the Internet

Enter the Static IP configuration probided by your ISP.

WAN IP	172	16	3	229	
Subnet Mask	255	255	0	0	
Gateway	172	16	3	4	
Primary DNS					
Secondary DNS					(optional)

WAN IP	Type the WAN IP address that obtained from ISP.
Subnet Mask	Type the subnet mask obtained from ISP.
Gateway	Type the gateway address obtained from ISP.
Primary DNS	Type the IP address as the primary DNS obtained from ISP.
Second DNS	Type the IP address as the secondary DNS.

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



Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. **Summary**

Summary

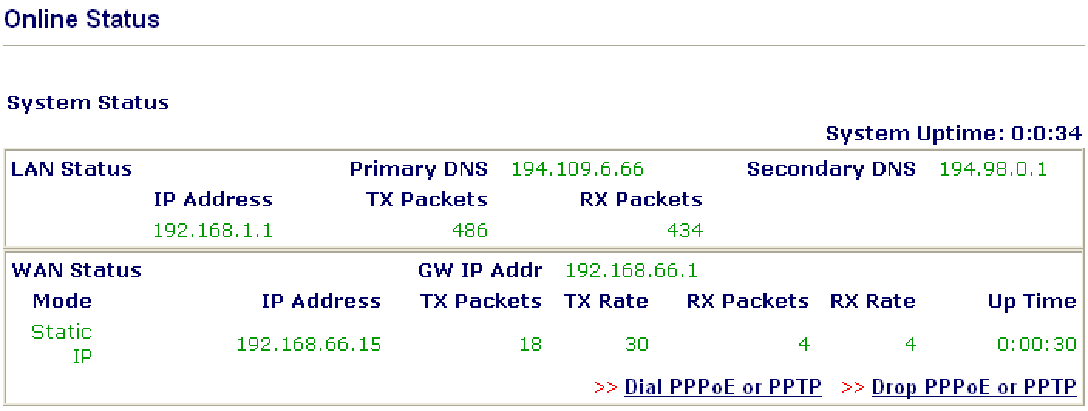
Please find your settings :

Internet Access : Static IP

Time Zone : (GMT) Greenwich Mean Time : Dublin

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2100.

Click **Finish.** The online status of this protocol will be shown as below.



Online Status

System Status

System Uptime: 0:0:34

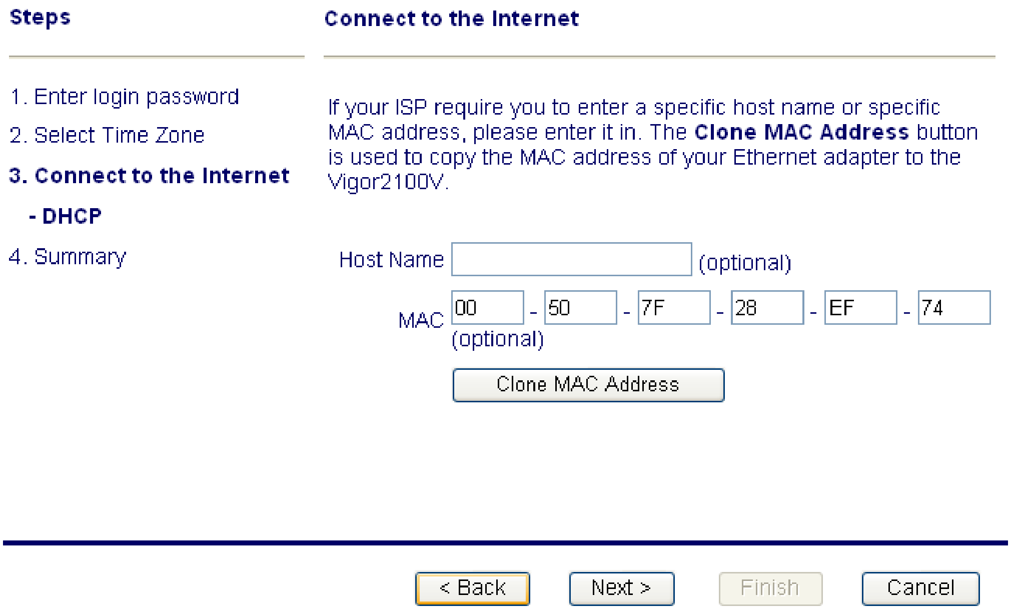
LAN Status		**Primary DNS**	194.109.6.66	**Secondary DNS**	194.98.0.1
	IP Address	**TX Packets**	**RX Packets**		
	192.168.1.1	486	434		

WAN Status		**GW IP Addr**	192.168.66.1			
Mode	**IP Address**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**	**Up Time**
Static IP	192.168.66.15	18	30	4	4	0:00:30

>> Dial PPPoE or PPTP >> Drop PPPoE or PPTP

DHCP

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



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
   - **- DHCP**
4. Summary

Connect to the Internet

If your ISP require you to enter a specific host name or specific MAC address, please enter it in. The **Clone MAC Address** button is used to copy the MAC address of your Ethernet adapter to the Vigor2100V.

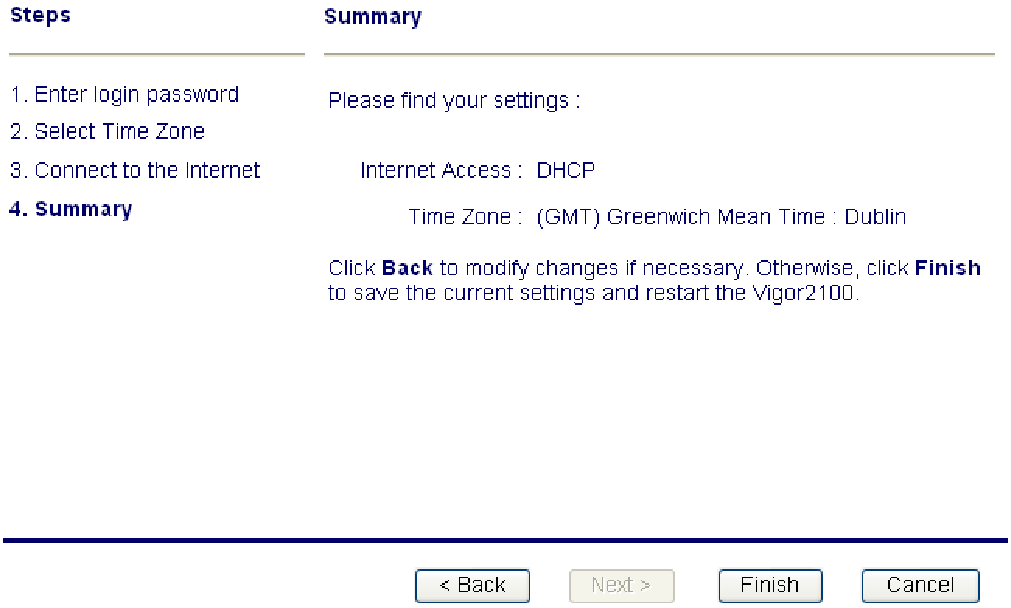
Host Name (optional)

MAC (optional) 00 - 50 - 7F - 28 - EF - 74

Host Name Specify the host name for the router.

MAC This is an optional setting. The router will detect the MAC address automatically. If not, click **Clone MAC Address** to obtain it.

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



Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. **Summary**

Summary

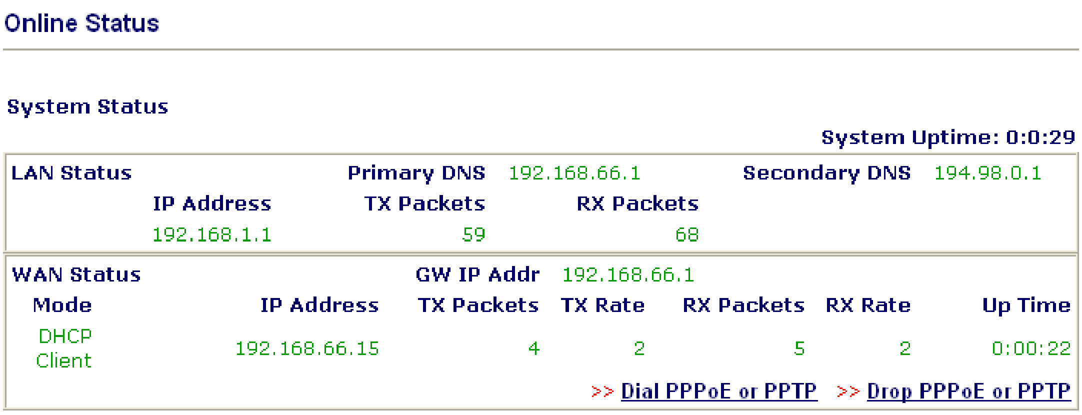
Please find your settings :

Internet Access : DHCP

Time Zone : (GMT) Greenwich Mean Time : Dublin

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2100.

Click **Finish.** The online status of this protocol will be shown as below.



Online Status

System Status

System Uptime: 0:0:29

LAN Status		Primary DNS	192.168.66.1	Secondary DNS	194.98.0.1
	IP Address	TX Packets		RX Packets	
	192.168.1.1	59		68	

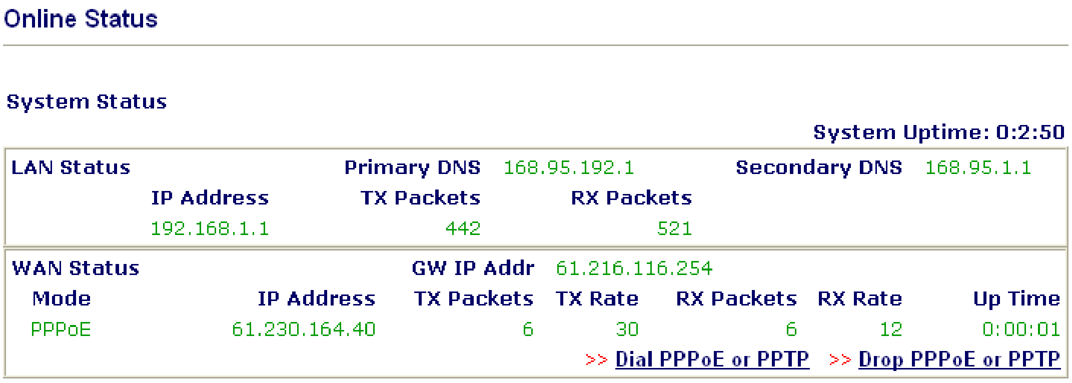
WAN Status		GW IP Addr	192.168.66.1			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
DHCP Client	192.168.66.15	4	2	5	2	0:00:22

>> Dial PPPoE or PPTP >> Drop PPPoE or PPTP

2.3 Online Status for Each Protocol

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

Online status for PPPoE



Online Status

System Status

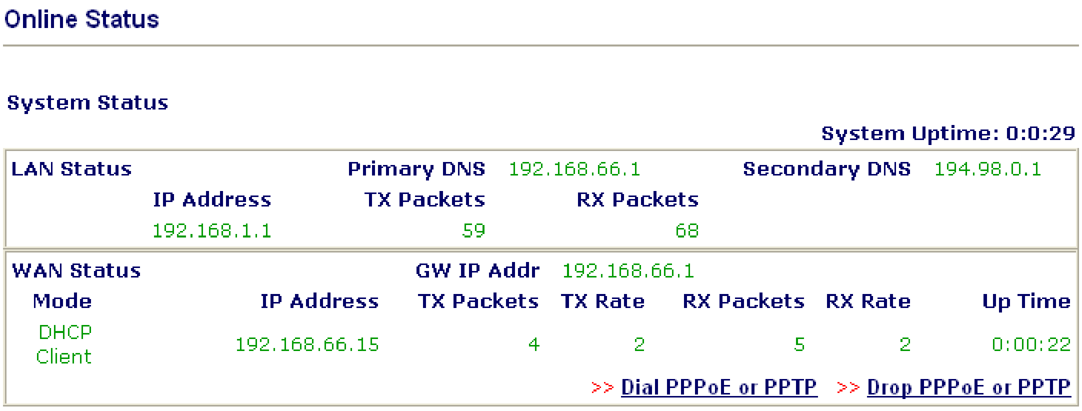
System Uptime: 0:2:50

LAN Status		Primary DNS	168.95.192.1	Secondary DNS	168.95.1.1
	IP Address	TX Packets		RX Packets	
	192.168.1.1	442		521	

WAN Status		GW IP Addr	61.216.116.254			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.164.40	6	30	6	12	0:00:01

>> Dial PPPoE or PPTP >> Drop PPPoE or PPTP

Online status for DHCP



Online Status

System Status

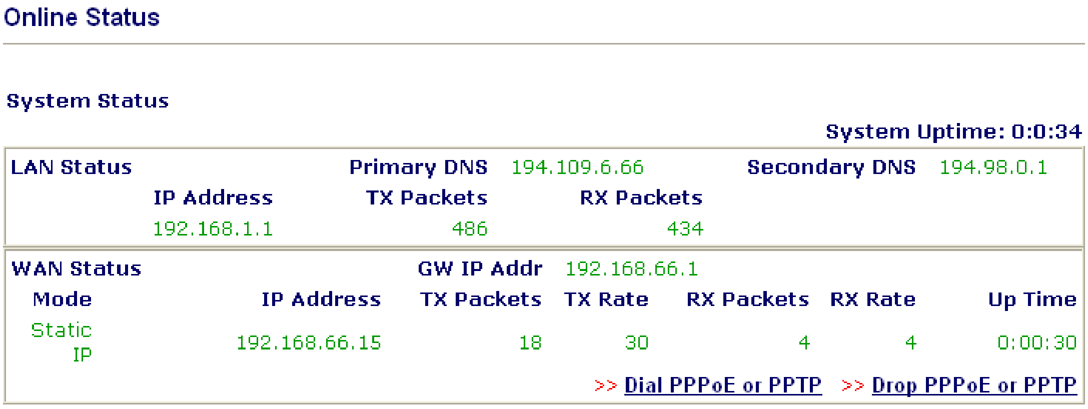
System Uptime: 0:0:29

LAN Status		Primary DNS	192.168.66.1	Secondary DNS	194.98.0.1
	IP Address	TX Packets		RX Packets	
	192.168.1.1	59		68	

WAN Status		GW IP Addr	192.168.66.1			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
DHCP Client	192.168.66.15	4	2	5	2	0:00:22

>> Dial PPPoE or PPTP >> Drop PPPoE or PPTP

Online status for Static IP



Online Status

System Status

System Uptime: 0:0:34

LAN Status		Primary DNS	194.109.6.66	Secondary DNS	194.98.0.1
	IP Address	TX Packets	RX Packets		
	192.168.1.1	486	434		

WAN Status		GW IP Addr	192.168.66.1			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
Static IP	192.168.66.15	18	30	4	4	0:00:30

>> Dial PPPoE or PPTP >> Drop PPPoE or PPTP

Primary DNS Displays the assigned IP address of the primary DNS.

Secondary DNS Displays the assigned IP address of the secondary DNS.

IP Address (in LAN) 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.

GW IP Addr: Displays the assigned IP address of the default gateway.

IP Address (in WAN) Displays the IP address of the WAN interface.

TX Rate Displays the speed of transmitted packets at the WAN interface.

RX Rate Displays the speed of received packets at the WAN interface.

Up Time Displays the total system uptime of the interface.

TX Blocks Displays the total number of transmitted ATM Blocks.

RX Blocks Displays the total number of received ATM Blocks.

Corrected Blocks Displays the total l number of received ATM Blocks corrupted but corrected.

Uncorrected Blocks Displays the total number of received ATM Blocks corrupted but uncorrected.

Mode Displays the modulation mode used: G.DMT, G.Lite, or T1.413.

State Displays the DSL line status.

Up Speed Displays the upstream speed (bits/ second).

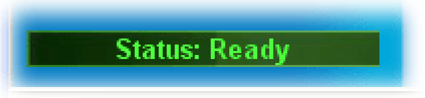
Down Speed Displays the downstream speed (bits/ second).

SNR Margin Displays the value of Signal Noise Ratio Margin (dB). The higher value has better signal quality.

Loop Att. Displays the value of subscribed Loop Attenuation.

2.4 Status Bar

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 Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more settings for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to Chapter 4.

3.1 Internet Access

3.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

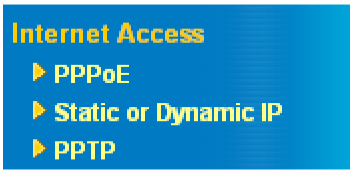
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

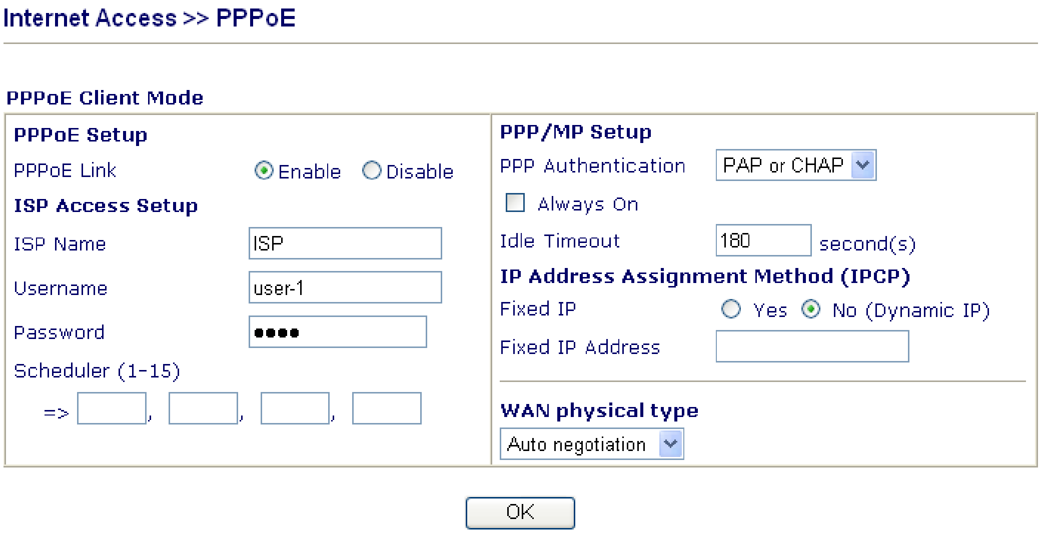
Below shows the menu items of Internet Access.



3.1.2 PPPoE

As a CPE device, Vigor router encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Multiplexer (SDLAM).

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.



Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup		**PPP/MP Setup**	
PPPoE Link	● Enable ○ Disable	PPP Authentication	PAP or CHAP
ISP Access Setup		□ Always On	
ISP Name	ISP	Idle Timeout	180 second(s)
Username	user-1	**IP Address Assignment Method (IPCP)**	
Password	●●●●	Fixed IP	○ Yes ● No (Dynamic IP)
Scheduler (1-15)		Fixed IP Address	
=> , , ,		**WAN physical type**	
		Auto negotiation	

OK

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

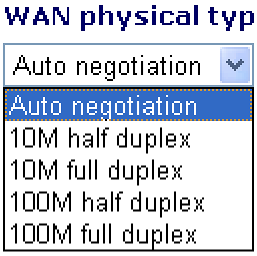
ISP Access Setup Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
ISP Name – Type in the ISP Name provided by ISP in this field.
Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
Scheduler -You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

PPP/MP Setup **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.
Always On – Check this box if you want the router keeping connecting to Internet forever.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

IPCP Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.

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

WAN physical type Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.



WAN physical type

Auto negotiation ▼

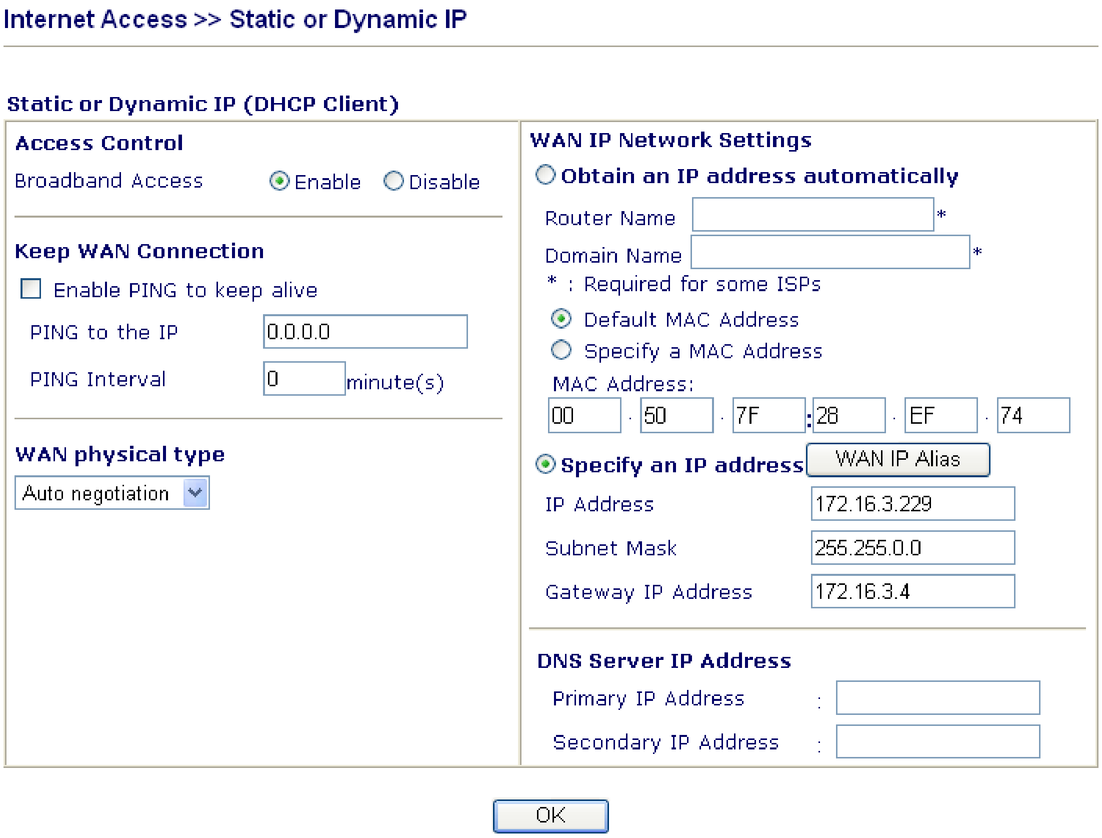
- Auto negotiation
- 10M half duplex
- 10M full duplex
- 100M half duplex
- 100M full duplex

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

3.1.3 Static or Dynamic IP

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 choose **Static or Dynamic IP** as the accessing protocol of the internet, please select **Static or Dynamic IP** from the **Internet Access** menu. The following web page will be shown.



Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

Keep WAN Connection

□ Enable PING to keep alive

PING to the IP: 0.0.0.0

PING Interval: 0 minute(s)

WAN physical type

Auto negotiation ▼

WAN IP Network Settings

○ Obtain an IP address automatically

Router Name: *

Domain Name: *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F : 28 . EF . 74

● Specify an IP address [WAN IP Alias]

IP Address: 172.16.3.229

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.3.4

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

OK

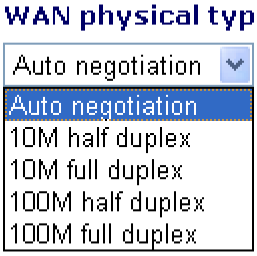
Access Control Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

Keep WAN Connection

Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function.
PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.
PING Interval - Enter the interval for the system to execute the PING operation.

WAN physical type

Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.



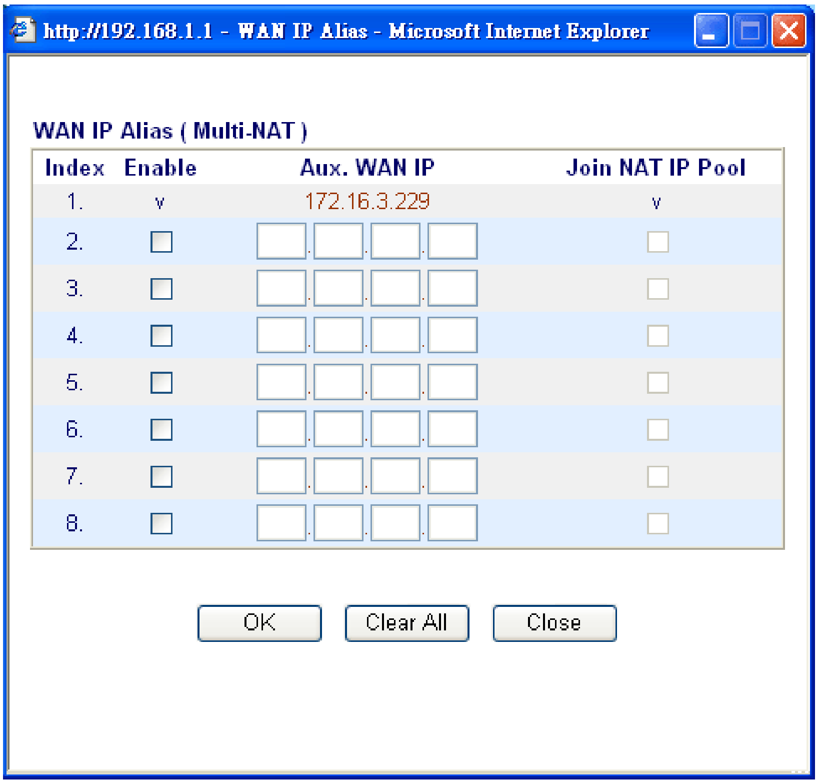
WAN physical type

Auto negotiation

WAN IP Network Settings

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.
Router Name – Type in the router name provided by ISP.
Domain Name – Type in the domain name that you have assigned.
Default MAC Address – Click this radio button to use default MAC address for the router.
Specify a MAC Address - Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. After finishing all the settings here, please click **OK** to activate them.



http://192.168.1.1 - WAN IP Alias - Microsoft Internet Explorer

WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.	□	. . .	□
3.	□	. . .	□
4.	□	. . .	□
5.	□	. . .	□
6.	□	. . .	□
7.	□	. . .	□
8.	□	. . .	□

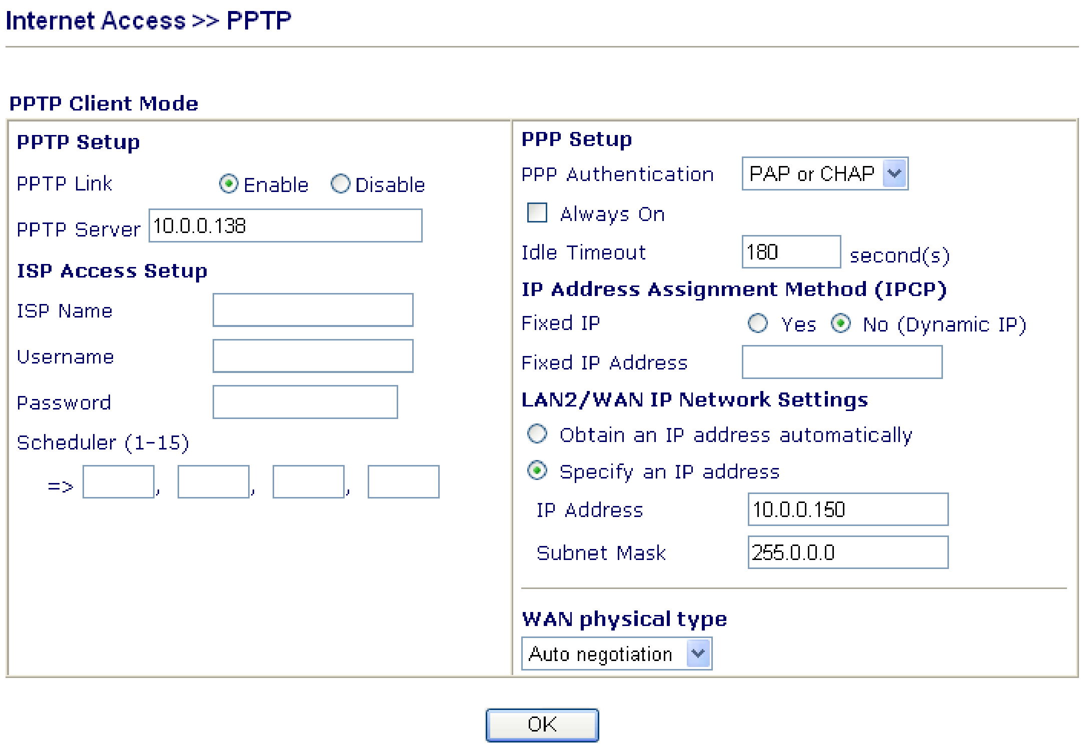
Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.
IP Address – Type the IP address.
Subnet Mask – Type the subnet mask.
Gateway IP Address – Type the gateway IP address.

DNS Server IP Address

Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

3.1.4 PPTP

To choose **PPTP** as the accessing protocol of the internet, please select **Internet Access Setup** on the **Quick Setup** page. **Next,** choose the **PPTP** link. The following web page will be shown.



Internet Access >> PPTP

PPTP Client Mode

PPTP Setup

PPTP Link ● Enable ○ Disable

PPTP Server 10.0.0.138

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

PPP Setup

PPP Authentication PAP or CHAP

□ Always On

Idle Timeout 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

LAN2/WAN IP Network Settings

○ Obtain an IP address automatically

● Specify an IP address

IP Address 10.0.0.150

Subnet Mask 255.0.0.0

WAN physical type

Auto negotiation

PPTP Setup

PPTP Link - Click **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
PPTP Server - Specify the IP address of the PPTP server.

ISP Access Setup

ISP Name - Type in the ISP Name provided by ISP in this field.
Username -Type in the username provided by ISP in this field.
Password -Type in the password provided by ISP in this field.
Scheduler - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

PPP Setup

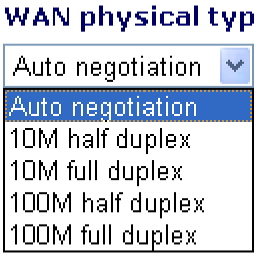
PPP Authentication - Select **PAP only** or **PAP or CHAP** for PPP.
Always On -Check this box if you want the router keeping connecting to Internet forever.
Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.
Fixed IP Address -Type a fixed IP address.

IPCP

Obtain an IP address automatically – Click this button to obtain the IP address automatically.
Specify an IP address – Click this radio button to specify some data.
IP Address – Type the IP address.
Subnet Mask – Type the subnet mask.

WAN physical type

Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.


