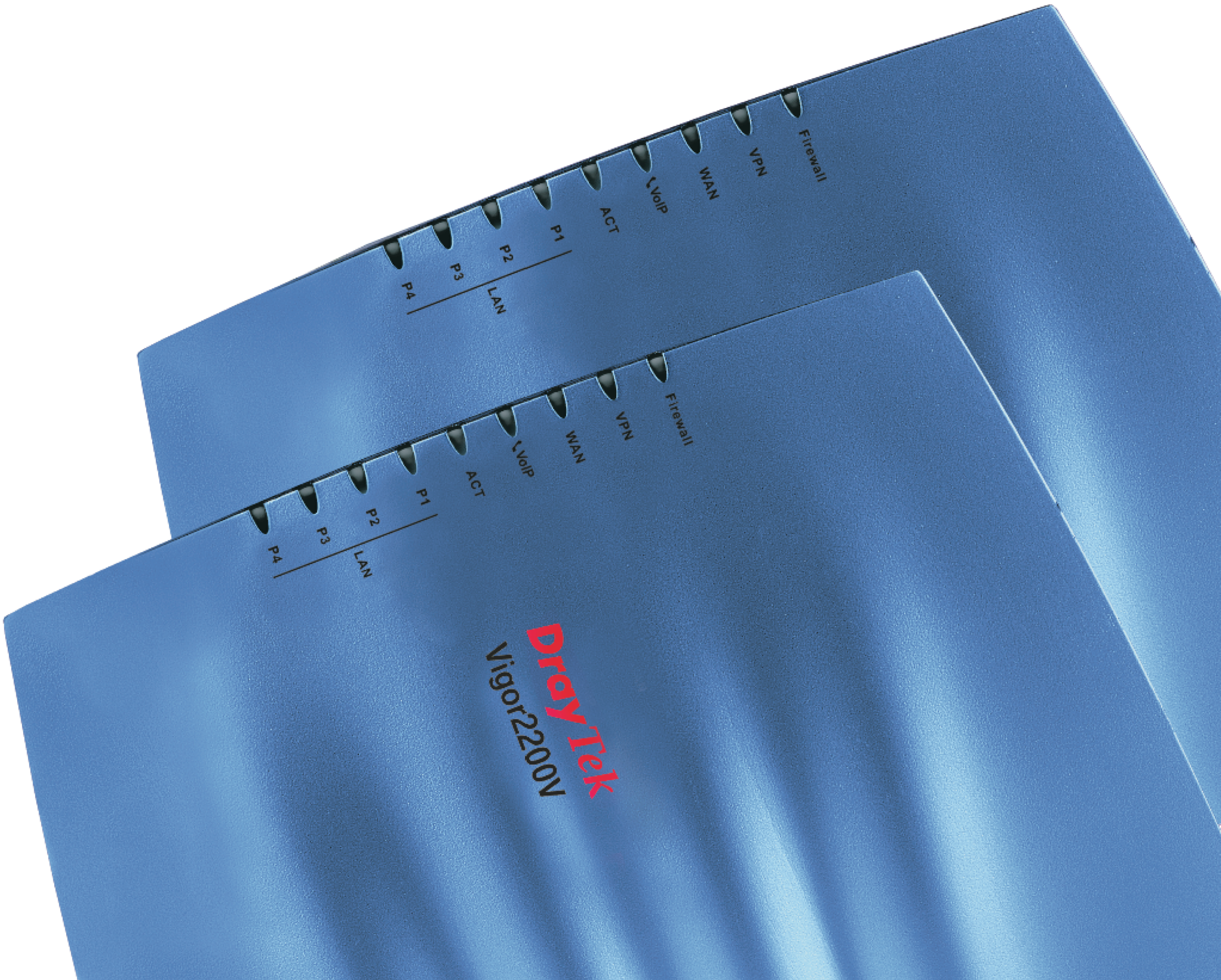
DrayTek
www.draytek.com

Vigor2200V/VG

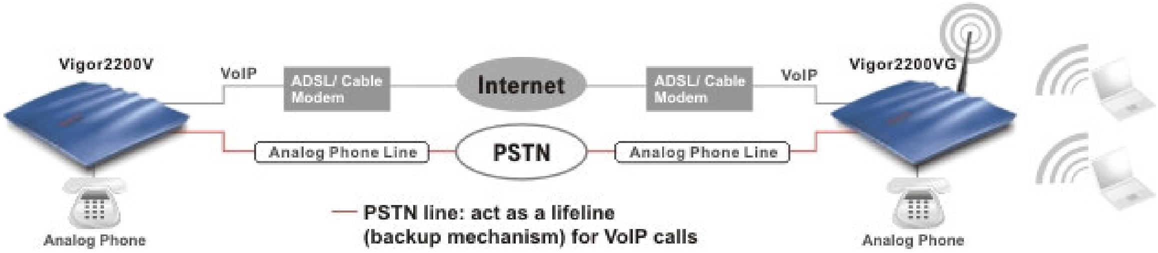
User's Guide



Preamble of Vigor2200V/VG series residential broadband Router

Introduction

- **Easy Internet-Sharing of your broadband* connection**
- **Robust firewall to help protect your network from external attacks**
- **Comprehensive VPN facilities provide deployment of linked branch offices and teleworkers.**
- **Built-in VoIP facilities enable to deploy cost-effective IP telephone infrastructure**
- **Plug in a telephone to use your broadband line for regular phone calls**
- **Integration with your existing phone line (POTS) with automatic failover during power cuts**
- **QoS assured priority for VoIP Internet traffic**
- **802.11g Compliant Wireless LAN access with security features (Vigor2200VG only)**
- **Compatible with Windows & MacOS**



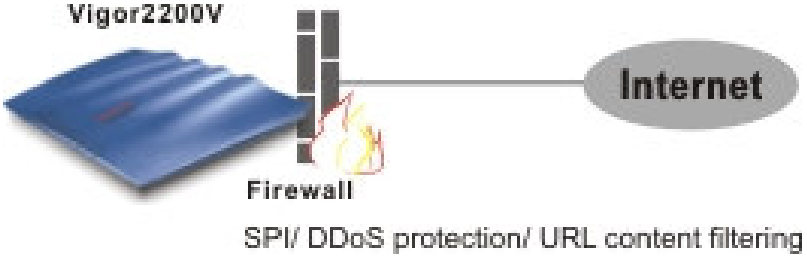
Brief Overview

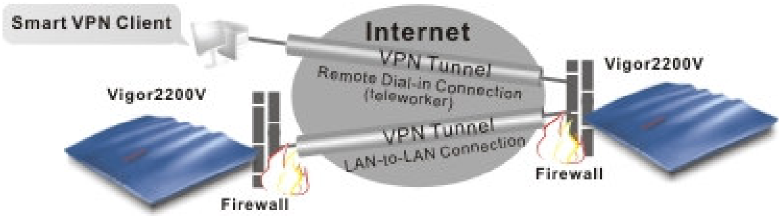
	Vigor2200V	Vigor2200VG
Broadband Router	*	*
802.11g WLAN AP	**-**	*
VoIP port	**One FXS**	**One FXS**
Life Line port	**one**	**one**

The Vigor2200VG is a user-friendly broadband router with a built-in VoIP (Voice over IP) telephone port and 802.11g Wireless LAN access point. The visual design, with its stylish pleasing lines and brushed silver finish provide looks good enough to fit into any environment.

The Vigor2200VG's VoIP facilities can provide a cost-saving alternative to having an additional fixed line. By using the DrayTEL PSTN gateway (ITSP) you can also make calls to any regular phone line too, including mobiles, as well as receive calls from anyone - the call is carried to your phone via your internet connection so your regular phone line remains free for other people or calls.

The POTS life-line facility provides for automatic failover to your regular phone line in the event of power or Internet failure, as well as letting you use the same phone to access either your regular phone line or VoIP facility when required.





Highlights

VoIP (Voice over IP)

- Connect a regular telephone to make and receive voice calls using your existing broadband connection, leaving your regular line free
- Make and receive calls using your regular phone line (POTS) or via VoIP using the same telephone handset
- Auto-Fallback - Phone switches to PSTN during power cut SIP, RTP/RTCP protocols compliance

WAN/Internet

- One 10/100M Base-TX port with a RJ-45 connector
- Quick Start Wizard for Internet access DHCP client for cable service
- Static IP address assignment for fixed IP networks
- PPPoE client

Firewall Facilities

- SPI (Stateful Packet Inspection) tracks packets and denies unsolicited incoming data
- Selectable DoS/DDoS protection
- Flexible URL content filtering
- User-configurable packet filtering
- NAT/PAT:

  Virtual server via port redirection or open ports

  DMZ host
- Supports ALGs (Application Layer Gateways) for applications

E-mail Detection

- LED flashes to indicate E-mail is waiting on your mail server (POP3)

LAN

- 4-port 10/100M Base-TX Ethernet switch
- DHCP server for IP assignment (up to 253 users)
- DNS cache and proxy

Virtual Private Network (VPN)

- Supports VPN pass-through
- Up to 8 simultaneous VPN tunnels
- Dial-in or dial-out, LAN-to-LAN or Teleworker-to-LAN
- Protocol support for PPTP, IPSec, L2TP, L2TP over IPSec
- Encryption support for AES, MPPE, and hardware- based DES/3DES encryption
- Authentication support for MD5 and SHA-1
- IKE key management
- Interoperable with other leading 3rd party vendor VPN devices or software

Wireless Access Point (Vigor2200VG only)

- Supports 802.11g (54Mbps data rate)
- Backward compatible with 802.11b
- Station List
- Wireless security:

  64/128 bits WEP wireless encryption

  WPA/PSK encryption

  Client MAC-address locking

  SSID stealth

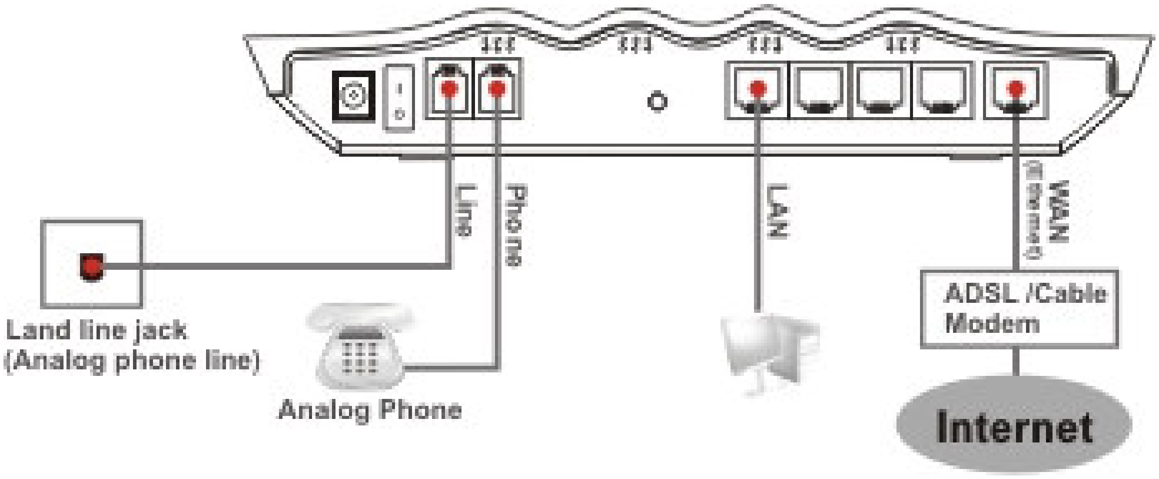
Application Support

- Supports VPN pass-through
- MSN Messenger V6.2, online gaming, and other multimedia applications
- UPnP protocol enables router control and enhances access for UPnP -ready multimedia applications

Router Management

- Web-based User Interface
- Command Line Interface (Telnet)
- Telnet Remote Access Support
- Built-in Diagnostic Function
- Syslog Monitoring

Hardware Connection



About This User's Guide

This manual is designed to assist users in using one of the Vigor2200V/VG series residential broadband router with VoIP. Information in this document has been carefully checked for accuracy and, however, no guarantee is given as to the correctness of the contents. The information contained in this document is subject to change without notice. Should you have any inquiries, please feel free to contact our support via E-mail, Fax or phone. For the latest product information and features, please visit our website at **www.draytek.com**.

We apply the sunshine-smile face of VigorBoy ☺ to some chapters in order to remind you of your special attention! Should you have any queries and suggestions, please do not hesitate to contact your local dealer or us via **support@draytek.com** or **info@draytek.com**!

The version of this User's Guide is version No.1.

Copyright

Copyright © 2004 by DrayTek Corporation

Trademark

Microsoft is a registered trademark of Microsoft Corp. Windows and Windows 95/98/98SE/Me/NT/XP/2000 are trademarks of Microsoft Corp. Other trademarks and registered trademarks of products mentioned in this manual may be the properties of their respective owners and are only used for identification purposes.

DrayTek Limited Warranty

We warrant to the original end user (purchaser) that the routers will be free from any defects in workmanship or materials for a period of three (3) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase.

During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or remanufactured 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

Online web registration at **www.draytek.com** is preferred. Alternatively, fill in the registration card and mail it to the address found on the reverse side of the card. Registered owners will receive future product and update information.

Safety Instructions

- Please read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic device that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range from +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.
- Keep the package out of reach of children.
- When you would like to dispose of the router, please follow the local regulations on conservation of the environment.

European Community Declarations

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

Product: Vigor2200V/VG Series Residential Broadband Routers

DrayTek Corp. declares that Vigor2200V/VG 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 Vigor2200VG is designed for the WLAN 2.4GHz network throughput EC region, Switzerland, and the restrictions of France.

Commission (FCC) Interference Statement

The Vigor2200V and Vigor2200VG have been tested and found to comply with the limits for a Class B digital device, pursuant to 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 must accept any interference received, including interference that may cause undesired operation. Class B 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 not guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Customer Support

Please prepare the following information as you contact your customer support.

- Product model and serial number.
- Warranty information.
- Date that you received your router.
- Brief description of your problem.
- Steps that you may take to solve it and their associated SysLog messages.

The information of customer support and sales representatives are support@draytek.com and sales@draytek.com, respectively.

Table of Contents

CHAPTER 1. Quick Start Wizard

CHAPTER 2. Online Status

CHAPTER 3. Internet Access Setup

CHAPTER 4. LAN Setup

CHAPTER 5. NAT Setup

CHAPTER 12. Diagnostic Setup

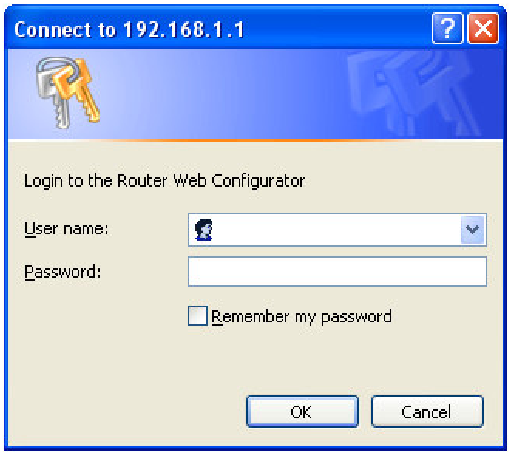
Chapter 1
Quick Start Wizard

1.1 Introduction

The Quick Start Wizard is designed for you to easily set up your broadband Internet access. We already integrated Quick Start Wizard into the Web Configurator of Vigor2200V/VG series. You can directly access the Quick Start Wizard via Web Configurator.

1.2 Configure Your Router via Quick Start Wizard

Step 1. Open the web browser on a PC which is connected to the router and then link to the gateway IP address of the router (the default setting is **192.168.1.1**). Once your link (**http://192.168.1.1**) is successful, a pop-up window will open to ask for username and password. Leave the default null value and press **OK** to continue.

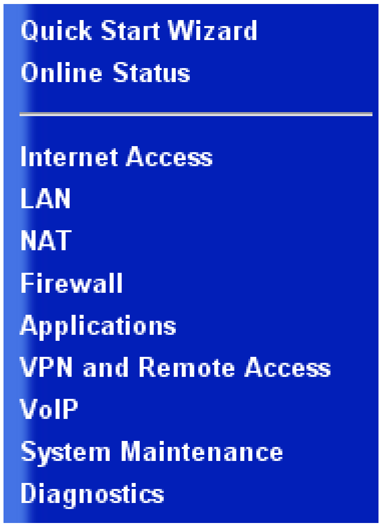


Connect to 192.168.1.1

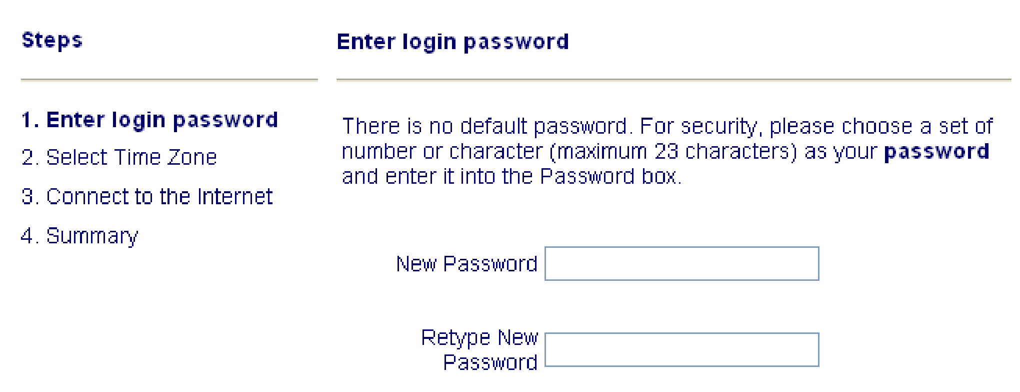
Login to the Router Web Configurator

If you fail to access to the web configuration, please refer to “Trouble Shooting” guide.

Step 2. The **Main Menu** will pop out after completing previous step.



Step 3. Now Quick Start Wizard is switched on. Enter login password. Then click **Next** to continue.



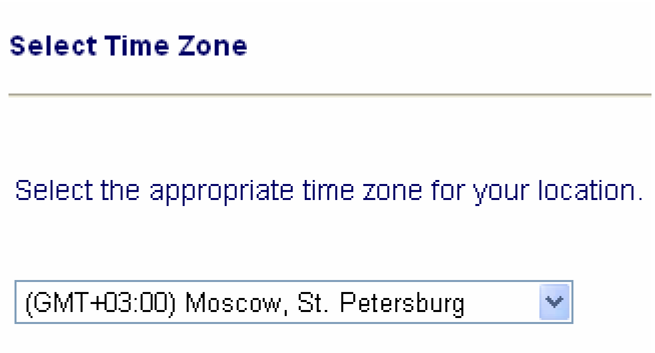
Enter login password

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

Step 4. Select the appropriate TIME ZONE for your location.

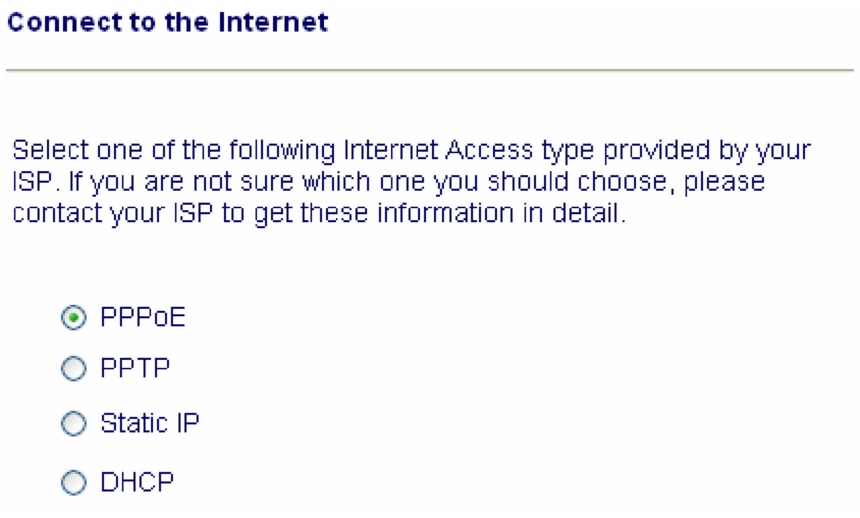


Select Time Zone

Select the appropriate time zone for your location.

(GMT+03:00) Moscow, St. Petersburg

Step 5 Select the appropriate Internet connection type to your ISP.



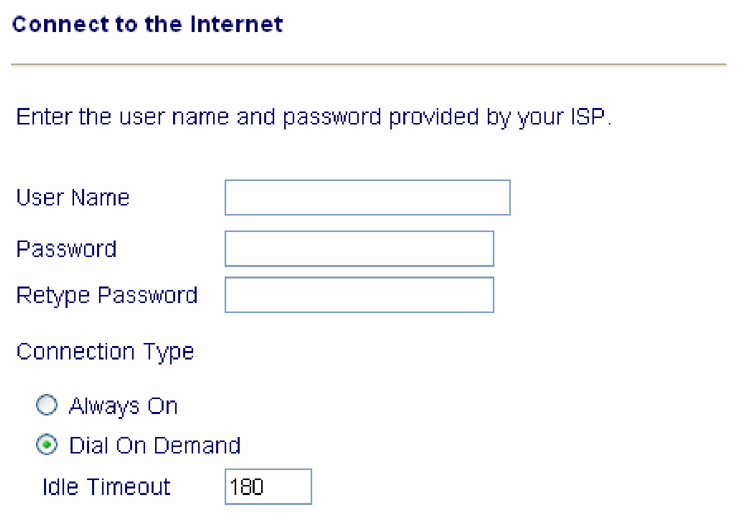
Connect to the Internet

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

In terms of several Internet connection type, please follow procedures as below:

PPPoE users Enter your user name and password provided by your ISP.



Connect to the Internet

Enter the user name and password provided by your ISP.

User Name	
Password	
Retype Password	

Connection Type

○ Always On
● Dial On Demand

Idle Timeout 180

Dial on Demand : The router will ONLY connect to your ISP on demand. By "on demand", it means when any LAN user attempt to send data onto the

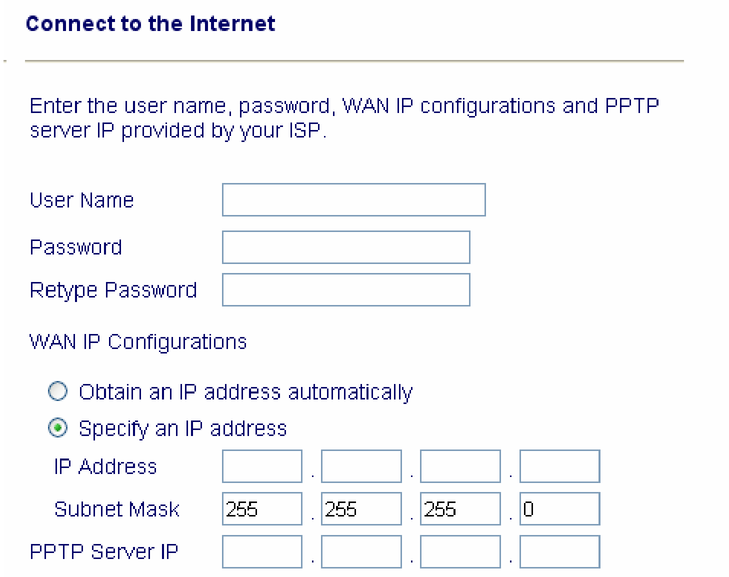
Internet. When there is no data traffic, the router will close the connection to the ISP because there is no demand.

Idle timeout: This is the time setting If there being no Internet traffic for a period, for example 10 minutes.

Always On: The router will keep a permanent connection to the ISP automatically.

PPTP users

Enter your user name and password provided by your ISP.



Connect to the Internet

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

User Name

Password

Retype Password

WAN IP Configurations

○ Obtain an IP address automatically

● Specify an IP address

IP Address . . .

Subnet Mask 255 . 255 . 255 . 0

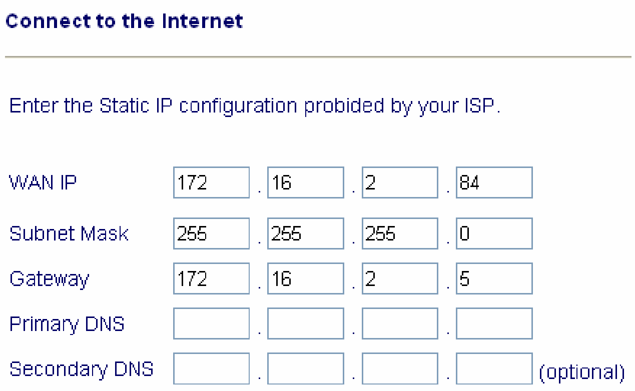
PPTP Server IP . . .

Obtain an IP address automatically: Set the WAN interface as a DHCP client that will ask for the IP network settings from the DHCP server or PPTP-enabled DSL modem.

Specify an IP address: If you are not sure whether there are any DHCP services on the WAN interface, you can manually assign an IP address to the interface. Note that the IP Address and Subnet Mask should be assigned within the same network as the PPTP-enabled DSL modem.

Static IP

Enter the static (fixed or permanent) IP address that your ISP offers to you.



Connect to the Internet

Enter the Static IP configuration probided by your ISP.

WAN IP 172 . 16 . 2 . 84

Subnet Mask 255 . 255 . 255 . 0

Gateway 172 . 16 . 2 . 5

Primary DNS . . .

Secondary DNS . . . (optional)

WAN IP address: this is the IP address assigned by your ISP for your router. You shall specify the IP address of the router here. e.g. 172.16.2.84

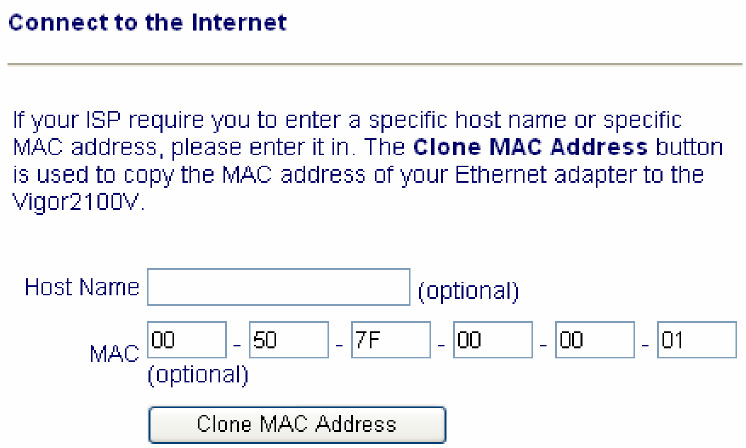
Subnet Mask: an address code that determines the size of the network; this is the subnet mask of the router, when seen by external users on the Internet (including your ISP). The subnet mask is provided by your ISP. e.g. 255.255.255.0

Gateway IP Address: an IP address forwards Internet traffic from your local area network (LAN) . e.g. 172.16.2.5

DNS Server IP address: you must specify DNS server IP address here if your ISP has the said address. If you do not specify it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

DHCP

Some Cable ISPs require user to provide or specify MAC address for access authentication purpose. Your can either manually enter the MAC address in the MAC Address fields or clone from your network adapter.



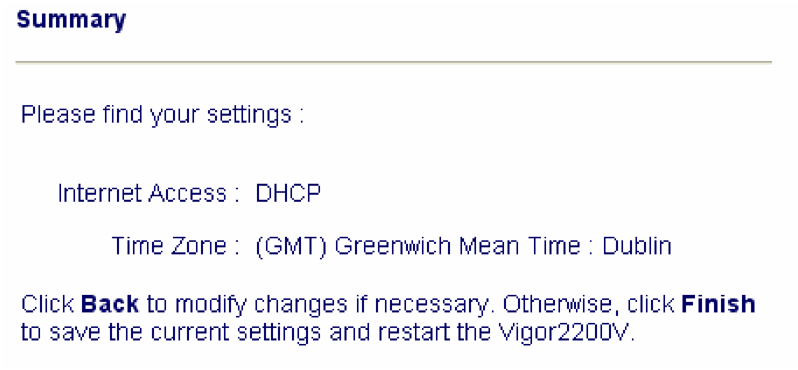
Connect to the Internet

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

Step 6 Review the summary of settings.



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 Vigor2200V.

Vigor2200V/VG series apply efficient codecs designed to make the best use of available bandwidth. Vigor2200V/VG also equips with **automatic QoS assurance**. QoS Assurance assists to assign higher priority to voice traffic via Internet for better talking/hearing enjoyment. To achieve that, you will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet. Your data will arrive a little bit later in a tolerable manner.

On the bottom of Web Configurator window, you can find messages showing the system interaction with you.

- "**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.

Chapter 2 Online Status

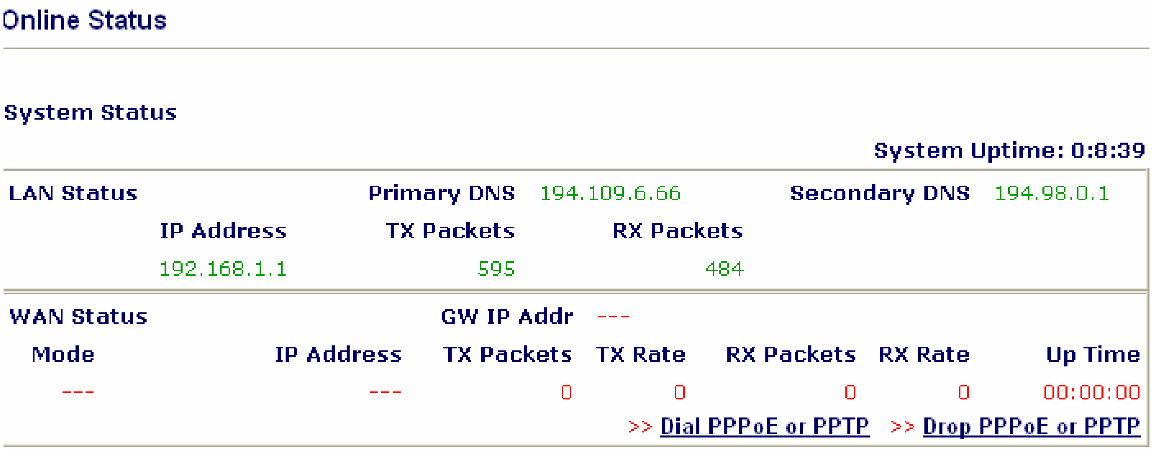
2.1 Introduction

The **Online Status** provides some useful information about the Vigor router, LAN and WAN interface. Also, you could use the status page to know the Internet access status.

2.2 Settings

Click **Online Status** to open the Online Status page.

Here in, we use an example to explain **the Online Status**. In the example, as shown in the following picture, the router is working on Dynamic IP mode to access the Internet.



Online Status

System Status

System Uptime: 0:8:39

LAN Status   Primary DNS 194.109.6.66   Secondary DNS 194.98.0.1

IP Address	TX Packets	RX Packets
192.168.1.1	595	484

WAN Status   GW IP Addr ---

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
---	---	0	0	0	0	00:00:00

2.2.1 System Status

System Uptime: This represents the router's running time. The format is HH:MM:SS, where HH, MM, and SS, indicate hours, minutes, and seconds, respectively.

2.2.2 LAN Status

IP Address	IP address of the LAN interface.
TX Packets	Total number of transmitted IP packets since the router was powered on.
RX Packets	Total number of received IP packets since the router was powered on.
Primary DNS	You must specify DNS server IP address here if your ISP has the said address. If you do not specify it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS	You must specify secondary DNS server IP address here if your ISP has the said address. If you do not specify it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

2.2.3 WAN Status

Mode	Indicate which broadband access mode is active. Depending upon the access mode, you may see **PPPoE, PPTP, PPPoA, or Static IP or DHCP.**
GW IP Addr	The gateway IP address.
IP Address	IP address of the WAN interface.
TX Packets	Total number of transmitted IP packets during this connection session.
TX Rate	Transmission rate in characters per second (cps) for outgoing data.

RX Packets	Total number of received IP packets during this connection session.
RX Rate	Reception rate in characters per second (cps) for incoming data.
Up Time	Connection time. The format is HH:MM:SS, where HH, MM, and SS, indicate hours, minutes, and seconds, respectively.
Drop/Dial PPPoE or PPTP	Click the link to dial/or disconnect the PPPoE or PPTP connection.

Chapter 3
Internet Access Setup

3.1 Introduction

The router connects the group of PCs in your home or office to the Internet. The data that travels between two networks is regulated by the router. The Network Address Translation (NAT) of the router translates a public IP address for the Internet to several private IP addresses of a local area network.

IP means Internet Protocol. Every device in an IP-based Network, including routers, print server, and PCs needs an IP address to identify its location on the network. The PPPoE, Dynamic/Static IP and PPTP are three major ways of assigning IP addresses for the Internet to your router. Setup screen and available features differ relying on what kind of connection type your ISP offers.

