www.draytek.com

Vigor2500V Series ADSL VoIP Router

Manual V1.0

Preamble of Vigor2500V/Vi series ADSL VoIP Routers

1. Benefits of Vigor2500V series

- **ADSL router for sharing your Internet connection**
- **Robust firewall to help protect your computers**
- **Make / Receive Voice calls over your ADSL connection using a regular telephone handset**
- **Integration with your existing phone line (POTS) with automatic failover during power cuts**
- **Free Voice-over-IP phone calls to other VoIP users**
- **ISDN backup/remote access/ISDN loop through are available on Vigor2500Vi series which have ISDN interface**
- **Compatible with Windows and Mac OS**

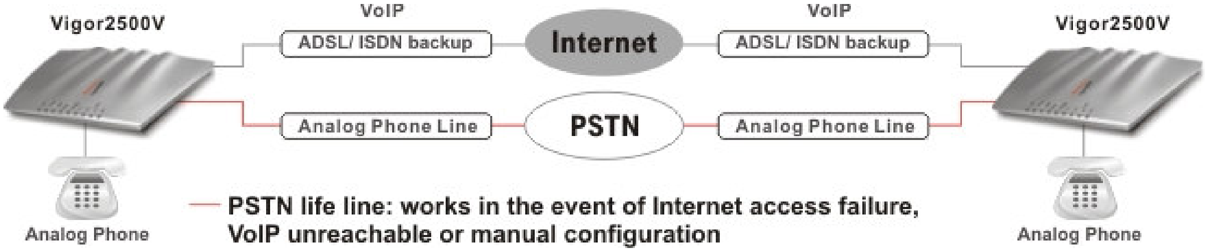
1.1 Brief Overview

	Vigor2500V	Vigor2500Vi
ADSL Router	*	*
VoIP	*	*
PSTN life line	*	*
ISDN loop through	-	*
ISDN backup	-	*

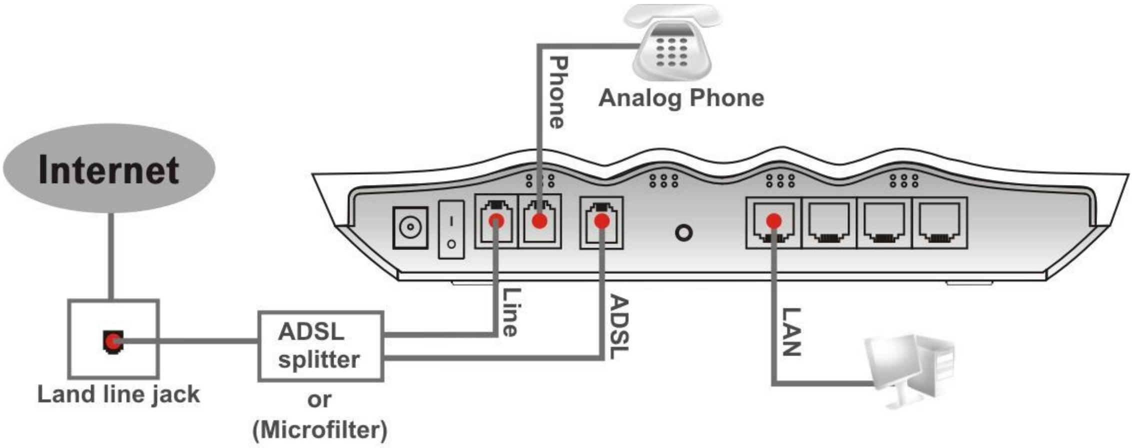
What does **"PSTN life line"** and **"ISDN loop through"** perform on Vigor2500V series**?**

The Vigor2500V has a “Line” port on the rear panel for connecting to a PSTN (regular analogue) line. The Loop Through option can be used to set an alternate telephone number for your contact on the PSTN, which the Vigor2500V will dial instead of the SIP account if you lose ADSL access or power to the Vigor2500V. Hence, the PSTN line can act as a lifeline (backup mechanism) for VoIP calls. The lifeline mechanism is activated automatically but can also be manually configured.

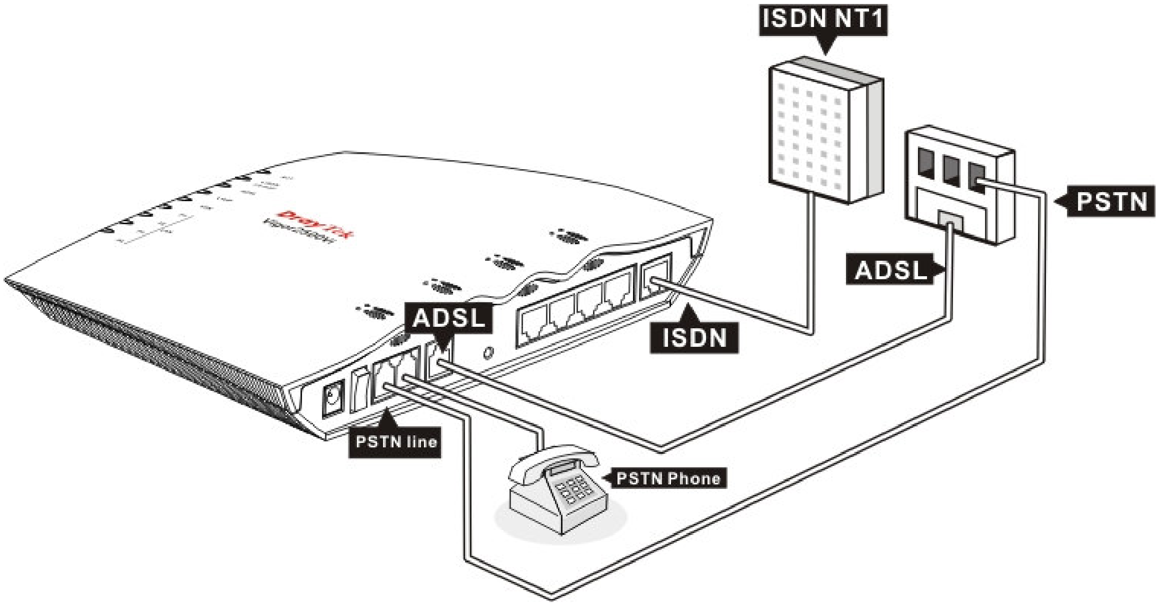
Because there is ISDN interface on the Vigor2500Vi series, you can use the ISDN line as phone line as well as Internet remote access/dial back-up for ADSL. You will be able to still make ISDN phone calls if the router loses power or the VoIP calls can not make as Internet access is broken. Hence, the ISDN line can also be lifeline (backup mechanism) for VoIP calls.



Annex- A countries:



Annex – B countries



1.2 Highlights

VoIP

- G.168 Line Echo-cancellation
- Gain Control
- Jitter Buffer (250ms)
- Voice CODEC: G.711 A/u law, G.729 A/B, VAD/CNG
- Tone Generation and Detection: DTMF, Dial, Busy, Ring Back
- Protocol: SIP, RTP/RTCP

ADSL

- Compatible with ADSL lines up to 8 Mbps.
- Support PPPoE, PPPoA, MPoA

LAN

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

Network Features

- DHCP server / relay
- Dynamic DNS
- Call Scheduling

Firewall

- Stateful Packet Inspection
- Selectable DoS/DDoS protection
- IP address anti-spoofing
- User-configurable packet filtering
- NAT/PAT with Port Forwarding/Redirection & DMZ
- E-mail alerting mechanism

E-mail Detection

- Detect user-defined e-mails and hold them in mail server (POP3).

Flexible URL Content Filtering

- URL blocking by user-defined keywords
- Preclude web surfing from using directly IP address
- Java/ActiveX/cookies/proxy blocking
- Executable/compressed/multimedia files blocking
- Time schedule support

Application Support

- Windows Messenger, Yahoo Messenger, MSN Messenger V6.0, NetMeeting, ICQ2001b/2002a, most online gaming, and other multimedia applications
- UPnP protocol support

Router Management

- Web-based User Interface
- Command line interface (Telnet)
- Telnet remote access support
- Built-in diagnostic tools
- Quick Start Wizard
- Attack alert by e-mail
- Syslog Monitoring

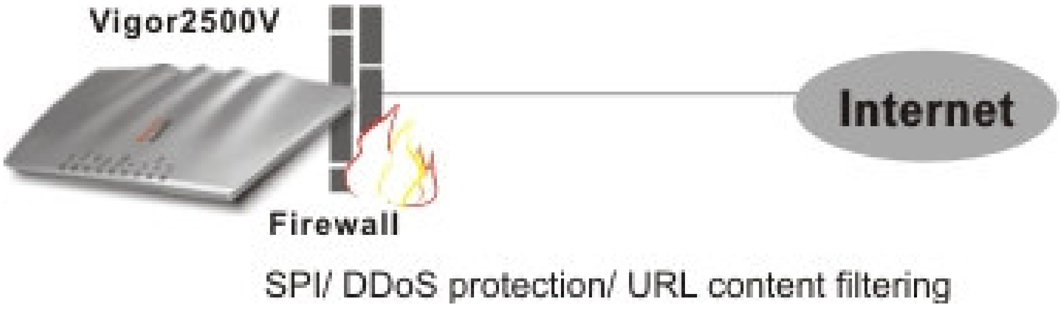
ISDN Facilities (for Vigor2500Vi only)

- Compatible with Euro ISDN
- Automatic ISDN backup
- Support for 64/128kbps (multilink-PPP)
- Bandwidth on demand (automatically switches between 64kbps and 128kbps)
- LAN-to-LAN connectivity
- Remote Activation
- Virtual TA

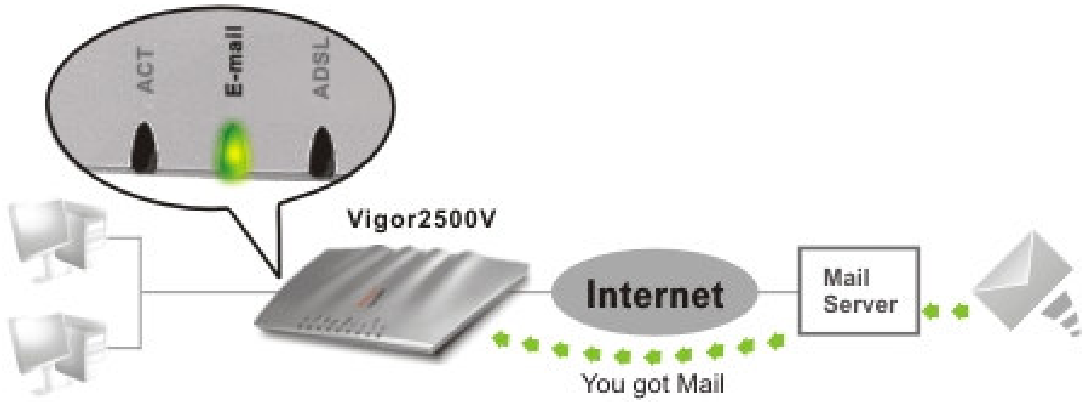
Routing Support

- RIPv2 **(not applicable to the UK)**
- Static Route **(not applicable to the UK)**

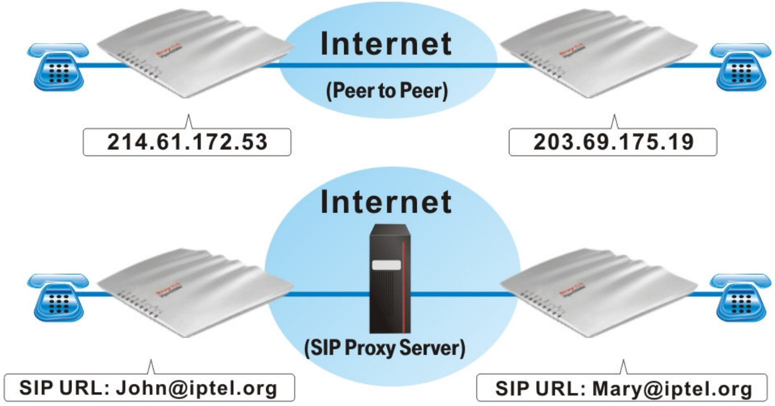
Robust Firewall:



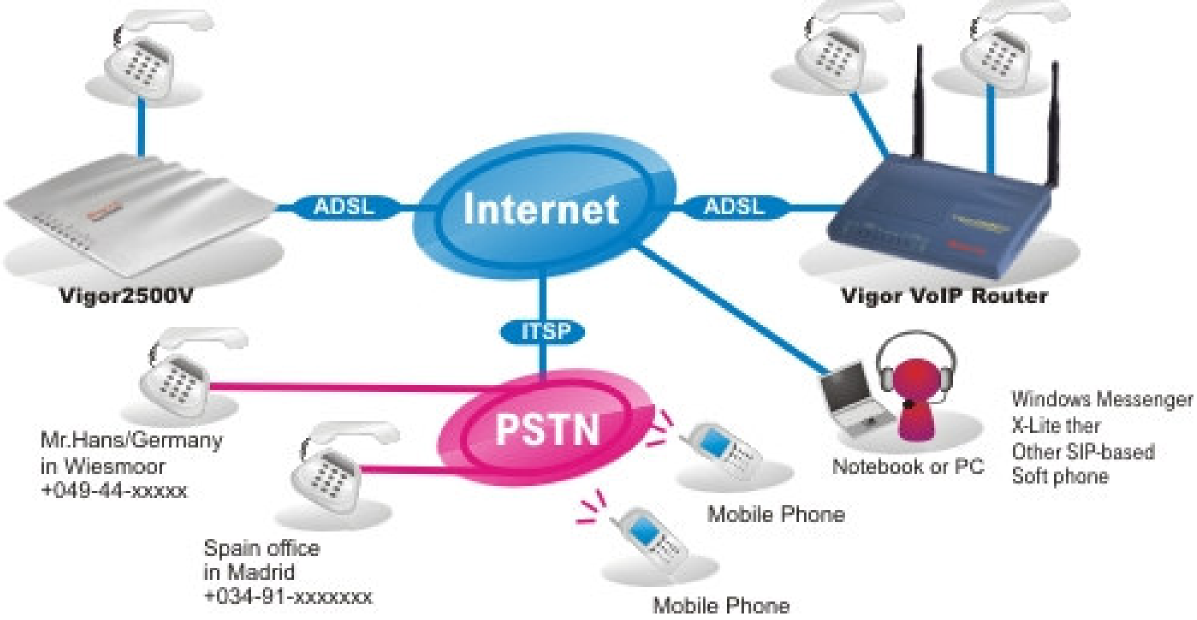
E-mail Detection:



Peer to Peer VoIP communications:



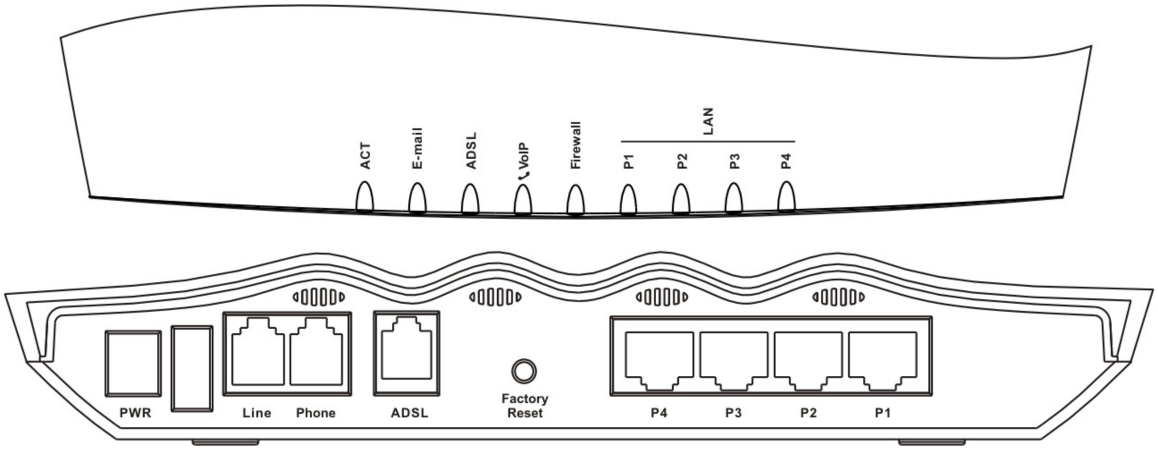
Vigor2500V series with the services of ITSP:



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)].

1.3 Front Panel LEDs and Rear Panel Interfaces

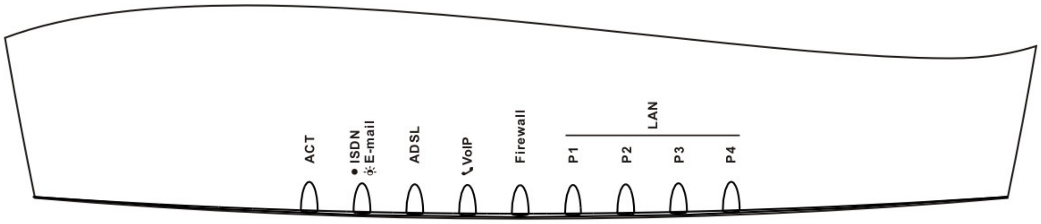
1.3.1 Vigor2500V

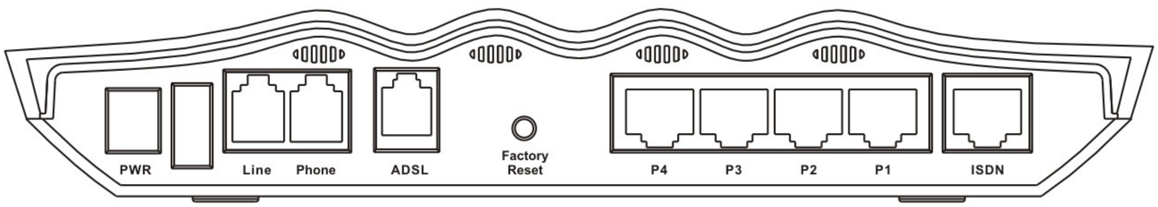


LED	Status	Explanation
ACT (Activity)	blinking	The router is powered on and running properly.
E-mail	blinking	When detecting one or more user-defined e-mails existing on mail server.
ADSL	on	The ADSL line is showtime.
VoIP	green	Solid light when the handset of phone is picked up (off hooked).
		Blinking per 0.3 second when phone call is via ISDN loop through.
		Blinking per 2 seconds when phone is connected through VoIP.
	orange	Solid light when phone call is via PSTN life line.
Firewall	on	The firewall function is active.
	blinking	When encountering DoS attacks.
LAN **(P1, P2, P3, P4)**	green	A normal 100Mbps connection is through its corresponding port.
	orange	A normal 10Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.

Interface	Description
PWR	Connect the included power adapter to the power outlet.
Line	Connect to the analog phone line for PSTN life line.
Phone	Connect to the analog phone for VoIP communication.
ADSL	Connect the ADSL line to access the Internet.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1, P2, P3, P4	Connect to the local network devices.

1.3.2 Vigor2500Vi

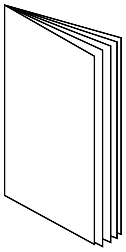




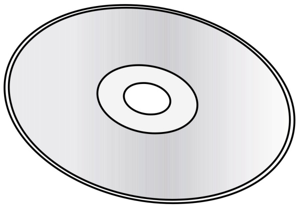
LED	Status	Explanation
ACT (Activity)	blinking	The router is powered on and running properly.
ISDN/E-mail	on	The ISDN network is correctly setup.
	blinking	When detecting one or more user-defined e-mails existing on mail server.
ADSL	on	The ADSL line is showtime.
VoIP	green	Solid light when the handset of phone is picked up (off hooked).
		Blinking per 0.3 second when phone call is via ISDN loop through.
		Blinking per 2 seconds when phone is connected through VoIP.
	orange	Solid light when phone call is via PSTN life line.
Firewall	on	The firewall function is active.
	blinking	When encountering DoS attacks.
LAN (P1, P2, P3, P4)	green	A normal 100Mbps connection is through its corresponding port.
	orange	A normal 10Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.

Interface	Description
PWR	Connect the included power adapter to the power outlet.
Line	Connect to the analog phone line for PSTN life line.
Phone	Connect to the analog phone for VoIP communication.
ADSL	Connect the ADSL line to access the Internet.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1, P2, P3, P4	Connect to the local network devices.
ISDN	Connected to an external NT1(or NT1+) box provided by your ISDN service provider.

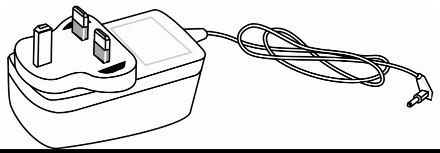
1.4 Package Contents



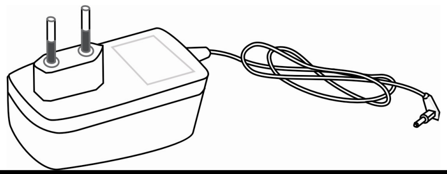
Quick Installation Guide



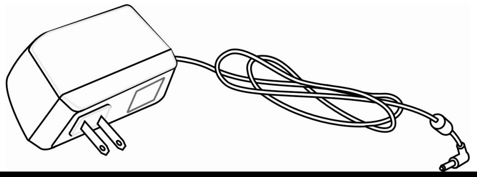
CD (Manual and Utilities)



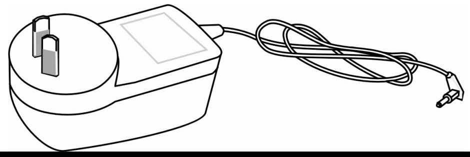
UK-type power adapter



EU-type power adapter



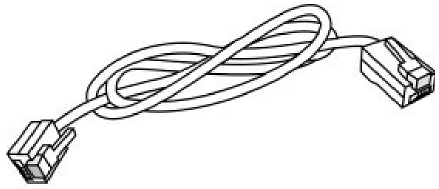
USA/Taiwan-type power adapter



AU/NZ-type power adapter

RJ-45 (Ethernet)

RJ-11 to RJ-11 (Annex A / B)



RJ-11 to RJ-45 (Annex B)

RJ-45 to RJ-45 (ISDN)
(for Vigor2500Vi only)

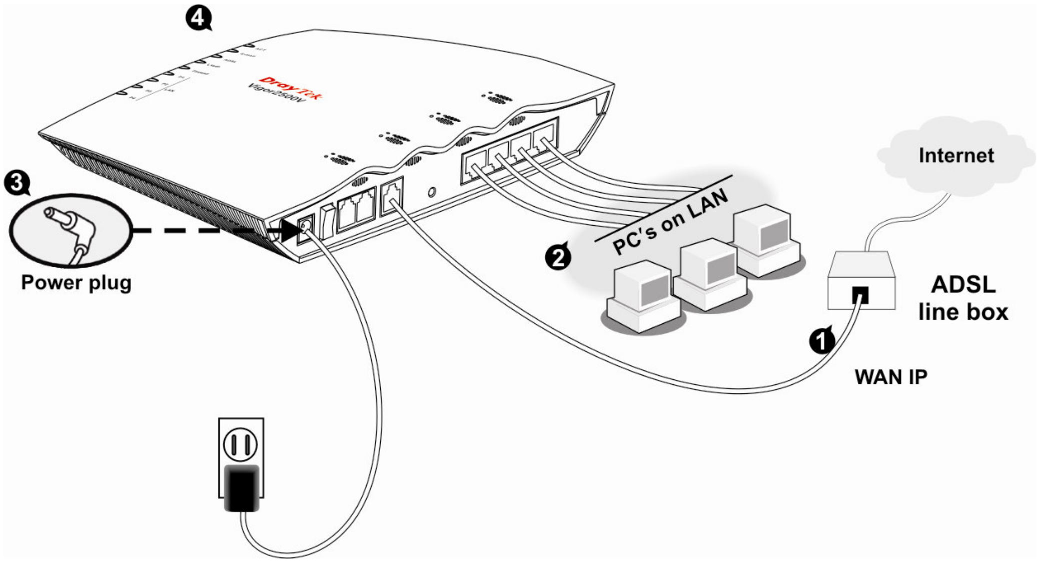
2. Hardware Installation of Your Vigor2500V/Vi Router

2.1 Hardware Installation

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

1. Connect the ADSL interface to the external splitter with a RJ-11 cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
3. Connect the attached power adapter to the power port.
4. Check the **ACT**, **ADSL** and **LAN** LEDs to assure network connections.
   (Regarding detailed LED status explanation please refer to section 1.3)

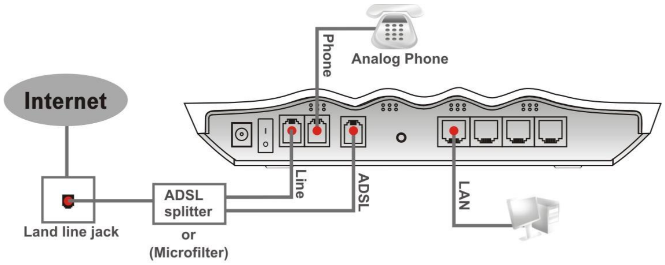
Connection scenario is shown as below:



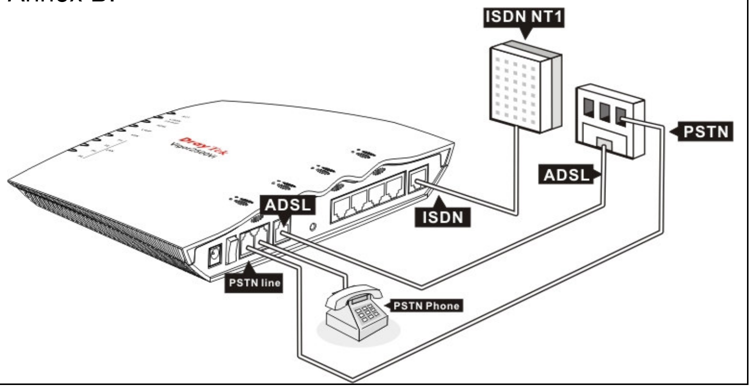
The splitter or microfilter is the optional accessories.

There are some variant connection in Annex A and Annex B countries. Followings are more reference for you:

Annex A:



Annex B:



About This User's Manual

This manual is designed to assist users in using the Vigor2500V of Internet security routers. 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**!

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: Vigor2500V Series ADSL VoIP Routers

DrayTek Corp. declares that Vigor2500V 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 ISDN interface of Vigor2500Vi series is designed for the Euro-ISDN network throughout the EC-region and where Telcos/ISPs are also adopting Euro-ISDN to their ISDN services.

Commission (FCC) Interference Statement

The Vigor2500V series 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

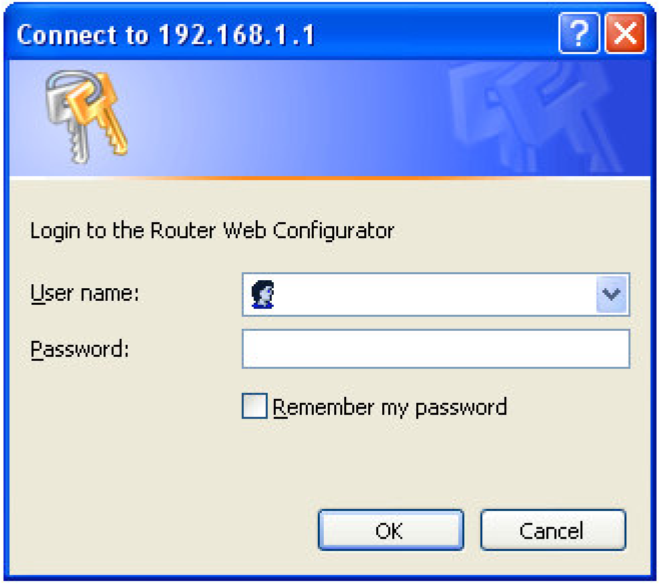
1.1 Introduction

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 Vigor2500V series. You can directly access the Quick Start Wizard via Web Configurator.

You can also find the Quick Start Wizard from the router tool of firmware CD enclosed with the package. As considering the convenience, we suggest you to set up the Internet access via Quick Start Wizard built-in within the web configurator.

Configure Your Router via Quick Start Wizard

Step1. 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

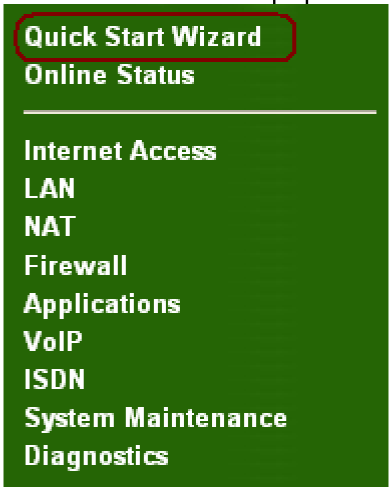
User name:

Password:

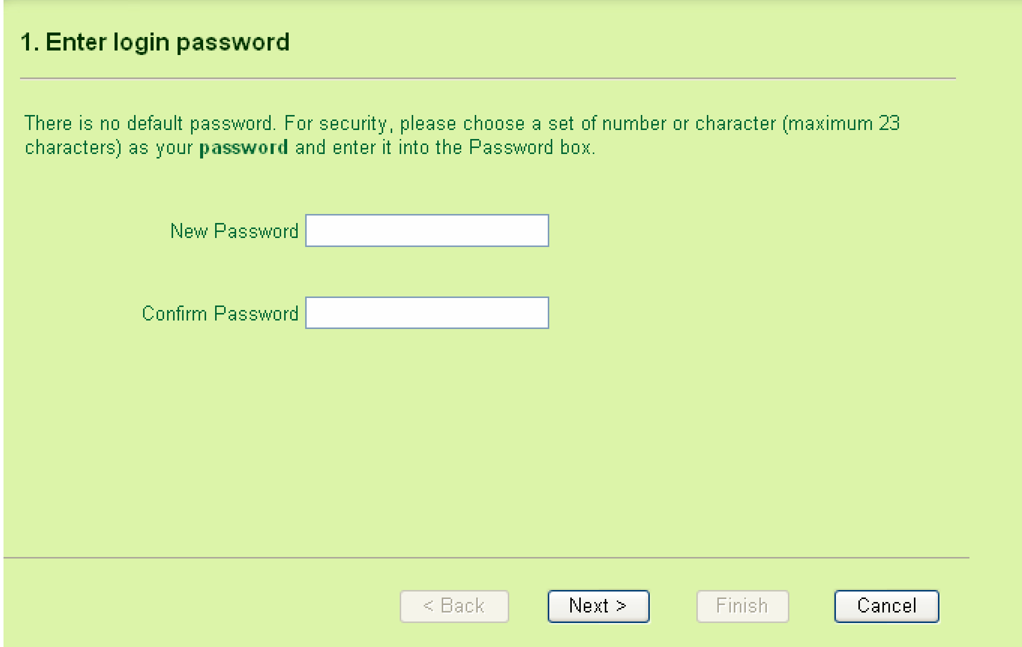
☐ Remember my password

If you fail in access to the web configuration, please refer to "Trouble Shooting" guide.

Step2. The **Main Menu** will pop out after completing previous step.



Step3. Now Quick Start Wizard is switched on. Enter login password. Then click **Next** to continue.



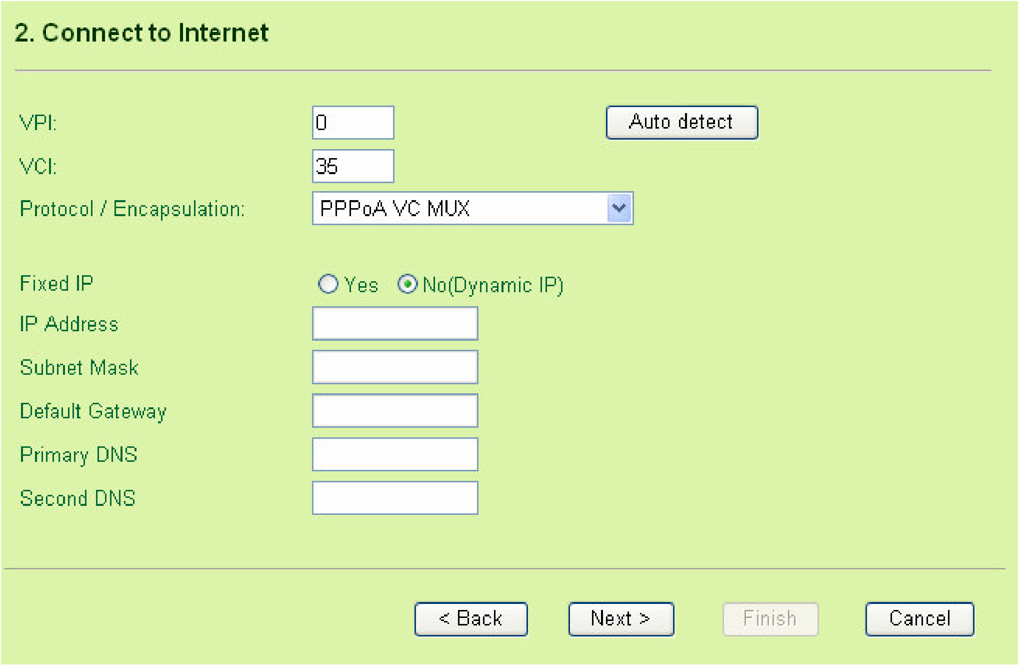
1. Enter login password

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

Confirm Password

Step 4 Select the value of connecting to your subscribed ISP.
Note: If your router is provided by your ISP, you might not be able to allow change any settings to switch to another ISP. You shall check your contract clauses requested by your ISP before you would like to change settings or select new ISP.



VPI: 0

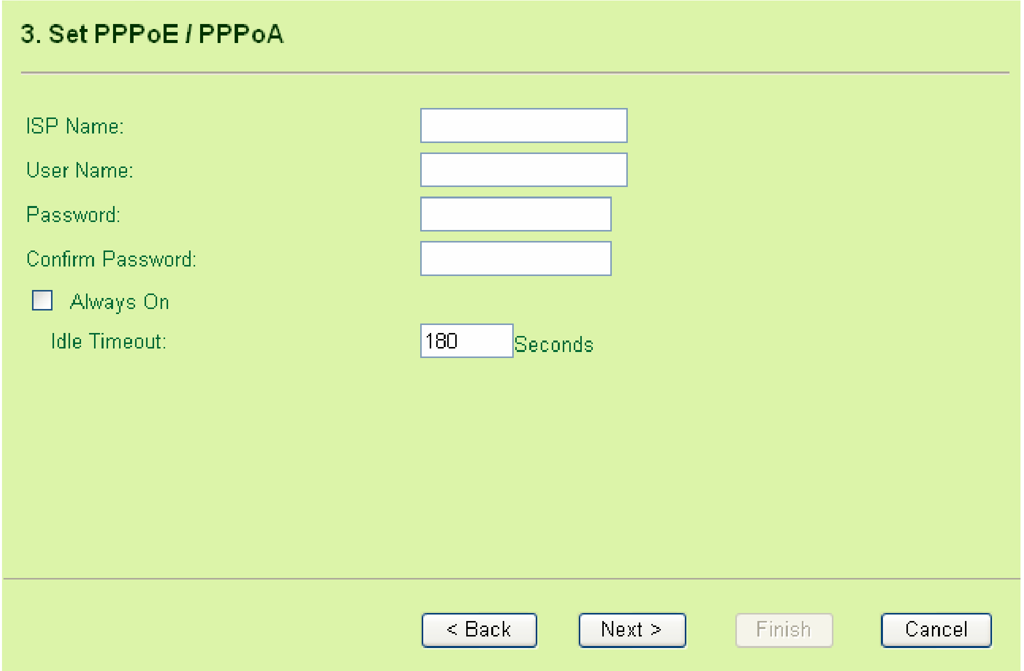
VCI: 35

Protocol / Encapsulation: PPPoA VC MUX

Fixed IP ○ Yes ● No(Dynamic IP)

Enter the IP address information originally provided by your ISP if you obtained fixed IP from your ISP.

Step 5 The router will connect into your ISP "on demand". Demand is determined as being when any LAN user tries 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** " is determined by there being no Internet traffic for a period, for example 10 minutes. You can select 0 (zero) for no timeout-the router stays connected once the router logs in. You can also select -1 (minus one) which selects "**Always On**"—the router will try to keep a permanent connection. The 0 and -1 settings are only recommended for AO (always on) connections such as ADSL. You can also simply click "**Always On**".



3. Set PPPoE / PPPoA

ISP Name:

User Name:

Password:

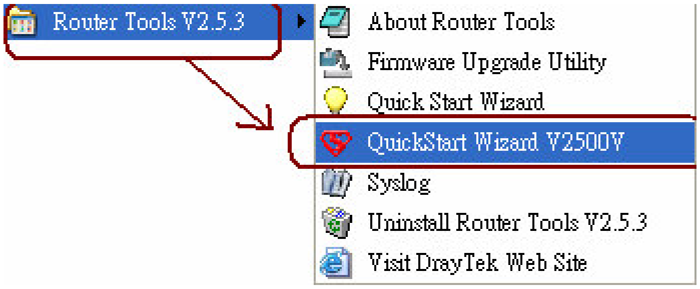
Confirm Password:

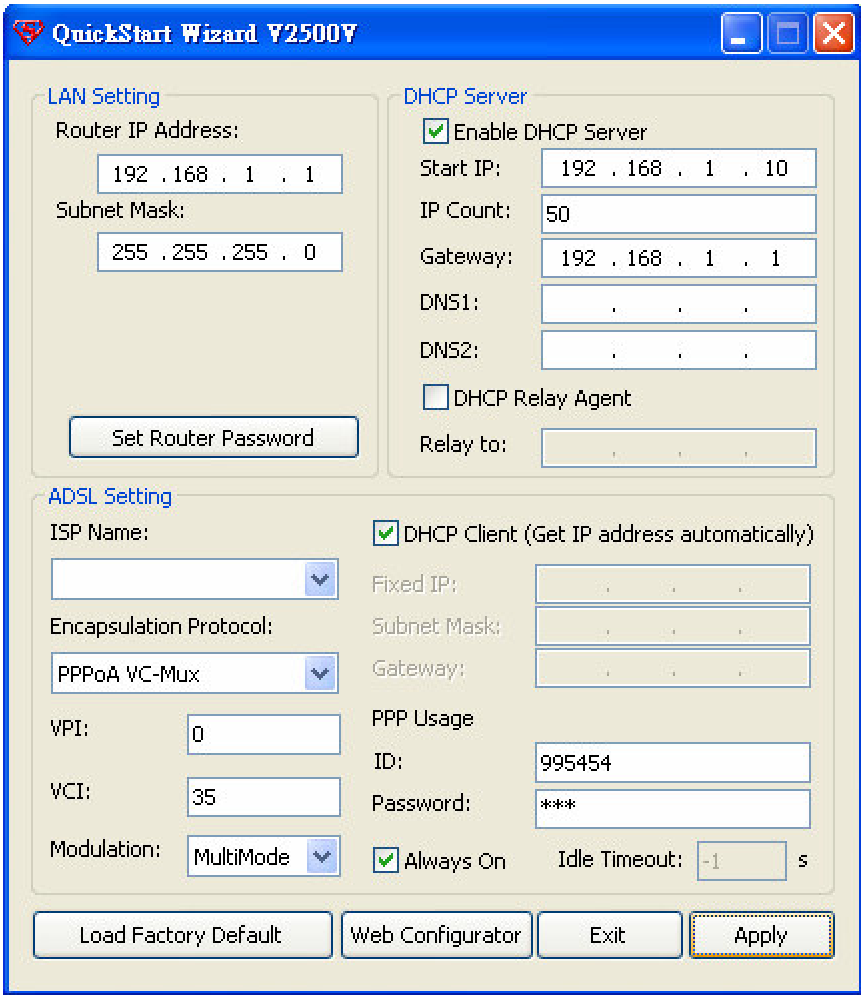
☐ Always On

Idle Timeout: 180 Seconds

Because we also have the Quick Start Wizard on the router CD, you will not need to get Quick Start Wizard from the CD after you already followed the previous procedure and get on the Internet access.

If you do not want to follow previous procedure, you still can use Quick Start Wizard from the router CD. You shall firstly get into the router tool and install the Quick Start Wizard:





Router IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255 . 255 . 255 . 0

☑ Enable DHCP Server
Start IP: 192 . 168 . 1 . 10
IP Count: 50
Gateway: 192 . 168 . 1 . 1
DNS1: . . .
DNS2: . . .
☐ DHCP Relay Agent
Relay to: . . .

ISP Name:
Encapsulation Protocol: PPPoA VC-Mux
VPI: 0
VCI: 35
Modulation: MultiMode

☑ DHCP Client (Get IP address automatically)
Fixed IP: . . .
Subnet Mask: . . .
Gateway: . . .
PPP Usage
ID: 995454
Password: ***
☑ Always On
Idle Timeout: -1 s

Once you select the ADSL setting, the Quick Start Wizard will help you detect Encapsulation protocol, VPI/VCI and Modulation. After the necessary information is set to entries, you click **Apply** and you will be able to get Internet access very easily. You will read "**Router is now configured**"!

Our Vigor2500V firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor2500V also equips 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.