WAN physical type

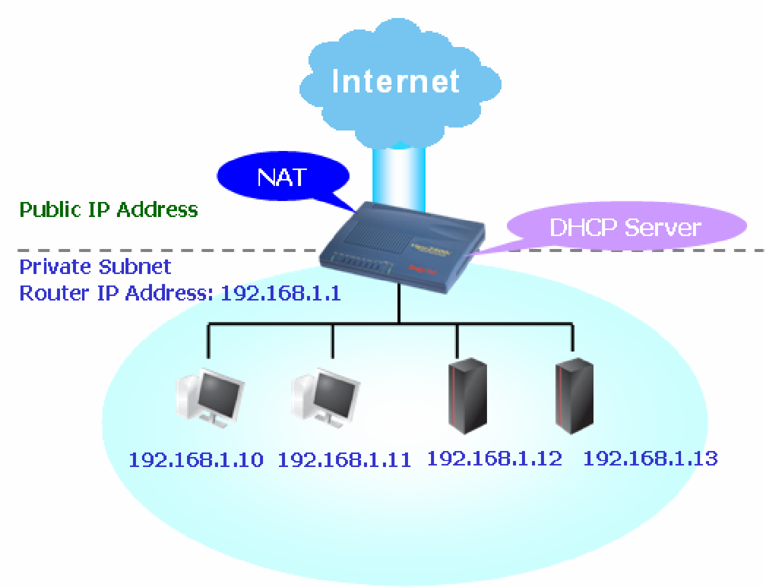
Auto negotiation

3.2 LAN

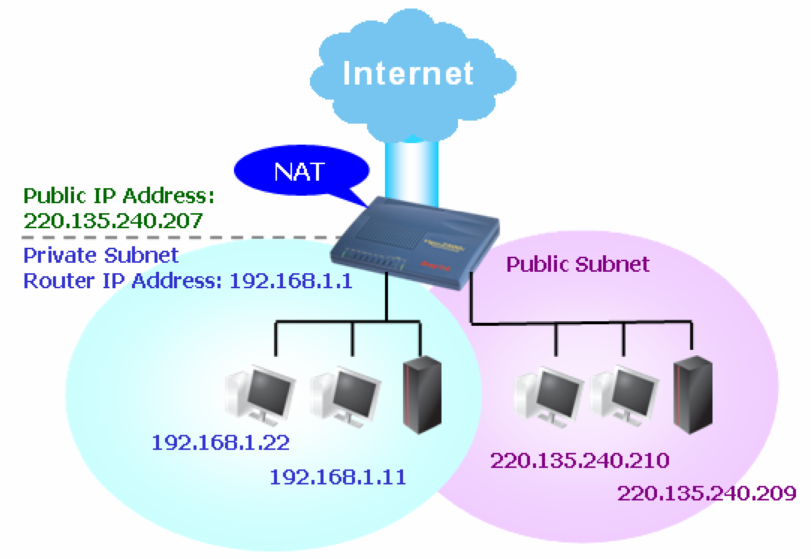
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

3.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

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

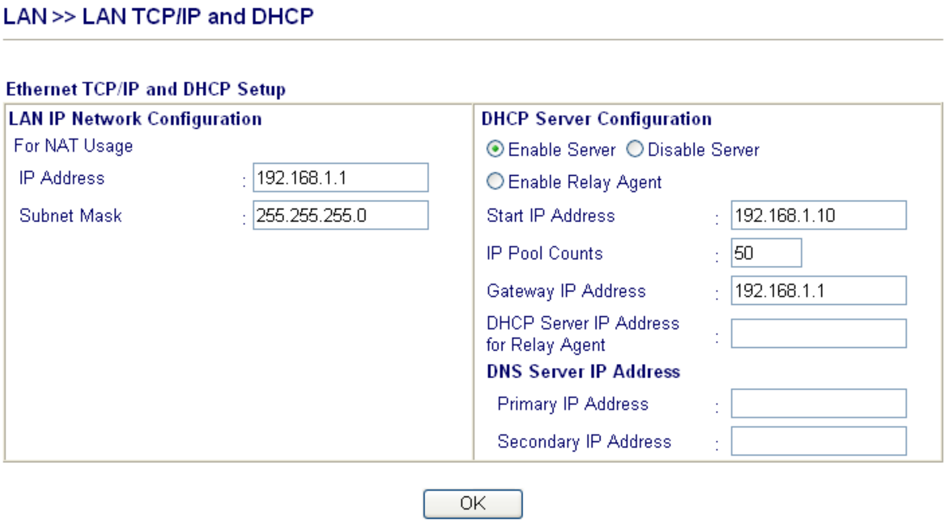
What is Static Route

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.

3.2.2 LAN TCP/IP and DHCP

This page provides you the general settings for LAN.

Click **LAN** to open the LAN settings page and choose **LAN TCP/IP and DHCP**.



LAN >> LAN TCP/IP and DHCP

Ethernet TCP/IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server Configuration

● Enable Server ○ Disable Server

○ Enable Relay Agent

Start IP Address : 192.168.1.10

IP Pool Counts : 50

Gateway IP Address : 192.168.1.1

DHCP Server IP Address for Relay Agent :

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

OK

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

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

DHCP Server Configuration

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

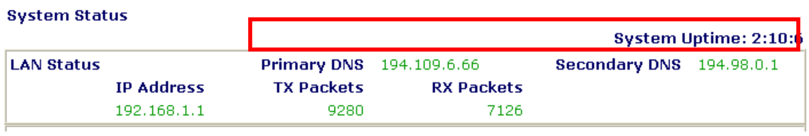
If you want to use another DHCP server in the network other than Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Enable Relay Agent – Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

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



System Status

System Uptime: 2:10:6

LAN Status		Primary DNS	194.109.6.66	Secondary DNS	194.98.0.1
	IP Address	TX Packets	RX Packets		
	192.168.1.1	9280	7126		

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

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

There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that Chapter to get more information for your necessity.

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.

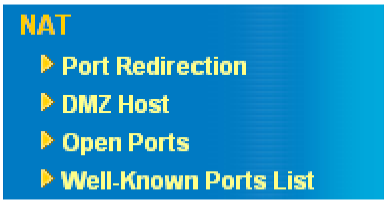
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize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

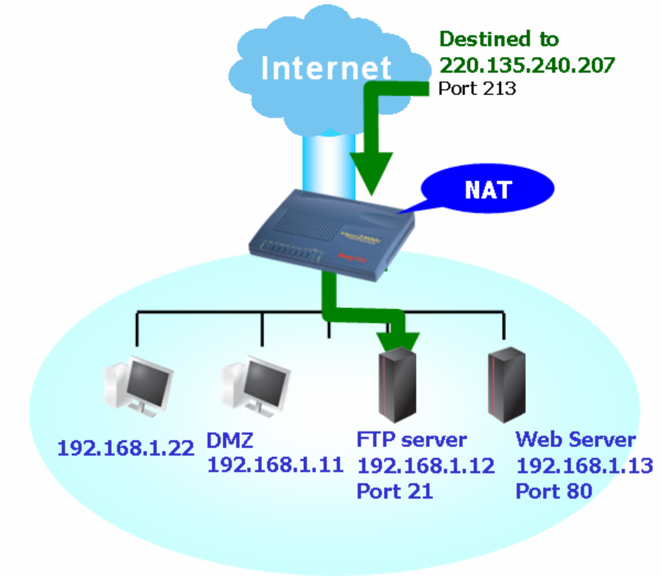
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items of NAT.



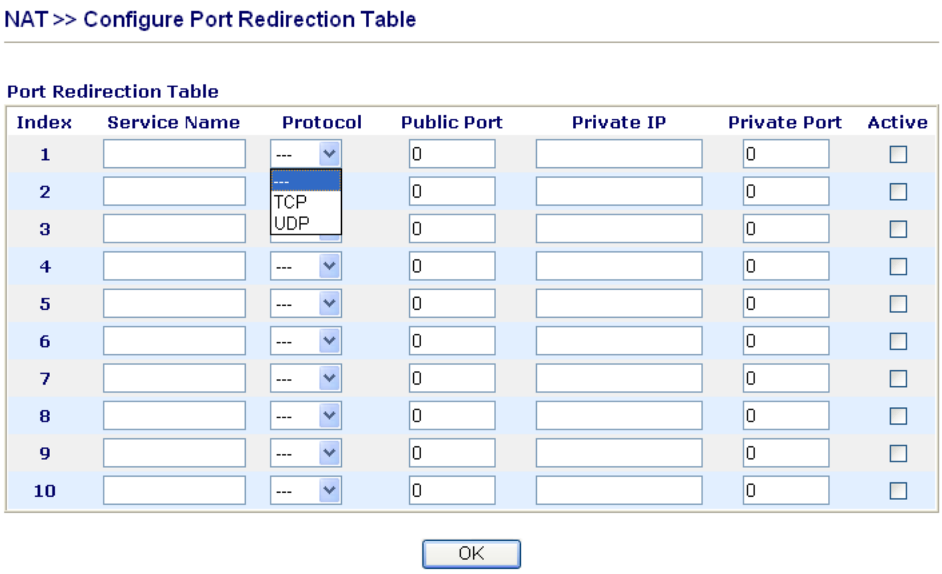
3.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 10 port-mapping entries for the internal hosts.



NAT >> Configure Port Redirection Table

Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1		---	0		0	□
2		---	0		0	□
3			0		0	□
4		---	0		0	□
5		---	0		0	□
6		---	0		0	□
7		---	0		0	□
8		---	0		0	□
9		---	0		0	□
10		---	0		0	□

Service Name Enter the description of the specific network service.

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

Public Port Specify which port can be redirected to the specified **Private IP and Port** of the internal host.

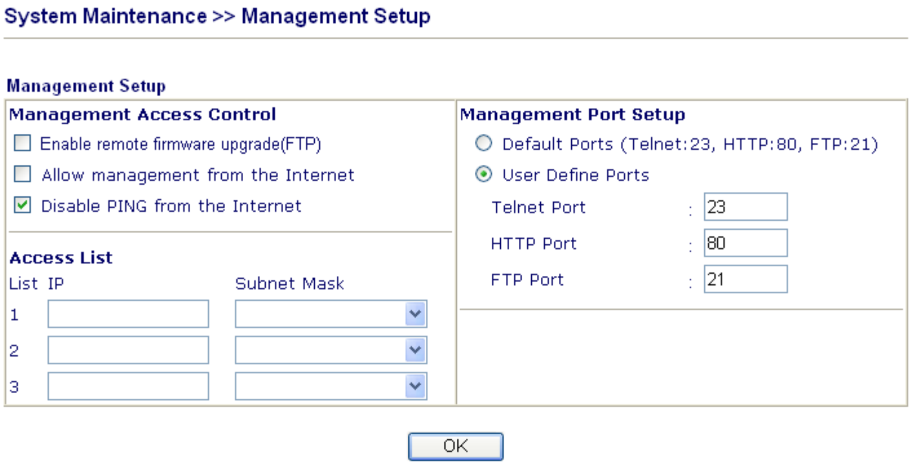
Private IP Specify the private IP address of the internal host providing the service.

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

Active Check this box to activate the port-mapping entry you have defined.

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

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



System Maintenance >> Management Setup

Management Setup

Management Access Control

□ Enable remote firmware upgrade(FTP)
□ Allow management from the Internet
☑ Disable PING from the Internet

Access List

List	IP	Subnet Mask
1		
2		
3		

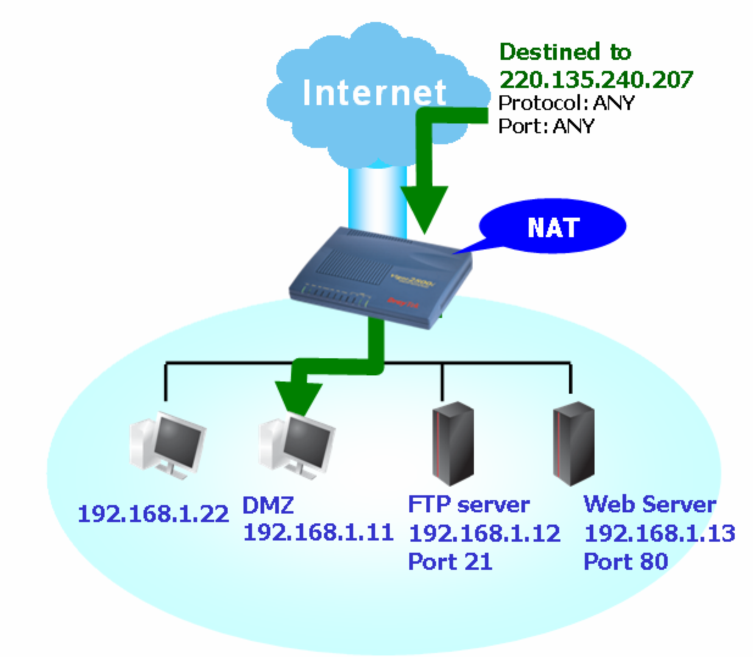
Management Port Setup

○ Default Ports (Telnet:23, HTTP:80, FTP:21)
● User Define Ports

Telnet Port : 23
HTTP Port : 80
FTP Port : 21

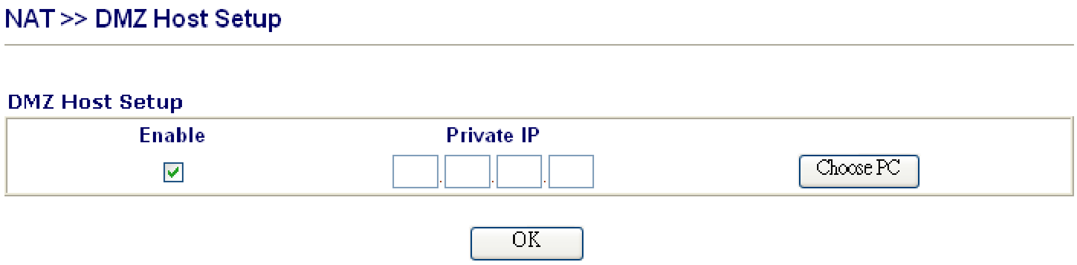
3.3.2 DMZ Host

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



Note: The inherent 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:



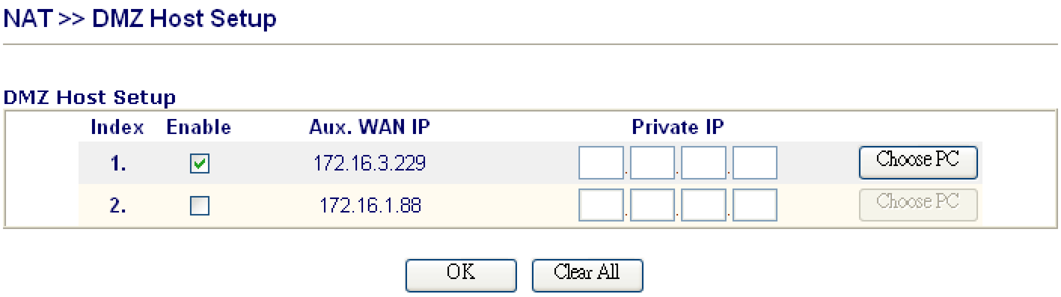
NAT >> DMZ Host Setup

DMZ Host Setup

Enable	Private IP
☑	. . .

Private IP If you choose Private IP as the selection for DMZ host, please type in private IP or select any one by clicking the Choose PC button.

If you previously have set up **WAN Alias** in **Internet Access>>PPPoE,** you will find them in **Aux. WAN IP list** for your selection.



NAT >> DMZ Host Setup

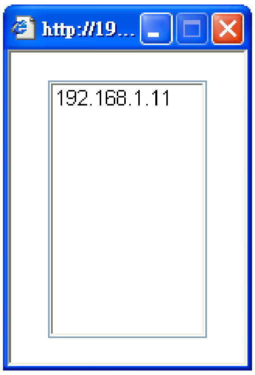
DMZ Host Setup

Index	Enable	Aux. WAN IP	Private IP
1.	☑	172.16.3.229	. . .
2.	□	172.16.1.88	. . .

Enable Check to enable the DMZ Host function.

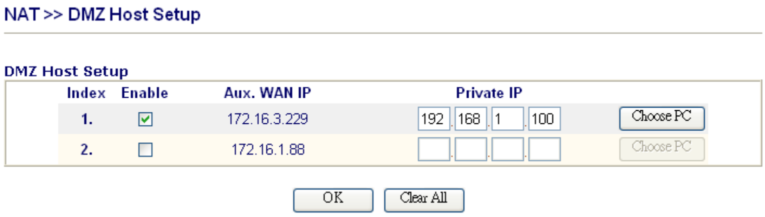
Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

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



192.168.1.11

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



NAT >> DMZ Host Setup

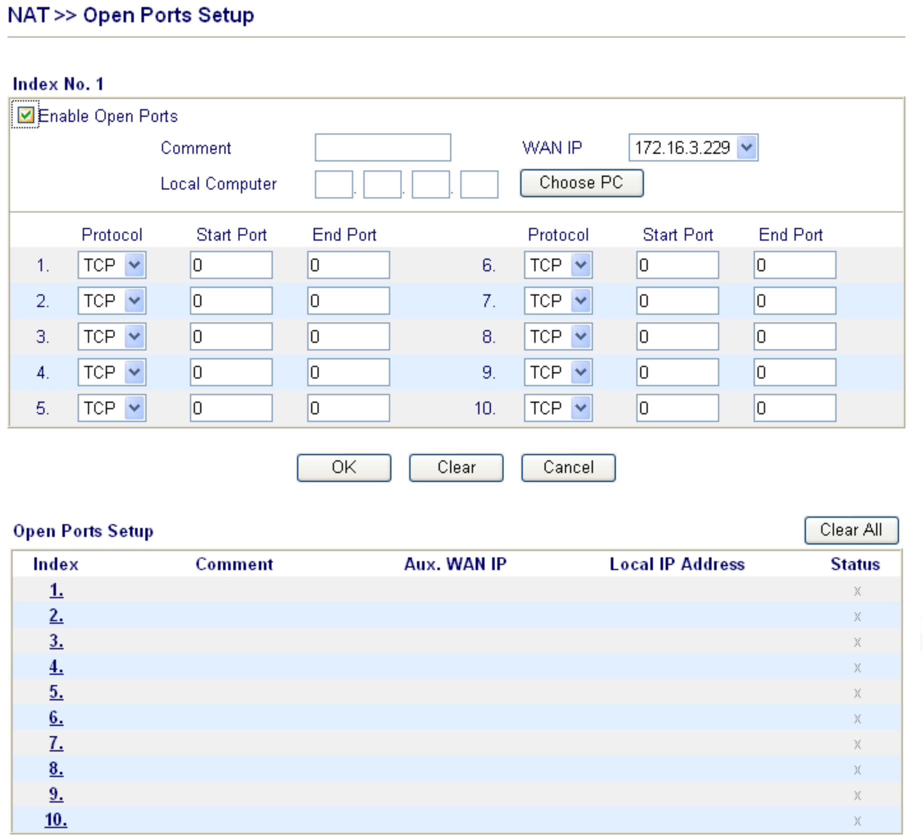
DMZ Host Setup

Index	Enable	Aux. WAN IP	Private IP	
1.	☑	172.16.3.229	192 . 168 . 1 . 100	Choose PC
2.	□	172.16.1.88	. . .	Choose PC

3.3.3 Open Ports

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

Click **Open Ports** to open the following page. However, if you previously have set up **WAN Alias** in **Internet Access>>PPPoE,** you will find that **WAN IP** appeared for your selection.



NAT >> Open Ports Setup

Index No. 1

☑ Enable Open Ports

Comment:

WAN IP: 172.16.3.229

Local Computer: . . . Choose PC

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

Open Ports Setup

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

Index Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

Comment Specify the name for the defined network service.

Aux. WAN IP Display the private IP address of the local host that you specify in WAN Alias. This field will not appear if you did not specify any WAN IP in the WAN Alias page.

Local IP Address Display the private IP address of the local host offering the service.

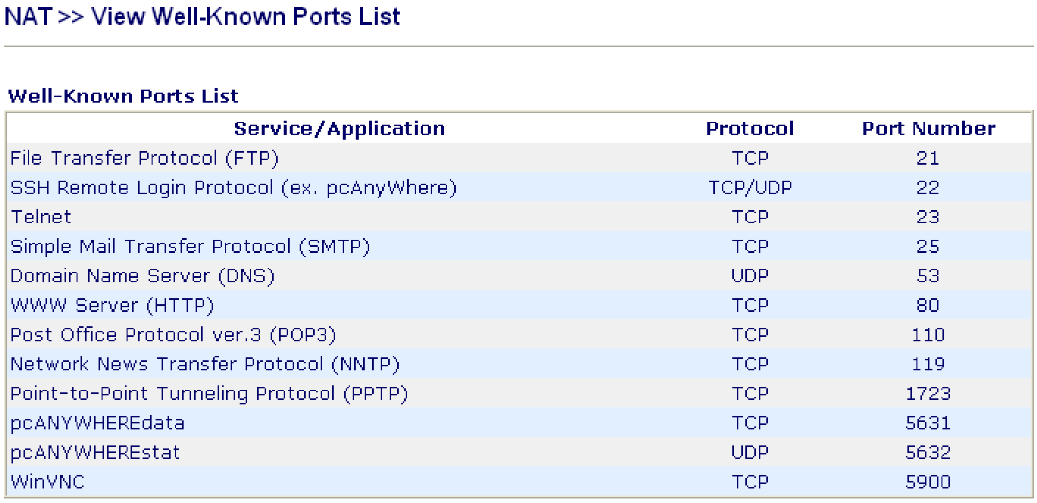
Status Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

To add or edit port settings, click one index number on the page. The configuration page for that index will be shown on the top side of this page. For each index entry, you can specify **10** port ranges for diverse services.

Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or ----- (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

3.3.4 Well-Known Ports List

This page provides you a view of well-known ports.



NAT >> View Well-Known Ports List

Well-Known Ports List

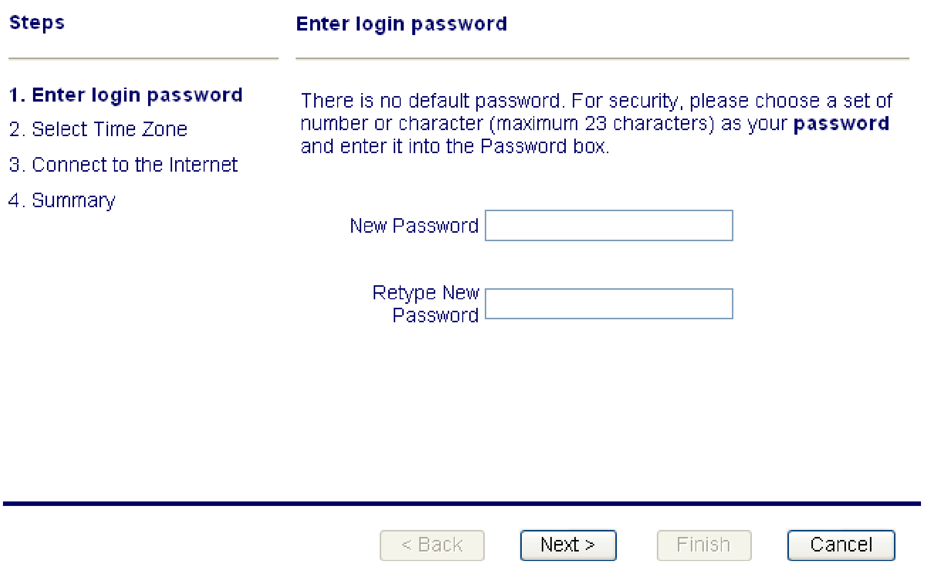
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	TCP/UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

3.4 Firewall

3.4.1 Basics for Firewall

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

The most basic security concept is to set user name and password while you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.



Steps

1. **Enter login password**
2. Select Time Zone
3. Connect to the Internet
4. Summary

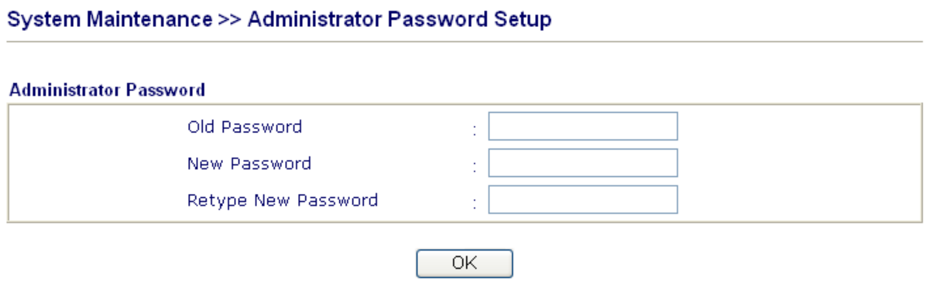
Enter login password

There is no default password. For security, please choose a set of number or character (maximum 23 characters) as your **password** and enter it into the Password box.

New Password

Retype New Password

If you did not set password during installation; you can go to **System Maintenance** to set up your password.



System Maintenance >> Administrator Password Setup

Administrator Password

Old Password :

New Password :

Retype New Password :

Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

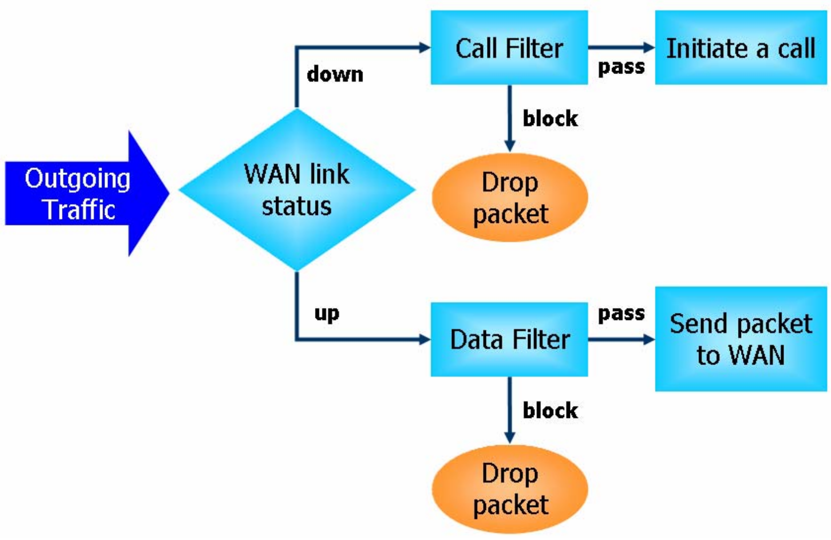
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

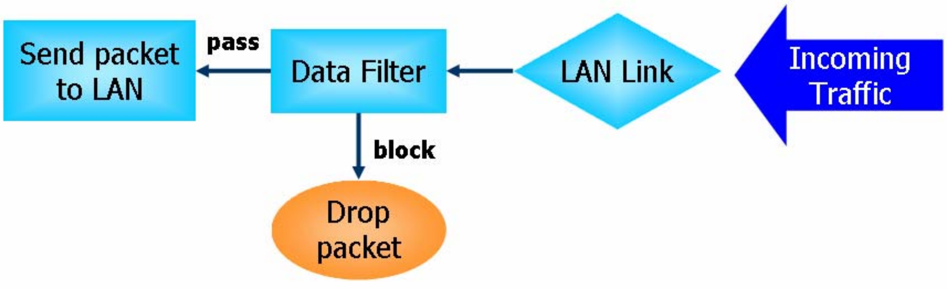
IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter -** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter -** When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.





Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

Instant Messenger (IM) and Peer-to-Peer (P2P) Application Blocking

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide IM and P2P blocking functionality.

Denial of Service (DoS) Defense

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

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

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

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

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

URL Content Filtering

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

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

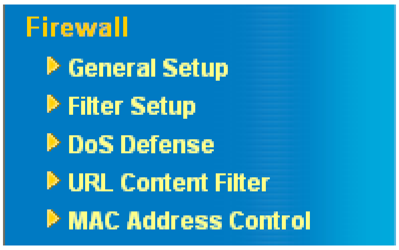
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It’s very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from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

Web Filtering

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

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

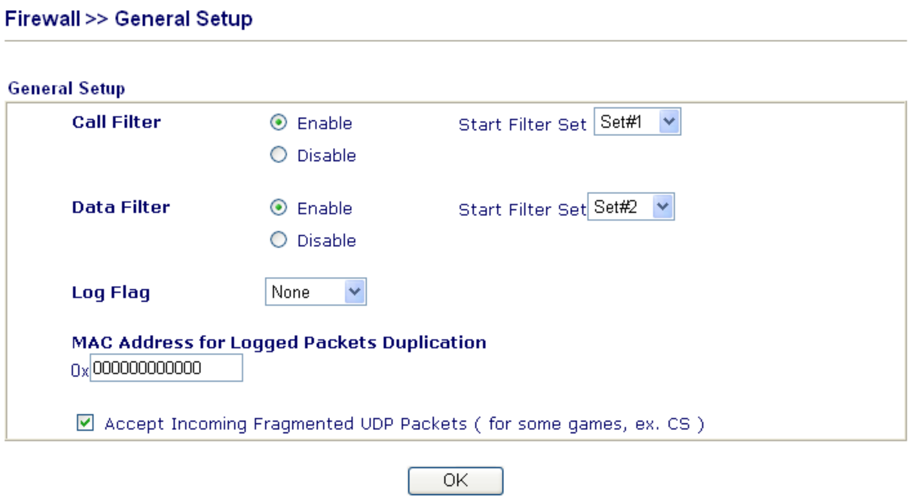
Below shows the menu items of Firewall.



3.4.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Enable Stateful packet inspection**, **Drop non-http connection on TCP port 80**, and **Accept incoming fragmented UDP packets**.

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



Firewall >> General Setup

General Setup

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

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

Log Flag None

MAC Address for Logged Packets Duplication
0x 000000000000

☑ Accept Incoming Fragmented UDP Packets (for some games, ex. CS)

Call Filter Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.

Data Filter Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.

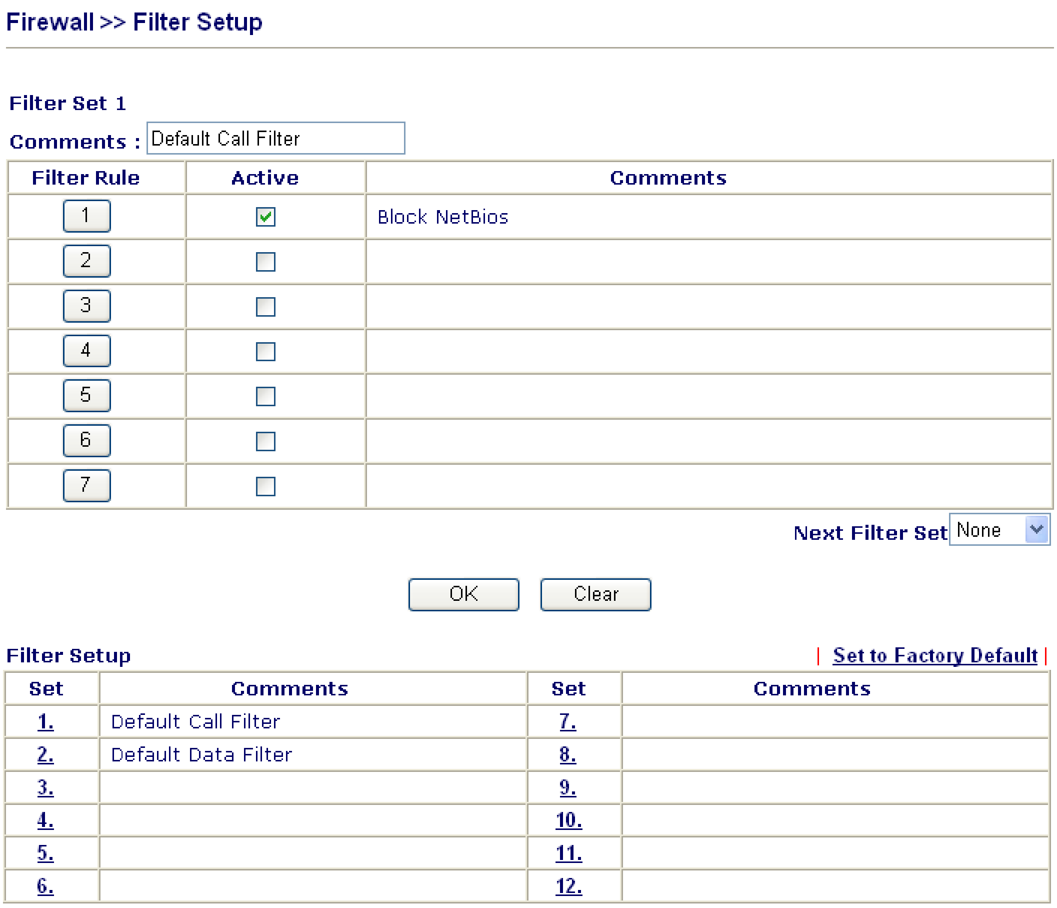
Log Flag For troubleshooting needs you can specify the filter log here.
None - The log function is not activated.
Block - All blocked packets will be logged.
Pass - All passed packets will be logged.
No Match - The log function will record all packets that are not matched.
Note that the filter log will be displayed on the Telnet terminal when you type the ***log -f*** command.

MAC Address for Logged Packet Duplication Logged packets may also be logged to another location via Ethernet. If you want to duplicate logged packets from the router to another network device, you must enter the other devices' MAC Address (HEX Format). Type "0" to disable the feature. The feature will be helpful under Ethernet environments.

Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable **Accept Incoming Fragmented UDP Packets**. By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable **Accept Incoming Fragmented UDP Packets**.

3.4.3 Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page. There are twelve filter sets provided by this router for users to set different filter rules. Simply click the set number on the field of **Filter Setup.** Then you can set filter rules for that index number individually.



Firewall >> Filter Setup

Filter Set 1

Comments : Default Call Filter

Filter Rule	Active	Comments
1	☑	Block NetBios
2	□	
3	□	
4	□	
5	□	
6	□	
7	□	

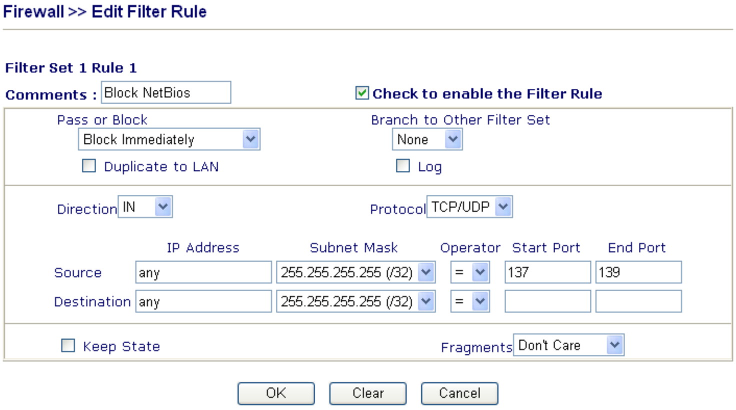
Next Filter Set None

Filter Setup | Set to Factory Default |

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

To edit or add a filter, click on the set number to edit the individual set. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.