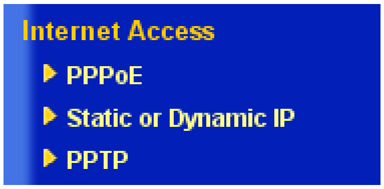
The router supports the Ethernet WAN interface for Internet access. The following sections will explain more details of various broadband access setup.

Once you already access Internet via the procedure of “Chapter 1 Quick Start Wizard”, you do not need to re-set your settings for Internet connection unless you would like to change your configuration.

3.2 Settings

For broadband access, you need to know what kind of Internet access is provided by your ISP.

Click **Internet Access** to open the Internet access page.



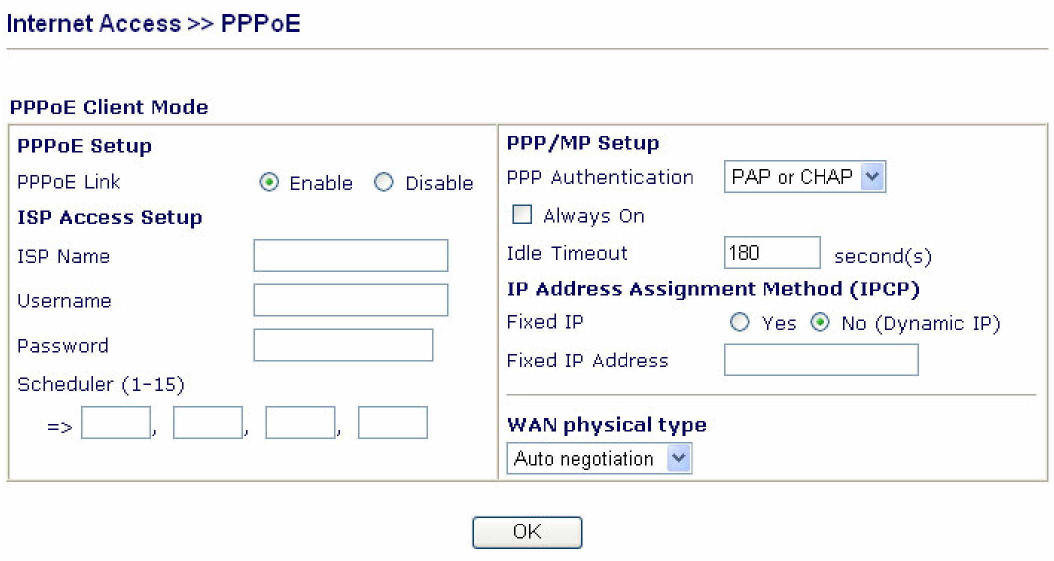
There are four widely-used broadband access services, **PPPoE Client, PPTP Client, Static IP** for DSL, and **Dynamic IP (DHCP Client)** for Cable. In most cases, you will get a DSL or Cable modem from the broadband access service provider.

PPPoE	Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to let users establish Internet access. All local users can share one PPPoE connection to access the Internet.
Static IP	It means a fixed or permanent IP address. Choose Static IP if your ISP provides you with a permanent IP address.
Dynamic IP	It means that "Obtain an IP automatically". In most circumstances, the cable modem that you are connecting shall obtain a dynamic IP address from the ISP.
PPTP	Some DSL-based ISPs use PPTP (Point-to-Point Tunneling Protocol) to establish Internet connection for users. The PPTP is available in Europe and Israel. As a result, your DSL modem only supports the PPTP tunnel to access the Internet. You shall create a PPTP tunnel that carries a PPP session and terminates on the DSL modem. Once the tunnel has been established, this kind of DSL modem will forward

	the PPP session to the ISP. As long as the PPP session is connected, all the local users will be able to share this PPP session to access to the Internet.

3.2.1 Using PPPoE with a DSL modem

Click **Internet Access Setup** > **PPPoE** to enter the setup page.



Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup

PPPoE Link ● Enable ○ Disable

ISP Access Setup

ISP Name

Username

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

PPPoE Setup

PPPoE Link: Check **Enable** to enable the PPPoE client protocol on the WAN interface.

Please remember to remove PPPoE applications, which are already installed on your PCs if you need to enable PPPoE and you are DSL users.

ISP Access Setup

ISP Name: Enter the service name if provided by your ISP.

Username/Password**:** Enter the username and password supplied by your ISP

Scheduler **(*1-15*):** Enter the index of schedule profile to control the Internet access by time plan.

PPP/MP Setup

PPP Authentication**:** Select PAP or CHAP for widest compatibility.

Always On**:** Check to force the Internet access is always online, and you will see the **Idle Timeout** field will be blocked for input.

Idle Timeout**:** Idle timeout means the router will disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the PPP session will not terminate itself.

IP Address Assignment Method (IPCP)

Fixed IP**:** Check **No (Dynamic IP)** unless your ISP has provided you with a static IP address.

Fixed IP Address**:** If your ISP has provided you with a static IP address enter it here.

Click **OK**.

3.2.2 Using a Static IP with a DSL/Cable Modem

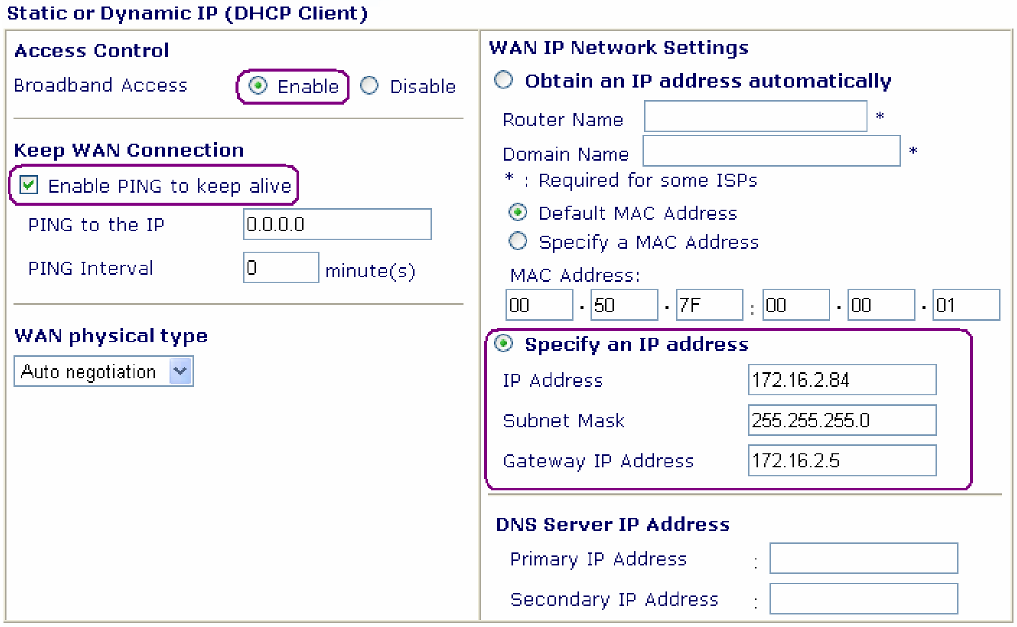
You can receive a fixed public IP address or a public subnet (i.e. Multiple public IP addresses) from your DSL or Cable ISP. Because of NAT (Network Address Translation) function, you just need to assign a fixed public IP address to assign to the WAN interface of your router. Your router will let your every PC share the broadband access as NAT transform the said fixed IP address to several private IP address. Click **Internet Access Setup** > **Static or Dynamic IP** to enter the setup page, which is depicted as follows:

Access Control

Broadband Access**:** Select **Enable** to turn on the broadband access capability.

Keep WAN Connection

Enable PING to keep alive**:** If you specify "Enable PING to keep alive" function, the router will periodically check your Internet connection. The router will automatically re-establish the connection if the connection is down. Normally, this function is used for Dynamic IP environment. Here will ignore the settings.



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 : 00 - 00 - 01

● Specify an IP address

IP Address 172.16.2.84

Subnet Mask 255.255.255.0

Gateway IP Address 172.16.2.5

DNS Server IP Address

Primary IP Address :

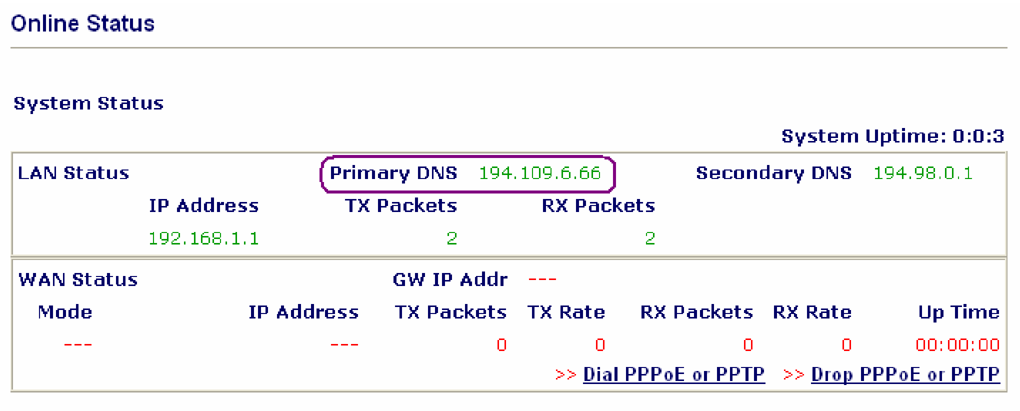
Secondary IP Address :

WAN IP Network Settings

Specify an IP address	If your ISP offers you a static (fixed or permanent) IP address, you have to enable "***Specify an IP address".***
IP address	This is the IP address assigned by your ISP for your router. You shall specify the IP address of the router here. e.g. 172.16.2.84.
Subnet Mask	An address code that determines the size of the network; this is the subnet mask of the router, when seen by external users on the Internet (including your ISP). (Default: 255.255.255.0/ 24)

Gateway IP Address	An IP address forwards Internet traffic from your local area network (LAN) . e.g. 172.16.2.5.
DNS Server IP address	You must specify a DNS server IP address here because your ISP will at least provide you with at least one DNS Server IP address. If you do not specify it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. **The Domain Name System (DNS) functions how the Internet translates domain or website names into Internet addresses or URLs.**
Secondary DNS Server IP address	You must specify secondary DNS server IP address here because your ISP often can let you have at least one DNS Server IP address. If you do not specify 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:



Online Status

System Status

System Uptime: 0:0:3

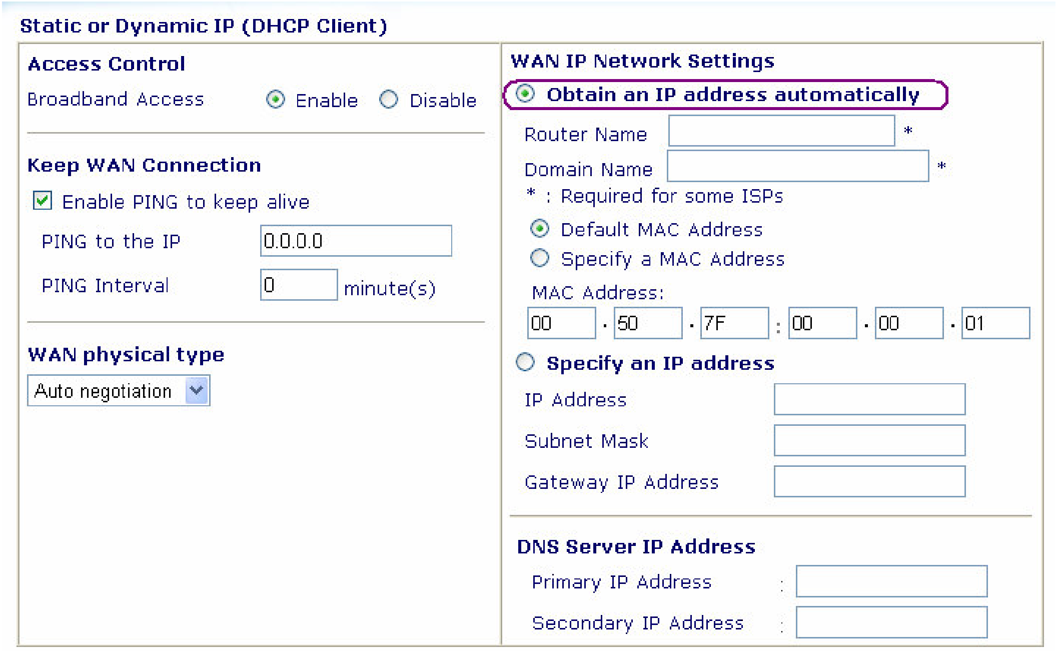
LAN Status		Primary DNS 194.109.6.66		Secondary DNS 194.98.0.1
	IP Address	TX Packets	RX Packets	
	192.168.1.1	2	2	

WAN Status		GW IP Addr	---			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
---	---	0	0	0	0	00:00:00

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

3.2.3 Using a Dynamic IP (DHCP Client) with a DSL/Cable Modem

This application is mostly used by Cable ISPs. Click **Internet Access Setup > Static or Dynamic IP** to enter the setup page.



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 : 00 : 00 : 01

○ Specify an IP address

IP Address

Subnet Mask

Gateway IP Address

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

Access Control

Broadband Access**:** Select **Enable** to turn on the broadband access capability.

Keep WAN Connection

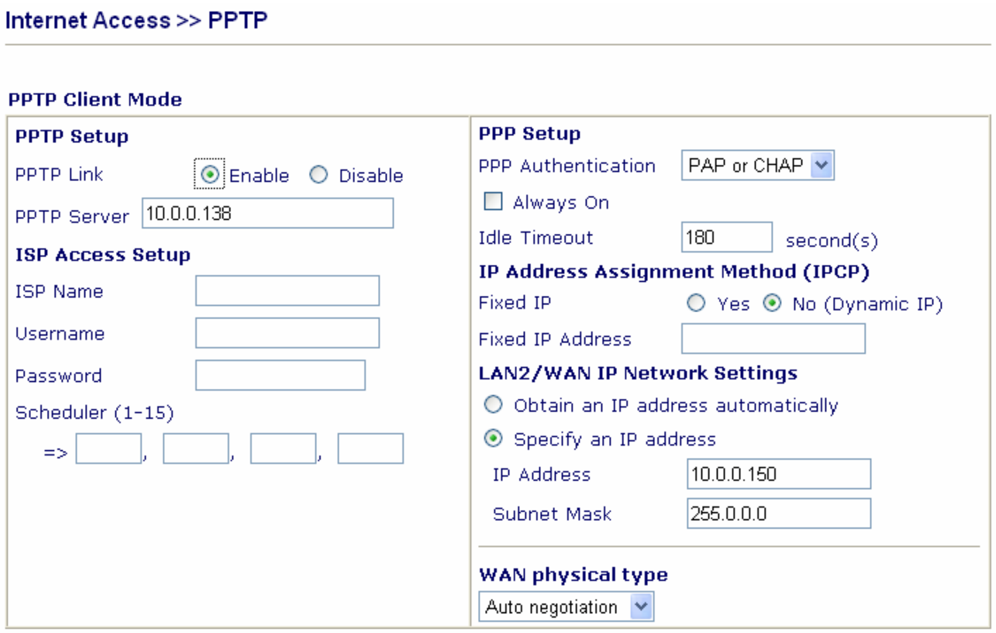
***Enable PING to keep alive*:** Check to enable PING to keep alive function. Normally, this function is for Dynamic IP environment. If you need to enable the function, assign a public IP address in the PING to the IP and a timer in the PING Interval.

WAN IP Network Settings

Obtain an IP address automatically	The option must be enabled.
Router Name	Depending on your Cable ISP, this option may or may not be left blank. Some ISPs require this name for access authentication.
Domain Name	Depending on your Cable ISP this field may or may not be left blank.
Default MAC Address & Specify a MAC Address	These two options are mutually exclusive. Some Cable ISPs use a specific MAC address for access authentication. In such cases you need to check the **Specify a MAC Address box** and enter the MAC address in the MAC Address fields. Click **OK** and restart the router to allow the settings to take affect.

3.2.4 Using PPTP with a DSL Modem

Click **Internet Access Setup** > **PPTP** to enter the setup page, as shown below. Herein, we use an example to explain the corresponding setting. The exact settings should be provided by your DSL service provider.



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	Check **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
PPTP Server IP Address	Specify the IP address of the PPTP-enabled DSL modem. Refer to the user manual of the PPTP-enabled DSL modem.

ISP Access Setup

ISP Name: Enter the service name if provided by your ISP.

Username/Password: Enter the username and password supplied by your ISP.

Scheduler (1-15): Enter the index of schedule profile to control the Internet access by time plan.

PPP/MP Setup

PPP Authentication	Select PAP or CHAP for widest compatibility.
Always On	Check to force the Internet access is always online, and you will see the Idle Timeout field will be blocked for input.
Idle Timeout	Idle timeout means the router will disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the PPP session will not terminate itself.
IP Address Assignment Method (IPCP)	***Fixed IP*****:** Check No (Dynamic IP) unless your ISP has provided you with a static IP address. ***Fixed IP Address*****:** If your ISP has provided you with a fixed IP address enter it here.

WAN IP Network Settings

Obtain an IP address automatically	Set the WAN interface as a DHCP client that will ask for the IP network settings from the DHCP server or PPTP-enabled DSL modem.
Specify an IP address	If you are not sure whether there are any DHCP services on the WAN interface, you can manually assign an IP address to the interface. Note that the IP Address and Subnet Mask should be assigned within the same network as the PPTP-enabled DSL modem.

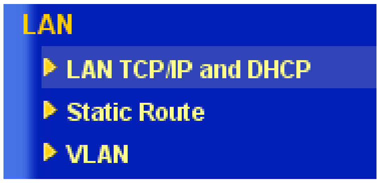
Chapter 4
LAN Setup

4.1 Introduction

In this chapter, we will explain about the **LAN Setup**.

4.2 Settings

Click **LAN** to open the LAN settings page.

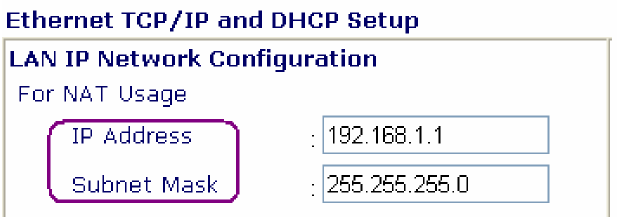


4.2.1 LAN TCP/IP and DHCP

LAN IP Network Configuration

The IP address/subnet mask is for grouping users on your LAN. For example, you can let the computer of your kids be connected together with your own computer to share the broadband access and to share files.

For NAT Usage: (Default: Always Enable)



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

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

Subnet Mask: An address code that determines the size of the network; this is the subnet mask of the router, when seen by external users on the Internet (including your ISP).

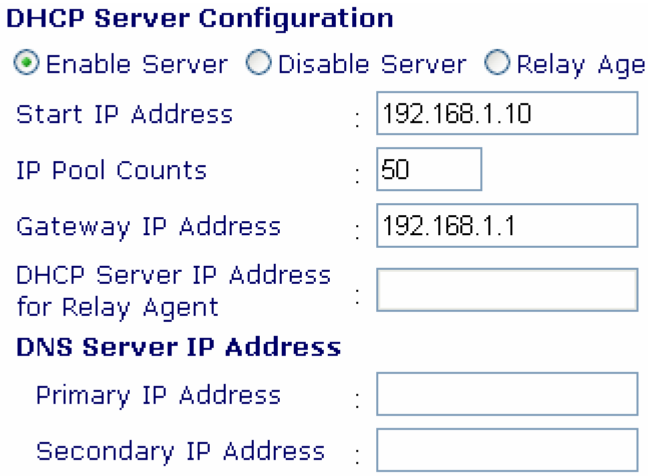
(Default: 255.255.255.0/ 24)

DHCP Server Configuration

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

Please refer to the following picture for DHCP Server Configuration.



DHCP Server Configuration

● Enable Server ○ Disable Server ○ 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

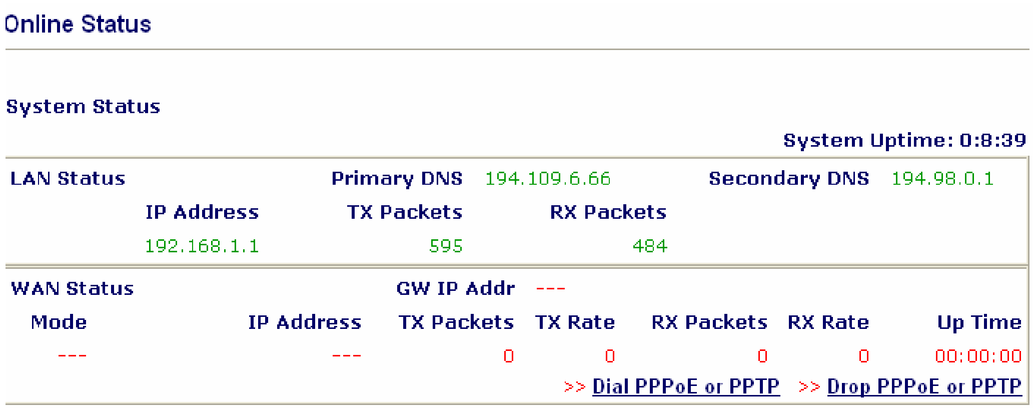
Primary IP Address :

Secondary IP Address :

Enable Server	Let the router automatically assign IP address to every PC on the LAN
Disable Server	You manually assign IP address from the router to every PC on the LAN
Relay Agent	Allows PCs on the LAN to request IP address from other DHCP server. e.g. You shall get IP from the DHCP server located at your office.
Start IP Address	Set the start IP address of the IP address pool.
IP Pool Counts	Set the number of IP address pool.
Gateway IP Address	Sets the gateway IP address for the DHCP server. Usually, it should be the same as the said IP address when the router works as a default gateway.
Start IP Address	Set the start IP address of the IP address pool.
DNS Server IP Address **(Default: None)**	DNS stands for Domain Name System. Every Internet host must have an 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 will at least provide you with at least one DNS Server IP address. If you do not specify it, the router will

	automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address	You must specify secondary DNS server IP address here because your ISP often can let you have at least one DNS Server IP address. If you do not specify 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:



Online Status

System Status

System Uptime: 0:8:39

LAN Status		Primary DNS	194.109.6.66	Secondary DNS	194.98.0.1
	IP Address	TX Packets	RX Packets		
	192.168.1.1	595	484		

WAN Status		GW IP Addr	---			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
---	---	0	0	0	0	00:00:00

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

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

Chapter 5
NAT Setup

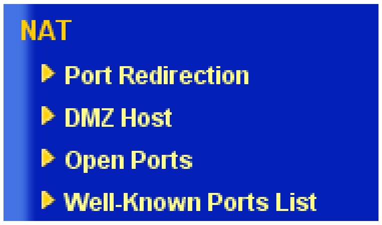
5.1 Introduction

NAT is a method of mapping one or more IP addresses and/or service ports into different specified services, where NAT stands for Network Address Translation. It allows the internal IP addresses of many computers on a Local Area Network (LAN) to be translated to one public address, saving users' cost. It also plays a security role by obscuring the true IP addresses of important machines from potential hackers on the Internet. For convenience, we called a router having the NAT facility as a NAT-enabled router.

Usually you will use your Vigor router as a NAT-enabled router. The NAT-enabled router gets one globally re-routable IP address from the ISP and assigns private network IP addresses defined by RFC-1918 to local hosts. The NAT-enable router translates the private network IP addresses to such a globally routable IP address so that local hosts can communicate with the router and access the Internet.

5.2 Settings

Click **NAT Setup** to open the setup page.



On the 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. Also, 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 method.

In the Vigor routers, we support three variants of port mapping methods: **Port Redirection**, **Open Ports**, and **DMZ host**

Port Redirection	The packet is forwarded to a specific local host if the port number matches that defined in the table. A user can also translate the port to another port locally.
Open Ports	Similar to the Port Redirection, the Open Ports facility also supports users to define a range of ports.
DMZ host	This opens up a single host completely. All incoming packets will be forwarded to the host with the local IP address you designated. The only exception is packets received in response to outgoing requests from other local computers or incoming packets that match rules in the other two methods.

It should be noticed that, while you are using combinations of these three systems, there is a priority structure. That is, if a rule in one method conflicts with a rule in another method, then there is strict precedence. This leads to a predictable result and resolution of rule-conflict. The precedence is defined as follows.

Port Redirection > Open Ports > DMZ host

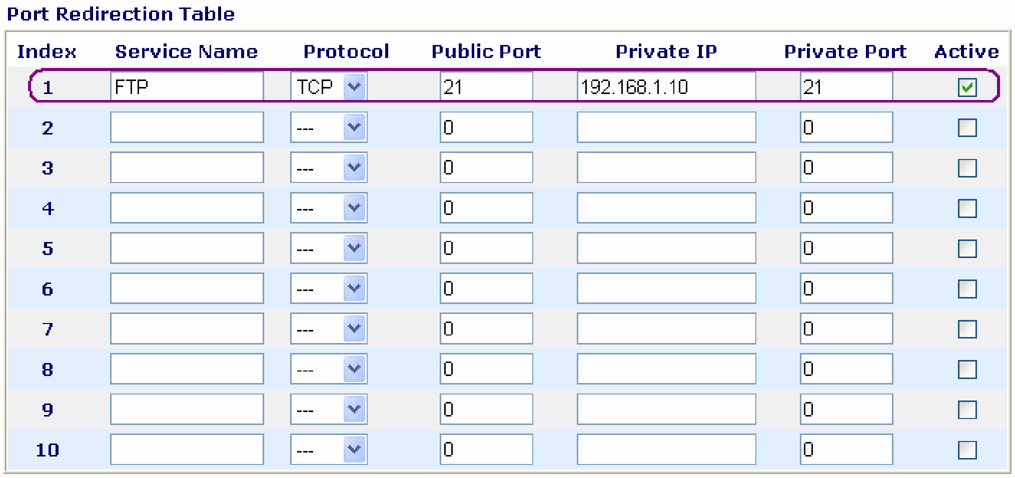
Example**:** If the port number of an incoming packet matches a rule specified in both **Port Redirection** and **Open Ports**, then the packet will be forwarded to the local address designated in **Port Redirection.**

Now, let us move on individual setting of these three port-mapping methods.

5.2.1 Port Redirection Table

The **Port Redirection** is for you to expose internal servers to the public domain. For example, you run a web server and some users want to access this web server. You also run an internal SMTP mail server for your home office and you shall allow your ISP to send whole E-mail to your SMTP mail server. Consequently, you assign different port number on the **Port Redirection Table** to different services such as http, smtp, ftp etc. External users, i.e. people elsewhere on the Internet can then access your web server via your public IP address. Even if your public IP address is a dynamic IP address, you can apply the Dynamic DNS service to obtain an online WAN IP address (such as hostnmae.dyndns.org) where is able to be mapped to your current dynamic IP address. Any external user can visit your web server simply via your online WAN IP address.

The following example shows how an internal FTP server is exposed to the public domain. The internal FTP server is running on the local host addressed as 192.168.1.10.



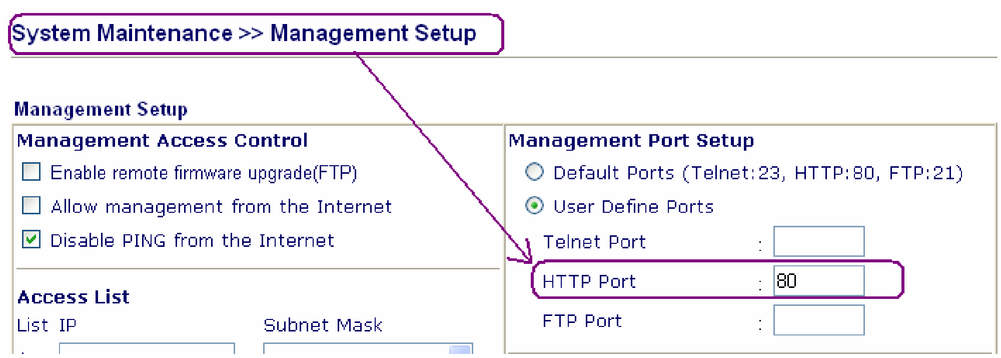
Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	FTP	TCP	21	192.168.1.10	21	☑
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	□

As shown above, the **Port Redirection Table** provides10 port-mapping entries for internal hosts.

Service Name	Specify the name for the specific network service.
Protocol	Specify the transport layer protocol (TCP or UDP).
Public Port	Specify which port should be redirected to the internal host.
Private IP	Specify the private IP address of the internal host offering the service.
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check here to activate the port-mapping entry.

Because the router has its own built-in web server for the configuration, if you want to access to the web configurator remotely and to a web server behind the router, you need to change the router's http "port" to something other than the **default port 80**. You shall change the admin port from the **Management Setup** menu and you then access the admin screen by suffixing the normal IP address of Vigor router's web configurator with 8080. e.g. **http://192.168.1.1:8080**



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

Management Port Setup

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

● User Define Ports

Telnet Port	:	
HTTP Port	:	80
FTP Port	:	

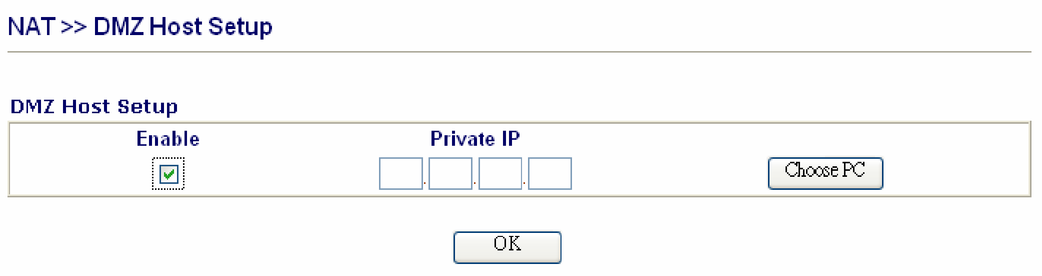
The port redirection can only be applied to external users only - i.e. the incoming traffic. The Internet users behind your LAN can not access your external public IP address and come back in; the internal users shall access the server on its local private IP address, or you can set up an alias in a Windows hosts file. Please only redirect the ports you know you have to forward rather than forward all ports. Otherwise, you will compromise the firewall-type security initially deployed by the NAT facility.

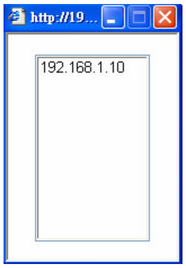
5.2.2 DMZ Host Setup

The **Port Redirection** can direct UDP/TCP traffic on particular ports to specified internal clients on the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH) do not have port numbers so you can not decide which local client to forward the data to. Vigor router has a facility called DMZ host which you can specify a single local client (with private IP address) to which ALL unsolicited data on all protocols shall be forwarded. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption.

The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. You can consider adding additional filter rules or a secondary firewall.

Click **DMZ Host Setup** to open the setup page, as shown below. The DMZ Host setting allows a defined internal user to be exposed to the Internet in order to use some special purpose applications such as Netmeeting or Internet Games etc. Each item in the setup page is described below.

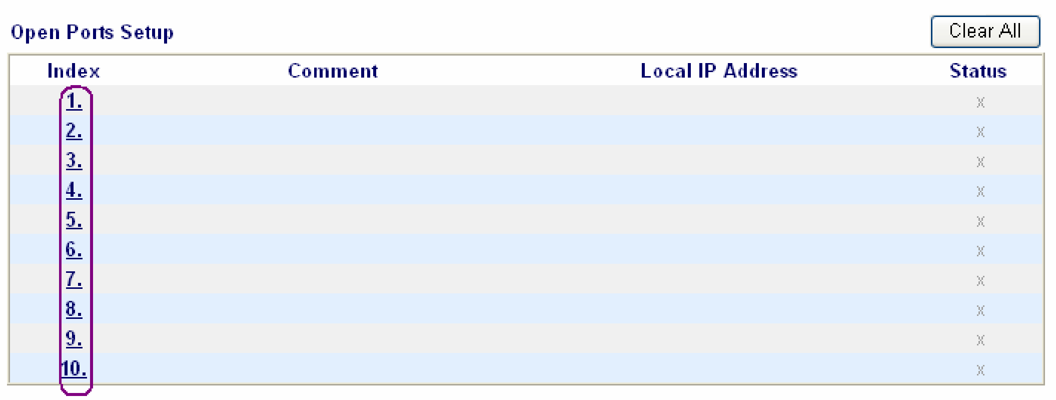


Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host.
Choose PC  http://19... 192.168.1.10	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.

5.2.3 Open Ports

As Port Redirection (above) but allows you to define **a range of** ports.