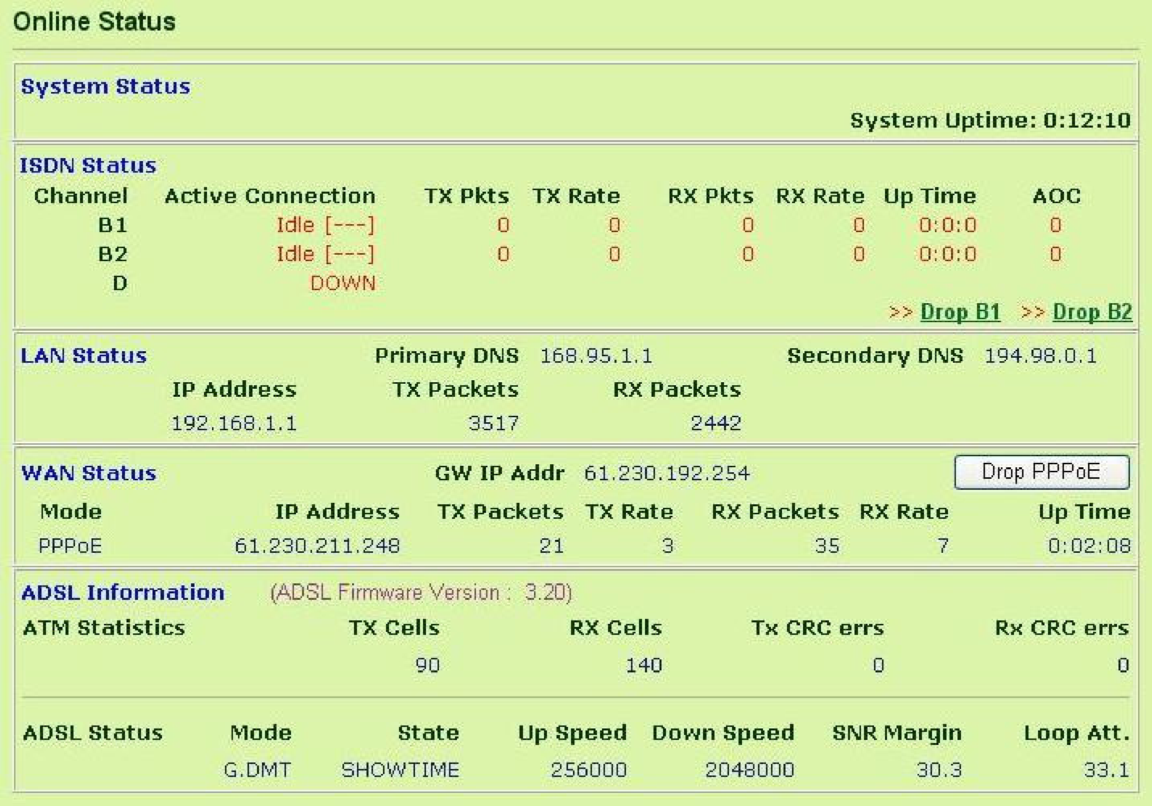
Chapter 2
Online Status

2.1 Introduction

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

2.2 Online Status Descriptions

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: 0:12:10

ISDN Status

Channel	Active Connection	TX Pkts	TX Rate	RX Pkts	RX Rate	Up Time	AOC
B1	Idle [---]	0	0	0	0	0:0:0	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	DOWN						

LAN Status

Primary DNS 168.95.1.1
Secondary DNS 194.98.0.1

IP Address	TX Packets	RX Packets
192.168.1.1	3517	2442

WAN Status

GW IP Addr 61.230.192.254

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.211.248	21	3	35	7	0:02:08

ADSL Information (ADSL Firmware Version : 3.20)

ATM Statistics	TX Cells	RX Cells	Tx CRC errs	Rx CRC errs
	90	140	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	30.3	33.1

One may find that the Online Status page contains three basic subgroups. That is, System Status, LAN Status, WAN Status, and ADSL Information. However, for the ISDN model, the Online Status page also displays the status of ISDN connection.

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.

2.2.3 WAN Status

Mode: Indicate which ADSL access mode is active. Depending upon the ADSL access mode, you may see **PPPoE, PPPoA, or MPoA.**

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 PPPoE or PPPoA: Click the link to disconnect the PPPoE or PPPoA connection.

2.2.4 ISDN Status (for ISDN model only)

Active Connection: The ISP, active remote ISDN dial-in user, or LAN-to-LAN connection name and also the IP address for each B channel.

TX Pkts: Total number of transmitted IP packets during this connection session.

TX Rate: Transmission rate in characters per second (cps) for outgoing data.

RX Pkts: 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 represent hours, minutes, and seconds, respectively.

Drop B1: Click to disconnect the B1 channel.

Drop B2: Click to disconnect the B2 channel.

2.2.5 ADSL Information

The router's online status screen (as well as the telnet logs) show you two figures which relate to the level and quality of ADSL line signal.

A good ADSL signal is more reliable and generates less errors. When you order your ADSL line, your telephon company or ISP will assure your ADSL connection is working.

ADSL Firmware Version: Indicates the ADSL modem chipset firmware (it is different from router firmware).

ATM Statistics:

TX Blocks: Total number of transmitted ATM Blocks.

RX Blocks: Total number of received ATM Blocks.

Corrected Blocks: Total number of received ATM Blocks which is corrupted but corrected.

Uncorrected Blocks: Total number of received ATM Blocks which is corrupted but uncorrected

ADSL Status:

Mode: Indicate which modulation mode is used: G.DMT, G.Lite, or T1.413.

State: Indicate the DSL line status.

Up Speed: Indicate Up Stream Speed (bits/ second).

Down Speed: Indicate Down Stream Speed (bits/ second).

SNR Margin: Indicate Signal Noise Ratio Margin (dB). The higher value has better signal quality.

Loop Att. : Indicate subscribed Loop Attenuation.

Chapter 3
Internet Access

3.1 Introduction

For most users, Internet access is the primary application. The Vigor2500V series supports the ADSL WAN interface for Internet access and remote access. The following sections will explain more detailed ADSL access setup. When you click **Internet Access Setup**, you can configure the router to access the Internet with different modes (e.g. PPPoE, PPPoA and MPoA)

The following is the setting path for this function.

Internet Access Setup > **PPPoE / PPPoA**
> **MPoA (RFC 1483 / 2684)**
> **Multi-PVCs**

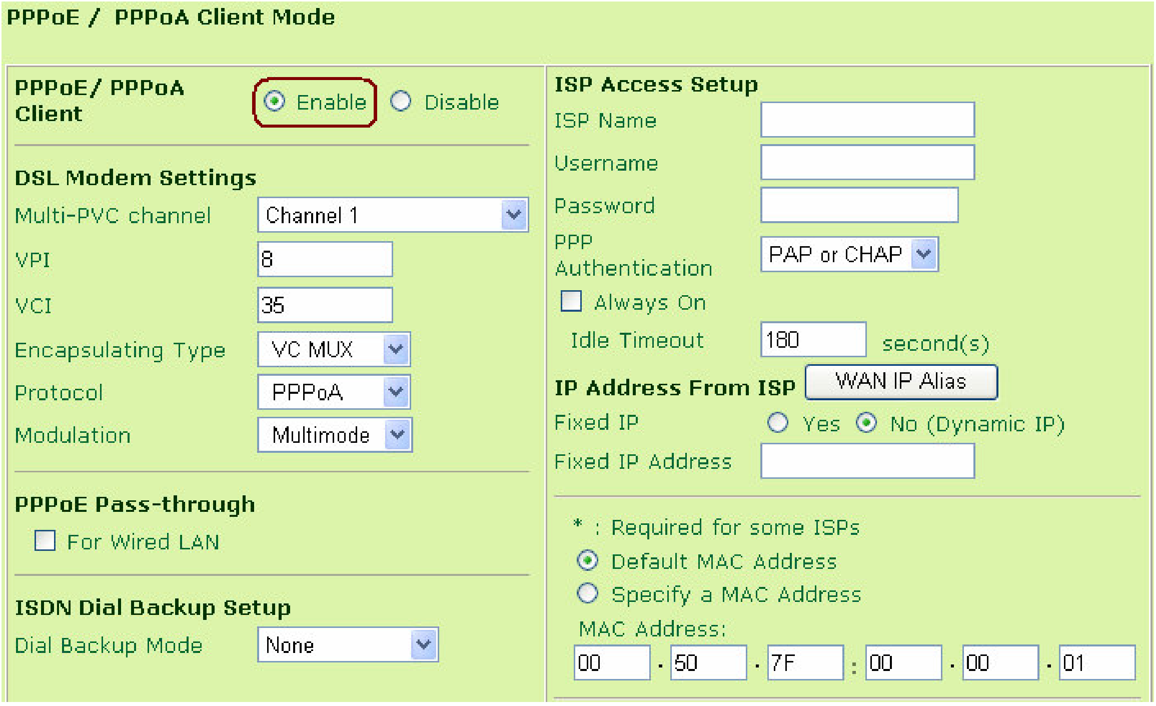
For ADSL access users, you need to know what kind of internet access is provided by your ISP. The PPPoE / PPPoA and MPoA (RFC 1483 / 2684) are mutually exclusive.

Note: We recommend you to consult with your dealer or ISP before you would like to run Multi-PVC. In most cases, you do not need to activate any settings on the menu of multi-PVC because our MultiPVC is currently with framework for ISP or Telco to integrate its detailed infrastructure.

3.2 Configuration

3.2.1 For PPPoE/PPPoA Users

Enter your allocated username, password and DSL parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check '**Always On**'.



PPPoE / PPPoA Client Mode

PPPoE/ PPPoA Client ● Enable ○ Disable

DSL Modem Settings

Multi-PVC channel: Channel 1
VPI: 8
VCI: 35
Encapsulating Type: VC MUX
Protocol: PPPoA
Modulation: Multimode

PPPoE Pass-through

☐ For Wired LAN

ISDN Dial Backup Setup

Dial Backup Mode: None

ISP Access Setup

ISP Name:
Username:
Password:
PPP Authentication: PAP or CHAP
☐ Always On
Idle Timeout: 180 second(s)

IP Address From ISP

Fixed IP ○ Yes ● No (Dynamic IP)
Fixed IP Address:

* : Required for some ISPs
● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 . 50 . 7F : 00 . 00 . 01

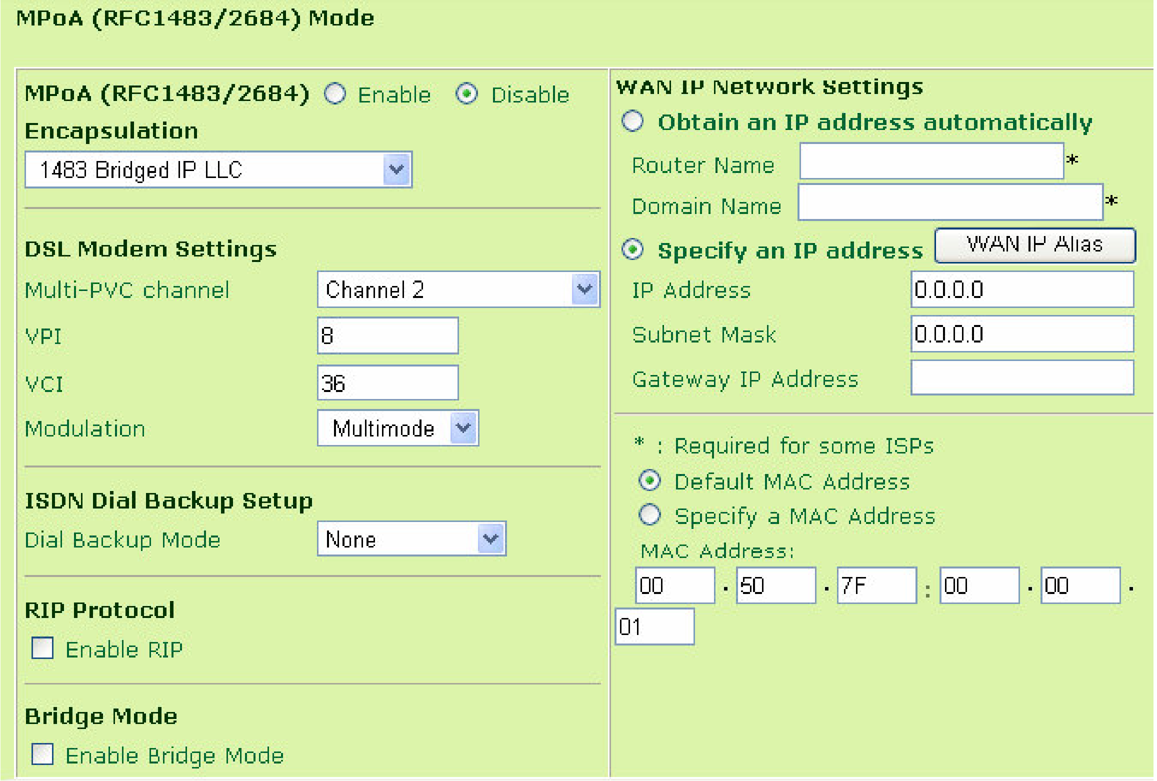
PPPoE Pass-through

The Vigor router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router.

For Wired LAN: Check this checkbox. The PPPoE connection from local clients to the ISP goes straight through wired LAN.

3.2.2 For MPoA (RFC 1483/2684) Users

Enter your allocated WAN IP address (or enabling DHCP client to get IP from ISP) and DSL parameters according to the information provided by your ISP.



MPoA (RFC1483/2684) Mode

MPoA (RFC1483/2684) ○ Enable ● Disable

Encapsulation
1483 Bridged IP LLC

DSL Modem Settings
Multi-PVC channel: Channel 2
VPI: 8
VCI: 36
Modulation: Multimode

ISDN Dial Backup Setup
Dial Backup Mode: None

RIP Protocol
☐ Enable RIP

Bridge Mode
☐ Enable Bridge Mode

WAN IP Network Settings
○ **Obtain an IP address automatically**
Router Name: *
Domain Name: *
● **Specify an IP address**
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway IP Address:

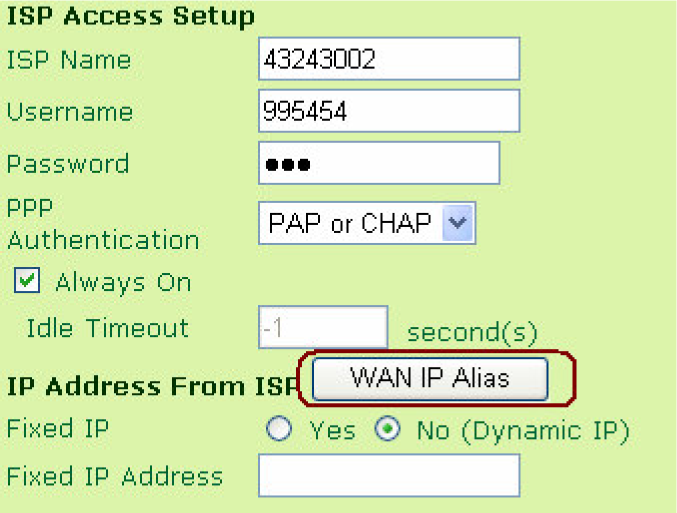
* : Required for some ISPs
● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 - 50 - 7F : 00 - 00 - 01

RIP Protocol

Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information.

Enable RIP：Check this checkbox. The router periodically exchanges entire routing tables.

If you have multiple public IPs, they are assigned from the WAN interface. Click WAN IP Alias, the following windows will be pop-up. You can assign additional IPs on the page, and click OK.



ISP Access Setup

ISP Name	43243002
Username	995454
Password	●●●
PPP Authentication	PAP or CHAP

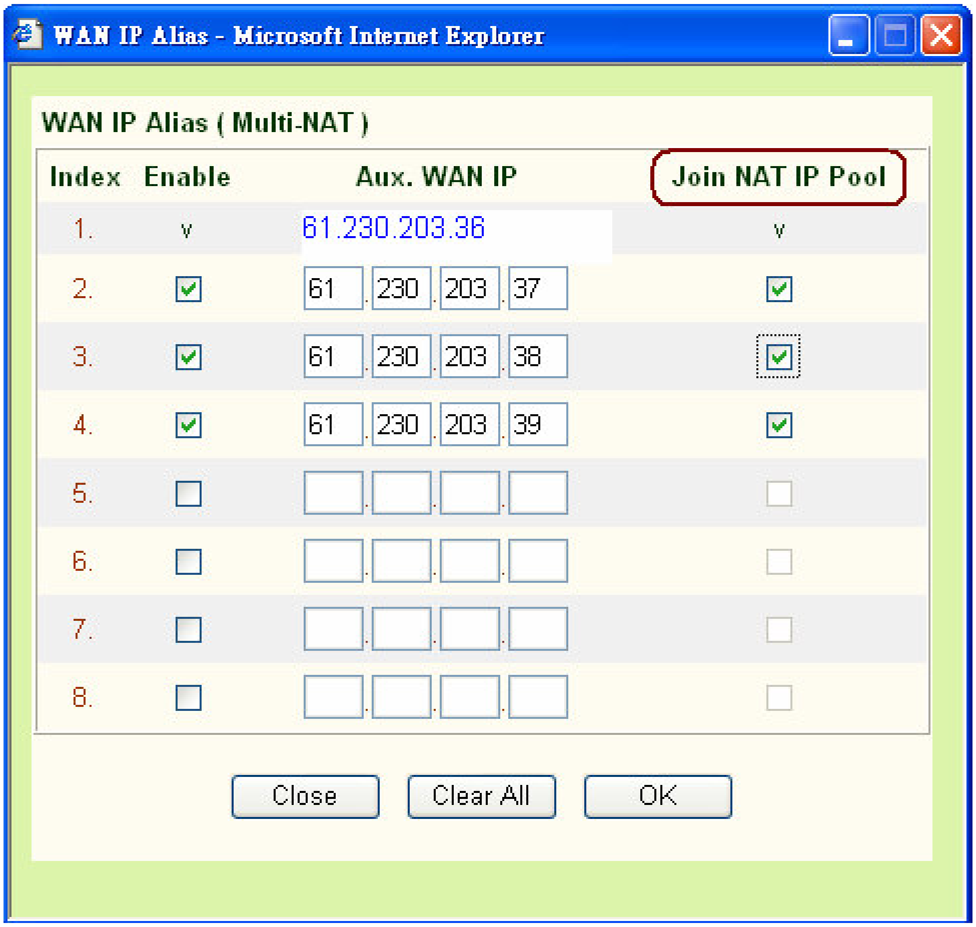
☑ Always On

Idle Timeout -1 second(s)

IP Address From ISP

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address



WAN IP Alias (Multi-NAT)

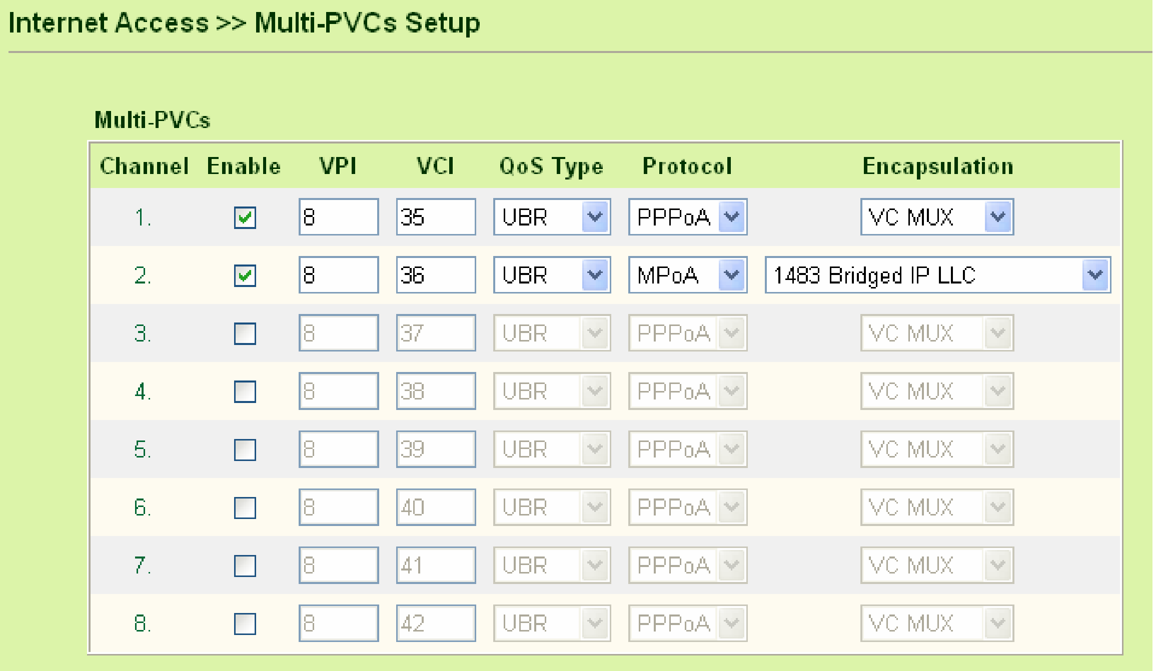
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	61.230.203.36	v
2.	☑	61 . 230 . 203 . 37	☑
3.	☑	61 . 230 . 203 . 38	☑
4.	☑	61 . 230 . 203 . 39	☑
5.	☐	. . .	☐
6.	☐	. . .	☐
7.	☐	. . .	☐
8.	☐	. . .	☐

3.2.3 Multi-PVCs

The MultiPVCs are related to the services and management policy of ISP or Telco. In most countries, **the MultiPVC is designed for remote management in order to save the labour of technical support of ISP or Telco.**

Enter your allocated DSL parameters according to the information provided by your ISP. QoS Type means QoS offered by ATM, default UBR is recommend.

We recommend you to consult with your dealer or ISP before you would like to run Multi-PVC. In most cases, you do not need to activate any settings on the menu of multi-PVC because our MultiPVC is currently with framework for ISP or Telco to integrate its detailed infrastructure.



Internet Access >> Multi-PVCs Setup

Multi-PVCs

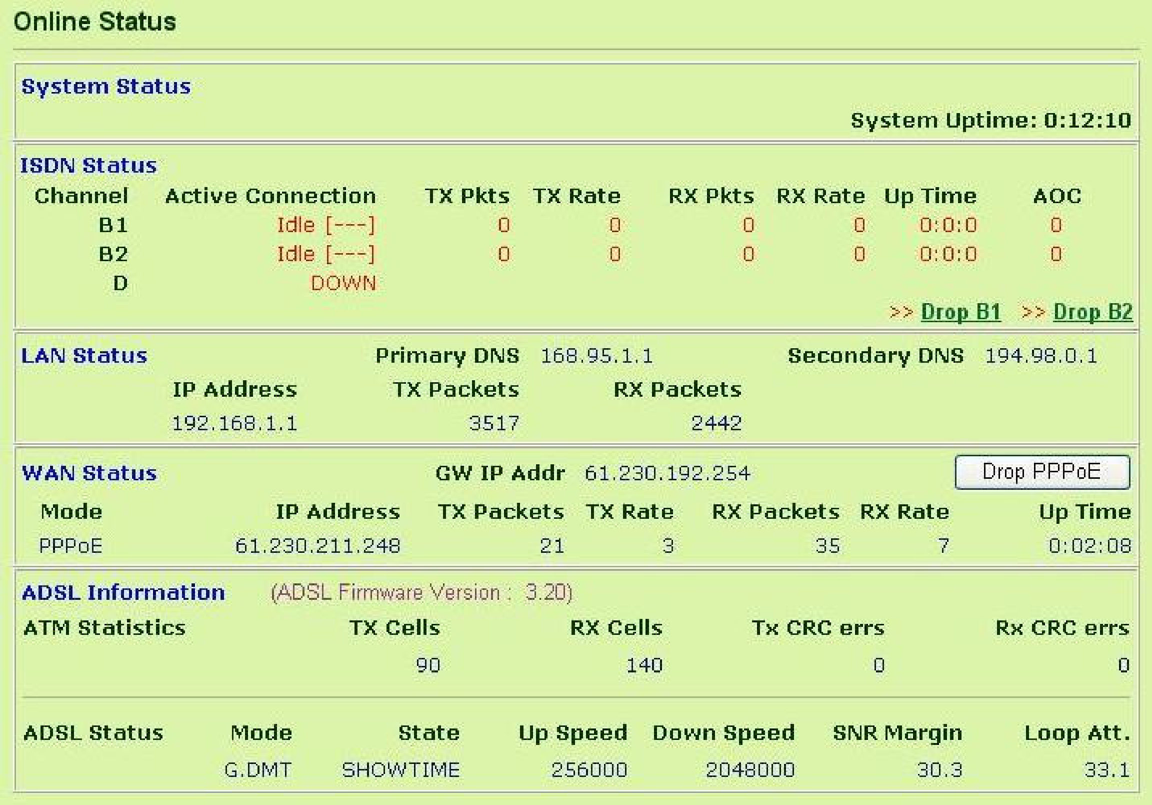
Channel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.	☑	8	35	UBR	PPPoA	VC MUX
2.	☑	8	36	UBR	MPoA	1483 Bridged IP LLC
3.	☐	8	37	UBR	PPPoA	VC MUX
4.	☐	8	38	UBR	PPPoA	VC MUX
5.	☐	8	39	UBR	PPPoA	VC MUX
6.	☐	8	40	UBR	PPPoA	VC MUX
7.	☐	8	41	UBR	PPPoA	VC MUX
8.	☐	8	42	UBR	PPPoA	VC MUX

Detect ATM/ DSL Setting from Quick Start Wizard

You can also be guided by **Quick Start Wizard** to detect ATM/ DSL setting. Please follow the instructions to operate. If your country is not on the list, it may take longer time to detect.

Internet Statistics

You can know the DSL status via status monitor.



Online Status

System Status

System Uptime: 0:12:10

ISDN Status

Channel	Active Connection	TX Pkts	TX Rate	RX Pkts	RX Rate	Up Time	AOC
B1	Idle [---]	0	0	0	0	0:0:0	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	DOWN						

LAN Status

Primary DNS 168.95.1.1

Secondary DNS 194.98.0.1

IP Address	TX Packets	RX Packets
192.168.1.1	3517	2442

WAN Status

GW IP Addr 61.230.192.254

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.211.248	21	3	35	7	0:02:08

ADSL Information (ADSL Firmware Version : 3.20)

ATM Statistics	TX Cells	RX Cells	Tx CRC errs	Rx CRC errs
	90	140	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	30.3	33.1

Chapter 4
LAN TCP/IP and DHCP

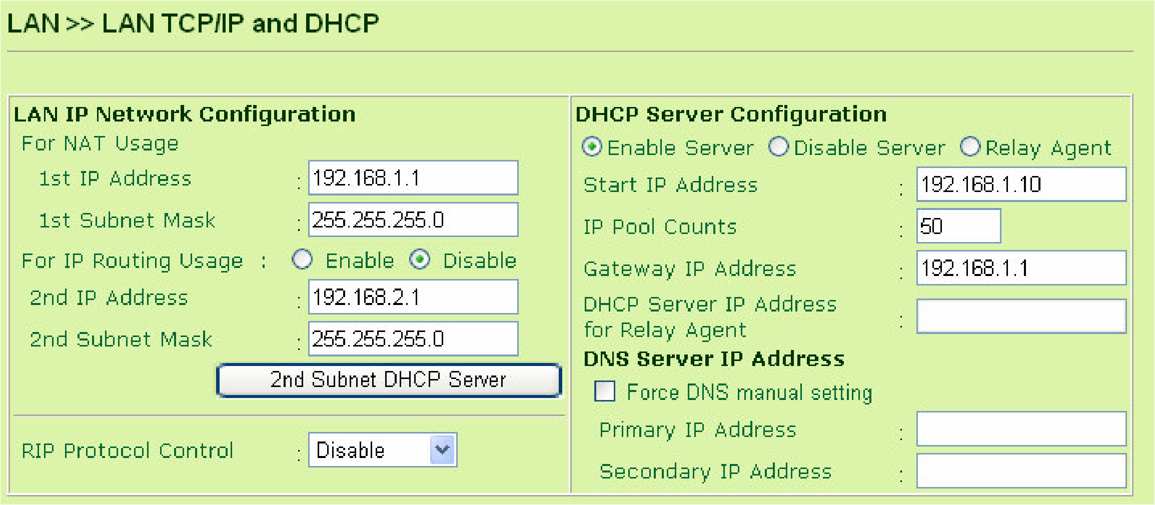
4.1 LAN IP Network Configuration

In the Vigor router, there are two sets of IP address settings for the LAN interface, as shown below. The 1st IP address/subnet mask is for private users or NAT users, and the 2nd IP address/subnet mask is for public users. To allow public users, you need to have subscribed to a globally reachable subnet from your ISP.

For example, for some DSL accounts, the ISP will assign a few public IP addresses for your local network. You could use one IP address for your router, and the 2nd IP address/subnet mask should be configured with the public IP address. Other local PCs should set the router IP address as the default gateway. When the DSL connection to the ISP has been established, each local PC will directly route to the Internet. Also, you could use the 1st IP address/subnet mask to connect to other private users (PCs). These IP addresses of the users will be translated to the 2nd IP address by the router and sent out via the DSL connection.

The following is the setting path for this function.

Internet Access Setup > **LAN TCP/IP and DHCP**



LAN >> LAN TCP/IP and DHCP

LAN IP Network Configuration

For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage : ○ Enable ● Disable

2nd IP Address : 192.168.2.1

2nd Subnet Mask : 255.255.255.0

RIP Protocol Control : Disable

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

☐ Force DNS manual setting

Primary IP Address :

Secondary IP Address :

For NAT Usage: (Default: Always Enable)

***1st IP Address*:** Private IP address for connecting to a local private network (Default: 192.168.1.1).

***1st Subnet Mask*:** Subnet mask for the local private network (Default: 255.255.255.0/ 24).

For IP Routing Usage: (Default: Disable)

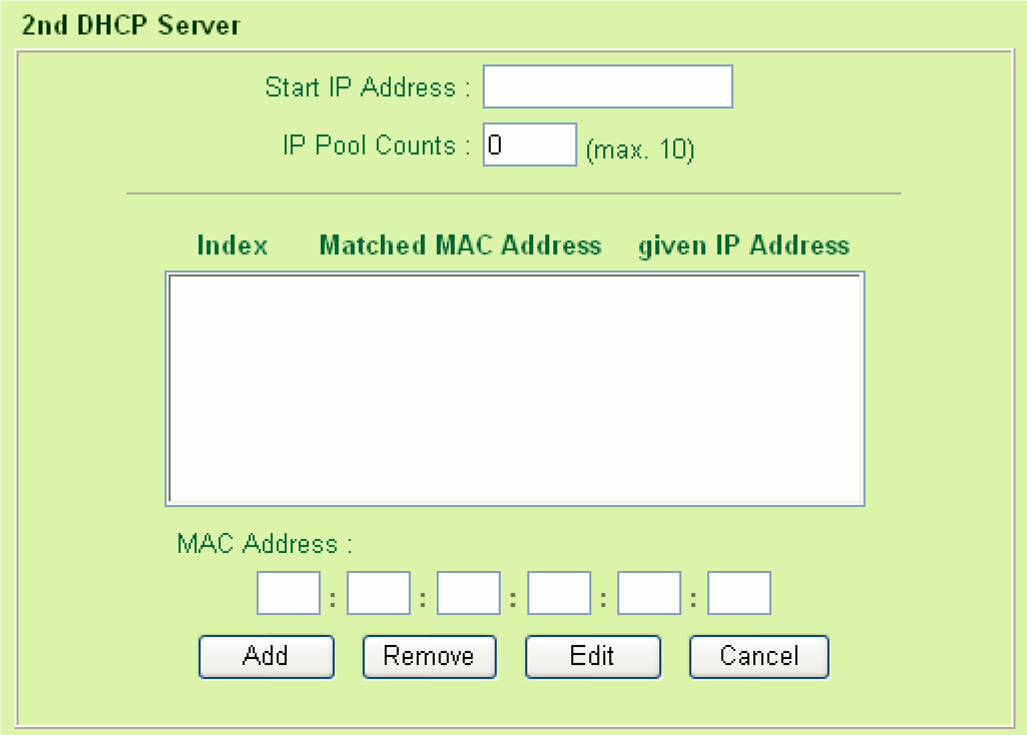
***Enable*:** Enable the 2nd IP address settings.

***Disable*:** Disable the 2nd IP address settings.

***2nd IP Address*:** Set a public IP address.

***2nd Subnet Mask*:** Set a subnet mask for the public IP address.

2nd Subnet DHCP Server: The following picture is for 2nd subnet DHCP Server of the Vigor Router.



2nd DHCP Server

Start IP Address :

IP Pool Counts : 0 (max. 10)

Index	Matched MAC Address	given IP Address

MAC Address : _ : _ : _ : _ : _ : _

***Start IP Address**:* Set the starting IP address of the IP address pool.

***IP Pool Counts**:* Set the number of IP addresses in the pool.

***MAC Address**:* Type the specific MAC Address that could be added, removed or edited on the access list.

- ***ADD**:* To add a MAC address on the list.
- ***Remove**:* To delete the selected MAC address on the list.
- ***Edit**:* To edit the selected MAC address on the list.
- ***Cancel**:* Give up the MAC address access control setup.

***Close**:* Close this window.

***Clear All**:* Clean all entries of MAC addresses on the list.

***OK**:* Save the access control list.

RIP Protocol Control:

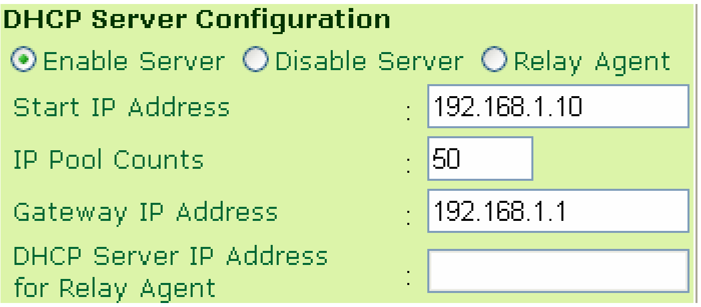
Disable**:** Disable the exchange of RIP packets on LAN interface.

1st Subnet**:** Set the 1st subnet to exchange RIP packets with neighbor routers connected to LAN interface.

2nd Subnet: Set the 2nd subnet to exchange RIP packets with neighbor routers connected to LAN interface.

4.2 DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. It can automatically dispatch related IP settings to any local user configured as a DHCP client. 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 :

Enable Server: Assign IP address to LAN PC automatically.

Disable Server: Assign IP address to LAN PC manually.

Relay Agent: Allows PCs on LAN to request IP address from other DHCP server.

Start IP Address: Set the start IP address of the IP address pool.

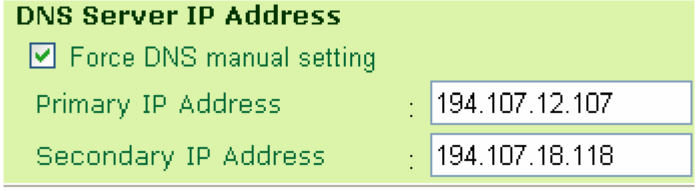
IP Pool Counts: Set the number of IP address pool.

Gateway IP Address: Sets the gateway IP address for the DHCP server. Usually, it should be same as 1st IP address when the router works as a default gateway.

4.3 How you operate DNS on the Vigor router?

The Internet traffic travels between two points addresses by their numeric IP address. To make the Internet friendly, we are more accustomed to using names rather than numbers (e.g. www.draytek.com) but those names often need to be converted back into their real numeric address for the data to be sent; this is known as "name resolution". A DNS server proceed this conversion for us so all users on the LAN need to know about a DNS server in order to resolve addresses.

Your PC will be told of the DNS server to use if your PC is getting its own IP address automatically from the router (using **DHCP**). The router will pre-set DNS servers initially, but the ISP will allocate their own DNS servers which are then used once the router has connected to the ISP. As a result, you can over-ride all DNS server settings and force your own by entering them into the DNS fields on the LAN setup menu



☑ Force DNS manual setting

Primary IP Address : 194.107.12.107

Secondary IP Address : 194.107.18.118

Primary IP Address: Sets the IP address of the primary DNS server.

Secondary IP Address: Sets the IP address of the secondary DNS server.

Your ISP allocates its own DNS servers when the router logs into the ISP. These DNS servers will then over-ride the manual settings. If you still want to force the manual settings to apply, you can use telnet command " **srv dhcp frcdnsmanl on**" (use "**off**" to disable it. Requires firmware version 2.5.6 or later)

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 (Network Address Translation)

5.1 Introduction

NAT (Network Address Translation) provides you with a method of mapping one or more IP addresses and/or service ports into different specified applications. The Vigor router takes a single public IP address, allocated by your ISP and automatically forwards data between the Vigor router and the local computer or laptop on your local network. For the outside world, the public IP address of the router is visible by external users. However, the external users cannot address the internal private IP address of every computer / laptop. Any “unsolicited” TCP/IP packet to your public IP address will arrive at your router but the router can not send the packet to any computer or laptop on the LAN. The NAT plays an important guard for your network clients because the internal private IP address of every computer or laptop is hidden from the outside world, unless you open up ports/protocols to allow contact.

Through a single public IP address, several computers of your internal local network can share the broadband access of an ADSL line. For cost concern, you do not need to subscribe more than one public IP address for every computer or laptop because the NAT facility of Vigor router can transform a single public IP address to many internal private IP addresses.

5.2 NAT Setup

In the most common type of router installation, you use the NAT facility of the router. The NAT-enabled router gets one (in Single ISP, PPPoE, PPPoA, MPoA) globally re-routable IP addresses from the ISP and assigns private network IP addresses defined by RFC-1918 to local hosts. The NAT-enable router translates the private network addresses to such a globally routable IP address so that local hosts can communicate with the router and access the Internet. The Vigor router let you have three types of port mapping as follows:

Port Redirection
DMZ Host
Open Ports

In terms of the definition of RFC1918 for the private IP addresses, the users apply the 192.168.1.0/24 to local network clients. e.g. you have three computers located at different room and you assign three private addresses to these three computers. You can access Internet from these three computers because Vigor router can transform these three private IP addresses to a single public IP address which you subscribed from your ISP.

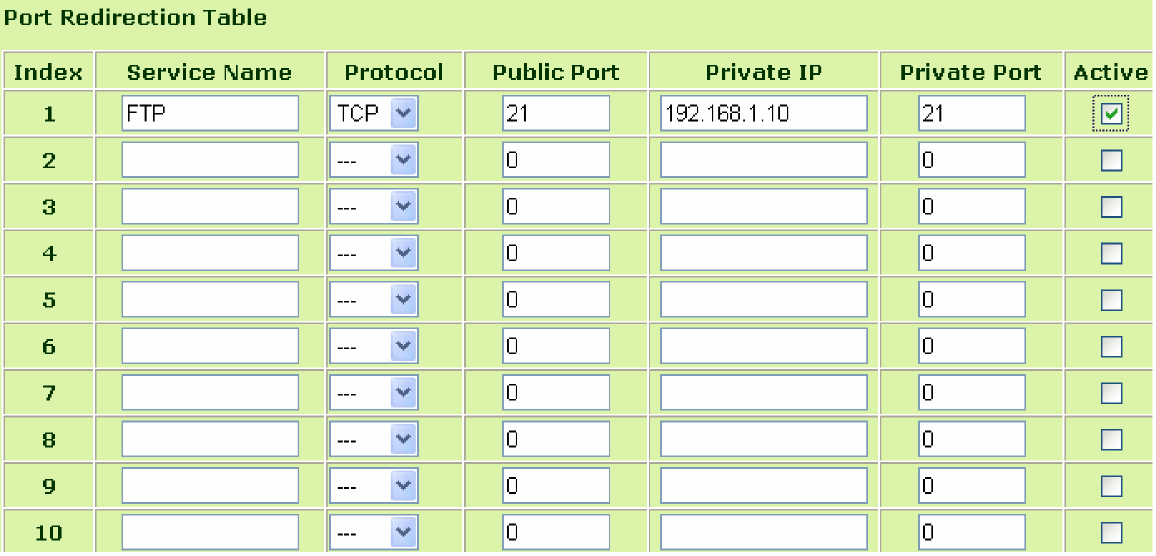
The following is the setting path for this function.

NAT > **Port Redirection**
> **DMZ Host**
> **Open Ports**
> **Well-Known Ports List**

5.3 Configure 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.

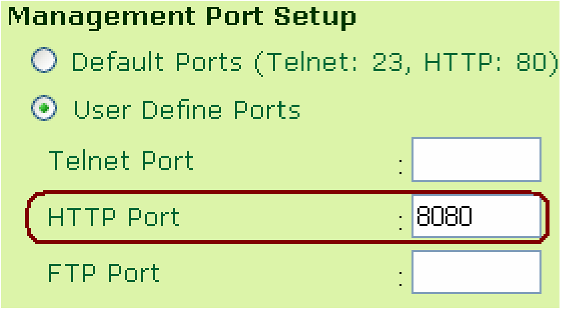
Private IP: Specify the private IP address of the internal host offering the service.

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

Active: Check here to activate the port-mapping entry.

Click **OK**

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**



Management Port Setup

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

● User Define Ports

Telnet Port :

HTTP Port : 8080

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.

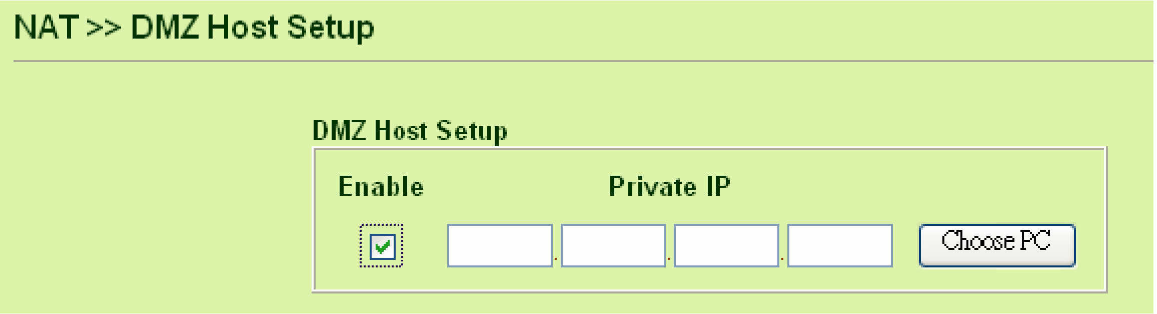
5.4 DMZ Host Setup

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 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. You can consider adding additional filter rules or a secondary firewall.

There are some non-NAT-friendly protocols although a DMZ will pass all data. The “AH” extension to IPSec is designed in such principle. It prevents NAT – the header encodes the source IP address, which in this case would be your private IP address. The receiving end will see the packet as having come from your public IP address and thus reject the packet. AH protocol therefore will not work. ESP is more tolerant.

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-IP-Protocol applications such as Netmeeting or Internet Games etc. Each item in the setup page is described below.



NAT >> DMZ Host Setup

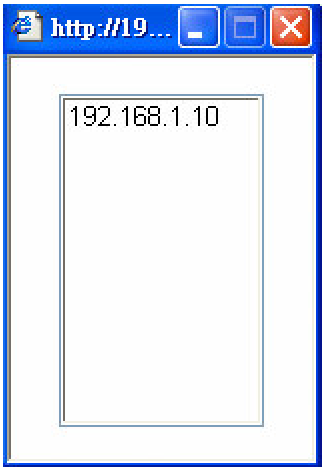
DMZ Host Setup

Enable	Private IP
☑	___ . ___ . ___ . ___

Enable: Check to enable the DMZ Host function.

Private IP: Enter the private IP address of the DMZ host.