Filter Rule Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.



Firewall >> Edit Filter Rule

Filter Set 1 Rule 1

Comments : Block NetBios

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Duplicate to LAN

□ Log

Direction: IN

Protocol: TCP/UDP

	IP Address	Subnet Mask	Operator	Start Port	End Port
Source	any	255.255.255.255 (/32)	=	137	139
Destination	any	255.255.255.255 (/32)	=		

□ Keep State

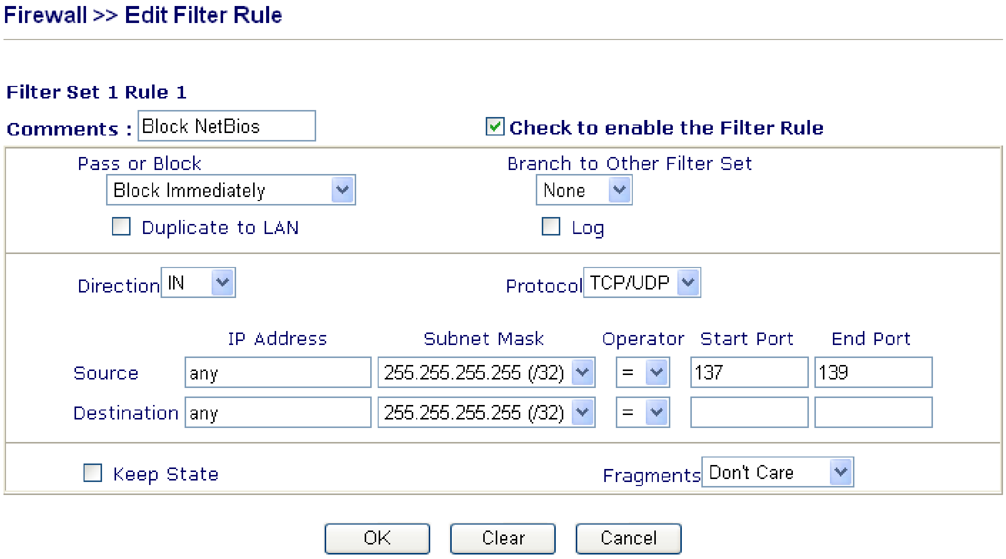
Fragments: Don't Care

Active Enable or disable the filter rule.

Comment Enter filter set comments/description. Maximum length is 23–character long

Next Filter Set Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

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



Firewall >> Edit Filter Rule

Filter Set 1 Rule 1

Comments : Block NetBios

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Duplicate to LAN

□ Log

Direction: IN

Protocol: TCP/UDP

	IP Address	Subnet Mask	Operator	Start Port	End Port
Source	any	255.255.255.255 (/32)	=	137	139
Destination	any	255.255.255.255 (/32)	=		

□ Keep State

Fragments: Don't Care

Comments Enter filter set comments/description. Maximum length is 14-character long.

Check to enable the Filter Rule Check this box to enable the filter rule.

Pass or Block Specifies the action to be taken when packets match the rule.
Pass Immediately - Packets matching the rule will be passed immediately.
Block Immediately - Packets matching the rule will be dropped immediately.
Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.
Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.

Duplicate to LAN If you want to log the matched packets to another network device, check this box to enable it. The MAC Address of the specified network device or PC is defined in **Firewall >>General Setup >> MAC Address for Logged Packets Duplication.**

Branch to other Filter Set If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu.

Log Check this box to enable the log function. Use the Telnet command ***log-f*** to view the logs.

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

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

IP Address Specify the source and destination IP addresses for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter **any** or leave the field blank.

Subnet Mask Select the **Subnet Mask** for the IP Address column for this filter rule to apply from the drop-down menu.

Operator, Start Port and End Port The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number.
(=) If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port).
(!=)If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port).
(>) Specify the port number is larger than the Start Port (includes the Start Port).
(<) Specify the port number is less than the Start Port (includes the Start Port).

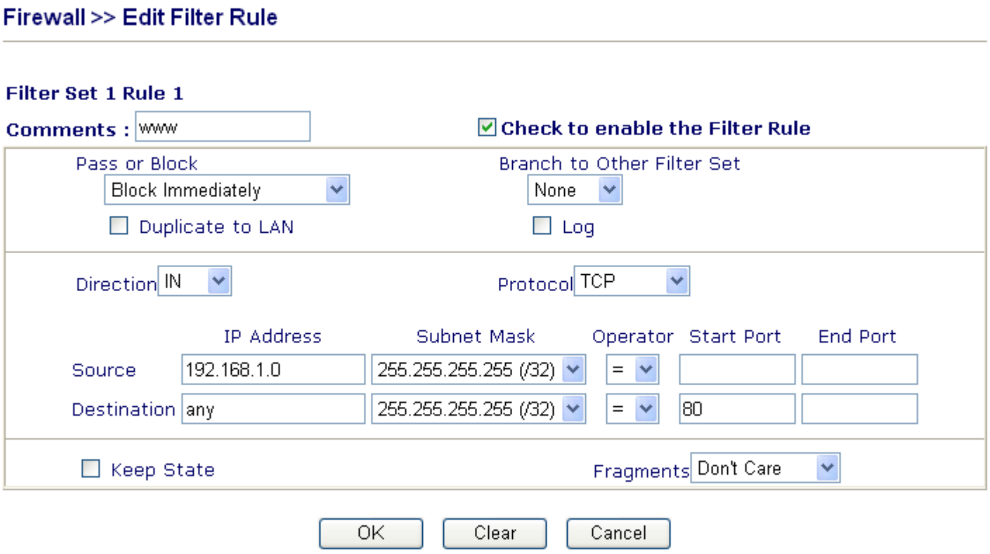
Keep State This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only.

Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP.

Fragments Specify the action for fragmented packets. And it is used for **Data Filter** only.
Don't care -No action will be taken towards fragmented packets.
Unfragmented -Apply the rule to unfragmented packets.
Fragmented - Apply the rule to fragmented packets.
Too Short - Apply the rule only to packets that are too short to contain a complete header.

An Example of Restricting Unauthorized Internet Services

This section will show a simple example to restrict someone from accessing WWW services. In this example, we assume the IP address of the access-restricted user is 192.168.1.10. The filter rule is created in the Data Filter set and is shown as below. Port 80 is the HTTP protocol port number for WWW services.



Firewall >> Edit Filter Rule

Filter Set 1 Rule 1

Comments : www

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Duplicate to LAN

□ Log

Direction: IN

Protocol: TCP

	IP Address	Subnet Mask	Operator	Start Port	End Port
Source	192.168.1.0	255.255.255.255 (/32)	=		
Destination	any	255.255.255.255 (/32)	=	80	

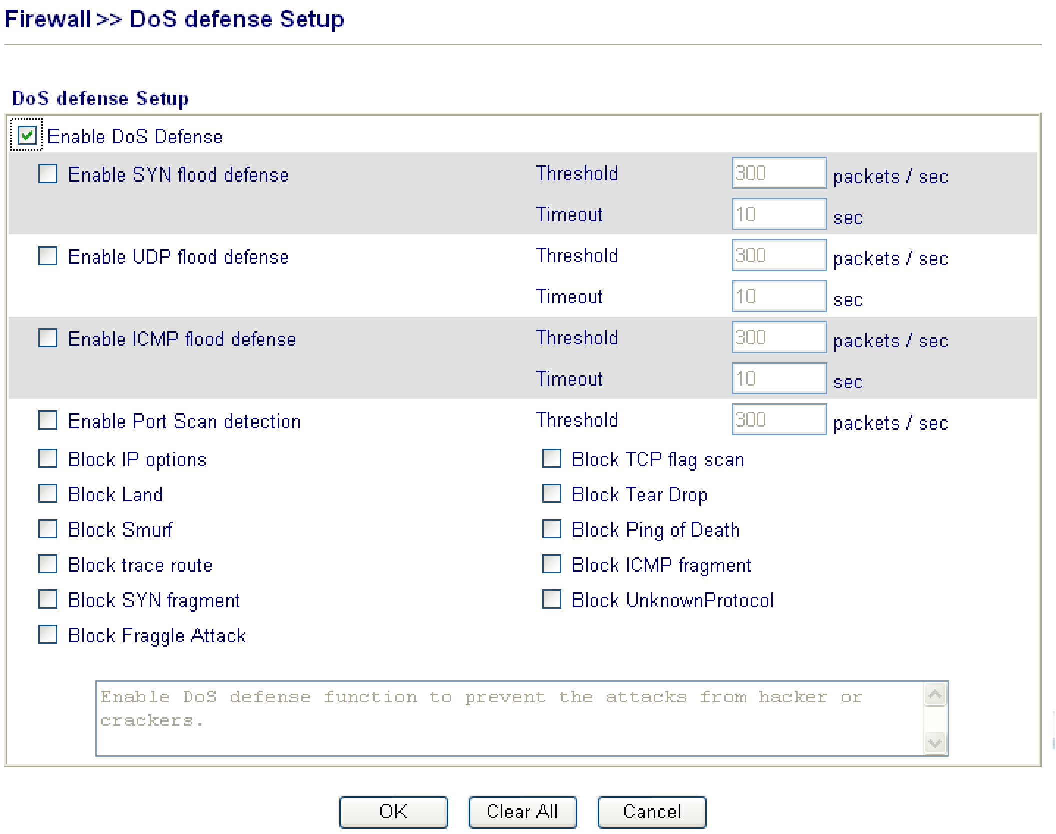
□ Keep State

Fragments: Don't Care

3.4.4 DoS Defense

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

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



Firewall >> DoS defense Setup

DoS defense Setup

☑ Enable DoS Defense

□ Enable SYN flood defense	Threshold	300	packets / sec
	Timeout	10	sec
□ Enable UDP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
□ Enable ICMP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
□ Enable Port Scan detection	Threshold	300	packets / sec
□ Block IP options	□ Block TCP flag scan		
□ Block Land	□ Block Tear Drop		
□ Block Smurf	□ Block Ping of Death		
□ Block trace route	□ Block ICMP fragment		
□ Block SYN fragment	□ Block UnknownProtocol		
□ Block Fraggle Attack			

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

Enable Dos Defense Check the box to activate the DoS Defense Functionality.

Enable SYN flood defense Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.

Enable UDP flood defense Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.

Enable ICMP flood defense Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.

Enable PortScan detection Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.

Block IP options Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.

Block Land Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.

Block Smurf Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.

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

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

Block Fraggle Attack Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.

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

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

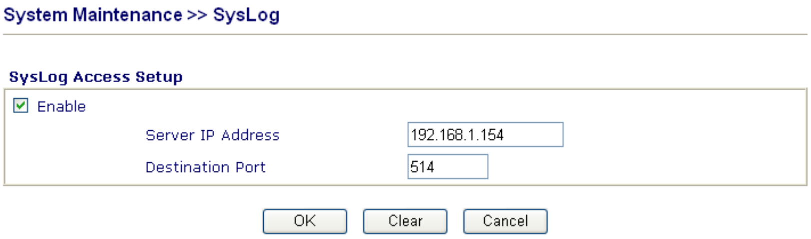
Block Ping of Death Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.

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

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

Warning Messages We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. (Refer to **System Maintenance** >> **Syslog** for detail information.)

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

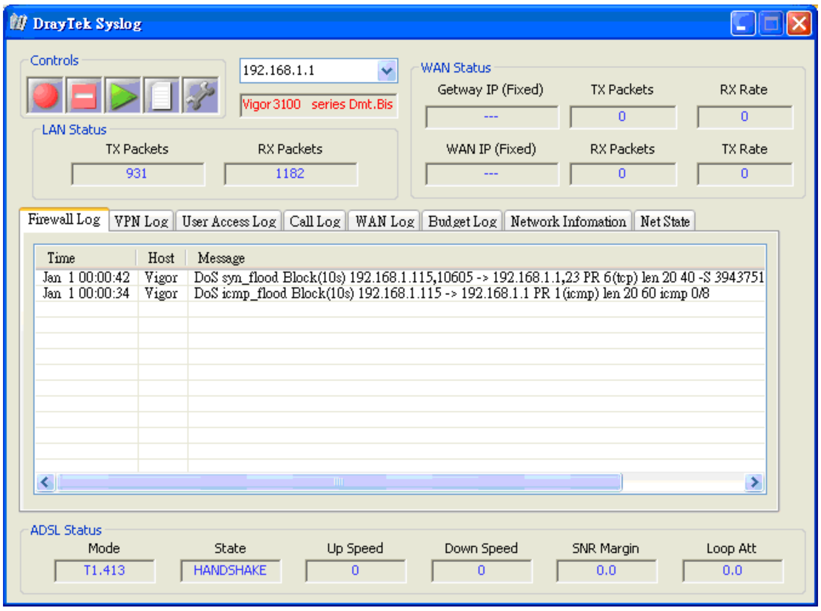


System Maintenance >> SysLog

SysLog Access Setup

☑ Enable

Server IP Address	192.168.1.154
Destination Port	514



DrayTek Syslog

Controls

192.168.1.1

Vigor3100 series Dmt.Bis

WAN Status

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

LAN Status

TX Packets	RX Packets
931	1182

Time	Host	Message
Jan 1 00:00:42	Vigor	DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 3943751
Jan 1 00:00:34	Vigor	DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
T1.413	HANDSHAKE	0	0	0.0	0.0

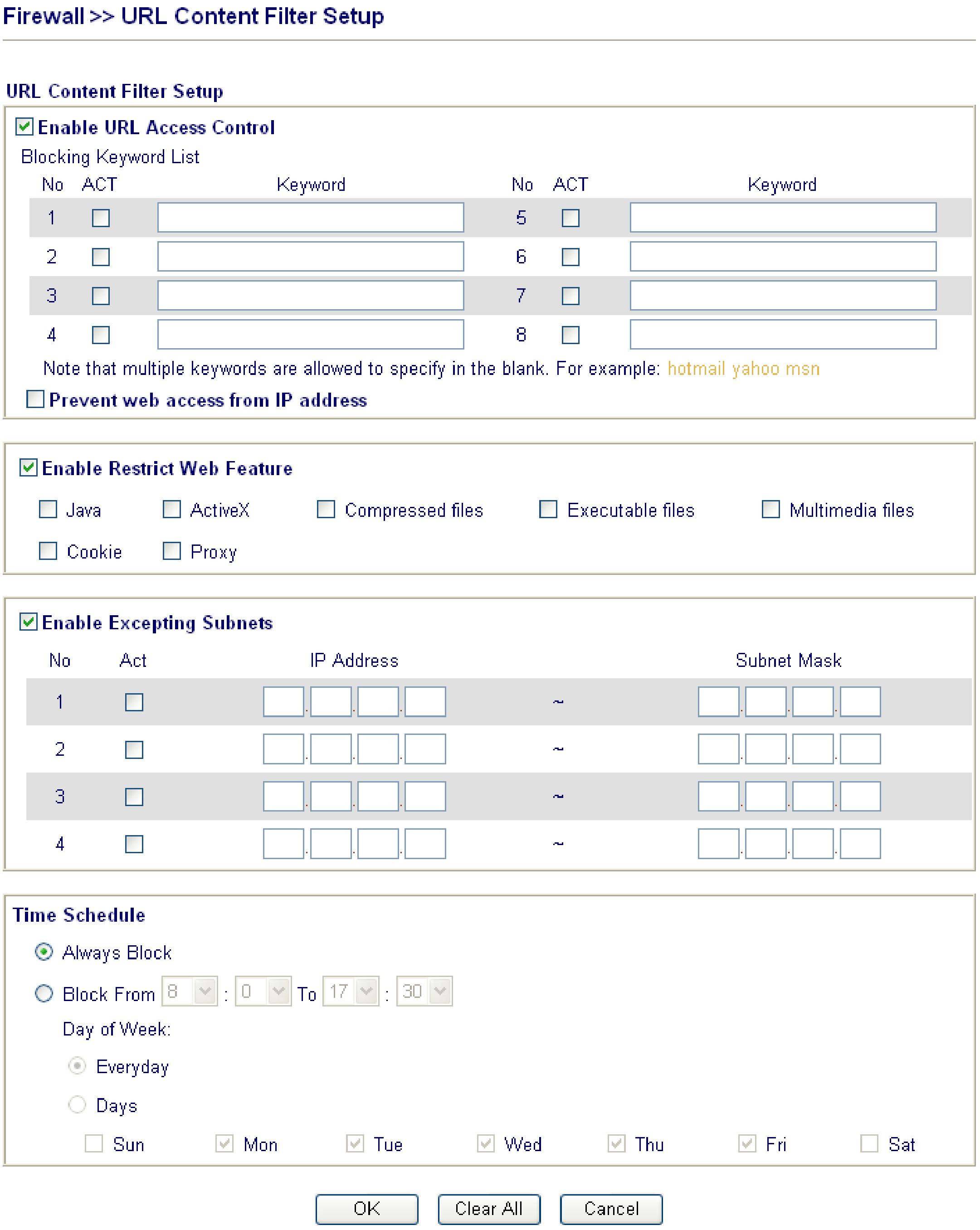
3.4.5 URL Content Filter

Based on the list of user defined keywords, the **URL Content Filter** facility in Vigor router inspects the URL string in every outgoing HTTP request. No matter the URL string is found full or partial matched with a keyword, the Vigor router will block the associated HTTP connection.

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

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

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



Firewall >> URL Content Filter Setup

URL Content Filter Setup

☑ Enable URL Access Control

Blocking Keyword List

No	ACT	Keyword	No	ACT	Keyword
1	□		5	□	
2	□		6	□	
3	□		7	□	
4	□		8	□	

Note that multiple keywords are allowed to specify in the blank. For example: hotmail yahoo msn

□ Prevent web access from IP address

☑ Enable Restrict Web Feature

□ Java □ ActiveX □ Compressed files □ Executable files □ Multimedia files

□ Cookie □ Proxy

☑ Enable Excepting Subnets

No	Act	IP Address		Subnet Mask
1	□	. . .	~	. . .
2	□	. . .	~	. . .
3	□	. . .	~	. . .
4	□	. . .	~	. . .

Time Schedule

● Always Block

○ Block From 8 : 0 To 17 : 30

Day of Week:

● Everyday

○ Days

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

OK Clear All Cancel

Enable URL Access Control Check the box to activate URL Access Control.

Keyword The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.

Prevent web access from IP address

Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control.

You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

Enable Restrict Web Feature

Check the box to activate the function.
Java **-** Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.

ActiveX **-** Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.
Compressed file **-** Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router.
zip, rar, .arj, .ace, .cab, .sit
Executable file **-** Check the box to reject any downloading behavior of the executable file from the Internet.
.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg
Cookie **-** Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.
Proxy **-** Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router.
.mov .mp3 .rm .ra .au .wmv
.wav .asf .mpg .mpeg .avi .ram

Enable Excepting Subnets

Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the *URL Access Control*. To enable an entry, click on the empty checkbox, named as **ACT**, in front of the appropriate entry.

Time Schedule

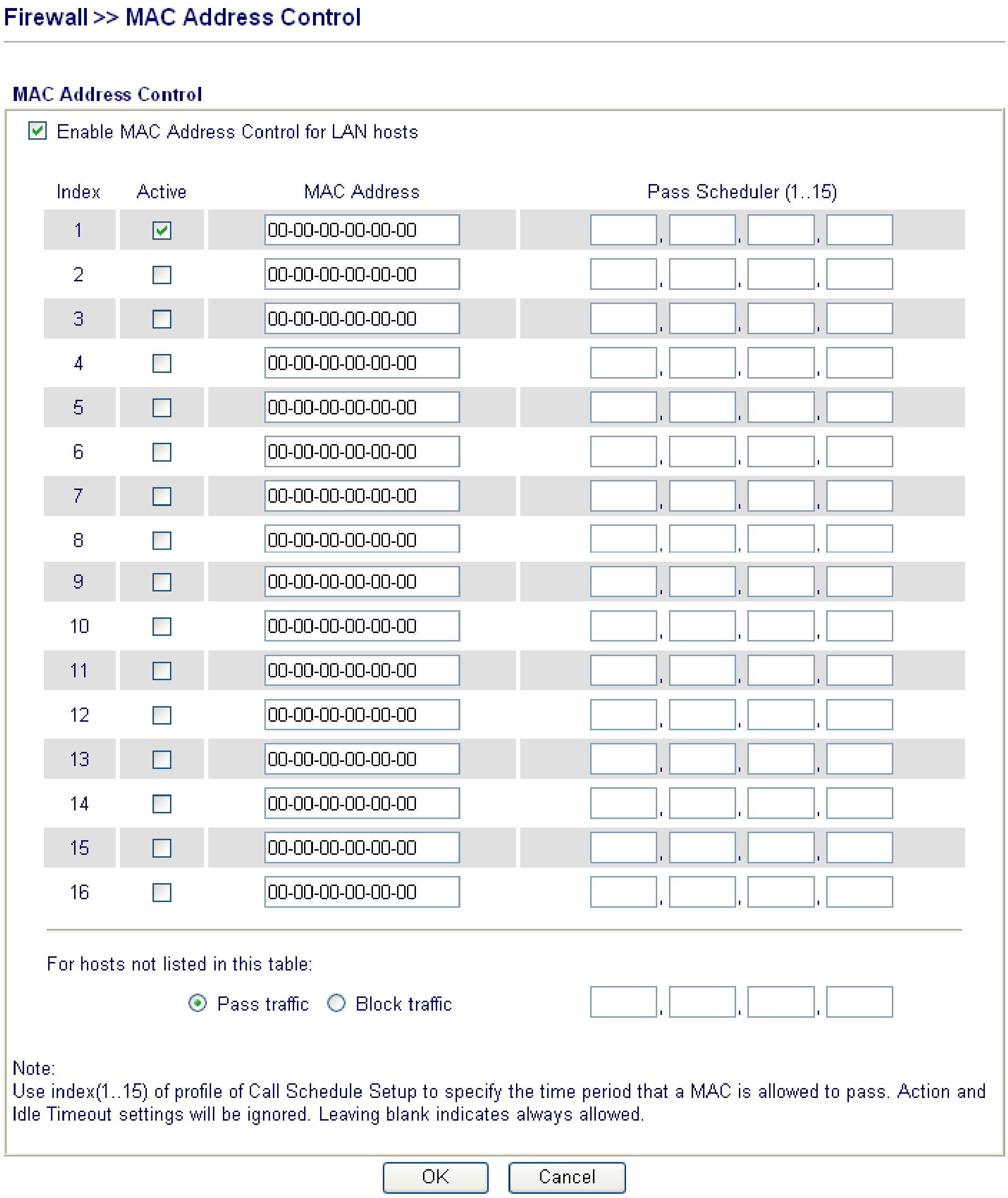
Specify what time should perform the URL content filtering facility.
Always Block - Click it so that the URL content filtering facility can be executed on the Vigor router anytime.
Block from H1:M1 To H2:M2 - Specify the appropriate time duration from *H1*:*M1* to *H2*:*M2* in one day, where *H1* and *H2* indicate the hours. *M1* and *M2* represent the minutes.
Days of Week - Specify which days in one week should apply the URL content filtering facility. The Vigor router supports two exclusive options for users, i.e. everyday or some days in one week. If you expect that the URL content filtering facility is active for whole week, you should click the checkbox “**Everyday**”. Otherwise, you should point clearly out the days in one week. For example, if you want the URL content filtering facility to work from Monday to Wednesday, then you should click the appropriate checkboxes (Monday, Tuesday,

and Wednesday). Other days the URL content filtering facility will be silent.

If you want your kids not to be addicted to on-line gaming, you apply the URL content filtering facility to your router and you set time schedule for school days in order to let your kids have good sleep.

3.4.6 MAC Address Control

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **MAC Address Control** link.



Firewall >> MAC Address Control

MAC Address Control

☑ Enable MAC Address Control for LAN hosts

Index	Active	MAC Address	Pass Scheduler (1..15)
1	☑	00-00-00-00-00-00	, , ,
2	□	00-00-00-00-00-00	, , ,
3	□	00-00-00-00-00-00	, , ,
4	□	00-00-00-00-00-00	, , ,
5	□	00-00-00-00-00-00	, , ,
6	□	00-00-00-00-00-00	, , ,
7	□	00-00-00-00-00-00	, , ,
8	□	00-00-00-00-00-00	, , ,
9	□	00-00-00-00-00-00	, , ,
10	□	00-00-00-00-00-00	, , ,
11	□	00-00-00-00-00-00	, , ,
12	□	00-00-00-00-00-00	, , ,
13	□	00-00-00-00-00-00	, , ,
14	□	00-00-00-00-00-00	, , ,
15	□	00-00-00-00-00-00	, , ,
16	□	00-00-00-00-00-00	, , ,

For hosts not listed in this table:

● Pass traffic ○ Block traffic , , ,

Note:
Use index(1..15) of profile of Call Schedule Setup to specify the time period that a MAC is allowed to pass. Action and Idle Timeout settings will be ignored. Leaving blank indicates always allowed.

OK Cancel

Active Check this box to invoke this setting.

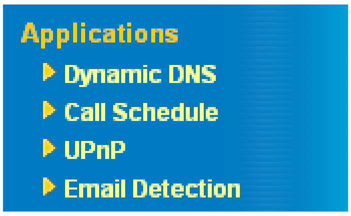
MAC Address Type in the MAC Address of the device that the router connects to.

Pass Scheduler (1..15) Let the device with the specific MAC address to be passed within certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Call Schedule Setup** in **Advanced**

	Setup group setup. If the four boxes are left blank, that means the traffic for the MAC address is “always pass”. If only one disabled schedule typed in the box, it means the related MAC address will be always blocked.
For hosts not listed in this table	This setting allows you to set for all other hosts that not listed in the above table to be passed or be blocked in certain time. Again, please choose four schedules from Call Schedule Setup.

3.5 Applications

Below shows the menu items of Application.



3.5.1 Dynamic DNS

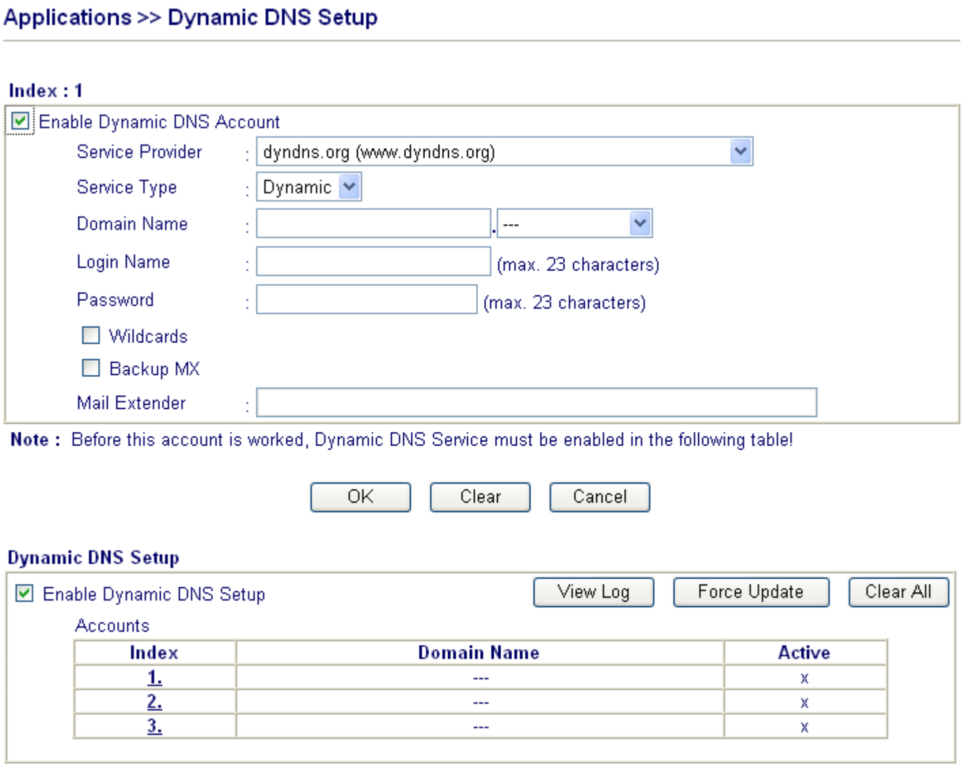
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router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

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

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.

2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.



Applications >> Dynamic DNS Setup

Index : 1

☑ Enable Dynamic DNS Account

Service Provider	:	dyndns.org (www.dyndns.org)
Service Type	:	Dynamic
Domain Name	:	. ---
Login Name	:	(max. 23 characters)
Password	:	(max. 23 characters)
☐ Wildcards		
☐ Backup MX		
Mail Extender	:	

Note : Before this account is worked, Dynamic DNS Service must be enabled in the following table!

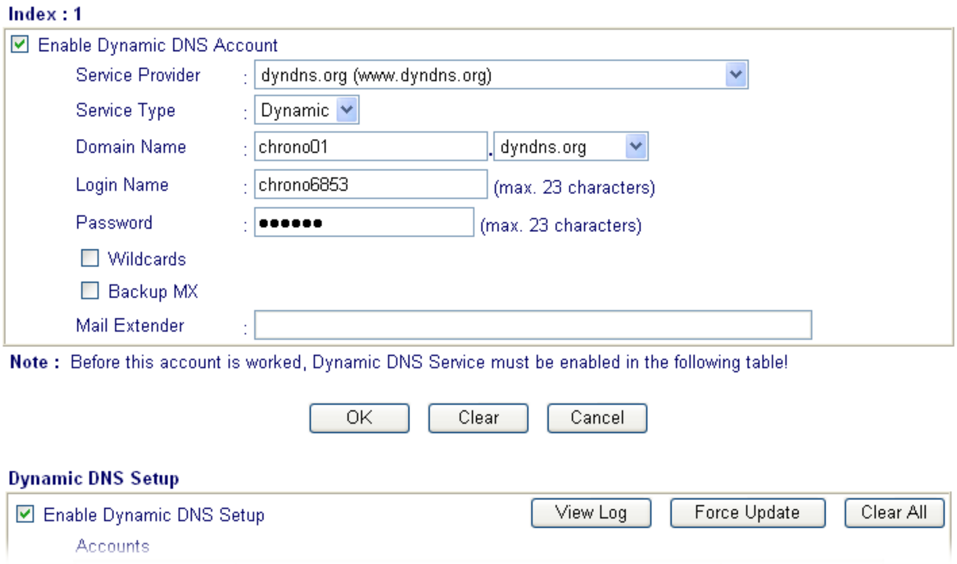
Dynamic DNS Setup

☑ Enable Dynamic DNS Setup

Accounts

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

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



Index : 1

☑ Enable Dynamic DNS Account

Service Provider	:	dyndns.org (www.dyndns.org)
Service Type	:	Dynamic
Domain Name	:	chrono01 . dyndns.org
Login Name	:	chrono6853 (max. 23 characters)
Password	:	•••••• (max. 23 characters)
☐ Wildcards		
☐ Backup MX		
Mail Extender	:	

Note : Before this account is worked, Dynamic DNS Service must be enabled in the following table!