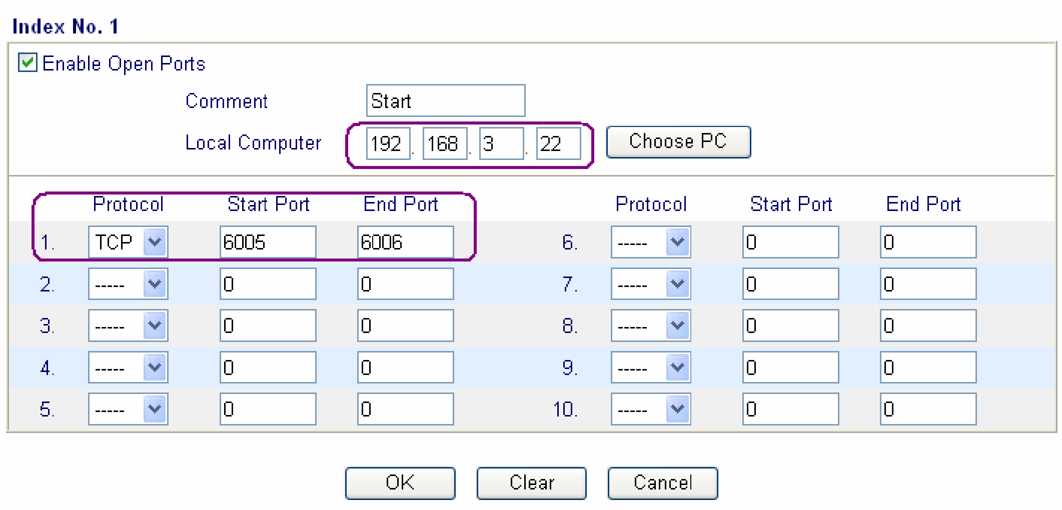
The following screen shows the **Open Ports Setup**. In the Vigor router, the **Open Ports** facility provides 10 entries for internal hosts.



Index	Comment	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.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. We use X or V to represent the Inactive or Active state.

As stated above, after you click one index number, say index No. 1, in the above figure, you will see the following setup page for the entry with index No. 1. Further, each entry (local host) can specify 10 port-ranges for diverse services. More details for individual items in the setup page are described below.



Index No. 1

☑ Enable Open Ports

Comment: Start

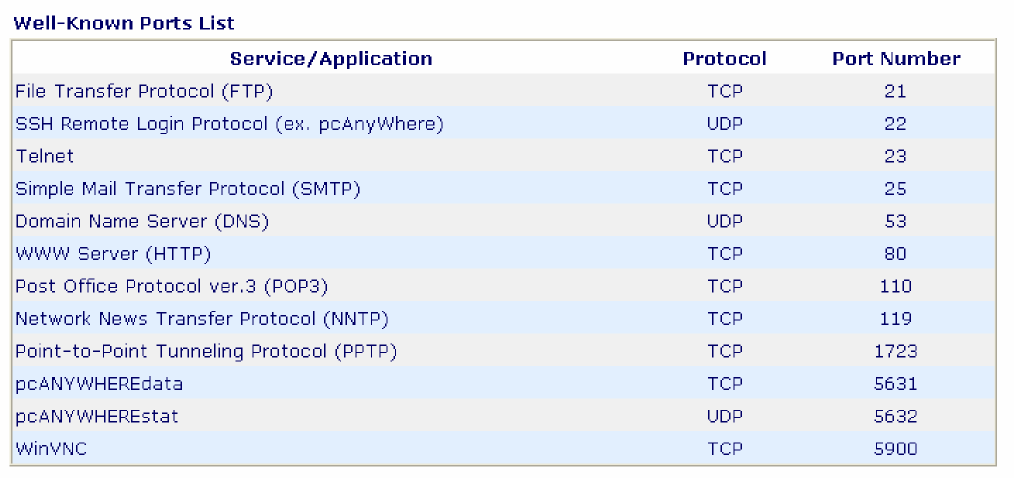
Local Computer: 192 . 168 . 3 . 22

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	6005	6006	6.	-----	0	0
2.	-----	0	0	7.	-----	0	0
3.	-----	0	0	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

Enable Open Ports	Check to enable the Open Port function for this entry.
Comment	Specify the name for the defined network service.
Local Computer	Enter the private IP address of the local host.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select one 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.

5.2.4 Well-known Port Number List

This page provides some well-known port numbers for your reference.



Well-Known Ports List

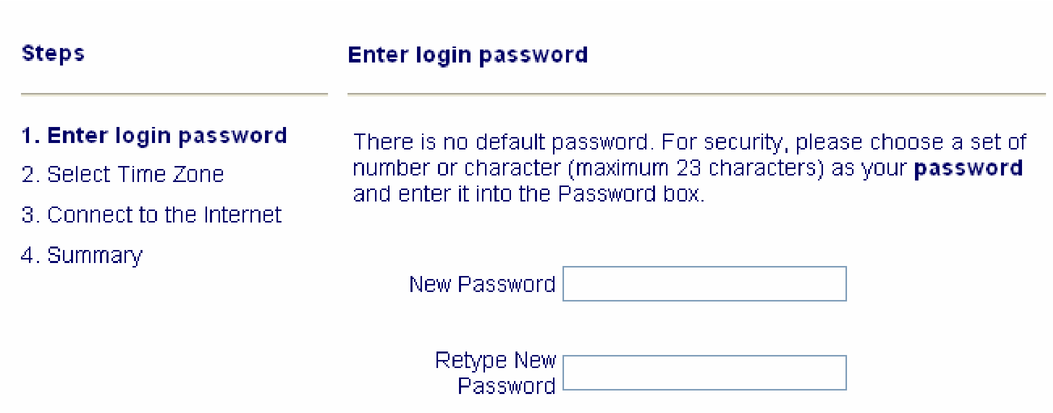
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer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

Chapter 6 Firewall Setup

6.1 Introduction

Security is top priority to be took into consideration as the users of broadband line demands more bandwidth for multimedia, interactive applications, or distance learning. The Firewall function helps protect your local network against attack from unauthorized outsiders. It also provides a way of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

Basic security is that you are recommended to set user name and password to your router when you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.



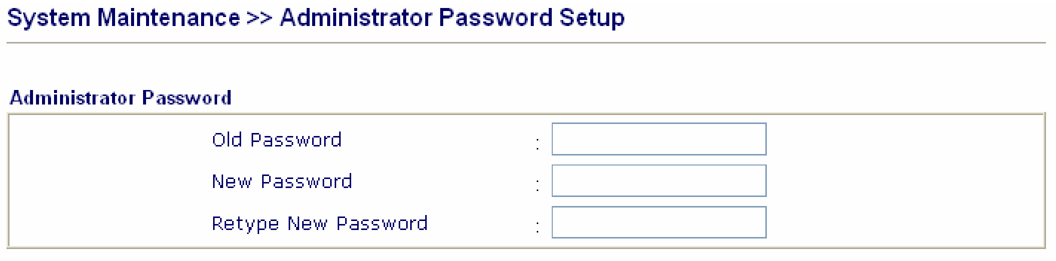
Enter login password

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

Even your installation is not set with password, you can still enter system maintenance to set up your password.



System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	:	
New Password	:	
Retype New Password	:	

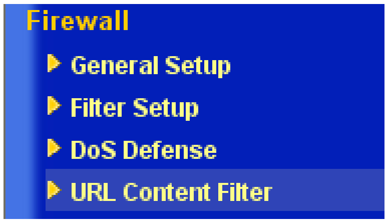
The users on the LAN are provided with secured protection by means of following firewall facilities:

- IP Filter
- Stateful Packet Inspection: tracks packets and denies unsolicited incoming data
- Selectable DoS/DDoS protection
- User-configurable packet filter

When you would like to activate SPI (Stateful Packet Inspection), please follow the path: Firewall>Edit Filter Rule>Keep State

6.2 Settings

Click **Firewall Setup** to open the setup page.

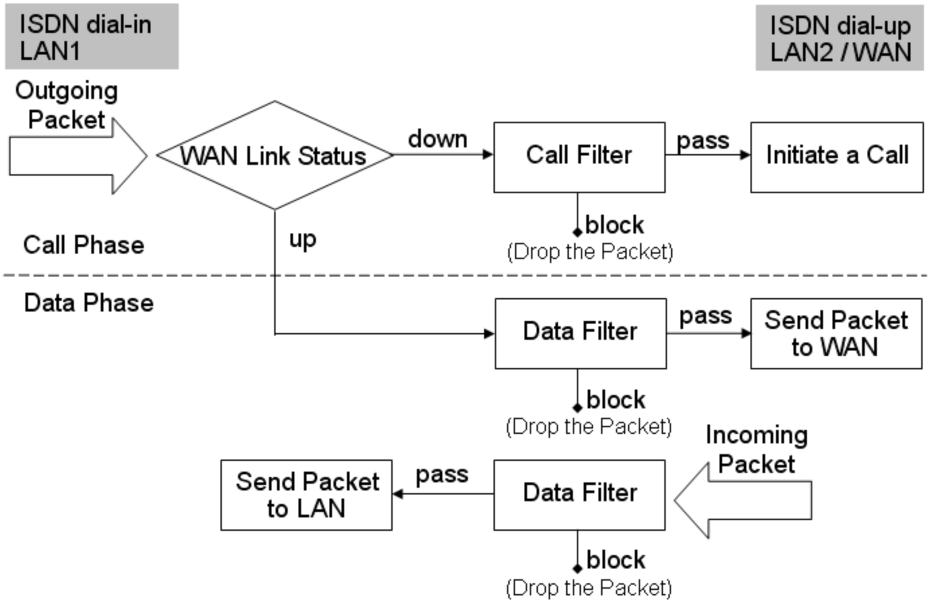


General Setup	Some general settings of Call Filter and Data Filter are available from this link.
Filter Setup	Here are 12 filter sets for IP Filter configurations..
Dos Defense	Click it to set up the DoS defense facility for detecting and mitigating the DoS attacks.
URL Content Filter	Here provides the capability of blocking inappropriate web sites to protect child in school or at home.

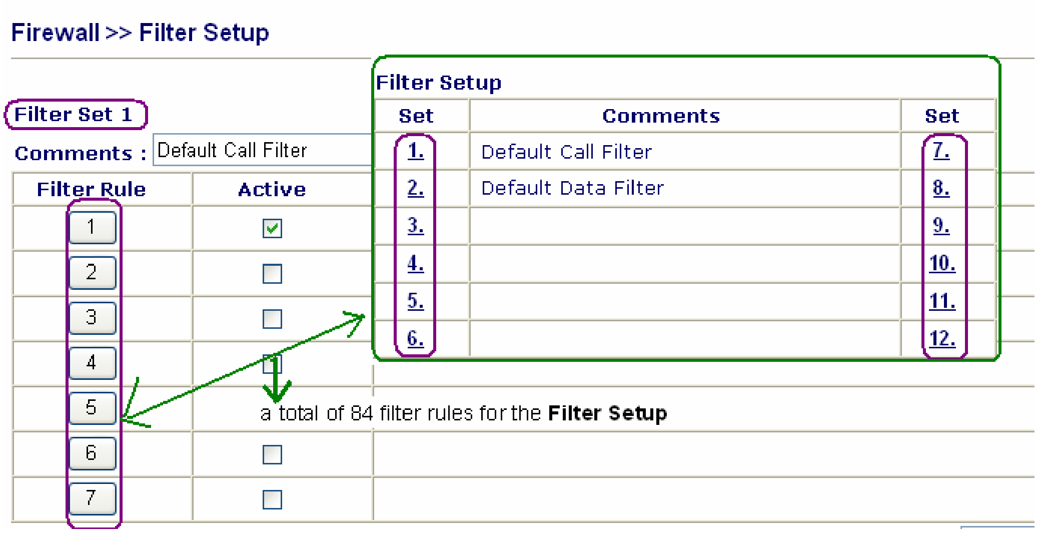
The **General Setup** function contains, by default, two types of filter sets: Call Filter set and Data Filter set. The Call Filter is used for users that attempt to establish a connection from LAN side to the Internet. The Data Filter set is used to determine what kind of IP packets is allowed to pass through the router when the WAN connection has been established.

Conceptually, when an outgoing packet is to be routed to the WAN, the IP Filter will decide if the packet should be forwarded to the Call Filter or Data Filter. If the WAN link is down, the packet will enter the Call Filter. If the packet is not allowed to trigger router dialing, it will be dropped. Otherwise, it will initiate a call to establish the WAN connection.

If the WAN link of the router is up, the packet will pass through the Data Filter. If the packet type is set to be blocked, it will be dropped. Otherwise, it will be sent to the WAN interface. Alternatively, if an incoming packet enters from the WAN interface, it will pass through the Data Filter directly. If the packet type is set to be blocked, it will be dropped. Otherwise, it will be sent to the internal LAN. The filter architecture is shown below.



The following sections will explain the settings in conjunction with the **General Setup** and **Filter Setup** The Vigor router provides 12 filter sets with 7 filter rules for each set.   As a result, there are a total of 84 filter rules for the **Filter Setup**.



Firewall >> Filter Setup

Filter Set 1

Comments : Default Call Filter

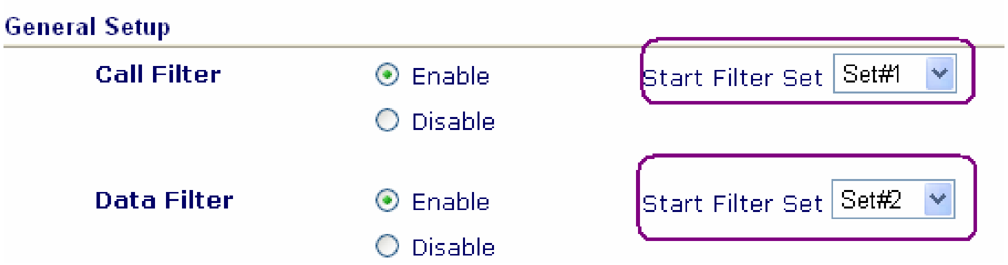
Filter Rule	Active
1	☑
2	□
3	□
4	□
5	
6	□
7	□

Filter Setup

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

a total of 84 filter rules for the **Filter Setup**

By default, the Call Filter rules are defined in Filter Set 1 and the Data Filter rules are defined in Filter Set 2.



General Setup

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

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

The **DoS Defense** functionality helps you to detect and mitigate the DoS attacks. Those attacks include the flooding-type attacks and the vulnerability attacks. The flooding-type attacks attempt to use up all your system's resource while the vulnerability attacks try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The DoS Defense Engine inspects each incoming packet against the attack signature database. Any packet that may paralyze the host in the security zone is blocked and a syslog message is sent to the client. Also the DoS Defense Engine monitors the traffic behavior. Any odd situation violating the administrator's configuration is reported and the corresponding defense function is performed in order to mitigate the attack.

The DoS/DDoS defense function can detect and protect the following attacks:

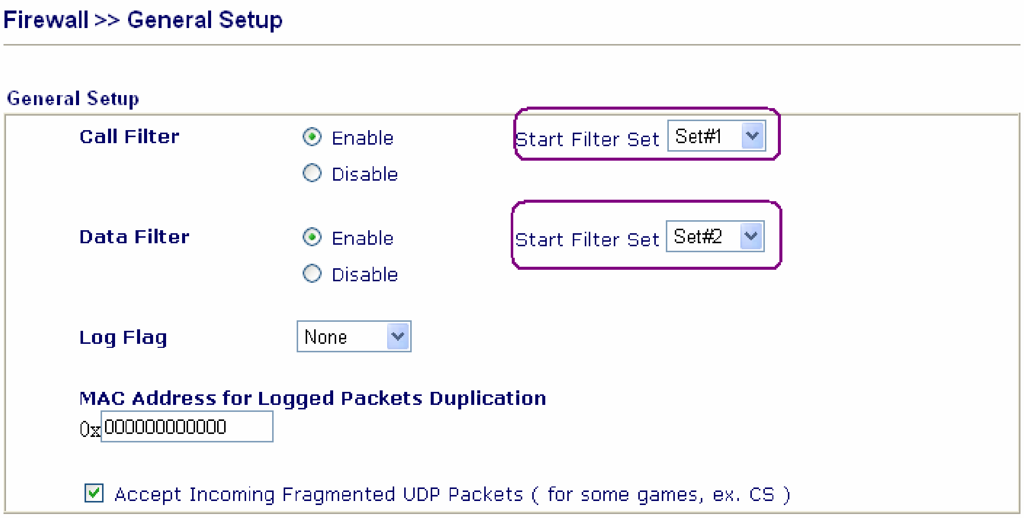
1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. TCP Flag scan
5. Trace route
6. IP options
7. Unknown protocol
8. Land attack
9. Smurf attack
10. SYN fragment
11. ICMP fragment
12. Tear drop attack
13. Fraggle attack
14. Ping of Death attack
15. TCP/UDP port scan

URL content filter systems are seen as tools that would provide the cyberspace equivalent of the physical separations that are used to limit access to some particular materials. In rating a site as objectionable, and refusing to display it on the user's computer screen, URL content filtering facilities can be used to prevent children from seeing material that their parents find objectionable. In preventing access, the URL content filtering facility acts as an automated version of the convenience-store clerk who refuses to sell adult magazines to high-school students. The URL content filtering facilities are also used by businesses to prevent employees from accessing Internet resources that are either not work related or otherwise deemed inappropriate.

The name of the URL content filtering comes from checking the content of the URL strings. Traditional firewall inspects packets based on the fields of TCP/IP headers, while the URL content filtering checks the URL strings or the payload of TCP/IP packets. In the Vigor routers, the URL content filtering facility inspects the URL string and some of HTTP data hiding in the payload of TCP packets.

6.2.1 General Setup

In the General Setup page you can enable/disable the Call Filter or Data Filter and assign a Start Filter Set for each, configure the log settings, and set a MAC address for the logged packets to be duplicated to.



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)

Some on-line games (for example: Half Life) will use UDP packets with large length to transfer data. These large UDP packets need to be fragmented. As secure firewall, Vigor router will reject these kinds of packets to avoid to be attacked by outside hackers if you do not enable “Accept Incoming Fragmented UDP Packets”. You can enable "Accept Incoming fragmented UDP Packet" function to accept these kinds of packets. Then you can play these kinds of on-line games. If you take security concern as high priority, you shall disable “Accept Incoming Fragmented UDP Packets”.

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 inactive.
Block	All blocked packets will be logged.
Pass	All passed packets will be logged.
No Match	The log function will record all packets which are matched.

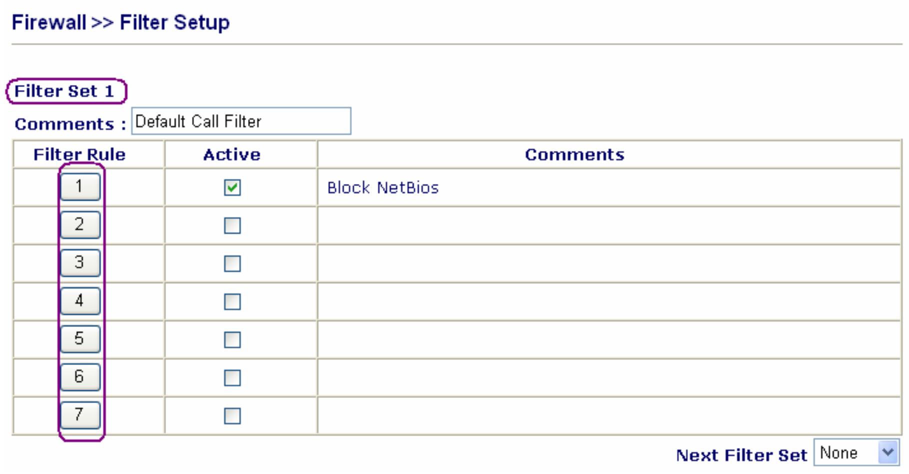
The filter log will be displayed on the Telnet terminal when you type the "log -f" command.

MAC Address for 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.

6.2.2 Filter Setup

Editing Filter Sets



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

Comments

Enter filter set comments/description.   Maximum length is 23 characters.

Filter Rules

Click a button numbered **1** ~ **7** to edit the filter rule.

Active

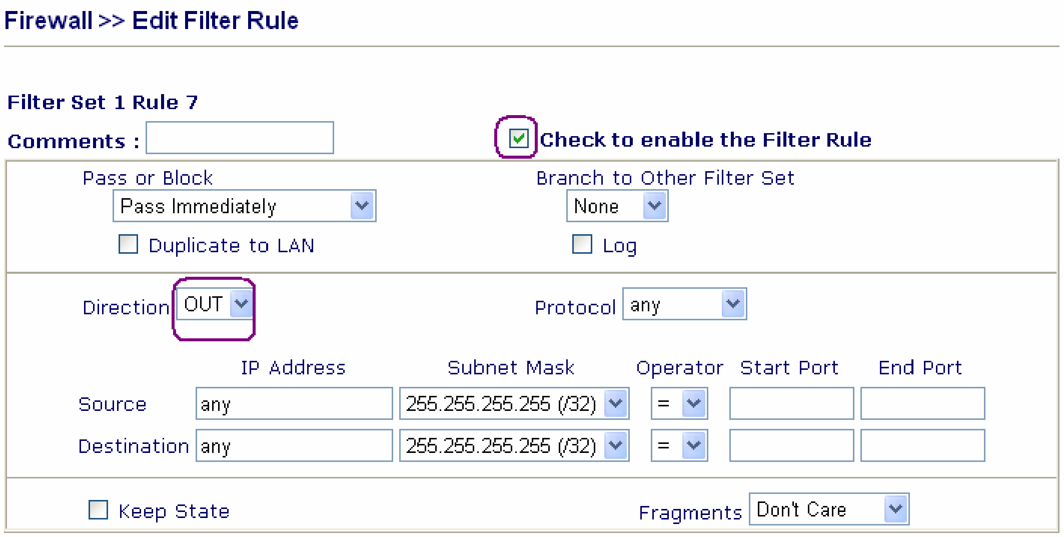
Enable or disable the filter rule.

Next Filter Set

Specifies the next filter set to be linked behind the current filter set. The filters cannot be looped.

Editing Filter Rules

Click the Filter Rule index button to enter the Filter Rule setup page for each filter. The following explains each configurable item in detail.



Firewall >> Edit Filter Rule

Filter Set 1 Rule 7

Comments :

☑ **Check to enable the Filter Rule**

Pass or Block: Pass Immediately

Branch to Other Filter Set: None

□ Duplicate to LAN

□ Log

Direction: OUT

Protocol: any

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

□ Keep State

Fragments: Don't Care

Comments

Enter filter set comments/description. Maximum length is 14 characters.

Check to enable the Filter Rule

Enables the filter rule.

Pass or Block

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

Block Immediately	Packets matching the rule will be dropped immediately.
Pass Immediately	Packets matching the rule will be passed immediately.
Block If No Further Match	A packet matching the rule, and that does not match further rules, will be dropped.
Pass If No Further Match	A packet matching the rule, and that does not match further rules, will be passed through.

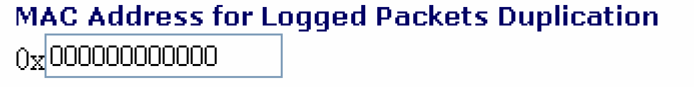
Branch to other Filter Set

If the packet matches the filter rule, the next filter rule will branch to the specified filter set.

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.**



MAC Address for Logged Packets Duplication

0x 000000000000

Log

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

Direction

Sets the direction of packet flow. For the Call Filter, this setting is irrelevant.

Keep State and Fragments (for Data Filter only)

These should be accompanied by the below settings also.

IN: Specify the rule for filtering incoming packets.

OUT: Specify the rule for filtering outgoing packets.

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

IP Address: Specify a source and destination IP address for this filter rule to apply to. Place the symbol **!** before a particular IP Address will prevent this rule from being applied to that IP address. It is equal to the logical NOT operator.

Subnet Mask: Specify the Subnet Mask for the IP Address column for this filter rule to apply to.

Operator: 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.

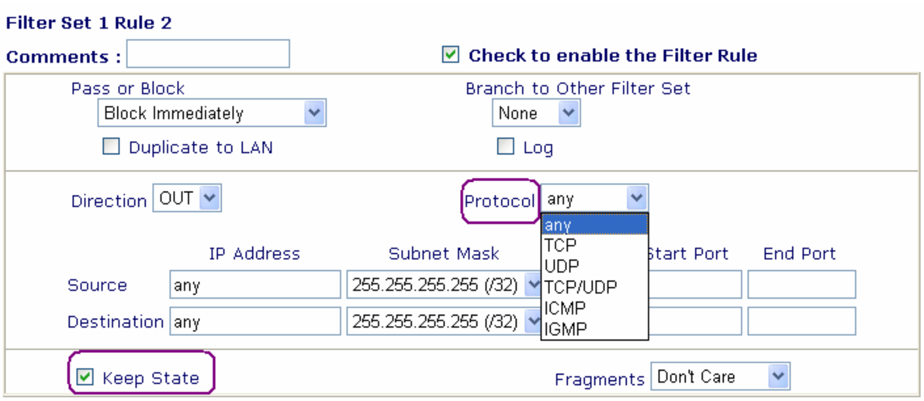
= : If the **End Port** is empty, the filter rule will set the port number to be the value of the **Start Port**. Otherwise, the port number ranges between the **Start Port** and the **End Port** (including the **Start Port** and the **End Port**).

!= : 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: i.e. **Stateful Packet Inspection.** It tracks packets and denies unsolicited incoming data. On the protocol entry, you can choose TCP or UDP or TCP/UDP or ICMP.



Filter Set 1 Rule 2

Comments :

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Duplicate to LAN

□ Log

Direction: OUT

Protocol: any

	IP Address	Subnet Mask	Start Port	End Port
Source	any	255.255.255.255 (/32)		
Destination	any	255.255.255.255 (/32)		

☑ Keep State

Fragments: Don't Care

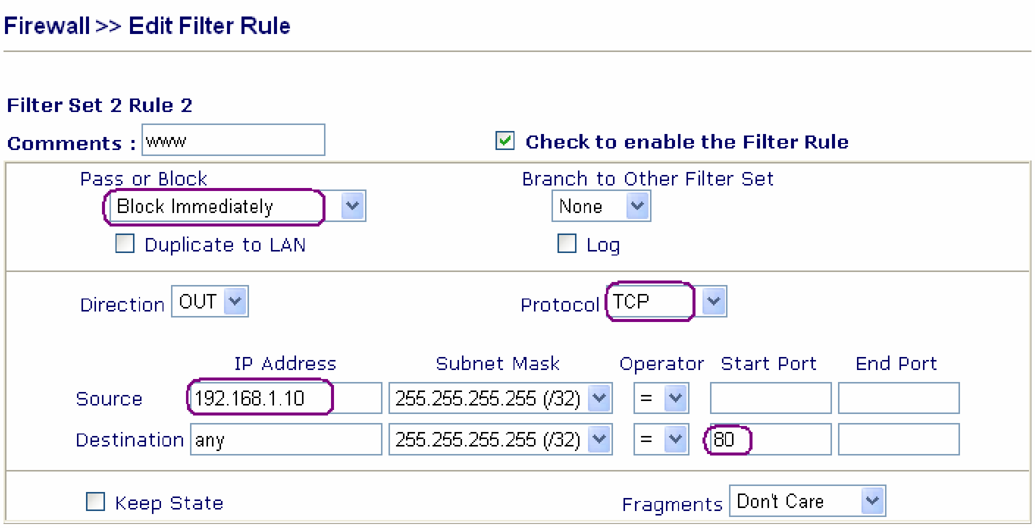
Fragments: Specify a fragmented packets action.

Don't care	Specify no fragment options in the filter rule.
Unfragmented	Apply the rule to unfragmented packets.
Fragmented	Apply the rule to fragmented packets.
Too Short	Apply the rule only to packets which 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 2 Rule 2

Comments : www

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Duplicate to LAN

□ Log

Direction: OUT

Protocol: TCP

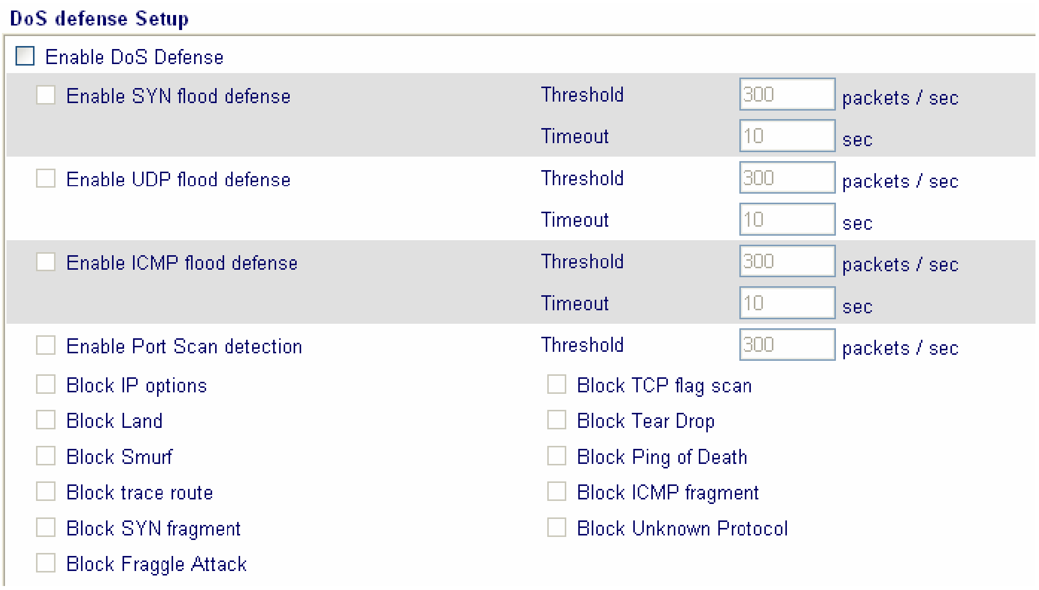
	IP Address	Subnet Mask	Operator	Start Port	End Port
Source	192.168.1.10	255.255.255.255 (/32)	=		
Destination	any	255.255.255.255 (/32)	=	80	

□ Keep State

Fragments: Don't Care

6.2.3 DoS (Denial of Service) Defense

The following sections will explain in more detail about DoS Defense Setup by using the Web Configurator. It is a sub-functionality of IP Filter/Firewall. There are a total of 15 kinds of defense function for the DoS Defense Setup. By default, the DoS Defense functionality is disabled. Further, once the DoS Defense functionality is enabled, the default values for the threshold and timeout values existing in some functions are set to 300 packets per second and 10 seconds, respectively. A brief description for each item in the DoS defense function is shown below.



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 Unknown Protocol
□ Block Fraggle Attack	

Enable Dos Defense

Click the checkbox to activate the DoS Defense Functionality.

Enable SYN flood defense

Click the checkbox to activate the SYN flood defense function. If the amount of the TCP SYN packets from the Internet exceeds the user-defined threshold value, the Vigor router will be forced to discard randomly the sequent TCP SYN packets in the user-defined timeout period. The main goal is to protect the Vigor router against the TCP SYN packets that intend to use up the router's limited-resource. By default, the threshold and timeout values are set to 300 packets per second and 10 seconds, respectively.

Enable UDP defense

Click the checkbox to activate the UDP flood defense function. Once the UDP packets from the Internet exceed the user-defined threshold value, the router will be forced to discard all sequent UDP packets in the user-defined timeout period. The default setting for threshold and timeout are 300 packets per second and 10 seconds, respectively.

Enable ICMP flood defense

Click the checkbox to activate the ICMP flood defense function. Similar to the UDP flood defense function, the router will discard the ICMP echo requests coming from the Internet, once they exceed the user-defined threshold (by default, 300 packets per second) in a period of time (by default, 10 second for timeout).

Enable PortScan detection

Port scan attacks occur by sending packets with different port numbers in an attempt to scanning the available services that one port will respond. To examine such exploration behavior, please click the checkbox to activate the Port Scan detection function in your Vigor router. The Vigor router will identify it and report a warning message if the port-scanning rate in packets per second exceeds the user-defined threshold value. By default, the Vigor router sets the threshold as 300 packets per second to detect such a scanning activity.

Block IP options

Click it to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field appeared in the datagram header. The IP option provides a way for hosts to send some significant information, such as security, compartmentation, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc., which an outsider can analyze to learn details about your private networks.

Block Land

Click the associated checkbox and then enforce the Vigor router to defense the Land attacks. The LAN attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets having the identical source and destination addresses, as well as the port number, with those of the victim.

Block Smurf

Click the checkbox to activate the Block Smurf function. The Vigor router will reject any ICMP echo request destined to the broadcast address.

Block Block trace router

Click the checkbox to activate this function. The Vigor router will not forward any trace route packets.