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

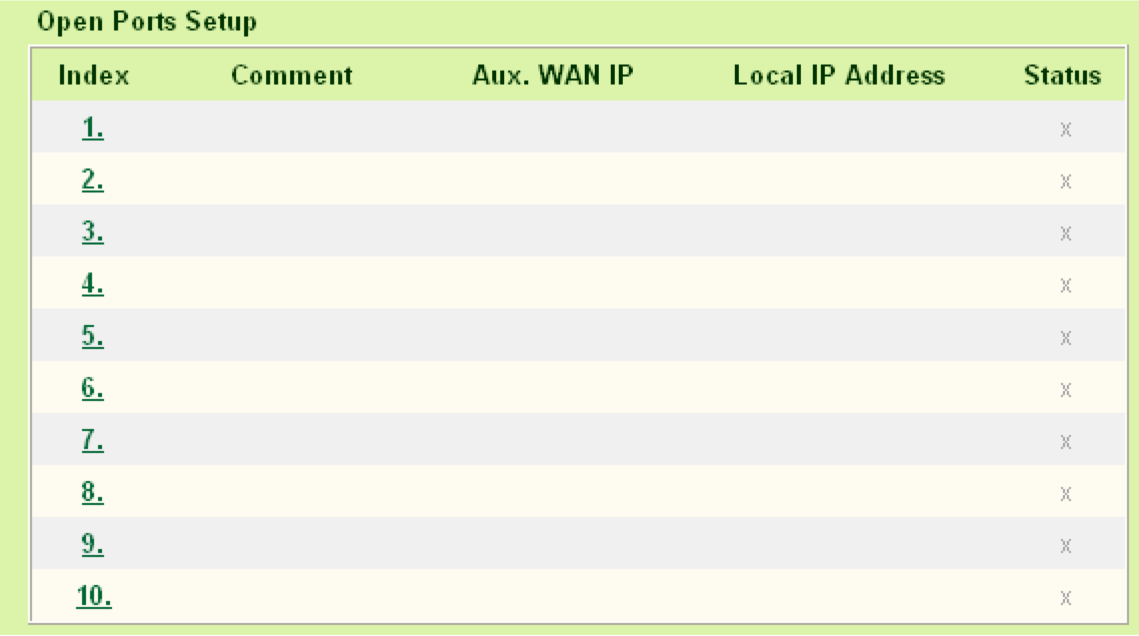


192.168.1.10

5.5 Open Port Setup

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.



Open Ports Setup

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

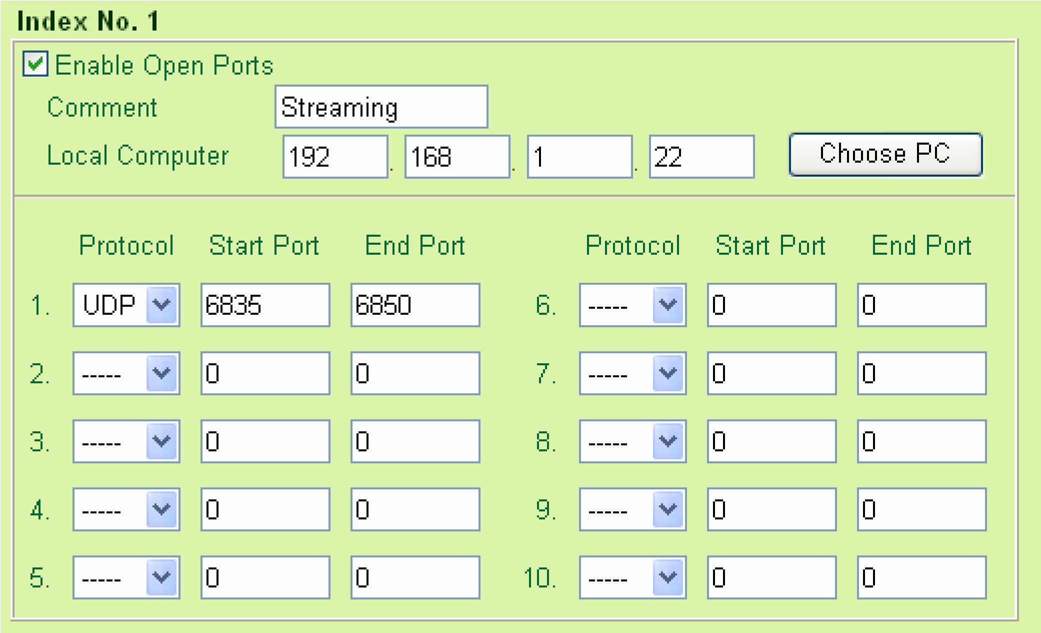
Index: Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

Comment: Display the name for the specified 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 varied services. The computer with private IP address of 192.168.1.22 will be the host for the specified incoming packet of named as “streaming”. Following example, the UDP port ranges from 6835 to 6850.



Index No. 1

☑ Enable Open Ports

Comment: Streaming

Local Computer: 192 . 168 . 1 . 22

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	UDP	6835	6850	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.

5.6 The Precedence of three variants of port mapping

The Vigor router supports three variants of port mapping methods: Port Redirection, Open Ports and DMZ.

Port Redirection –The incoming packet is redirected to a specific local computer or laptop if the port number matches that defined. You can forward the port to another port locally.

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

DMZ Host – This opens up a single computer or laptop completely. All incoming packets will be forwarded onto the PC with the local IP address you specified. The only exceptions are packets received in response to outgoing requests form other local PCs or incoming packets which match rules in the other two methods.

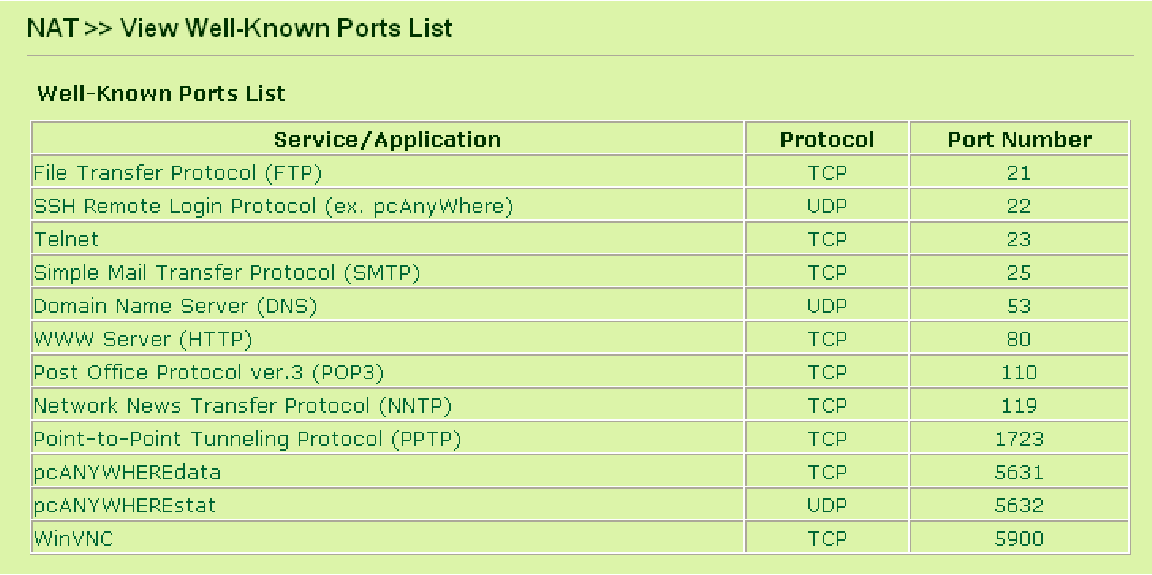
While you are using combinations of these three systems, there is a priority structure. **The precedence of these three types of port mapping is defined as follows:**

Port Redirection > Open Ports > DMZ

For example: The packet will be forwarded to the local address defined in **Port Redirection** if the port number of an incoming packet matches a rule specified in both **Port Redirection and Open Ports.**

5.7 Well-known Port Number List

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



NAT >> View Well-Known Ports List

Well-Known Ports List

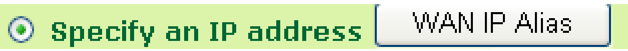
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer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

5.8 Multi-NAT Setup

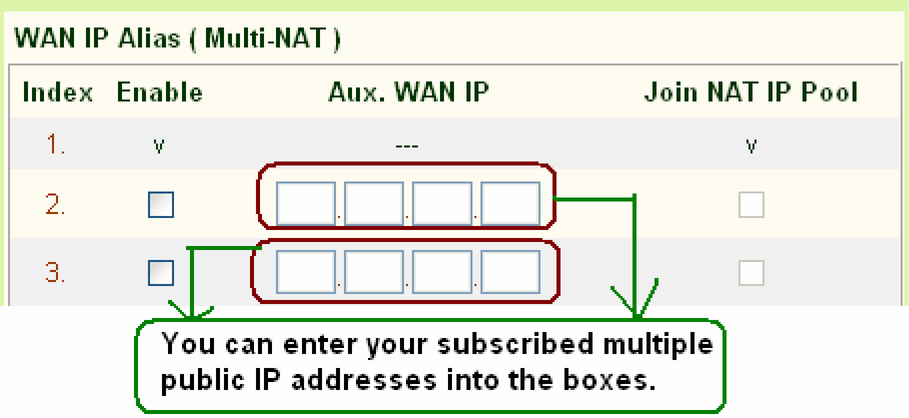
The NAT, Network Address Translation establishes a many-to-one relationship from your private IP address to your single public IP address. In the most common type of router usage, the user uses the NAT facility of the router to utilize the broadband access. i.e. Your family members can have their own computer or laptop for Internet access but you just subscribe one public IP address. Every computer or laptop receives a private IP address from Vigor router. The NAT provides essential security to your network clients because their private address is hidden from the outside world and can not be reached directly, unless they are authorized to be contacted by opening up ports/protocols.

The MultiNAT can be deployed where your ISP offers you multiple public IP addresses by your ISP. As a result, you can have a one-to-one relationship between a public address and a private IP address. This means that you still have the security from NAT but the computer or laptop can be addressed directly from the outside world by its associated public IP address, but still by only opening specific ports to it (e.g. TCP port 80 for an http/web server).

To achieve it, you should find the path to click the button of **WAN IP Alias** which is located inside **Internet Access Setup**.



● Specify an IP address

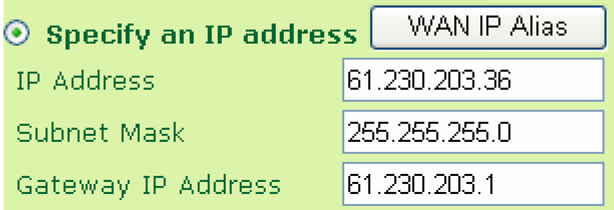


WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	---	v
2.	☐	___.___.___.___	☐
3.	☐	___.___.___.___	☐

You can enter your subscribed multiple public IP addresses into the boxes.

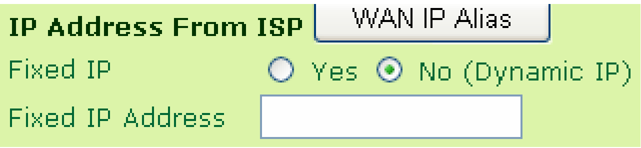
You follow the path Internet Access>>MPoA if your ISP offer you with MPoA:



● Specify an IP address

IP Address: 61.230.203.36
Subnet Mask: 255.255.255.0
Gateway IP Address: 61.230.203.1

You follow the path Internet Access>>PPPoE/PPPoA if your ISP offer you with PPPoE or PPPoA:

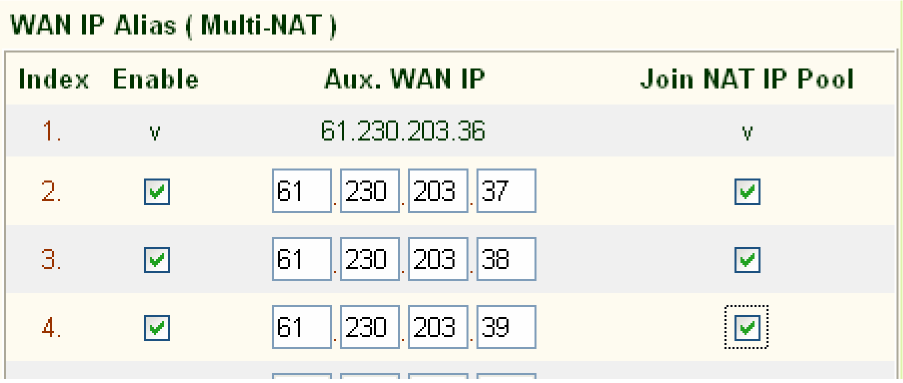


IP Address From ISP WAN IP Alias

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

When you click the **WAN IP Alias** button, it will show up a window for you to set your public IP addresses, as shown below. After set the public addresses in the appropriate boxes, you shall check **Join NAT IP Pool** to let your network client to use these public IP addresses to communicate outside world. i.e. you can specify one computer to be your web server for showing your personal data when you would like to make friends. Furthermore, you can assign another public IP addresses for your kids to participate in the distance learning over Internet.

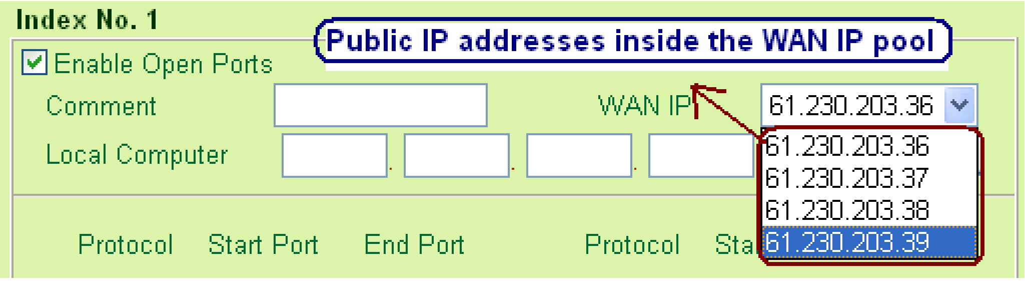


WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	61.230.203.36	v
2.	☑	61 . 230 . 203 . 37	☑
3.	☑	61 . 230 . 203 . 38	☑
4.	☑	61 . 230 . 203 . 39	☑

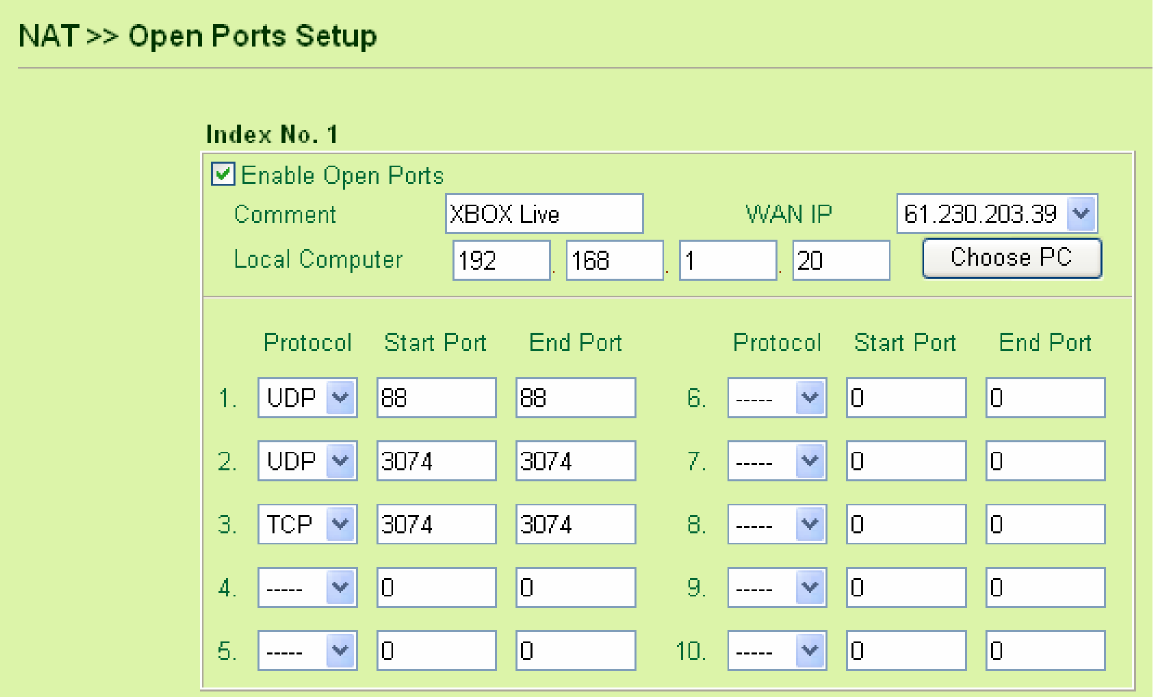
After you enter some of your public IP addresses into the **WAN IP Alias (Multi-NAT)** menu, these addresses will then be selectable on either the **NAT/Open ports** menu or the **NAT/DMZ** menu.

After the public IP addresses are kept within NAT IP pool, these public IP addresses are selectable on **NAT/Open Ports** menu. For example, you can specify one computer for XBox Live by open UDP port and TCP port:



The Vigor2500V series shall be compatible with XBox Live. If it does not work in the default configuration, you can open UDP Ports 88 and 3074 and TCP Port 3074 to redirect the Xbox's local IP address.

You select one public IP (e.g. 61.230.203.39) to the specified computer on the LAN. The specified computer is with private IP address 192.168.1.20. XBox Live will not be prevented from Vigor router after you open UDP Ports 88 and 3074, and TCP Port 3074.



NAT >> Open Ports Setup

Index No. 1

☑ Enable Open Ports

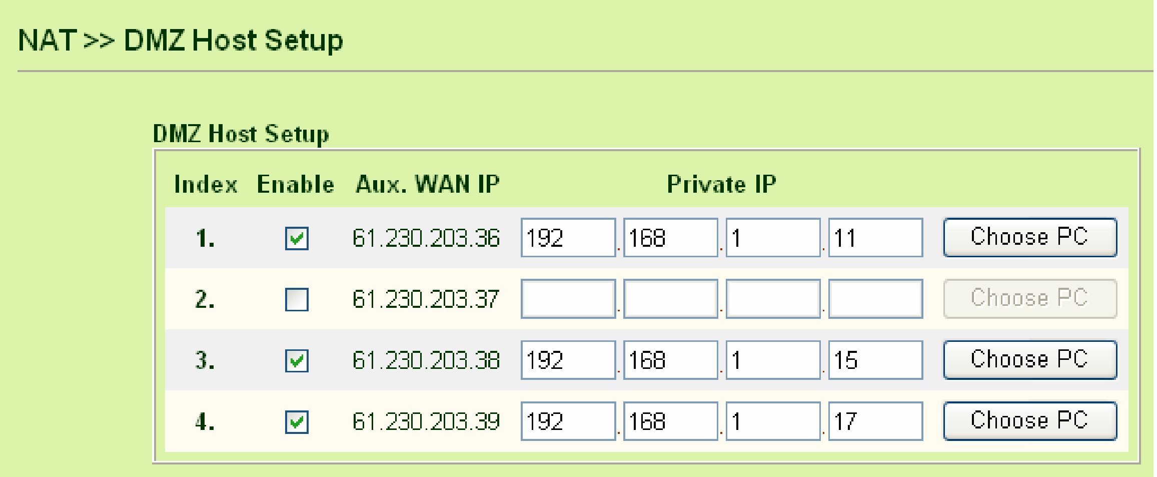
Comment: XBOX Live

WAN IP: 61.230.203.39

Local Computer: 192 . 168 . 1 . 20

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	UDP	88	88	6.	-----	0	0
2.	UDP	3074	3074	7.	-----	0	0
3.	TCP	3074	3074	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

After the public IP addresses are kept within NAT IP pool, these public IP addresses are selectable on **NAT/DMZ Ports** menu. You can specify computer on the LAN to be with public IP address and let all incoming packets be forwarded onto the PC with local IP address you set. For example, you let your PC with private IP 192.168.1.17 be able to play Netmeeting. This computer is also assigned with public IP address 61.230.203.39. The Netmeeting will not be blocked by the inherent security function of NAT.



NAT >> DMZ Host Setup

DMZ Host Setup

Index	Enable	Aux. WAN IP	Private IP				
1.	☑	61.230.203.36	192	168	1	11	Choose PC
2.	☐	61.230.203.37					Choose PC
3.	☑	61.230.203.38	192	168	1	15	Choose PC
4.	☑	61.230.203.39	192	168	1	17	Choose PC

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

The Vigor2500V series ADSL router is already equipped with the ALG's (Application Level Gateways) in order to increase the interoperability with multimedia applications for the limitation of NAT. DrayTek ALG's is already integrated with the router firmware so that you do not need to set any settings onto Vigor router.

Chapter 6
Firewall

6.1 Introduction

Security is top priority to be took into consideration as the users of ADSL broadband 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.

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

- Stateful Packet Inspection: tracks packets and denies unsolicited incoming data
- Selectable DoS/DDoS protection
- User-configurable packet filter
- NAT/PAT with Port Forwarding/Redirection & DMZ
- Supports ALGs (Application Layer Gateways)
- Virtual server via port redirection or open ports feature
- E-mail alerting mechanism

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

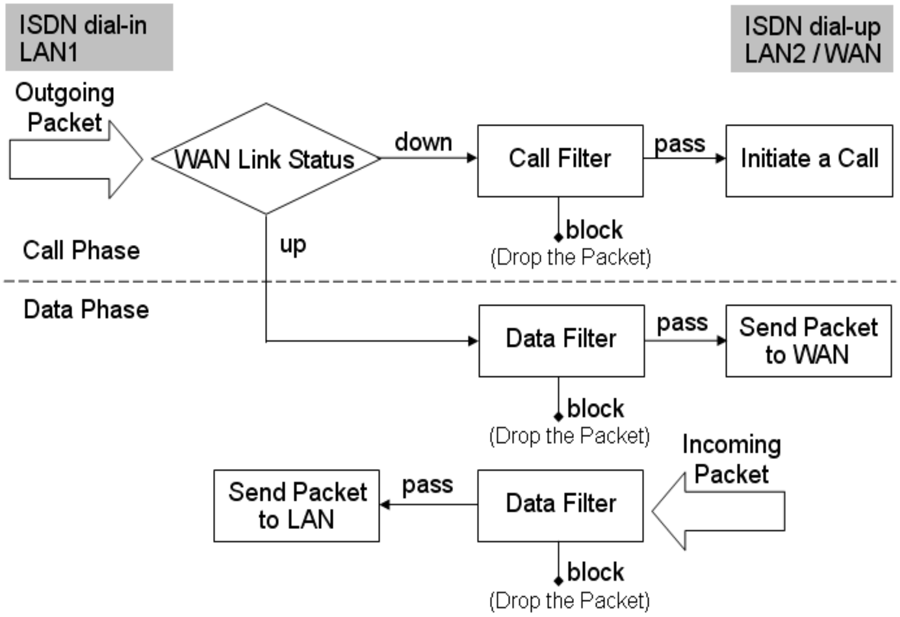
6.2 An Overview of the Firewall

The **Firewall Setup** in the Vigor router mainly consists of the packet filtering, DoS (Denial of Service) defense, and URL (Universal Resource Locator) content filtering facilities. In this chapter, we focus on the introduction of the packet filtering function. In the **Supplement A and B chapters**, we will explain more about DoS defense and URL content filtering facilities.

The packet filtering 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 more about the **General Setup** and **Filter Setup** in the **Firewall Setup** section using the Web Configurator. 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**. By default, the Call Filter rules are defined in Filter Set 1 and the Data Filter rules are defined in Filter Set 2.

The following is the setting path for this function.

Firewall > **General Setup**

> **Filter Setup**

> **DoS Defense**

> **URL Content Filter**

General Setup: Some general settings are available from this link.

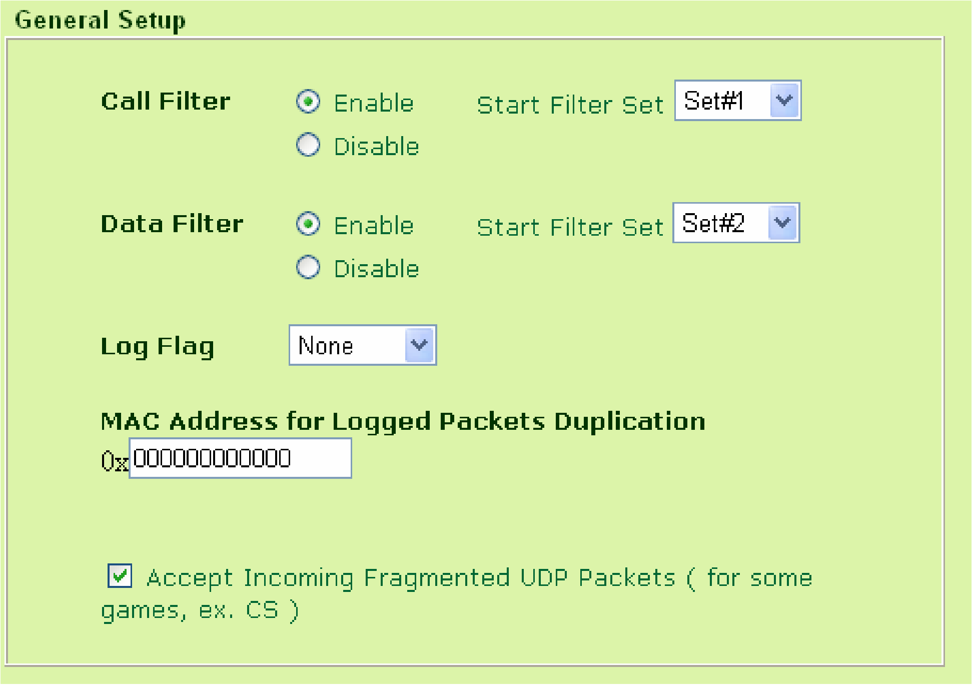
Filter Setup: Here are 12 filter sets for IP Filter configurations.

DoS defense: Click it to set up the DoS defense facility for detecting and mitigating the DoS attacks. The more details can be found in the Supplement A of Chapter 6.

URL Content Filter: Here provides the capability of blocking inappropriate web-sites to protect child in school or at home. The more details can be found in the Supplement B of Chapter 6.

6.3 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.



General Setup

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

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

Log Flag: None

MAC Address for Logged Packets Duplication
0x 000000000000

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

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

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

Log Flag: For troubleshooting needs you can specify the filter log here.

None: The log function is 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 not 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.

6.4 Editing the Filter Sets

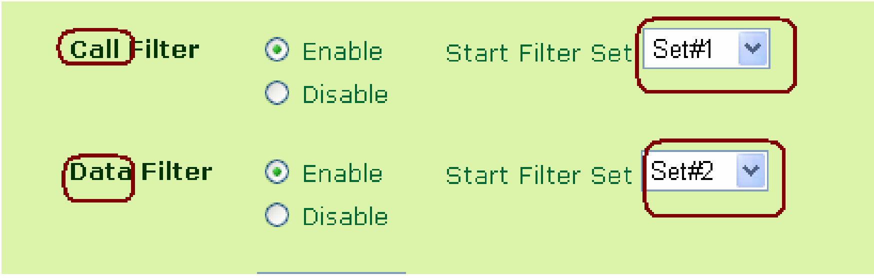
Comments: Enter filter set comments/description. Maximum length is 23 characters.

Filter Rule: 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.

The following setup pages show the default settings for the Call Filter and the Data Filter. <u>You will see the Call Filter set is assigned to Set 1 and the Data Filter set to Set 2</u>.



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

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

6.5 Editing the 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.

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

Check to enable the Filter Rule: Enables the filter rule.

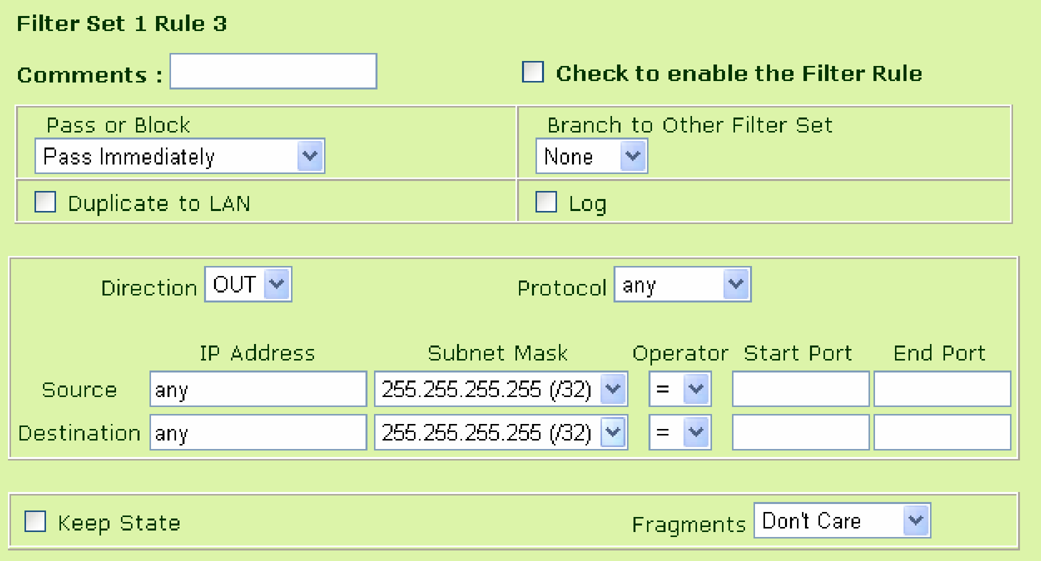
Pass or Block: Specifies the action to be taken when packets match the rule.

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.



Filter Set 1 Rule 3

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

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 is defined in **General Setup** > **MAC Address for Logged Packets Duplication**.

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.

For the Data Filter:

IN: Specifies the rule for filtering incoming packets.

OUT: Specifies the rule for filtering outgoing packets.

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

IP Address: Specifies a source and destination IP address for this filter rule to apply to. Placing 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: Specifies 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.

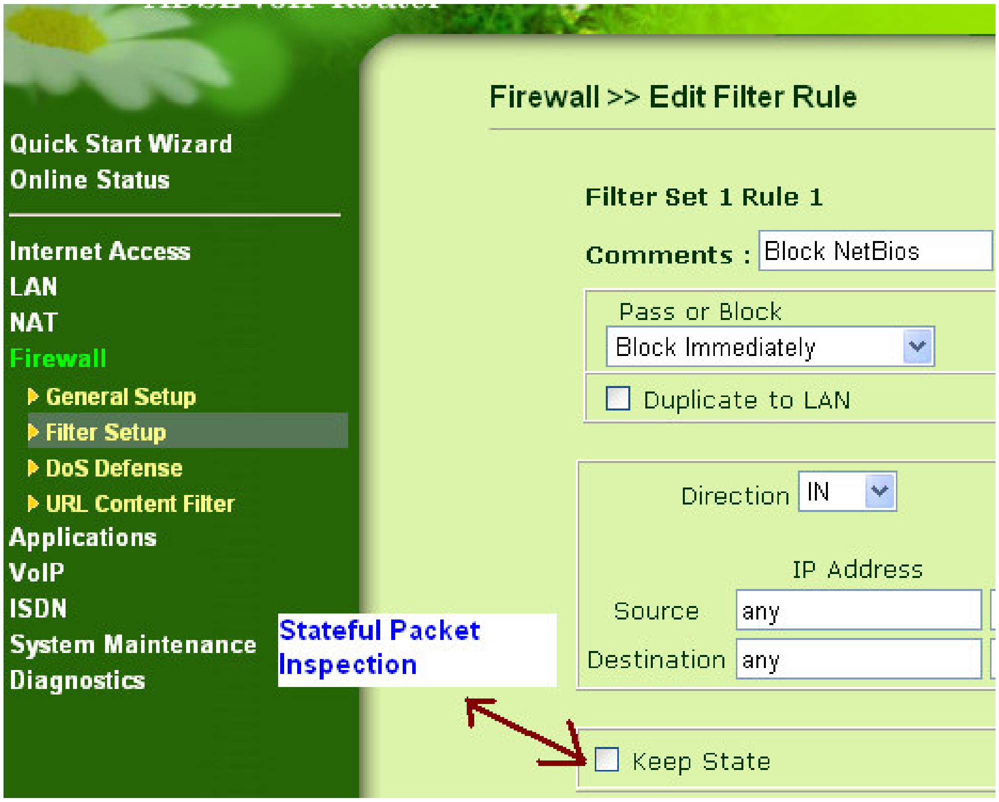
= : If the **End Port** is empty, the filter rule will set the port number to be the value of the **Start Port**. Otherwise, the port number ranges between the **Start Port** and the **End Port** (including the **Start Port** and the **End Port**).

!= : 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**).

> : Specifies the port number is larger than the **Start Port** (includes the **Start Port**).

< : Specifies the port number is less than the **Start Port** (includes the **Start Port**).

Keep State (Stateful Packet Inspection): When checked, protocol information about the TCP/UDP/ICMP communication sessions will be kept by the IP Filter/Firewall (the Firewall **Protocol** option (see page 5-21) requires that TCP or UDP or TCP/UDP or ICMP be selected for this to operate correctly).



Firewall >> Edit Filter Rule

Filter Set 1 Rule 1

Comments : Block NetBios

Pass or Block: Block Immediately

☐ Duplicate to LAN

Direction: IN

IP Address

Source: any

Destination: any

Stateful Packet Inspection

☐ Keep State

Fragments: Specifies a fragmented packets action.

(Do not Care): Specifies no fragment options in the filter rule.

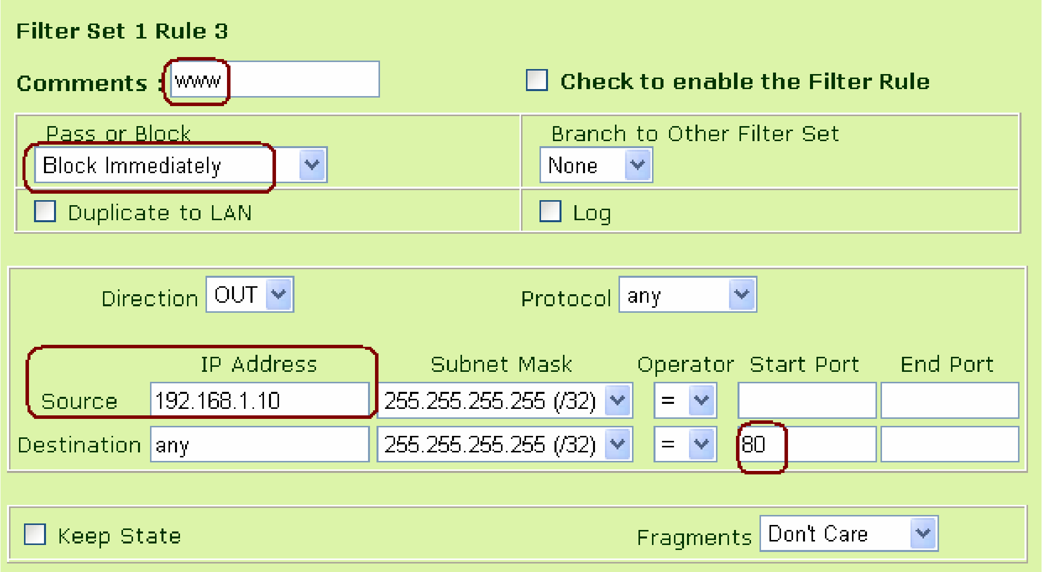
Unfragmented: Applies the rule to unfragmented packets.

Fragmented: Applies the rule to fragmented packets.

Too Short: Applies the rule only to packets which are too short to contain a complete header.

6.6 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 where Port 80 is the HTTP protocol port number for WWW services and is shown as below.



Filter Set 1 Rule 3

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: any

	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

Supplement A

Prevention of Denial of Service Attacks

A.1 Introduction

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.

A.2 An Overview of DoS Defense Functionality

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 anomaly situation violating the administrator's configuration is reported and the corresponding defense function is performed in order to mitigate the attack.

A.3 Configuration

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.

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 flood 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 Port Scan 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 an 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.

Enable 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.

Enable 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.

Enable 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.

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

Enable 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.

Enable Block fraggle Attack: Click the checkbox to activate the

Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

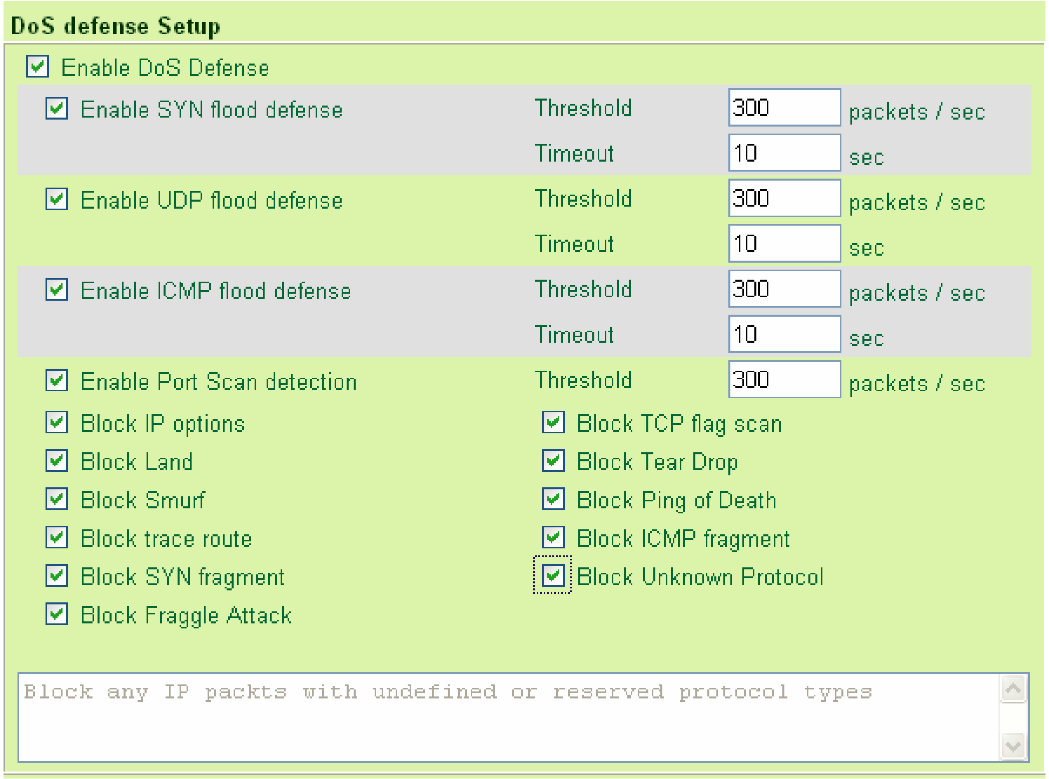
Enable TCP flag scan: Click the checkbox to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include ***no flag scan***, ***FIN without ACK scan***, ***SYN FIN scan***, ***Xmas scan*** and ***full Xmas scan***.

Enable Tear Drop: 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 host will hang once they re-construct the packets. Any packets realizing this attacking activity will be blocked by the Vigor router.

Enable Ping of Death: Click the checkbox to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams 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.

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

Enable 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 has ability to detect and reject this kind of packets.



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 Land

☑ Block Smurf

☑ Block trace route

☑ Block SYN fragment

☑ Block Fraggle Attack

☑ Block TCP flag scan

☑ Block Tear Drop

☑ Block Ping of Death

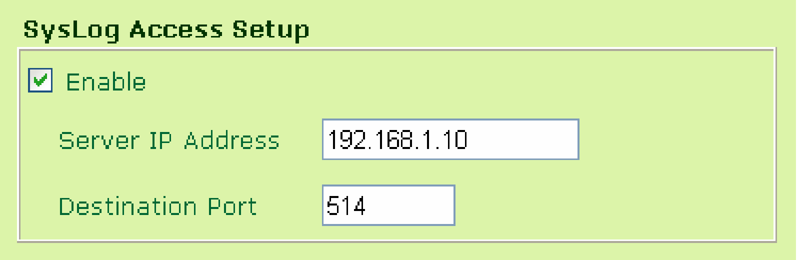
☑ Block ICMP fragment

☑ Block Unknown Protocol

Block any IP packts with undefined or reserved protocol types

A.4 Warning Message

All the warning messages will be sent to syslog client after you enable the syslog function. The administrator can go to **System Maintenance >> Syslog Setup** / **Mail Alert** to setup the syslog client. 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 **Firewall** except for the preamble keyword "DoS", followed by a name to indicate what kind of attacks is detected.

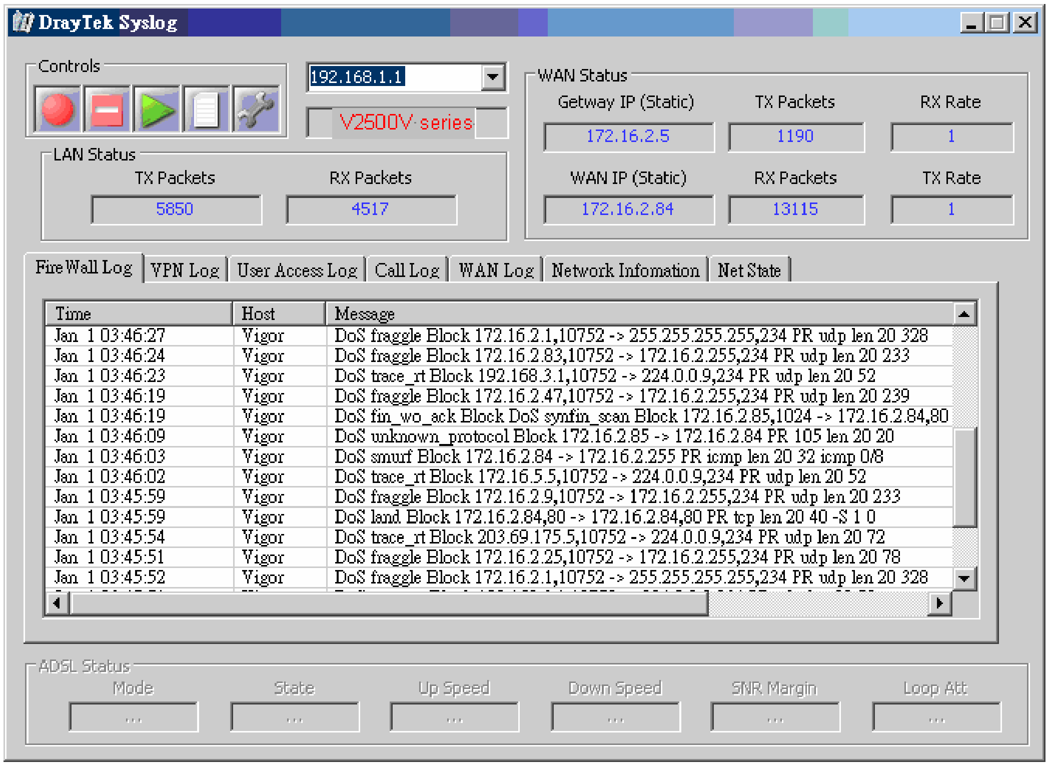


SysLog Access Setup

☑ Enable

Server IP Address 192.168.1.10

Destination Port 514



192.168.1.1

V2500V series

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
...	...	...	...	...	...