Dynamic DNS Setup

☑ Enable Dynamic DNS Setup

Accounts

Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static).
Domain Name	Type in a domain name that you applied previously.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

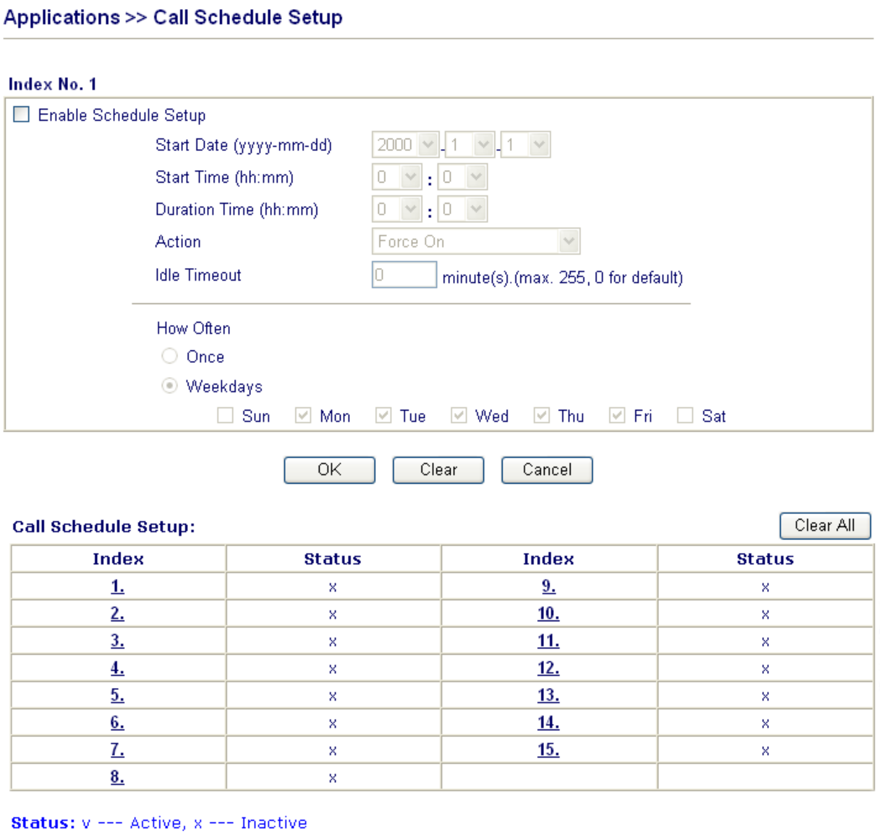
Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.5.2 Call 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 Setup** 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 >> Call Schedule Setup

Index No. 1

☐ Enable Schedule Setup

Start Date (yyyy-mm-dd)	2000 - 1 - 1
Start Time (hh:mm)	0 : 0
Duration Time (hh:mm)	0 : 0
Action	Force On
Idle Timeout	0 minute(s).(max. 255, 0 for default)

How Often

○ Once

● Weekdays

☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

Call Schedule Setup:

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

You can set up to 15 schedules. Then you can apply them to your **Internet Access**.

To add a schedule, please click any index, say Index No. 1. Then adjust the detailed setting for that one on the field just above Call Schedule Setup.

Enable Schedule Setup Check to enable the schedule.

Start Date (yyyy-mm-dd) Specify the starting date of the schedule.

Start Time (hh:mm) Specify the starting time of the schedule.

Duration Time (hh:mm) Specify the duration (or period) for the schedule.

Action Specify which action Call Schedule should apply during the period of the schedule.
Force On -Force the connection to be always on.
Force Down -Force the connection to be always down.
Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field.
Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

Idle Timeout Specify the duration (or period) for the schedule.

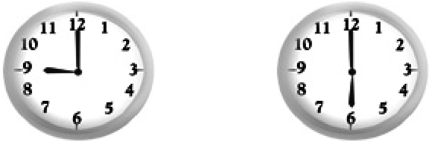
How often Specify how often the schedule will be applied
Once -The schedule will be applied just once
Weekdays -Specify which days in one week should perform the schedule.

Example

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

Office Hour:

(Force On)

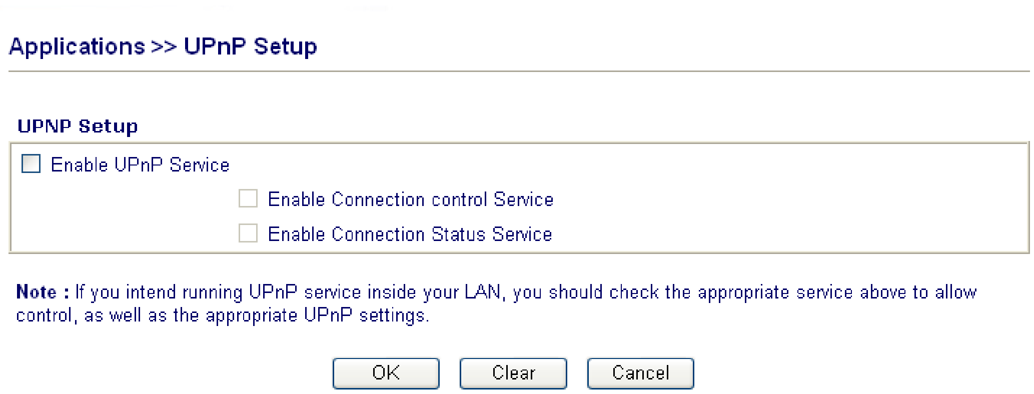


Mon - Sun **9:00 am** **to** **6:00 pm**

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

3.5.3 UPnP

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



Applications >> UPnP Setup

UPNP Setup

□ Enable UPnP Service

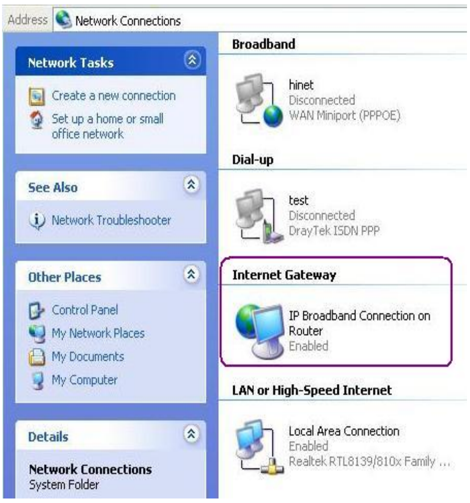
□ Enable Connection control Service

□ Enable Connection Status Service

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

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

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



Address Network Connections

Network Tasks

Create a new connection

Set up a home or small office network

See Also

Network Troubleshooter

Other Places

Control Panel

My Network Places

My Documents

My Computer

Details

Network Connections
System Folder

Broadband

hinet
Disconnected
WAN Miniport (PPPOE)

Dial-up

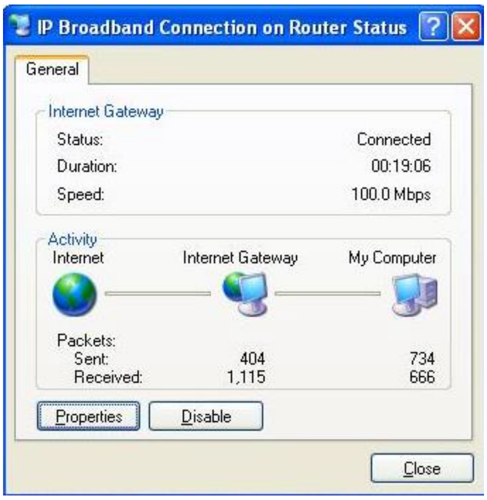
test
Disconnected
DrayTek ISDN PPP

Internet Gateway

IP Broadband Connection on Router
Enabled

LAN or High-Speed Internet

Local Area Connection
Enabled
Realtek RTL8139/810x Family ...



IP Broadband Connection on Router Status

General

Internet Gateway

Status: Connected

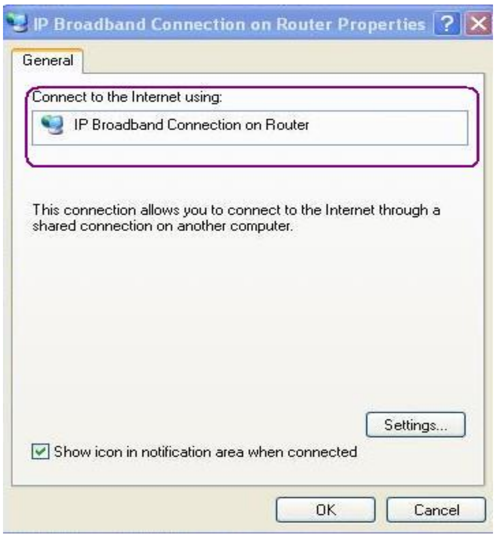
Duration: 00:19:06

Speed: 100.0 Mbps

Activity

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

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

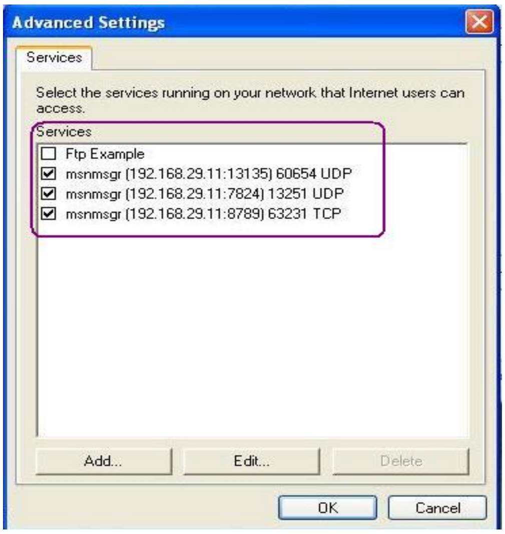


Connect to the Internet using:

IP Broadband Connection on Router

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

☑ Show icon in notification area when connected



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

Services

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

The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

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

Security Considerations

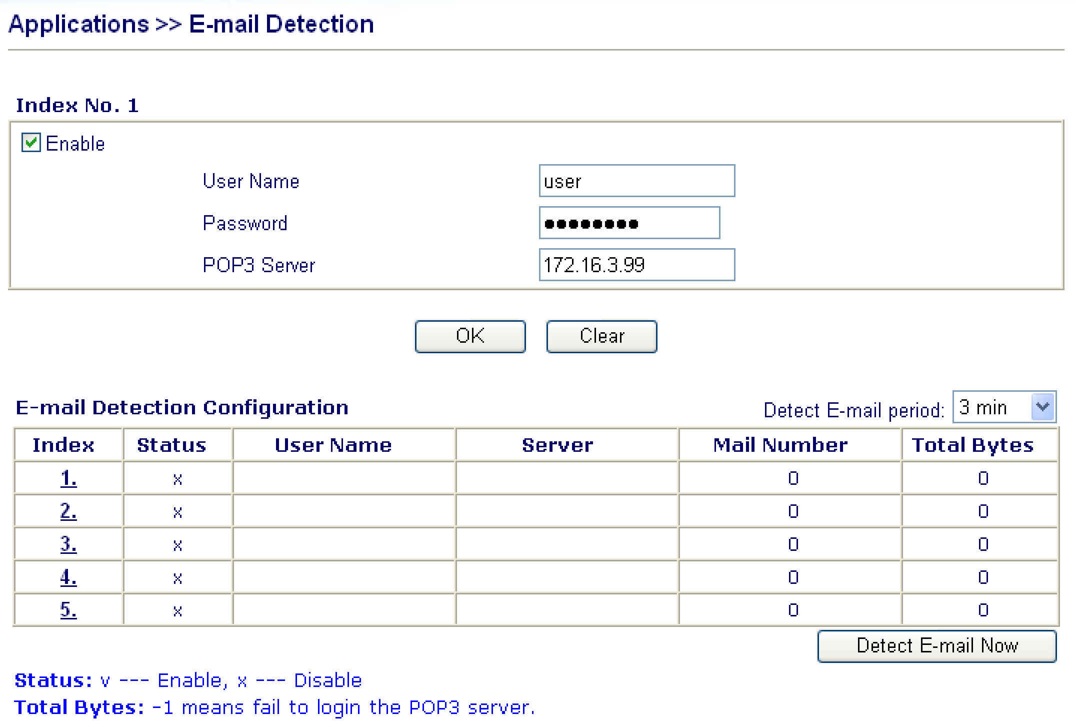
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

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

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

3.5.4 Email Detection

The router can help you detect whether any new email on the assigned mail account. Up to 5 mail accounts can be set.



Applications >> E-mail Detection

Index No. 1

☑ Enable

User Name	user
Password	●●●●●●●●
POP3 Server	172.16.3.99

E-mail Detection Configuration

Detect E-mail period: 3 min

Index	Status	User Name	Server	Mail Number	Total Bytes
1.	x			0	0
2.	x			0	0
3.	x			0	0
4.	x			0	0
5.	x			0	0

Status: v --- Enable, x --- Disable
Total Bytes: -1 means fail to login the POP3 server.

To set email detection, please click any index, say Index No. 1. Then adjust the detailed setting for that one on the field just above E-mail Detection Configuration.

User Name Type the user name or mail account name.

Password Type the password of the mail account.

POP3 Server The IP address of the POP3 mail server.

Detect E-mail period Use the drop-down list to choose the interval of e-mail detection job automatically.

Detect E-mail Now Click this button to execute e-mail detection job.

3.6 VoIP

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

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

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

sip: user:password @ host: port

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

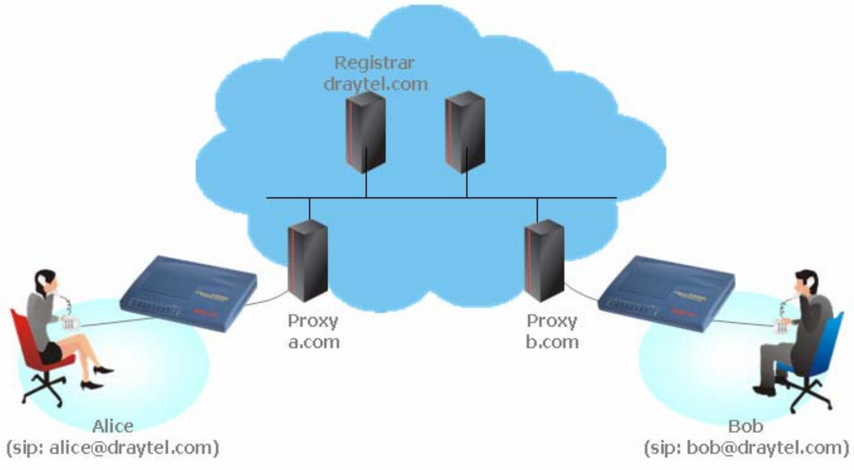
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different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

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

- **Calling via SIP Servers**

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

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



  The major benefit of this mode is that you don’t have to memorize your friend’s IP address, which might change very frequently if it’s dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **Example 1 and 2 in the Calling Scenario.**

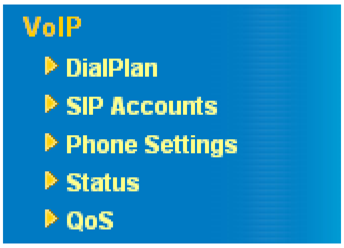
- **Peer-to-Peer**

  Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **Example 3 in the Calling Scenario.**

Vigor VoIP Router
VOIP
Vigor VoIP Router

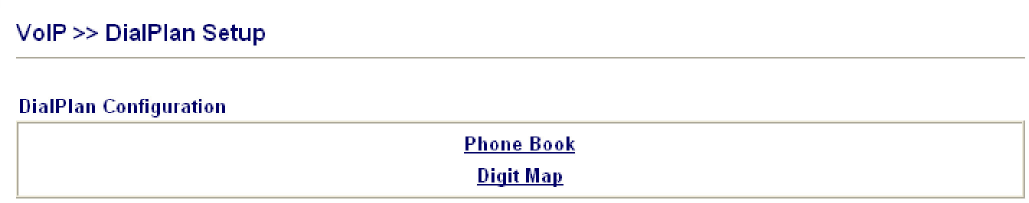
  Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth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

Below shows the menu items of VoIP.



3.6.1 DialPlan

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



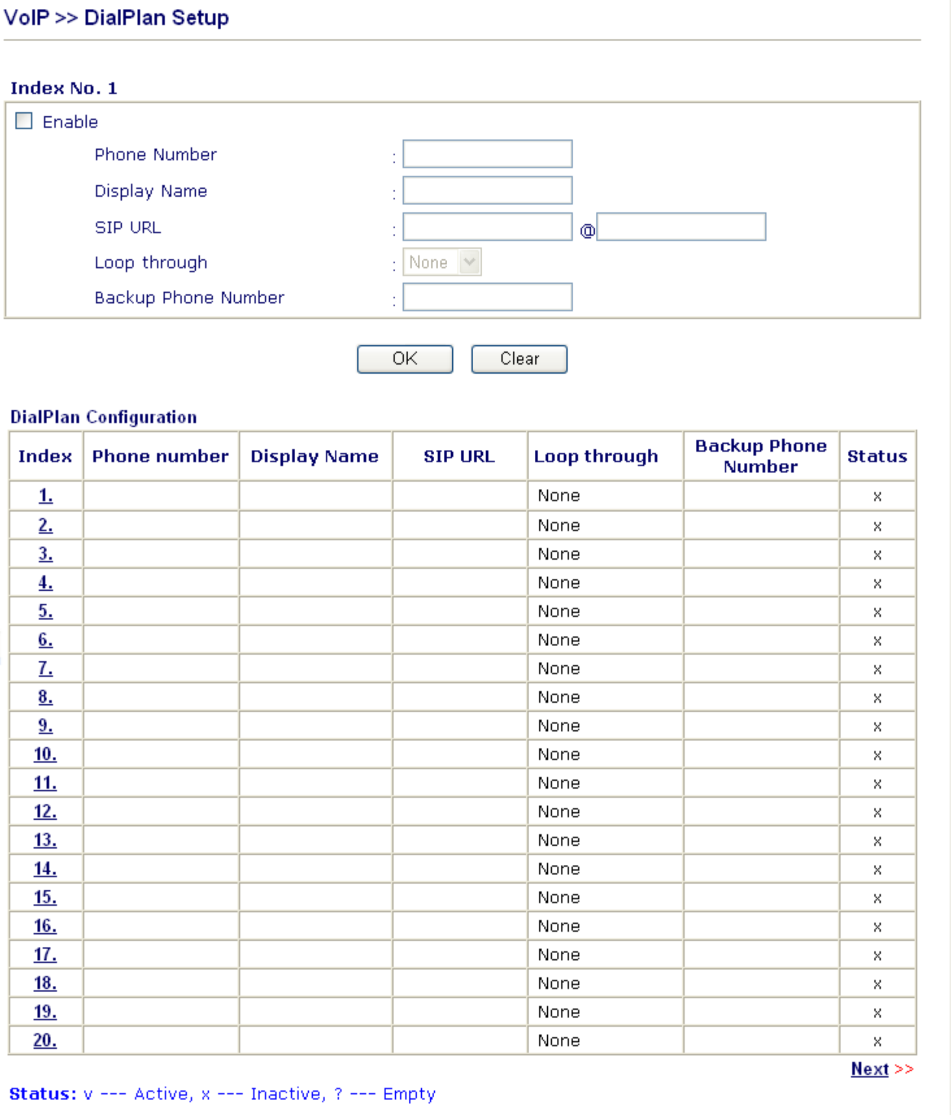
VoIP >> DialPlan Setup

DialPlan Configuration

Phone Book
Digit Map

Phone Book

In this section, you can set your VoIP contacts in the “phonebook”, called DialPlan. It can help you to make calls quickly and easily by using “speed-dial” **Phone Number**. There are total 50 index entries in the DialPlan for you to store all your friends and family members’ SIP addresses.



VoIP >> DialPlan Setup

Index No. 1

☐ Enable

Phone Number	:
Display Name	:
SIP URL	: @
Loop through	: None
Backup Phone Number	:

OK Clear

DialPlan Configuration

Index	Phone number	Display Name	SIP URL	Loop through	Backup Phone Number	Status
1.				None		x
2.				None		x
3.				None		x
4.				None		x
5.				None		x
6.				None		x
7.				None		x
8.				None		x
9.				None		x
10.				None		x
11.				None		x
12.				None		x
13.				None		x
14.				None		x
15.				None		x
16.				None		x
17.				None		x
18.				None		x
19.				None		x
20.				None		x

Next >>

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

Note: There are 60 index entries for phone book in previous firmware version. But, it is reduced to 50 in this version.

To set phone book of dialplan, please click any index, say Index No. 1. Then adjust the detailed setting for that one on the field just above DialPlan Configuration.

Enable Click this to enable this entry.

Phone Number The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** .

Display Name The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.

SIP URL Enter your friend's SIP Address

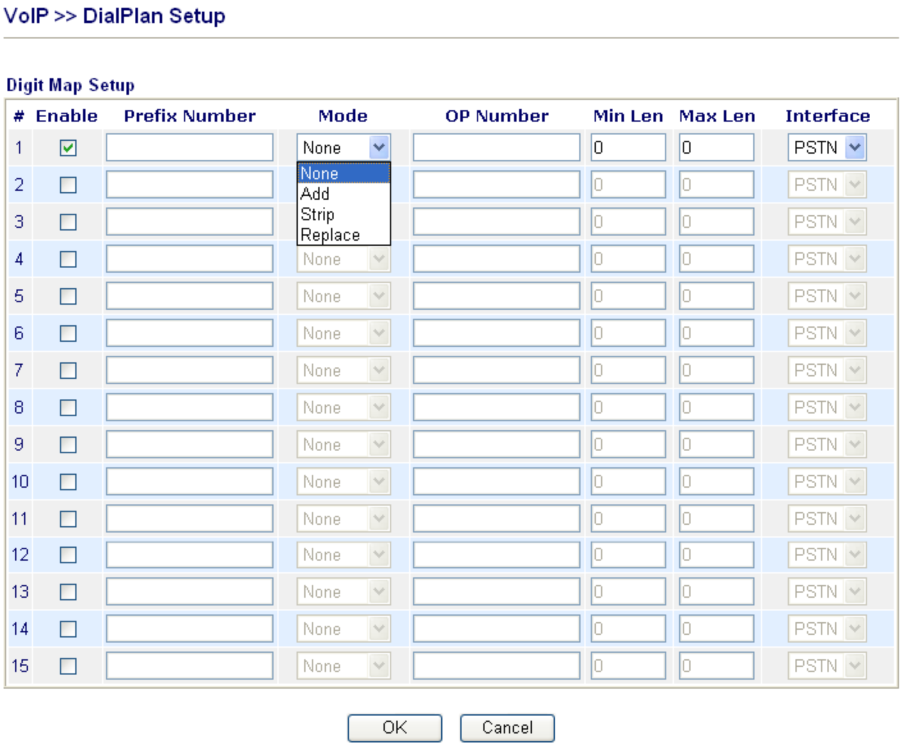
Loop through The selection is as the following:

Loop through: None

Backup Phone Number When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number) for this VoIP phone setting.

Digit Map

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



VoIP >> DialPlan Setup

Digit Map Setup

#	Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
1	☑		None		0	0	PSTN
2	□		None		0	0	PSTN
3	□		None		0	0	PSTN
4	□		None		0	0	PSTN
5	□		None		0	0	PSTN
6	□		None		0	0	PSTN
7	□		None		0	0	PSTN
8	□		None		0	0	PSTN
9	□		None		0	0	PSTN
10	□		None		0	0	PSTN
11	□		None		0	0	PSTN
12	□		None		0	0	PSTN
13	□		None		0	0	PSTN
14	□		None		0	0	PSTN
15	□		None		0	0	PSTN

Enable Check this box to invoke this setting.

Prefix Number The phone number set here is used to add, strip, or replace the OP number.

Mode **None -** No action.
Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.
Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of *886* will be deleted completely for the prefix number is set with *886*.
Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "88631111111" and sent to SIP server.

OP Number The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.

Min Len Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.

Max Len Set the maximum length of the dial number for applying the prefix number settings.

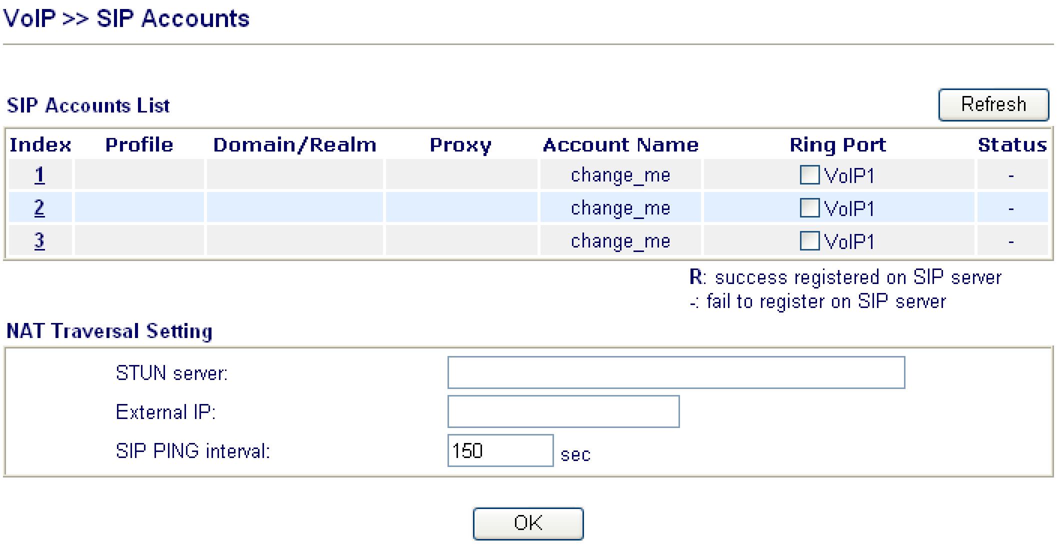
Interface Choose the one that you want to enable the prefix number settings from the four pre-saved SIP accounts (including PSTN).

3.6.2 SIP Accounts

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

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

Note: Vigor VoIP router supports three SIP accounts from firmware version 2.5.9 and later.



VoIP >> SIP Accounts

SIP Accounts List

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1				change_me	□ VoIP1	-
2				change_me	□ VoIP1	-
3				change_me	□ VoIP1	-

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

NAT Traversal Setting

STUN server:	
External IP:	
SIP PING interval:	150 sec

Index Click this link to access into next page for setting SIP account.

Profile Display the profile name of the account.

Domain/Realm Display the domain name or IP address of the SIP registrar server.

Proxy Display the domain name or IP address of the SIP proxy server.

Account Name Display the account name of SIP address before @.

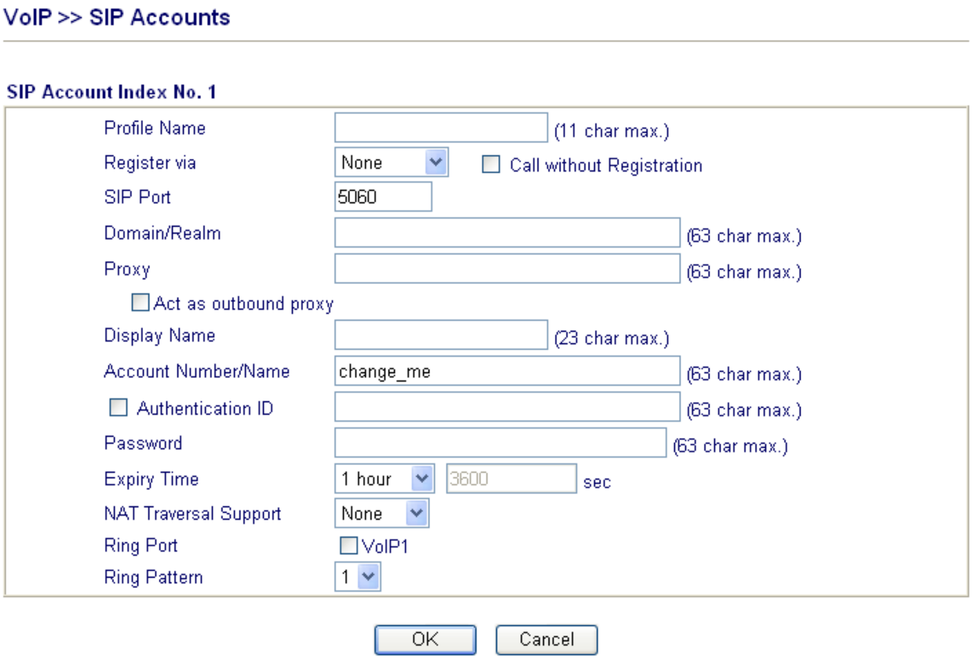
Ring Port Specify which port will ring when receiving a phone call.

STUN Server Type in the IP address of the STUN server.

External IP Type in the gateway IP address.

SIP PING interval The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.

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



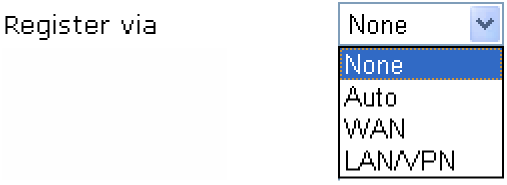
VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	(11 char max.)
Register via	None □ Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
□ Act as outbound proxy	
Display Name	(23 char max.)
Account Number/Name	change_me (63 char max.)
□ Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 3600 sec
NAT Traversal Support	None
Ring Port	□ VoIP1
Ring Pattern	1

Profile Name Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.

Register via If you do not want to register for VoIP phone, please choose **None**. In addition, some SIP server allows users to use VoIP function without registering. For such server, please check the box of **make call without register**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call.



Register via None

SIP Port Set the port number for sending/receiving SIP message for building a session. The default value is **5060.** Your peer must set the same value in his/her Registrar.

Domain/Realm Set the domain name or IP address of the SIP Registrar server.

Proxy Set domain name or IP address of SIP proxy server. By the time you can type**:port** number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org**:5065**)

Act as Outbound Proxy Check this box to make the proxy acting as outbound proxy.

Display Name The caller-ID that you want to be displayed on your friend's screen.

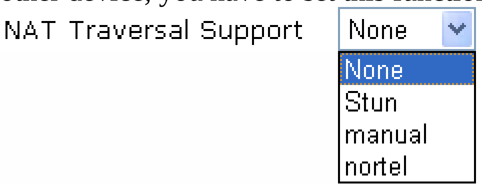
Account Number/Name Enter your account name of SIP Address, e.g. every text before @.

Authentication ID Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.

Password The password provided to you when you registered with a SIP service.

Expiry Time The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.

NAT Traversal Support If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.

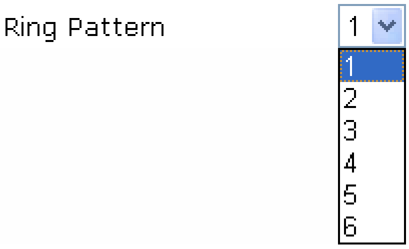


NAT Traversal Support None

None – Disable this function.
Stun – Choose this option if there is Stun server provided for your router.
Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.
Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.

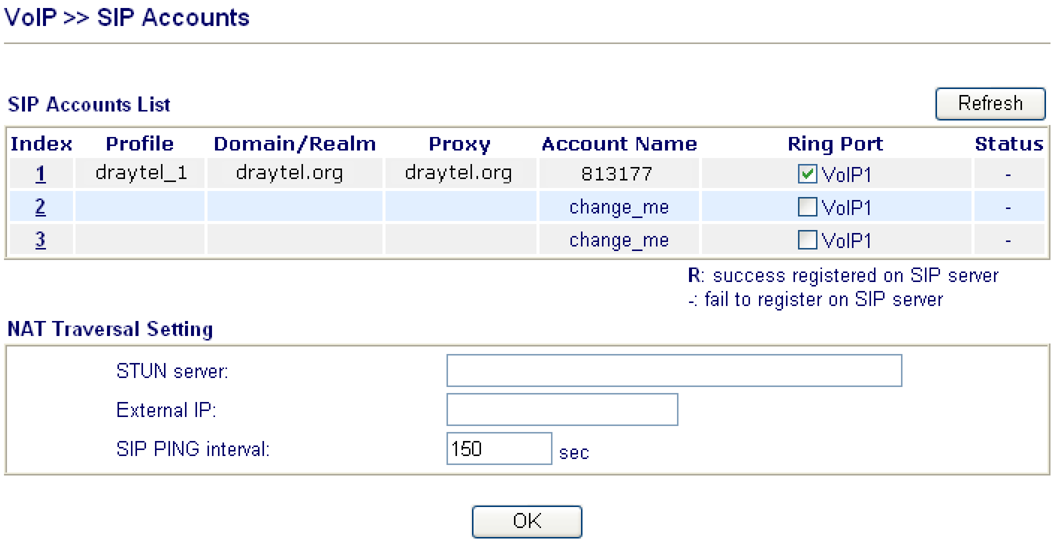
Ring Port Set VoIP 1 or VoIP 2 as the default ring port.

Ring Pattern Choose a ring tone type for the VoIP phone call.



Ring Pattern: 1

Below shows successful SIP accounts for your reference.