Block SYN fragment

Click the checkbox to activate the Block SYN fragment function. Any packets having SYN flag and more fragment bit set will be dropped.

Block Fraggle Attack

Click the checkbox 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 broadcst UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.

Block TCP flag scan

Click the checkbox 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

Click the checkbox 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

Click the checkbox 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. Any packets realizing this attacking activity will be blocked by the Vigor routers.

Block ICMP Fragment

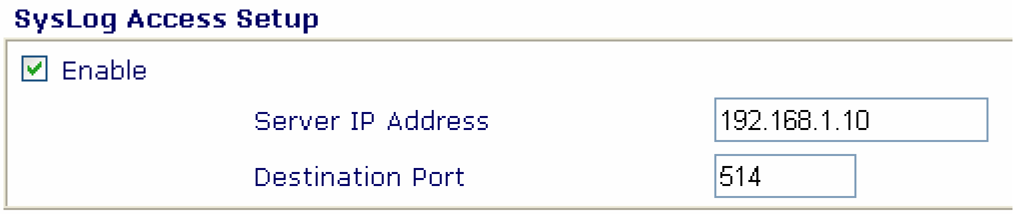
Click the checkbox to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

Block Unknown Protocol

Click the checkbox 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

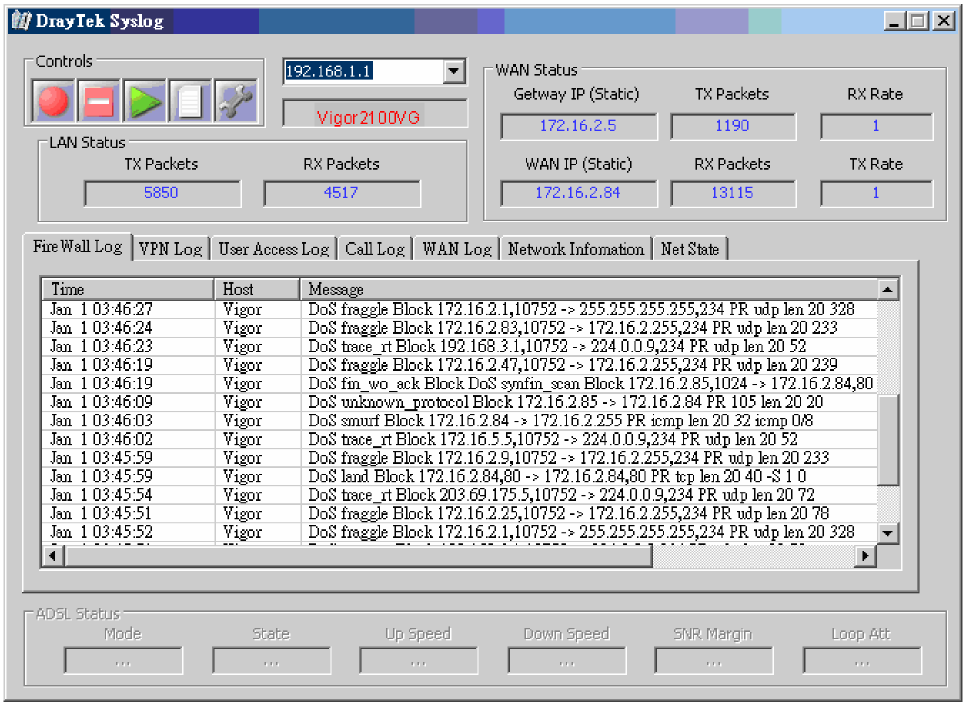
All the warning messages will be sent to syslog client after you enable the syslog function. The administrator can setup the syslog client in the **Syslog Setup** by using Web Configurator. Thus, the administrator can look at the warning messages from DoS Defense functionality through the DrayTek Sylsog daemon. The format for this kind of the warning messages is similar to those in **IP Filter**/**Firewall** except for the preamble keyword "DoS", followed by a name to indicate what kind of attacks is detected.



SysLog Access Setup

☑ Enable

Server IP Address	192.168.1.10
Destination Port	514



DrayTek Syslog

Controls: 192.168.1.1 — Vigor2100VG

LAN Status

TX Packets	RX Packets
5850	4517

WAN Status

Getway IP (Static)	TX Packets	RX Rate
172.16.2.5	1190	1
WAN IP (Static)	**RX Packets**	**TX Rate**
172.16.2.84	13115	1

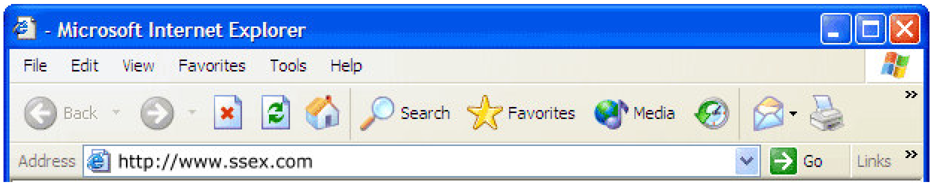
Time	Host	Message
Jan 1 03:46:27	Vigor	DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328
Jan 1 03:46:24	Vigor	DoS fraggle Block 172.16.2.83,10752 -> 172.16.2.255,234 PR udp len 20 233
Jan 1 03:46:23	Vigor	DoS trace_rt Block 192.168.3.1,10752 -> 224.0.0.9,234 PR udp len 20 52
Jan 1 03:46:19	Vigor	DoS fraggle Block 172.16.2.47,10752 -> 172.16.2.255,234 PR udp len 20 239
Jan 1 03:46:19	Vigor	DoS fin_wo_ack Block DoS synfin_scan Block 172.16.2.85,1024 -> 172.16.2.84,80
Jan 1 03:46:09	Vigor	DoS unknown_protocol Block 172.16.2.85 -> 172.16.2.84 PR 105 len 20 20
Jan 1 03:46:03	Vigor	DoS smurf Block 172.16.2.84 -> 172.16.2.255 PR icmp len 20 32 icmp 0/8
Jan 1 03:46:02	Vigor	DoS trace_rt Block 172.16.5.5,10752 -> 224.0.0.9,234 PR udp len 20 52
Jan 1 03:45:59	Vigor	DoS fraggle Block 172.16.2.9,10752 -> 172.16.2.255,234 PR udp len 20 233
Jan 1 03:45:59	Vigor	DoS land Block 172.16.2.84,80 -> 172.16.2.84,80 PR tcp len 20 40 -S 1 0
Jan 1 03:45:54	Vigor	DoS trace_rt Block 203.69.175.5,10752 -> 224.0.0.9,234 PR udp len 20 72
Jan 1 03:45:51	Vigor	DoS fraggle Block 172.16.2.25,10752 -> 172.16.2.255,234 PR udp len 20 78
Jan 1 03:45:52	Vigor	DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328

ADSL Status

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

6.2.4 URL Content Filter

The URL content filtering facility in Vigor routers inspects every URL string in the HTTP request initiated inside against the keyword list. If the entire or part of the URL string (for instance, http://www.ssex.com as shown) matches any activated keyword, the Vigor router will block its associated HTTP request and a syslog message will be automatically sent to the syslog client. Also any request that tries to retrieve the malicious code will be discarded by the Vigor router. Similarly, a syslog message will be sent to the syslog client.



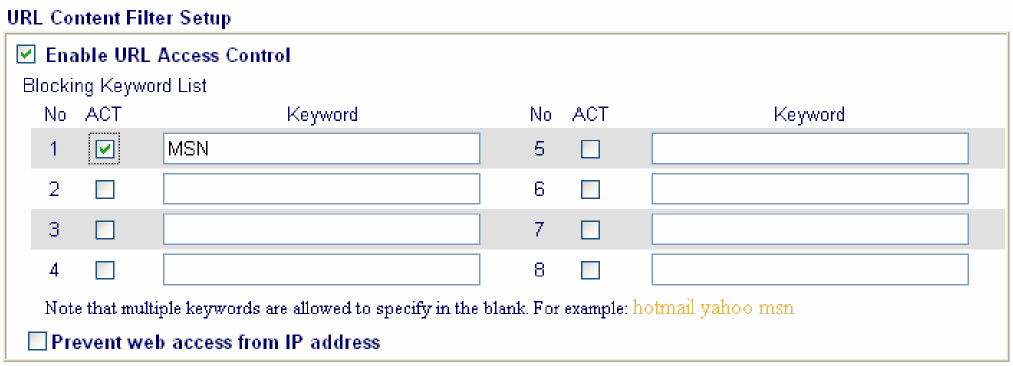
Address: http://www.ssex.com

The URL content filtering facility prevents users from accessing inappropriate websites whose URL strings are identified as prohibition.

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

<u>Enable URL Access Control</u>

One checkbox appears giving the choice to activate the *URL Access Control* or not. To enable it, click on the empty box image and, subsequently, the hook image (√) will appear.



URL Content Filter Setup

☑ Enable URL Access Control

Blocking Keyword List

No	ACT	Keyword	No	ACT	Keyword
1	☑	MSN	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

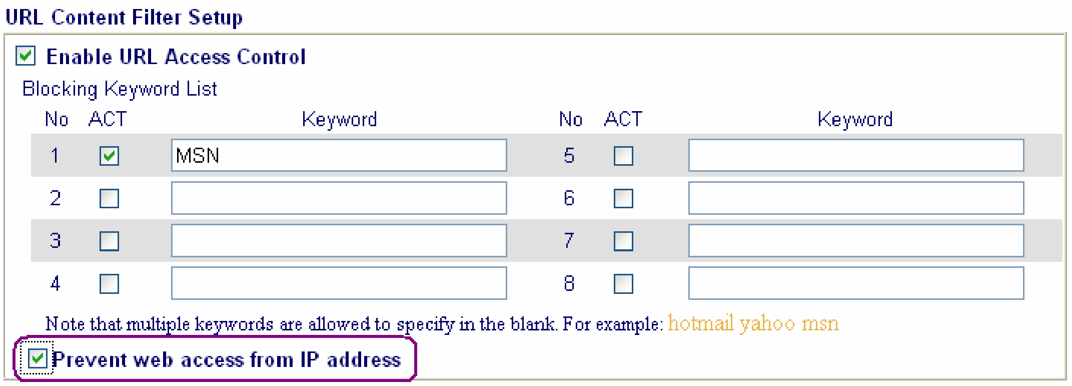
Block Keyword List: The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal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

If you want to filter any website whose URL string contains “sex”, “fuck”, “gun”, or “drug”, you should add these words into the frames. Thus, your Vigor router will automatically deny any web surfing that its associated URL string contains any one of the list’s keywords.

Considering that the user tries to access www.backdoor.net/images/sex /p_386.html, the Vigor router will cut the connection because this website is prohibited.

Further, the URL content filtering facility also allows you to specify either a complete URL string (e.g., “www.whitehouse.com” and “www.hotmail.com”) or a partial URL string (e.g., “yahoo.com”) in the blocking keyword list.

Prevent Web Access by IP Address: One checkbox is available to activate this function that will deny any web surfing activity by directly using IP address. To enable it, click on the empty box image and, subsequently, the hook image (√) will appear.



URL Content Filter Setup

☑ Enable URL Access Control

Blocking Keyword List

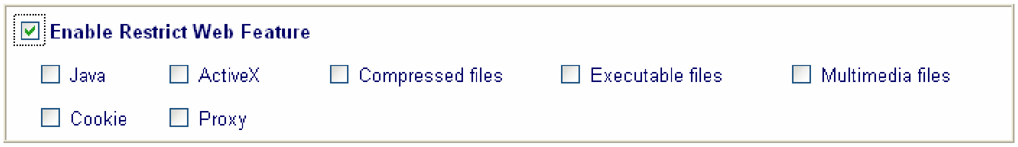
No	ACT	Keyword	No	ACT	Keyword
1	☑	MSN	5	□	
2	□		6	□	
3	□		7	□	
4	□		8	□	

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

It will be of great value to provide the protection mechanism that prohibits the malicious codes from downloading from web pages. The malicious codes may embed in some executable objects, such as *ActiveX*, *Java Applet*, *compressed files*, and *executable files*, and, if they have been downloaded from websites, would bring a threat of the user's system. For example, an ActiveX object can be downloaded and run from the web page. If the ActiveX object has some malicious code in it, it may own unlimited access to the user's system.



☑ Enable Restrict Web Feature

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

□ Cookie □ Proxy

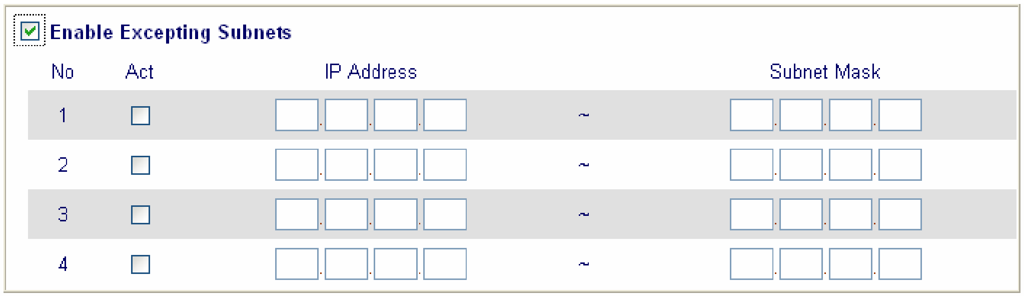
Java	Click the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.
ActiveX	Click the checkbox to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.
Compressed file	One checkbox appears giving the choice 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** To enable it, click on the empty box image and, subsequently, the hook image (√) will appear.
Executable file	Similar to the above function, click the checkbox to enable the Block Executable file function to reject any downloading behavior of the executable file from the Internet. To enable it, click on the empty box image and, subsequently, the hook image (√) will appear. Accordingly, files with the following extensions will be blocked by the Vigor router. **.exe,.com,.scr,.pif,.bas,.bat,inf,.reg**

A so-called *cookie* feature introduced by Netscape allows you to keep a close watch on the activities of HTTP request and responses of individual sessions. Many websites use them to create stateful sessions for tracking Internet users, which will violate the users' privacy. Thus, the Vigor router provides the *Cookies filtering facility* that allows you to filter cookie transmission from inside to outside world. Furthermore, the Vigor router also allows you to filter out all proxy-related transmission in order to support stronger security.

Cookie	Click the checkbox to activate the Block Cookie transmission. The Vigor router will filter out the cookie transmission from inside to outside world in order to protect the local user's privacy.
Proxy	One checkbox appears giving the choice to activate this function to reject any proxy transmission. To enable it, click on the empty box image and, subsequently, the hook image ( ) will appear. 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. To enable it, click on the empty box image and, subsequently, the hook image (√) will appear. 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

4 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. The hook image (√) appears to indicate the entry is active. To disable an entry, click on the hook image (√).

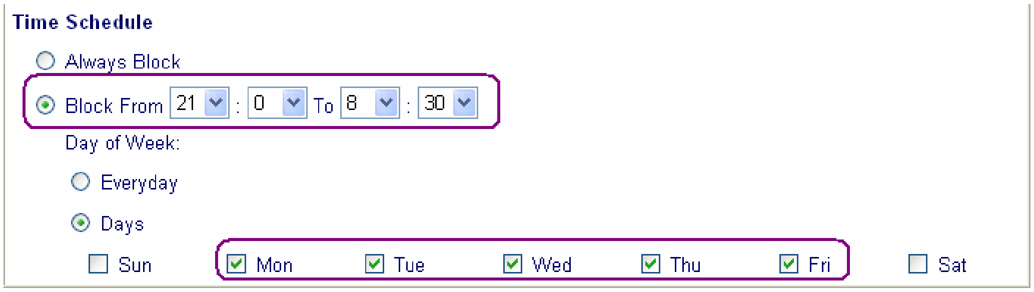


☑ Enable Excepting Subnets

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

Time Schedule

Specify what time should perform the URL content filtering facility.



Time Schedule

○ Always Block

● Block From 21 : 0 To 8 : 30

Day of Week:

○ Everyday

● Days

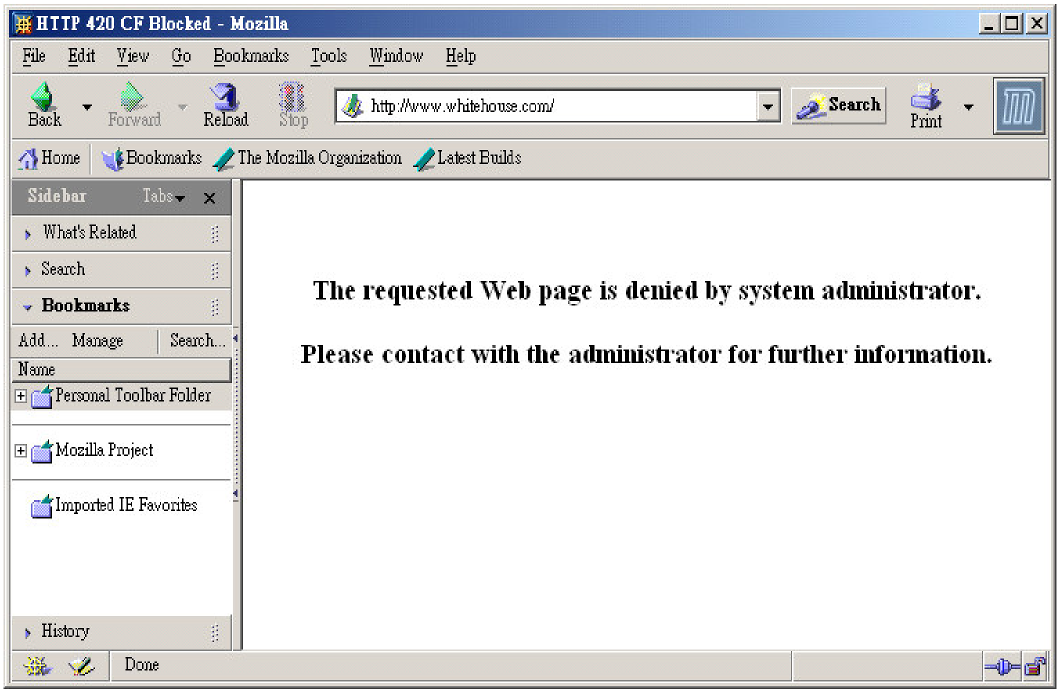
□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

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.

Warning Messages

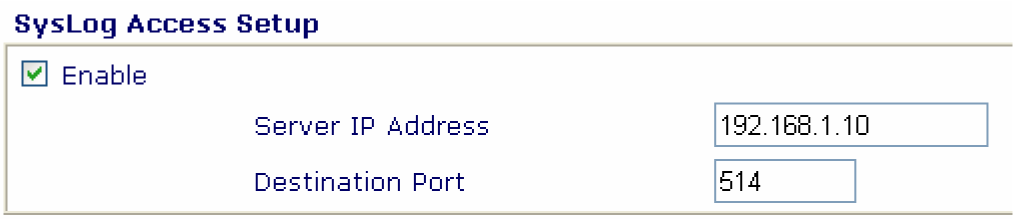
When a HTTP request is denied, an alert page will appear in your browser, as shown in the following figure.



The requested Web page is denied by system administrator.

Please contact with the administrator for further information.

Also, the warning message will be automatically sent to the syslog client after you enable the syslog function. The administrator can setup the syslog client in the **Syslog Setup** by using Web Configurator. Thus, the administrator can view the warning messages from the **URL Content Filtering** functionality through the DrayTek Sylsog daemon. The format for this kind of the warning messages is similar to those in the **IP Filter/Firewall** except for the preamble keyword “**CF**”, followed by a name to indicate what kind of the HTTP request is blocked.

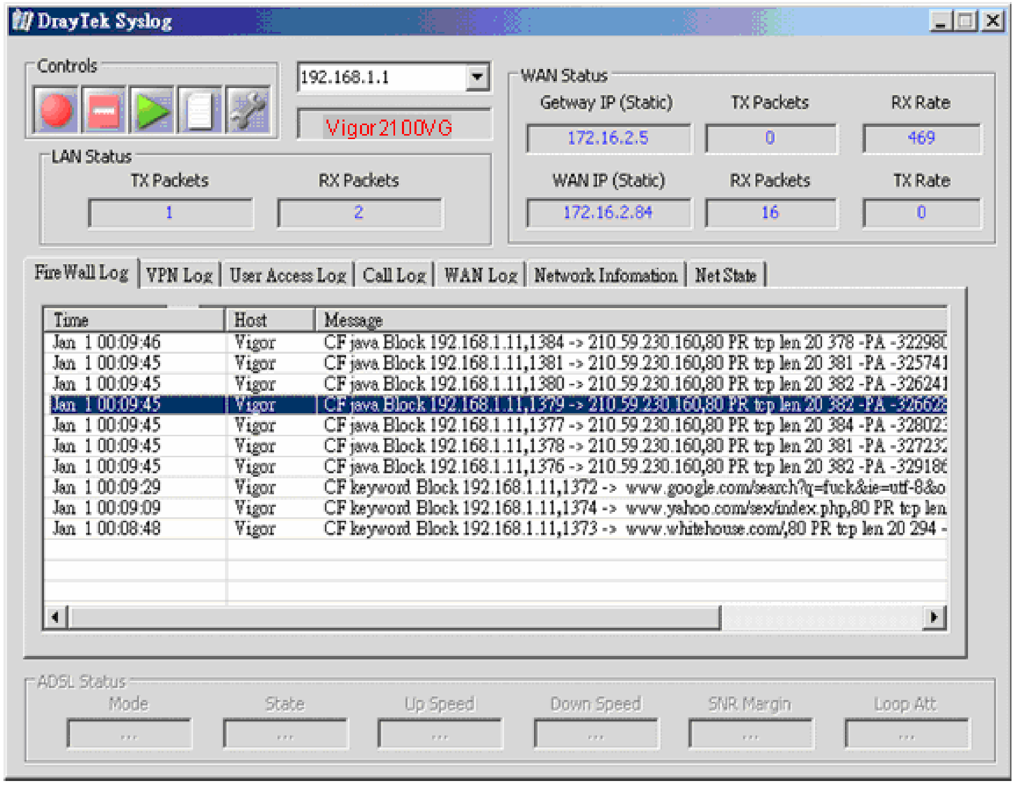


SysLog Access Setup

☑ Enable

Server IP Address: 192.168.1.10

Destination Port: 514



192.168.1.1

Vigor2100VG

WAN Status

Getway IP (Static)	TX Packets	RX Rate
172.16.2.5	0	469
WAN IP (Static)	**RX Packets**	**TX Rate**
172.16.2.84	16	0

LAN Status

TX Packets	RX Packets
1	2

```
Time             Host    Message
Jan  1 00:09:46  Vigor   CF java Block 192.168.1.11,1384 -> 210.59.230.160,80 PR tcp len 20 378 -PA -32298
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1381 -> 210.59.230.160,80 PR tcp len 20 381 -PA -325741
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1380 -> 210.59.230.160,80 PR tcp len 20 382 -PA -326241
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1379 -> 210.59.230.160,80 PR tcp len 20 382 -PA -32662
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1377 -> 210.59.230.160,80 PR tcp len 20 384 -PA -32802
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1378 -> 210.59.230.160,80 PR tcp len 20 381 -PA -32723
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1376 -> 210.59.230.160,80 PR tcp len 20 382 -PA -32918
Jan  1 00:09:29  Vigor   CF keyword Block 192.168.1.11,1372 ->  www.google.com/search?q=fuck&ie=utf-8&o
Jan  1 00:09:09  Vigor   CF keyword Block 192.168.1.11,1374 ->  www.yahoo.com/sex/index.php,80 PR tcp len
Jan  1 00:08:48  Vigor   CF keyword Block 192.168.1.11,1373 ->  www.whitehouse.com/,80 PR tcp len 20 294 -
```

ADSL Status

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

Chapter 7 Application Setup

7.1 Introduction

This section includes **Dynamic DNS, Call Schedule, RADIUS setup, UpnP settings**.

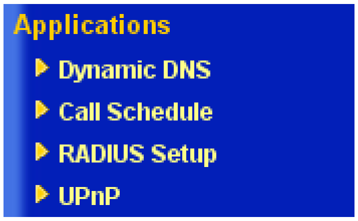
Before you set up the **Dynamic DNS** (Domain Name Server) function, you have to subscribe free domain names from the Dynamic DNS service providers. The Vigor router provides up to three accounts for the function and supports the following providers: www.dynsns.org, www.dynamic-nameserver.com, www.no-ip.com, www.dtdns.com, www.changeip.com. You should visit their websites to register your own domain name for the router. The Dynamic DNS function allows the router to update its online WAN IP address which assigned by ISP to 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.

Call Schedule facility is used to control the router's dialer or connection manager what time should be up or down according to the pre-defined call schedule profiles. Before configuring the Call Schedule function, you have to set up time function properly and arrange schedules for specified Internet access profile or LAN-to-LAN profile. The Vigor router has built a real time clock which can update itself from your browser manually or automatically from an Internet time server (NTP). As a result, you can schedule the router to dial to Internet at a pre-set time, but also to restrict Internet access to certain hours so that the router will only let users of LAN to access Internet at certain times (e.g. business hours).

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 provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

7.2 Settings

Click **Application Setup** to open the setup page.



Dynamic DNS	Settings of domain names you subscribe from up to three Dynamic DNS service providers.
Call Schedule	Settings of a real time clock that update automatically from an Internet time server (NTP).

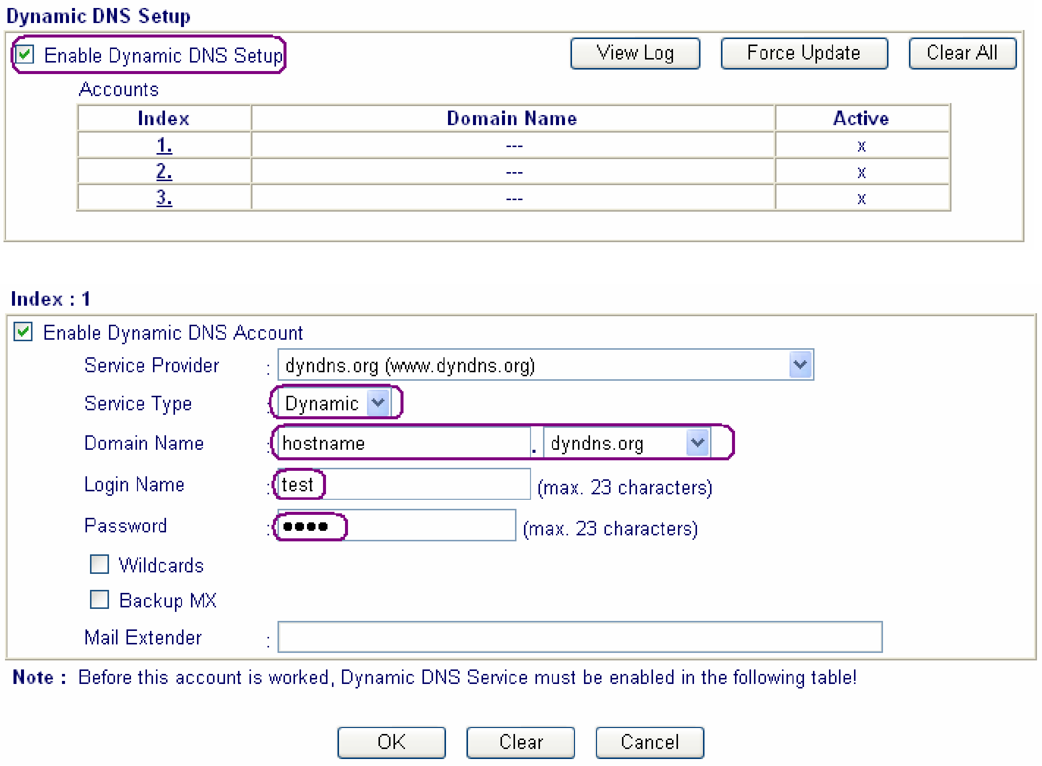
RADIUS Setup	Settings of RADIUS server
UPnP	Settings of UPnP protocol available for directly connected PC peripherals with the existing Windows 'Plug and Play' system.

7.2.1 Dynamic DNS

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** and Index number **1** to add an account for the router. And now, you will see the following web page.



Dynamic DNS Setup

☑ Enable Dynamic DNS Setup

Accounts

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

Index : 1

☑ Enable Dynamic DNS Account

Service Provider	:	dyndns.org (www.dyndns.org)
Service Type	:	Dynamic
Domain Name	:	hostname . dyndns.org
Login Name	:	test (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!

3. 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***.

4. Push **OK** button to activate the settings.

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.

Validation and Troubleshooting

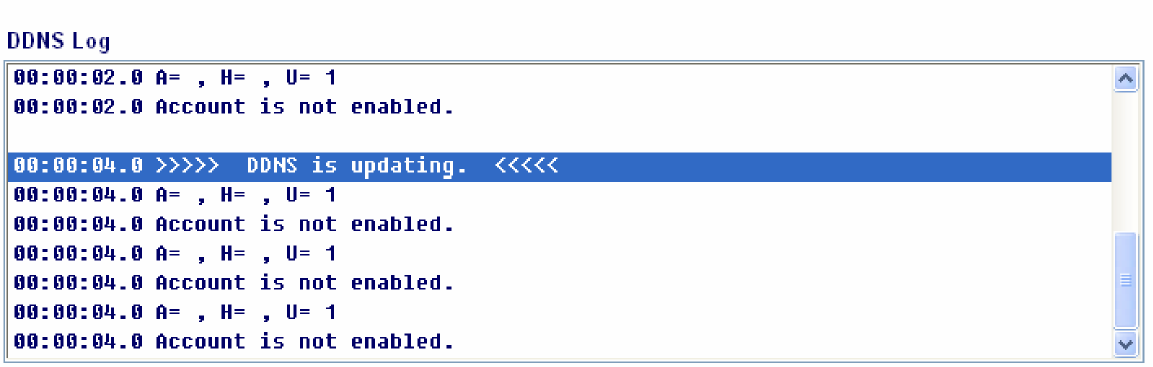
Ping the Registered Domain Name

1. After router is online, use PING utility to probe your registered domain name in order to verify if it works.
2. Login **Online Status** in the main menu to make sure the responded IP address from the Dynamic DNS server should be the same as router's WAN IP address.

View the DDNS Logs

1. Applications >> Dynamic DNS Setup.

2. Push **View Log** button. The logs of DDNS updates will be shown as follows.



DDNS Log

```
00:00:02.0 A= , H= , U= 1
00:00:02.0 Account is not enabled.

00:00:04.0 >>>>>  DDNS is updating.  <<<<<
00:00:04.0 A= , H= , U= 1
00:00:04.0 Account is not enabled.
00:00:04.0 A= , H= , U= 1
00:00:04.0 Account is not enabled.
00:00:04.0 A= , H= , U= 1
00:00:04.0 Account is not enabled.
```

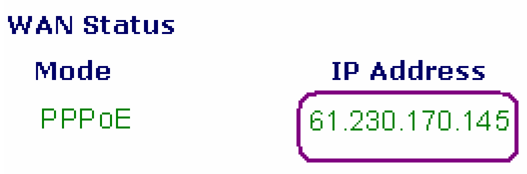
Where A : Login Name

H : Domain Name without suffix.

Return Code= good 61.230.170.145

If you have any DDNS update issues, the logs are useful to find where the problem is.