Supplement B

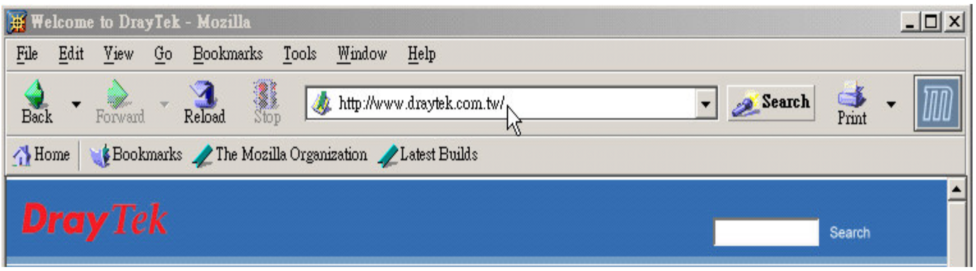
URL Content Filtering

B.1 Introduction

The Internet contains a wide range of materials, some of which may be offensive or even illegal in many countries. Unlike traditional media, the Internet does not have any obvious tools to segregate materials based on URL strings or content. URL content filtering 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.

B.2 An Overview of URL Content Filtering


Welcome to DrayTek - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://www.draytek.com.tw/
Search
Print
Home
Bookmarks
The Mozilla Organization
Latest Builds
DrayTek
Search

The URL content filtering facility in the Vigor series of broadband security 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.draytek.com, as shown above) matches any activated keyword, its associated HTTP request will be blocked by the Vigor router and a syslog message will be automatically sent to the syslog client. Also any request which tries to retrieve the malicious code will be discarded by the Vigor router. Similarly, a syslog message will be sent to the syslog client.

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

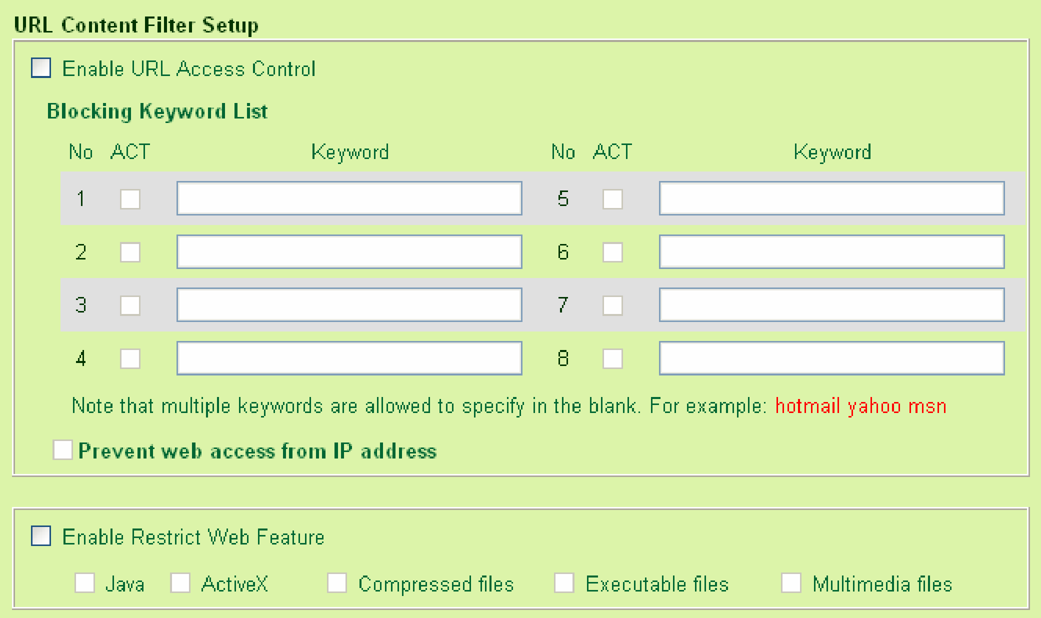
You must clear your browser cache first so that the URL content filtering facility can work properly on a web page that you visited before

B.3 Configuration

The following sections describe the web configuration for setting up the URL content filtering facility, including specific configuration information and any limitation they have. One can find the entrance of this setting, as depicted in the following figure, after clicking the **Firewall** in the main menu.

The URL content filtering facility implemented on the Vigor router consists of the ***URL Access Control***, ***Prevent web access from IP address***, ***Restrict Web Feature control***, ***Exceptional Subnet handling***, and ***Time schedule*** functions. The *URL Access Control* aims at controlling the access right of web sites by inspecting the URL string against user-defined keywords. The *Restrict Web Feature control* intends to block the malicious codes hidden in Web pages, such as *Java Applet*, *Active X*, *Cookies*, *Proxy*, *compressed* files, and *executable* files. Also, it is able to block all downloads of *multimedia* files from Web pages in order to control the bandwidth usage.

The function of *Prevent web access from IP address* is used to avoid that inappropriate web sites can be accessed through directly using IP address in the URL locator, even though their URL strings match the user-defined keywords. The function of *Exceptional Subnet handling* allows the administrator to specify a group of hosts that are free from the *URL Access Control*. This group of hosts could be defined as a set of IP addresses or subnets. Finally, the Vigor router supports the *Time schedule* function to control what time should perform the URL content filtering facility. Now, let us move on the description of each item's usage in more detail.



URL Content Filter Setup

☐ Enable URL Access Control

Blocking Keyword List

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

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

☐ Prevent web access from IP address

☐ Enable Restrict Web Feature

☐ Java ☐ ActiveX ☐ Compressed files ☐ Executable files ☐ Multimedia files

Enable URL Access Control: 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.

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.

Example: 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. But, the user is able to access the website www.backdoor.net/firewall/forum/d_123.html. 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. Accordingly, the Vigor router will identify the forbidden URL and perform the blocking action for these websites by cutting the associated connections.

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.

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 ( ). (2.5.6 later version)

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.

***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. Similarly, 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 cookie from any website.

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**

Time Schedule: Specify what time should perform the URL content filtering facility. (2.5.6 later version)

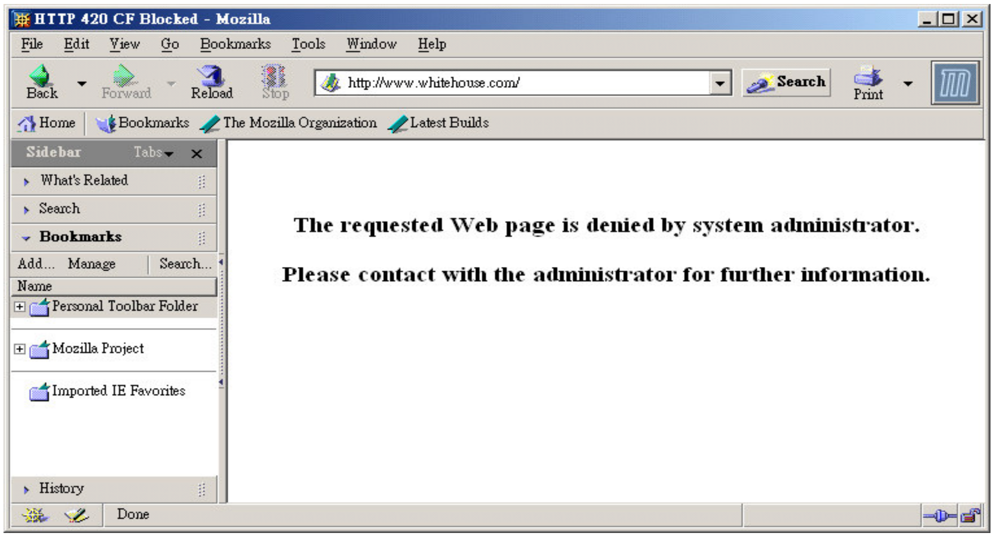
Always Block*:* Click it so that the URL content filtering facility can be executed on the Vigor router anytime.

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.

B.4 Warning Message

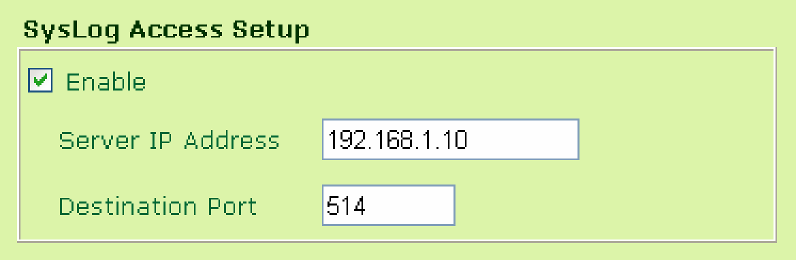


The requested Web page is denied by system administrator.

Please contact with the administrator for further information.

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

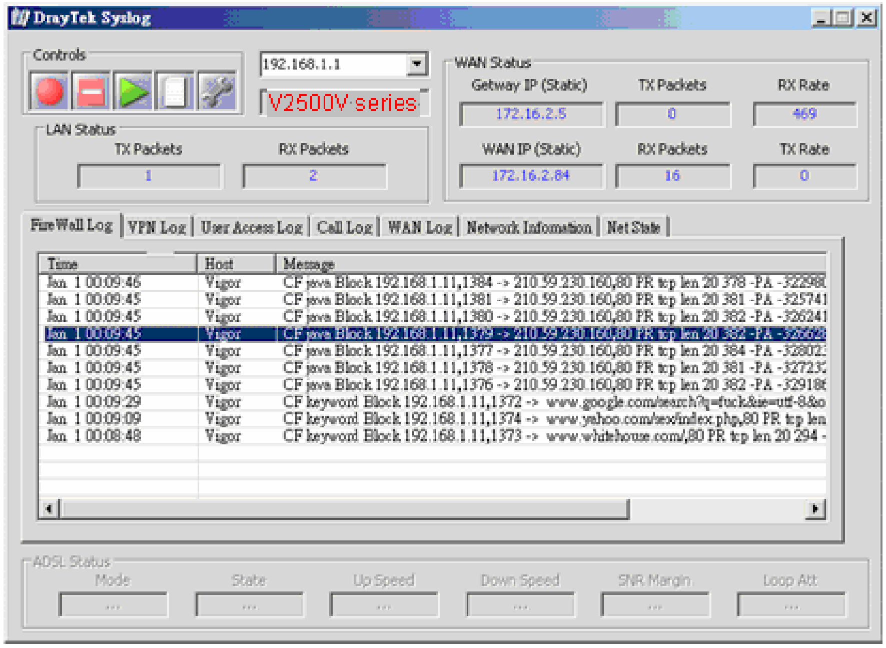
Also, the warning message will be automatically sent to the syslog client after you enable the syslog function. The administrator can setup the syslog client in the **Syslog Setup** by using Web Configurator. Thus, the administrator can view the warning messages from the **URL Content Filtering** functionality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



☑ Enable

Server IP Address: 192.168.1.10

Destination Port: 514



192.168.1.1

LAN Status: TX Packets 1, RX Packets 2

WAN Status: Getway IP (Static) 172.16.2.5, TX Packets 0, RX Rate 469, WAN IP (Static) 172.16.2.84, RX Packets 16, TX Rate 0

```
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 -
```

Chapter 7
Dynamic DNS

7.1 Introduction

The ISP often provides you with a dynamic IP address when you connect to your ISP. It means that the public IP address allocated to your router changes each time you connect to the ISP. The remote users can not predict your current IP address to find you if you are planning to run a local server.

The facilities of Dynamic DNS let remote users be able to get to your network via the registered online WAN IP address (such as hostnmae.dyndns.org) offered by from the Dynamic DNS service providers. i.e. 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.

You can position the Dynamic DNS service providers as **the postman** and the registered online WAN IP address (such as **hostnmae.dyndns.org**) as your **mail box No**. as you interpret your dynamic IP address as your tentative address of your rented house. Your friends want to reach you and they can always send package to your mail box if you often changed rented house.

Before you set up the Dynamic DNS function, you have to subscribe free domain names from the Dynamic DNS service providers. The router provides up to three accounts for three different DNS services. Vigor routers are compatible with most popular Dynamic DNS service providers such as **www.dynsns.org**, **www.no-ip.com**, **www.dtdns.com**, **www.changeip.com**, **www.dynamic- nameserver.com**. You should visit their websites for registering your own domain name for the router.

7.2 Configuration

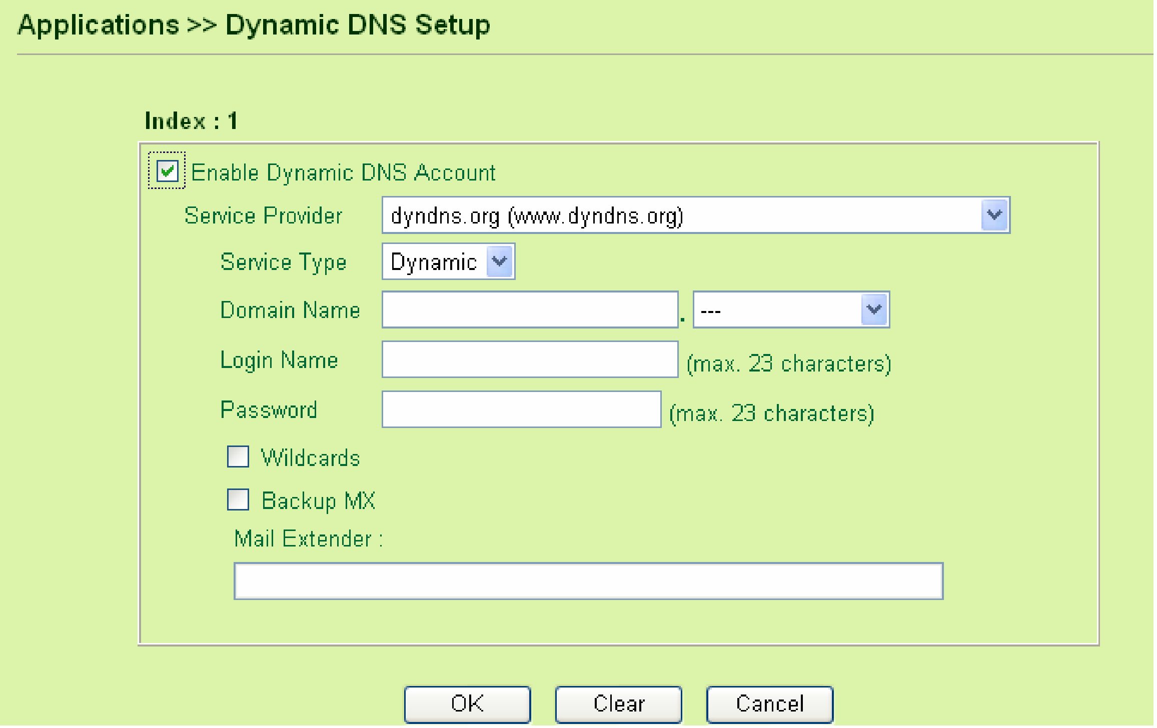
Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider named ***hostname.dyndns.org***, and an account with username: ***test*** and password: ***test***.
2. Go to **Applications** > **Dynamic DNS**

   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***.

   Click **OK** button to activate the settings.

The **Wildcard** and **Backup MX** features are not supported by all Dynamic DNS providers. Please carefully read the user instructions of your preferred Dynamic DNS providers.



Applications >> Dynamic DNS Setup

Index : 1

☑ Enable Dynamic DNS Account

Service Provider: dyndns.org (www.dyndns.org)

Service Type: Dynamic

Domain Name: . ---

Login Name: (max. 23 characters)

Password: (max. 23 characters)

☐ Wildcards

☐ Backup MX

Mail Extender :

Disable the Function and Clear all Dynamic DNS Accounts

1. Go to **Applications** > **Dynamic DNS**.
2. Uncheck **Enable Dynamic DNS Setup**, and click **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

1. Go to **Applications** > **Dynamic DNS**.
2. Click the **Index** number you want to delete, and click **Clear All** button to delete the account.

7.3 Validation and Troubleshooting

Ping the Registered Domain Name

1. After router is online, use **PING** utility to ping your registered domain name to verify if it works.
2. Go to **Online Status** 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

You can check the update status of your service from the router's Telnet interface (use Windows telnet.exe for example). The command ***ddns log*** shows the results. Here is an example, in this case using dyndns.org:

1. Go to **Applications** > **Dynamic DNS**.
2. Click **View Log** button. The logs of DDNS updates will be shown as follows.

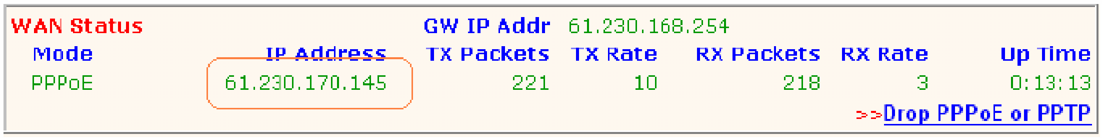
```
>ddns log
###1 DDNS is updating…
>>>2 A=username H=hostname, U=1
>>>3 Connecting to the DDNS server (0x4225dad2)
<<<4 Return Code= nochg 61.230.170.145 (hostname.dyndns.org)
```

H: means Domain Name without suffix [check that you enter the correct data for the hostname and username-these do vary with each service, sometimes including the domain suffix.

Return Code= good 61.230.170.145

If you encounter any difficulties of using DDNS, you can send the DDNS log to your local dealer or us **support@draytek.com** to offer you with more assistance.

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



WAN Status GW IP Addr 61.230.168.254

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.170.145	221	10	218	3	0:13:13

>>Drop PPPoE or PPTP

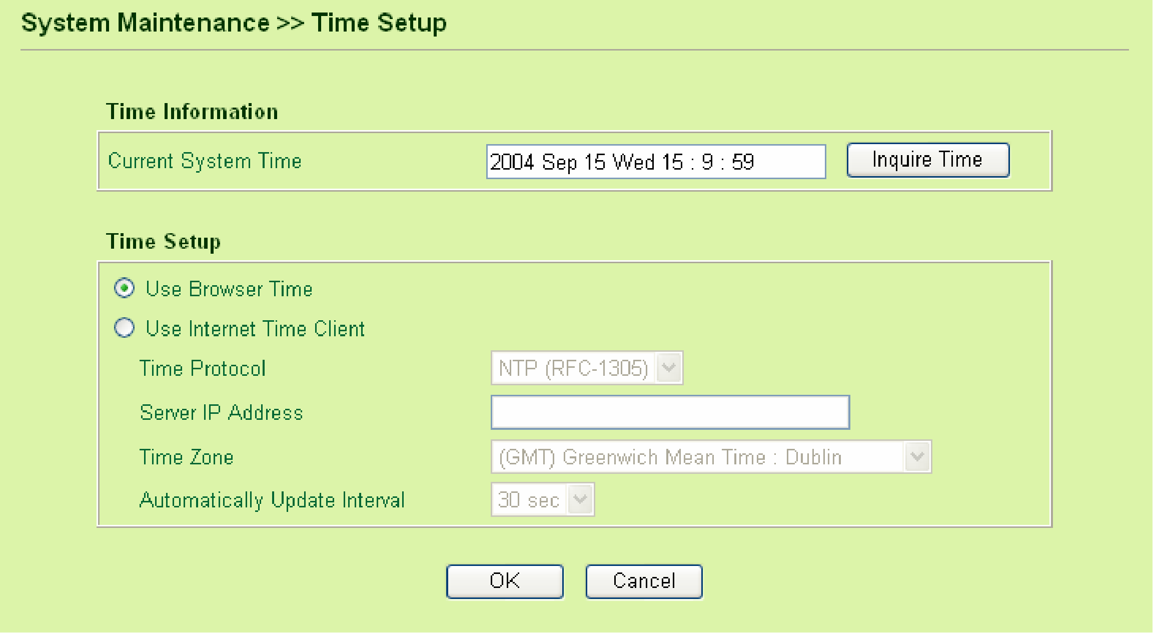
You will see the IP address in the circle, which is the same as the Return Code in the DDNS logs. This indicates that the DDNS update is done.

Chapter 8
Call Schedule

8.1 Introduction

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 or dial-in access (if there is ISDN interface) at certain times (e.g. business hours). The call schedule can also be applied to LAN-to-LAN profiles.

On the **Time Setup** menu, you can firstly ensure your router time to be correct before you would like to enforce **Call Scheduling**.



System Maintenance >> Time Setup

Time Information

Current System Time: 2004 Sep 15 Wed 15 : 9 : 59

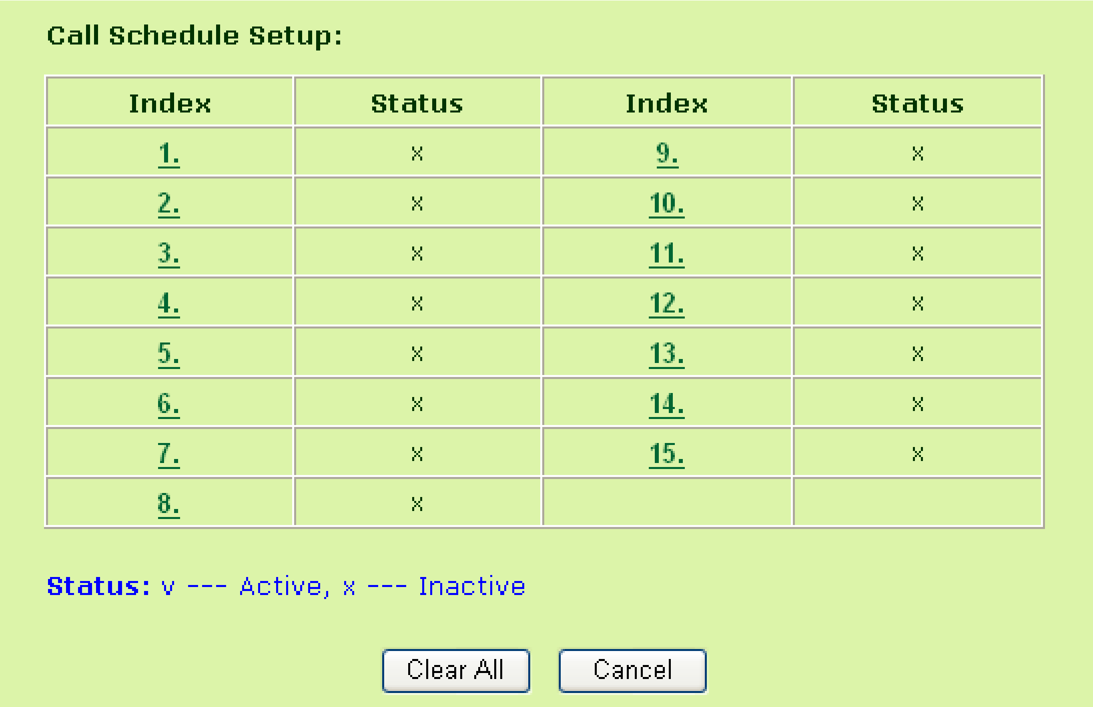
Time Setup

● Use Browser Time
○ Use Internet Time Client

Time Protocol: NTP (RFC-1305)
Server IP Address:
Time Zone: (GMT) Greenwich Mean Time : Dublin
Automatically Update Interval: 30 sec

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.

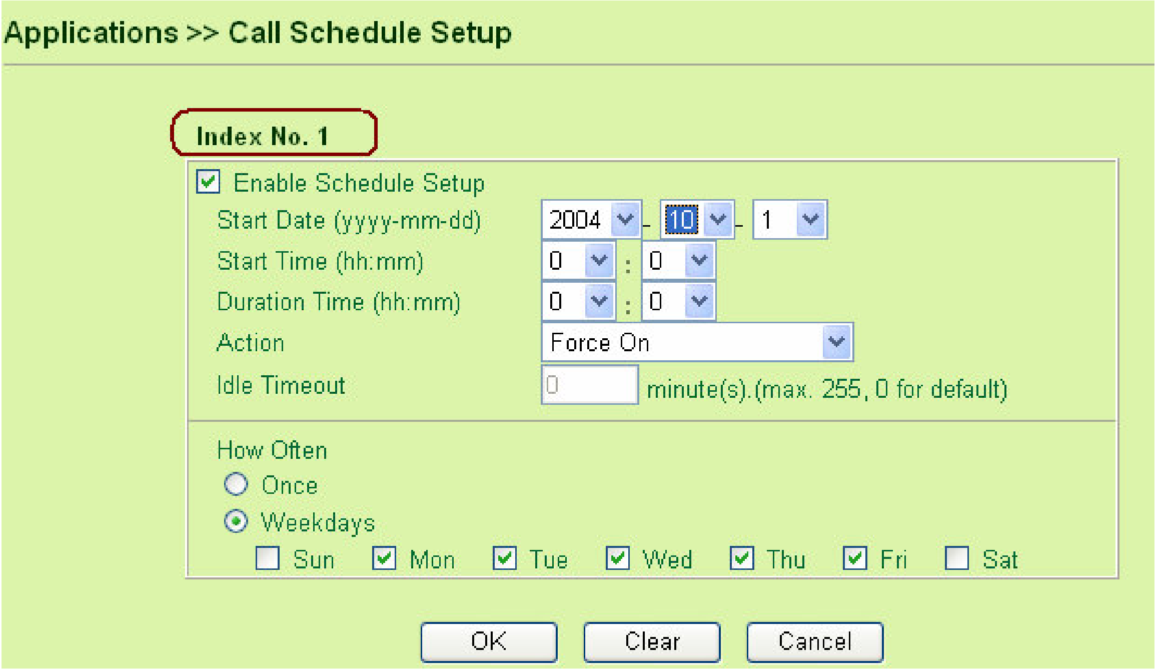
You can have up to 15 entries of different schedules and you must then apply the required schedule(s) to the appropriate ISP by entering the schedule number into the ISP setup:



Call Schedule Setup:

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



Applications >> Call Schedule Setup

Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd): 2004 - 10 - 1

Start Time (hh:mm): 0 : 0

Duration Time (hh:mm): 0 : 0

Action: Force On

Idle Timeout: 0 minute(s).(max. 255, 0 for default)

How Often

○ Once

● Weekdays

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

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: Specify the connection up.

Force Down: Specify the connection 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**.

***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.

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.

Specify appropriate time duration and action to the profile and then click **OK** button to apply.

Specify the call schedule to specific Internet access profile or LAN-to-LAN profile.

Delete a Call Schedule

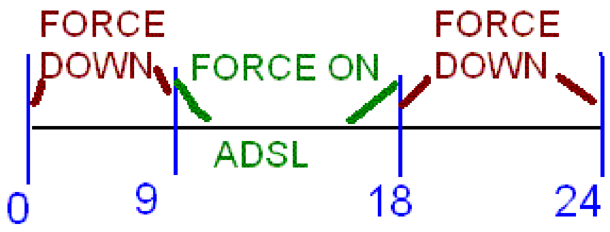
1. Click **Call Schedule Setup** and the **Index** number that you want to remove.

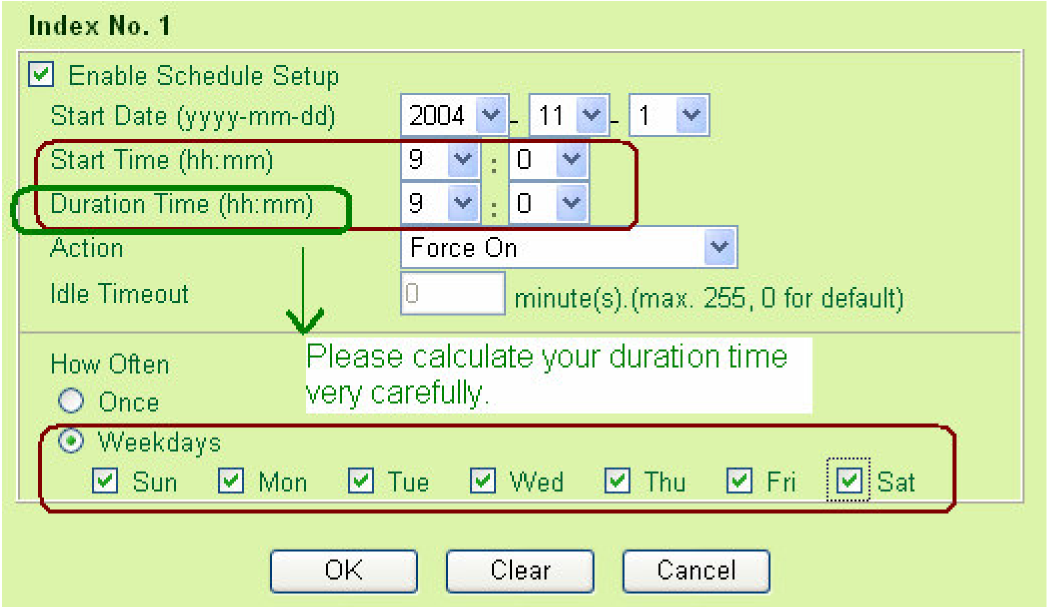
2. Click **Clear** button to clear current profile.

8.2 Example of ADSL ISP users

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 (the duration is 9 hours) for whole week.



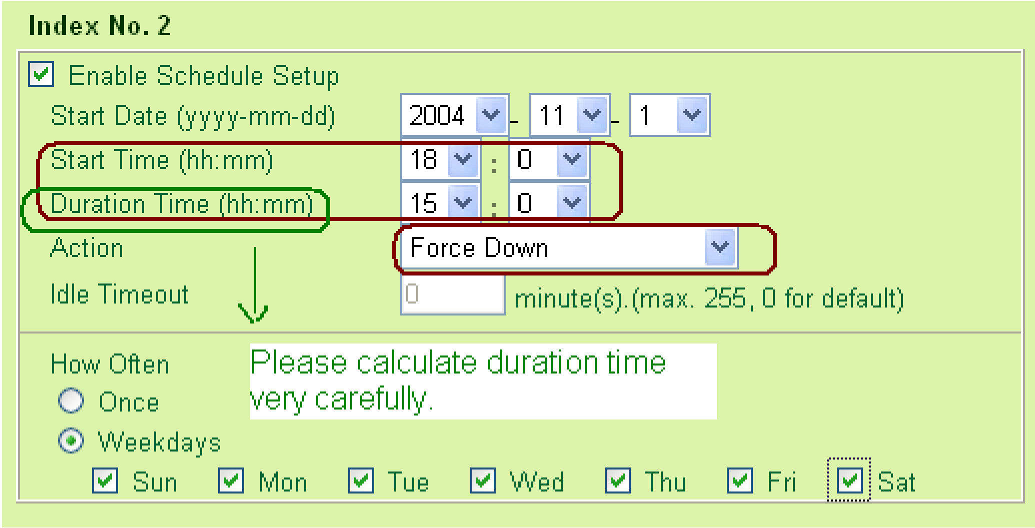

Index No. 1

☑ Enable Schedule Setup
Start Date (yyyy-mm-dd) 2004 - 11 - 1
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)

Please calculate your duration time very carefully.

How Often
○ Once
● Weekdays
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

3. **Force Down** from 18:00 to next day 9:00 (the duration is 15 hours) for a week.

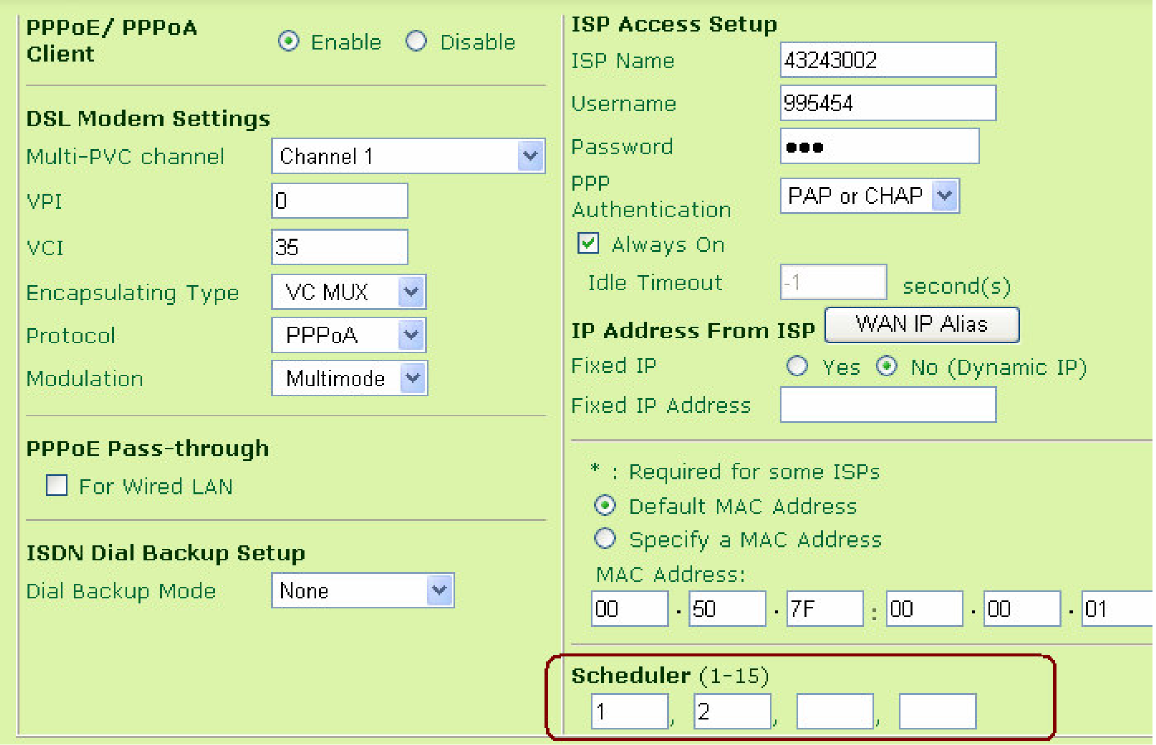

Index No. 2

☑ Enable Schedule Setup
Start Date (yyyy-mm-dd) 2004 - 11 - 1
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)

Please calculate duration time very carefully.

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** actions by time plan which has been predefined in the schedule profiles.



PPPoE/ PPPoA Client ● Enable ○ Disable

DSL Modem Settings

Multi-PVC channel: Channel 1

VPI: 0

VCI: 35

Encapsulating Type: VC MUX

Protocol: PPPoA

Modulation: Multimode

PPPoE Pass-through

☐ For Wired LAN

ISDN Dial Backup Setup

Dial Backup Mode: None

ISP Access Setup

ISP Name: 43243002

Username: 995454

Password: ●●●

PPP Authentication: PAP or CHAP

☑ Always On

Idle Timeout: -1 second(s)

IP Address From ISP WAN IP Alias

Fixed IP: ○ Yes ● No (Dynamic IP)

Fixed IP Address:

* : Required for some ISPs

● Default MAC Address

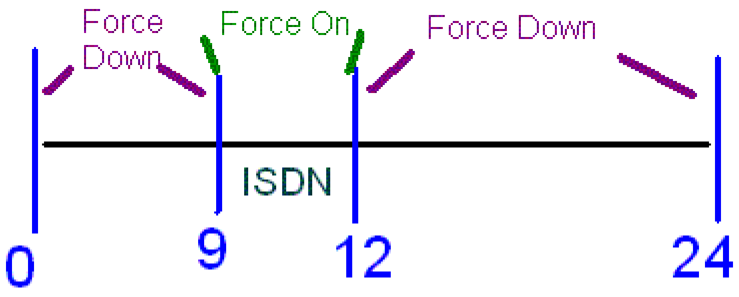
○ Specify a MAC Address

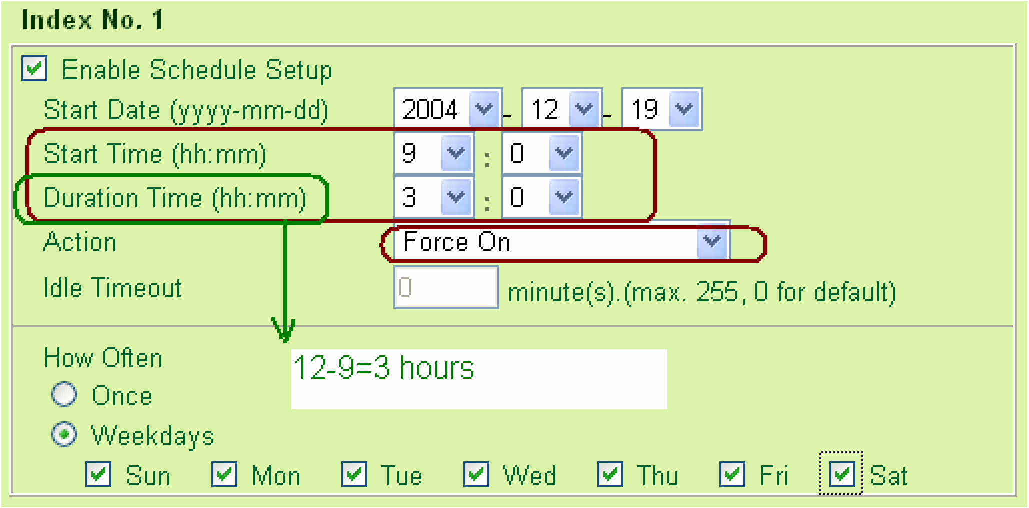
MAC Address: 00 . 50 . 7F : 00 . 00 . 01

Scheduler (1-15): 1 , 2 , ,

8.3 Example of ISDN ISP users

Because you need to send important files to your company from your home via ISDN, you can use the ISDN interface of Vigor2500Vi series to set the duration of ISDN be always-on (Force On) from 9:00 to 12:00 for whole week. The rest of time shall be on ISDN connection. i.e. The ISDN shall be **Force Down**.




Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd) 2004 - 12 - 19

Start Time (hh:mm) 9 : 0

Duration Time (hh:mm) 3 : 0

Action Force On

Idle Timeout 0 minute(s).(max. 255, 0 for default)

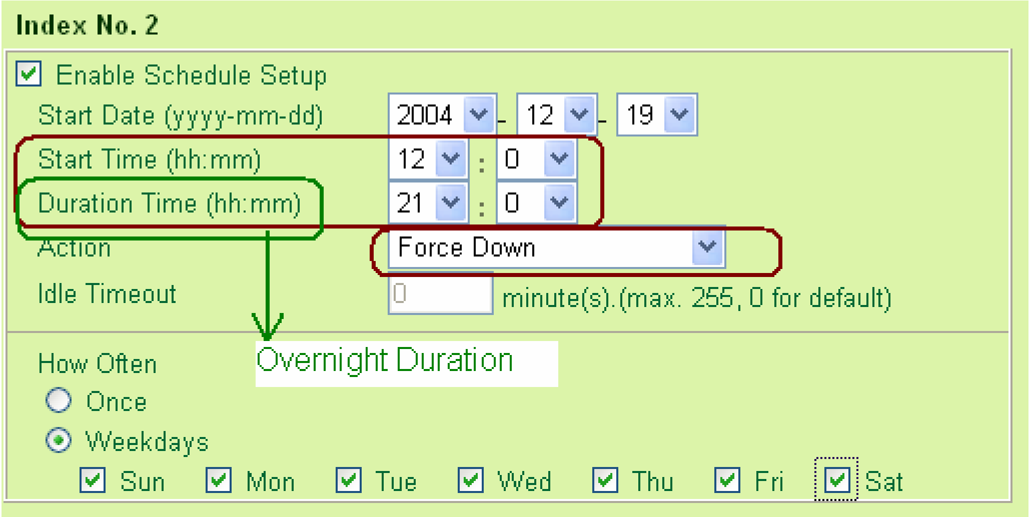
How Often

○ Once

● Weekdays

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

3. Configure the Force Down from 12:00 to next day 9:00 (the duration is 21 hours) for whole week.


Index No. 2

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd) 2004 - 12 - 19

Start Time (hh:mm) 12 : 0

Duration Time (hh:mm) 21 : 0

Action Force Down

Idle Timeout 0 minute(s).(max. 255, 0 for default)

How Often

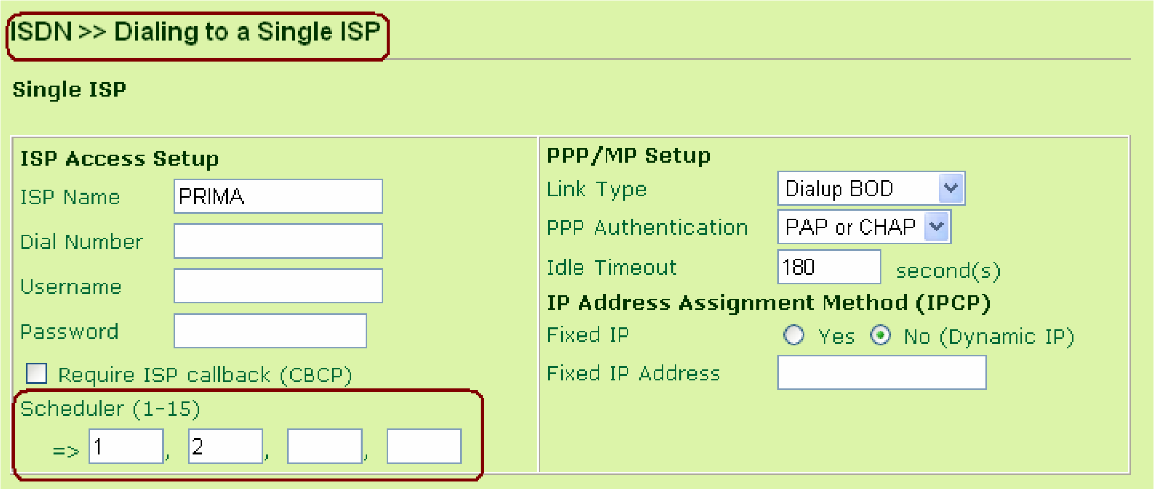
○ Once

● Weekdays

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

The “**Duration Time**” mechanism is for you to calculate the overnight period.

4. Assign these two profiles to the ISDN Internet access profile.



ISDN >> Dialing to a Single ISP

Single ISP

ISP Access Setup

ISP Name	PRIMA
Dial Number	
Username	
Password	

☐ Require ISP callback (CBCP)

Scheduler (1-15)

=> 1, 2, ,

PPP/MP Setup

Link Type	Dialup BOD
PPP Authentication	PAP or CHAP
Idle Timeout	180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP	○ Yes ● No (Dynamic IP)
Fixed IP Address	

Chapter 9
Static Route

9.1 Introduction

If you subscribed multiple public IP addresses (i.e. a subnet allocated by your ISP as opposed to just a single public IP address), you can set up the router's second IP address on your first allocated public address. The rest of your ISP allocated subnet will then be passed through to your LAN.

You shall manually set the TCP/IP properties of PC on the LAN. After you assign the PC with one of your public IP addresses, you must also specify the default gateway to the PC (the router's 2nd IP address) and some DNS server addresses (your ISP can advise of these addresses). On your LAN, you can mix NATed IP addresses and public IP addresses. Consequently, some PCs really have public IP addresses but some PCs are on your private (NATed) subnet.

Static routes in your Vigor router provide a quick and effective way to route data from one subnet to different subnet without using the Routing Information Protocol (RIP). Basically, a static route is a guiding path in the router that specifies how the router will get to a certain subnet by using a certain path. If you have many private subnets behind the router, or you want to access another public subnet via an inside router, you can configure the router to route IP packets to those inside IP networks using 1st IP address/subnet mask fields on the **LAN TCP/IP and DHCP Setup** page.