VoIP >> SIP Accounts

SIP Accounts List

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1	draytel_1	draytel.org	draytel.org	813177	☑ VoIP1	-
2				change_me	□ VoIP1	-
3				change_me	□ VoIP1	-

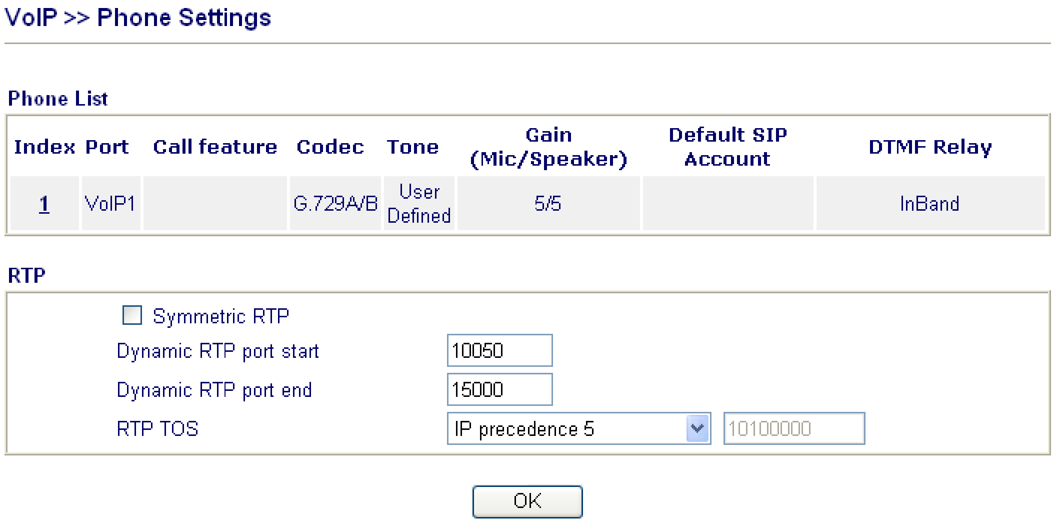
R: success registered on SIP server
-: fail to register on SIP server

NAT Traversal Setting

STUN server:	
External IP:	
SIP PING interval:	150 sec

3.6.3 Phone Settings

This page allows user to set phone settings for VoIP 1.



VoIP >> Phone Settings

Phone List

Index	Port	Call feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	VoIP1		G.729A/B	User Defined	5/5		InBand

RTP

□ Symmetric RTP

Dynamic RTP port start	10050
Dynamic RTP port end	15000
RTP TOS	IP precedence 5 / 10100000

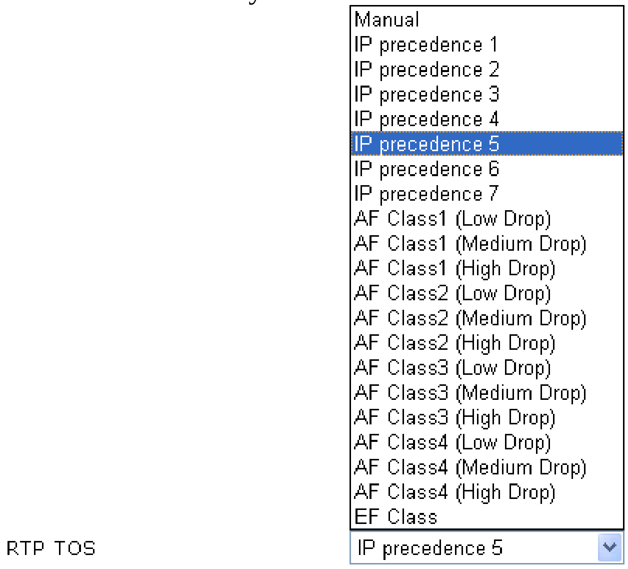
RTP **Symmetric RTP** – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.

Dynamic RTP port start - Specifies the start port for RTP stream.

The default value is 10050.

Dynamic RTP port end - Specifies the end port for RTP stream. The default value is 15000.

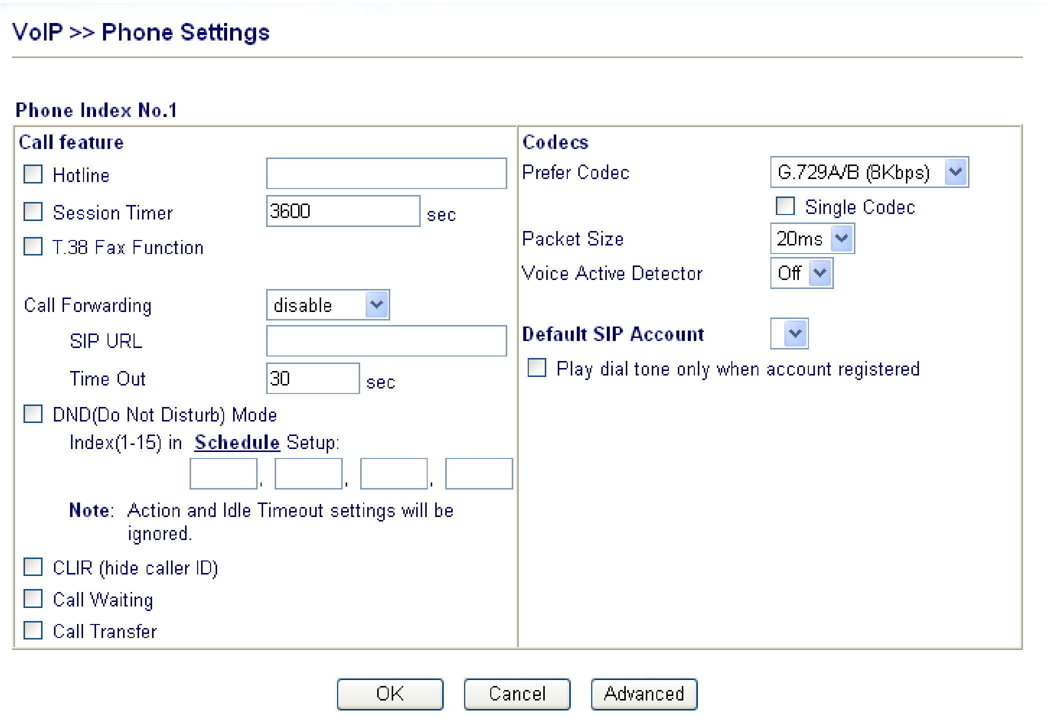
RTP TOS – It decides the level of VoIP package. Use the drop down list to choose any one of them.



Manual
IP precedence 1
IP precedence 2
IP precedence 3
IP precedence 4
IP precedence 5
IP precedence 6
IP precedence 7
AF Class1 (Low Drop)
AF Class1 (Medium Drop)
AF Class1 (High Drop)
AF Class2 (Low Drop)
AF Class2 (Medium Drop)
AF Class2 (High Drop)
AF Class3 (Low Drop)
AF Class3 (Medium Drop)
AF Class3 (High Drop)
AF Class4 (Low Drop)
AF Class4 (Medium Drop)
AF Class4 (High Drop)
EF Class

RTP TOS: IP precedence 5

Click the number **1** link under Index column, you can access into the following page for configuring Phone settings.



VoIP >> Phone Settings

Phone Index No.1

Call feature

□ Hotline
□ Session Timer: 3600 sec
□ T.38 Fax Function

Call Forwarding: disable
SIP URL:
Time Out: 30 sec

□ DND(Do Not Disturb) Mode
Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

□ CLIR (hide caller ID)
□ Call Waiting
□ Call Transfer

Codecs

Prefer Codec: G.729A/B (8Kbps)
□ Single Codec
Packet Size: 20ms
Voice Active Detector: Off

Default SIP Account:
□ Play dial tone only when account registered

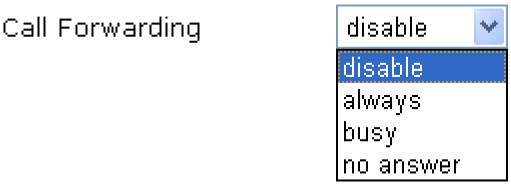
Hotline Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

Session Timer Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

T.38 Fax function If the remote end also supports FAX function, you can check this box to enable this function.

Call Forwarding

There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.



Call Forwarding disable

SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.
Time Out – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb) mode

Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.5.2 Schedule** for detailed configuration.

CLIR (hide caller ID)

Check this box to hide the caller ID on the display panel of the phone set for the remote side.

Call Waiting

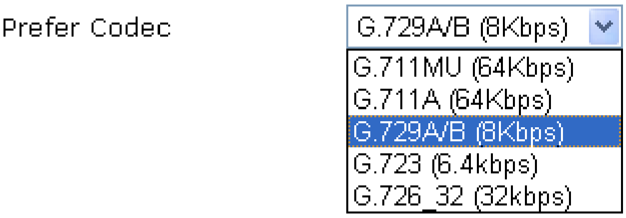
Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

Call Transfer

Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

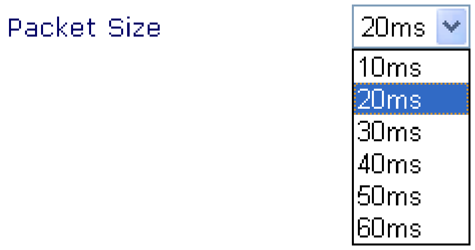
Prefer Codec

Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so many not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.



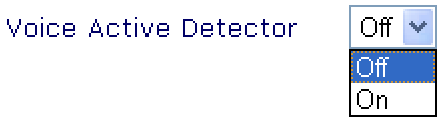
Prefer Codec G.729A/B (8Kbps)

Single Codec – If the box is checked, only the selected Codec will be applied.
Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.



Packet Size: 20ms

Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

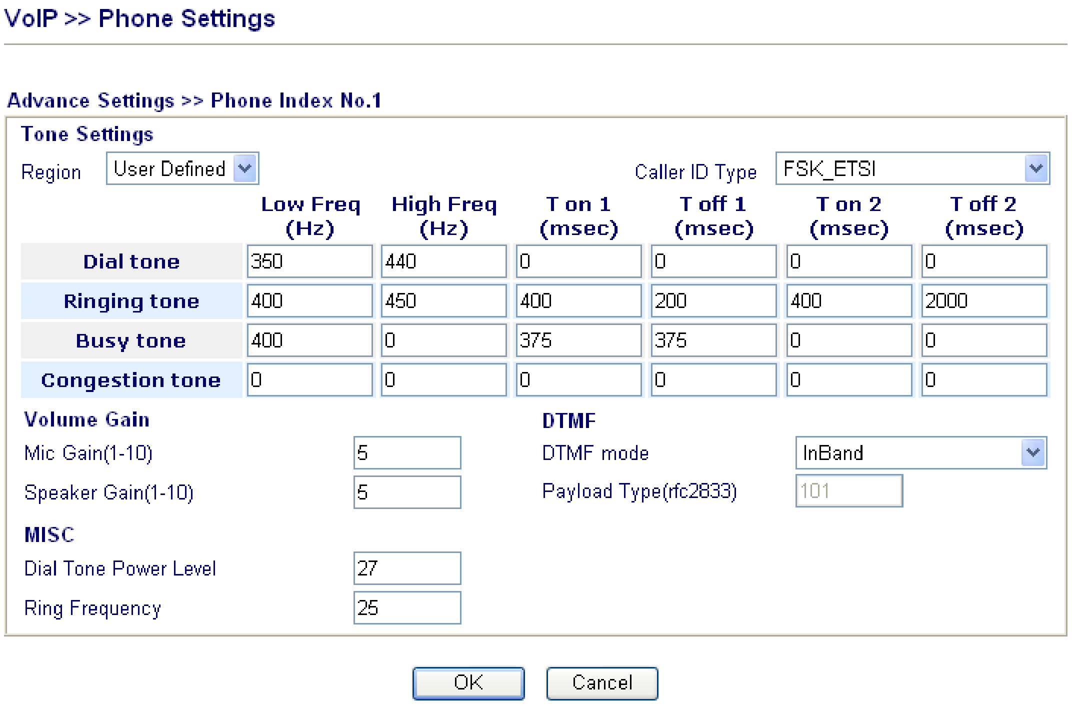


Voice Active Detector: Off

Default SIP Account There are six groups of SIP accounts that you can set. Use the drop down list to choose the profile name of the account as the default one.

Play dial tone only when account registered - Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.



VoIP >> Phone Settings

Advance Settings >> Phone Index No.1

Tone Settings

Region: User Defined

Caller ID Type: FSK_ETSI

	Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	350	440	0	0	0	0
Ringing tone	400	450	400	200	400	2000
Busy tone	400	0	375	375	0	0
Congestion tone	0	0	0	0	0	0

Volume Gain

Mic Gain(1-10): 5

Speaker Gain(1-10): 5

DTMF

DTMF mode: InBand

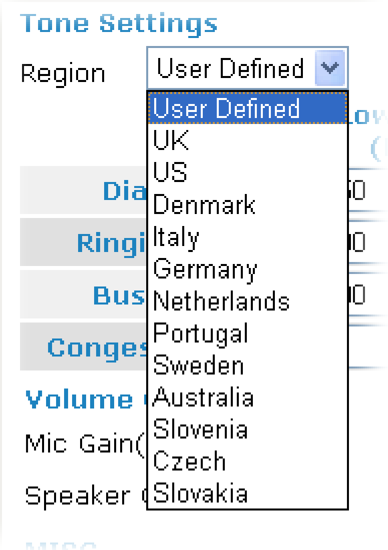
Payload Type(rfc2833): 101

MISC

Dial Tone Power Level: 27

Ring Frequency: 25

Region Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.



Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain

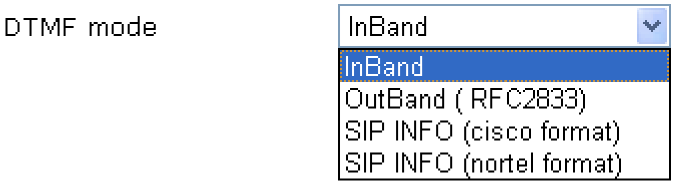
Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.

MISC

Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.

DTMP

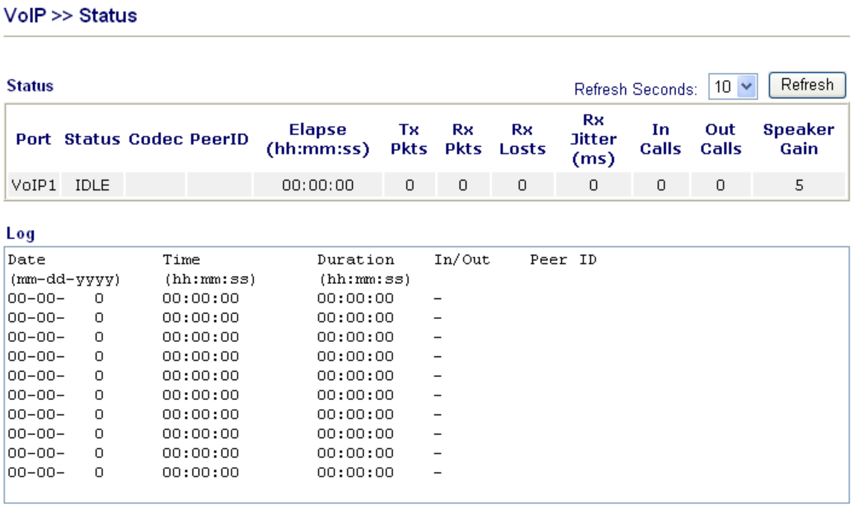
DTMF mode – There are four selections provided here:
InBand: Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone
OutBand: Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.
SIP INFO: Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.



Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

3.6.4 Status

On VoIP call status, you can find codec, connection and other important call status for both ports of VoIP 1 and 2.



VoIP >> Status

Status

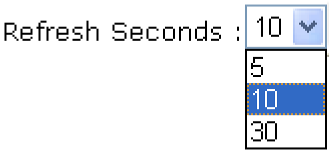
Refresh Seconds: 10 Refresh

Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
VoIP1	IDLE			00:00:00	0	0	0	0	0	0	5

Log

```
Date            Time            Duration     In/Out    Peer ID
(mm-dd-yyyy)    (hh:mm:ss)      (hh:mm:ss)
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
00-00-    0     00:00:00        00:00:00     -
```

Refresh Seconds Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.



Port It shows current connection status for the port of VoIP1.

Status It shows the VoIP connection status.
IDLE - Indicates that the VoIP function is idle.
HANG_UP - Indicates that the connection is not established (busy tone).
CONNECTING - Indicates that the user is calling out.
WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer.
ALERTING - Indicates that a call is coming.
ACTIVE-Indicates that the VoIP connection is launched.

Codec Indicates the voice codec employed by present channel.

PeerID The present in-call or out-call peer ID (the format may be IP or Domain).

Elapse Displays the duration of VoIP phone.

Tx Pkts Total number of transmitted voice packets during this connection session.

Rx Pkts Total number of received voice packets during this connection session.

Rx Losts Total number of lost packets during this connection session.

Rx Jitter The jitter of received voice packets.

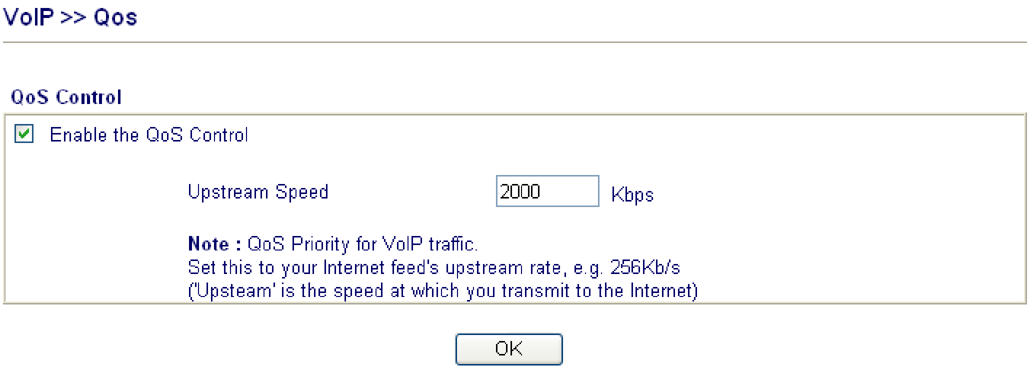
In Calls The accumulating times of in-call.

Out Calls The accumulating times of out-call.

Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.6.5 QoS

This setting allows you to set upstream to have high priority for VoIP call.



VoIP >> Qos

QoS Control

☑ Enable the QoS Control

Upstream Speed 2000 Kbps

Note : QoS Priority for VoIP traffic.
Set this to your Internet feed's upstream rate, e.g. 256Kb/s
('Upsteam' is the speed at which you transmit to the Internet)

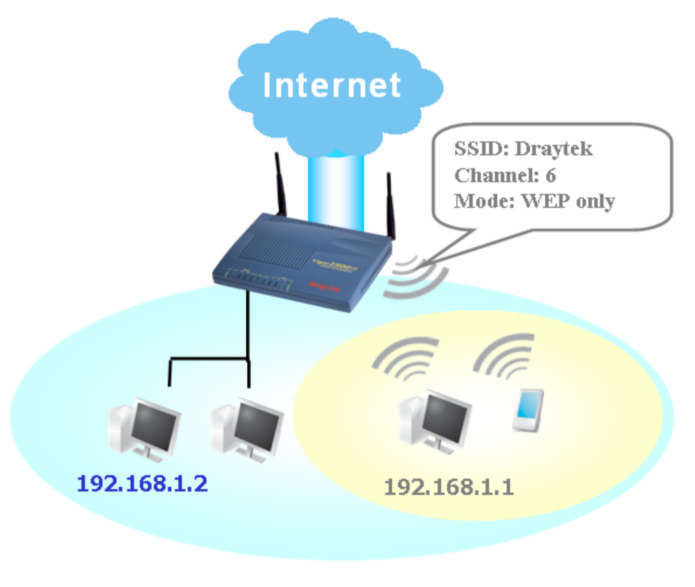
3.7 Wireless LAN

Note: This function is used for *G* models only.

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 G 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.

3.7.1 Basic Concept

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 with other wired hosts 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.

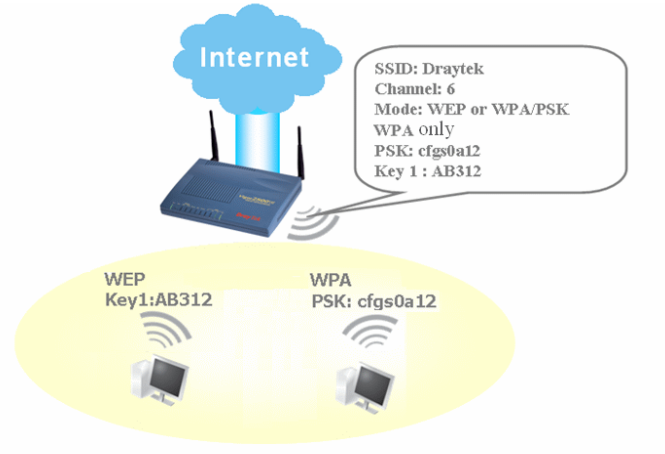
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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.

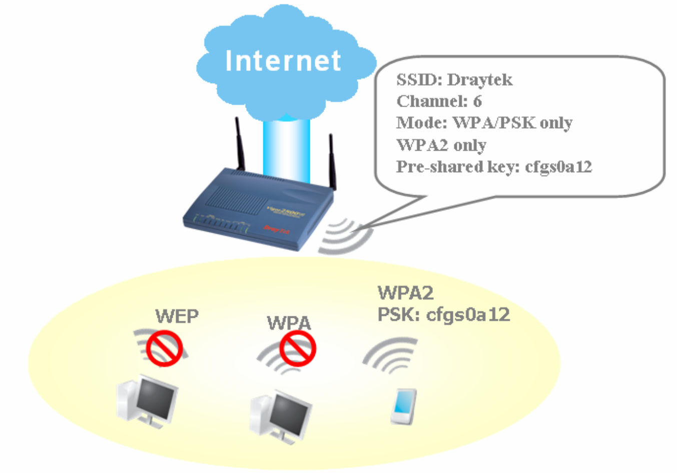
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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.

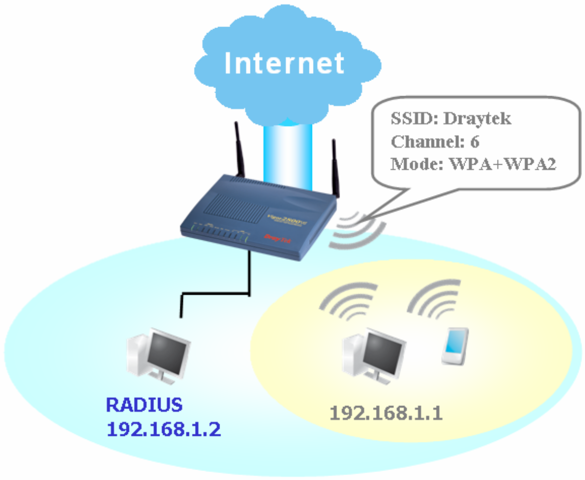
Example 1



Example 2



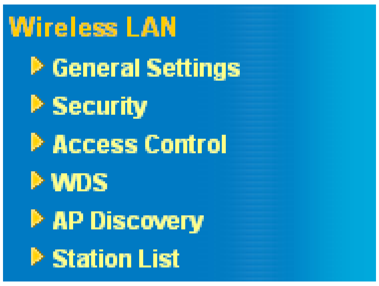
Example 3



Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add a filter of MAC address to isolate single user's access from wired LAN.

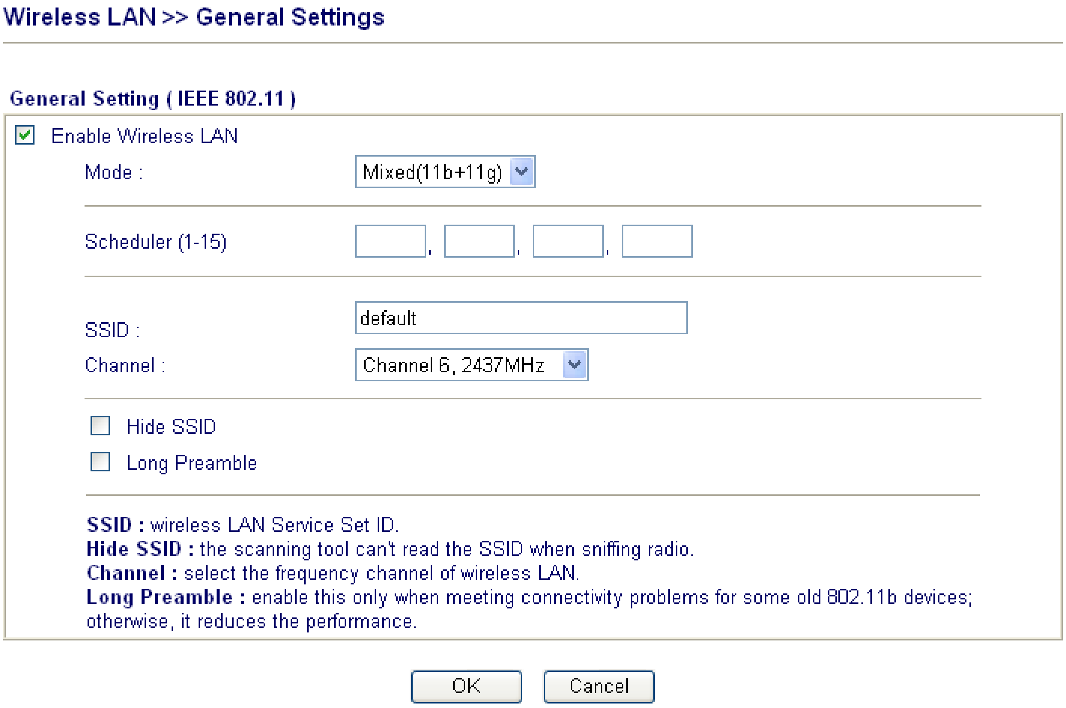
Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items of Wireless LAN.



3.7.2 General Settings

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.



Wireless LAN >> General Settings

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

Mode : Mixed(11b+11g)

Scheduler (1-15) ___, ___, ___, ___

SSID : default

Channel : Channel 6, 2437MHz

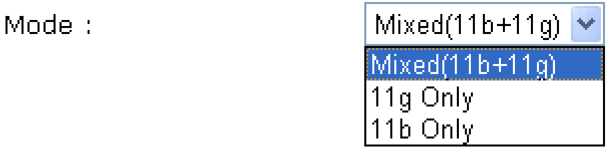
□ Hide SSID

□ Long Preamble

SSID : wireless LAN Service Set ID.
Hide SSID : the scanning tool can't read the SSID when sniffing radio.
Channel : select the frequency channel of wireless LAN.
Long Preamble : enable this only when meeting connectivity problems for some old 802.11b devices; otherwise, it reduces the performance.

Enable Wireless LAN	Check the box to enable wireless function.
Mode	Select an appropriate wireless mode. ***Mixed (11b+11g)***-The router communicates with standard 802.11b and standard 802.11g STAs simultaneously. ***11g only***-The router communicates with standard 802.11b STAs.

11b only-The router communicates with standard 802.11b STAs.



Mode : Mixed(11b+11g)

Scheduler (1-15)

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

SSID

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

Channel

Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.

Hide SSID

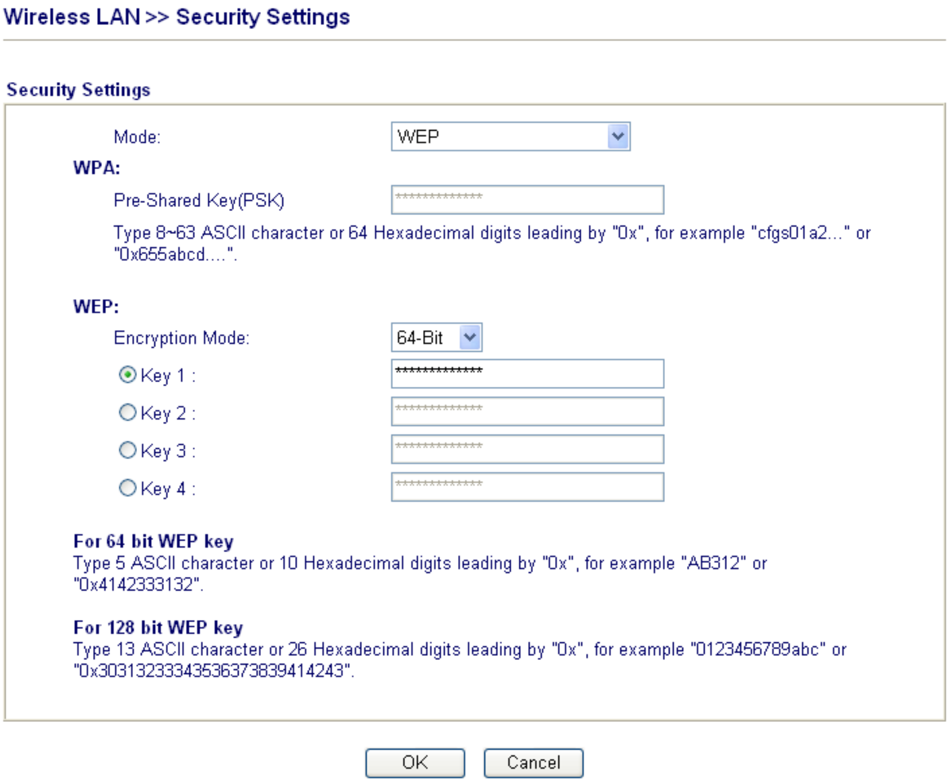
Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while doing site survey.

Long Preamble

This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network device only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

3.7.3 Security

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



Wireless LAN >> Security Settings

Security Settings

Mode: WEP

WPA:

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

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

WEP:

Encryption Mode: 64-Bit

● Key 1 : **************

○ Key 2 : **************

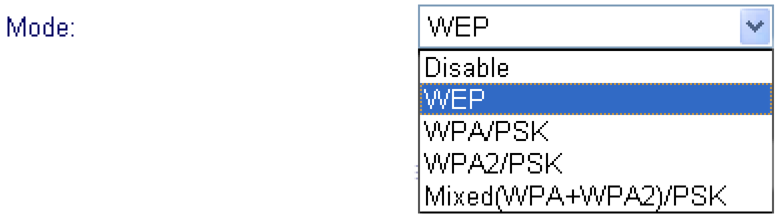
○ Key 3 : **************

○ Key 4 : **************

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

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

Mode **Disable**-Turn off the encryption mechanism. For the security of your router, please select any one of the encryption mode here.
WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.
WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.
WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.
Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.



Mode: WEP

WPA The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

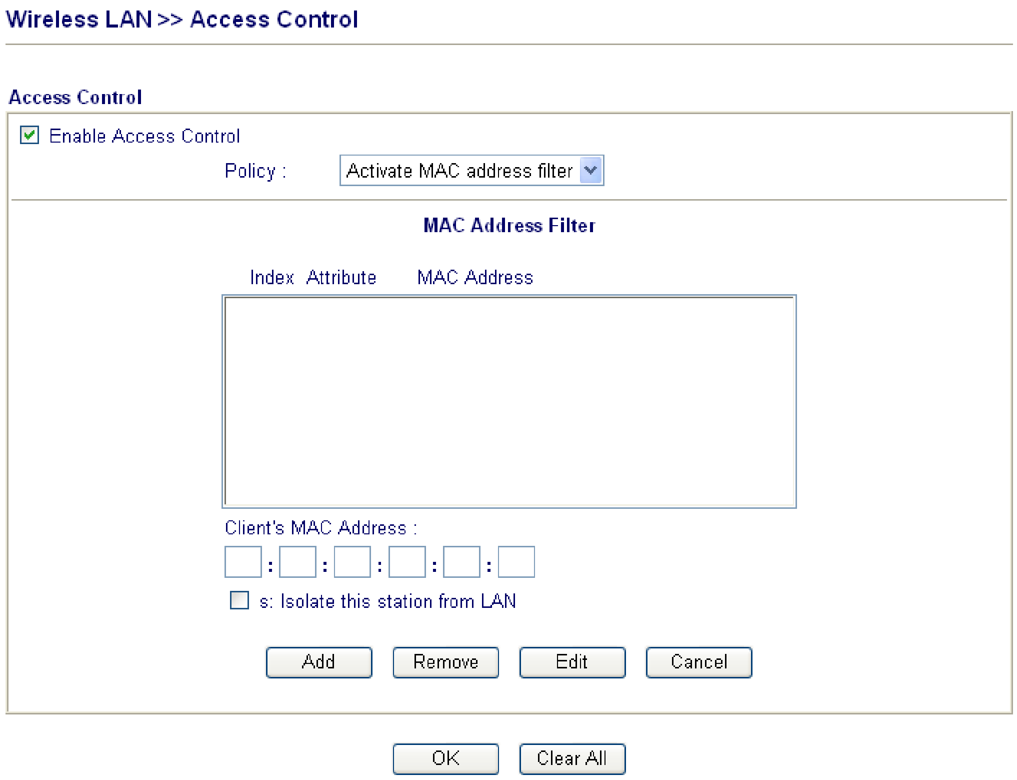
WEP **For key length 64 bits -** For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

For key length 128 bits - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM. (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D)

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

3.7.4 Access Control

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



Wireless LAN >> Access Control

Access Control

☑ Enable Access Control

Policy : Activate MAC address filter

MAC Address Filter

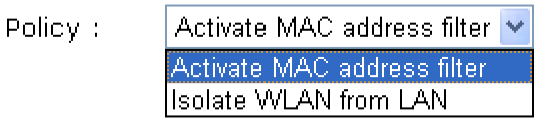
Index	Attribute	MAC Address

Client's MAC Address : □ : □ : □ : □ : □ : □

□ s: Isolate this station from LAN

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

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



Policy : Activate MAC address filter

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

s Check this box to isolate the stations from LAN.