3. Click **Online Status** to know what the current WAN IP address is.



WAN Status

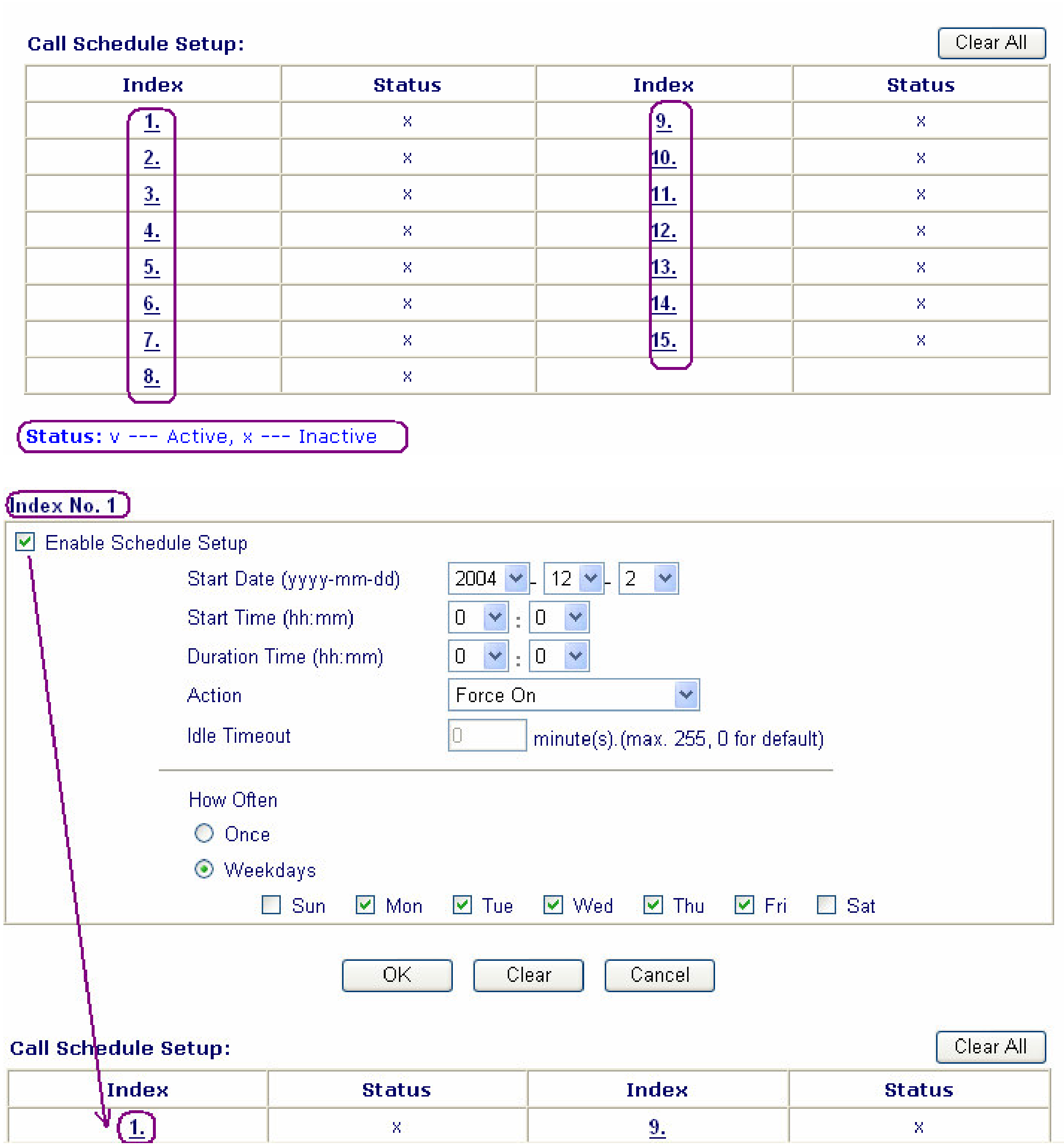
Mode	IP Address
PPPoE	61.230.170.145

You will see the IP address in the circle, which is the same as the Return Code in the DDNS logs. This indicates that the update is successful.

7.2.2 Call Schedule

On the **Time Setup** menu, if you press **Inquire Time** button, the router's clock will be set to current time of your PC. The clock will reset if you power down or reset the router so you may prefer to use an NTP server on the Internet (a time server) to update the clock automatically. NTP updates only occur when the router is online to the Internet; they will not trigger calls themselves.

You can have up to 15 entries of different schedules and you must then apply the required schedule(s) to the appropriate ISP by entering the schedule number into the ISP setup:



Call Schedule Setup: [Clear All]

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

Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd)	2004 - 12 - 2
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

[OK] [Clear] [Cancel]

Call Schedule Setup: [Clear All]

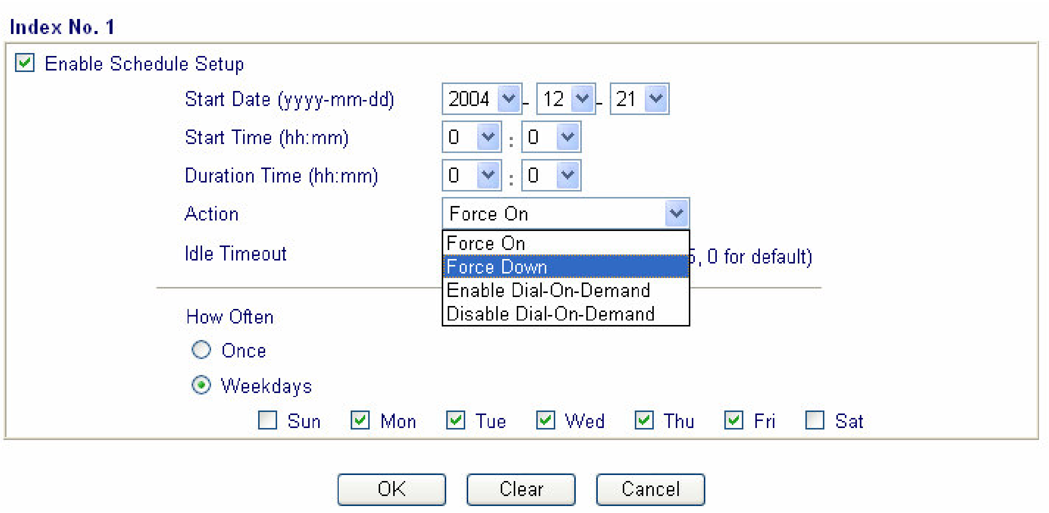
Index	Status	Index	Status
1.	x	9.	x

Click **Clear All** button to remove all schedules in the router.

Click **Cancel** button to give up the current editing-operation and then return back to the Main Setup menu.

Add a Call Schedule

1. Click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown as follows.



Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd) 2004 - 12 - 21

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

Idle Timeout 5, 0 for default)

How Often

○ Once

● Weekdays

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

2. The detailed descriptions for each setting are:

Enable Schedule Setup: Check to enable the schedule.

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

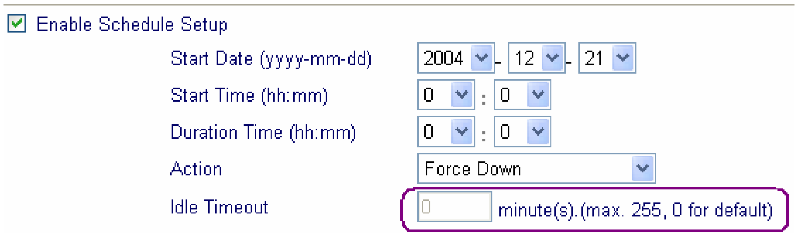
Start Time (hh:mm): Specify the starting time of the schedule.

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

Action:

Specify which action should be applied by Call Schedule during the time 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 as following **Idle Timeout** field.  ☑ Enable Schedule Setup Start Date (yyyy-mm-dd) 2004 - 12 - 21 Start Time (hh:mm) 0 : 0 Duration Time (hh:mm) 0 : 0 Action Force Down Idle Timeout 0 minute(s).(max. 255, 0 for default)
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.

<u>Idle Timeout</u>: 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.

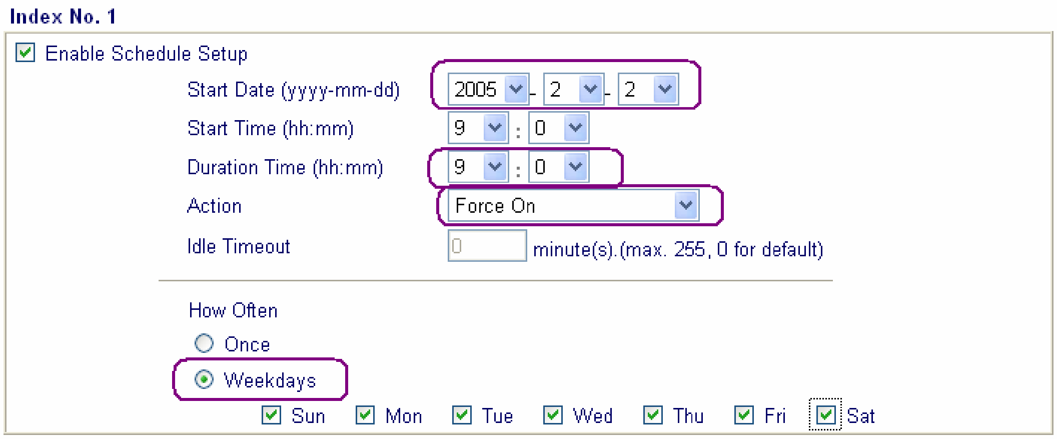
3. Specify appropriate time duration and action to the profile and then click **OK** button to apply.
4. Specify the call schedule to specific Internet access profile or LAN-to-LAN profile.

An Example

If 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).

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.



Index No. 1

☑ Enable Schedule Setup

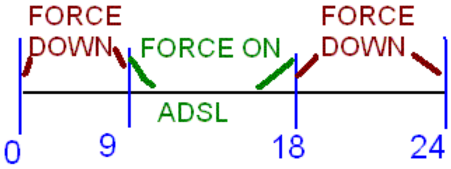
Start Date (yyyy-mm-dd)	2005 - 2 - 2
Start Time (hh:mm)	9 : 0
Duration Time (hh:mm)	9 : 0
Action	Force On
Idle Timeout	0 minute(s).(max. 255, 0 for default)

How Often

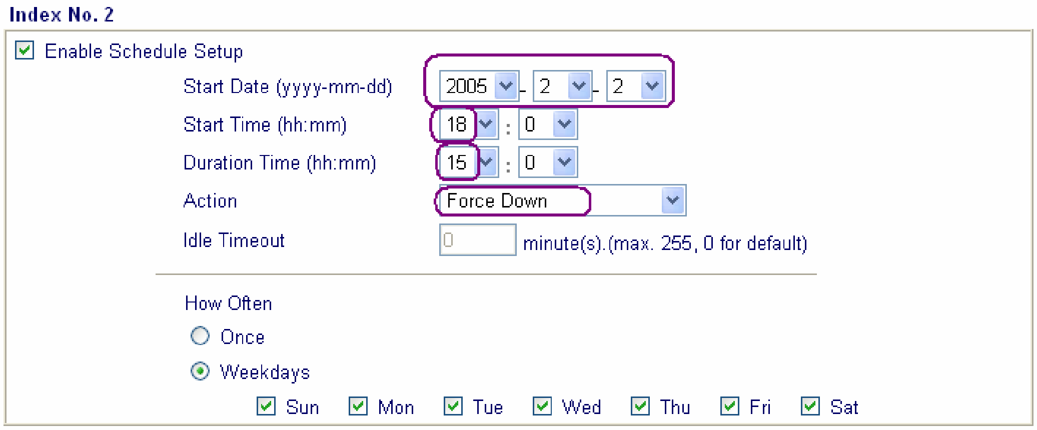
○ Once

● Weekdays

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



3. Configure the Force Down from 18:00 to next day 9:00 for whole week.



Index No. 2

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd)	2005 - 2 - 2
Start Time (hh:mm)	18 : 0
Duration Time (hh:mm)	15 : 0
Action	Force Down
Idle Timeout	0 minute(s).(max. 255, 0 for default)

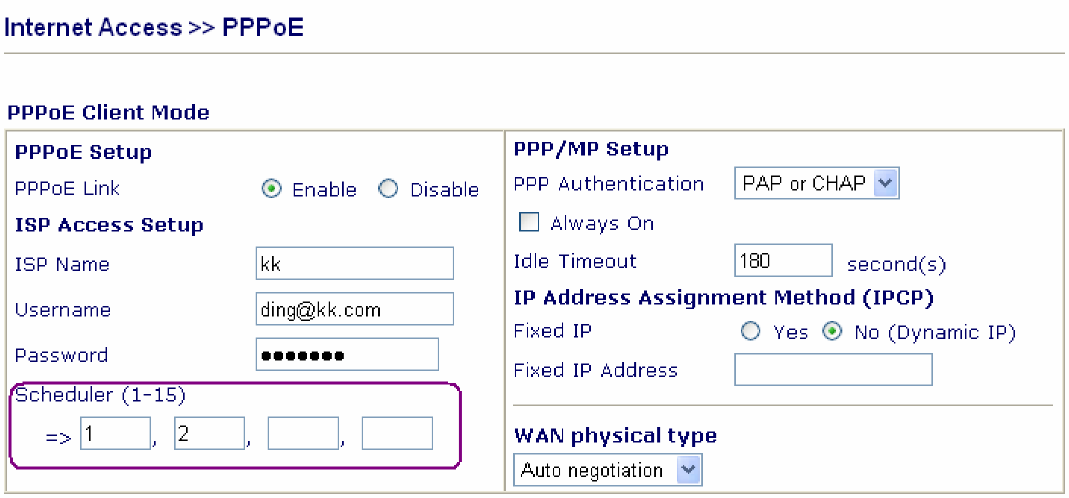
How Often

○ Once

● Weekdays

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

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 which has been pre-defined in the schedule profiles.



Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup

PPPoE Link ● Enable ○ Disable

ISP Access Setup

ISP Name: kk

Username: ding@kk.com

Password: ●●●●●●●

Scheduler (1-15)

=> 1 , 2 , ,

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)

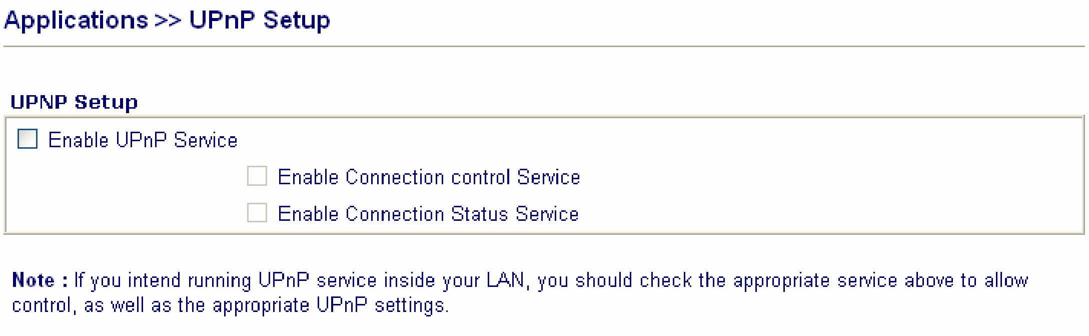
Fixed IP Address:

WAN physical type

Auto negotiation

7.2.3 UPnP

You can enter the **UPNP Setup** as below as below picture shown.



Applications >> UPnP Setup

UPNP Setup

□ Enable UPnP Service

□ Enable Connection control Service

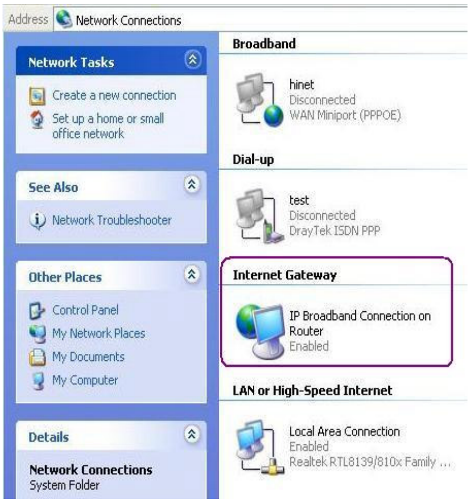
□ Enable Connection Status Service

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**.

Click the **IP Broadband Connection on DrayTek Router** on Windows XP/Network Connections, as shown below. 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

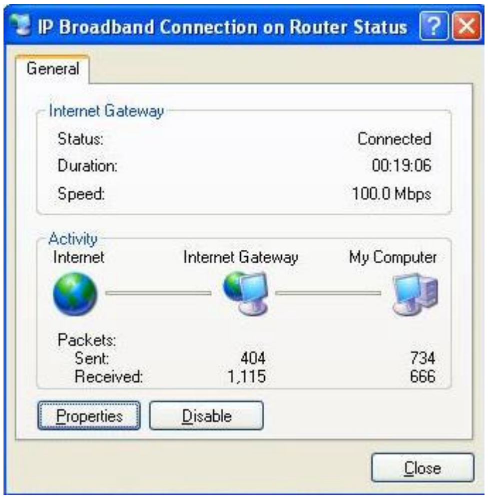
Network Connections
System Folder

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

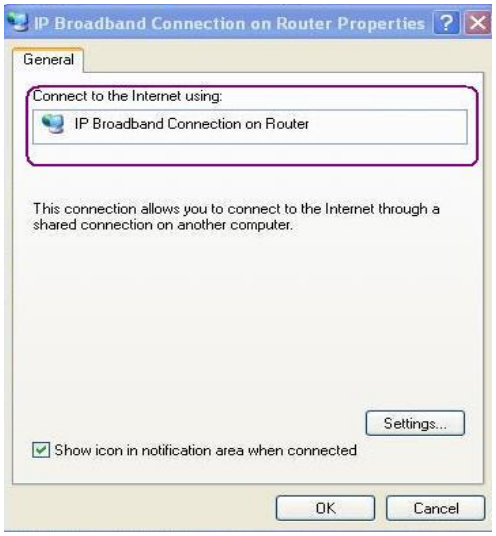
Internet Gateway

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

Activity

	Internet 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, learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.



IP Broadband Connection on Router Properties

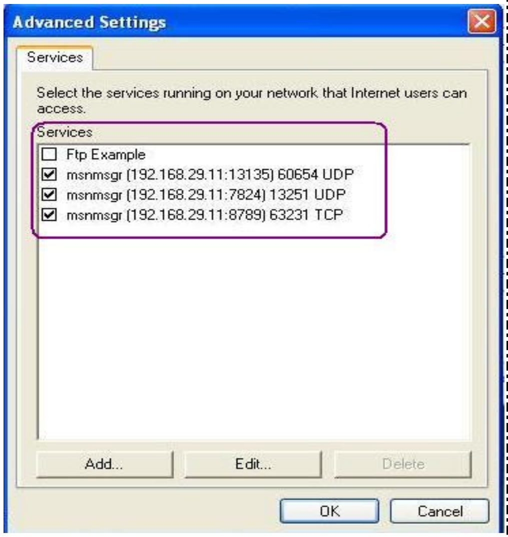
General

Connect to the Internet using:

IP Broadband Connection on Router

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

☑ Show icon in notification area when connected



Advanced Settings

Services

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

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

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

1. 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.
2. Non-privileged users can control some router functions, including removing and adding port mappings.
3. 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.

Chapter 8
VPN and Remote Access Setup

8.1 Introduction

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

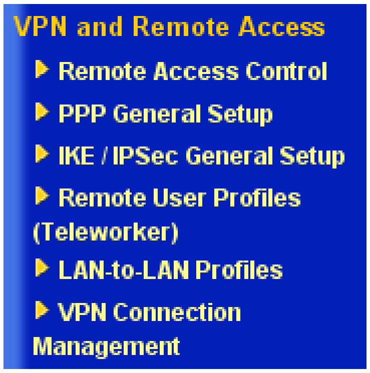
There are two types of VPN connections: the remote dial-in access VPN connection and the LAN-to-LAN VPN connection. The “Remote Dial-In Access” facility allows a remote access node, a NAT router or a single user computer, to dial into a VPN router through the Internet to access the network resources of the remote network. The “LAN-to-LAN Access” facility provides a solution to connect two independent LANs for mutual sharing of network resources. For example, the head office network can access the branch office network, and vice versa.

The VPN technology employed in the Vigor routers supports Internet-industry standard to provide customers with interoperable VPN solutions, such as Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP).

This chapter explains the capabilities of the VPN facility and the remote access on the router. Use the following setup links on the Setup Main Menu to configure the VPN and remote access functions.

8.2 Settings

Click **VPN and Remote Access Setup** to open the setup page.


VPN and Remote Access
Remote Access Control
PPP General Setup
IKE / IPSec General Setup
Remote User Profiles (Teleworker)
LAN-to-LAN Profiles
VPN Connection Management

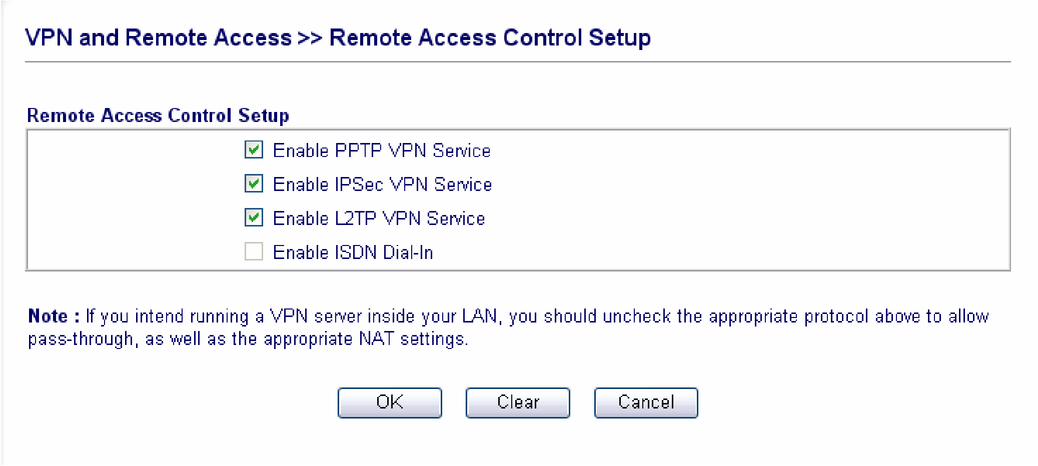
Remote Access Control	Allows you to enable each type of VPN service or disable it for VPN pass-through purpose. For example, you can enable IPSec and L2TP VPN service on your router and disable PPTP VPN service if you intend running a PPTP server inside your LAN. Further, you also can enable or disable the ISDN remote access including remote dial-in and LAN-to-LAN access.
PPP General Setup	To configure your router's PPP authentication method as well as IP assignment range for remote dial-in user. This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec, and ISDN-based remote access.
IKE/IPSec General Setup	To configure a common Pre-shared key and security method for remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address.
Remote User Profiles (Teleworkers)	To create dial-in user accounts. Vigor router supports three types of dial-in methods, PPTP, L2TP, and L2TP over IPSec and ISDN. The PPTP VPN connection is compatible with all Windows platforms which have

	built-in PPTP protocol. The L2TP and L2TP over IPSec are compatible with Window 2000 and XP.
LAN to LAN Profiles	To create profiles for LAN to LAN VPNs. The Vigor router supports four types of LAN-to-LAN VPN, IPSec Tunnel, PPTP, L2TP, and L2TP over IPSec and ISDN. You can establish simultaneously up to 32 VPN tunnels including remote dial-in users.

8.2.1 Remote Access Control

Assume you have a registered domain name from the DDNS provider,

As depicted in the following picture, click the appropriate checkbox to enable the VPN service type that you want to provide. If you intend to run a VPN server inside your LAN, you should disable the appropriate protocol to allow pass-through, as well as the appropriate NAT settings. For example, DMZ or open port. You also can allow the ISDN dial-in by checking **Enable ISDN Dial-In.**



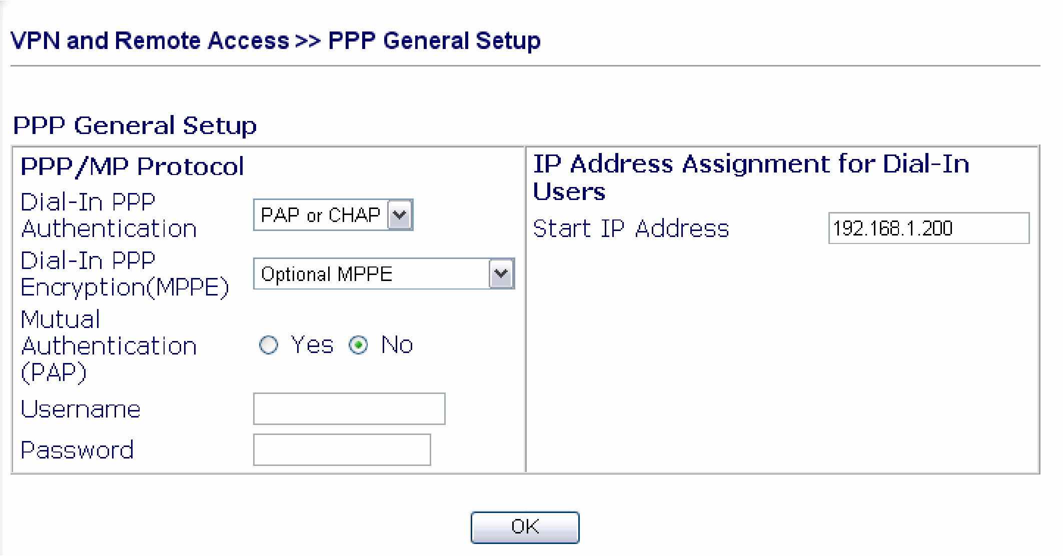
VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

☑ Enable PPTP VPN Service
☑ Enable IPSec VPN Service
☑ Enable L2TP VPN Service
☐ Enable ISDN Dial-In

Note : If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

8.2.2 PPP General Setup



VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Dial-In PPP Encryption(MPPE): Optional MPPE

Mutual Authentication (PAP): ○ Yes ● No

Username:

Password:

IP Address Assignment for Dial-In Users

Start IP Address: 192.168.1.200

Dial-In PPP Authentication:

PAP Only	Select this option to force the router to authenticate dial-in users with the PAP protocol.
PAP or CHAP	Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

Dial-In PPP Encryption:

Optional MPPE	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit “no MPPE encrypted packets”.
Require MPPE(40/120bits)	Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 40-bit MPPE encryption method is not available, then 128-bit encryption scheme will be applied to encrypt the data.

Maximum MPPE	This option indicates that the router will use the MPPE encryption scheme with maximum bits (128 bits) to encrypt the data.

Mutual Authentication (PAP):

The Mutual Authentication function is mainly used to communicate with other routers or clients which need bidirectional authentication in order to provide stronger security. For example, Cisco routers. That is, enable it only if the connecting router requires mutual authentication. By default, the option is set to No. Notice that if you enable the Mutual Authentication function, you should further specify the Username and Password for communication purpose.

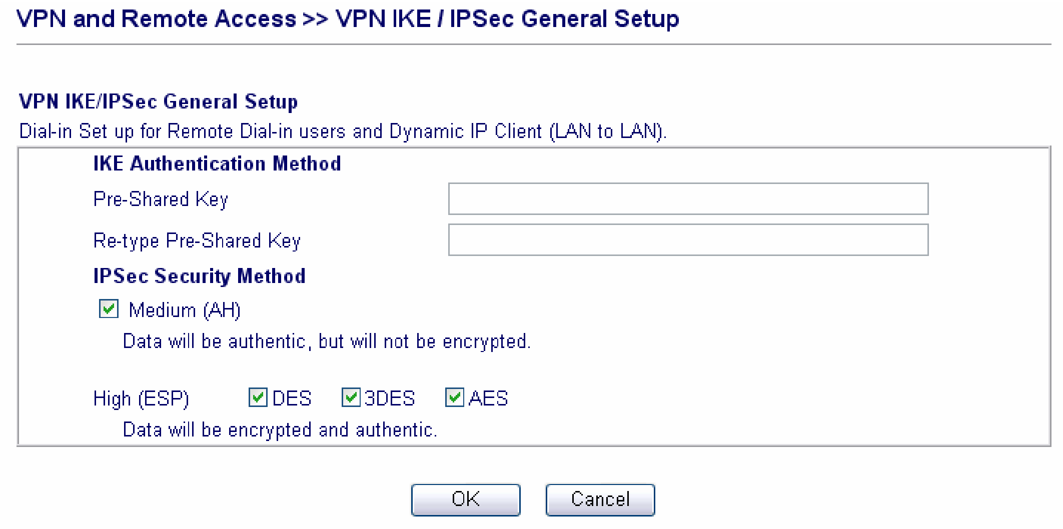
Username	Specify the username for the purpose of the Mutual Authentication.
Password	Specify the password for the purpose of the Mutual Authentication.

IP Address Assignment for Dial-In Users:

Start IP Address	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 to be the Start IP Address.

8.2.3 IKE/IPSec General Setup

Set up a common Pre-shared key and security method for remote dial-in user or non-specified node (LAN to LAN) which do not have fixed IP address. This setup only applies to IPSec-related VPN connections. For example, L2TP over IPSec and IPSec tunnel.



VPN and Remote Access >> VPN IKE / IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key	
Re-type Pre-Shared Key	

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

<u>IKE Authentication Method</u> :

Currently Only support Pre-Shared Key authentication.

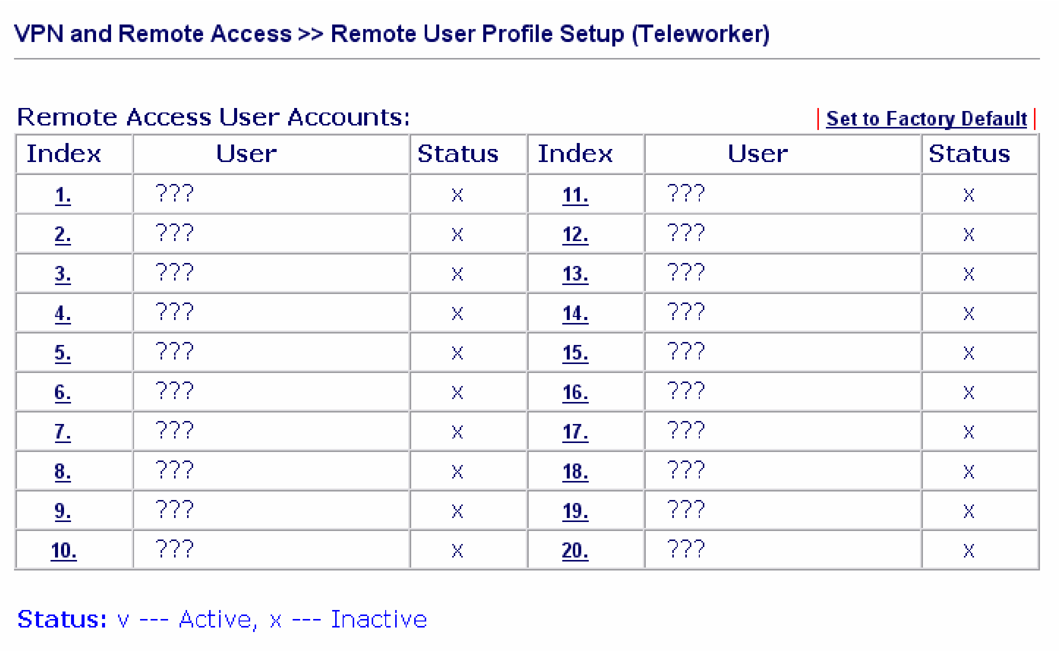
Pre-Shared Key	Specify a key for IKE authentication.
Password	Confirm the pre-shared key.

<u>IPSec Security Method</u> :

Medium(AH)	Data will be authenticated, but not be encrypted. By default, this option is active.
High(ESP)	Data will be encrypted and authenticated. Herein, we support DES, 3DES, and AES encryption methods. By default, these methods are available to support.

8.2.4 Remote User Profiles (Teleworkers)

After completing the general setup, you must create an access account for each remote dial-in user. The router provides 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the Remote User Profile Setup for up to 32 access accounts.



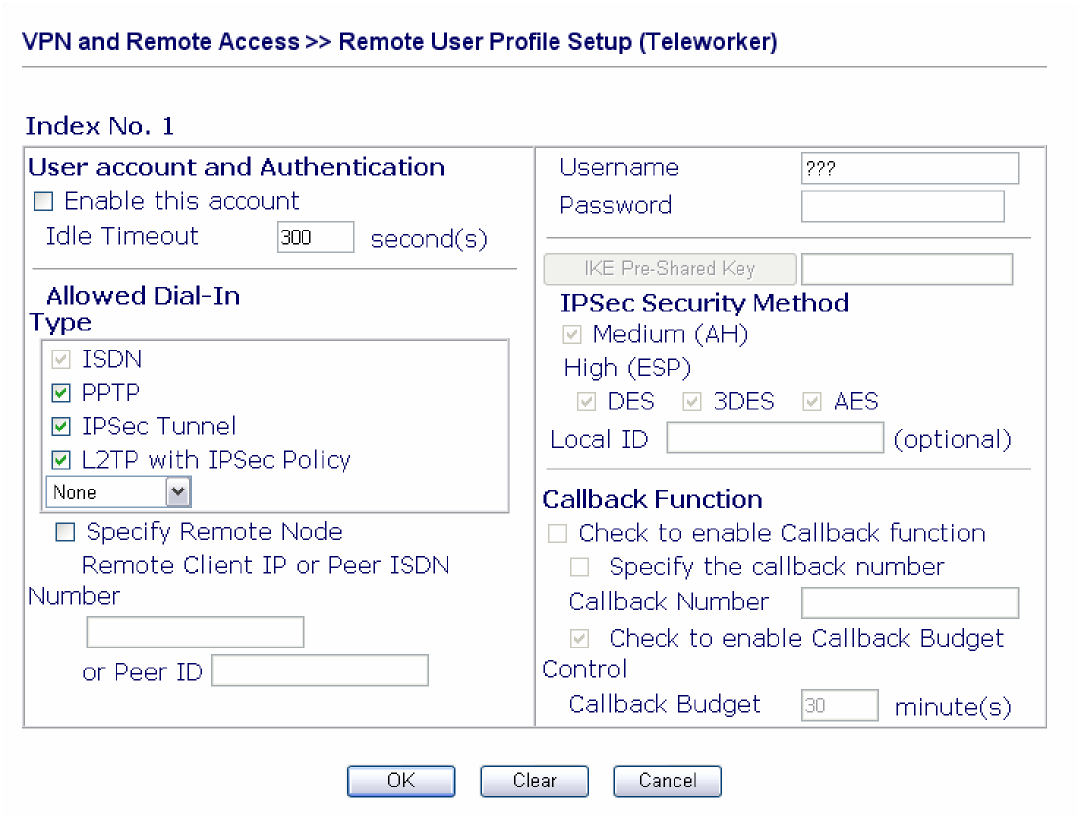
VPN and Remote Access >> Remote User Profile Setup (Teleworker)

Remote Access User Accounts: | Set to Factory Default |

Index	User	Status	Index	User	Status
1.	???	x	11.	???	x
2.	???	x	12.	???	x
3.	???	x	13.	???	x
4.	???	x	14.	???	x
5.	???	x	15.	???	x
6.	???	x	16.	???	x
7.	???	x	17.	???	x
8.	???	x	18.	???	x
9.	???	x	19.	???	x
10.	???	x	20.	???	x

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

Set to Factory Default	Click here to clear all dial-in user accounts.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.
Index	Click the index number to open an individual setup page for a dial-in user account, as shown below.