The router also has built-in RIP (Routing Information Protocol) by default. If the neighbor routers have the same protocol, the RIP will be used for exchanging routing information. Here, the **Static Route Setup** just provides a way to guide specified IP packets through specified routers statically. This chapter is for you to configure static routes with your Vigor router.

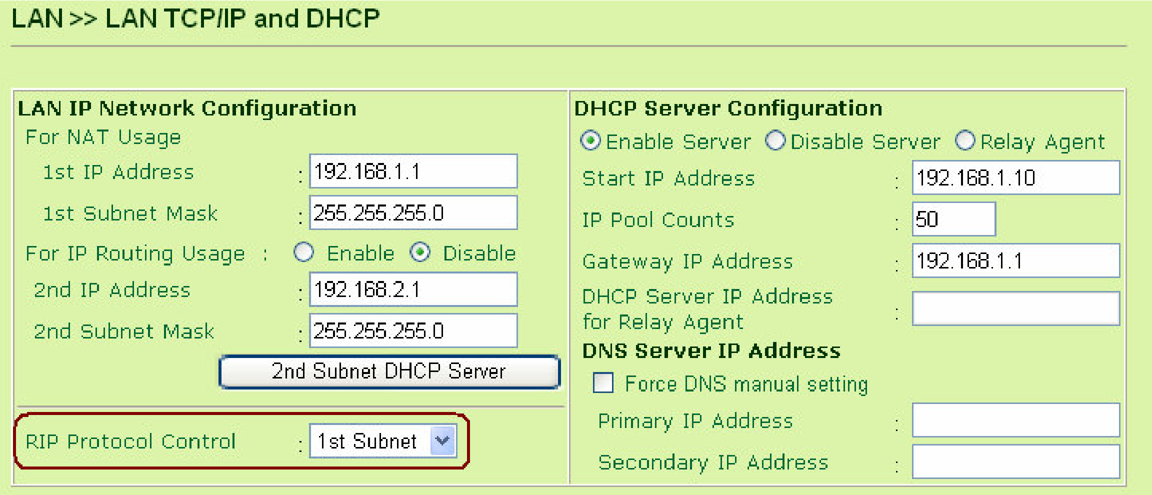
9.2 Configuration

Add Static Routers to Inside Private and Public Networks

Assume the Internet access setup has been configured and the router worked properly. You use the 1st subnet address 192.168.1.0/24 to surf the Internet and also an internal private subnet 192.168.10.0/24 via an internal router (192.168.1.2/24) and an internal public subnet 211.100.88.0/28 via an internal router (192.168.1.3/24). Also, the router 192.168.1.1/24 is a default gateway for the router 192.168.1.2/24.

1. Click **LAN TCP/IP and DHCP Setup,** select **RIP Protocol Control** as **1st Subnet**, and then click **OK** button.

To set **RIP Protocol Control** as **1st Subnet** has two different purposes. The first one is that the LAN interface could be exchanged RIP packets with neighbor routers via 1st subnet (192.168.1.0/24). The second one is that those inside private subnets (ex. 192.168.1.0/24) could be NATed by the router to the Internet, but do IP routing for each other as well.



LAN >> LAN TCP/IP and DHCP

LAN IP Network Configuration

For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage : ○ Enable ● Disable

2nd IP Address : 192.168.2.1

2nd Subnet Mask : 255.255.255.0

RIP Protocol Control : 1st Subnet

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 :

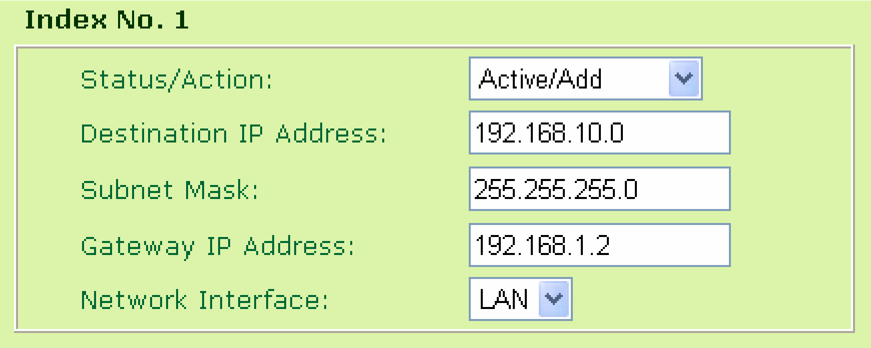
DNS Server IP Address

☐ Force DNS manual setting

Primary IP Address :

Secondary IP Address :

2. Add a static route to the inside private subnet 192.168.10.0/24 via the internal router 192.168.1.2/24. Click **Static Route > Index Number** to add a static route to destination subnet 192.168.10.0/24 as follows.



Index No. 1

Status/Action: Active/Add

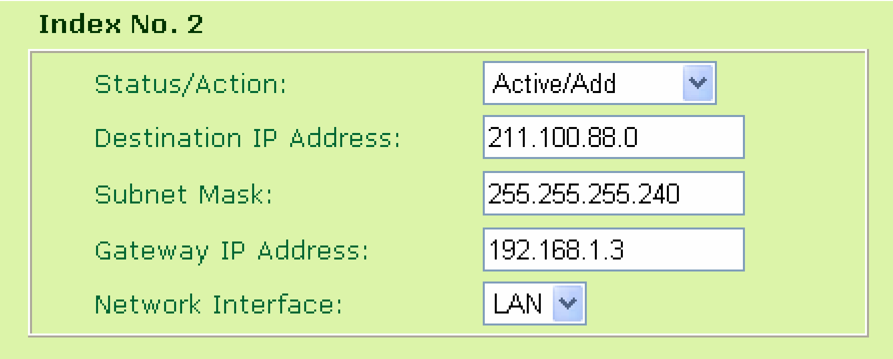
Destination IP Address: 192.168.10.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.2

Network Interface: LAN

3. Add a static route to the inside public subnet 211.100.88.0/28 via 192.168.1.3/24 as below:



Index No. 2

Status/Action: Active/Add

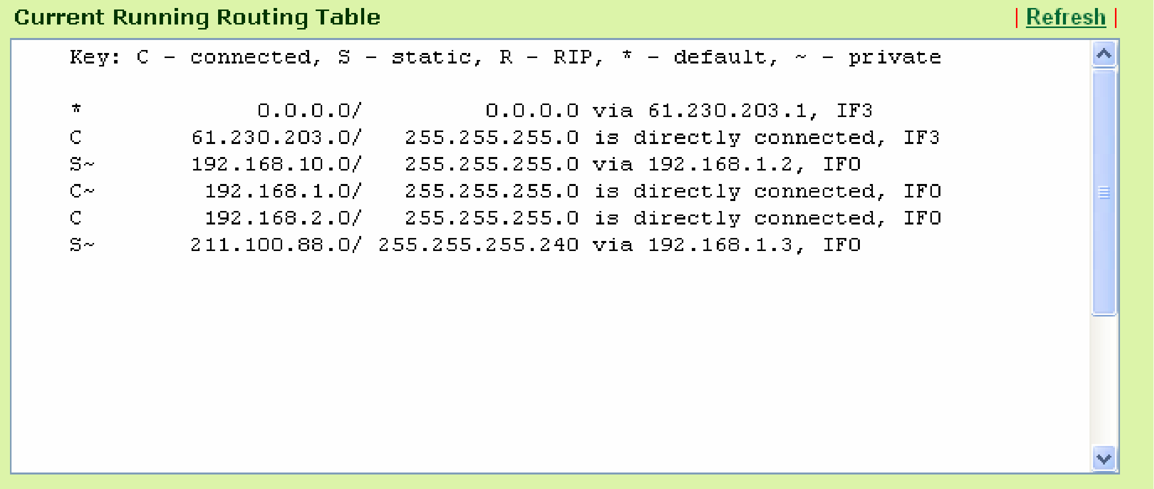
Destination IP Address: 211.100.88.0

Subnet Mask: 255.255.255.240

Gateway IP Address: 192.168.1.3

Network Interface: LAN

4. Click **Static Route > View Routing Table** to verify the current routing table.

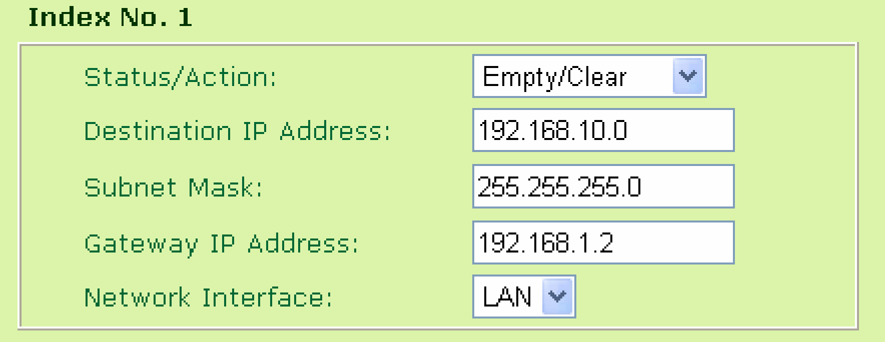


```
Key: C - connected, S - static, R - RIP, * - default, ~ - private

*           0.0.0.0/         0.0.0.0 via 61.230.203.1, IF3
C        61.230.203.0/   255.255.255.0 is directly connected, IF3
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2, IF0
C~        192.168.1.0/   255.255.255.0 is directly connected, IF0
C         192.168.2.0/   255.255.255.0 is directly connected, IF0
S~       211.100.88.0/ 255.255.255.240 via 192.168.1.3, IF0
```

Delete or Clear the setting of Static Route

1. Click **Static Route Setup > Index Number** which you want to delete.

2. Select **Status/Action** to **Empty/Clear**. Click **OK** button to delete the route.



Index No. 1

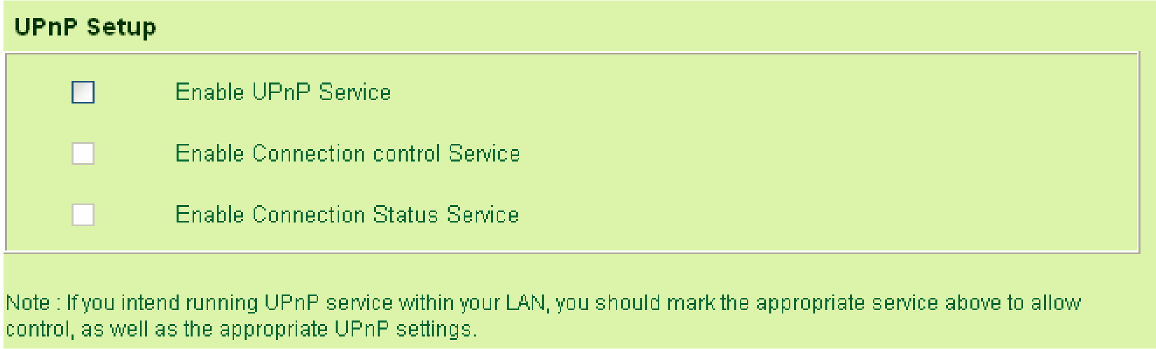
Status/Action: Empty/Clear
Destination IP Address: 192.168.10.0
Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.1.2
Network Interface: LAN

Chapter 10
UPnP (Universal Plug and Play)

10.1 Introduction

The UPnP protocol is intended 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 Vigor 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 and without the user having to manually set up port mappings or a DMZ.



UPnP Setup

☐ Enable UPnP Service

☐ Enable Connection control Service

☐ Enable Connection Status Service

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

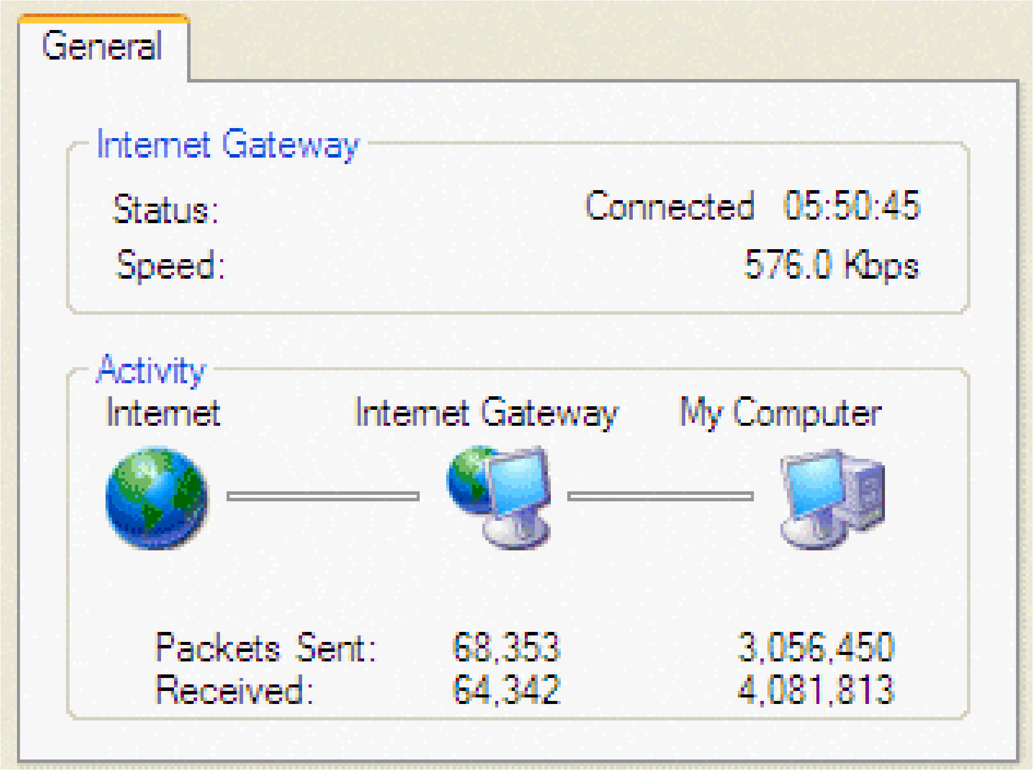
UPnP is available on Windows XP and the Vigor router provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

10.2 Configuration

You can enter the **UPNP Setup** via **Advanced Setup > UPNP Service Setup** on the Web Configurator in your Vigor router.

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

An “Internet Gateway” icon will appear in the “Network Connections” window. When disconnected, you double-click this icon to set up a connection to the Internet starting from the Internet Gateway.

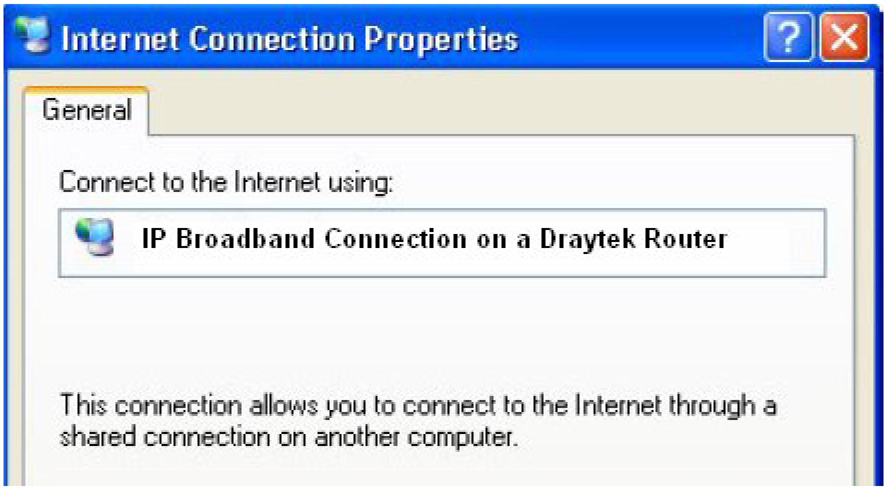


Status: Connected 05:50:45

Speed: 576.0 Kbps

	Internet Gateway	My Computer
Packets Sent:	68,353	3,056,450
Received:	64,342	4,081,813

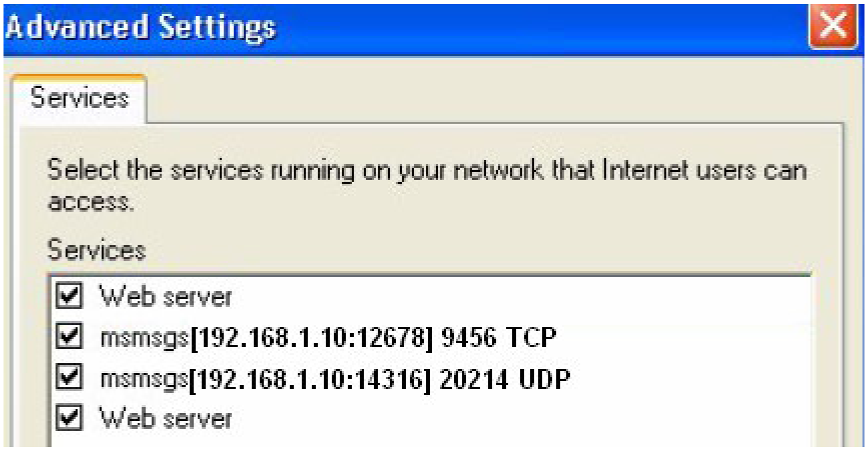
Click the **IP Broadband Connection on DrayTek Router** on Windows XP/Network Connections. The NAT Traversal of UPnP enables the services on your LAN to be operated only by making an explicit port mappings to the internal host that is running the web or FTP server, your router can know where to forward the packets coming from the Internet to. The screenshots below show examples of this facility.



Connect to the Internet using:

IP Broadband Connection on a Draytek Router

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



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

Services

- ☑ Web server
- ☑ msmsgs[192.168.1.10:12678] 9456 TCP
- ☑ msmsgs[192.168.1.10:14316] 20214 UDP
- ☑ Web server

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

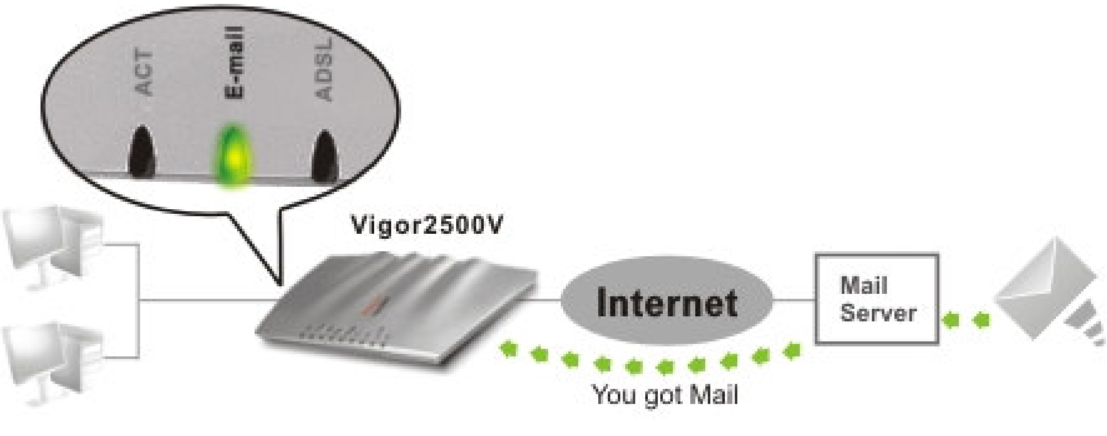
The Vigor2500V series ADSL router is already equipped with the ALG's (Application Level Gateways) in order to increase the interoperability with multimedia applications for the limitation of NAT. DrayTek ALG's is already integrated with the router firmware so that you do not need to set any settings onto Vigor router.

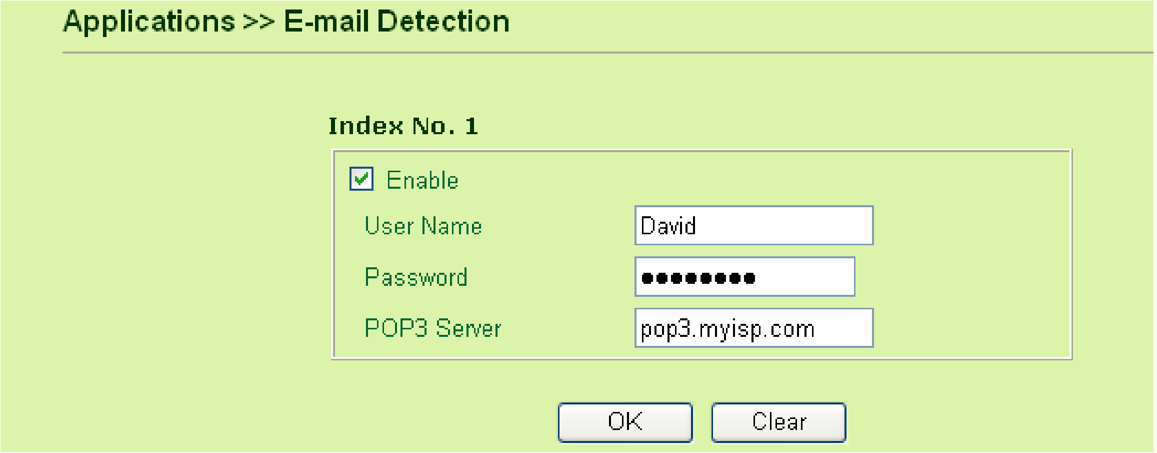
Chapter 11
E-mail Detection

11.1 Introduction

The Vigor2500V series router has E-mail detection mechanism for notifying users that the POP3-mail server is holding E-mail. There is an LED marked “e-mail”. You can set your router to periodically check for whether there are E-mail at POP3-protocol mail server of your ISP or other E-mail provider. The E-mail LED will light if there is E-mail waiting for you to retrieve them. You have up to five different POP3 accounts checked. The E-mail detection lets you see whether you have E-mail waiting without turning on or log into your PC.

Be sure that your E-mail software can receive E-mail using the POP3 protocol. The POP3 protocol is the world most common method. However, the web-based services such as Hotmail (unless they provide an interface too). You have to check the POP3 server address, your E-mail user name and password. The setting procedure is exactly the same as you set up your regular E-mail software.





Applications >> E-mail Detection

Index No. 1

☑ Enable

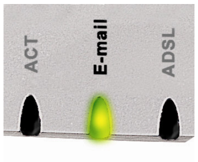
User Name: David

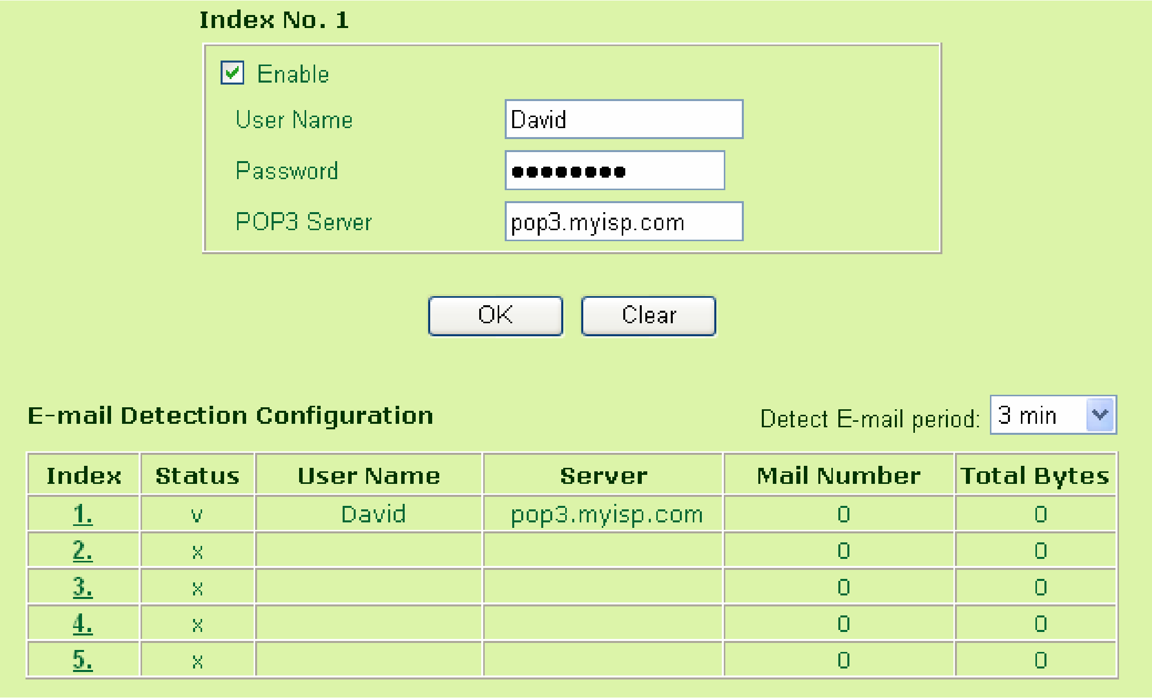
Password: ●●●●●●●●●

POP3 Server: pop3.myisp.com

You can enter up to five profiles for different mail servers. If there are E-mail waiting, the **Mail Number** waiting will be shown as well as the total size of mail box.

The E-mail LED on the router will notify you by flashing.





Index No. 1

☑ Enable

User Name: David

Password: ●●●●●●●●●

POP3 Server: pop3.myisp.com

E-mail Detection Configuration

Detect E-mail period: 3 min

Index	Status	User Name	Server	Mail Number	Total Bytes
1.	v	David	pop3.myisp.com	0	0
2.	x			0	0
3.	x			0	0
4.	x			0	0
5.	x			0	0

By default, the E-mail will be checked every 3 minutes. You can change the default frequency as shown on the screenshot.

Chapter 12
VoIP

12.1 Introduction

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

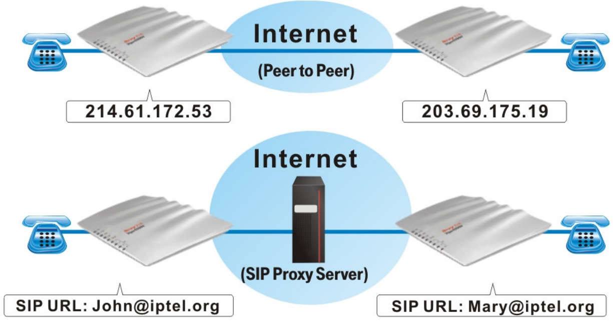
There are many different call signaling protocols; methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and the older H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor2500V 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 use 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. Vigor2500V series provides Gvarious CODECs, including G.711 A/μ-law 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 Vigor2500V's VoIP facilities 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)

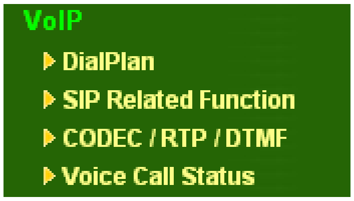


Before you can set up the router for SIP you need to open an account with a SIP registrar [e.g. IPTEL, DrayTEL (www.draytel.org)].

Our Vigor2500V firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor2500V also equips 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.

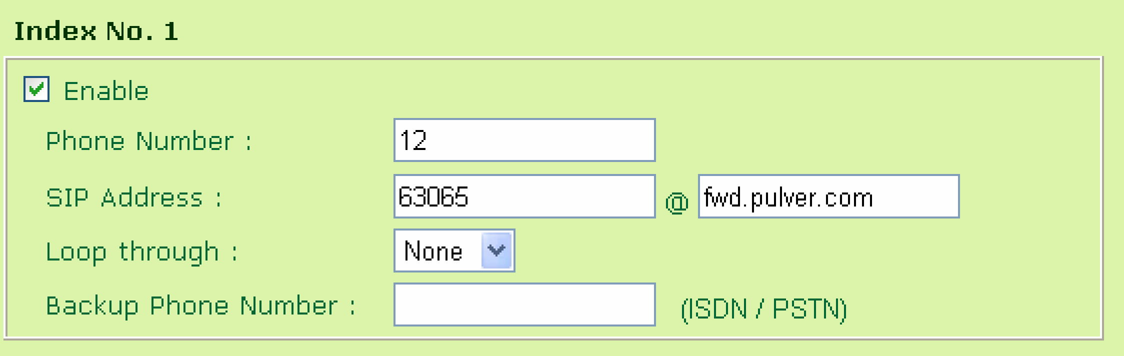
12.2 VoIP Settings

The following is the setting path for this function.



12.2.1 DialPlan Setup

The Vigor2500V has 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 Vigor2500V 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

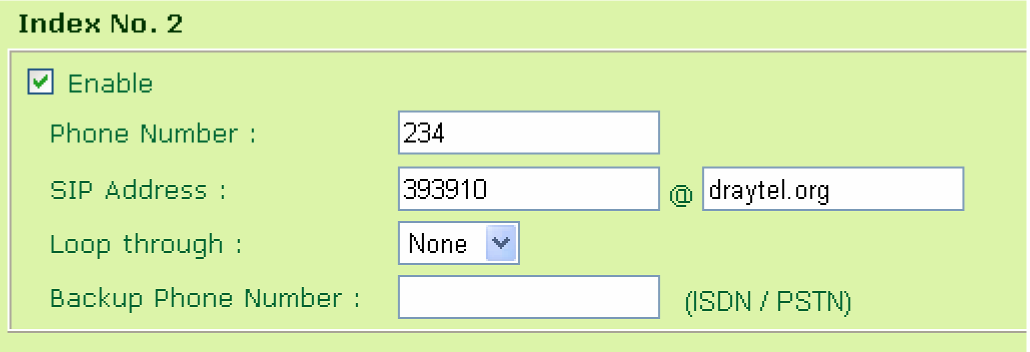
☑ Enable

Phone Number : 12

SIP Address : 63065 @ fwd.pulver.com

Loop through : None

Backup Phone Number : (ISDN / PSTN)



Index No. 2

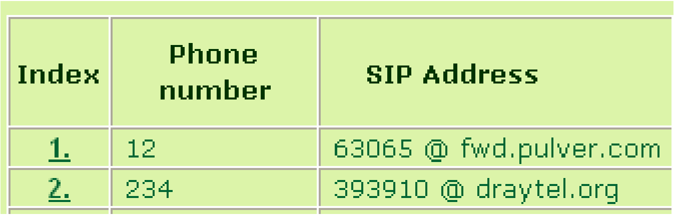
☑ Enable

Phone Number : 234

SIP Address : 393910 @ draytel.org

Loop through : None

Backup Phone Number : (ISDN / PSTN)



Index	Phone number	SIP Address
1.	12	63065 @ fwd.pulver.com
2.	234	393910 @ draytel.org

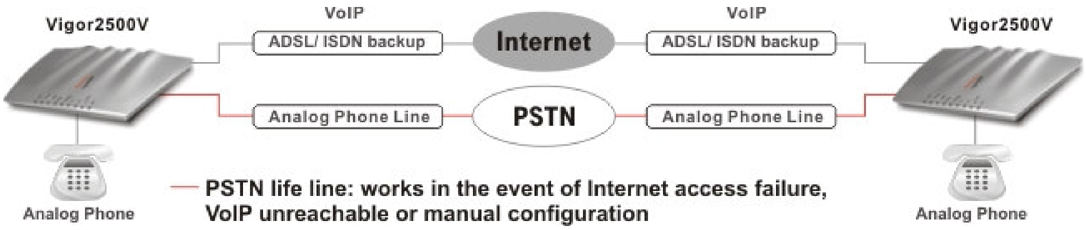
Enable: Tick this to enable this entry.

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*

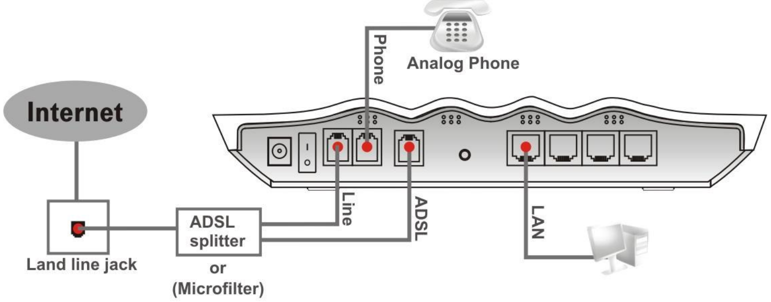
SIP Address: Enter the SIP address of your contact (e.g. 98141@draytel.org)

Loop Through: The Vigor2500V has a “Line” port on the rear panel for connecting to a PSTN (regular analogue) line. The Loop Through option can be used to set an alternate telephone number for your contact on the PSTN, which the Vigor2500V will dial instead of the SIP account if you lose ADSL access or power to the Vigor2500V. Hence, the PSTN line can act as a lifeline (backup mechanism) for VoIP calls. The lifeline mechanism is activated automatically but can also be manually configured.

Because there is ISDN interface on the Vigor2500Vi series, you can use the ISDN line as phone line as well as Internet remote access/dial back-up for ADSL. You will be able to still make ISDN phone calls if the router loses power or the VoIP calls can not make as Internet access is broken. Hence, the ISDN line can also be lifeline (backup mechanism) for VoIP calls.

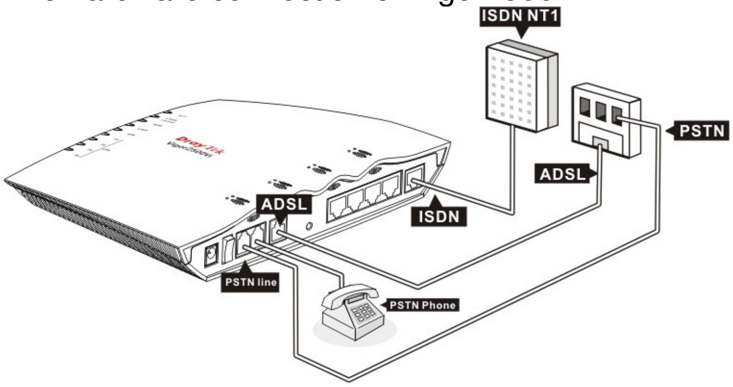


The hardware connection of Vigor2500V:



In most AnnexA (ADSL over POTS) countries, the subscription of ADSL and the subscription of ISDN is separate. The Vigor2500V is highly recommended to those who only subscribe the ADSL broadband access.

The hardware connection of Vigor2500Vi:

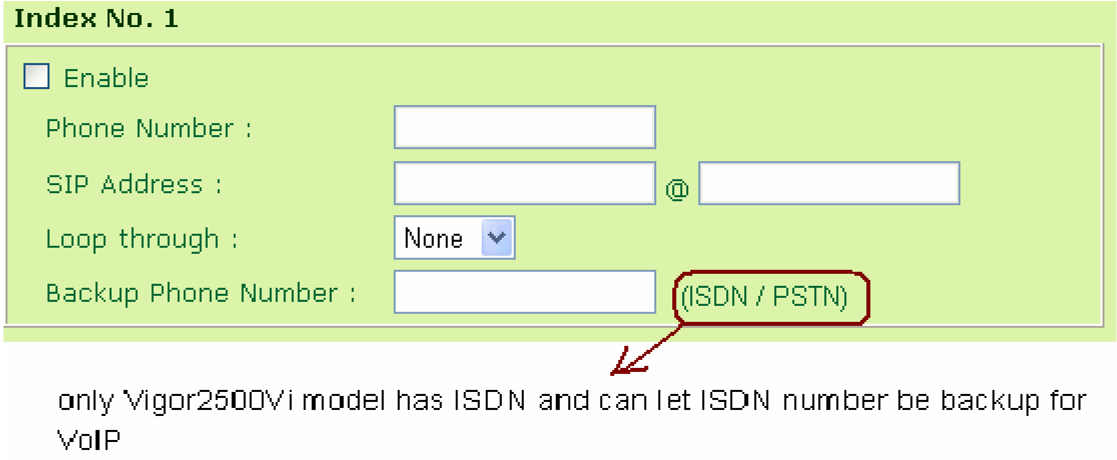


In Annex B (ADSL over ISDN) countries, the subscription of ADSL will let you get the ADSL line box and ISDN NT1 from Telco/or ISP. The Vigor2500Vi will be ideal product for you when you already have ADSL and ISDN. We let users of AnnexB environment can fully utilize ISDN line because Vigor2500Vi has ISDN interface.

If your ADSL environment is Annex A, you can still additionally subscribe ISDN line as backup/remote access. Or, you already had ISDN Internet access before you subscribe ADSL internet access. Hence, the Vigor2500Vi will be much suitable for you.

Vigor2500V: highly recommended to those who only have ADSL line
Vigor2500Vi: highly recommended to those who already have ADSL line and ISDN line. Or, you plan to additionally subscribe ISDN line.

Backup Phone Number: The alternate PSTN/or ISDN number (only Vigor2500Vi model has ISDN and can let ISDN number be backup for VoIP) to dial if "PSTN phone number" or "ISDN phone number" is set in **Loop Through entry**.



Index No. 1

☐ Enable

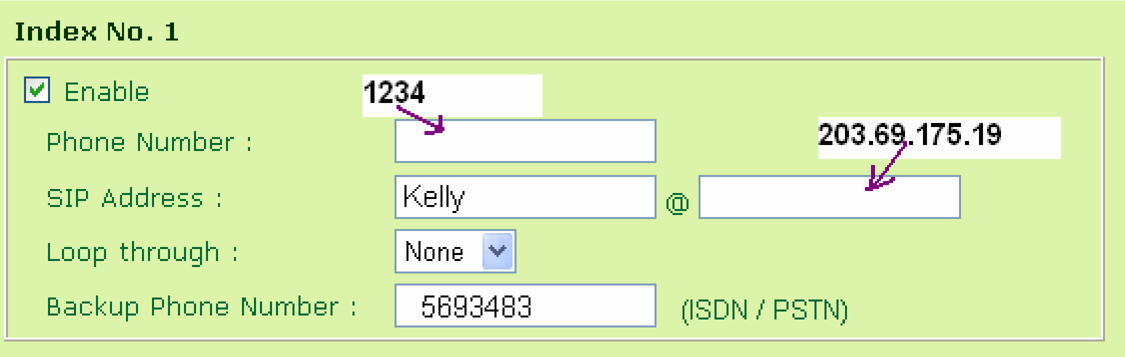
Phone Number :	
SIP Address :	@
Loop through :	None
Backup Phone Number :	(ISDN / PSTN)

only Vigor2500Vi model has ISDN and can let ISDN number be backup for VoIP

Even your home has the ISDN line and you get ISDN phone number, you can not set the ISDN phone number into **Backup Phone Number** entry if your model is Vigor2500V which has no ISDN port for connecting to your ISDN NT1 which is installed by ISP or Telco. If you want to run ISDN phone number as backup line for VoIP calls, you shall purchase Vigor2500Vi series which has ISDN interface..

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. For **ISDN network, the manual key shall be "#9"** as your model is Vigor2500Vi.

Example 2:
If Kelly gives you her SIP Address as **kelly@203.69.175.19 and PSTN number is 5693483** then you can enter the DialPlan as:



Index No. 1

☑ Enable

Phone Number : 1234

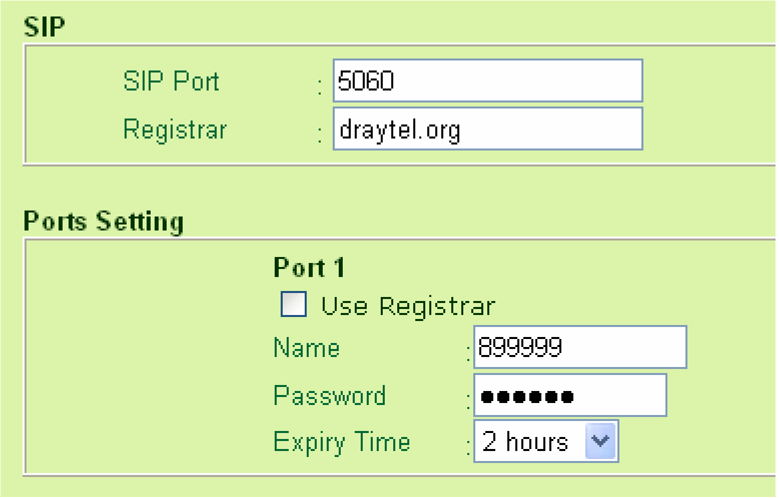
SIP Address : Kelly @ 203.69.175.19

Loop through : None

Backup Phone Number : 5693483 (ISDN / PSTN)

Example 3:
If David give you his IP address 203.69.175.16 only, and it is not in your DialPlan, you still can press keypad on the phone to dial as **#203*69*175*16#**

12.2.2 SIP Related Function Setup



SIP

SIP Port : 5060

Registrar : draytel.org

Ports Setting

Port 1

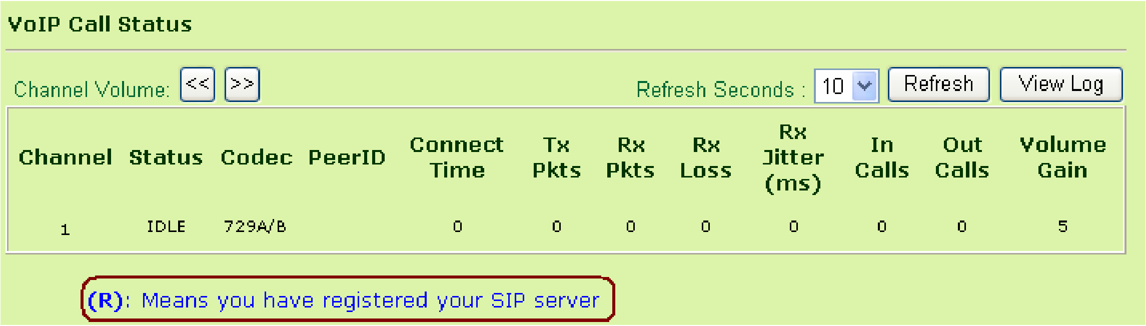
☐ Use Registrar

Name : 899999

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 Call Status

Refresh Seconds : 10

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Loss	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1	IDLE	729A/B		0	0	0	0	0	0	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.