Add Add a new MAC address into the list.

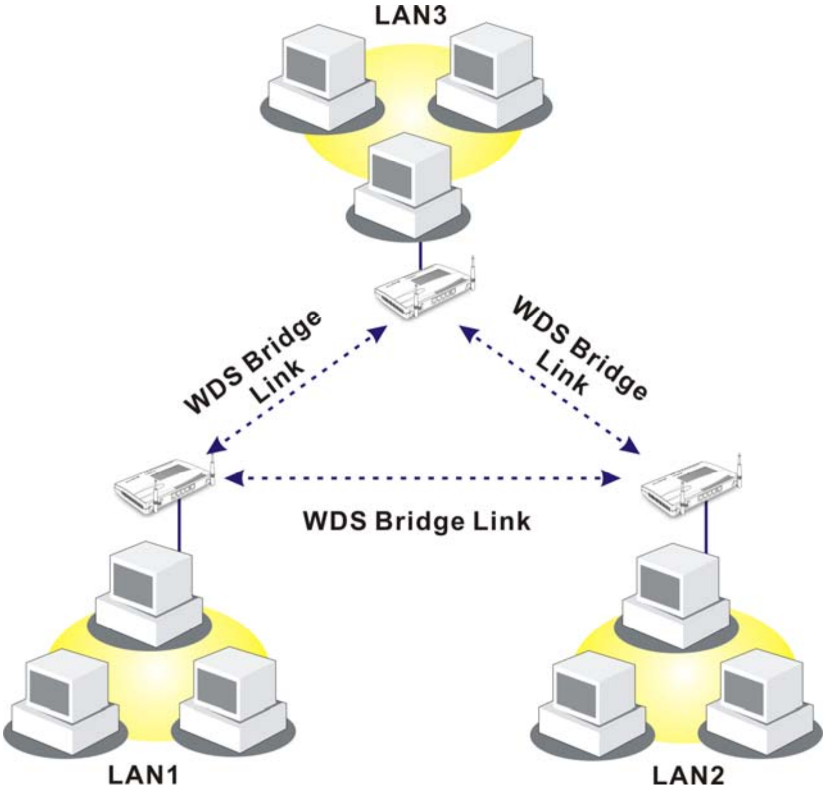
Remove	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.7.5 WDS

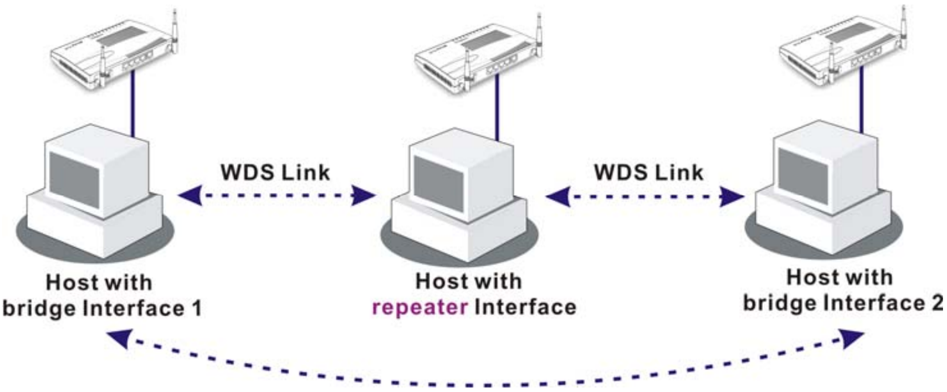
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

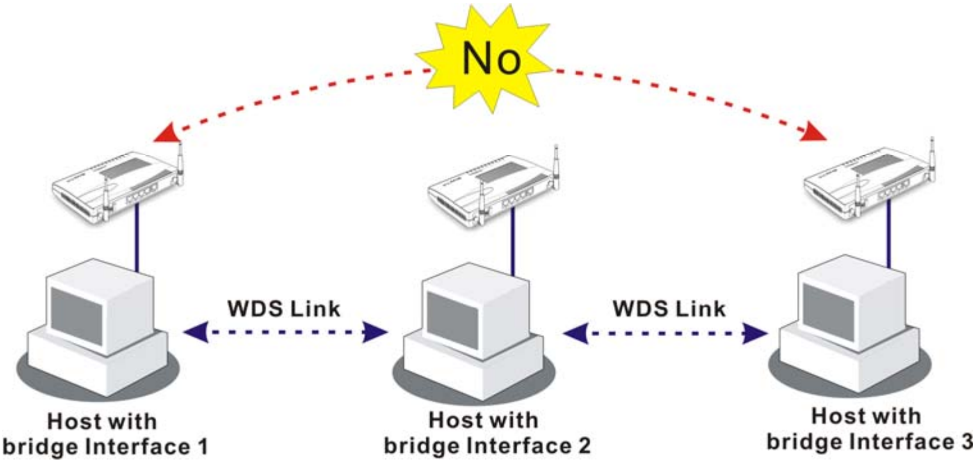


The application for the WDS-Repeater mode is depicted as below:

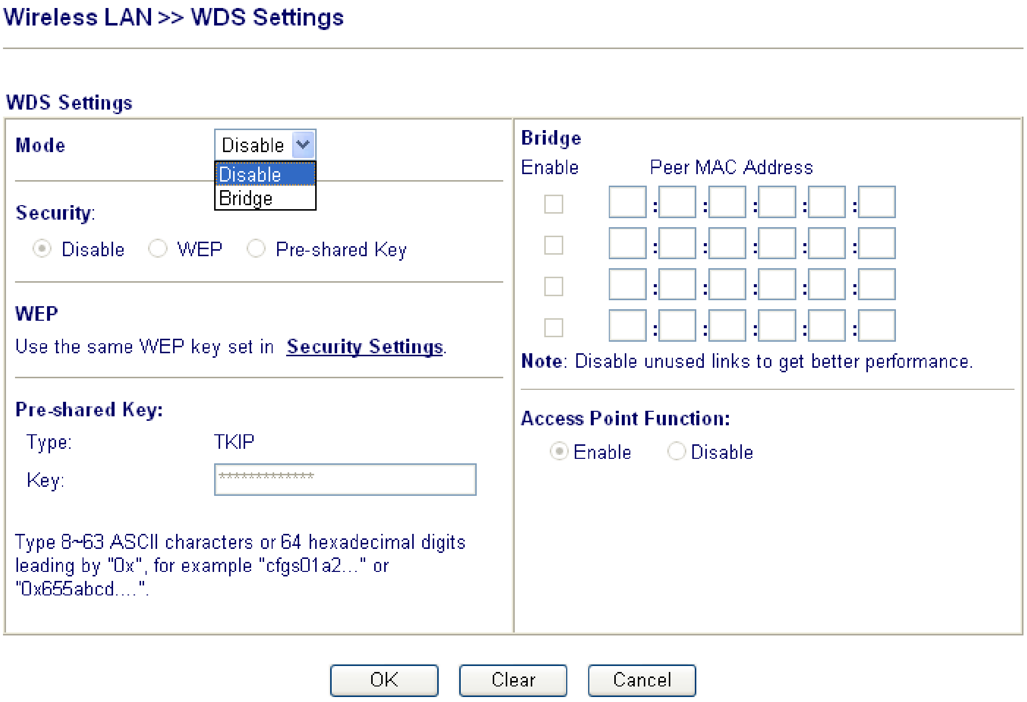

WDS Link
WDS Link
Host with bridge Interface 1
Host with repeater Interface
Host with bridge Interface 2

The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.


No
WDS Link
WDS Link
Host with bridge Interface 1
Host with bridge Interface 2
Host with bridge Interface 3

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



Wireless LAN >> WDS Settings

WDS Settings

Mode: Disable (Disable / Bridge)

Security: ● Disable ○ WEP ○ Pre-shared Key

WEP
Use the same WEP key set in Security Settings.

Pre-shared Key:
Type: TKIP
Key: **************

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

Bridge

Enable	Peer MAC Address
□	[ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□	[ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□	[ ]:[ ]:[ ]:[ ]:[ ]:[ ]
□	[ ]:[ ]:[ ]:[ ]:[ ]:[ ]

Note: Disable unused links to get better performance.

Access Point Function: ● Enable ○ Disable

Mode Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting.

Security There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.

WEP Check this box to use the same key set in **Security Settings** page. If you did not set any key in **Security Settings** page, this check box will be dimmed.

Settings **Encryption Mode -** If you checked the box of **Use the same WEP key …**, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page.
Key Index - Choose the key that you want to use after selecting the proper encryption mode.
Key - Type the content for the key.

Pre-shared Key Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.

Bridge If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. **Six** peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.

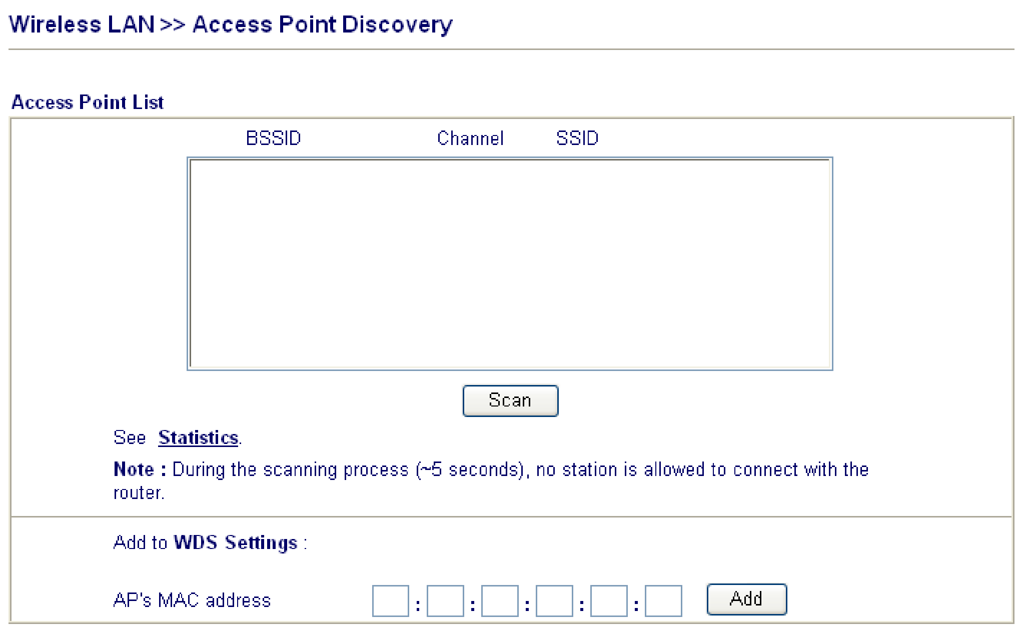
Access Point Function Click **Enable** to make this router serving as an access point; click **Disable** to cancel this function.

Status It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.

3.7.6 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.



Wireless LAN >> Access Point Discovery

Access Point List

BSSID	Channel	SSID

See **Statistics**.

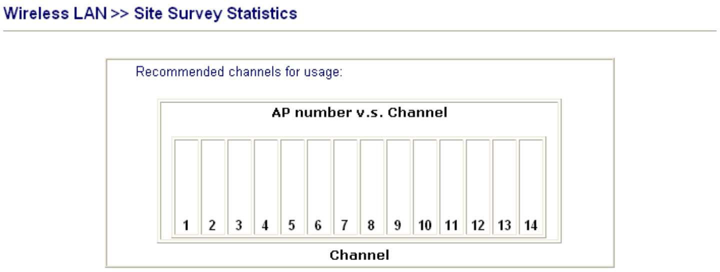
Note : During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to **WDS Settings** :

AP's MAC address : : : : :

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

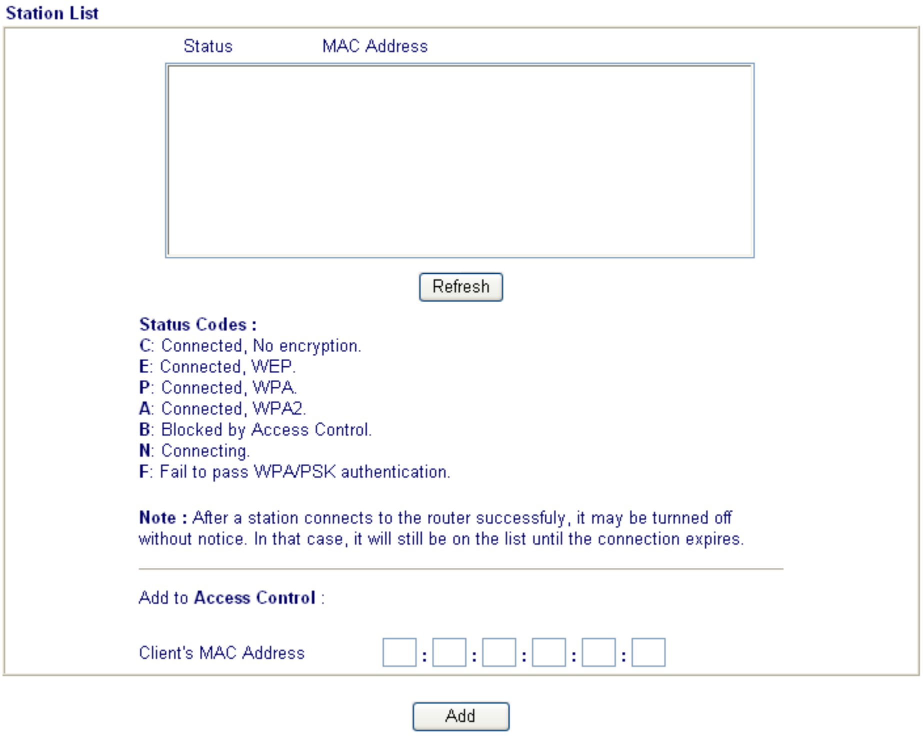
Statistics It displays the statistics for the channels used by APs.


Wireless LAN >> Site Survey Statistics
Recommended channels for usage:
AP number v.s. Channel
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Channel

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

3.7.7 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.



Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Note : After a station connects to the router successfuly, it may be turnned off without notice. In that case, it will still be on the list until the connection expires.

Add to **Access Control** :

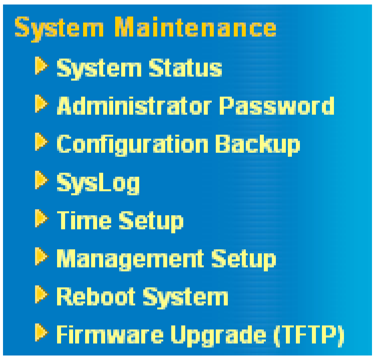
Client's MAC Address □ : □ : □ : □ : □ : □

Refresh Click this button to refresh the status of station list.

Add Click this button to add current selected MAC address into **Access Contro**l.

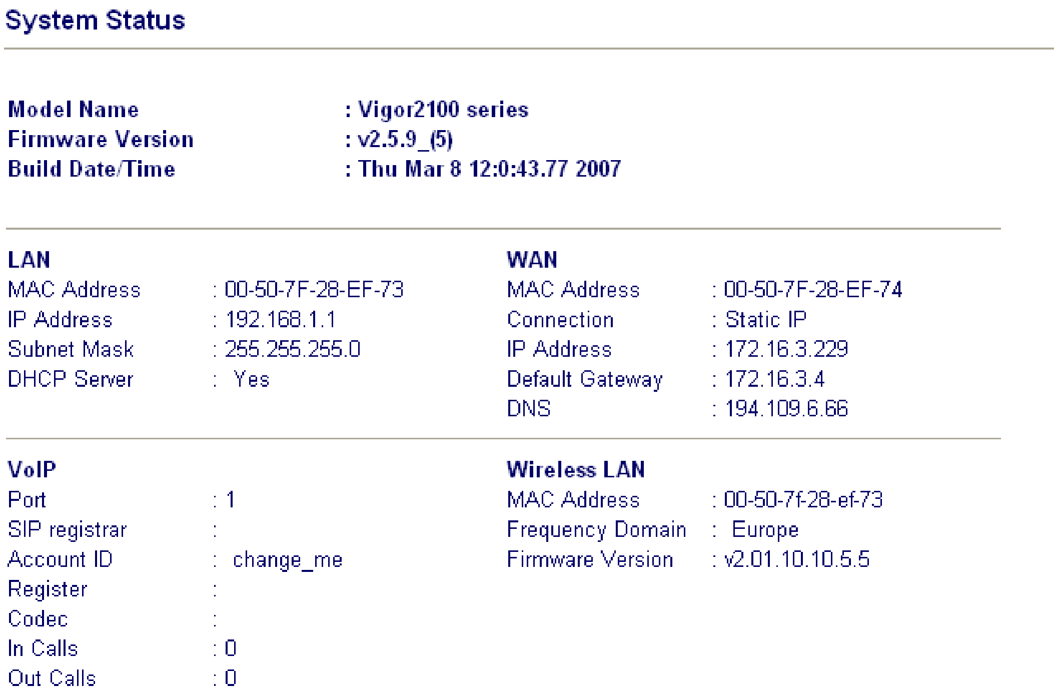
3.8 System Maintenance

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



3.8.1 System Status

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



System Status

Model Name : Vigor2100 series
Firmware Version : v2.5.9_(5)
Build Date/Time : Thu Mar 8 12:0:43.77 2007

LAN
MAC Address : 00-50-7F-28-EF-73
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DHCP Server : Yes

WAN
MAC Address : 00-50-7F-28-EF-74
Connection : Static IP
IP Address : 172.16.3.229
Default Gateway : 172.16.3.4
DNS : 194.109.6.66

VoIP
Port : 1
SIP registrar :
Account ID : change_me
Register :
Codec :
In Calls : 0
Out Calls : 0

Wireless LAN
MAC Address : 00-50-7f-28-ef-73
Frequency Domain : Europe
Firmware Version : v2.01.10.10.5.5

Model Name Displays the model name of the router.

Firmware Version Displays the firmware version of the router.

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

MAC Address Displays the MAC address of the LAN Interface.

IP Address Displays the IP address of the LAN interface.

Subnet Mask Displays the subnet mask address of the LAN interface.

DHCP Server Displays the current status of DHCP server of the LAN interface.

MAC Address Displays the MAC address of the WAN Interface.

IP Address Displays the IP address of the WAN interface.

Connection Displays the connection mode of WAN interface.

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

DNS Displays the assigned IP address of the primary DNS.

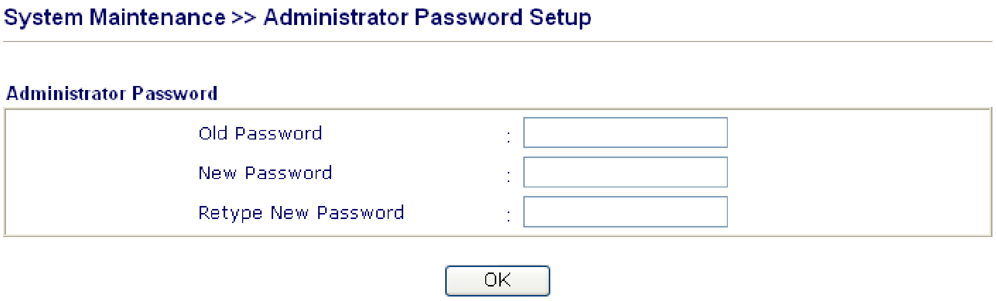
MAC Address Displays the MAC address of the wireless Interface.

Frequency Domain Displays the available channel supported by the wireless product. It varies in different country, Europe (13 usable channels), USA (11 usable channels).

Firmware Version Displays information about equipped WLAN card driver.

3.8.2 Administrator Password

This page allows you to set new password.



System Maintenance >> Administrator Password Setup

Administrator Password

Old Password :

New Password :

Retype New Password :

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

New Password Type in new password in this filed.

Retype New Password Type in the new password again.

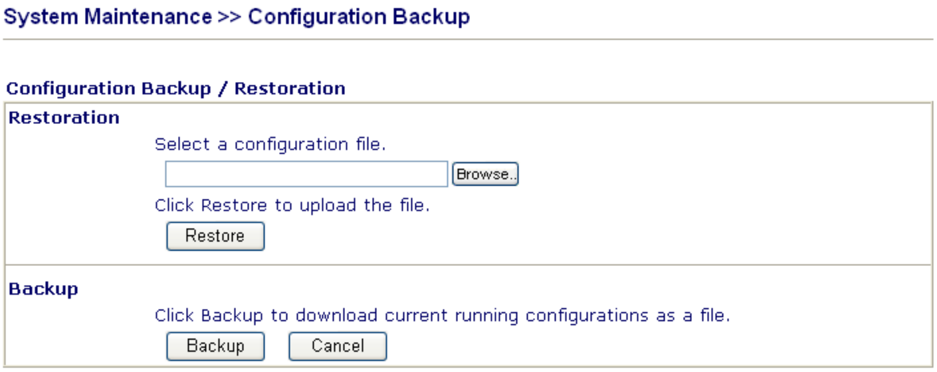
When you click **OK**, the login window will appear. Please use the new password to access into the web configurator again.

3.8.3 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

Restoration

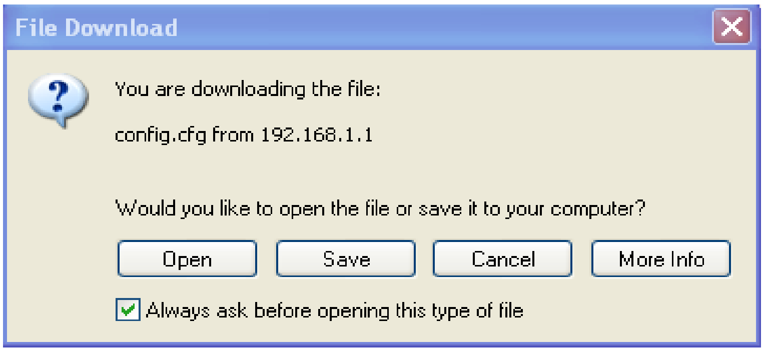
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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



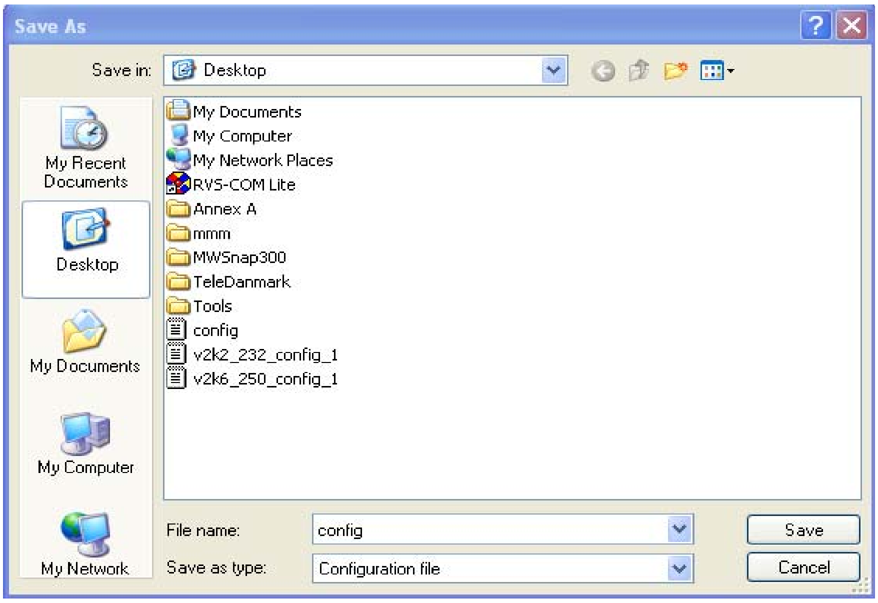
File Download

You are downloading the file:

config.cfg from 192.168.1.1

Would you like to open the file or save it to your computer?

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



Save As

Save in: Desktop

File name: config

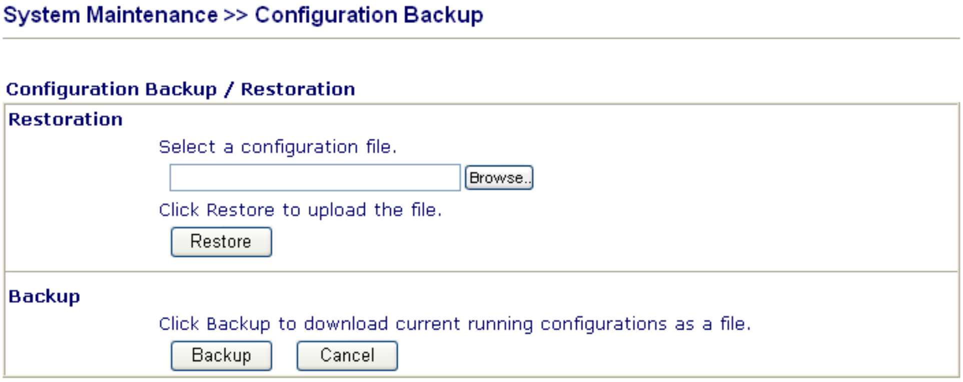
Save as type: Configuration file

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

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

Restore Configuration

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


System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Click Restore to upload the file.

Backup

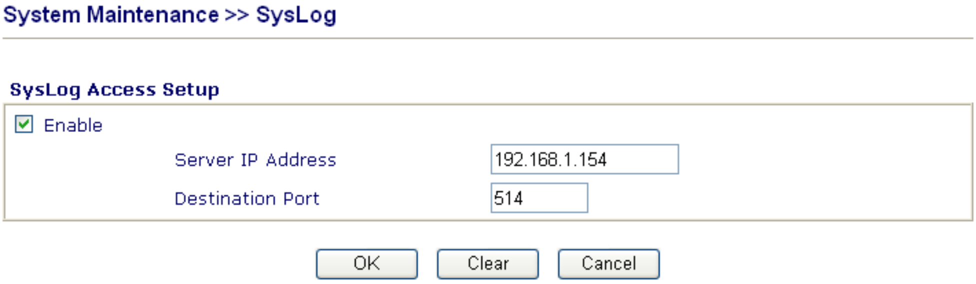
Click Backup to download current running configurations as a file.

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

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

3.8.4 Syslog

SysLog function is provided to help 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

SysLog Access Setup

☑ Enable

Server IP Address 192.168.1.154

Destination Port 514

Enable Check "**Enable**" to activate this function.

Server IP Address The IP address of the Syslog server.

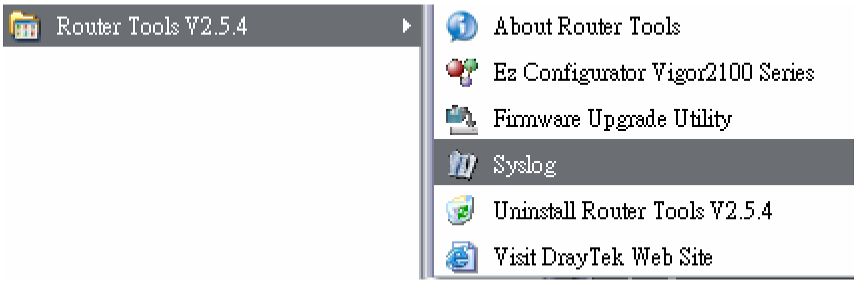
Destination Port Assign a port for the Syslog protocol.

Click **OK** to save these settings.

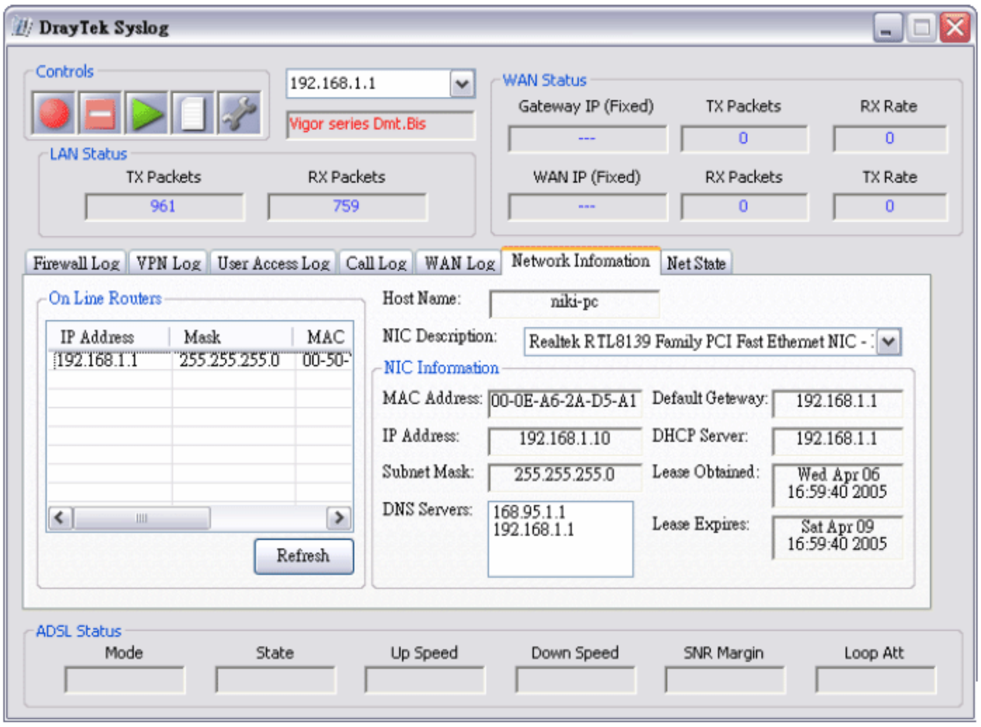
For viewing the Syslog, please do the following:

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.



192.168.1.1

Vigor series Dmt.Bis

LAN Status: TX Packets 961, RX Packets 759

WAN Status: Gateway IP (Fixed) ---, TX Packets 0, RX Rate 0; WAN IP (Fixed) ---, RX Packets 0, TX Rate 0

IP Address	Mask	MAC
192.168.1.1	255.255.255.0	00-50-

Host Name: niki-pc

NIC Description: Realtek RTL8139 Family PCI Fast Ethernet NIC -

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

Default Geteway: 192.168.1.1

IP Address: 192.168.1.10

DHCP Server: 192.168.1.1

Subnet Mask: 255.255.255.0

Lease Obtained: Wed Apr 06 16:59:40 2005

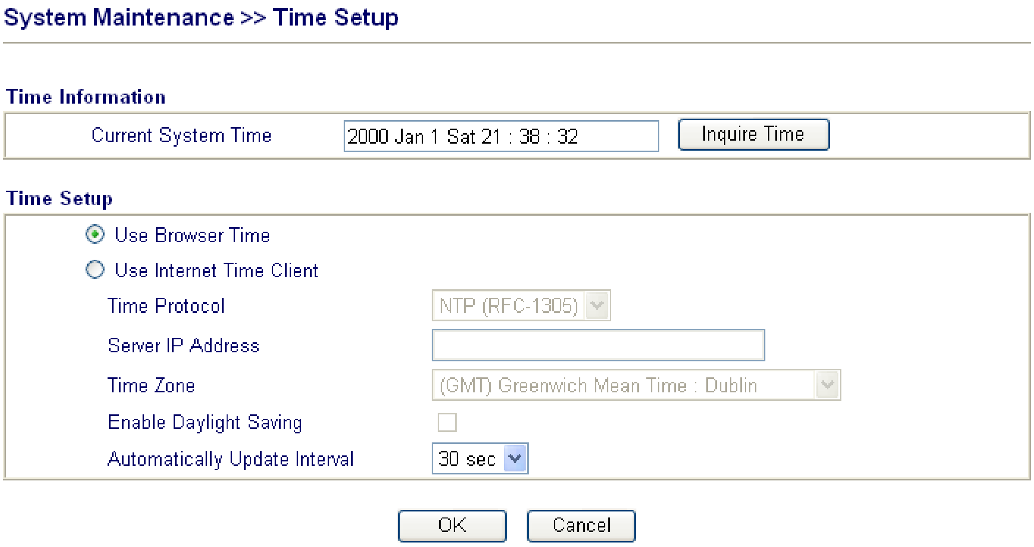
DNS Servers: 168.95.1.1 192.168.1.1

Lease Expires: Sat Apr 09 16:59:40 2005

ADSL Status: Mode, State, Up Speed, Down Speed, SNR Margin, Loop Att

3.8.5 Time Setup

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



System Maintenance >> Time Setup

Time Information

Current System Time: 2000 Jan 1 Sat 21 : 38 : 32

Time Setup

● Use Browser Time

○ Use Internet Time Client

Time Protocol: NTP (RFC-1305)

Server IP Address:

Time Zone: (GMT) Greenwich Mean Time : Dublin

Enable Daylight Saving: □

Automatically Update Interval: 30 sec

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

Use Browser Time Select this option to use the browser time from the remote administrator PC host as router's system time.