VPN and Remote Access >> Remote User Profile Setup (Teleworker)

Index No. 1

User account and Authentication

□ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☑ ISDN

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy

None

□ Specify Remote Node

Remote Client IP or Peer ISDN Number

or Peer ID

Username ???

Password

IKE Pre-Shared Key

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Local ID (optional)

Callback Function

□ Check to enable Callback function

□ Specify the callback number

Callback Number

☑ Check to enable Callback Budget Control

Callback Budget 30 minute(s)

User Account and Authentication :

Enable this account	Check this item to activate the individual dial-in user account.
Idle Timeout	If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.

Allow Dial-In Type :

Select the allowed dial-in type. Herein, the Vigor routers provides three types: PPTP, IPSec Tunnel, and L2TP with IPSec Policy. For the L2TP with IPSec Policy, you have other three choices (None, Nice to Have, and Must) to set up the dial-in VPN type.

PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet.
IPSec Tunnel	Allow the remote dial-in user to trigger a IPSec VPN connection through Internet.
L2TP	Allow the remote dial-in user to make a L2TP VPN connection through the Internet. Specify the IPSec policy to be “None”, “Nice to Have”, or “Must”. **None**: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec Policy can be viewed as one pure L2TP connection. **Nice to Have**: Apply the IPSec policy first, if it is available. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. **Must**: Specify the IPSec policy to be definitely applied on the L2TP connection.

PPTP or **L2TP with IPSec Policy (None)**	Only Specify the Username and Password.
PPTP or **L2TP with IPSec Policy (Must or Nice to Have)**	Specify the Username and Password. Also set *IKE Pre-Shared Key, IPSec Security Method, Remote Client IP or Peer ID, and optional Local ID*.

<u>Specify Remote Node</u> :

For extra security, you should enable the option to allow the remote client to connect only from a specific IP address.

Remote Client IP or Peer ID	Specify the IP address of the remote client or the peer ID in the field. Afterward, you should fill a Pre-Shared Key for this

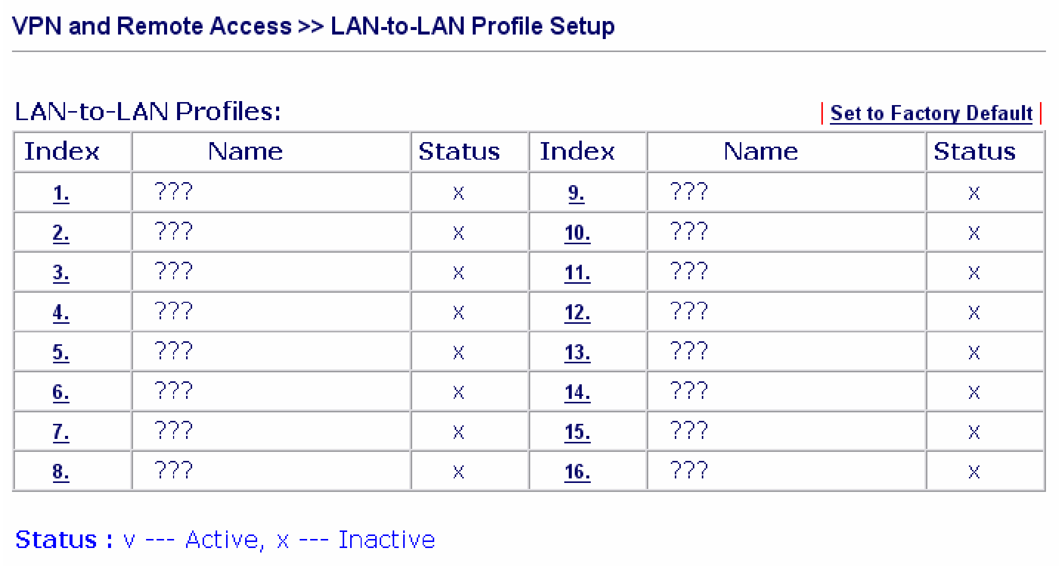
	specific node.
IKE Pre-Shared Key	Click it and a window will be automatically poped up for you, as depicted below. Please fill a Pre-shared Key and confirm it for this specific node.
IPSec Security Method	Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one. **Medium(AH):** Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted. **High(ESP):** Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are DES, 3DES, and AES. By default, these three algorithms are available.
Local ID	Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional.

if you do not activate the “**Specify Remote Node**” and leave the field of “**Remote Client IP or Peer ID**” to be empty, the settings of **IKE Pre-Shared Key, IPSec Security Method, Remote Client IP or Peer ID**, and optional **Local ID** will be disabled and, therefore, no IPSec-related VPN connection can be triggered successfully.

Callback Function won’t be enabled for this version.

8.2.5 LAN to LAN Profiles

In this section, we will explain how to set up the **LAN-to-LAN Profile** in more detail. You can create up to 32 LAN-to-LAN profiles.



VPN and Remote Access >> LAN-to-LAN Profile Setup

LAN-to-LAN Profiles:

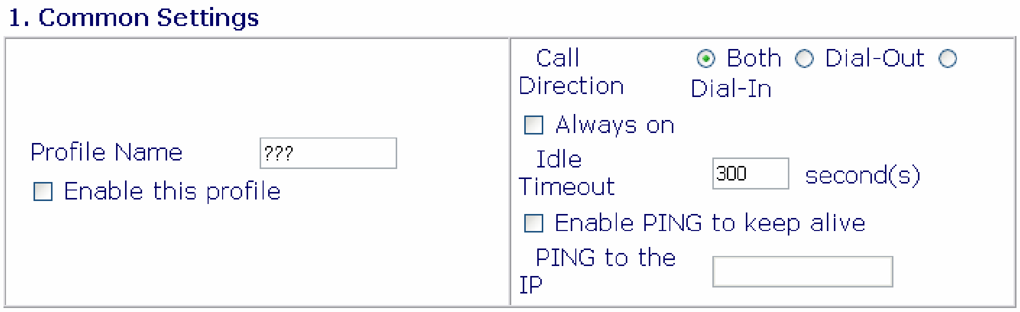
Index	Name	Status	Index	Name	Status
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

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

Set to Factory Default	Click here to clear all the LAN-t-LAN profiles.
Index	Click a number to open a detailed setting page for each profile.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Each LAN-to-LAN profile includes 4 subgroups: **Common Settings, Dial-Out Settings, Dial-In Settings, and TCP/IP Network Settings.** In the following, we explain each subgroup in detail.

Common Settings



1. Common Settings

Profile Name ???

□ Enable this profile

Call Direction ● Both ○ Dial-Out ○ Dial-In

□ Always on

Idle Timeout 300 second(s)

□ Enable PING to keep alive

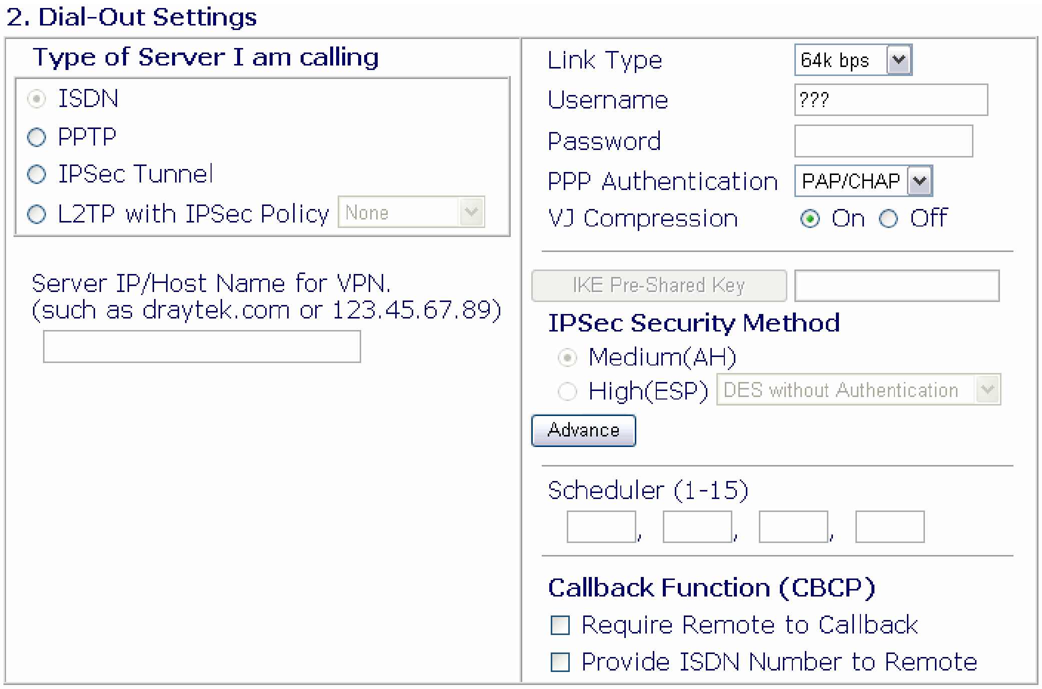
PING to the IP

Profile Name	Specify a name for the remote network.
Enable this profile	Check here to activate this profile
Call Direction	Specify the call direction for this profile. Both means it can be used for outgoing and incoming access. Dial-Out means it can only be used for outgoing access. Dial-In allows only incoming access.
Always on	Click it to always activate this profile. The field of Idle Timeout will be grayed to disallow any input.
Idle Timeout	By default, set as 300 seconds. If the profiles connection is idle over the limitation of the timer, the router will drop the connection.
Enable PING to keep alive	Click this item to enable the transmission of PING packets to an IP address defined in the field of “PING to the IP”
PING to the IP	Specify the IP address of the remote host that located at the other-end of the VPN tunnel.

In the normal condition, when the remote host wants to disconnect its VPN connection to Vigor Router, it should send several specific type of packets to inform the Router. Accordingly, the Vigor Router will drop the designated VPN connection and clear its parameters(e.g. key for encryption).

However, once if the remote host abnormally disconnects a VPN connection, the Router won't be aware of it and assume the connection is still alive. To resolve this dilemma, enable **PING to keep alive** let the Router probe the status of the VPN connection by continuously sending PING packets to the remote host.

Dial-Out Settings



2. Dial-Out Settings

Type of Server I am calling

- ● ISDN
- ○ PPTP
- ○ IPSec Tunnel
- ○ L2TP with IPSec Policy: None

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

Link Type	64k bps
Username	???
Password	
PPP Authentication	PAP/CHAP
VJ Compression	● On ○ Off

IKE Pre-Shared Key

IPSec Security Method
- ● Medium(AH)
- ○ High(ESP): DES without Authentication

Advance

Scheduler (1-15)

Callback Function (CBCP)
- □ Require Remote to Callback
- □ Provide ISDN Number to Remote

Choose one out of three main options, PPTP, IPSec Tunnel, and L2TP with IPSec Policy (sub-options: None, Nice to Have, and Must).

Be sure to fill in the Server IP/Host Name for VPN as the destination address.

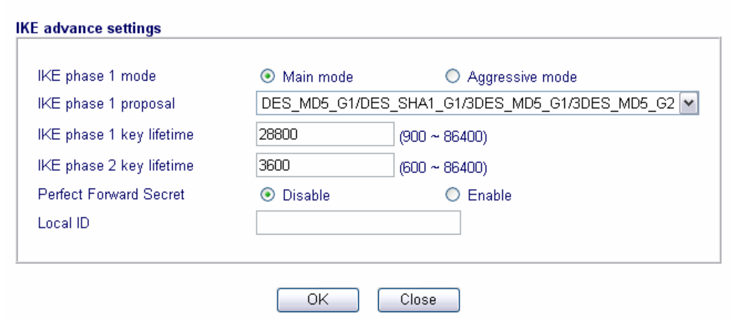
Please see the settings instruction for each options.

PPTP or **L2TP with IPSec Policy (None)** Specify Server IP/Host Name for VPN. Specify Username, Password, PPP Authentication, and VJ Compression.

IPSec Tunnel or **L2TP with IPSec Policy (Must** or **Nice to Have)** Specify Server IP/Host Name for VPN. Specify Username, Password, PPP Authentication, and VJ Compression. Also specify *IKE Pre-Shared Key, IPSec Security Method (Advance), and Scheduler*

PPTP	Specify the dial-out VPN connection to be the PPTP connection
IPSec Tunnel	Specify the dial-out VPN connection to be the IPSec Tunnel connection.
L2TP	Specify the IPSec policy for the L2TP connection. **None**: Do not apply IPSec. Accordingly, the VPN connection employed the L2TP without IPSec Policy can be viewed as one pure L2TP connection. **Nice to Have**: Apply the IPSec policy first, if it is available. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection.
Server IP/Host Name for VPN	Specify the IP address of the **destination VPN server** or the Host Name for dialup.
Username	Specify a username for authentication by the remote router.
Password	Specify a password for authentication by the remote router.

PPP Authentication	Specify the PPP authentication method for PPTP, and L2TP over IPSec. Normally set to PAP/CHAP for the widest compatibility.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.
IKE Pre-Shared Key	Click it and a window will be automatically pop out for you. Please fill a Pre-shared Key and confirm it for this specific node.
IPSec Security Method	Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one. **Medium(AH)**: Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted. **High (ESP)**: Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are listed below. **DES without Authentication**: Use DES encryption algorithm and not apply any authentication scheme. **DES with Authentication**: Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. **3DES without Authentication**: Use triple DES encryption algorithm and not apply any authentication scheme. **3DES with Authentication**: Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
Advanced Setting	To decide which mode to be used for Phase 1 IKE negotiation process, specify the authentication and encryption algorithms, fill the lifetime for the IKE phase 1 and phase 2, enable or disable the “Perfect Forward Secret”, and provide the Local ID for remote VPN gateway.



IKE advance settings

IKE phase 1 mode ● Main mode ○ Aggressive mode

IKE phase 1 proposal DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2

IKE phase 1 key lifetime 28800 (900 ~ 86400)

IKE phase 2 key lifetime 3600 (600 ~ 86400)

Perfect Forward Secret ● Disable ○ Enable

Local ID

IKE phase 1 mode: Main mode and Aggressive mode. Most VPN servers support Main mode and Aggressive mode is a more recent implementation to speed up the negotiation process, but may incur less security. The default is Main mode for consideration of greatest compatibility.

IKE phase 1 proposal: Then the router will query the remote VPN server if it supports the designated algorithm. There are two options of query for Aggressive mode and nine options for Main mode. We suggest to select the latest one, "DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2", for Main mode.

IKE phase 1 key lifetime: For the greater security, the router should limit the key lifetime. The default key lifetime is 28800 seconds. We suggest you specify a value in between 900 and 86400 seconds.

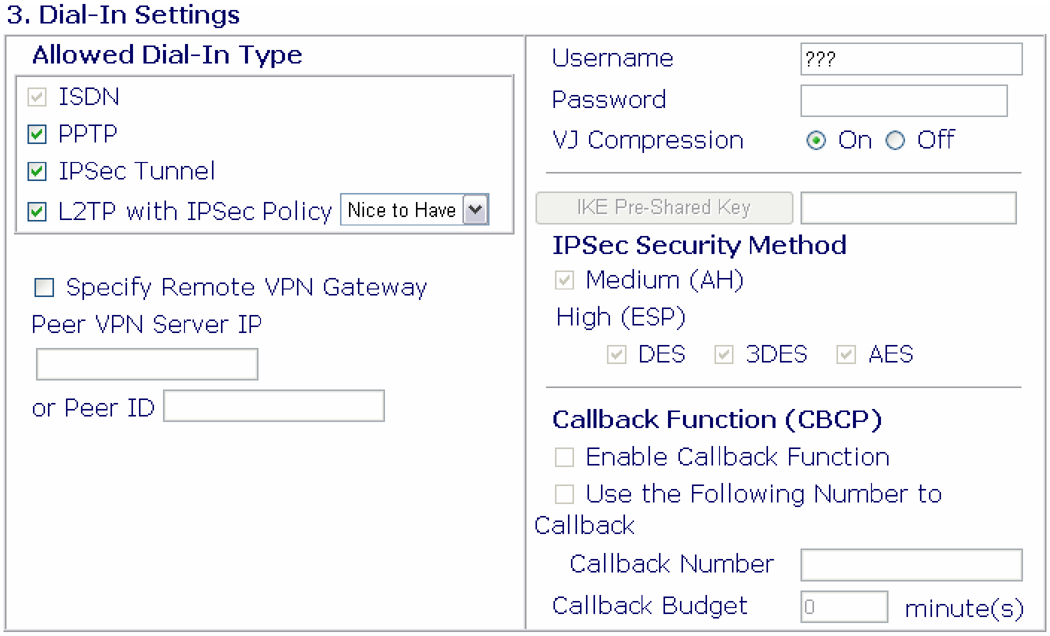
IKE phase 2 key lifetime: For the greater security, the router should limit the key lifetime. The default key lifetime is 3600 seconds. We suggest you specify a value in between 600 and 86400 seconds.

Perfect Forward Secret: If this function enabled, the function the Phase 1 key will be reused to reduce the computation complexity in phase 2. Otherwise, a new key will be generated for phase 2 key. The default of this option is inactive.

Local ID: This function is used in Aggressive mode. It is on behalf of the IP address to perform identity

	authentication with remote VPN server.
Scheduler	Specify the index of the call schedule

Dial-In Settings



3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN
☑ PPTP
☑ IPSec Tunnel
☑ L2TP with IPSec Policy [Nice to Have]

□ Specify Remote VPN Gateway

Peer VPN Server IP [ ]

or Peer ID [ ]

Username [???]

Password [ ]

VJ Compression ● On ○ Off

IKE Pre-Shared Key [ ]

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)

□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number [ ]

Callback Budget [0] minute(s)

This indicate what types the Router accepts. There are three main options, PPTP, IPSec Tunnel, and L2TP with IPSec Policy (sub-options: None, Nice to Have, and Must). By default, all three options are active. If you only choose some of three, please see the below settings instruction.

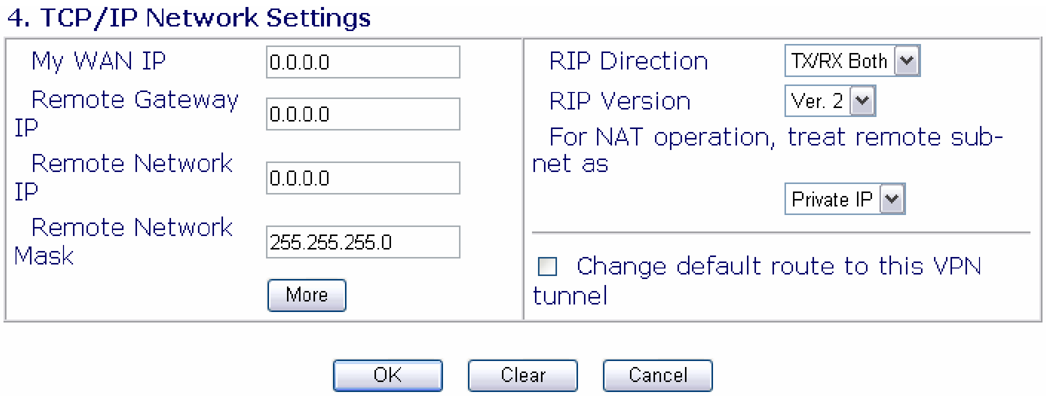
PPTP	Check to allow the PPTP dial-in connection
IPSec Tunnel	Click it to allow the IPSec tunnel dial-in connection.
L2TP	Specify the IPSec policy for the L2TP connection. **None:** Do not apply the IPSec policy.

	Nice to Have: Apply the IPSec policy first. If it fails, the dial-in VPN connection will be the L2TP connection without employing the IPSec policy. **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify Remote VPN Gateway	For extra security, you should enable the option to allow the remote client to connect only from a specific IP address.
Peer VPN Server IP or Peer ID	Specify the IP address of the remote VPN server or the peer ID in the field. Afterward, you should fill a Pre-Shared Key for this specific node.
Username	Specify a username for authentication by the remote router.
Password	Specify a password to authenticate the dial-in router.
PPP Authentication	Specify the PPP authentication method for PPTP, L2TP, and L2TP over IPSec. Normally set to PAP/CHAP for the widest compatibility.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.
IKE Pre-Shared Key	Click it and a window will be automatically popped up for you, as depicted below. Please fill a Pre-shared Key for this specific node.
IPSec Security Method	Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one. **Medium(AH)**: Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted. **High (ESP)**: Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are DES, 3DES, and AES. By default, these three algorithms are available.

if you do not activate the "**Specify Remote Node**" and leave the field of "**Peer VPN Server IP or Peer ID**" to be empty, the settings of **IKE Pre-Shared Key, and IPSec Security Method**, will be disabled and, therefore, no IPSec-related VPN connection can be triggered successfully.

Callback Function won't be enabled for this version.

TCP/IP Network Settings


4. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	TX/RX Both
Remote Gateway IP	0.0.0.0	RIP Version	Ver. 2
Remote Network IP	0.0.0.0	For NAT operation, treat remote sub-net as	Private IP
Remote Network Mask	255.255.255.0	□ Change default route to this VPN tunnel	

My WAN IP	In most cases, you may accept the default value of 0.0.0.0 in this field. The router will then get a WAN IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
Remote Gateway IP	In most cases, you may accept the default value of 0.0.0.0 in this field. The router will then get a Remote Gateway IP address from the remote router during the IPCP negotiation phase. If the Remote Gateway IP address is fixed, specify the fixed IP address here.
Remote Network IP	Specify the network identification of the remote network. For example, 192.168.1.0 is a network identification of a class-C subnet with subnet mask of 255.255.255.0 (/24).

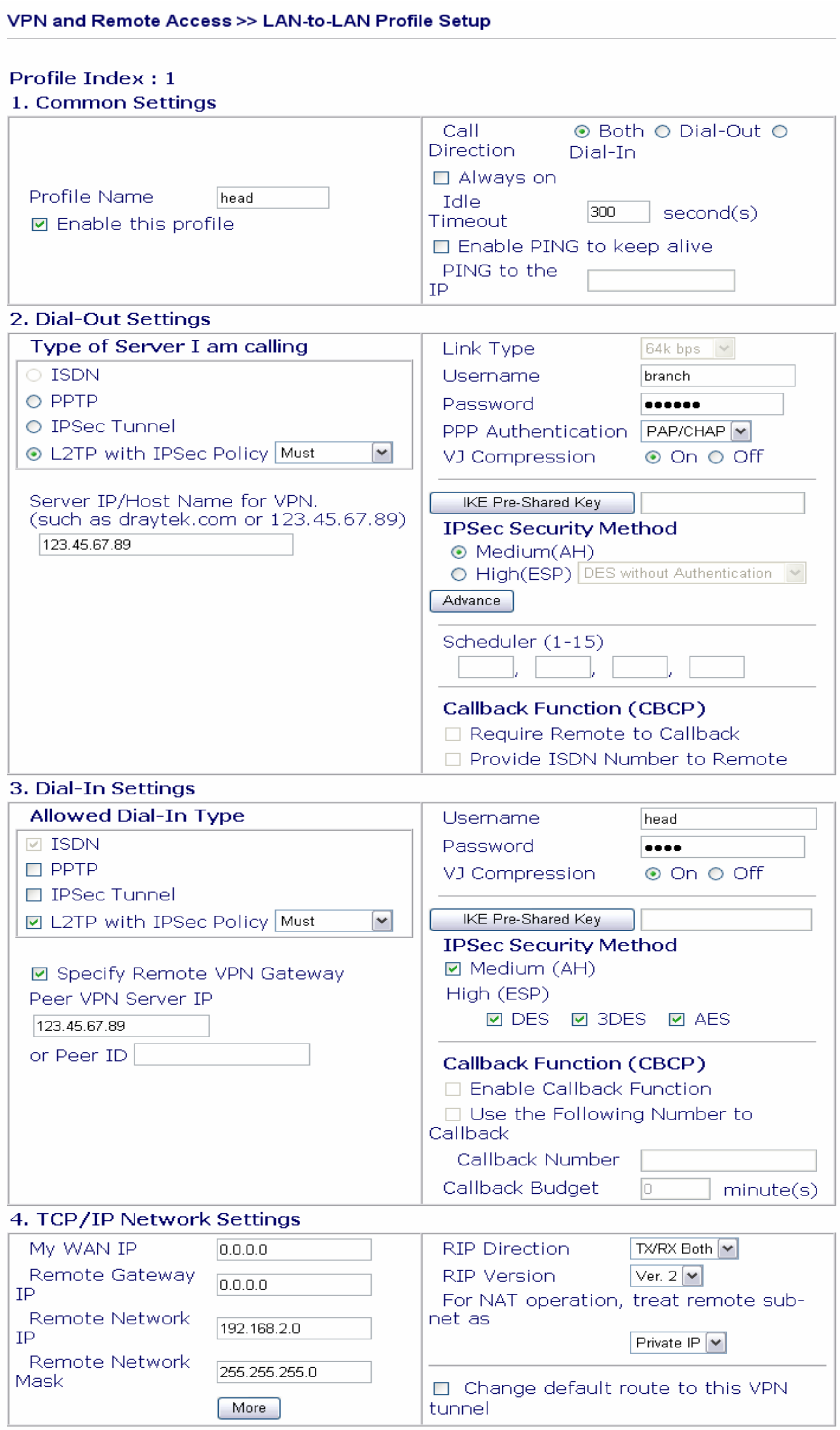
Remote Network Mask	Specify the subnet mask of the remote network.
More	To add a static route when this connection is up, if needed.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
For NAT operation, treat remote sub-net as	The Vigor router supports two local IP networks: the 1st subnet and 2nd subnet. Thus, you can set which subnet will be used as the local network for VPN connection and exchange RIP packets with the remote network. Usually set to Private IP for routing between the 1st subnet and the remote network.

Example of LAN-to-LAN Connection

The example describes how to set up a LAN-to-LAN profile to connect two private networks through Internet. In this example, the private network 192.168.1.0/24 is located at head office. The network of off-site branch office is 192.168.2.0/24.

1. First, you need to configure the pre-shared key in the menu **IKE/IPSec General Setup** of **VPN and Remote Access**, “ABC123”, for example.

2. Create a LAN-to-LAN profile at Head Office.



VPN and Remote Access >> LAN-to-LAN Profile Setup

Profile Index : 1

1. Common Settings

Profile Name: head
☑ Enable this profile

Call Direction: ● Both ○ Dial-Out ○ Dial-In
□ Always on
Idle Timeout: 300 second(s)
□ Enable PING to keep alive
PING to the IP:

2. Dial-Out Settings

Type of Server I am calling
○ ISDN
○ PPTP
○ IPSec Tunnel
● L2TP with IPSec Policy: Must

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

Link Type: 64k bps
Username: branch
Password: ●●●●●●
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Pre-Shared Key:
IPSec Security Method
● Medium(AH)
○ High(ESP): DES without Authentication
Advance

Scheduler (1-15)
, , ,

Callback Function (CBCP)
□ Require Remote to Callback
□ Provide ISDN Number to Remote

3. Dial-In Settings

Allowed Dial-In Type
☑ ISDN
□ PPTP
□ IPSec Tunnel
☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway
Peer VPN Server IP: 123.45.67.89
or Peer ID:

Username: head
Password: ●●●●
VJ Compression: ● On ○ Off

IKE Pre-Shared Key:
IPSec Security Method
☑ Medium (AH)
High (ESP)
☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)
□ Enable Callback Function
□ Use the Following Number to Callback
Callback Number:
Callback Budget: 0 minute(s)

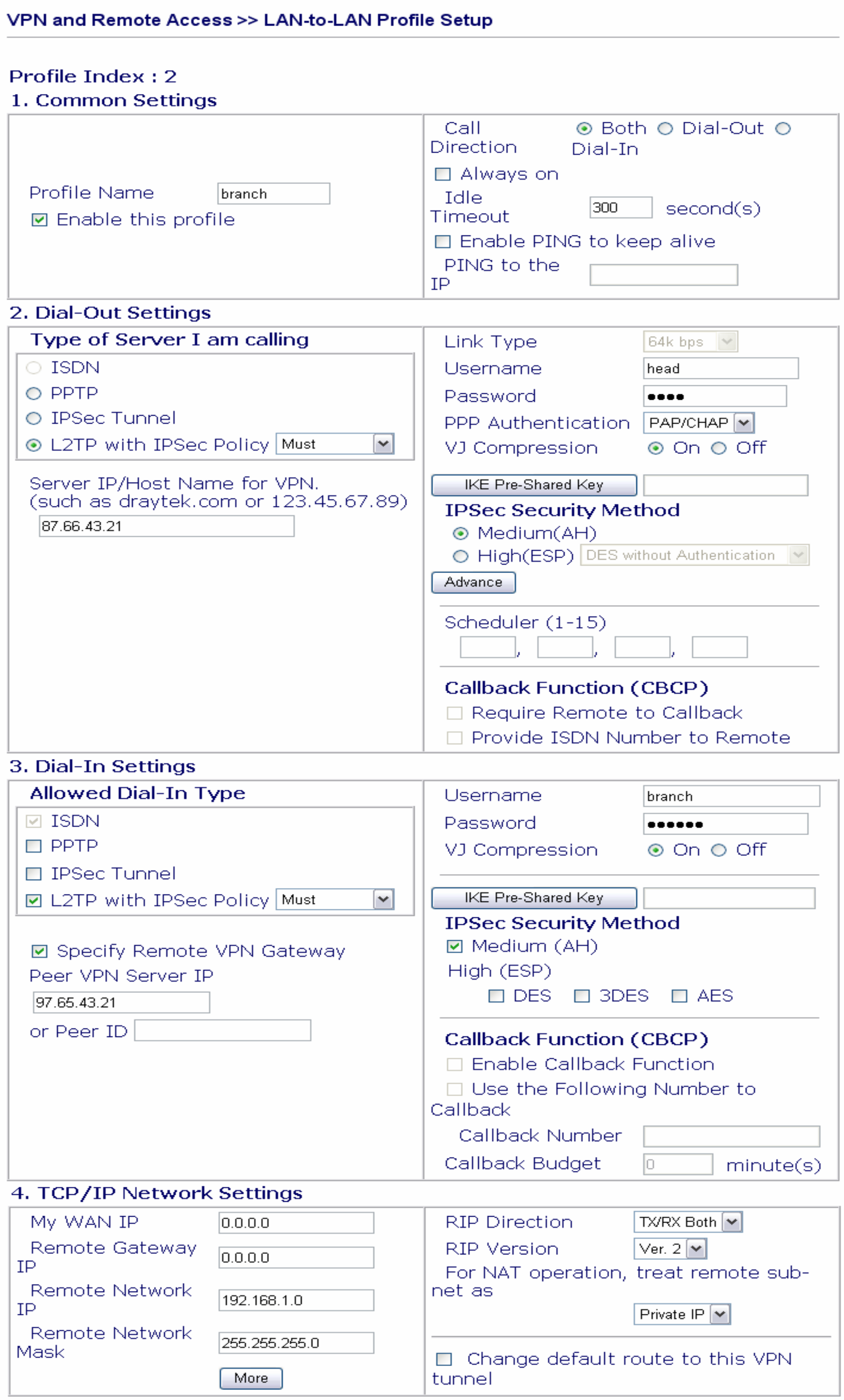
4. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 0.0.0.0
Remote Network IP: 192.168.2.0
Remote Network Mask: 255.255.255.0
More

RIP Direction: TX/RX Both
RIP Version: Ver. 2
For NAT operation, treat remote sub-net as: Private IP

□ Change default route to this VPN tunnel

3. Create a LAN-to-LAN profile at Branch Office.



VPN and Remote Access >> LAN-to-LAN Profile Setup

Profile Index : 2

1. Common Settings

Profile Name: branch

☑ Enable this profile

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

□ Always on

Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

○ IPSec Tunnel

● L2TP with IPSec Policy: Must

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
87.66.43.21

Link Type: 64k bps

Username: head

Password: ●●●●

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key:

IPSec Security Method

● Medium(AH)

○ High(ESP): DES without Authentication

Advance

Scheduler (1-15): , , ,

Callback Function (CBCP)

□ Require Remote to Callback

□ Provide ISDN Number to Remote

3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN

□ PPTP

□ IPSec Tunnel

☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 97.65.43.21

or Peer ID:

Username: branch

Password: ●●●●●●

VJ Compression: ● On ○ Off

IKE Pre-Shared Key:

IPSec Security Method

☑ Medium (AH)

High (ESP)

□ DES □ 3DES □ AES

Callback Function (CBCP)

□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number:

Callback Budget: 0 minute(s)

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.1.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: TX/RX Both

RIP Version: Ver. 2

For NAT operation, treat remote sub-net as: Private IP

□ Change default route to this VPN tunnel

Chapter 9
VoIP Setup

9.1 Introduction

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

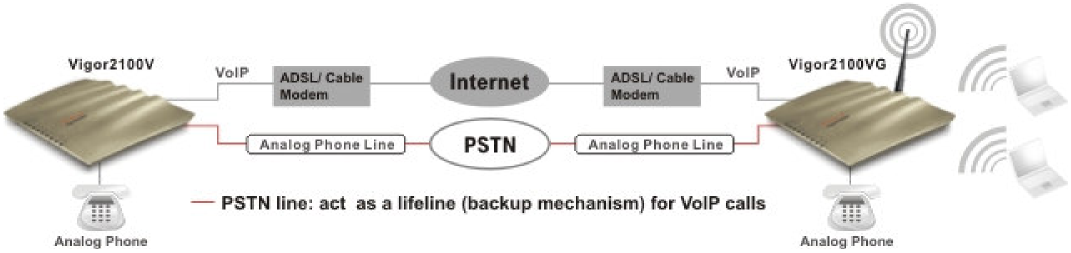
There are many different call signaling protocols; methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and the older H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor2200V/VG series 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 supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks). The MGCP protocol uses a 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 encodec the voice) can be embedded into RTP packets. Vigor2200V/VG series 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.