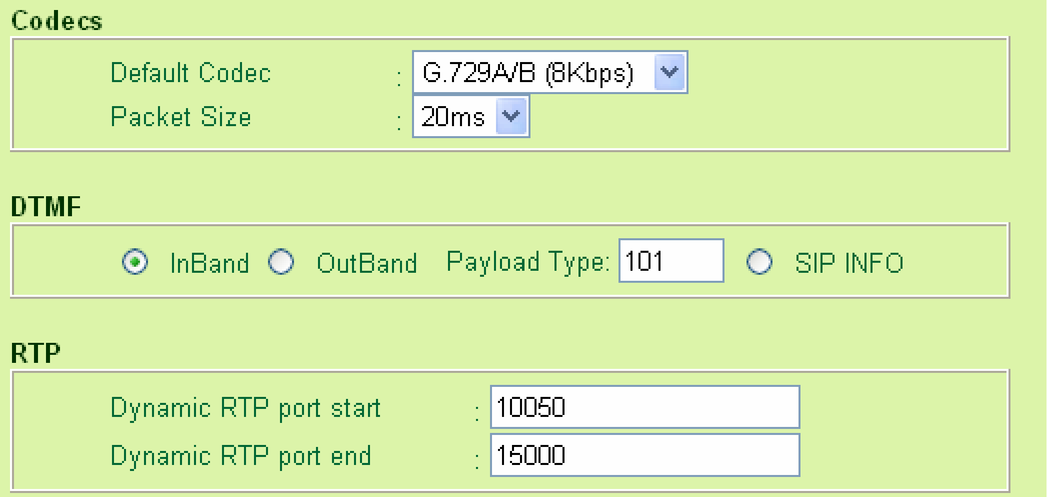
Use Registrar: With the Registrar domain entered above, check this box to let the Vigor2500V use the SIP Registrar.

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

Password: Your SIP 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.

12.2.3 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.

12.3 Calling Scenario

12.3.1 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: **203.69.175.19**

A. Arnor's settings

A-1. DialPlan index 1

Phone Number**: 1234**
(any number you like)
Name**: paulin**
IP Address / Domain**: 203.69.175.19**

A-2. SIP Related Function

SIP Port**: 5060**
Registrar**: (leave blank)**
Port 1:
Use Register**: (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**
Registrar**: (leave blank)**
Port 1:
Use Register**: (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#**

12.3.2 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 Register**: (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**: 5060**
Registrar**: draytel.org**

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

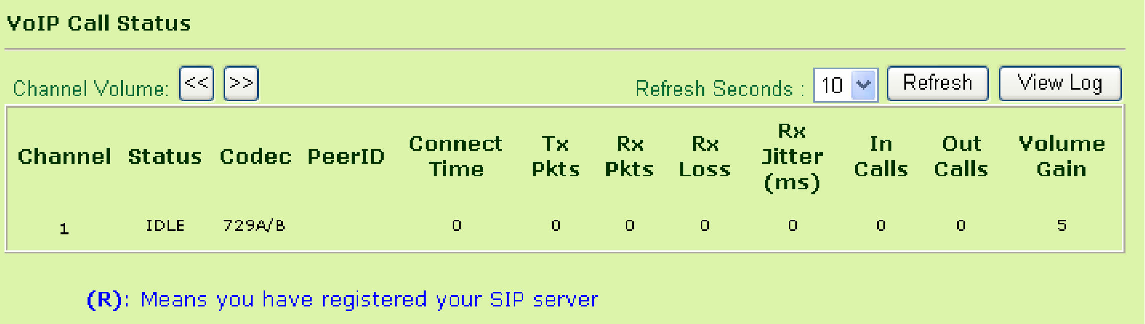
B-3. CODEC/RTP/DTMF

(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#**

12.4 Voice Call Status



VoIP Call Status

Channel Volume: << >>

Refresh Seconds : 10

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Loss	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1	IDLE	729A/B		0	0	0	0	0	0	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).
COLLECTING **:** 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.

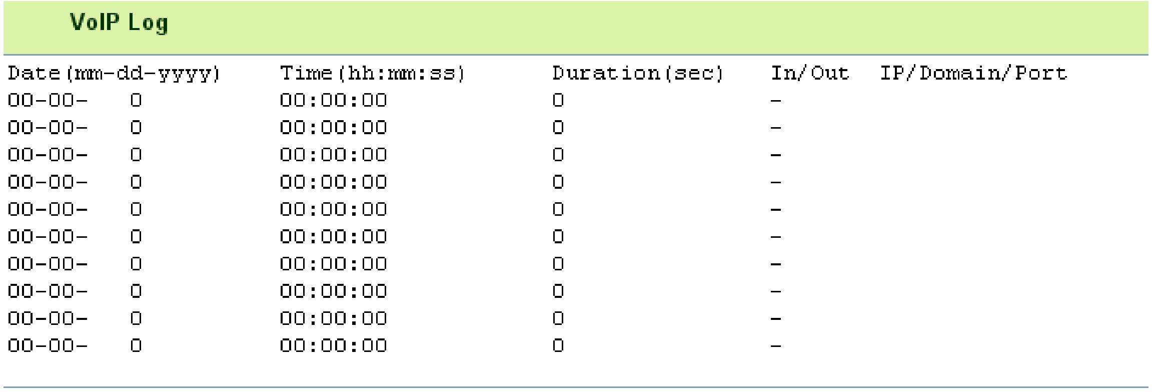
Rx Jitter: The jitter of received voice packets.

In Calls: The accumulating in-call times.

Out Calls: The accumulating out-call times.

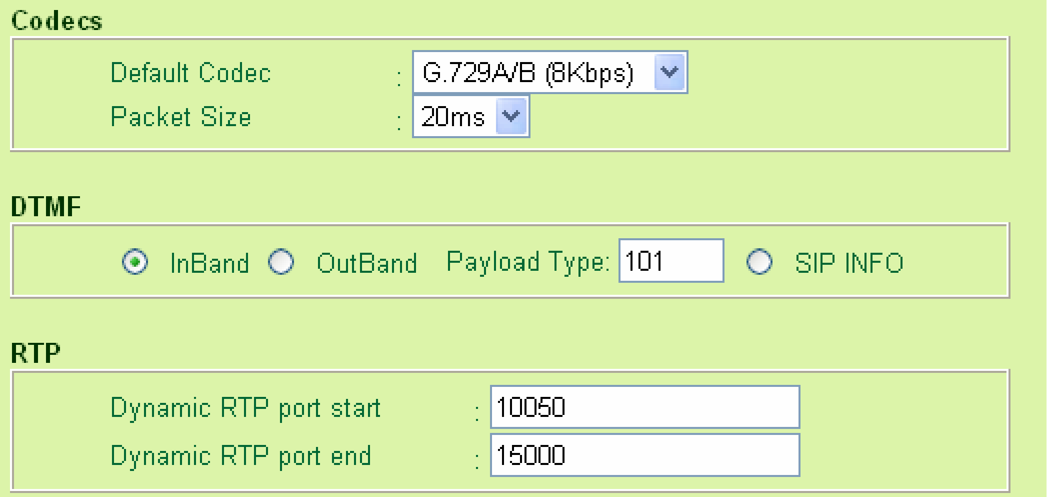
Volume Gain: The volume of present call.

View Log: To show the logs of VoIP calls as below.



```
Date(mm-dd-yyyy)    Time(hh:mm:ss)       Duration(sec)   In/Out  IP/Domain/Port
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
00-00-   0          00:00:00             0               -
```

12.2.3 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.

12.3 Calling Scenario

12.3.1 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: **203.69.175.19**

A. Arnor's settings

A-1. DialPlan index 1

Phone Number**: 1234**
(any number you like)
Name**: paulin**
IP Address / Domain**: 203.69.175.19**

A-2. SIP Related Function

SIP Port**: 5060**
Registrar**: (leave blank)**
Port 1:
Use Register**: (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**
Registrar**: (leave blank)**
Port 1:
Use Register**: (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#**

12.3.2 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 Register**: (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**: 5060**
Registrar**: draytel.org**

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

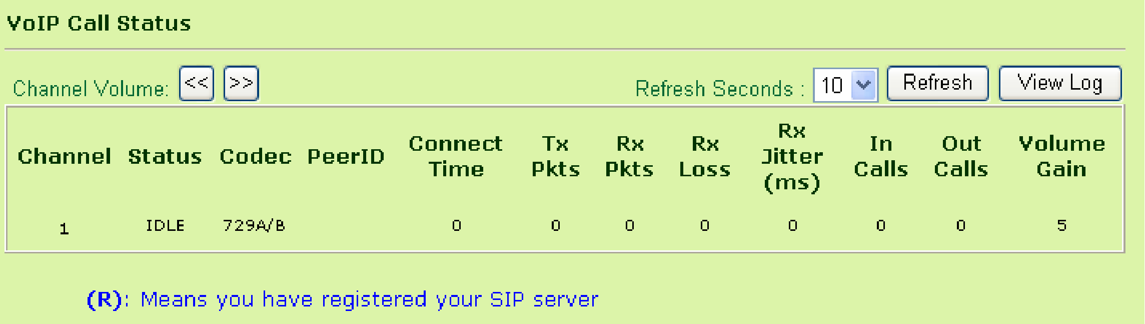
B-3. CODEC/RTP/DTMF

(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#**

12.4 Voice Call Status



VoIP Call Status

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Loss	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1	IDLE	729A/B		0	0	0	0	0	0	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).
COLLECTING : 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.

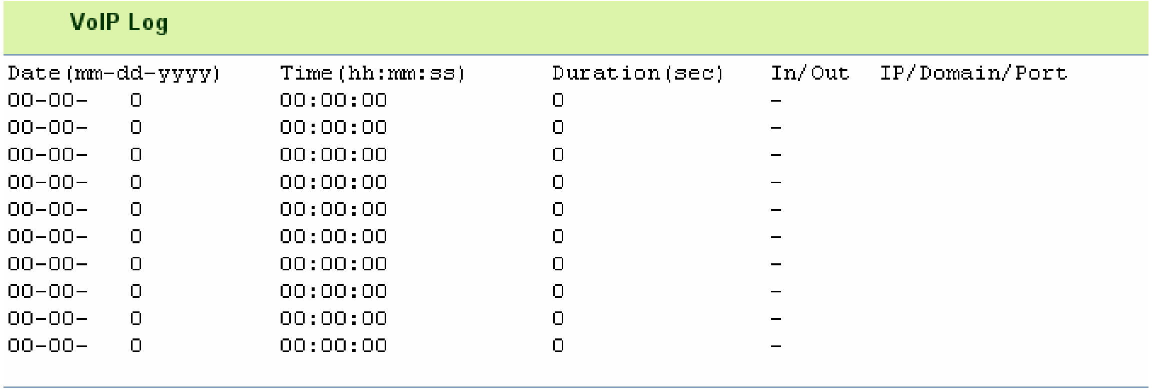
Rx Jitter: The jitter of received voice packets.

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.

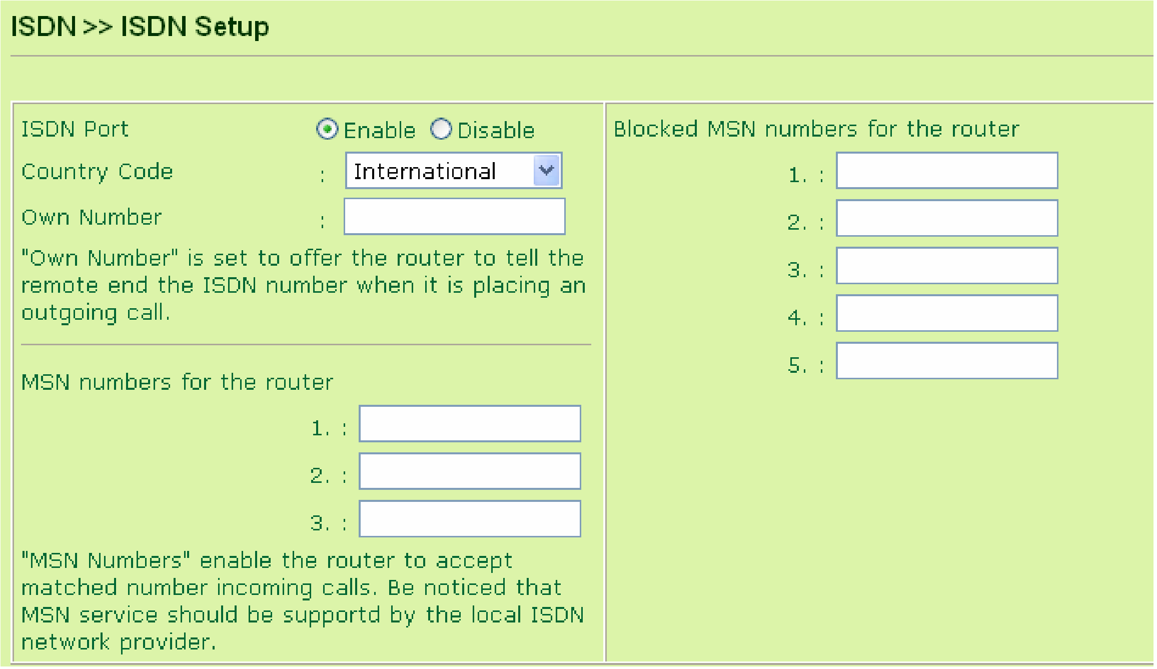


```
Date(mm-dd-yyyy)     Time(hh:mm:ss)       Duration(sec)    In/Out   IP/Domain/Port
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
00-00-    0          00:00:00             0                -
```

Chapter 13
ISDN Setup

13.1 Introduction

In this chapter, we focus on the explanation of the **ISDN Setup.** The following content is suitable for **ISDN model** only.



ISDN >> ISDN Setup

ISDN Port ● Enable ○ Disable

Country Code : International

Own Number :

"Own Number" is set to offer the router to tell the remote end the ISDN number when it is placing an outgoing call.

MSN numbers for the router

1. :
2. :
3. :

"MSN Numbers" enable the router to accept matched number incoming calls. Be noticed that MSN service should be supportd by the local ISDN network provider.

Blocked MSN numbers for the router

1. :
2. :
3. :
4. :
5. :

13.2 Configuring the ISDN Interface

ISDN Port: Click **Enable** to turn on the ISDN port, **Disable** to turn off.

Country Code: For proper operation on your local ISDN network you should set the correct country code.

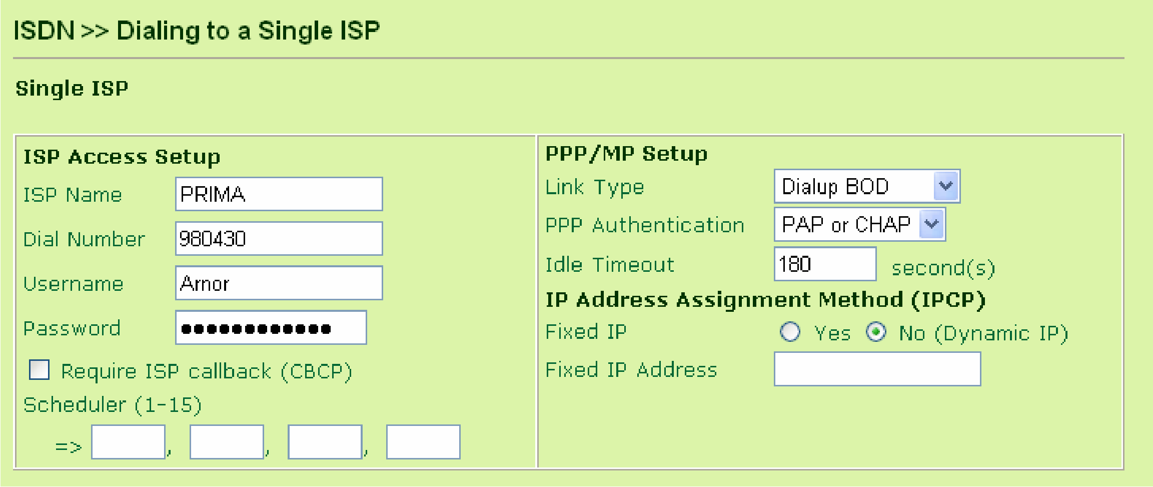
Own Number: Sets your ISDN number. If the field has been configured, every outgoing call will carry the number to the called user.

MSN Numbers for the Router: MSN Numbers means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by local ISDN network provider. The router provides three MSN number fields. Note that MSN services must be subscribed for from your local telecom.
By default, MSN function is disabled. Leave the MSN number fields blank, under which all incoming calls will be accepted without number matching.

DrayTek provides the **Remote Activation** facility for the teleworkers who have subscribed ISDN Internet and would like to dial in to the head office . Through the **Remote Activation** facility, a teleworker can make a phone call to the router at the head office and ask the router to dial up to the ISP. As a result, the teleworkers can be authorized with their office account for utilizing ISDN dial-up services and the said office can utilize ISDN LAN-to-LAN for secured communications and efficient work.

The ISDN interface on Vigor2500Vi series supports the **VTA** (**Virtual Terminal Adapter**) facility. The VTA offers a "CAPI" software interface, similar to that which an actual ISDN terminal adapter installed on your PC. You can install CAPI-compliant software for dial-up networking, fax or voice activities – relying on the capabilities of your adopted CAPI software. To use the VTA facility, please download VTA drivers (available only for Windows 98SE/2000/XP) from http://www.draytek.com/english/support/download.php .

13.3 Dialing to a Single ISP



ISDN >> Dialing to a Single ISP

Single ISP

ISP Access Setup

ISP Name: PRIMA

Dial Number: 980430

Username: Arnor

Password: ●●●●●●●●●●●●●

☐ Require ISP callback (CBCP)

Scheduler (1-15)

=> __, __, __, __

PPP/MP Setup

Link Type: Dialup BOD

PPP Authentication: PAP or CHAP

Idle Timeout: 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP: ○ Yes ● No (Dynamic IP)

Fixed IP Address:

ISP Access Setup

ISP Name: Enter your ISP name.

Dial Number: Enter the ISDN access number provided by your ISP.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

***Require ISP Callback* (*CBCP*)**: If your ISP supports the callback function, click this checkbox to activate the Callback Control Protocol during PPP negotiation.

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

PPP/MP Setup

Link Type: There are four link types: Link Disable, Dialup 64 Kbps, Dialup 128 Kbps, and Dialup BOD.

Link Disable: Disable the ISDN dial-out function.

Dialup 64Kbps: Use one ISDN B channel for Internet access.

Dialup 128Kbps: Use both ISDN B channels for Internet access.

Dialup BOD: BOD stands for bandwidth-on-demand. The router will use only one B channel under low traffic situations. Once the single B channel bandwidth is filled, the other B channel will be dialed automatically. For more detailed BOD parameter settings, refer to the **Advanced Setup** group > **Call Control and PPP/MP Setup**.

***PPP Authentication*:**

PAP Only: Set the PPP session to use the PAP protocol to negotiate the username and password with the ISP.

PAP or CHAP: Set the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.

***Idle Timeout*:**

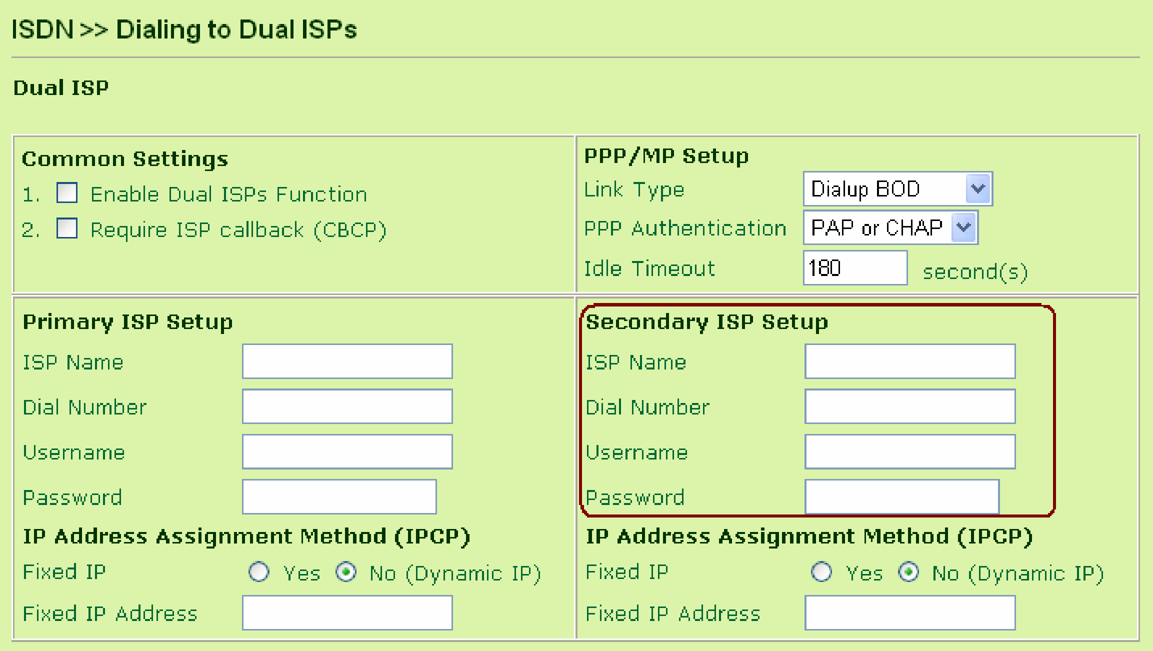
Idle timeout means the router will disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection will remain always connected to the ISP.

IP Address Assignment Method (IPCP)

***Fixed IP, and Fixed IP Address*:**

In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of Fixed IP Address.

13.4 Dialing to Dual ISPs



ISDN >> Dialing to Dual ISPs

Dual ISP

Common Settings

1. ☐ Enable Dual ISPs Function
2. ☐ Require ISP callback (CBCP)

PPP/MP Setup

Link Type: Dialup BOD

PPP Authentication: PAP or CHAP

Idle Timeout: 180 second(s)

Primary ISP Setup

ISP Name

Dial Number

Username

Password

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

Secondary ISP Setup

ISP Name

Dial Number

Username

Password

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

Most configuration parameters are the same as that in the last section. This page provides a checkbox to enable the Dual ISPs Function and adds a secondary ISP Setup section. Check the corresponding box and enter the second ISP information. The setup page is depicted above.

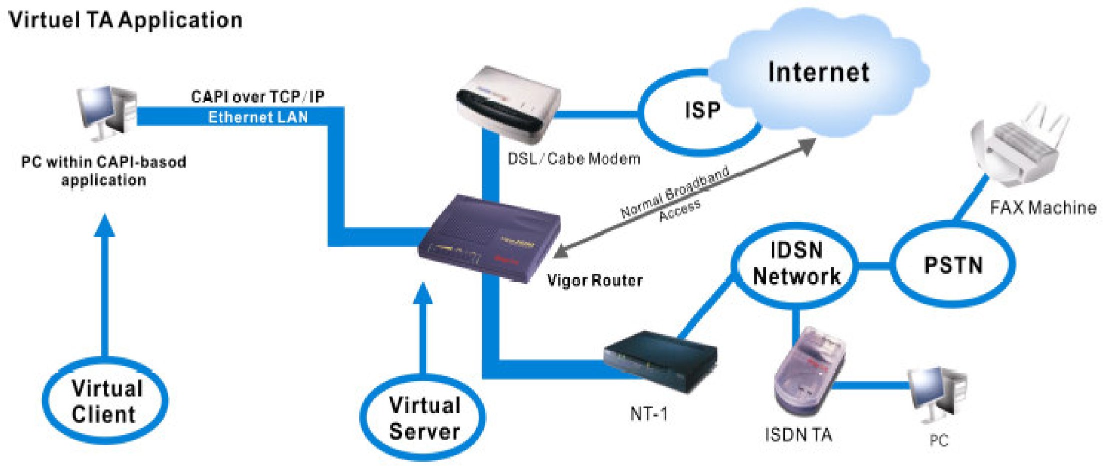
Chapter 14
Virtual TA (Remote CAPI)

14.1 Introduction

This chapter is only applied to Vigor2500Vi series models which have the **ISDN interface** and the **Virtual TA** facilities are available. Our Virtual TA facilities can be available from bundled firmware CD and www.draytek.com/support ..

The term **Virtual TA** means the local Ethernet-connected hosts or PCs use popular CAPI-based software such as RVS-COM or BVRP etc. to access the router as a local ISDN TA for FAX sending or receiving via the ISDN line. Basically, it is a client/server network model. The Virtual TA server built into the router handles the connection establishment and release. The Virtual TA client, installed in the Ethernet-connected host, creates a CAPI-based driver to relay all CAPI messages between applications and the router CAPI module. Before describing the configuration of **Virtual TA** in the Vigor routers, please mention the following limitations.

1. The Virtual TA client is only supported on Microsoft™ Windows 95 OSR2.1/98/98SE/Me/2000 platforms.
2. The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
3. One ISDN BRI interface only has two B channels. The maximum number of active clients is also 2.
4. Before you set up the Virtual TA, you must set the correct country code. Click **ISDN Setup** in the **ISDN** group.



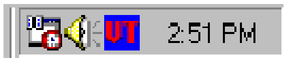
As depicted in the following application chart, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA etc. Use the following setup link on the Setup Main Menu to configure the Virtual TA facility.

ISDN > Virtual TA (Remote CAPI)

14.2 Install a Virtual TA Client

1. Insert the CD-ROM supplied with your Vigor router, or directly double-click the installer file. Vsetup95.exe is for Windows 95 OSR2.1 or higher, Vsetup98.exe is for Windows 98, 98SE and Me, and Vsetup2k.exe is for Windows 2000.
2. Follow on-screen instructions of the installer. The last step requires you to restart your computer. Click **OK** to restart.
3. After the computer restarts, you will see a VT icon on the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.

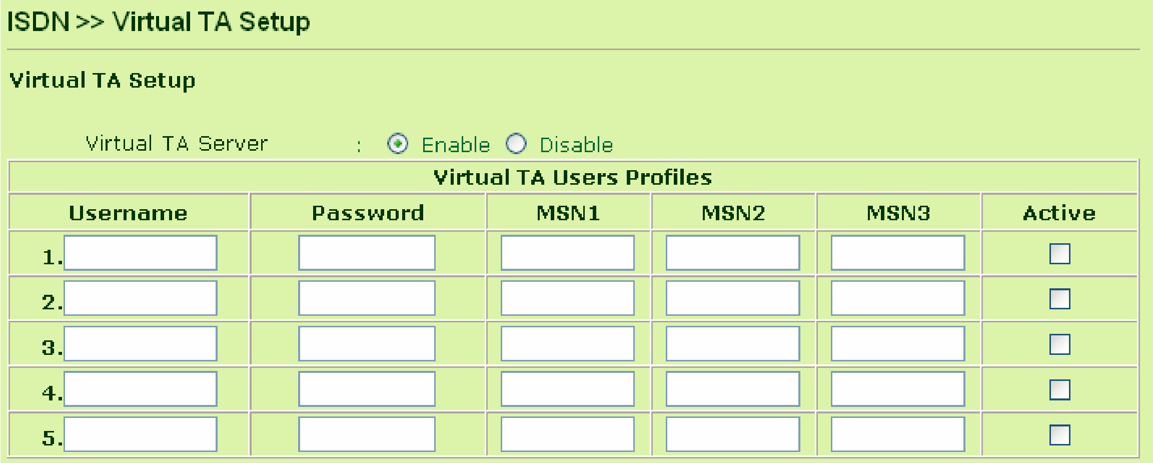
When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Read your software user guide for detailed configuration. If the icon text is RED, it means the client lost the connection with the server. Check the physical Ethernet connection.



14.3 Configure a Virtual TA Client/ Server

The Virtual TA application is a client/server model. You must set it up on both ends to operate properly your Virtual TA application.

By default, the Virtual TA server is enabled and the Username/Password fields are empty. Any Virtual TA client may login to the server. Once a single Username/Password field has been filled, the Virtual TA server will only allow clients with a valid Username/Password to login. The web configuration of Virtual TA Setup is shown below.



ISDN >> Virtual TA Setup

Virtual TA Setup

Virtual TA Server : ● Enable ○ Disable

Virtual TA Users Profiles

Username	Password	MSN1	MSN2	MSN3	Active
1.					☐
2.					☐
3.					☐
4.					☐
5.					☐

Virtual TA Server

Enable: Check it to activate the server.

Disable: Check it to deactivate the server. All Virtual TA applications will be stopped.

Virtual TA User Profiles

Username: Specify the username for a specific client.

Password: Specify the password for a specific client.

MSN1, MSN2, MSN3: MSN stands for Multiple Subscriber Number. It means you can subscribe to more than one ISDN line number on a single subscribed line. Note that the service must be subscribed to with your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field to be empty.

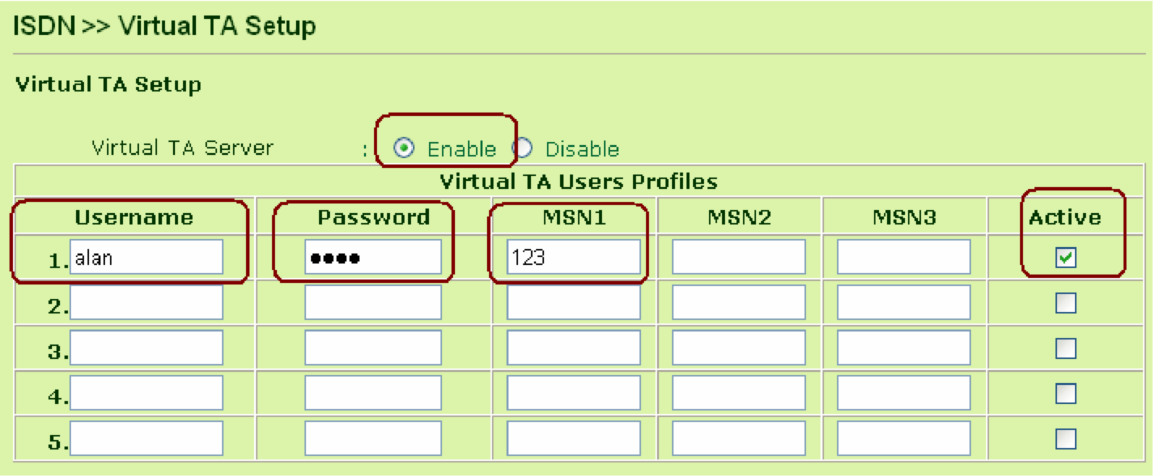
Active: Check it to enable the client for accessing the server.

Creating a User Profile

Note that creating a single user access account limits access to the Virtual TA server to only the specified account holders.

In the following, we assume you have no MSN service from your ISDN network provider.

1. On the server: Click **Virtual TA (Remote CAPI) Setup**, and fill in the Username and Password fields. Click the **Active** checkbox to enable the account.



ISDN >> Virtual TA Setup

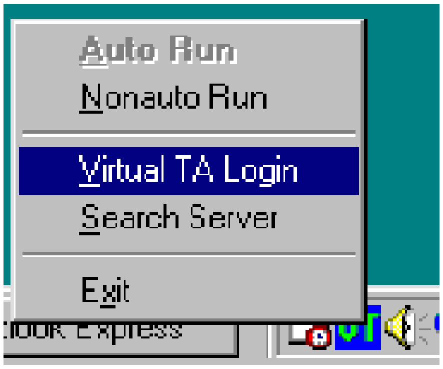
Virtual TA Setup

Virtual TA Server : ● Enable ○ Disable

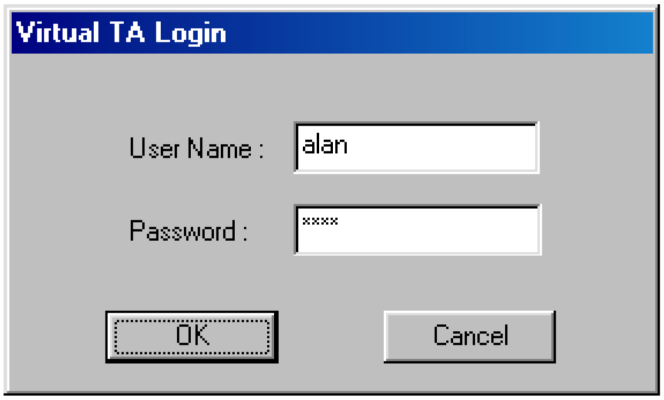
Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	●●●●	123			☑
2.						☐
3.						☐
4.						☐
5.						☐

2. On the client: Right-click the mouse on the VT icon. The following pop-up menu will be shown.



3. Click the **Virtual TA Login** to open the login box.



User Name : alan

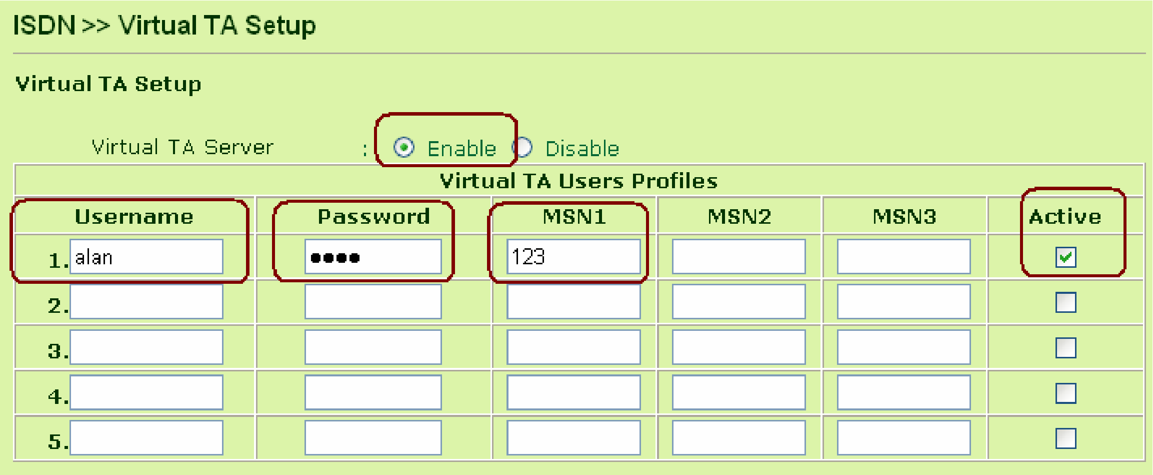
Password : ****

4. Enter the Username/Password and then click **OK**. After a short time, the VT icon text will become green server.

Configuring the MSN number

If you have subscribed to an MSN number service, the Virtual TA server can specify which client has the specified MSN number. When an incoming call arrives, the server will alert the Username-Password-matched and MSN-matched client. In the following, we use an example to explain the configuration of the MSN number.

1. Suppose that you could assign the MSN number **123** to the "alan" client.



ISDN >> Virtual TA Setup

Virtual TA Setup

Virtual TA Server : ● Enable ○ Disable

Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	●●●●	123			☑
2.						☐
3.						☐
4.						☐
5.						☐

2. Set the specified MSN number in the CAPI-based software. When the Virtual TA server sends an alert signal to the specified Virtual TA client, the CAPI-based software will also receive the alert signal. If the MSN number is incorrect, the software will not accept the incoming call.

Chapter 15
Call Control and PPP/MP Setup

15.1 Introduction

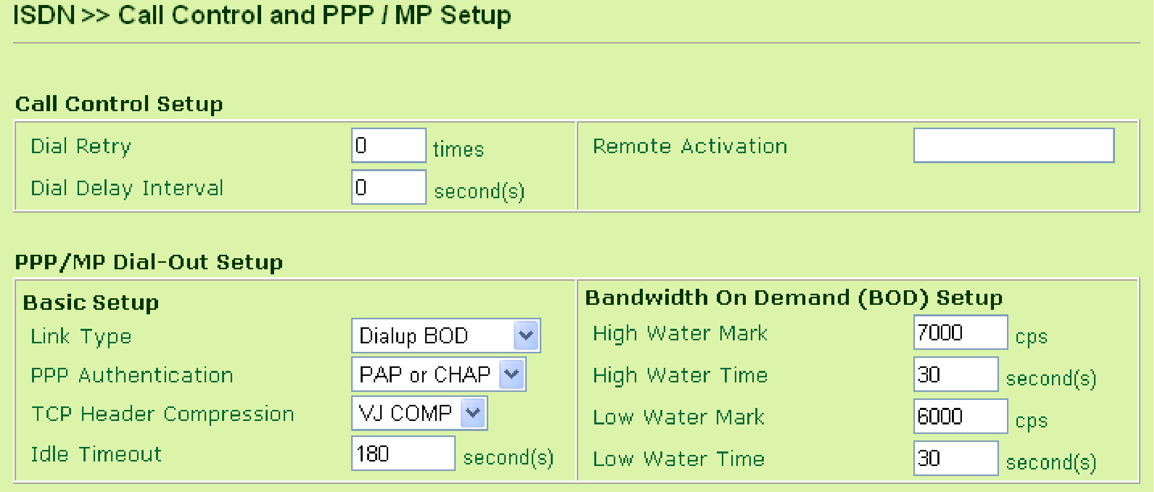
Some applications require that the router (only for ISDN model) could be remotely activated, or dial up to the ISP using the ISDN interface. For instance, if you want to access the Internet via ISDN from home, usually the dialup connection is idle when you are not at home. It may be that, while working in the office, you want to get some files from home. Hence, the Vigor routers provide this function that allows you to make a phone call to the router and then ask it to dial up to the ISP. Accordingly, you can access your home network to retrieve the files. Of course, you should have a fixed IP address and expose some internal network resources to outside world, for example FTP, WWW and so on.

In the following, we explain how to setup call control and PPP/MP in Advanced Setup. You can use the following setup link on the Setup Main Menu to configure it. **ISDN > Call Control and PPP/MP Setup**.

The Call Control and PPP/MP are only available on the ISDN interface of Vigor2500Vi series. This chapter is not applied to Vigor2500V which does not have ISDN interface.

15.2 Configuration

After you click Call Control and PPP/MP Setup. The following screen will automatically appear on your browser.



ISDN >> Call Control and PPP / MP Setup

Call Control Setup

Dial Retry 0 times

Dial Delay Interval 0 second(s)

Remote Activation

PPP/MP Dial-Out Setup

Basic Setup

Link Type Dialup BOD

PPP Authentication PAP or CHAP

TCP Header Compression VJ COMP

Idle Timeout 180 second(s)

Bandwidth On Demand (BOD) Setup

High Water Mark 7000 cps

High Water Time 30 second(s)

Low Water Mark 6000 cps

Low Water Time 30 second(s)

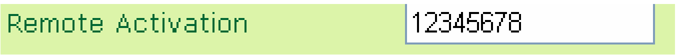
Call Control Setup:

On the **Call Control and PPP/MP Setup** setup page, you will see **Dial Retry** and **Dial Delay Interval**. These two parameters set global settings for ISDN dialup access.

Dial Retry: Specify the dial retry counts per triggered packet. A triggered packet is any packet whose destination is outside the local network. The default setting is no dial retry. If set to 5, for each triggered packet, the router will dial 5 times until it is connected to the ISP or remote access router.

Dial Delay Interval: Specify the interval between dialup retry. By default, the interval is 0 seconds.

Remote Activation: Specify a phone number in the Remote Activation field to enable the remote activation function. If the router accepts a call from the number 12345678, it will disconnect the incoming call immediately and dial to the pre-specified ISP.



Remote Activation 12345678

Internet Access Setup > **Dialing to a Single ISP** should be pre-set properly.

PPP/MP Dial-Out Setup

Basic Setup :

Link Type: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD

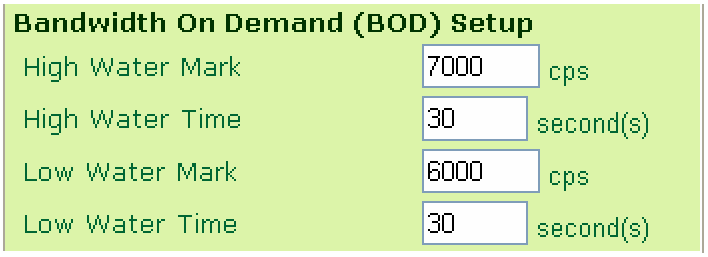
PPP Authentication: Specify the PPP authentication method for PPP/MP connection. Normally set to **PAP/CHAP** for the widest compatibility.

TCP Header Compression: **VJ Compression** is used for TCP/IP protocol header compression. Normally activate **VJ Compression** to improve bandwidth utilization.

Idle Timeout: The ISDN connection will be dropped once there is no further data traffic within the specified duration.

BOD Setup :

BOD stands for bandwidth-on-demand for Multiple-Link PPP (ML-PPP or MP). The corresponding parameters are shown below.



Bandwidth On Demand (BOD) Setup

High Water Mark	7000	cps
High Water Time	30	second(s)
Low Water Mark	6000	cps
Low Water Time	30	second(s)

These parameters are activated when you set the **Link Type** to **Dialup BOD**. Usually the ISDN will use one B channel to access the Internet or remote network when you use the Dialup BOD link type. The router will use the parameters here to make a decision on when you activate/drop the additional B channel. Note that **cps** (characters-per-second) measures the total link utilization.

High Water Mark and High Water Time: These parameters specify the condition that the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).

Low Water Mark and Low Water Time: These parameters specify the condition for dropping the second channel. Considering the two B channels, if their utilization is under the Low Water Mark and these two channels are used over the High Water Time, the additional channel will be dropped. As a result, the link speed will be 64kbps (one B channel).

If you are not sure whether your ISP can support BOD and/or ML-PPP's operations, please firstly get advice from your ISP or local dealers or support@draytek.com .

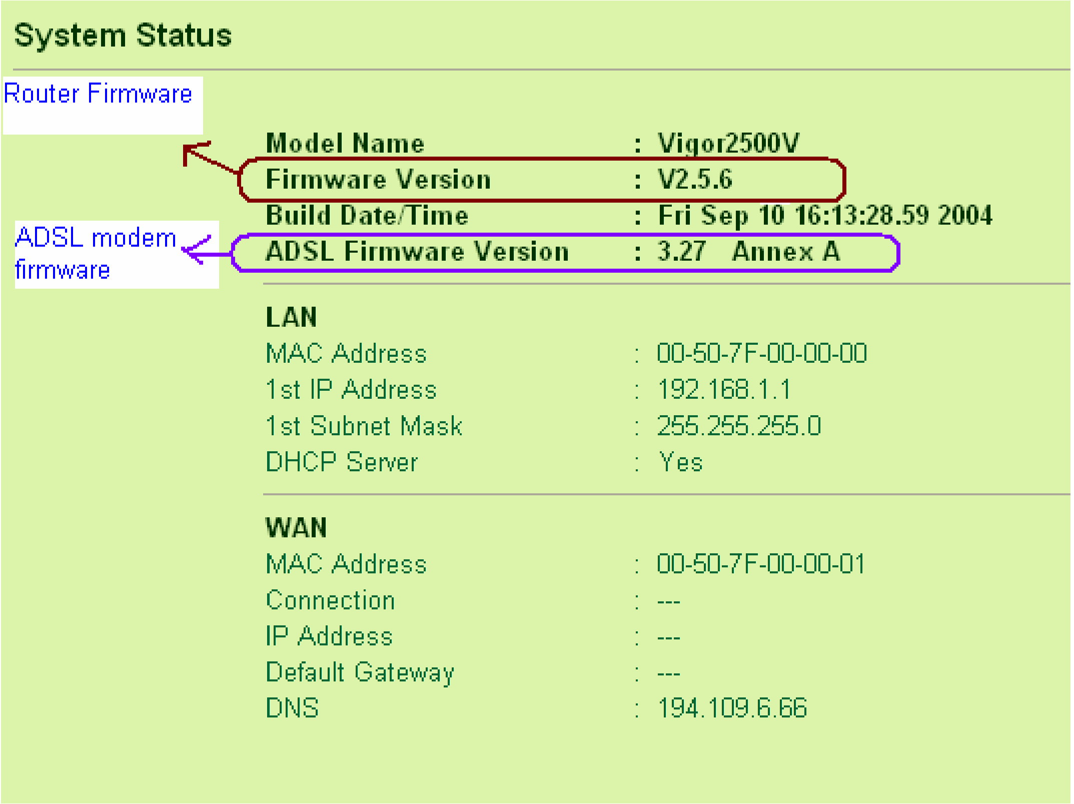
Chapter 16
System Status

16.1 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.