Use Internet Time Client Select to inquire time information from Time Server on the Internet using assigned protocol.

Time Protocol Select a time protocol.

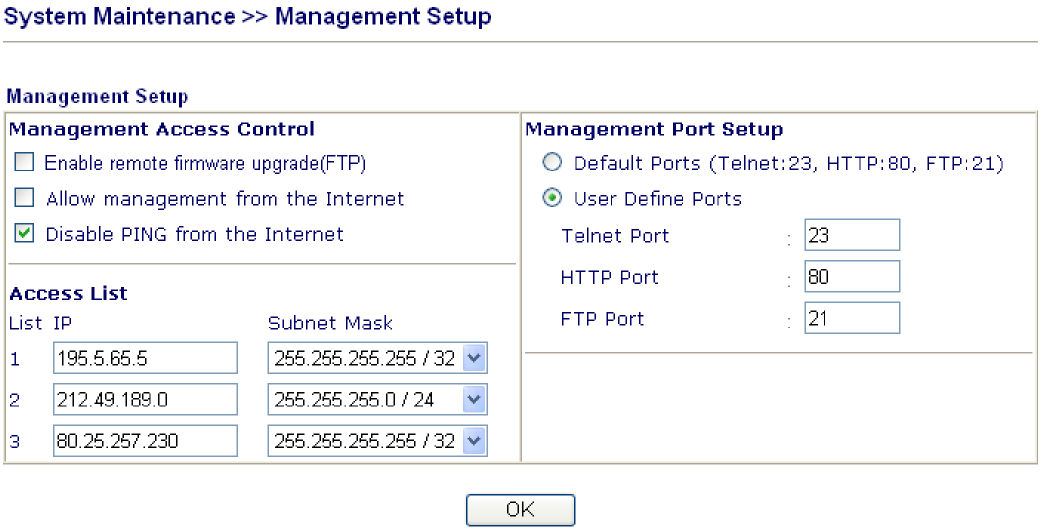
Server IP Address Type the IP address of the time server.

Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check this box to invoke daylight saving function.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.8.6 Management Setup

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



System Maintenance >> Management Setup

Management Setup

Management Access Control

□ Enable remote firmware upgrade(FTP)

□ Allow management from the Internet

☑ Disable PING from the Internet

Access List

List	IP	Subnet Mask
1	195.5.65.5	255.255.255.255 / 32
2	212.49.189.0	255.255.255.0 / 24
3	80.25.257.230	255.255.255.255 / 32

Management Port Setup

○ Default Ports (Telnet:23, HTTP:80, FTP:21)

● User Define Ports

Telnet Port : 23

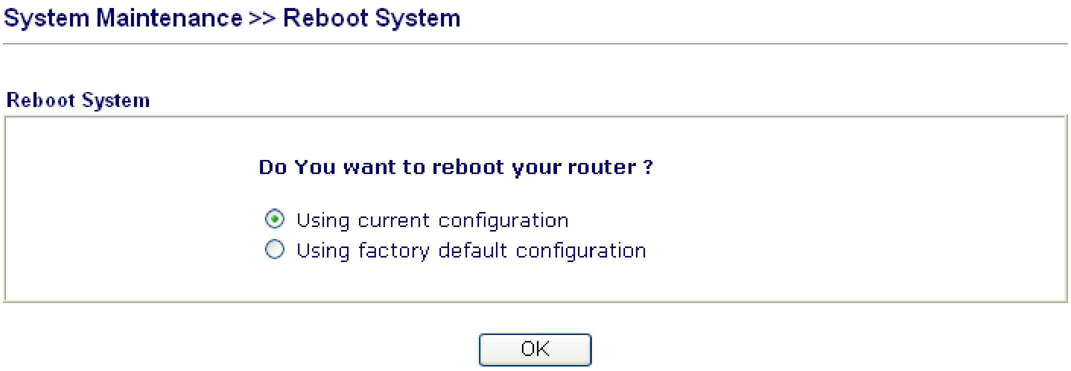
HTTP Port : 80

FTP Port : 21

Enable remote firmware upgrade	Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP -** Indicate an IP address allowed to login to the router. **Subnet Mask -** Represent a subnet mask allowed to login to the router.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet and HTTP servers.

3.8.7 Reboot System

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



System Maintenance >> Reboot System

Reboot System

Do You want to reboot your router ?

● Using current configuration
○ Using factory default configuration

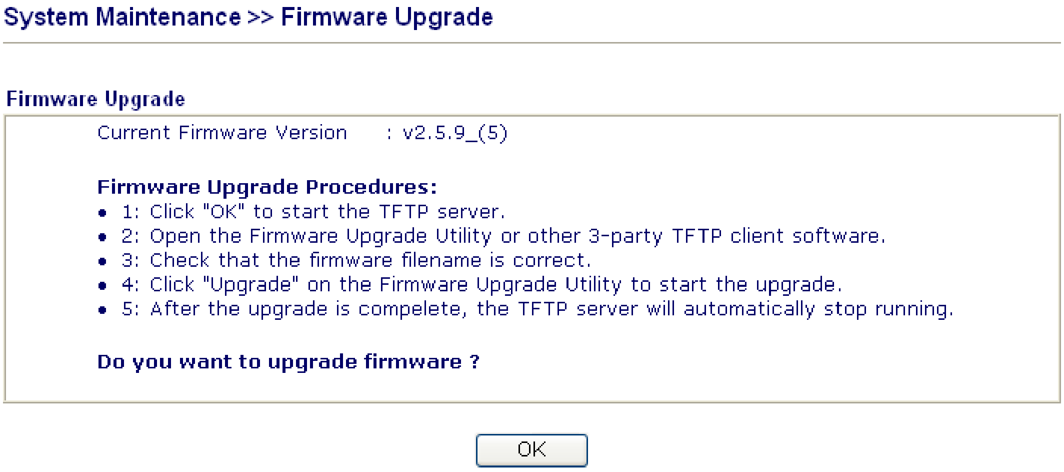
If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

3.8.8 Firmware Upgrade

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

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

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



System Maintenance >> Firmware Upgrade

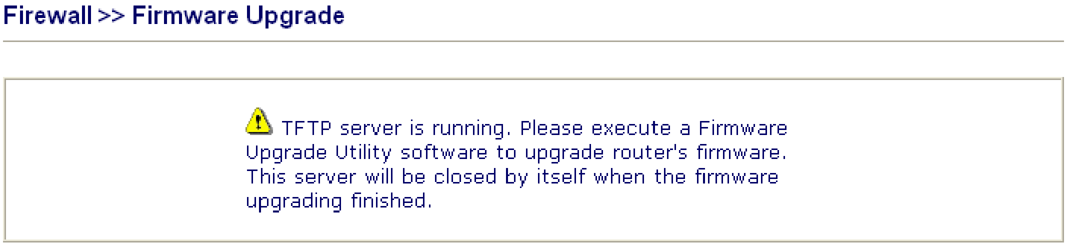
Firmware Upgrade

Current Firmware Version : v2.5.9_(5)

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

Do you want to upgrade firmware ?

Click **OK**. The following screen will appear.



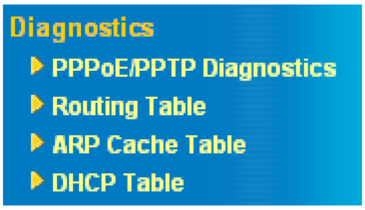
Firewall >> Firmware Upgrade

⚠ TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

For the detailed information about firmware update, please go to Chapter 4.

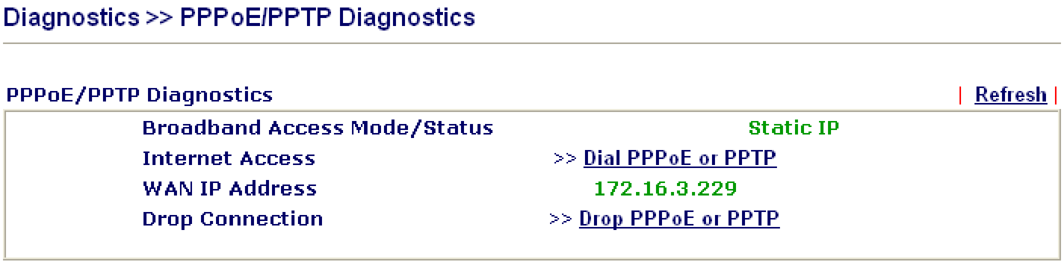
3.9 Diagnostics

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



3.9.1 PPPoE/PPTP Diagnostics

Click **Diagnostics** and click **PPPoE/PPTP Diagnostic**s to open the web page.



Diagnostics >> PPPoE/PPTP Diagnostics

PPPoE/PPTP Diagnostics | Refresh |

Broadband Access Mode/Status	Static IP
Internet Access	>> Dial PPPoE or PPTP
WAN IP Address	172.16.3.229
Drop Connection	>> Drop PPPoE or PPTP

Refresh To obtain the latest information, click here to reload the page.

Broadband Access Mode/Status Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show "---".

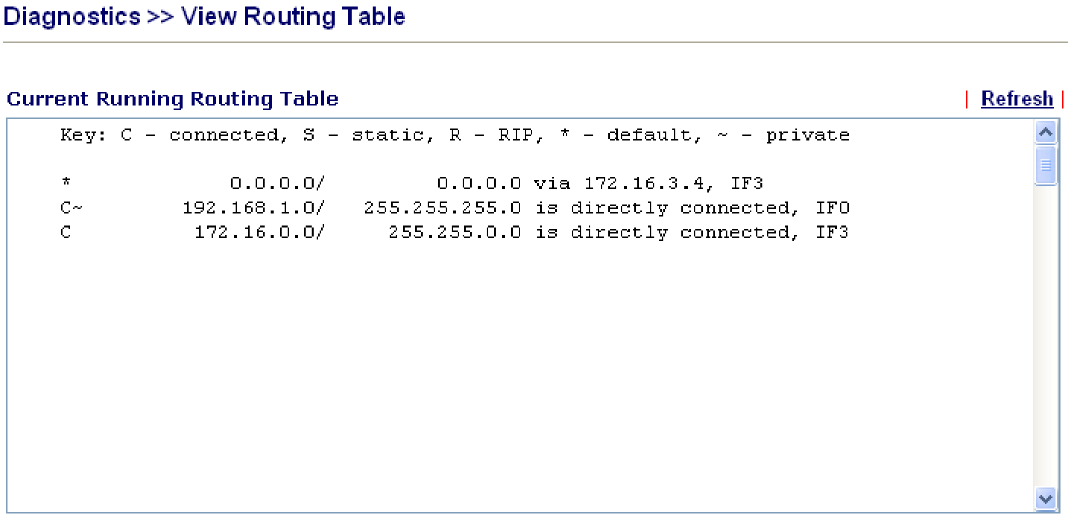
WAN IP Address The WAN IP address for the active connection.

Dial PPPoE or PPPT Click it to force the router to establish a PPPoE or PPPoA connection.

Drop PPPoE or PPTP Click it to force the router to cut off a PPPoE or PPPoA connection.

3.9.2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.



Diagnostics >> View Routing Table

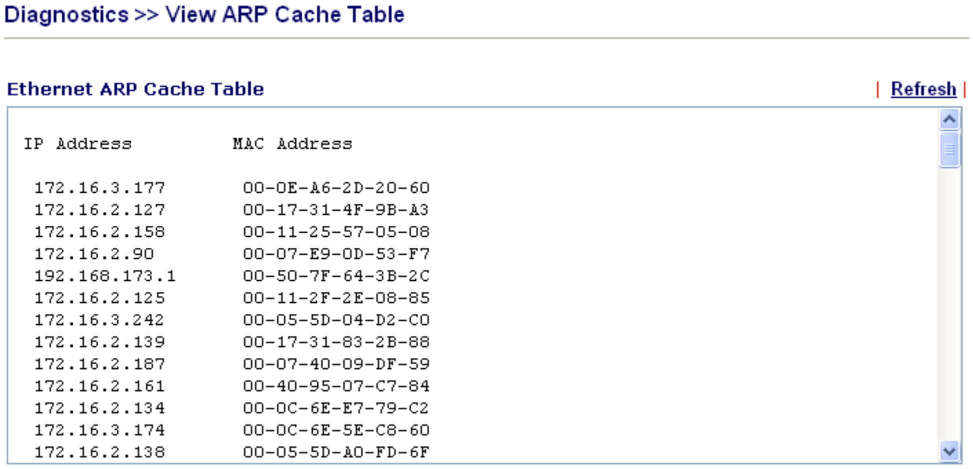
Current Running Routing Table | Refresh |

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

*              0.0.0.0/          0.0.0.0 via 172.16.3.4, IF3
C~           192.168.1.0/    255.255.255.0 is directly connected, IF0
C             172.16.0.0/      255.255.0.0 is directly connected, IF3
```

Refresh Click it to reload the page.

3.9.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



Diagnostics >> View ARP Cache Table

Ethernet ARP Cache Table | Refresh |

```
IP Address          MAC Address

 172.16.3.177        00-0E-A6-2D-20-60
 172.16.2.127        00-17-31-4F-9B-A3
 172.16.2.158        00-11-25-57-05-08
 172.16.2.90         00-07-E9-0D-53-F7
 192.168.173.1       00-50-7F-64-3B-2C
 172.16.2.125        00-11-2F-2E-08-85
 172.16.3.242        00-05-5D-04-D2-C0
 172.16.2.139        00-17-31-83-2B-88
 172.16.2.187        00-07-40-09-DF-59
 172.16.2.161        00-40-95-07-C7-84
 172.16.2.134        00-0C-6E-E7-79-C2
 172.16.3.174        00-0C-6E-5E-C8-60
 172.16.2.138        00-05-5D-A0-FD-6F
```

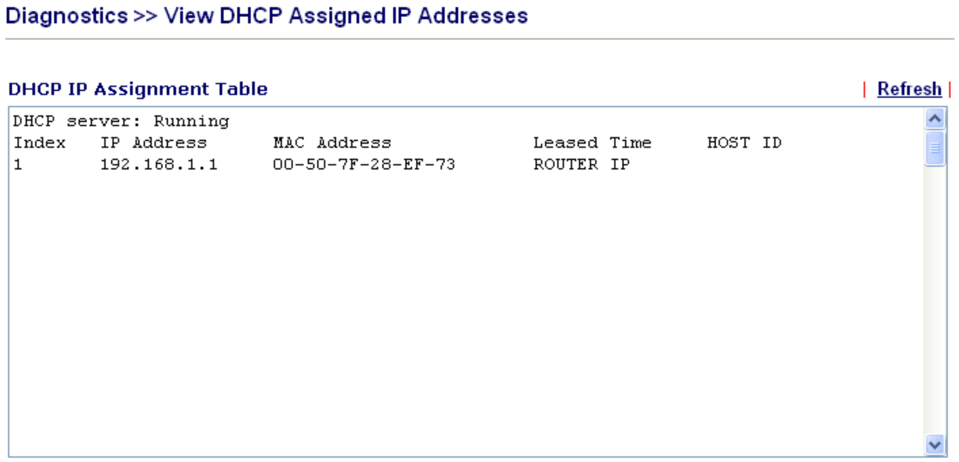
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

3.9.4 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.



Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table | Refresh |