The VoIP facilities of Vigor2200V/VG series can provide a cost-saving alternative to having an additional fixed-line. By using the ITSP (e.g. **DrayTEL**, **www.draytel.org**) you can also make calls to any regular phone line too, including mobiles, as well as receive calls from anyone - the call is carried to your phone via your internet connection so your regular phone line remains free for other people/calls.

There are two ways for you to make a call to other Vigor VoIP router users; by dialling their IP address directly on the phone handset or using a SIP registrar. A SIP server on the Internet enables your router to log its current location (IP Address) and availability so that other users can call you on your SIP address (e.g. 98141@draytel.org)

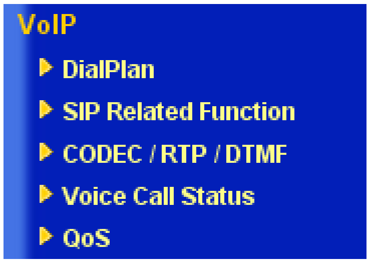


Before you can set up the router for SIP you need to open an account with a SIP registrar [e.g. IPTEL, DrayTEL (www.draytel.org)].

Our Vigor2200V/VG series firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor2200V/VG series 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 which is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.

9.2 Settings

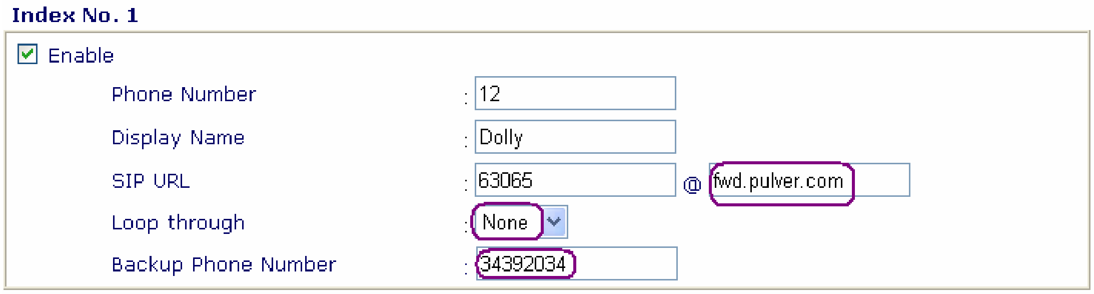
Click **VoIP Setup** to open the setup page.



DialPlan	Pre-settings of up to 60 SIP addresses of VoIP contacts.
SIP Related Function	Settings of SIP port, registrar, proxy, domain and Stun server.
CODEC/RTP/DTMF	Settings of default Codec, DTMF and RTP
Voice Call Status	Call Status including registered registrar, codec, connection and others.
QoS	Enter upstream speed wanted to assure for VoIP call

9.2.1 DialPlan

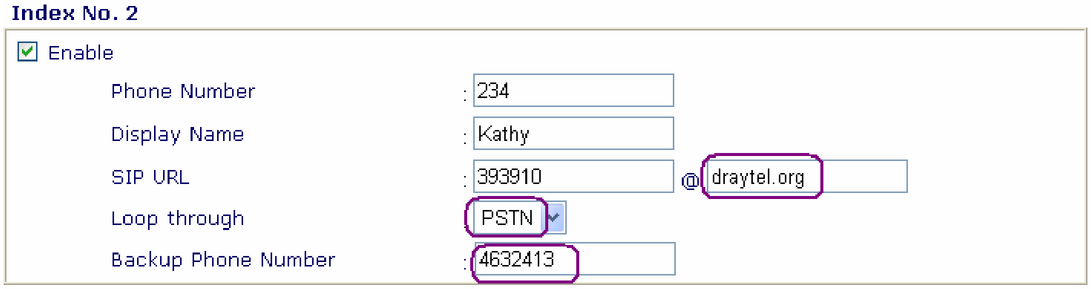
The Vigor2200V/VG series have one FXS port (the “Phone” port on the rear panel) to which you connect a conventional (analogue) phone, either corded or wireless (DECT). You can set the registered SIP address of your VoIP contacts into the DialPlan of the Vigor2200V/VG series to make calling them quick and easy. There are 60 entries in the DialPlan for you to store all your friends and family members SIP address.



Index No. 1

☑ Enable

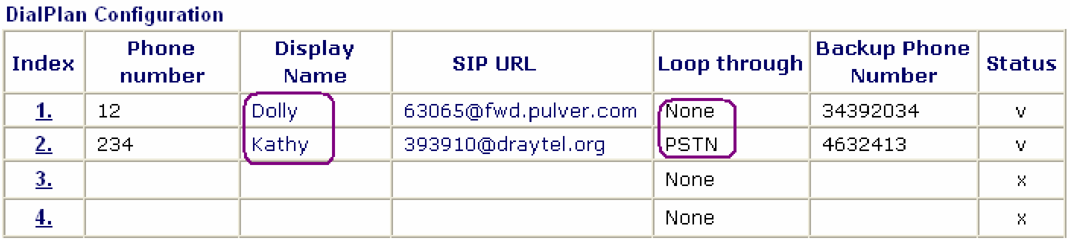
Phone Number	: 12	
Display Name	: Dolly	
SIP URL	: 63065	@ fwd.pulver.com
Loop through	: None	
Backup Phone Number	: 34392034	



Index No. 2

☑ Enable

Phone Number	: 234	
Display Name	: Kathy	
SIP URL	: 393910	@ draytel.org
Loop through	: PSTN	
Backup Phone Number	: 4632413	



DialPlan Configuration

Index	Phone number	Display Name	SIP URL	Loop through	Backup Phone Number	Status
1.	12	Dolly	63065@fwd.pulver.com	None	34392034	v
2.	234	Kathy	393910@draytel.org	PSTN	4632413	v
3.				None		x
4.				None		x

Enable

Tick this to enable this entry

Phone Number

The number you want to dial from your handset to call this contact. This can be any number you choose, using digits 0-9 and*

Display Name

This field contains a name or a number which easily let you identify the person who you wan to call. It can also be the name for SIP display.

SIP URL Address

Enter the SIP address of your contact (e.g. 393910@draytel.org)

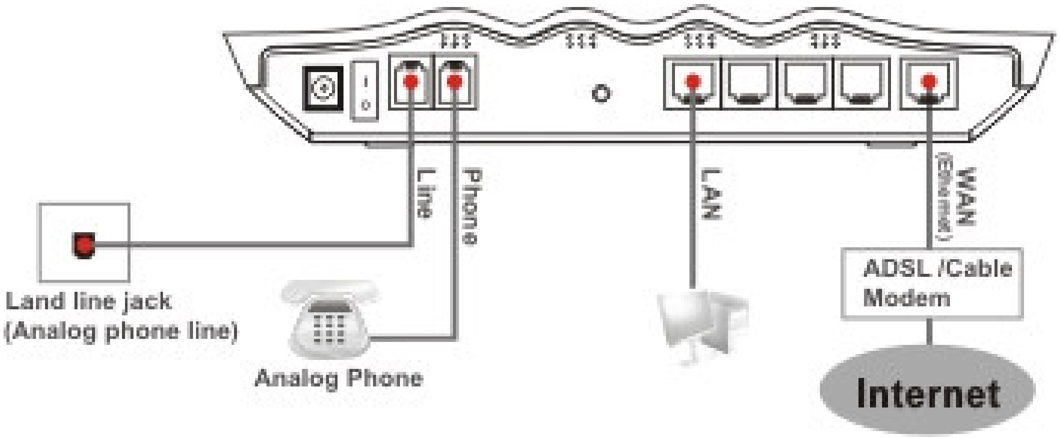
Loop Through

The Vigor2200V/VG series have 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 Vigor2200V/VG series will dial instead of the SIP account if you lose broadband access or power to the Vigor2200V/VG series. Hence, the PSTN line can act as a lifeline (backup mechanism) for VoIP calls. The default is VoIP mode. The lifeline mechanism is activated automatically if you specify "**PSTN**" as Loop Through and enter **Backup Phone Number**.

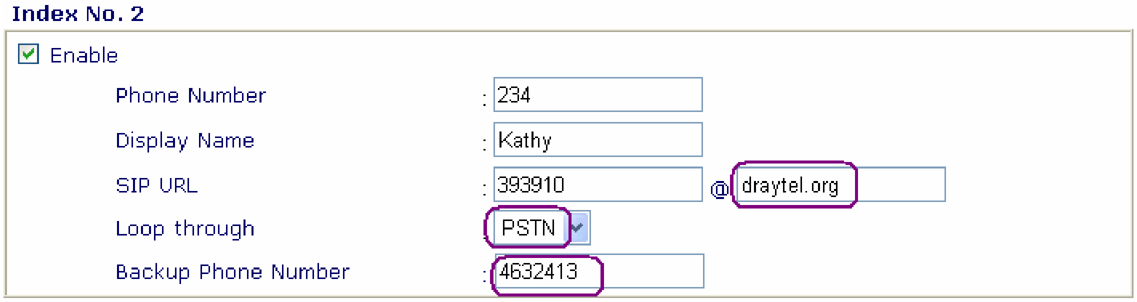
Example 1

If Dolly gives you her SIP URL as **sip:63065@fwd.pulver.com,** then you can enter the number just as the previous figure. You can apply easy-to-search Display Name and Phone Number to settings.

The hardware connection of Vigor2200V series:



<u>Backup Phone Number</u>: The alternate PSTN number to dial if “PSTN” is set in **Loop Through entry**.



Index No. 2

☑ Enable

Phone Number	: 234
Display Name	: Kathy
SIP URL	: 393910 @ draytel.org
Loop through	PSTN
Backup Phone Number	: 4632413

Example 2

If Kelly gives you her SIP URL as **sip:kelly@203.69.175.19 and PSTN number is 5972727** then you can enter the DialPlan as:

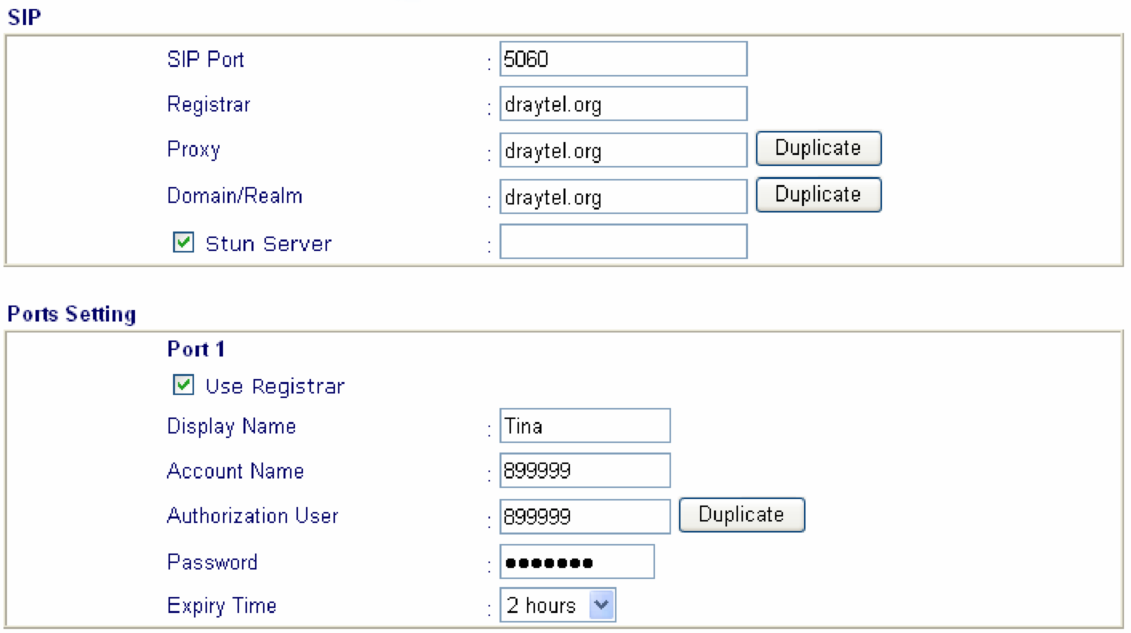
Phone Number:	1234 (any number you like)
Display Name:	Kelly
SIP URL:	Kelly@203.69.175.19
Loop through:	PSTN
Backup phone number:	5972727

Example 3

If Kelly gives you her IP address 203.69.175.19 only, and it is not in your DialPlan, you still can press keypad on the phone to dial as **#203*69*175*19#**

To manually dial the backup number **via PSTN enter "#0"** on your telephone handset, and then dial a PSTN phone number. If you are worried that the automatic loop through might over charge your PSTN phone number, we recommend you not to enter your PSTN phone number into the "Backup Phone Number" entry. That way you can only run loop through by manually dialing a PSTN number.

9.2.2 SIP Related Function



SIP

SIP Port	: 5060	
Registrar	: draytel.org	
Proxy	: draytel.org	Duplicate
Domain/Realm	: draytel.org	Duplicate
☑ Stun Server	:	

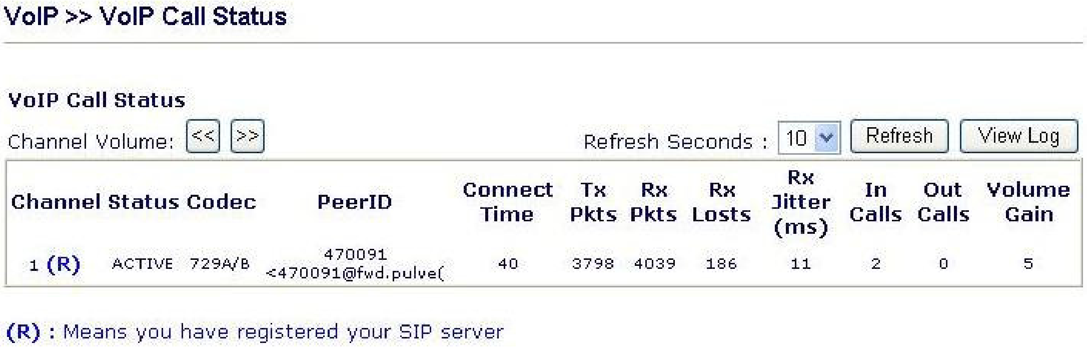
Ports Setting

Port 1

☑ Use Registrar

Display Name	: Tina	
Account Name	: 899999	
Authorization User	: 899999	Duplicate
Password	: ●●●●●●●	
Expiry Time	: 2 hours	

Once you are registered with a SIP Server (e.g. **DrayTEL**) set your SIP username and password in the appropriate boxes (detailed explanation below). In the Registrar box enter the entire domain of the SIP server – everything after the @ sign of your SIP address. Click **OK** and your router will log onto the SIP server. In the "**VoIP Call Status**" you will find an "**R**" indicating you have registered with your SIP server.



VoIP >> VoIP Call Status

VoIP Call Status

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1 (R)	ACTIVE	729A/B	470091 <470091@fwd.pulve(	40	3798	4039	186	11	2	0	5

(R) : Means you have registered your SIP server

SIP Port

The port number 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.

Registrar

Enter the domain name (or IP address) of your registered SIP Registrar server.

Proxy

You can enter domain name or IP address of SIP proxy server. If this setting value is the same as Registrar, please press “Duplicate”.

Domain/Realm

You can enter domain name or IP address of SIP URL. e.g., if SIP URL is **sip:63065@fwd.pulver.com**, then this field contains **fwd.pulver.com**. If this setting value is the same as Registrar, please press “Duplicate”.

Stun Server

This setting defines whether the Vigor2200V/VG NAT traversal mechanism is enabled (by checking checkbox) or not. If activated, please also specify IP address of STUN server. Under this mode, VoIP communication from Vigor2200V/VG can pass through with the specified STUN server behind firewall/NAT.

Use Registrar

With the Registrar domain entered above, check this box to let the Vigor2200V/VG use the SIP Registrar.

Display Name

This field contains a name or a number which easily let you identify the person who you wan to call. It can also be the name for SIP display.

Account Name

Enter your SIP username (the first part of your SIP address before the @ sign)

Authorization User

This field contains a name or a number. It is also the name for SIP Authorization. If this setting value is the same as Display Name, please press “Duplicate”.

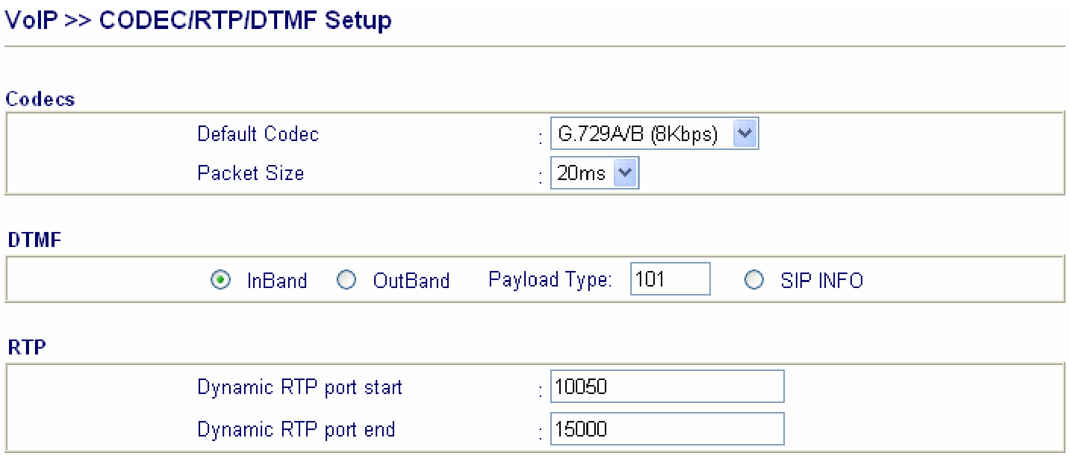
Password

Your SIP URL address as provided when you registered with a SIP service.

Expire Time

The time duration that your SIP registrar server keeps your registration record. Before the time expires the Vigor will issue another register message to registrar server again.

9.2.3 CODEC/RTP/DTMF



VoIP >> CODEC/RTP/DTMF Setup

Codecs

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

Packet Size : 20ms

DTMF

● InBand ○ OutBand Payload Type: 101 ○ SIP INFO

RTP

Dynamic RTP port start : 10050

Dynamic RTP port end : 15000

Default Codec

Select one of five CODECs as the default for your VoIP calls. The CODEC used for each call will be negotiate 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

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.

DTMF InBand

With this selected the Vigor will send DTMF tones as audio directly in the Voice stream when you press a key on the keypad.

DTMF OutBand

With OutBand selected the Vigor will capture the keypad number pressed, transform it to a digital form and send to the other side outside of the Voice stream; the receiver will generate the tone according to the digital form it receives. This function is very useful when network traffic congestion occurs to maintain the accuracy of DTMF tones.

DTMF Payload Type

The default value is 101, but can be anything from 96 to 127.

SIP Info

Enable this option to let the SIP proxy send DTMF tones to the dialed peer.

RTP

Specifies the start and end port for RTP stream. The default values are 10050 and 15000.

Calling Scenario

Peer-to-Peer Calling example

Arnor and Paulin each have a Vigor2500V router, here are their settings in order to call each other.

Arnor's IP address: **214.61.172.53**
Paulin's IP address: **203.69.175.24**

A. Arnor's settings

A-1. DialPlan index 1

Phone Number**: 1234**
(any number you like)
Name**: paulin**
IP Address / Domain**: 203.69.175.24**

A-2. SIP Related Function

SIP Port**: 5060(default)**
Registrar**: (leave blank)**
Port 1:
Use Registrar**: (leave blank)**
Name**: arnor**
Password**: (leave blank)**
Expiry Time**: (use default value)**

A-3. CODEC/RTP/DTMF

(use default value)

B. Paulin's settings

B-1. DialPlan index 1

Phone Number**: 123**
(any number you like)
Name**: arnor**
IP Address / Domain**: 214.61.172.53**

B-2. SIP Related Function

SIP Port**: 5060(default)**
Registrar**: (leave blank)**
Port 1:
Use Registrar**: (leave blank)**
Name**: paulin**
Password**: (leave blank)**
Expiry Time**: (use default value)**

B-3. CODEC/RTP/DTMF

(use default value)

C. Now, when Arnor wants to call Paulin, he picks up the phone and dials **1234#**.

D. When Paulin wants to call Arnor, she picks up the phone and dials **123#**

Calling via SIP Sever

Below are the settings for John and David to call each other using their DrayTEL registered SIP accounts, as neither Vigor user have a fixed public IP address.

John's SIP url: **john@draytel.org**
David's SIP url: **david@draytel.org**

A. John's settings

A-1. DialPlan index 1

Phone Number**: 2536**
(any number you like)
Name**: david**
IP Address / Domain**: draytel.org**

A-2. SIP Related Function

SIP Port**: 5060**
Registrar**:draytel.org**

Port 1:
Use Registrar**: (checked)**
Name**: john**
Password**:** ********
(enter John's registrar password)
Expiry Time**: (use default value)**

A-3. CODEC/RTP/DTMF

(use default value)

B. David's settings

B-1. DialPlan index 1

Phone Number**: 8989**
(any number you like)
Name**: john**
IP Address / Domain**: draytel.org**

B-2. SIP Related Function

SIP Port**: 5090**
Registrar**: draytel.org**

Port 1:
Use Registrar**: (checked)**
Name**: david**
Password**:** ********
(enter David's registrar password)
Expiry Time**: (use default value)**

B-3. CODEC/RTP/DTMF

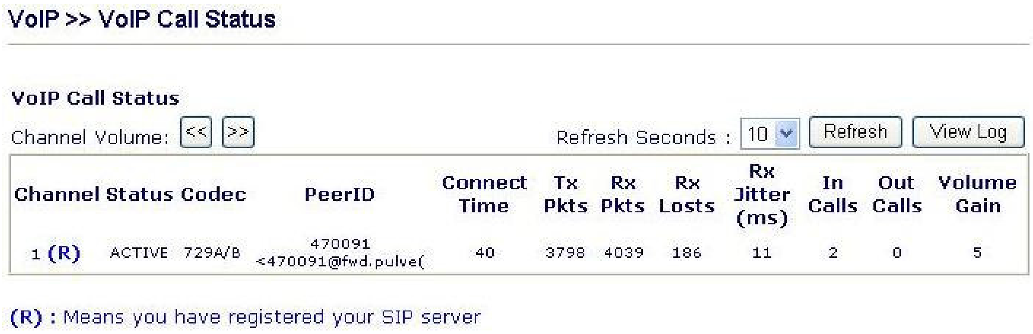
(use default value)

C. Now, when John wants to call David, he picks up the phone and dials **2536#**.

D. When David wants to call John, he picks up the phone and dials **8989#**

9.2.4 Voice Call Status

On VoIP call status, you can find the registered registrar, codec, connection and other important call status.   Because Vigor2200V/VG only has one VoIP port for regular analogue phone set, there is only one VoIP channel.



VoIP >> VoIP Call Status

VoIP Call Status

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1 (R)	ACTIVE	729A/B	470091 <470091@fwd.pulve(	40	3798	4039	186	11	2	0	5

(R) : Means you have registered your SIP server

Channel Volume

To adjust the volume of your VoIP calls.   Use these two buttons << >> to obtain appropriate **Volume Gain**.

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.

Status

To show 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

The voice CODEC employed by present channel.

PeerID

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

Connect Time

The format is represented as seconds.

Tx Pkts

Total number of transmitted voice packets during this connection session.

Rx Pkts

Total number of received voice packets during this connection session.

Rx Loss

Total number of lost packets during this connection session.

Rx Jitter

The jitter of received voice packets.

In Calls

The accumulating in-call times.

Out Calls

The accumulating out-call times.

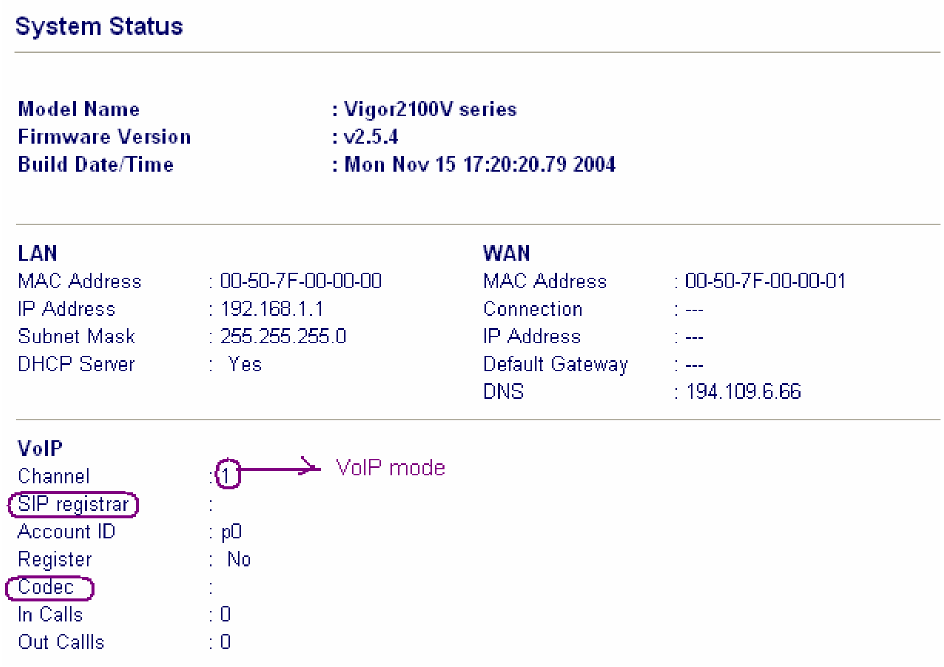
Volume Gain

The volume of present call.

View Log

To show the logs of VoIP calls as below.

Also on System Status, you can find the registered registrar and Codec. for Inbound calls and Outbound calls. The said status easily let you check whether your registration of SIP server is successful or not.



System Status

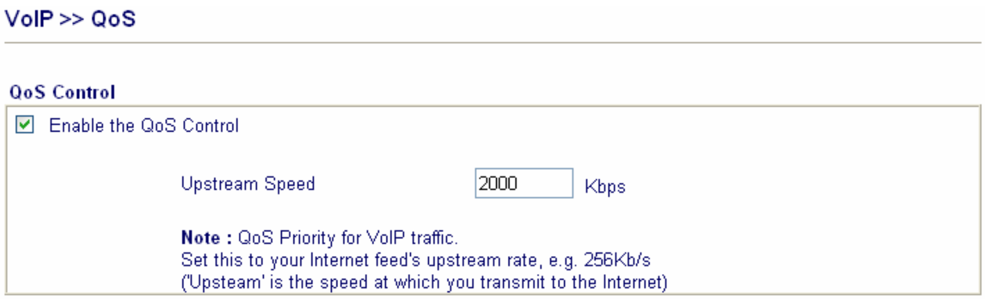
Model Name	: Vigor2100V series
Firmware Version	: v2.5.4
Build Date/Time	: Mon Nov 15 17:20:20.79 2004

LAN		WAN	
MAC Address	: 00-50-7F-00-00-00	MAC Address	: 00-50-7F-00-00-01
IP Address	: 192.168.1.1	Connection	: ---
Subnet Mask	: 255.255.255.0	IP Address	: ---
DHCP Server	: Yes	Default Gateway	: ---
		DNS	: 194.109.6.66

VoIP	
Channel	: 1
SIP registrar	:
Account ID	: p0
Register	: No
Codec	:
In Calls	: 0
Out Callls	: 0

9.2.5 QoS

Enter upstream speed to let Vigor2200V/VG assure 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)

Chapter 10
Wireless Setup

10.1 Introduction

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 face of the earth. Hundreds of millions of people exchange information every day using wireless communication products. Therefore, the Vigor2200VG series residential broadband routers are designed for increasing flexibility and efficiency of a small office/a home by deploying the WLAN network.

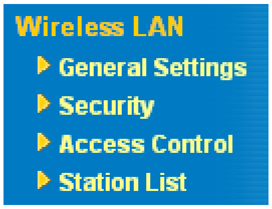
To elaborate one example, any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable.

One more example, parents can write E-mail at their studyoom and kids are also able to surf Internet at their bedrooms as the Vigor2200VG is set up in some corner of a home. Parents do not need to drill any hole for installing LAN cable everywhere in the house.

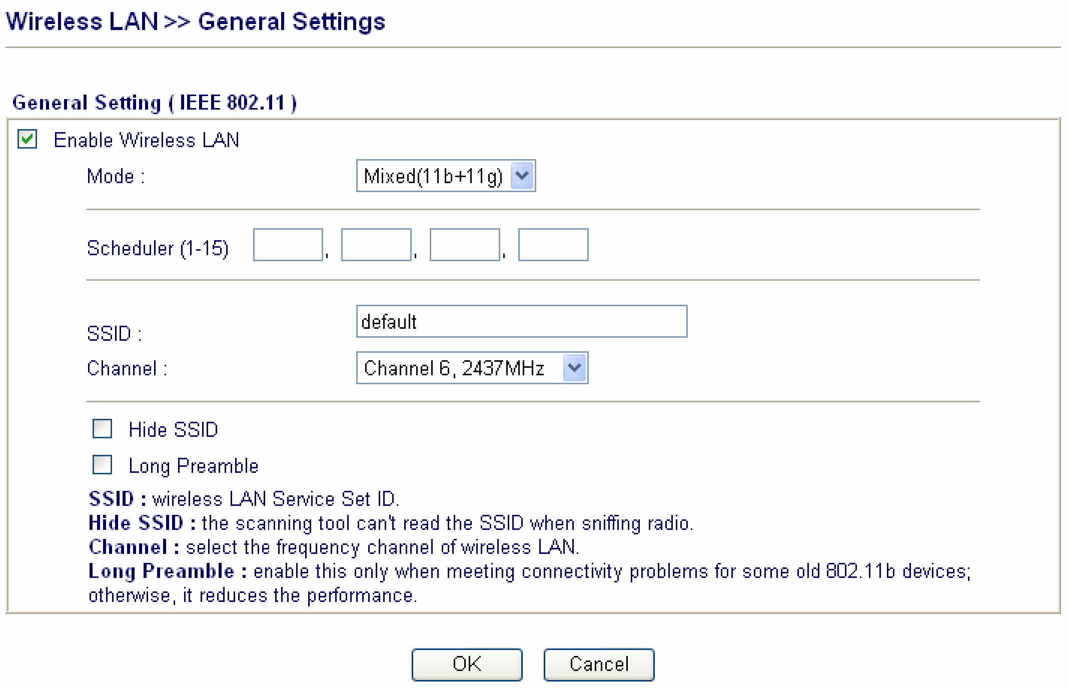
The Vigor2200VG series are equipped with a wireless LAN interface compliant with the IEEE 802.11g protocol supporting data rate of 54Mbps. The wireless LAN capability enables high mobility of several users so that they can simultaneously access all LAN facilities just like on a wired LAN as well as Internet and WAN access.