16.2 Online Status Descriptions

Go to the **System Maintenance > Online Status** and you will see the result shown on the right frame. The below figure is a demoed by Vigor 2500V.



System Status

Router Firmware

ADSL modem firmware

Model Name	:	**Vigor2500V**
Firmware Version	:	**V2.5.6**
Build Date/Time	:	**Fri Sep 10 16:13:28.59 2004**
ADSL Firmware Version	:	**3.27 Annex A**

LAN

MAC Address	:	00-50-7F-00-00-00
1st IP Address	:	192.168.1.1
1st Subnet Mask	:	255.255.255.0
DHCP Server	:	Yes

WAN

MAC Address	:	00-50-7F-00-00-01
Connection	:	---
IP Address	:	---
Default Gateway	:	---
DNS	:	194.109.6.66

Chapter 17
Configuration Backup

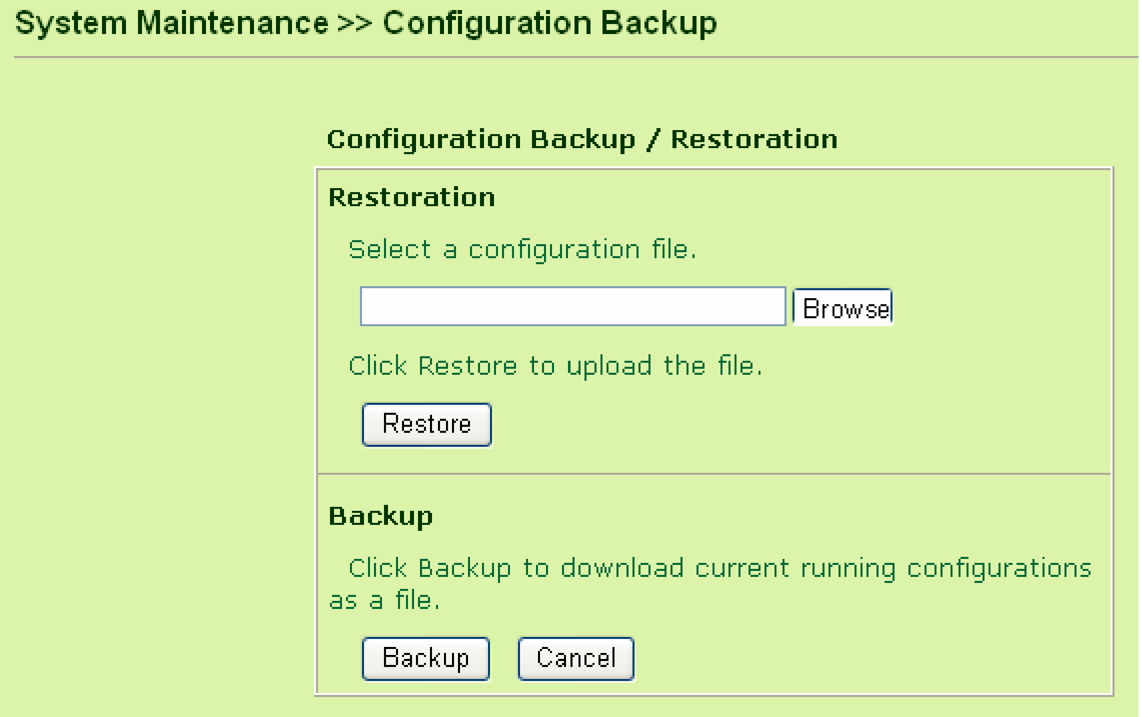
17.1 Introduction

Sometimes you want 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.

17.2 Usage

17.2.1 Backup the Running Configuration

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



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

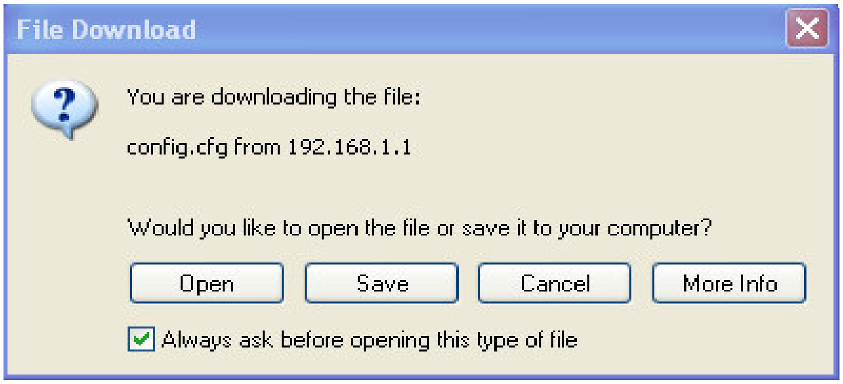
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

2. Click **Backup** button to get configurations.



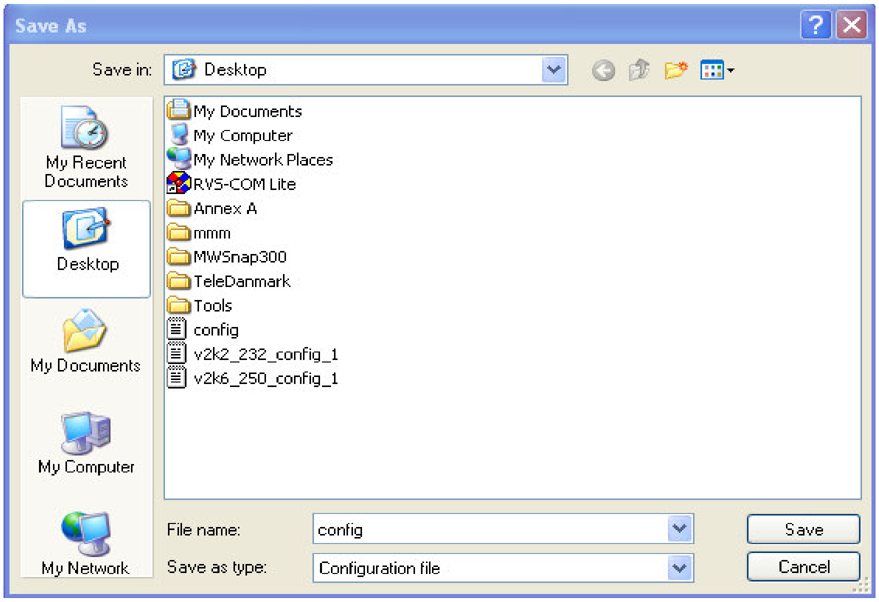
You are downloading the file:

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 in: Desktop

File name: config

Save as type: Configuration file

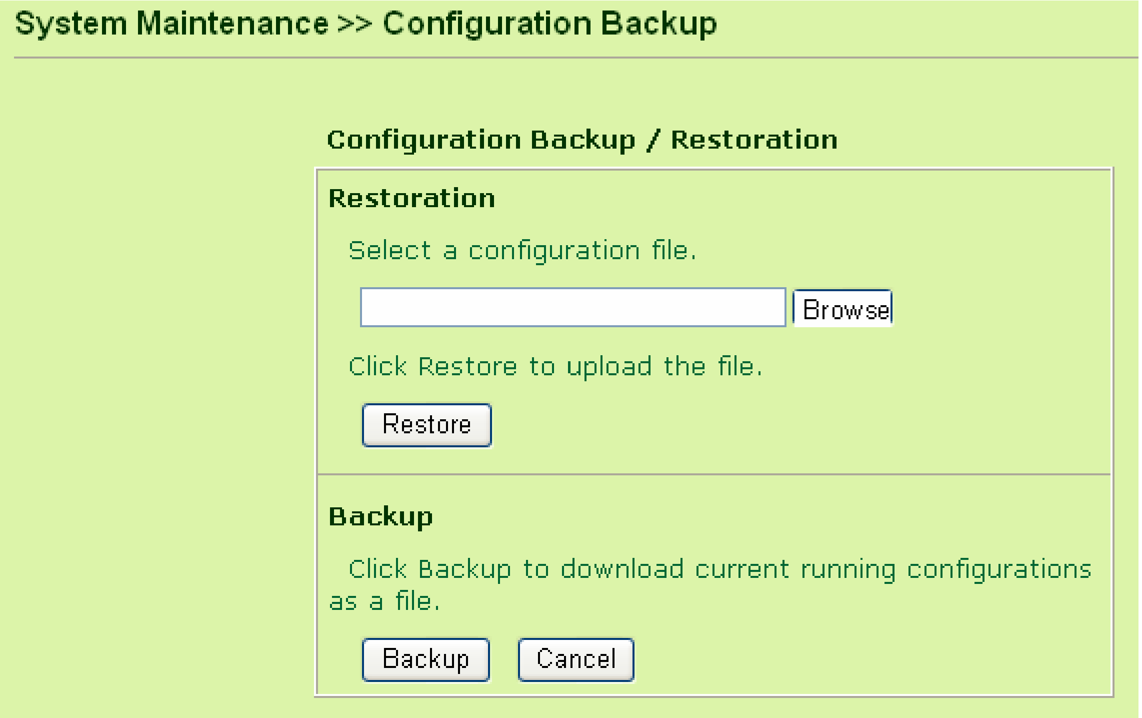
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.

17.2.2 Restore the Configuration with a Configuration File

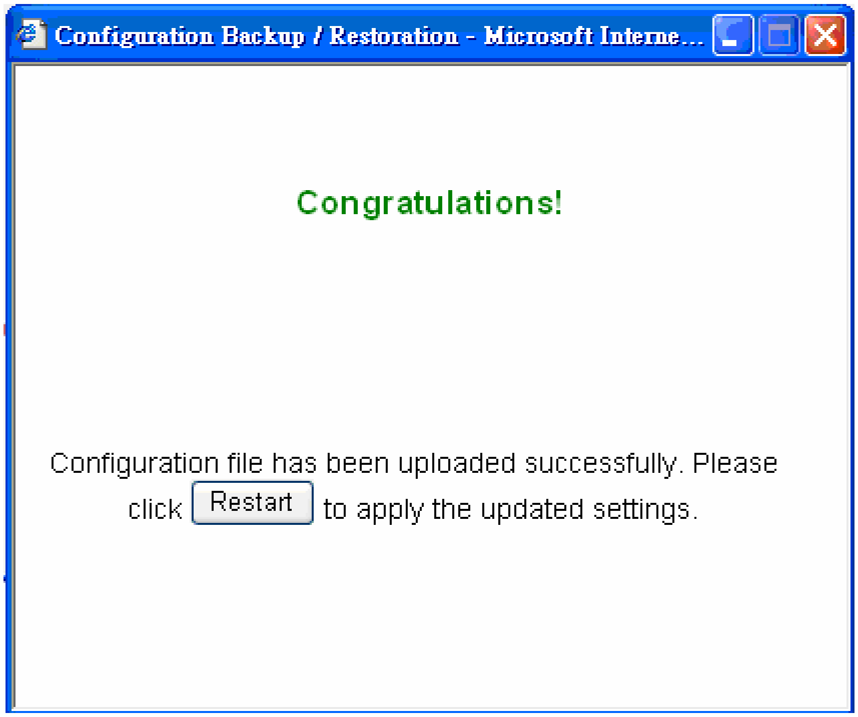
1. Go to **System Maintenance** > **Configuration Backup**. The following windows will be popped-up, as shown below.

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


System Maintenance >> Configuration Backup
Configuration Backup / Restoration
Restoration
Select a configuration file.
Browse
Click Restore to upload the file.
Restore
Backup
Click Backup to download current running configurations as a file.
Backup
Cancel

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

4. Click **Restart** button and wait for few seconds, the router will restart by using the updated configurations.



Congratulations!

Configuration file has been uploaded successfully. Please click Restart to apply the updated settings.

Chapter 18
SysLog / Mail Alert

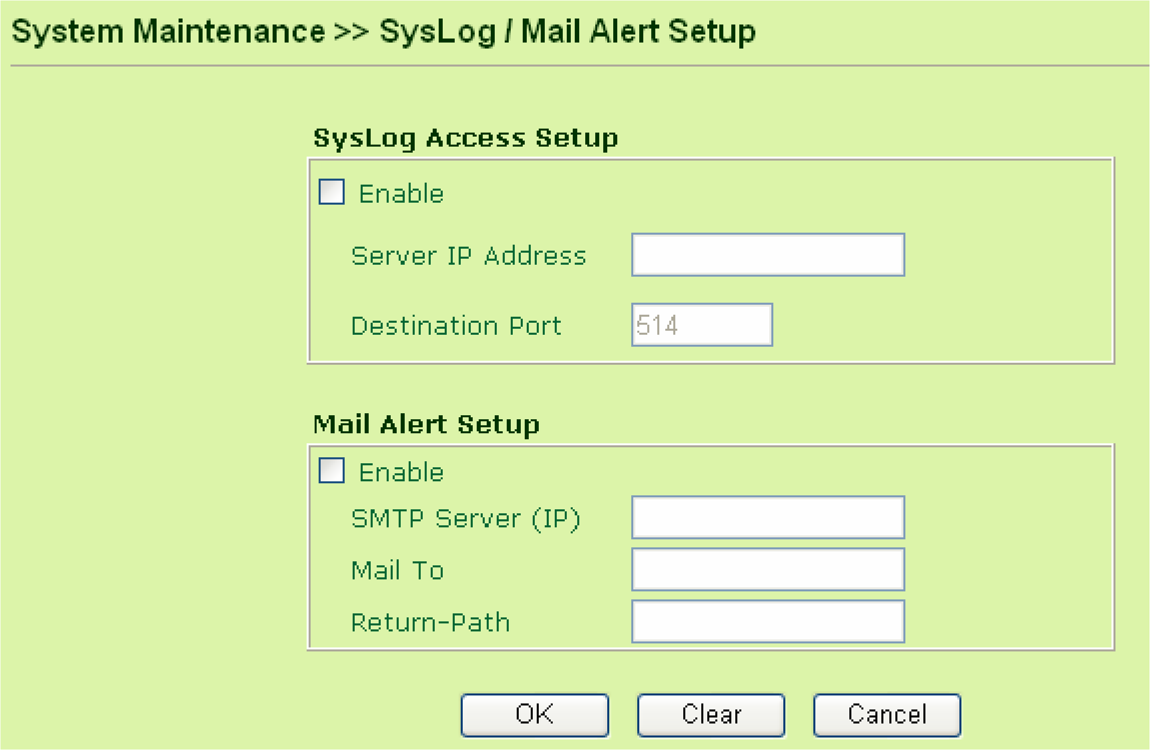
18.1 Introduction

Syslog is a popular utility in UNIX world. To monitor router activity, you can run a Syslog Daemon to capture all activities from the router. This Daemon program can run on a local PC or a remote one elsewhere on the Internet. In addition, the Vigor routers provide the Mail Alert facility so that the syslog messages can packed as an e-mail for someone who wants to receive these messages. In the following, we explain how to setup the syslog and mail alert functions. Use the following setup link on the System Management group of the Setup Main Menu to configure the Syslog / Mail Alert functions.

System Maintenance > Syslog/Mail Alert

18.2 Configuration

After clicking the link of Syslog / Mail Alert Setup, the web configuration will change to another scene, as shown below. In this figure, you can find two functions: one for syslog access setup and another one for mail alert setup.



System Maintenance >> SysLog / Mail Alert Setup

SysLog Access Setup

☐ Enable

Server IP Address:

Destination Port: 514

Mail Alert Setup

☐ Enable

SMTP Server (IP):

Mail To:

Return-Path:

Syslog Access Setup

1. Check the **Enable** box to activate the syslog service.
2. **Server IP Address:** Specify an IP address to which all syslog messages will be sent.
3. **Destination Port:** Specify a UDP port number to which the syslog server is listening. The default value is 514.

Mail Alert Setup

1. Check the **Enable** box to activate the mail alert service.
2. **SMTP Server (IP)**: Specify an IP address of the SMTP server which can send mails from your Vigor router to the recipients' mailboxes directly.
3. **Mail To**: Specify an e-mail address of the recipient's mailbox to which all syslog messages will be sent. The recipient could be an

administrator who intends to view or analyze the syslog messages.

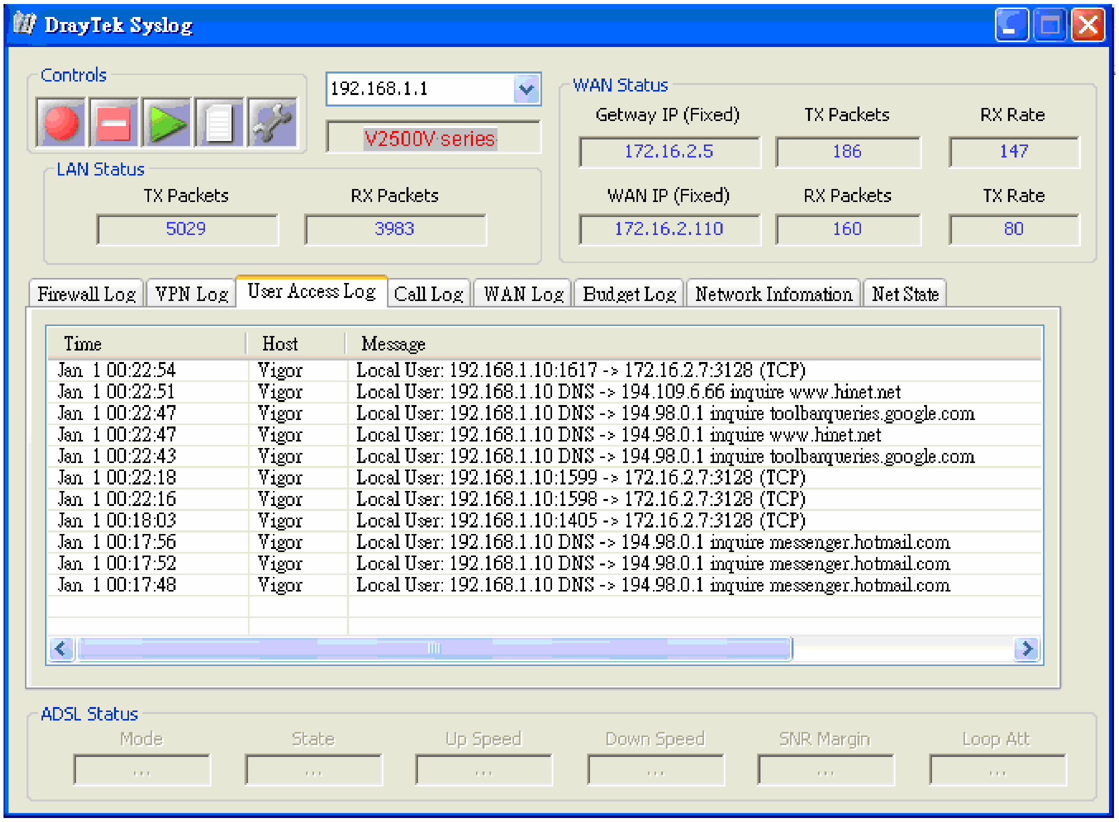
4. **Return-Path**: Specify an e-mail address of another mailbox to accept all returned messages if some fatal problems occur at the recipient mailbox.

The current mail alert function is only designed for sending you the syslog related to Denial-of-Servic (DoS) defense behaviors after you activate the DoS defense facilities.

18.3 Example

Your Vigor router will send many types of syslog messages. Some examples of the syslog messages with their individual formats are shown below.

An example of User Access log message:



192.168.1.1

V2500V series

LAN Status: TX Packets 5029, RX Packets 3983

WAN Status: Getway IP (Fixed) 172.16.2.5, TX Packets 186, RX Rate 147

WAN IP (Fixed) 172.16.2.110, RX Packets 160, TX Rate 80

```
Time            Host    Message
Jan  1 00:22:54 Vigor   Local User: 192.168.1.10:1617 -> 172.16.2.7:3128 (TCP)
Jan  1 00:22:51 Vigor   Local User: 192.168.1.10 DNS -> 194.109.6.66 inquire www.hinet.net
Jan  1 00:22:47 Vigor   Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan  1 00:22:47 Vigor   Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire www.hinet.net
Jan  1 00:22:43 Vigor   Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan  1 00:22:18 Vigor   Local User: 192.168.1.10:1599 -> 172.16.2.7:3128 (TCP)
Jan  1 00:22:16 Vigor   Local User: 192.168.1.10:1598 -> 172.16.2.7:3128 (TCP)
Jan  1 00:18:03 Vigor   Local User: 192.168.1.10:1405 -> 172.16.2.7:3128 (TCP)
Jan  1 00:17:56 Vigor   Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan  1 00:17:52 Vigor   Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan  1 00:17:48 Vigor   Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
```

Chapter 19
Time Setup

19.1 Introduction

If you want to use any time-based function (for example, **Call Schedule** and **URL Content filtering**), the system time function should be assured to work properly.

The router has two ways of updating itself with time clock. One is adopt the current time of your PC via HTTP protocol. The other is update the clock of router via an NTP (Network Time Protocol) server on the Internet.

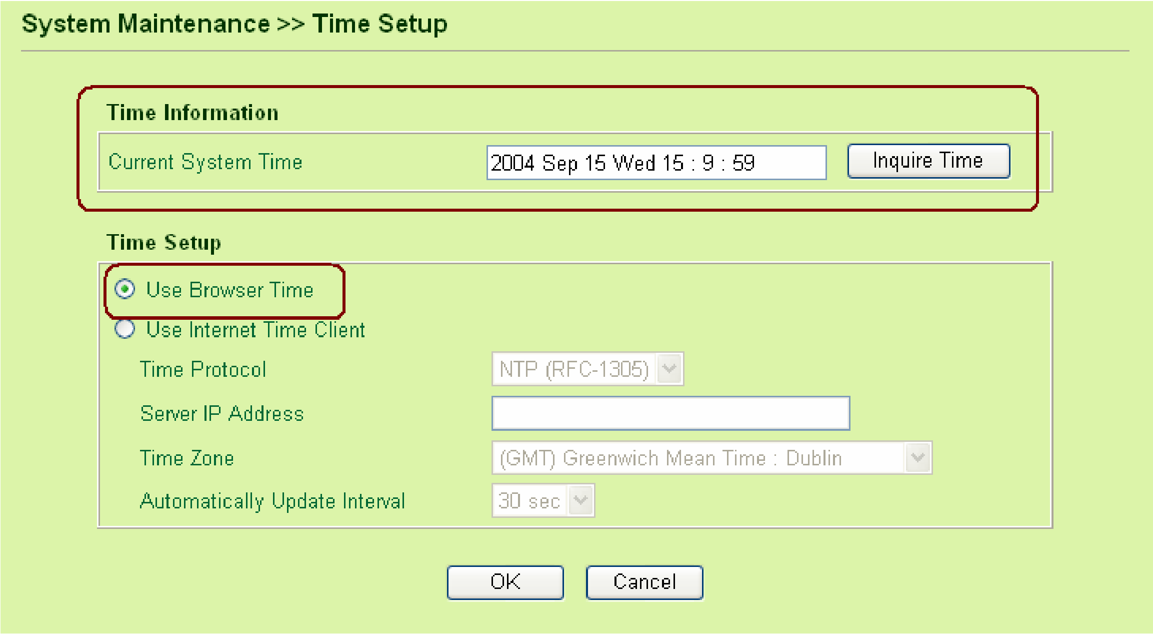
On the Time Setup menu, if you press **Inquire Time** button, the router's clock will be set to current time of your PC. The clock will reset if you power down or reset the router so you may prefer to use an NTP server on the Internet (a time server) to update the clock automatically. NTP updates only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

19.2 Configuration

19.2.1 Set Time Clock via Using Web Browser

1. Before setting time base via using web browser, you have to make sure whether the computer time is accurate or not. Enter **System Maintenance** and then click **Time Setup**.

If you press **Inquire Time** button, the router's clock will be set to current time of your PC.



System Maintenance >> Time Setup

Time Information

Current System Time: 2004 Sep 15 Wed 15 : 9 : 59

Time Setup

● Use Browser Time

○ Use Internet Time Client

Time Protocol: NTP (RFC-1305)

Server IP Address:

Time Zone: (GMT) Greenwich Mean Time : Dublin

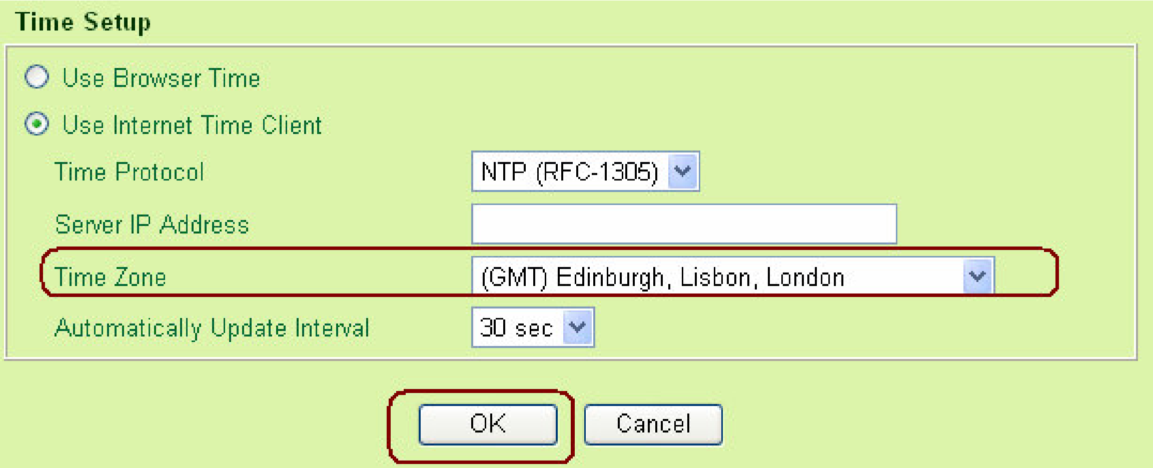
Automatically Update Interval: 30 sec

19.2.2 Use an NTP server on the Internet (a time server) to update the clock automatically

1. Before setting up the time base through the time client, you have

to make sure if the time server is working properly. If the time server is located at the Internet, you should also make sure the router has Internet access capability. Enter **System Maintenance** and then click **Time Setup**.

2. Click **Use Internet Time Client**, choose **Time Protocol** as **NTP**, specify an IP address of time server for the **Server IP Address**, choose an adequate time zone in the **Time Zone** and in turn select an updated time interval in **Automatically Update Interval**. The following screen shows an example.



Time Setup

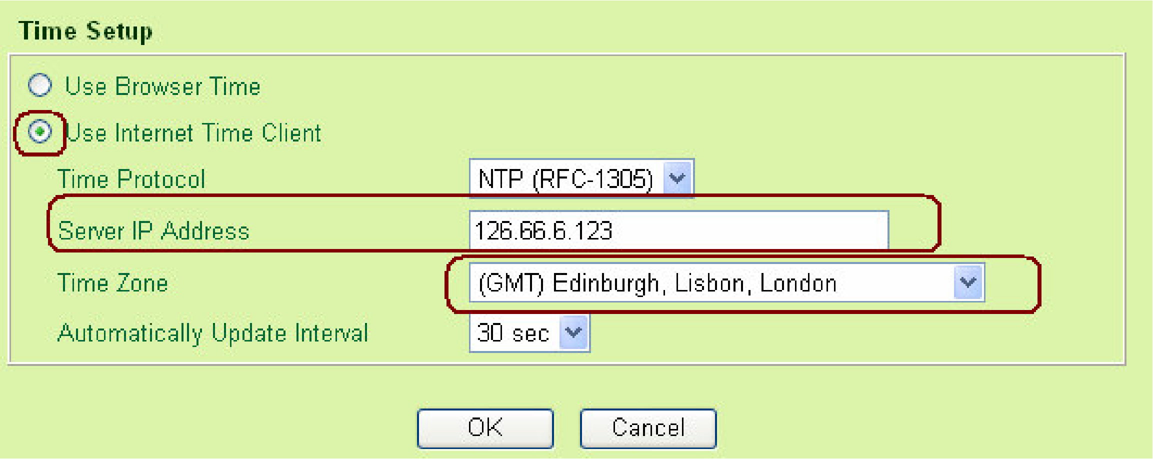
○ Use Browser Time

● Use Internet Time Client

Time Protocol	NTP (RFC-1305)
Server IP Address	
Time Zone	(GMT) Edinburgh, Lisbon, London
Automatically Update Interval	30 sec

3. Click **OK** button, wait for few seconds, and then the time client will get time base from the specified time server.

Click **Time Setup** again to check **Current System Time** information as shown below.



Time Setup

○ Use Browser Time

● Use Internet Time Client

Time Protocol: NTP (RFC-1305)

Server IP Address: 126.66.6.123

Time Zone: (GMT) Edinburgh, Lisbon, London

Automatically Update Interval: 30 sec

Chapter 20
Management Setup

20.1 Introduction

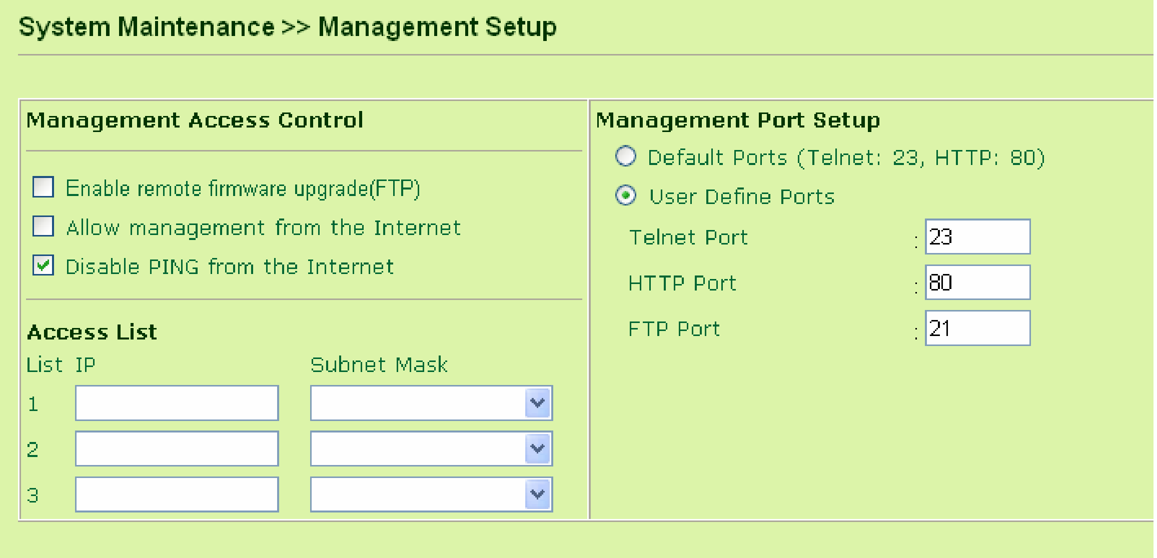
By default, the router may be configured and managed through any Telnet client or Web browser running on any operating system. There is no requirement for additional software or utilities. However, for some specific circumstances, you shall have authority of deciding whether you would like to allow changing the server port numbers for the built-in Telnet or HTTP server, creating access control lists to protect the router, or rejecting the system administrator to login from the Internet. i.e. you can allow or disallow management from the Internet. For example, a technician or support person will be able to access the router's management menus and adjust any settings or view the router's status.

The management include the remote management from web and telnet interfaces. Consequently, it is extremely important to set an admin password for the router, otherwise your router can be accessed and seen by anyone in the world. From the menu, you can set the rule to the router not to reply to pings from the Internet; this offers your router a little bit extra security because someone is scanning ranges of IP addresses searching for hosts as your public IP address will then not respond to a ping request.

For security concern, it's better for you to limit the clients that are allowed to access the router's management interfaces. If you only allow specific internal or external IP addresses to access the router's management, Only these IP addresses or subnets (ranges) you listed can access the router's menus. In order to assure you will not lose the ability to access the router management yourself (normal routing still works), you **HAVE TO** remember to include your own local IP address/subnet too.

20.2 Configuration

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



System Maintenance >> 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)
● User Define Ports

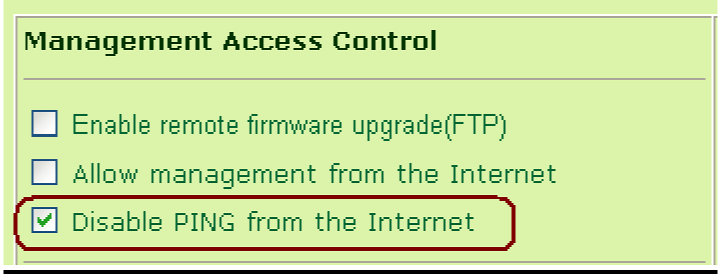
Telnet Port : 23
HTTP Port : 80
FTP Port : 21

20.2.1 Management Access Control

Enable remote firmware update (FTP): 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 concern, this function is enabled by default.



Management Access Control

☐ Enable remote firmware upgrade(FTP)

☐ Allow management from the Internet

☑ Disable PING from the Internet

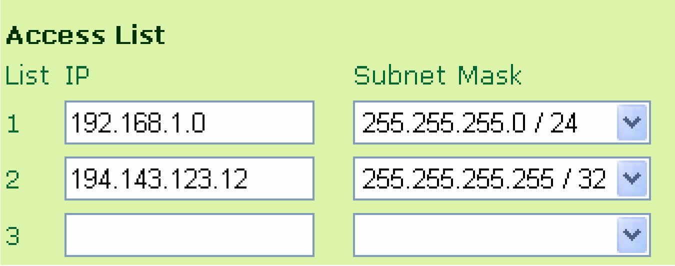
20.2.2 Access List

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 t

o the router.

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



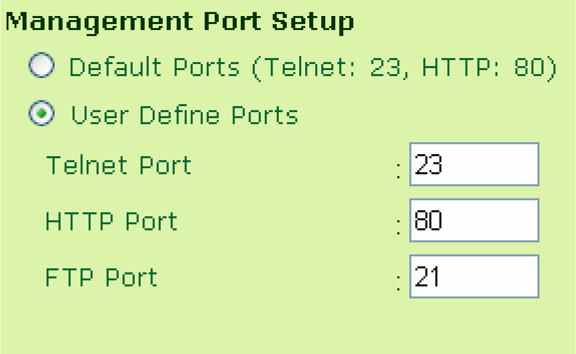
Access List

List	IP	Subnet Mask
1	192.168.1.0	255.255.255.0 / 24
2	194.143.123.12	255.255.255.255 / 32
3		

20.2.3 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.



Management Port Setup

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

● User Define Ports

Telnet Port : 23

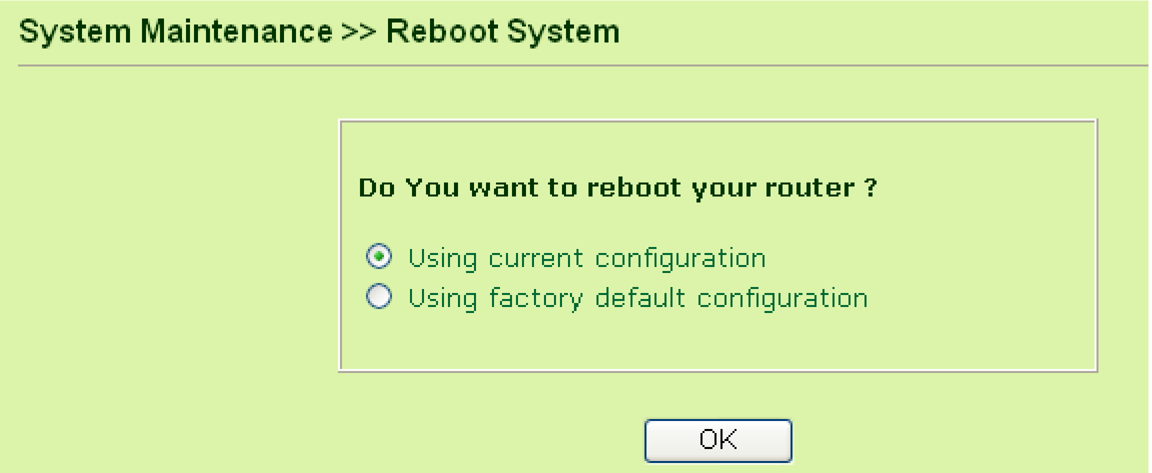
HTTP Port : 80

FTP Port : 21

Chapter 21
Reboot System / Firmware Upgrade

21.1 Reboot System

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



System Maintenance >> Reboot System

Do You want to reboot your router ?

● Using current configuration
○ Using factory default configuration

There are two reboot options:

1. Using current configuration: If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**.

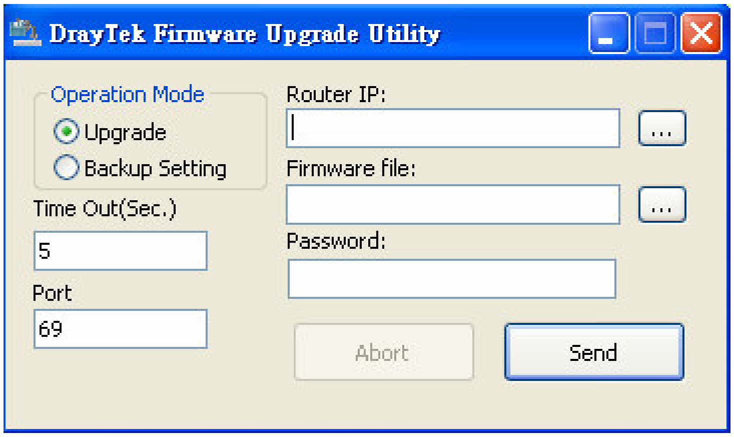
2. Using factory default configuration: To reset the router settings to default values, check **Using factory default configuration** and click **OK**.

The router will take about 3 to 5 seconds to reboot the system.

21.2 Firmware Upgrade (TFTP Server)

Before upgrading your router firmware, you need to install the Router Tools from our bundled CD. The Firmware Upgrade Utility is included in the tools. The following steps will guide you to upgrade firmware. In the following procedure, we use an example to explain the firmware upgrade. Note that this example is running over Windows OS (Operating System).

1. Download the latest 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. Go to **Start** > **Programs** > **Router Tools** > **Router Firmware Upgrade Utility** to launch the Firmware Upgrade Utility.



Operation Mode: ● Upgrade ○ Backup Setting

Time Out(Sec.): 5

Port: 69

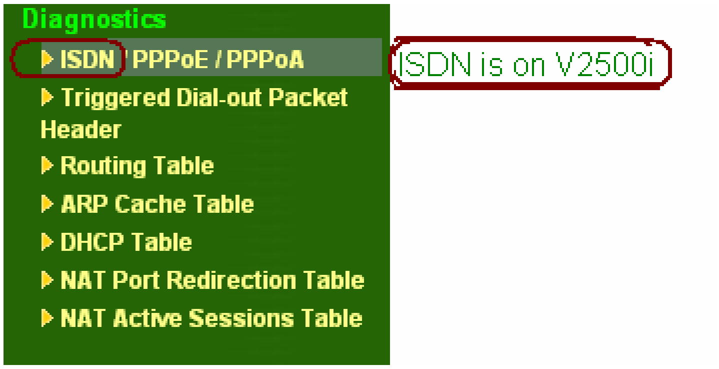
Click the **Browse** button to locate the new firmware file. The program will look for any Vigor routers on your LAN and display them by IP address. Select the 'IP address' of the appropriate router to upgrade, then press **Upgrade**. Enter the router's password when asked (or press **OK** if there is 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 Vigor router will resume flashing normally).

Chapter 22 Diagnostics

22.1 Introduction

Diagnostic Tools provide you with useful tools to view or diagnose the router. Once you encounter any technical queries, you can let your local dealer or us have your screenshot which is related to the result generated from Diagnostic tools.

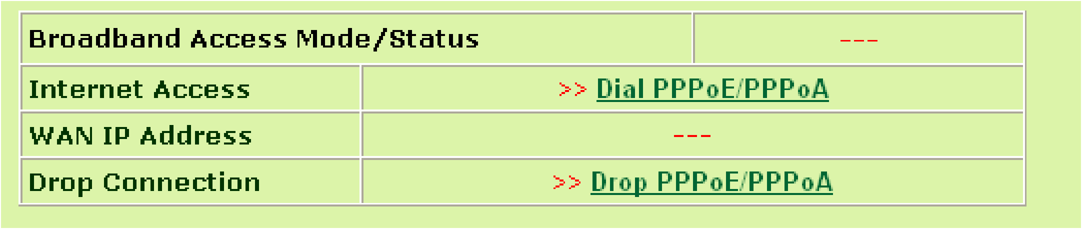
The following is the setting path for the Diagnostics.


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

ISDN is on V2500i

22.2 If your router is Vigor2500V:

PPPoE / PPPoA



Broadband Access Mode/Status	---
Internet Access	>> Dial PPPoE/PPPoA
WAN IP Address	---
Drop Connection	>> Drop PPPoE/PPPoA

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 “**---**”.

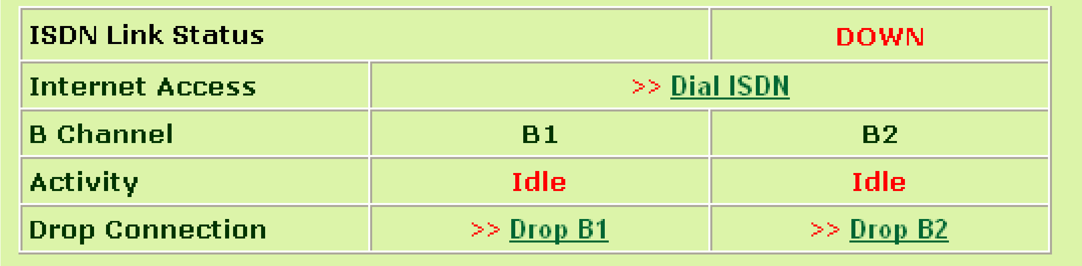
WAN IP Address: The WAN IP address for the active connection.

Dial PPPoE or PPTP: Click it to force the router to establish a PPPoE or PPTP connection.

Drop PPPoE or PPTP: Click it to force the router to disconnect the current active PPPoE or PPTP connection.