```
DHCP server: Running
Index    IP Address      MAC Address               Leased Time     HOST ID
1        192.168.1.1     00-50-7F-28-EF-73         ROUTER IP
```

Index It displays the connection item number.

IP Address It displays the IP address assigned by this router for specified PC.

MAC Address It displays the MAC address for the specified PC that DHCP assigned IP address for it.

Leased Time It displays the leased time of the specified PC.

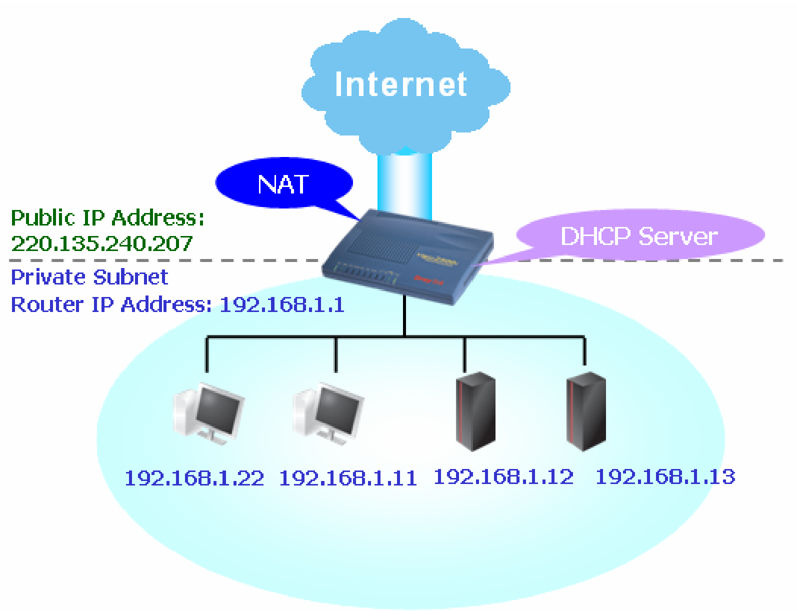
HOST ID It displays the host ID name of the specified PC.

Refresh Click it to reload the page.

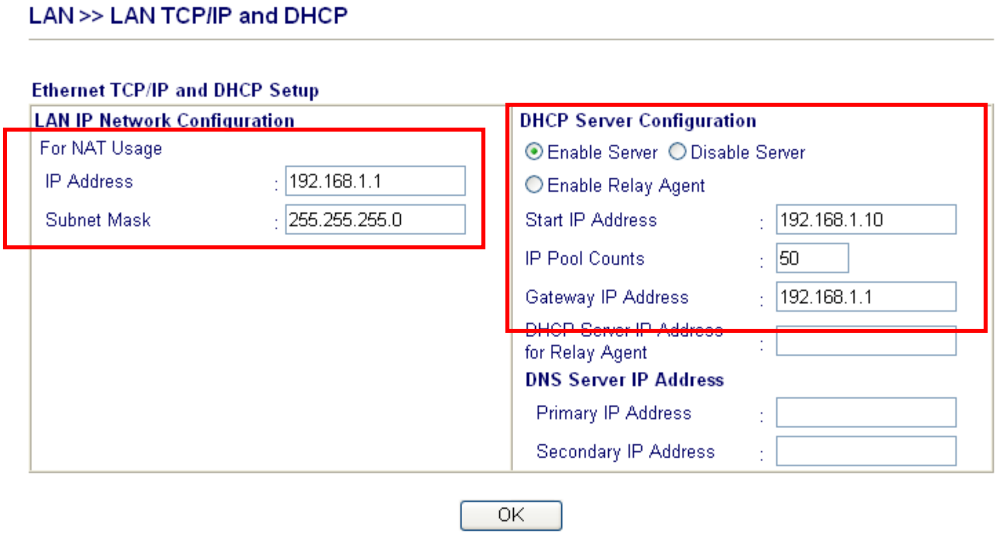
4 Application and Examples

4.1 LAN – Created by Using NAT

An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



LAN >> LAN TCP/IP and DHCP

Ethernet TCP/IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server Configuration

● Enable Server ○ Disable Server

○ Enable Relay Agent

Start IP Address : 192.168.1.10

IP Pool Counts : 50

Gateway IP Address : 192.168.1.1

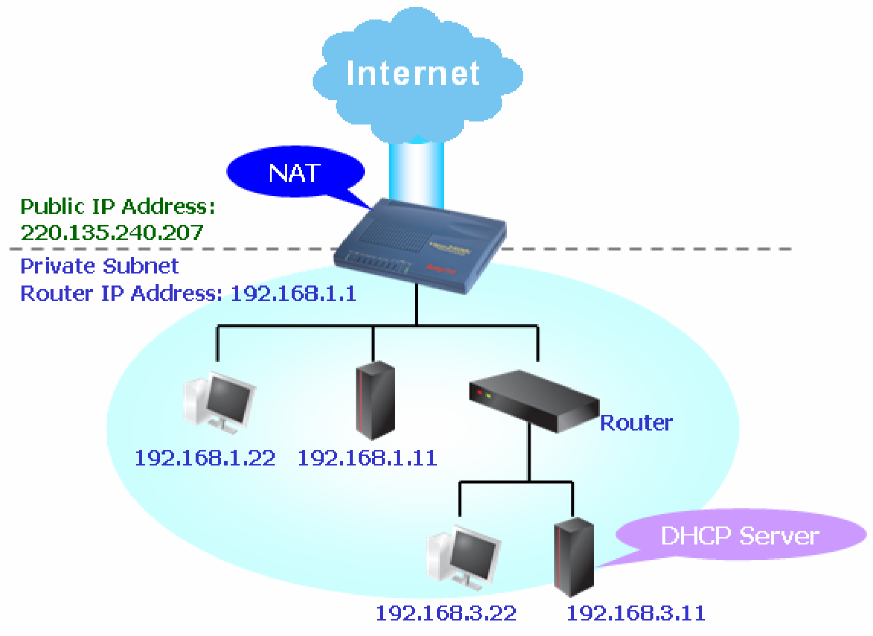
DHCP Server IP Address for Relay Agent :

DNS Server IP Address

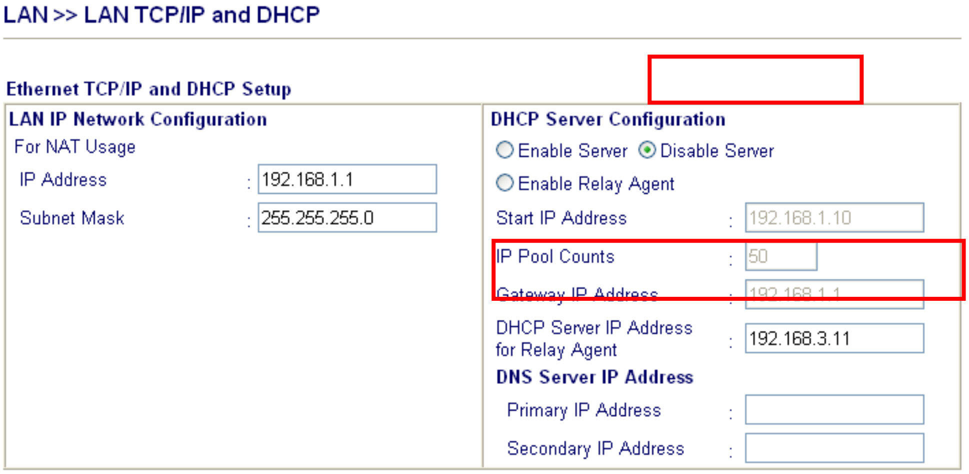
Primary IP Address :

Secondary IP Address :

To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as shown below.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



LAN >> LAN TCP/IP and DHCP

Ethernet TCP/IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server Configuration

○ Enable Server ● Disable Server

○ Enable Relay Agent

Start IP Address : 192.168.1.10

IP Pool Counts : 50

Gateway IP Address : 192.168.1.1

DHCP Server IP Address for Relay Agent : 192.168.3.11

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

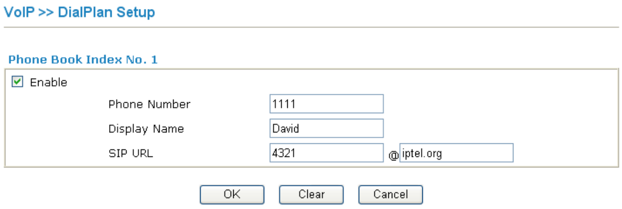
4.2 Calling Scenario for VoIP function

4.2.1 Calling via SIP Sever

Example 1: Both John and David have SIP Addresses from different service providers.

John’s SIP URL: 1234@draytel.org, David’s SIP URL: 4321@iptel.org

Settings for John
DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@iptel.org

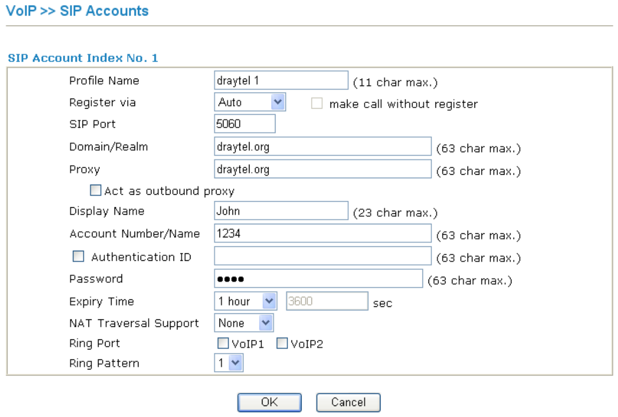


☑ Enable

Phone Number	1111
Display Name	David
SIP URL	4321 @ iptel.org

SIP Accounts Settings ---

Profile Name: draytel1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy: unchecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

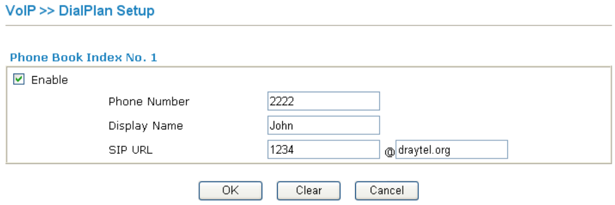


Profile Name	draytel 1	(11 char max.)
Register via	Auto	□ make call without register
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
□ Act as outbound proxy		
Display Name	John	(23 char max.)
Account Number/Name	1234	(63 char max.)
□ Authentication ID		(63 char max.)
Password	●●●●	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	□ VoIP1 □ VoIP2	
Ring Pattern	1	

CODEC/RTP/DTMF ---
(Use default value)

John calls David ---
He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

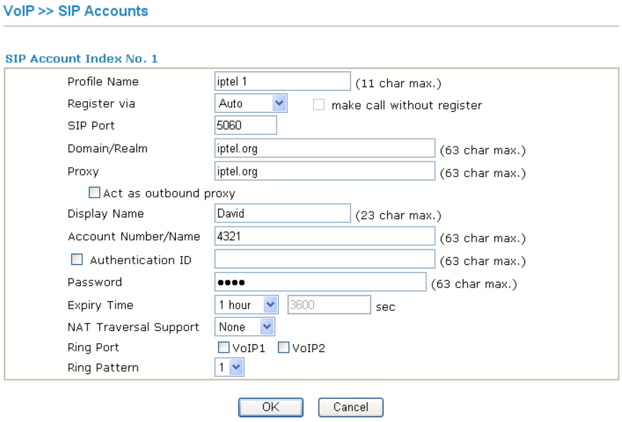
Settings for David
DialPlan index 1
Phone Number:2222
Display Name: John
SIP URL:1234@draytel.org



☑ Enable

Phone Number	2222
Display Name	John
SIP URL	1234 @ draytel.org

SIP Accounts Settings ---
Profile Name: iptel 1
Register via: Auto
SIP Port: 5060(default)
Domain/Realm: iptel.org
Proxy: iptel.org
Act as outbound proxy: unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)



Profile Name	iptel 1	(11 char max.)
Register via	Auto	□ make call without register
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
□ Act as outbound proxy		
Display Name	David	(23 char max.)
Account Number/Name	4321	(63 char max.)
□ Authentication ID		(63 char max.)
Password	●●●●	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	□ VoIP1 □ VoIP2	
Ring Pattern	1	

CODEC/RTP/DTMF ---
(Use default value)

David calls John
He picks up the phone and dials 2222# (DialPlan Phone Number for John)

Example 2: Both John and David have SIP Addresses from the same service provider.

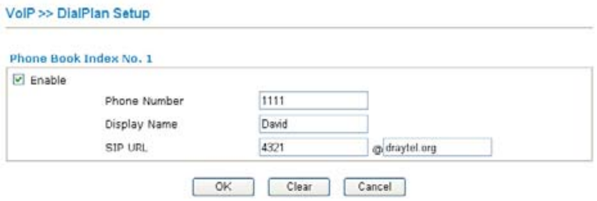
John’s SIP URL: 1234@draytel.org , David’s SIP URL: 4321@draytel.org

Settings for John
DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@draytel.org

SIP Accounts Settings ---

Profile Name: draytel 1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy: unchecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

CODEC/RTP/DTMF ---
(Use default value)



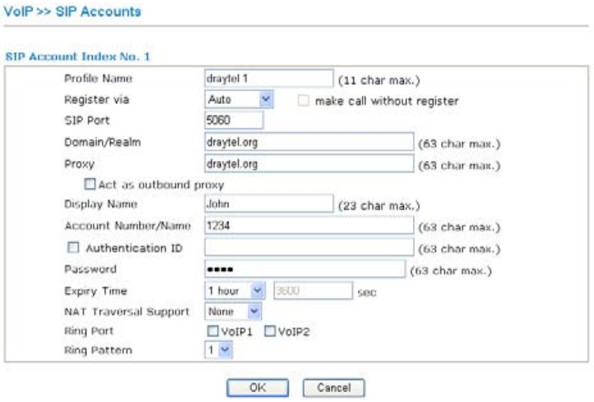
VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

Phone Number	1111
Display Name	David
SIP URL	4321 @ draytel.org

OK | Clear | Cancel



VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	draytel 1	(11 char max.)
Register via	Auto	□ make call without register
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
□ Act as outbound proxy		
Display Name	John	(23 char max.)
Account Number/Name	1234	(63 char max.)
□ Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	□ VoIP1 □ VoIP2	
Ring Pattern	1	

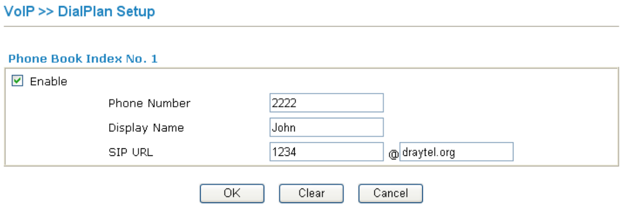
OK | Cancel

John calls David
He picks up the phone and dials 1111#. (DialPlan Phone Number for David)   Or,
He picks up the phone and dials 4321#. (David’s Account Name)

Settings for David
DialPlan index 1
Phone Number:2222
Display Name: John
SIP URL:1234@draytel.org

SIP Accounts Settings ---
Profile Name: John
Register via: Auto
SIP Port: 5060(default)
Domain/Realm: draytel.org
Proxy: iptel.org
Act as outbound proxy: unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

CODEC/RTP/DTMF---
(Use default value)



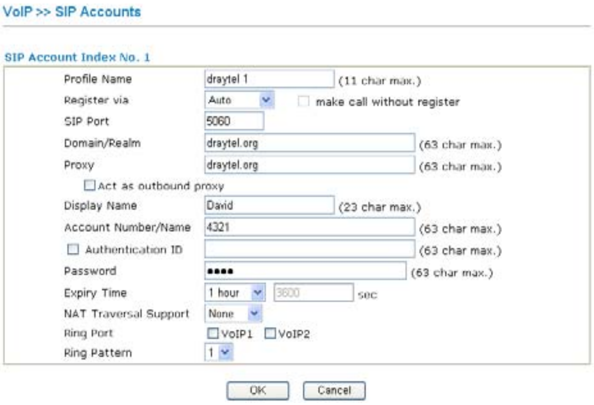
VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

Phone Number	2222
Display Name	John
SIP URL	1234 @ draytel.org

OK | Clear | Cancel



VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	draytel 1	(11 char max.)
Register via	Auto	□ make call without register
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
□ Act as outbound proxy		
Display Name	David	(23 char max.)
Account Number/Name	4321	(63 char max.)
□ Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	□ VoIP1 □ VoIP2	
Ring Pattern	1	

OK | Cancel

David calls John
He picks up the phone and dials 2222# (DialPlan Phone Number for John)   Or,
He picks up the phone and dials 1234# (John’s Account Name)

4.2.2 Peer-to-Peer Calling

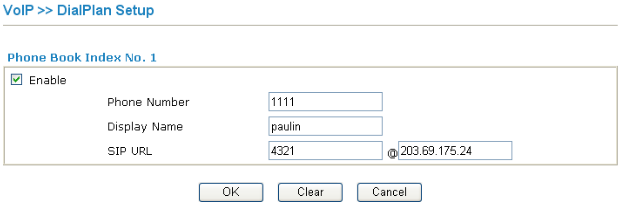
Example 3: Arnor and Paulin have Vigor routers respectively, they can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53 Paulin's SIP URL: 4321@ 203.69.175.24

Settings for Arnor
DialPlan index 1
Phone Number: 1111
Display Name: paulin
SIP URL: 4321@ 203.69.175.24

SIP Accounts Settings ---
Profile Name: Paulin
Register via: None
SIP Port: 5060(default)
Domain/Realm: (blank)
Proxy: (blank)
Act as outbound proxy: unchecked
Display Name: Arnor
Account Name: 1234
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

CODEC/RTP/DTMF---
(Use default value)



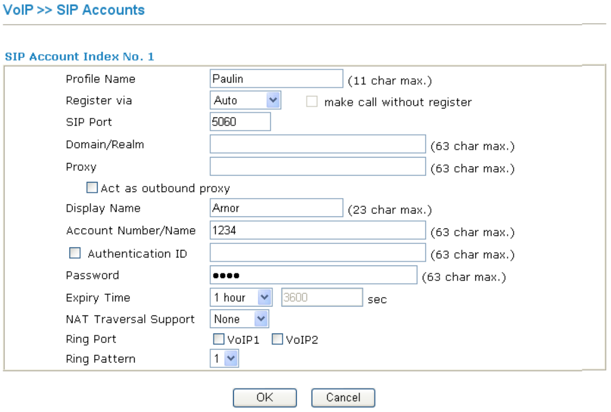
VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

Phone Number	1111	
Display Name	paulin	
SIP URL	4321	@ 203.69.175.24

OK Clear Cancel



VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	Paulin	(11 char max.)
Register via	Auto	□ make call without register
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
□ Act as outbound proxy		
Display Name	Arnor	(23 char max.)
Account Number/Name	1234	(63 char max.)
□ Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	□ VoIP1 □ VoIP2	
Ring Pattern	1	

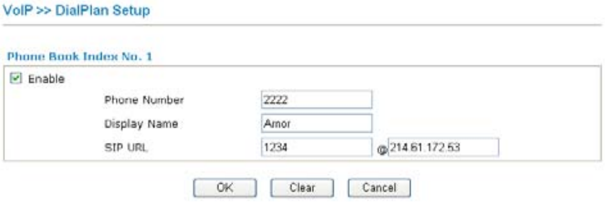
OK Cancel

Arnor calls Paulin
He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

Settings for Paulin
DialPlan index 1
Phone Number:2222
Display Name: Arnor
SIP URL: 1234@214.61.172.53

SIP Accounts Settings ---
Profile Name: Arnor
Register via: None
SIP Port: 5060(default)
Domain/Realm: (blank)
Proxy: (blank)
Act as outbound proxy: unchecked
Display Name: Paulin
Account Name: 4321
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

CODEC/RTP/DTMF---
(Use default value)



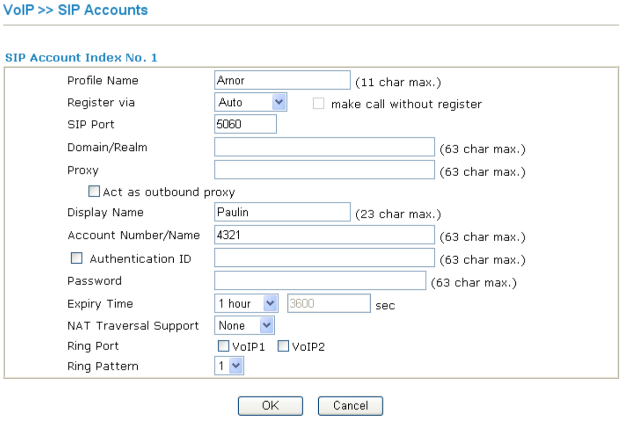
VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

Phone Number	2222	
Display Name	Arnor	
SIP URL	1234	@ 214.61.172.53

OK Clear Cancel



VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	Arnor	(11 char max.)
Register via	Auto	□ make call without register
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
□ Act as outbound proxy		
Display Name	Paulin	(23 char max.)
Account Number/Name	4321	(63 char max.)
□ Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	□ VoIP1 □ VoIP2	
Ring Pattern	1	

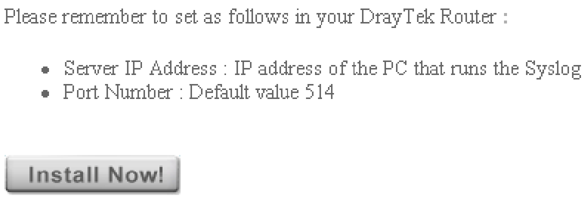
OK Cancel

Paulin calls Arnor
He picks up the phone and dials **2222#** (DialPlan Phone Number for John)

4.3 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

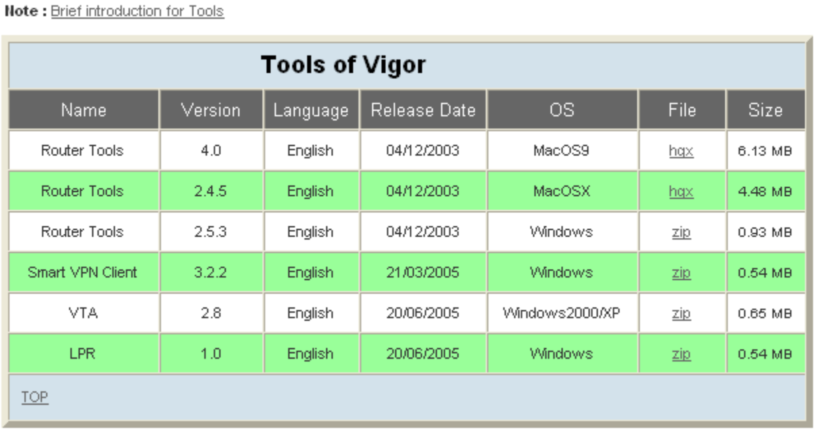
1. Insert CD of the router to your CD ROM.
2. From the webpage, please find out **Utility** menu and click it.
3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.



Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center >> Downloads**. Find out the model name of the router and click the firmware link. The Tools of Vigor router will display as shown below.



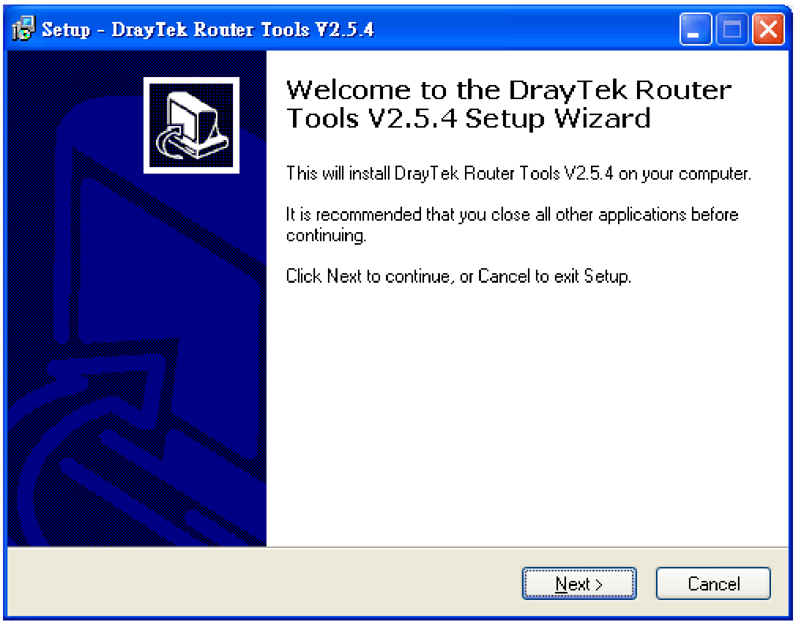
Note : Brief introduction for Tools

Tools of Vigor

Name	Version	Language	Release Date	OS	File	Size
Router Tools	4.0	English	04/12/2003	MacOS9	hqx	6.13 MB
Router Tools	2.4.5	English	04/12/2003	MacOSX	hqx	4.48 MB
Router Tools	2.5.3	English	04/12/2003	Windows	zip	0.93 MB
Smart VPN Client	3.2.2	English	21/03/2005	Windows	zip	0.54 MB
VTA	2.8	English	20/06/2005	Windows2000/XP	zip	0.65 MB
LPR	1.0	English	20/06/2005	Windows	zip	0.54 MB

7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
8. Next, decompress the zip file.

9. Double click on the icon of router tool. The setup wizard will appear.


Setup - DrayTek Router Tools V2.5.4

Welcome to the DrayTek Router Tools V2.5.4 Setup Wizard

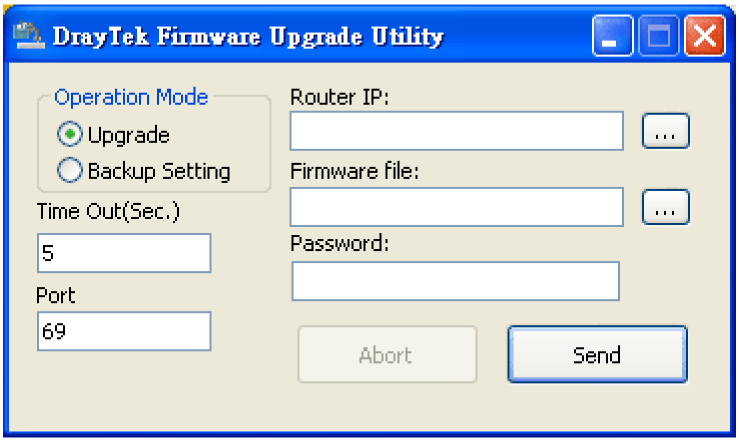
This will install DrayTek Router Tools V2.5.4 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.

11. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.


DrayTek Firmware Upgrade Utility

Operation Mode
● Upgrade
○ Backup Setting

Time Out(Sec.): 5

Port: 69

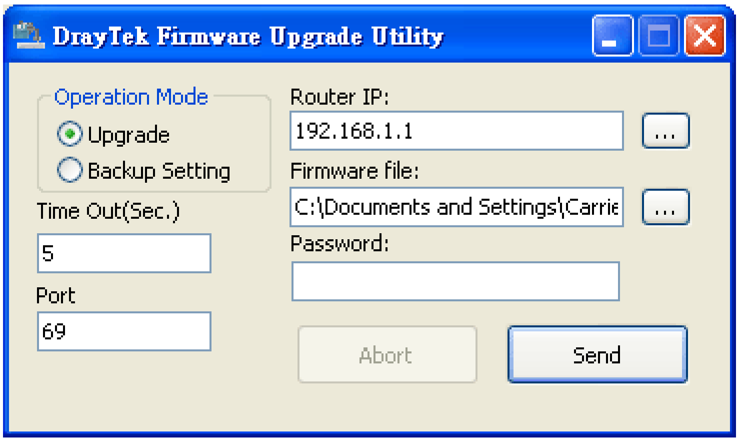
Router IP:

Firmware file:

Password:

12. Type in your router IP, usually **192.168.1.1**.

13. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.



Operation Mode

● Upgrade

○ Backup Setting

Time Out(Sec.): 5

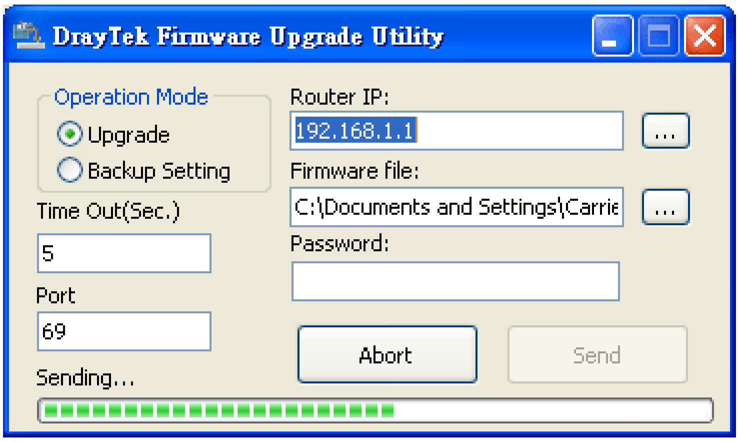
Port: 69

Router IP: 192.168.1.1

Firmware file: C:\Documents and Settings\Carrie

Password:

14. Click **Send**.



Operation Mode

● Upgrade

○ Backup Setting

Time Out(Sec.): 5

Port: 69

Router IP: 192.168.1.1

Firmware file: C:\Documents and Settings\Carrie

Password:

Sending...

15. Now the firmware update is finished.

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.

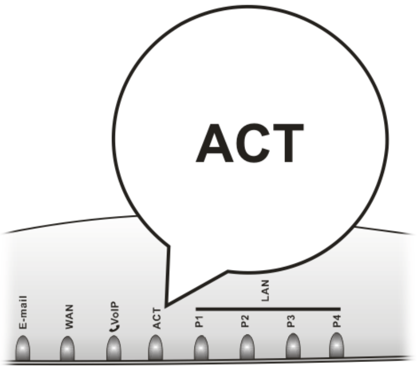
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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 “**2.1 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 **“2.1 Hardware Installation”** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

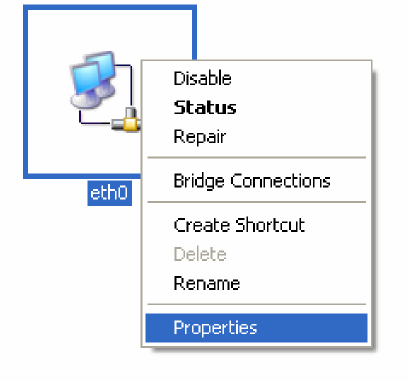
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

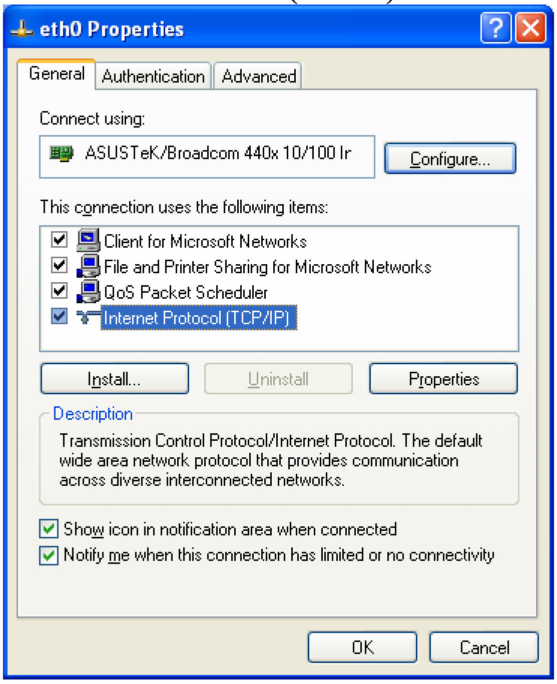
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Go to Control Panel and then double-click on Network Connections.

2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.



Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir

This connection uses the following items:

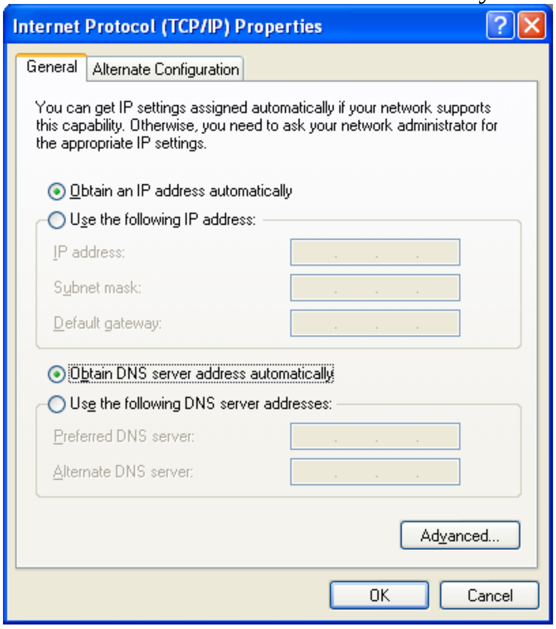
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

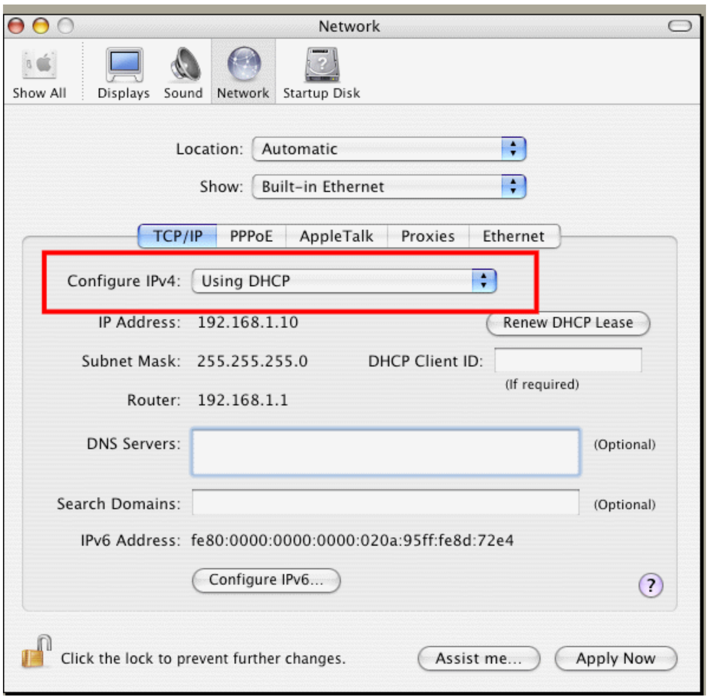
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

For 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.



Network

Location: Automatic

Show: Built-in Ethernet

TCP/IP | PPPoE | AppleTalk | Proxies | Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.1

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

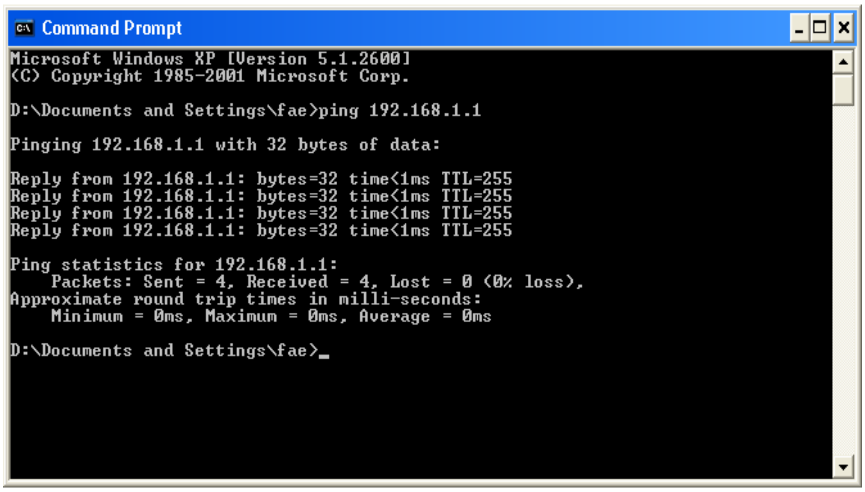
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 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.

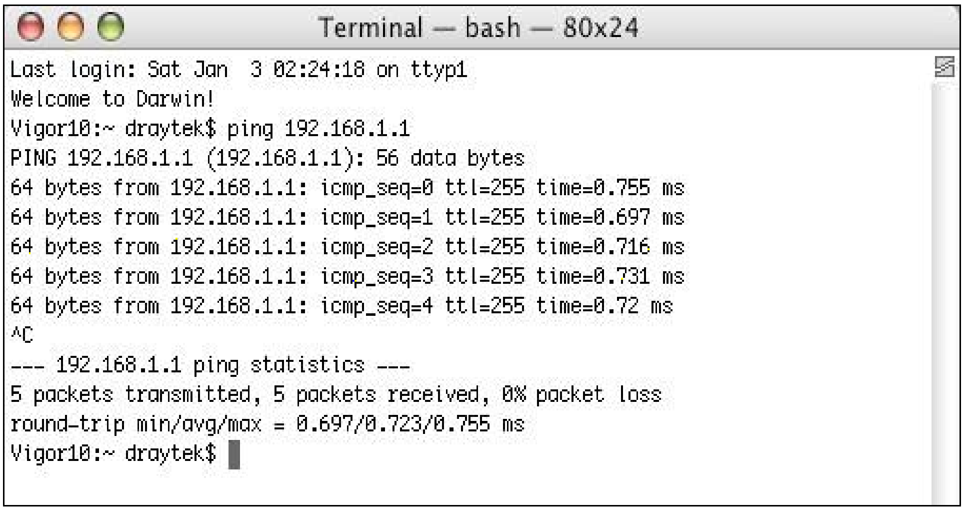


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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]. It 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)

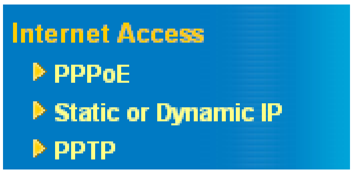
1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. It the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.



```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$ 
```

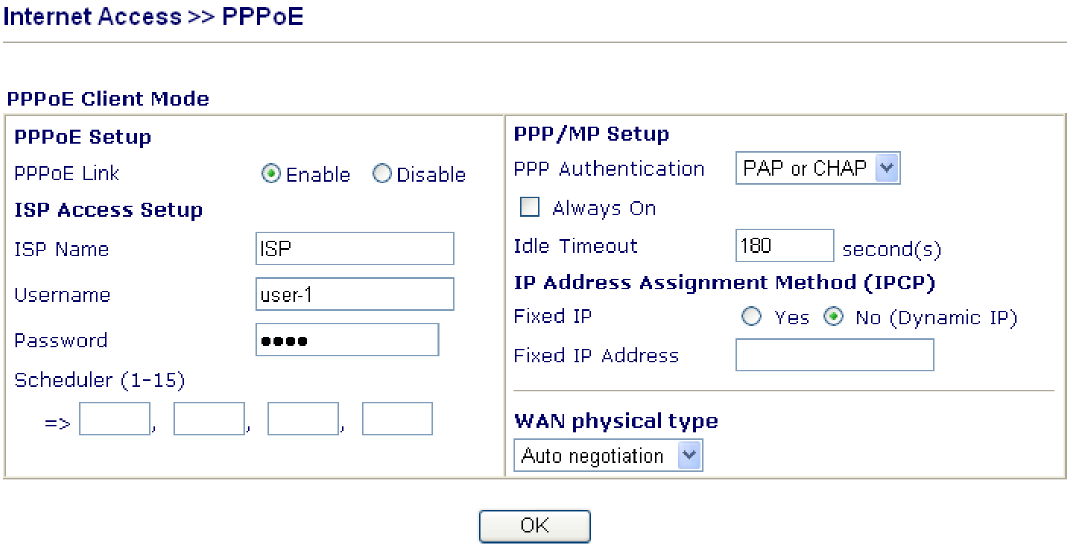
5.4 Checking If the ISP Settings are OK or Not

Click **Internet Access** group and then check whether the ISP settings are set correctly.



For PPPoE Users

1. Check if the **Enable** option is selected.
2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.



Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup

PPPoE Link ● Enable ○ Disable

ISP Access Setup

ISP Name: ISP

Username: user-1

Password: ●●●●

Scheduler (1-15)

=> ___, ___, ___, ___

PPP/MP Setup

PPP Authentication: PAP or CHAP

□ Always On

Idle Timeout: 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

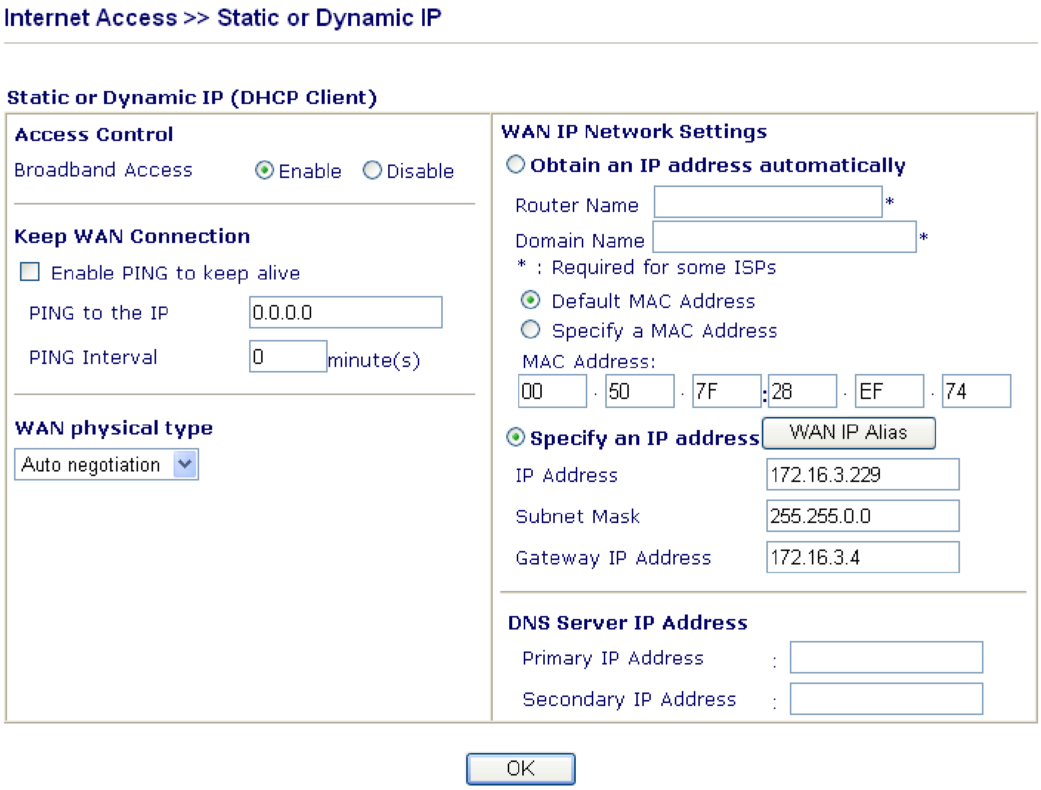
Fixed IP Address:

WAN physical type

Auto negotiation

For Static or Dynamic Users

1. Check if the **Enable** option for Broadband Access is selected.



Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

Keep WAN Connection

□ Enable PING to keep alive

PING to the IP: 0.0.0.0

PING Interval: 0 minute(s)

WAN physical type

Auto negotiation

WAN IP Network Settings

○ Obtain an IP address automatically

Router Name: *

Domain Name: *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F :28 . EF . 74

● Specify an IP address

IP Address: 172.16.3.229

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.3.4

DNS Server IP Address

Primary IP Address :

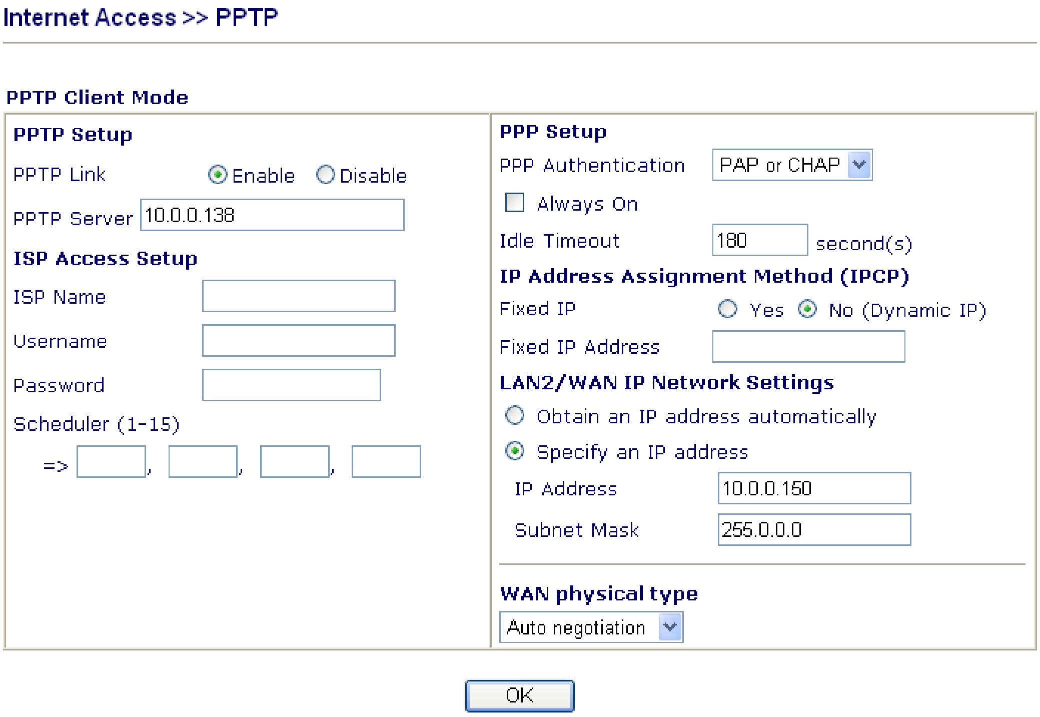
Secondary IP Address :

2. Check if **WAN IP Network Settings** is set appropriately.

3. Check if **IP Address, Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

For PPTP Users

1. Check if the **Enable** option for **PPTP** Link is selected.



Internet Access >> PPTP

PPTP Client Mode

PPTP Setup

PPTP Link ● Enable ○ Disable

PPTP Server 10.0.0.138

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

PPP Setup

PPP Authentication PAP or CHAP

□ Always On

Idle Timeout 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

LAN2/WAN IP Network Settings

○ Obtain an IP address automatically

● Specify an IP address

IP Address 10.0.0.150

Subnet Mask 255.0.0.0

WAN physical type

Auto negotiation

OK

2. Check if **PPTP Server, Username,** and **Password** are set correctly (must identify with the values from your ISP).

3. Check if **LAN2/WAN IP Network Settings** are set properly. If you select Specify an IP address, you have to type in the values of **IP Address** and **Subnet Mask** manually. Be sure the values that you type identify with the values from your ISP.

5.5 Backing to Factory Default Setting If Necessary

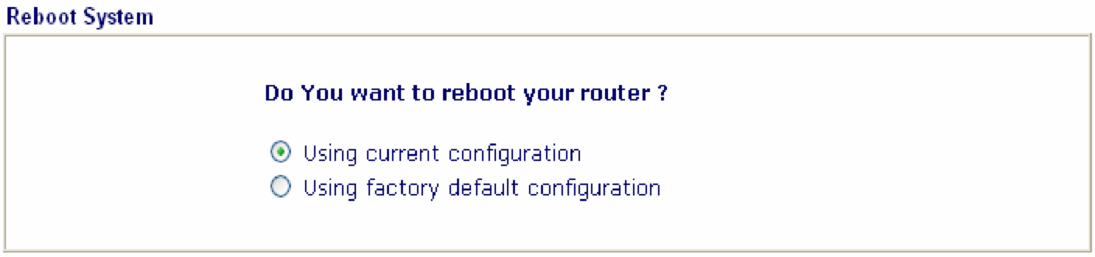
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page.

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

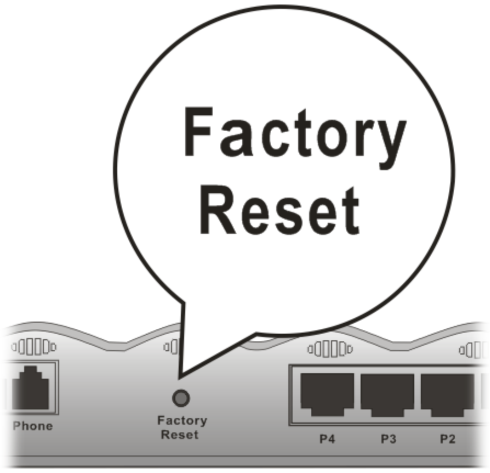
Do You want to reboot your router ?

● 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.