10.2 Settings

Click **Wireless Setup** to open the setup page.



10.2.1 General Settings



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.

<u>Enable Wireless LAN</u>

Check the box to enable wireless function.

Mode

Select an appropriate wireless mode.

Mixed(11b+11g)	The radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously.
11g Only	The radio only supports IEEE802.11g protocol.
11b Only	The radio only supports IEEE802.11b protocol.

Scheduler

Set the wireless LAN to work at some time interval only.

SSID and Channel

The default SSID is "default". We suggest you change it to a particular name. In this case, SSID was changed to “DrayTek”.

SSID	It is used to name the wireless LAN, and must have the same content in client PC/notebook wireless card(s). SSID can be any text numbers or various special characters
Channel	A wireless channel for the router. The default channel is 6. You can change it to more appropriate one if the selected channel is under serious interference.

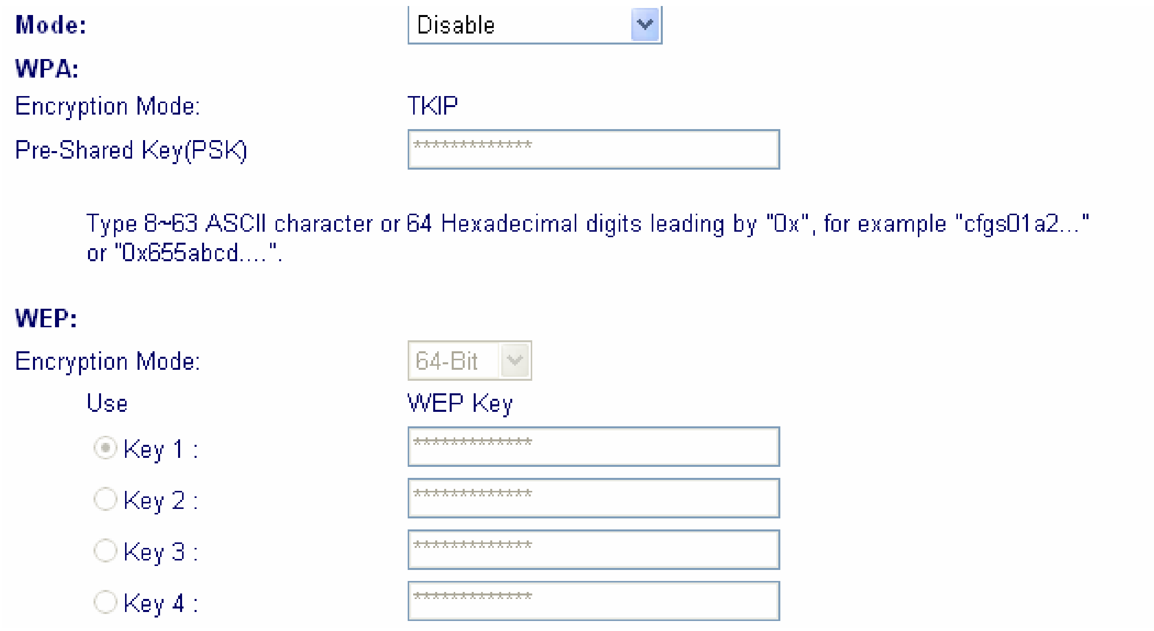
Hide SSID

Check it to prevent from wireless sniffing and make it harder for unauthorized clients to join your wireless LAN.

10.2.2 Security

To improve the security and privacy of your wireless data packets, the WEP and WPA encryption feature can be employed, where WEP stands for

Wireless Equivalent Privacy. The WEP facility that uses a set of four *default keys* encrypts each frame transmitted from the radio using only one of the given keys. Default keys are shared between the Vigor wireless router and WEP station in a service set. Once a station has obtained the default keys for its service set, it may communicate using WEP. WPA (Wi-Fi Protected Access) uses the Temporal Key Integrity Protocol (TKIP) for encryption. It greatly enhances the over-the-air data protection and access control on existing Wi-Fi networks. It addresses the weaknesses of WEP. By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.



Mode: Disable

WPA:

Encryption Mode: TKIP

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

Use	WEP Key
● Key 1 :	*************
○ Key 2 :	*************
○ Key 3 :	*************
○ Key 4 :	*************

Mode

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

Disable	Turn off the encryption mechanism
WEP Only	Accepts only WEP clients and the encryption key should be entered

	in WEP Key.
WEP or WPA/PSK	Accepts WEP and WPA clients simultaneously and the encryption key should be entered in WEP Key and PSK respectively.
WPA/PSK	Accepts only WPA clients and the encryption key should be entered in PSK.

WPA Encryption

The WPA encrypts each frame transmitted from the radio using the pre-shared key (PSK) which entered from this panel.

Pre-Shared Key (PSK): Either 8~63 ASCII characters or 64 Hexadecimal digits leading by 0x can be entered. For example "0123456789ABCD...." or "0x321253abcde.....".

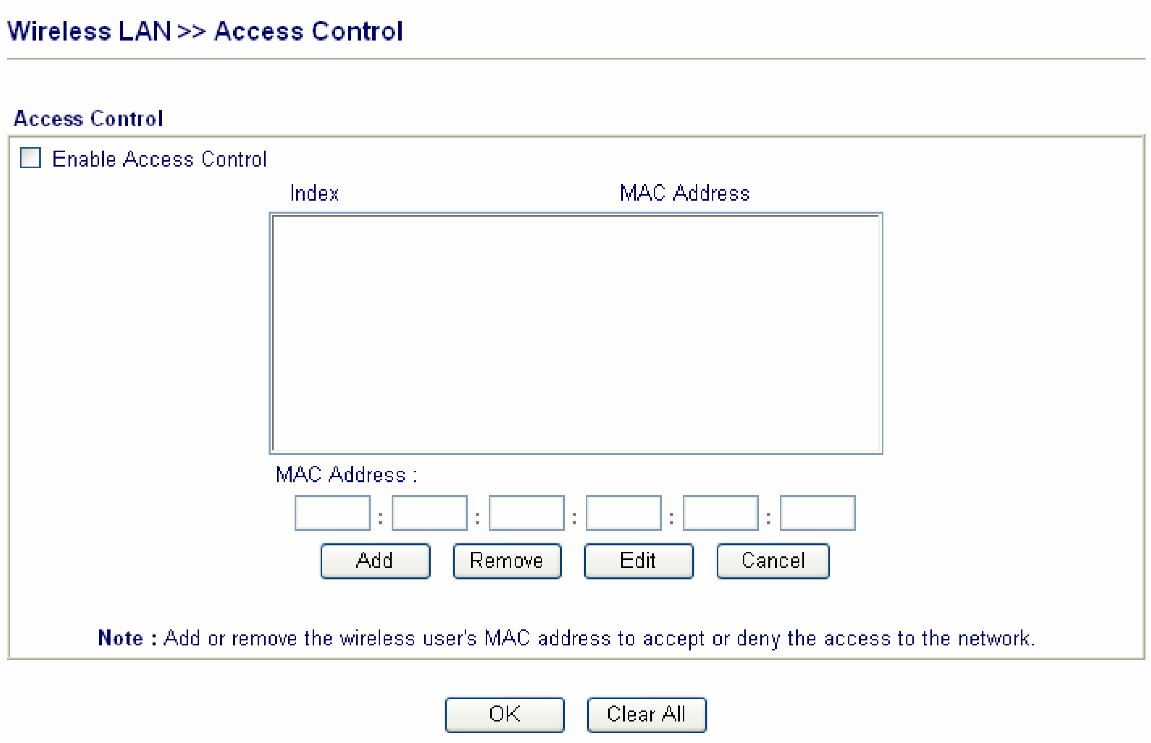
WEP Encryption

64-Bit	For 64bits WEP key, either 5 ASCII characters or 10 hexadecimal digitals leading by 0x can be entered. For example, ABCDE or 0x4142434445.
128-Bity	For 128bits WEP key, either 13 ASCII characters or 26 hexadecimal digits leading by 0x can be entered. For example, ABCDEFGHIJKLM or 0x4142434445464748494A4B4C4D.

128 bits WEP is most secure, but has more encryption/decryption overhead. Note that 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. Click the circle under Use next to the key you wish to use.

10.2.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address which 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.



Note : Add or remove the wireless user's MAC address to accept or deny the access to the network.

Enable Access Control

To check the **Enable Access Control** to enable the MAC Address access control feature.

MAC Address

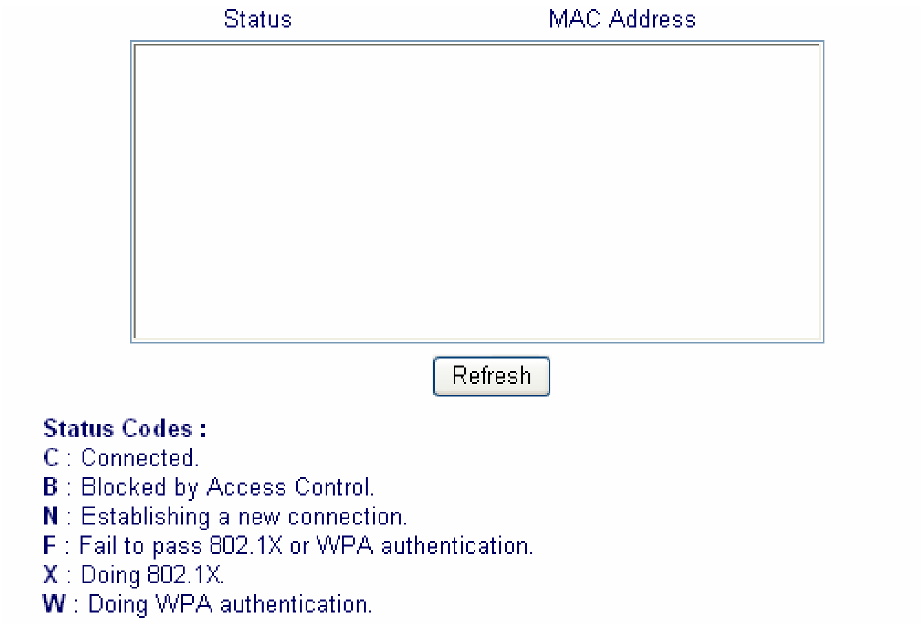
Display all MAC addresses that are edited before. Four buttons (Add, Remove, Edit, and Cancel) are provided to edit a MAC address.

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.
Clean All	Clean all entries in the MAC address list.
OK	Click it to save the access control list.

10.2.4 Station List

The Vigor router offers you a convenient **Station List facility** to scan the running WLAN clients being near the router. If neighbors or other WLAN clients are active, you can press "Refresh" to get available WLAN stations' information including its status and MAC address. You can select the wish WLAN station from **Station List** to add it to **Access Control** list by clicking highlight, then press "**Add**". Or editing a station's MAC address manually is another option. After the these operations, you go to **Access Control** and the listed WLAN stations which are allowed to access network resources via the Vigor router.



Status Codes :
C : Connected.
B : Blocked by Access Control.
N : Establishing a new connection.
F : Fail to pass 802.1X or WPA authentication.
X : Doing 802.1X.
W : Doing WPA authentication.

Chapter 11
System Maintenance Setup

11.1 Introduction

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.

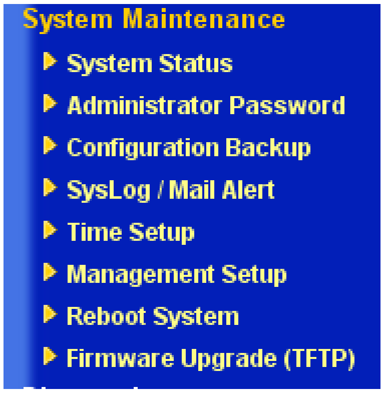
The **Configuration Backup** enable you to keep running configurations of your current router as a file or restore the configurations with the file. The router provides an web-based way to let you backup or restore the configuration very simple.

By default, the router may be configured and managed through any Telnet client or Web browser running on any operating system. There is no requirement for additional software or utilities. However, for some specific environments, in **Management**, you may change the server port numbers for the built-in Telnet or HTTP server, create access control lists to protect the router, or reject the system administrator to login from the Internet.

Also in **Reboot System** and **Firmware Upgrade**, you can reboot the system once you finish some set up and upgrade firmware via TFTP.

11.2 Settings

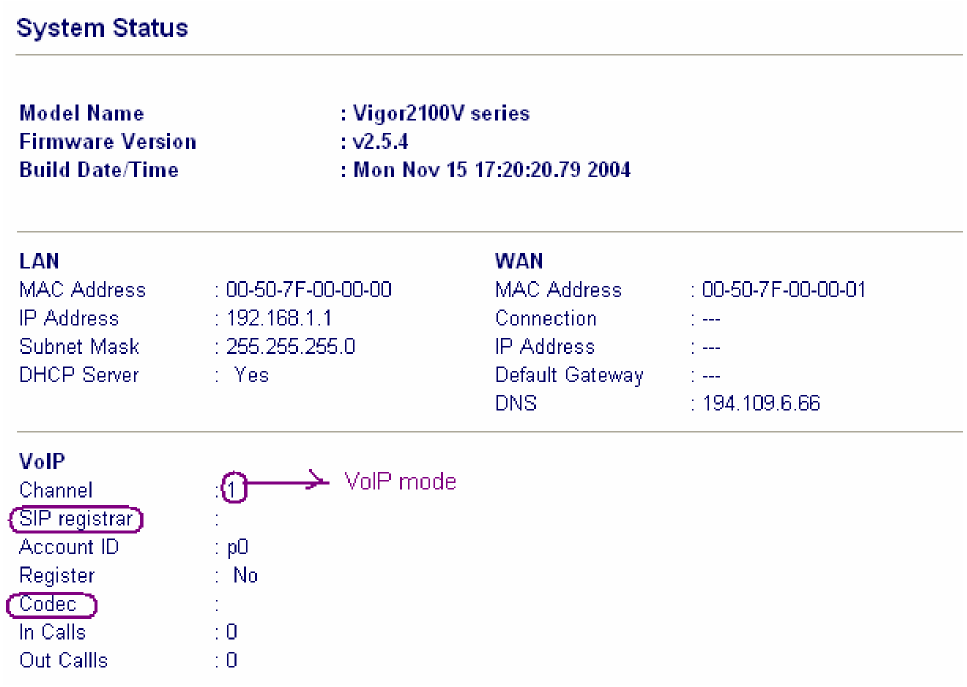
Click **System Maintenance Setup** to open the setup page.



System Status	Pre-settings of up to 60 SIP addresses of VoIP contacts.
Administrator Password	Settings of SIP port, registrar, proxy, domain and Stun server.
Configuration Backup	Settings of default Codec, DTMF and RTP
SysLog/Mail Alert	Call Status including registered registrar, codec, connection and others.
Time Setup	Settings for time, either inquiring from PC or from NTP server.
Management Setup	Settings of Management Access Control, SNMP, and Port.
Reboot System	Manually reboot the system
Firmware upgrade(TFTP)	Upgrade the firmware via TFTP

11.2.1 System Status

In **System Status**, you will see the result shown on the right frame.



System Status

Model Name : Vigor2100V series
Firmware Version : v2.5.4
Build Date/Time : Mon Nov 15 17:20:20.79 2004

LAN		WAN	
MAC Address	: 00-50-7F-00-00-00	MAC Address	: 00-50-7F-00-00-01
IP Address	: 192.168.1.1	Connection	: ---
Subnet Mask	: 255.255.255.0	IP Address	: ---
DHCP Server	: Yes	Default Gateway	: ---
		DNS	: 194.109.6.66

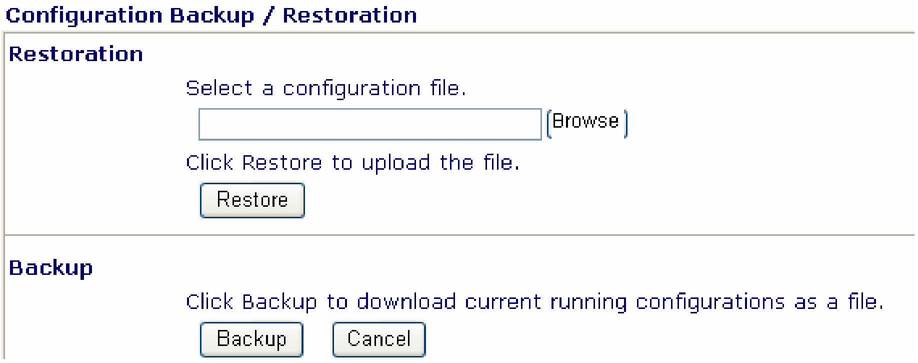
VoIP
Channel : 1
SIP registrar :
Account ID : p0
Register : No
Codec :
In Calls : 0
Out Callls : 0

In order to let you know the settings result, we design the Status bar on Set-up Menu. You can find the "**Ready**" indicates that you can enter settings. "Settings Saved" means your settings are saved once you click "**Finish**" or "**OK**" button. If the settings are wrong or get problematic, you can find fail message on **Status** bar.

11.2.2 Configuration Backup

Backup the Running Configuration

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



Configuration Backup / Restoration

Restoration

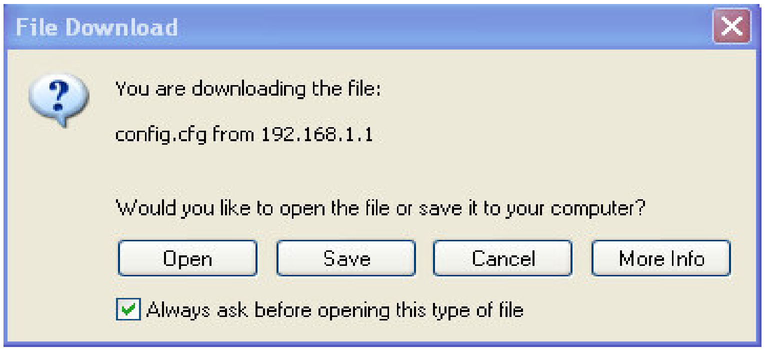
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

2. Click Backup button to get configurations.



File Download

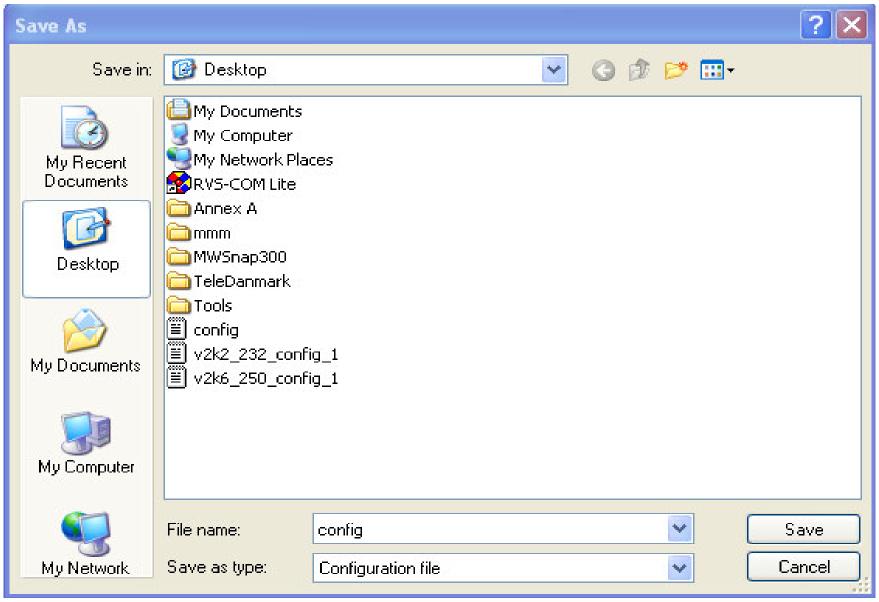
You are downloading the file:

config.cfg from 192.168.1.1

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

☑ Always ask before opening this type of file

3. Click OK button to save configuration as a file. The default filename is **config.cfg**. You could give it another name by yourself.



Save As

Save in: Desktop

File name: config

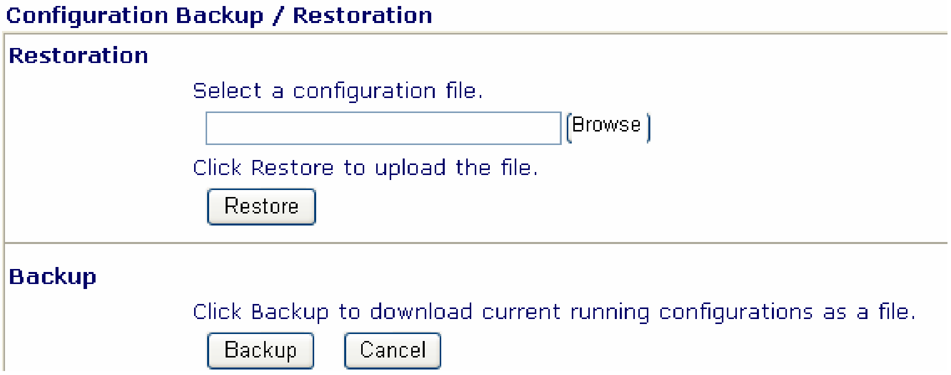
Save as type: Configuration file

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 the Configuration with a Configuration File

1. Go to **System Maintenance** > **Configuration Backup**. The following windows will be popped-up, as shown below.
2. Click **Browse** button to choose the correct configuration file for uploading to the router.



Configuration Backup / Restoration

Restoration

Select a configuration file.

Click Restore to upload the file.

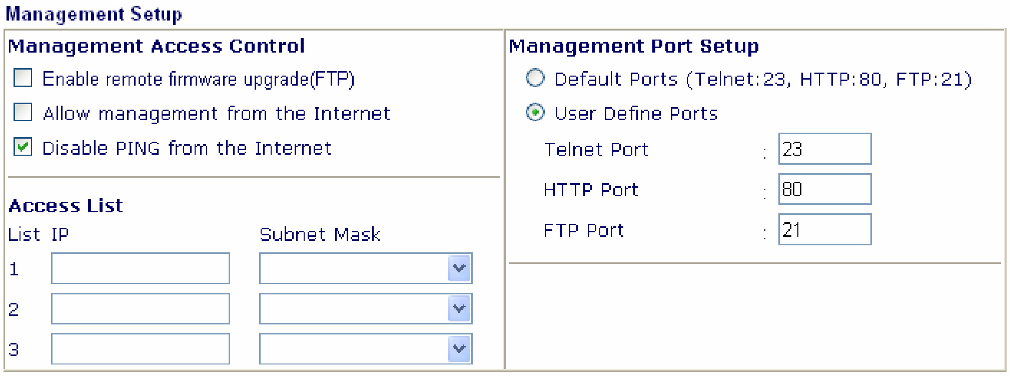
Backup

Click Backup to download current running configurations as a file.

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

11.2.3 Management

Click **Management Setup**. The following setup page will appear on your computer screen.



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

Management Setup

The port number 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.

Enable remote firmware update	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.

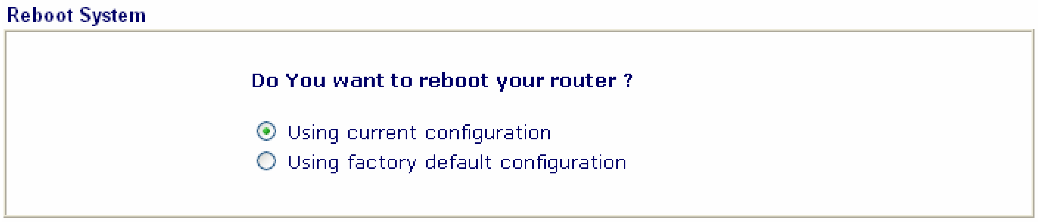
IP	Indicate an IP address allowed to login to the router
Subnet Mask	Represent a subnet mask allowed to login to the router.

Management Port Setup

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.
Enable SNMP Agent	Chick the checkbox to enable built-in SNMP agent.
Get Community	Specify a string to identify the management communities for the SNMP GET command.
Set Community	Specify a string to identify the management communities for the SNMP SET command.
Manager Host IP	Specify the IP address of the SNMP manager station.
Trap Community	Specify a string to identify the management communities for the SNMP TRAP notifications.
Notification Host IP	Specify the IP address of the station that wants to receive the TRAP notifications

Reboot System

The Web Configurator may be used to restart your router. Click **Reboot System** in the main menu to open the following page.



Reboot System

Do You want to reboot your router ?

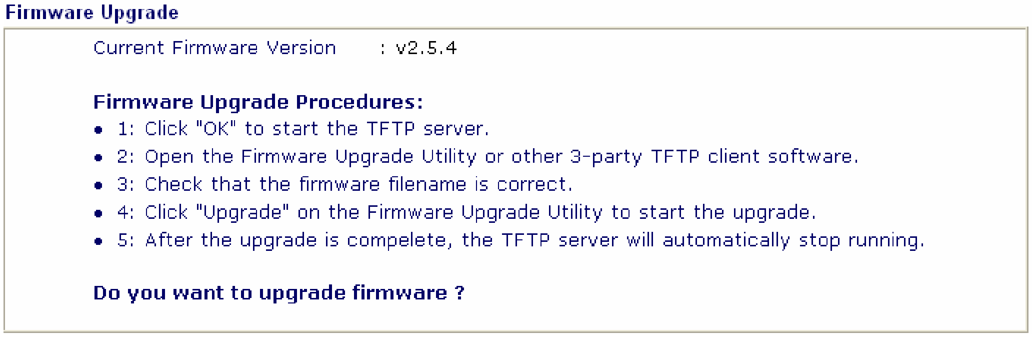
● Using current configuration
○ Using factory default configuration

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 3 to 5 seconds to reboot the system.

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 steps will guide you to upgrade firmware. In the following, we use an example to explain the firmware upgrade. Note that this example is running over Windows OS (Operating System).

1. Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com
2. Click System Maintenance>> Router Firmware Upgrade Utility to launch the Firmware Upgrade Utility.



Firmware Upgrade

Current Firmware Version : v2.5.4

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 the **Browse** button to locate the new firmware file. The program will look for any Vigor routers on your LAN and display them by IP address. Select the 'IP address' of the appropriate router to upgrade, then press **Upgrade**. Enter the router's password when asked (or press **OK** if there is no password). The upgrade action will start and the status will be shown on the progress bar. Once the upgrade operation has completed, wait approximately 30 seconds and the router will be ready (ACT light in the front panel of your router will resume flashing normally).

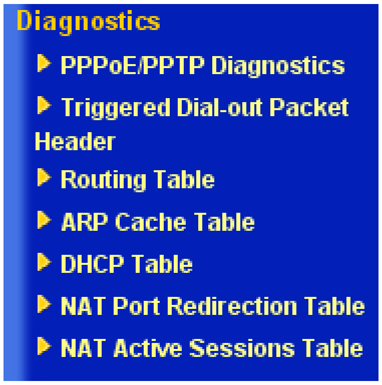
Chapter 12 Diagnostics Setup

12.1 Introduction

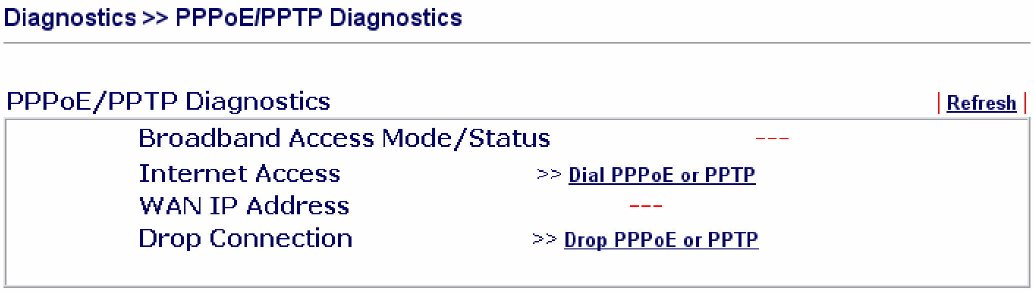
Diagnostic Tools provide a useful way to view or diagnose the status of you Vigor router.

12.2 Settings

Click **Diagnostics** to open the setup page.


Diagnostics
PPPoE/PPTP Diagnostics
Triggered Dial-out Packet Header
Routing Table
ARP Cache Table
DHCP Table
NAT Port Redirection Table
NAT Active Sessions Table

12.2.1 PPPoE/PPTP Diagnostics



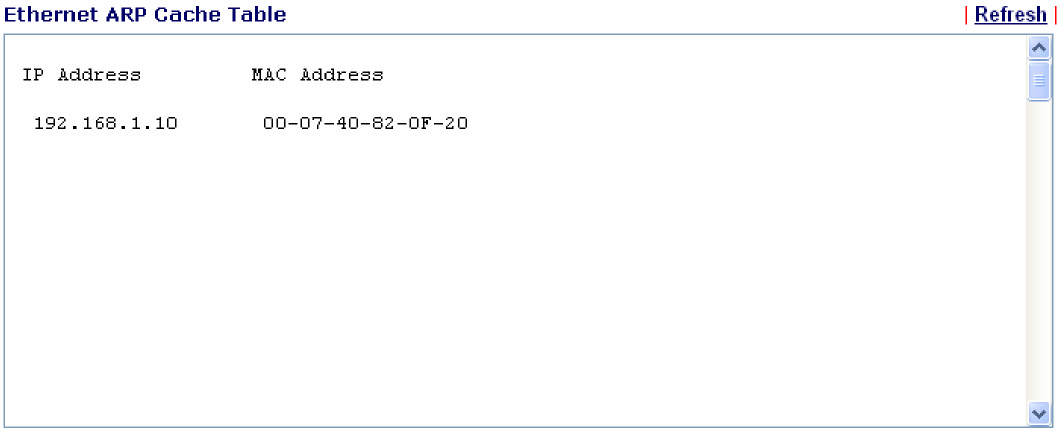
PPPoE/PPTP Diagnostics

Broadband Access Mode/Status	---
Internet Access	>> Dial PPPoE or PPTP
WAN IP Address	---
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 **PPPoE**, **PPTP**, **Static IP,** or **DHCP Client** depending on which 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 PPTP	Click it to force the router to establish a PPPoE or PPTP connection.
Dial PPPoE or PPTP	Click it to force the router to establish a PPPoE or PPTP connection.

12.2.2 ARP Cache Table

Click **View 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.



Ethernet ARP Cache Table

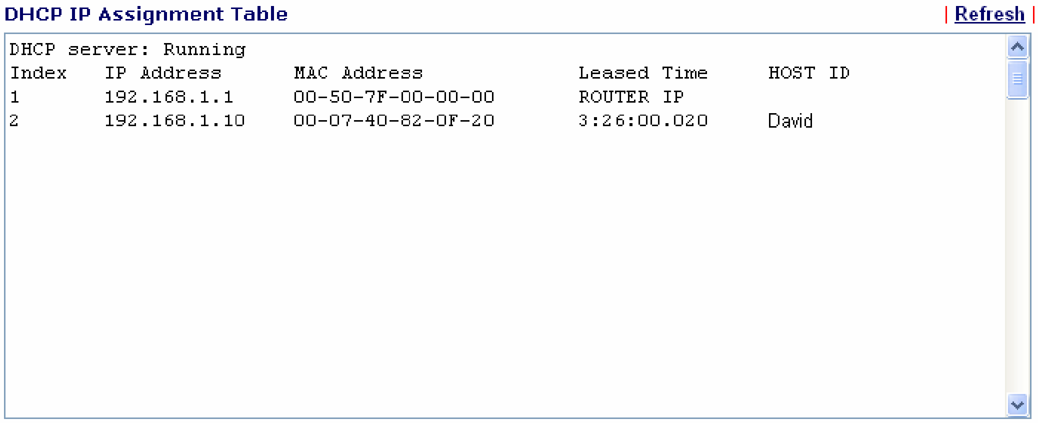
```
IP Address         MAC Address

 192.168.1.10       00-07-40-82-0F-20
```

Refresh: Click it to reload the page.

12.2.3 DHCP Assigned IP Address

The facility of **View DHCP Assigned IP Addresses** provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.



```
DHCP server: Running
Index    IP Address      MAC Address             Leased Time     HOST ID
1        192.168.1.1     00-50-7F-00-00-00       ROUTER IP
2        192.168.1.10    00-07-40-82-0F-20       3:26:00.020     David
```