22.3 If your router is Vigor2500Vi:

Please find the ISDN portion:



ISDN Link Status		DOWN
Internet Access	>> Dial ISDN	
B Channel	B1	B2
Activity	Idle	Idle
Drop Connection	>> Drop B1	>> Drop B2

ISDN Link Status: If the link is active, this field will show **UP**. Otherwise, it shows **DOWN**.

Dial ISDN: Clicking here causes the router to dial to the preset ISP. Click **ISDN > Dial to a Single ISP** to configure dial-up settings.

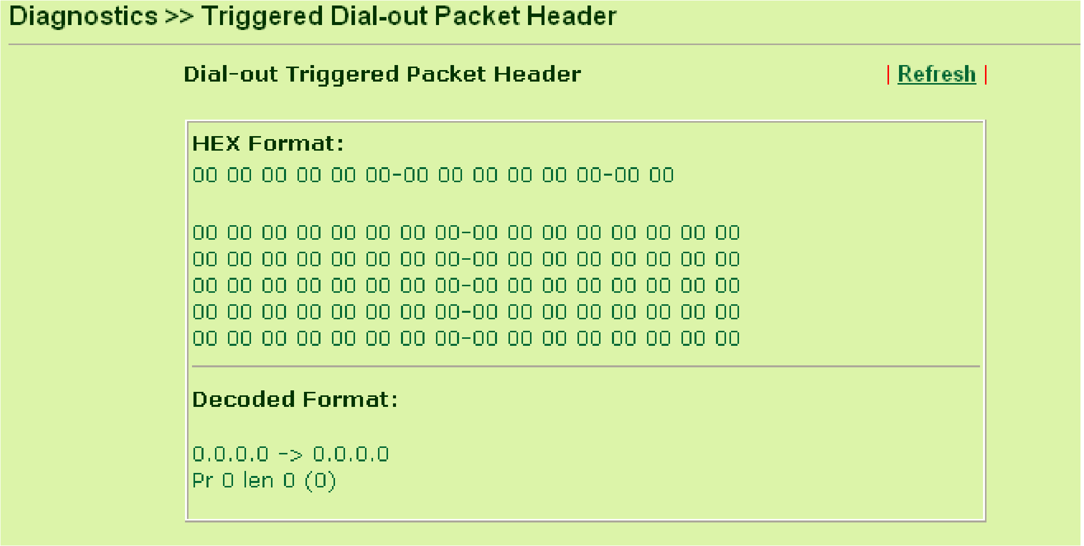
Activity: Displays the connection name for each B channel. If the B channel is idle, it will show **Idle**.

Drop B1: Click to disconnect the B1 channel.

Drop B2: Click to disconnect the B2 channel.

22.4 Triggered Dial-out Packet Header

Triggered Dial-out Packet Header shows the last IP packet header that triggered the router to dial out.



Diagnostics >> Triggered Dial-out Packet Header
Dial-out Triggered Packet Header
| Refresh |

HEX Format:

```
00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

22.5 Routing Table

Click **Routing Table** to view the router's routing table.

The table provides current IP routing information held in the router. In the left of each routing rule, you will see a key. These keys are defined as:

C --- Directly connected.

S --- Static route.

R --- RIP.

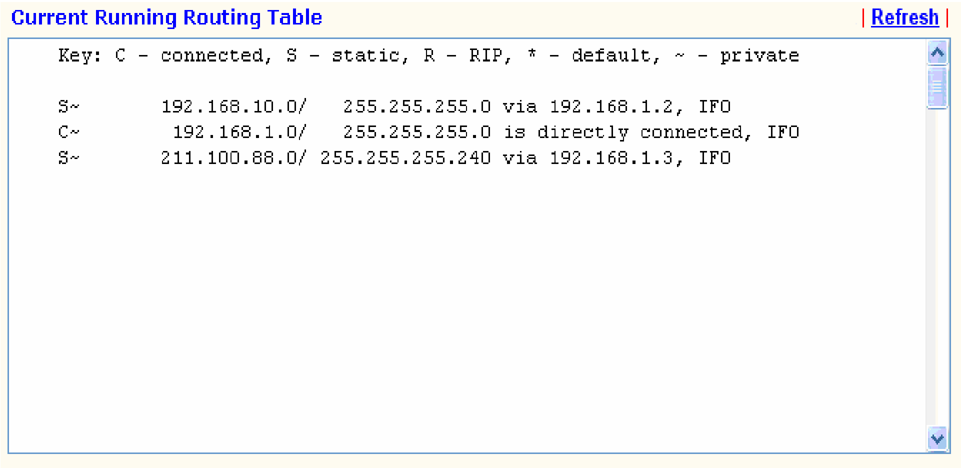
* --- Default route.

~ --- Routes for private routing domain.

In the right of each routing rule, you will see an interface identifier which are defined as follows.

IF0 --- Local LAN interface.

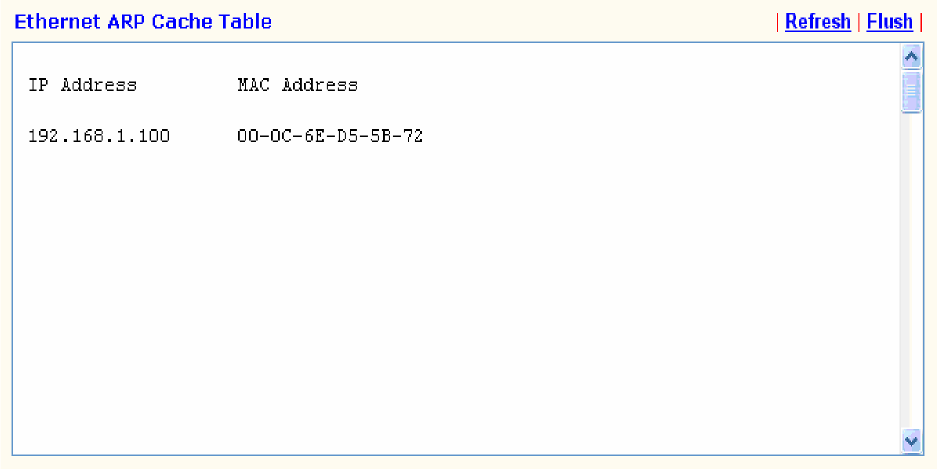
IF3 --- WAN interface.



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

    S~        192.168.10.0/   255.255.255.0 via 192.168.1.2, IF0
    C~         192.168.1.0/   255.255.255.0 is directly connected, IF0
    S~        211.100.88.0/ 255.255.255.240 via 192.168.1.3, IF0
```

22.6 ARP Cache Table

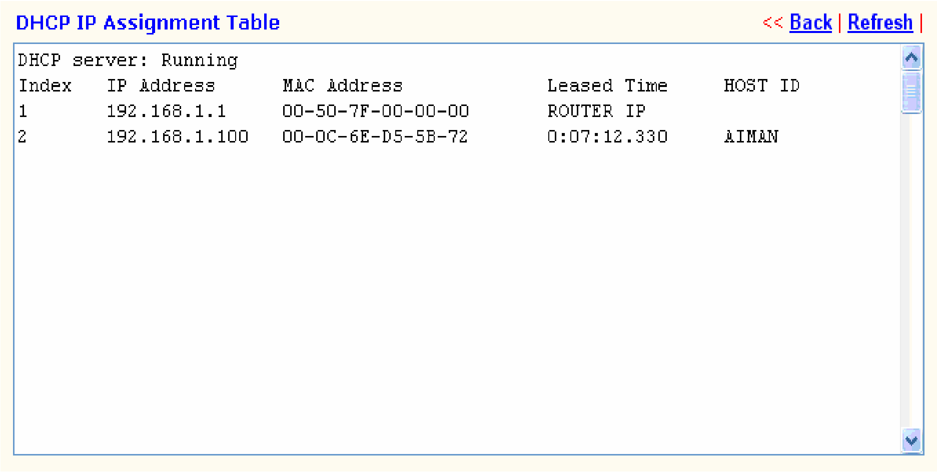
Click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



```
IP Address          MAC Address

192.168.1.100       00-0C-6E-D5-5B-72
```

22.7 DHCP Table

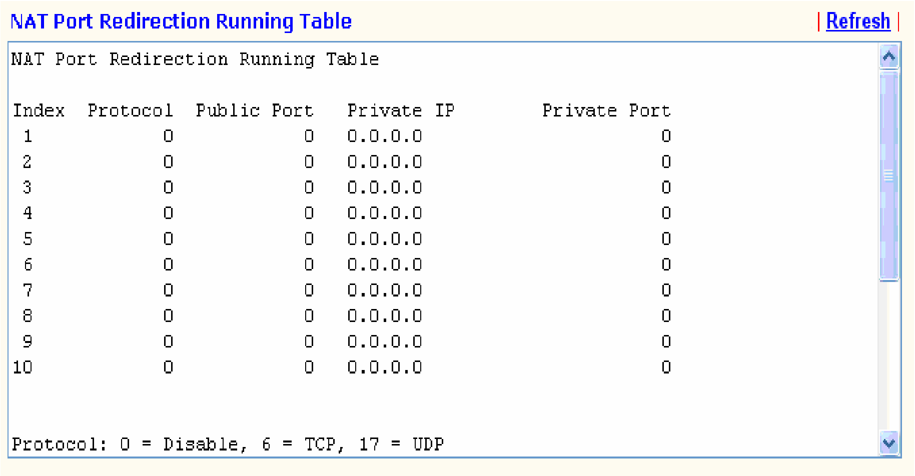
The facility of **DHCP Table** provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.



```
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        192.168.1.100    00-0C-6E-D5-5B-72    0:07:12.330      AIMAN
```

22.8 NAT Port Redirection Table

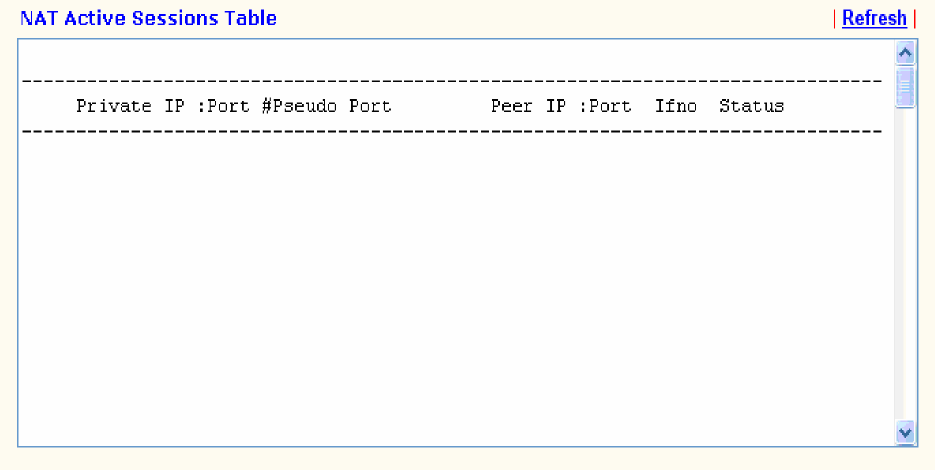
If you have configured **Port Redirection** (under **NAT Setup**), click it to verify that your settings are correct for redirecting specific port numbers to specified internal users.



```
NAT Port Redirection Running Table

Index  Protocol  Public Port   Private IP        Private Port
 1            0            0   0.0.0.0                      0
 2            0            0   0.0.0.0                      0
 3            0            0   0.0.0.0                      0
 4            0            0   0.0.0.0                      0
 5            0            0   0.0.0.0                      0
 6            0            0   0.0.0.0                      0
 7            0            0   0.0.0.0                      0
 8            0            0   0.0.0.0                      0
 9            0            0   0.0.0.0                      0
10            0            0   0.0.0.0                      0


Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

22.9 NAT Active Sessions Table

As the router accesses the Internet through the built-in NAT engine, click **NAT Active Sessions Table** to see which active outgoing sessions are online.



```

--------------------------------------------------------------------------------
     Private IP :Port #Pseudo Port         Peer IP :Port  Ifno  Status
--------------------------------------------------------------------------------
```

Each line across the screen indicates an active session. The following information is displayed:

Private IP, Port: The internal user's (PC's) IP address and port number.

#Pseudo Port: The public port number.

Peer IP, Port: The peer user’s (PC’s) IP address and port number.

Ifno: Stands for interface number. The definition is listed below:

0 --- LAN interface.

3 --- WAN interface.

Should you have any technical queries of using **Diagnostic Tools**, you can contact your local dealer or us **support@draytek.com** to let us be more helpful for you.

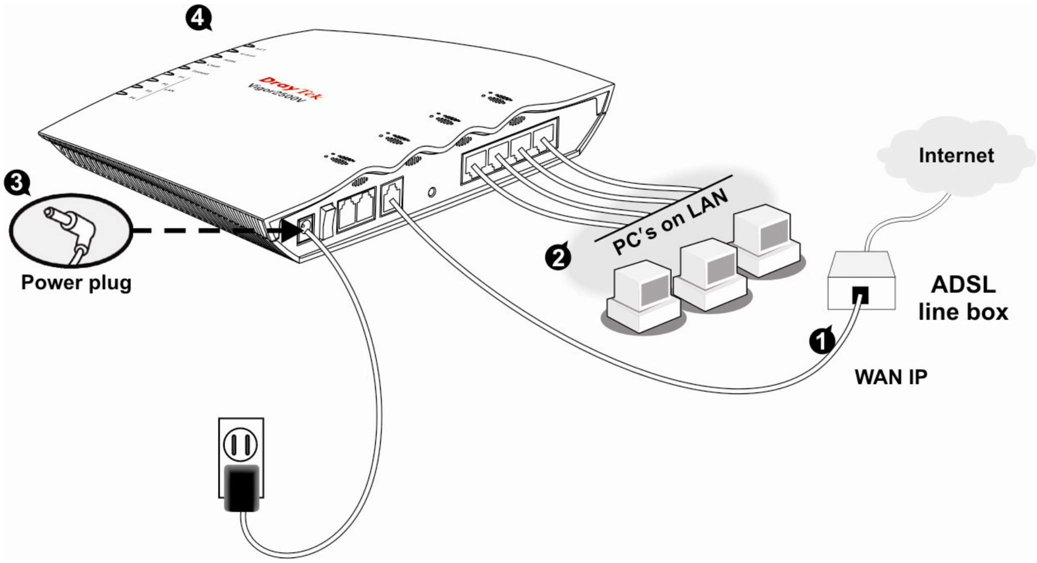
Trouble-Shooting of Vigor2500V/Vi series ADSL VoIP Routers

Firstly, Check your Hardware Installation!

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

1. Connect the ADSL interface to the external splitter with a RJ-11 cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
3. Connect the attached power adapter to the power port.
4. Check the **ACT**, **ADSL** and **LAN** LEDs to assure network connections.
   (Regarding detailed LED status explanation please refer to section 1.3)

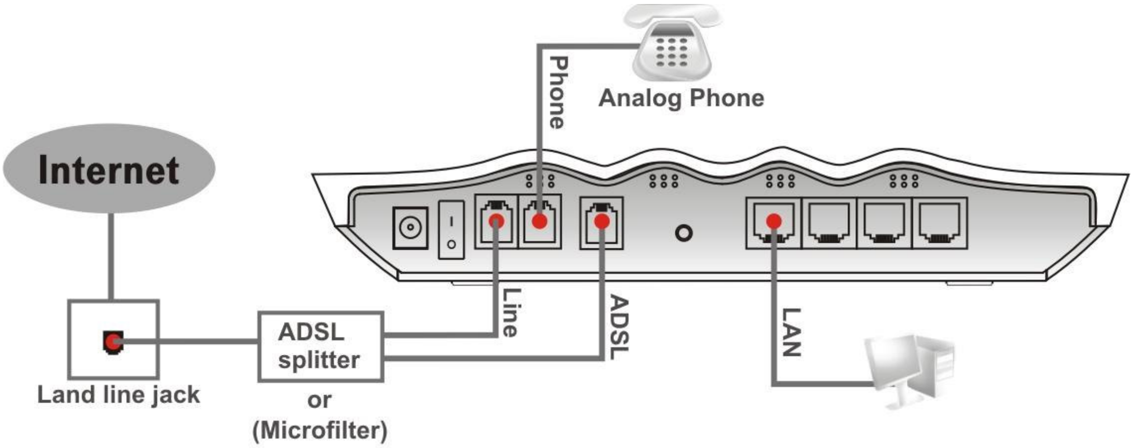
Connection scenario is shown as below:



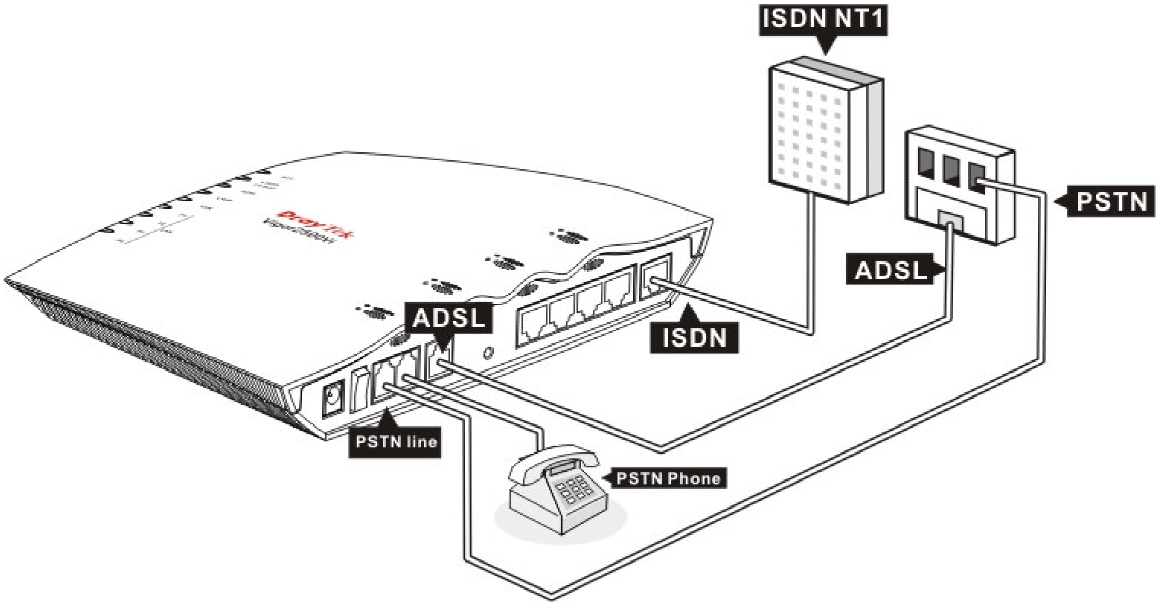
The splitter or microfilter is the optional accessories.

There are some variant connection in Annex A and Annex B countries. Followings are more reference for you:

Annex- A countries:

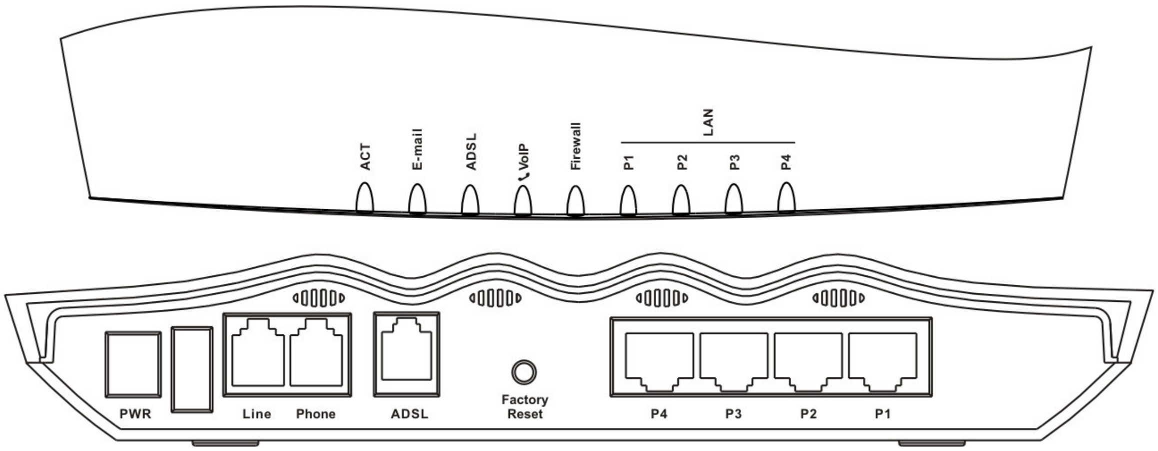


Annex – B countries



2. Review the definition of Front Panel LEDs and Rear Panel Interfaces

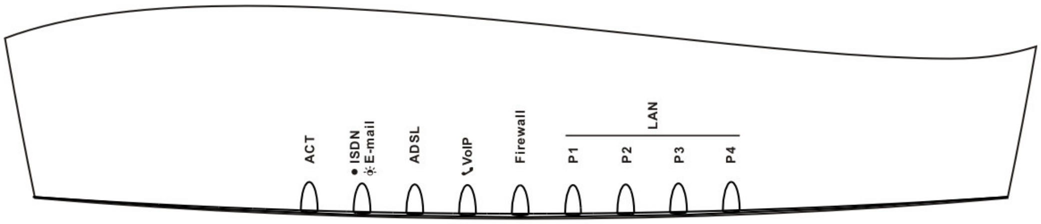
Vigor2500V

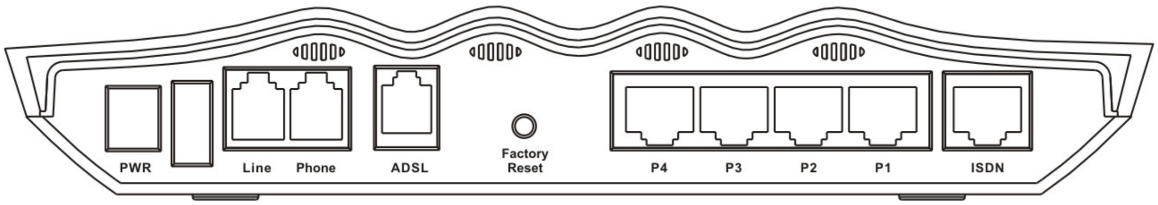


LED	Status	Explanation
ACT (Activity)	blinking	The router is powered on and running properly.
E-mail	blinking	When detecting one or more user-defined e-mails existing on mail server.
ADSL	on	The ADSL line is showtime.
VoIP	green	Solid light when the handset of phone is picked up (off hooked).
		Blinking per 0.3 second when phone call is via ISDN loop through.
		Blinking per 2 seconds when phone is connected through VoIP.
	orange	Solid light when phone call is via PSTN life line.
Firewall	on	The firewall function is active.
	blinking	When encountering DoS attacks.
LAN (P1, P2, P3, P4)	green	A normal 100Mbps connection is through its corresponding port.
	orange	A normal 10Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.

Interface	Description
PWR	Connect the included power adapter to the power outlet.
Line	Connect to the analog phone line for PSTN life line.
Phone	Connect to the analog phone for VoIP communication.
ADSL	Connect the ADSL line to access the Internet.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1, P2, P3, P4	Connect to the local network devices.

Vigor2500Vi





LED	Status	Explanation
ACT (Activity)	blinking	The router is powered on and running properly.
ISDN/E-mail	on	The ISDN network is correctly setup.
	blinking	When detecting one or more user-defined e-mails existing on mail server.
ADSL	on	The ADSL line is showtime.
VoIP	green	Solid light when the handset of phone is picked up (off hooked).
		Blinking per 0.3 second when phone call is via ISDN loop through.
		Blinking per 2 seconds when phone is connected through VoIP.
	orange	Solid light when phone call is via PSTN life line.
Firewall	on	The firewall function is active.
	blinking	When encountering DoS attacks.
LAN (P1, P2, P3, P4)	green	A normal 100Mbps connection is through its corresponding port.
	orange	A normal 10Mbps connection is through its corresponding port.
	blinking	Ethernet packets are transmitting.

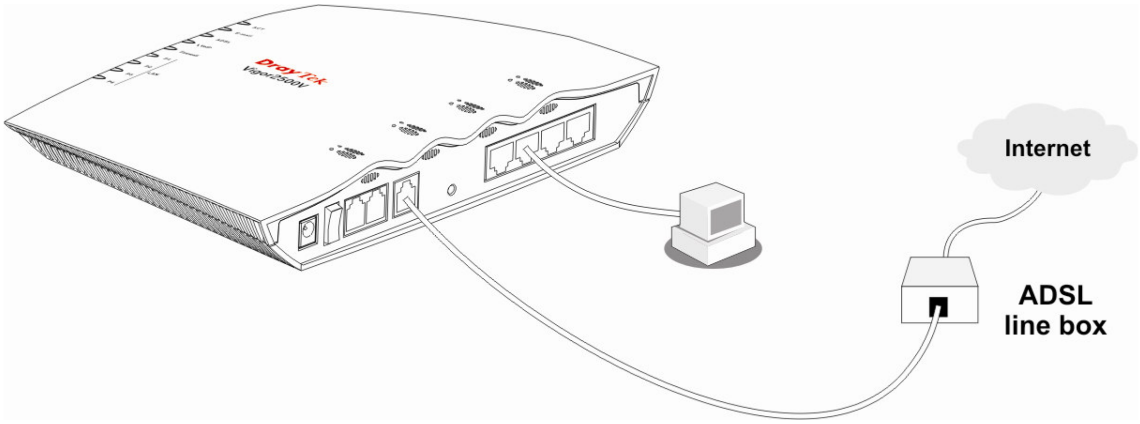
Interface	Description
PWR	Connect the included power adapter to the power outlet.
Line	Connect to the analog phone line for PSTN life line.
Phone	Connect to the analog phone for VoIP communication.
ADSL	Connect the ADSL line to access the Internet.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking), press the hole and keep for more than 5 seconds. When the ACT LED begins to blink rapidly, release the button. Then the router will restart with the factory default configuration.
P1, P2, P3, P4	Connect to the local network devices.
ISDN	Connected to an external NT1(or NT1+) box provided by your ISDN service provider.

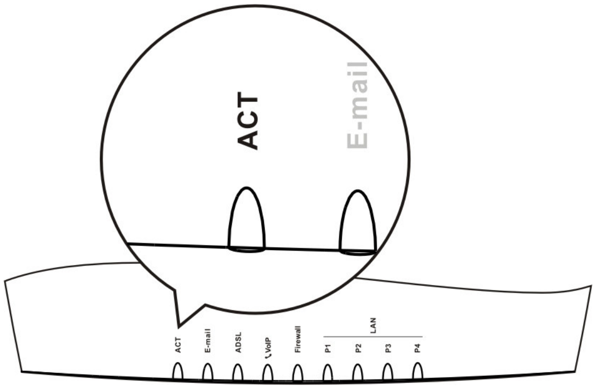
3. Trouble Shooting

This section will guide you how to shoot troubles on abnormal situations. Please follow the order of subsection as below to check your installation.

3.1 Is the Hardware Status OK?

1. Check that if the power line and ADSL/LAN cable are connected correctly.
2. Turn on the router, and then check that if the **ACT** LED blink once per second and the correspondent **LAN** LED is light.

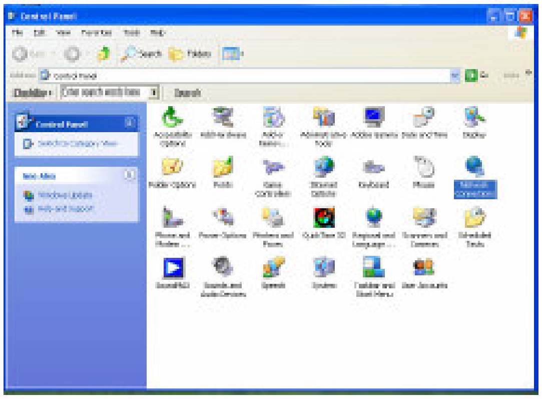




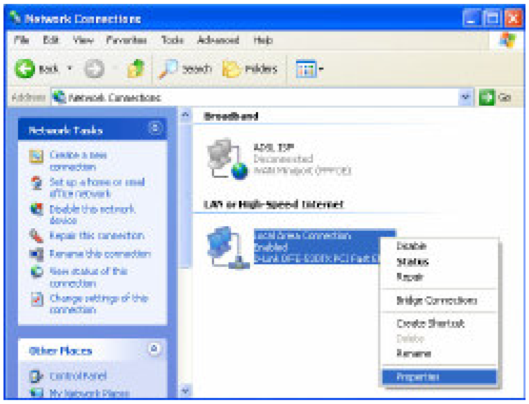
3.2 Are the Network Connection Settings on Your PC OK?

The following example is based on Windows XP case, regarding the other OS examples, please refer to the similar steps or support notes in **www.draytek.com**.

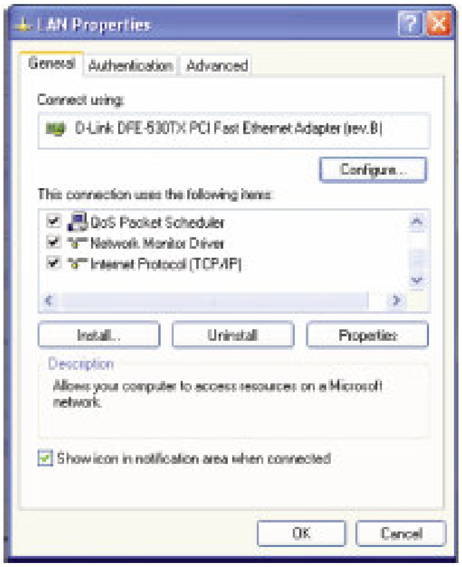
1. Go to **Control Panel** and then double-click on **Network Connections.**



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



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



Connect using:

D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.B)

This connection uses the following items:

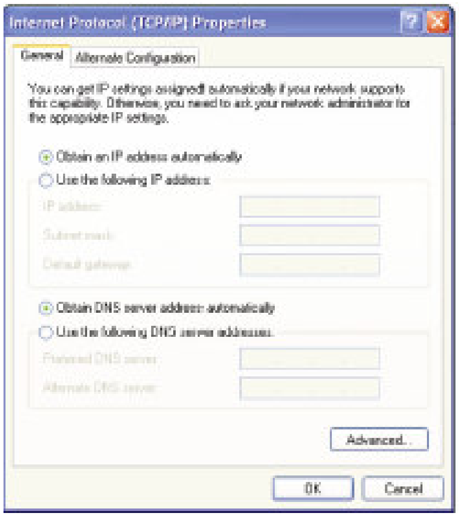
☑ QoS Packet Scheduler
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

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



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

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

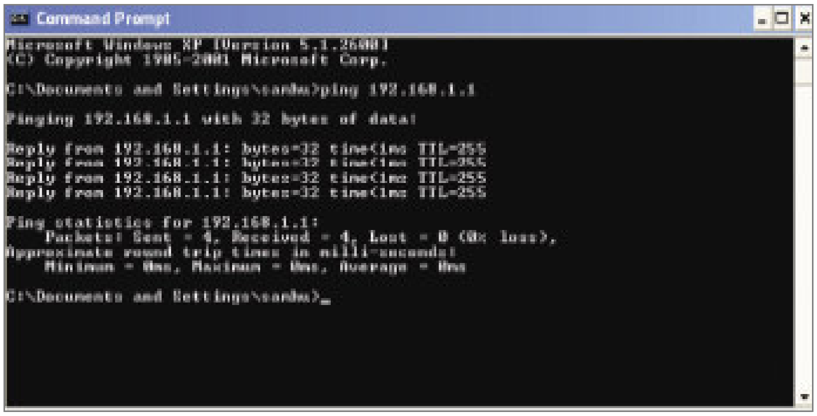
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

3.3 Can You Ping the Router from PC?

The default gateway IP of the router is 192.168.1.1. Please check that if you can ping the router correctly.

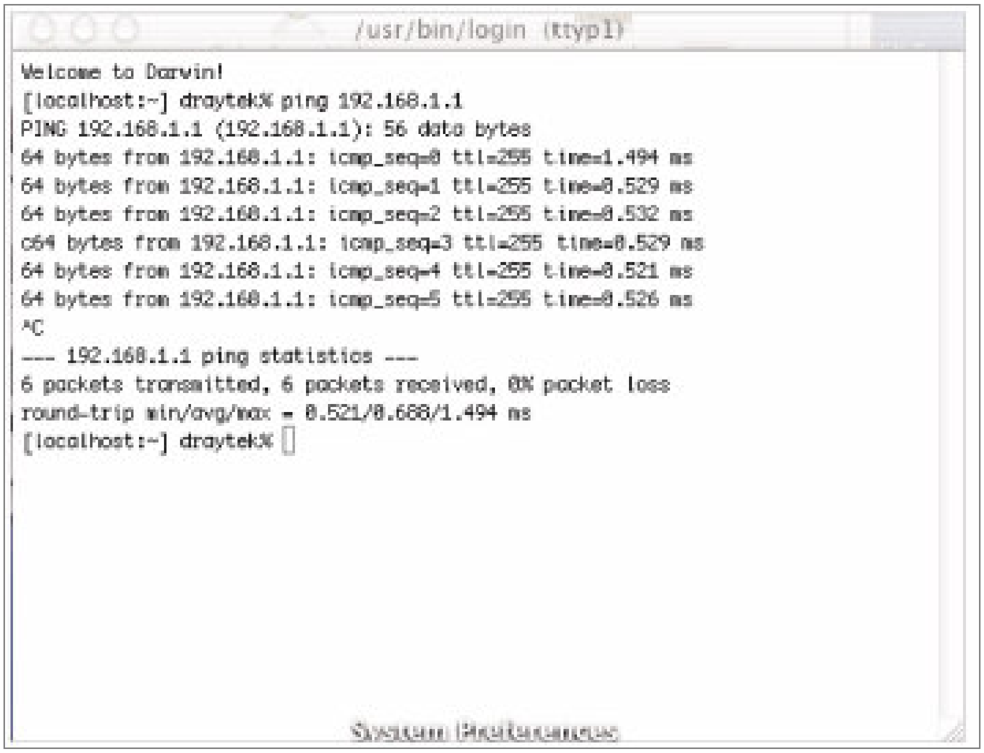
A. For Windows

1. Open the Command Prompt window (from start menu > Run)
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP).
3. Type **ping 192.168.1.1** and press [Enter]



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

C:\Documents and Settings\candw>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\candw>_
```

B. For Mac (Terminal)



```
Welcome to Darwin!
[localhost:~] draytek% ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=1.494 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.529 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.532 ms
c64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.529 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.521 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=255 time=0.526 ms
^C
--- 192.168.1.1 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.521/0.688/1.494 ms
[localhost:~] draytek% 
```

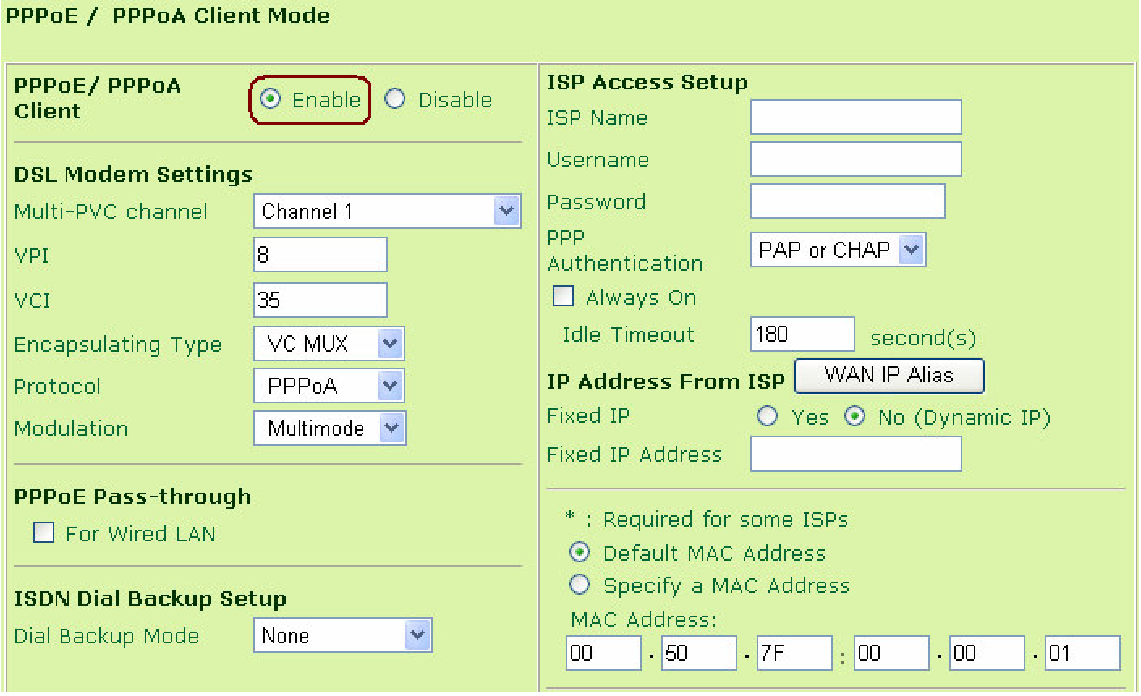
Note that if the computer receives a reply from 192.168.1.1. If not, please check the IP address of your PC. We recommend you set the network connection as get IP automatically. (Please refer to the next section)

3.4 Are the ISP Settings OK?

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

A. For PPPoE/PPPoA Users (refer to the following figure)

1. Check that if the **Enable** option is selected.
2. Verify if all parameters of **DSL Modem Settings** are entered with correct value which given by your ISP.
3. Verify if **Username** and **Password** are entered with correct value which given by your ISP.



PPPoE / PPPoA Client Mode

PPPoE/ PPPoA Client ● Enable ○ Disable

DSL Modem Settings

Multi-PVC channel: Channel 1
VPI: 8
VCI: 35
Encapsulating Type: VC MUX
Protocol: PPPoA
Modulation: Multimode

PPPoE Pass-through

☐ For Wired LAN

ISDN Dial Backup Setup

Dial Backup Mode: None

ISP Access Setup

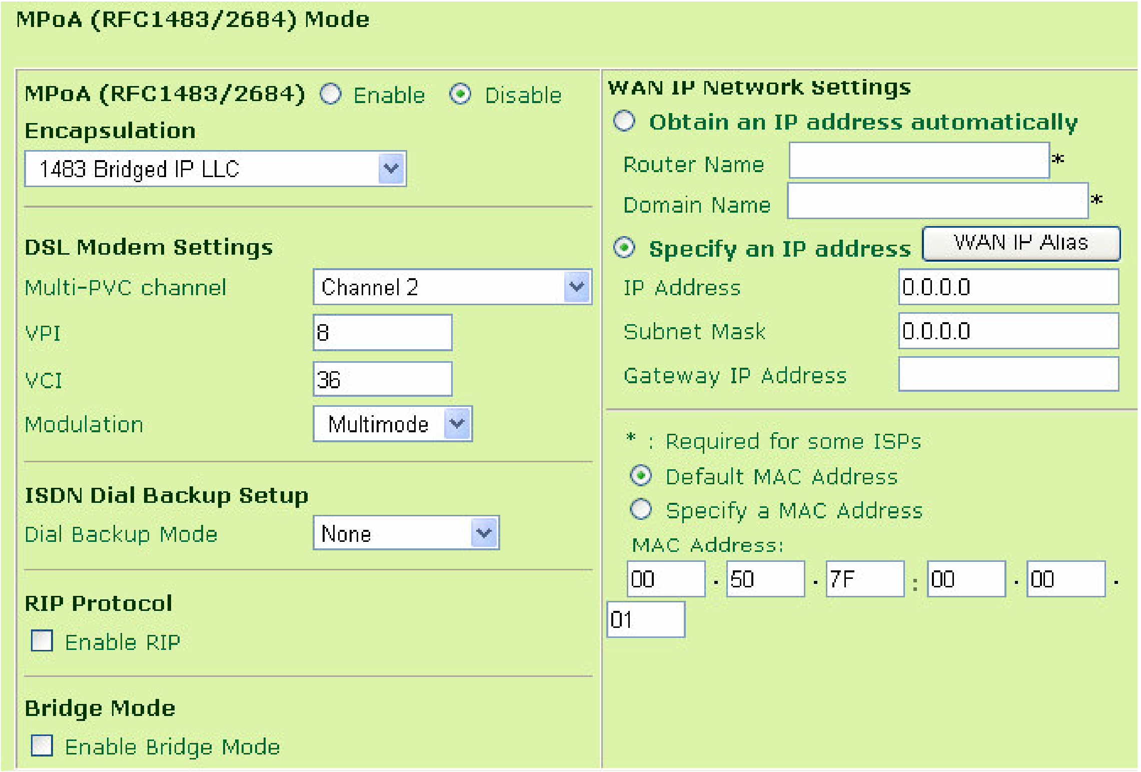
ISP Name:
Username:
Password:
PPP Authentication: PAP or CHAP
☐ Always On
Idle Timeout: 180 second(s)

IP Address From ISP WAN IP Alias

Fixed IP: ○ Yes ● No (Dynamic IP)
Fixed IP Address:

* : Required for some ISPs
● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 . 50 . 7F : 00 . 00 . 01

B. For MPoA (RFC1483/2684) Users (refer to the following figure)
1. Check that if the **Enable** option is selected.
2. Verify if all parameters of **DSL Modem Settings** are entered with correct value which given by your ISP.
3. Verify if **IP Address, Subnet Mask** and **Gateway** are set correctly, or that your ISP requires using DHCP clients to obtain IP automatically.



MPoA (RFC1483/2684) Mode

MPoA (RFC1483/2684) ○ Enable ● Disable

Encapsulation
1483 Bridged IP LLC

DSL Modem Settings
Multi-PVC channel: Channel 2
VPI: 8
VCI: 36
Modulation: Multimode

ISDN Dial Backup Setup
Dial Backup Mode: None

RIP Protocol
☐ Enable RIP

Bridge Mode
☐ Enable Bridge Mode

WAN IP Network Settings
○ Obtain an IP address automatically
Router Name: *
Domain Name: *
● Specify an IP address
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway IP Address:

* : Required for some ISPs
● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 . 50 . 7F : 00 . 00 . 01

3.5 Report to ISP and Dealer for Further Technical Support

1. If the router settings are correct at all, and the router still does not connect, please contact your ISP technical support representative to help you for configuration.
2. If the router does not work correctly, please contact your dealer for help. For any further questions, please send e-mail to **support@draytek.com**

We would like to remind you of the benefits of Vigor2500V series as below once your technical queries are resolved:

Benefits of Vigor2500V series

- **ADSL router for sharing your Internet connection**
- **Robust firewall to help protect your computers**
- **Make / Receive Voice calls over your ADSL connection using a regular telephone handset**
- **Integration with your existing phone line (POTS) with automatic failover during power cuts**
- **Free Voice-over-IP phone calls to other VoIP users**
- **ISDN backup/remote access/ISDN loop through are available on Vigor2500Vi series which have ISDN interface**
- **Compatible with Windows and Mac OS**

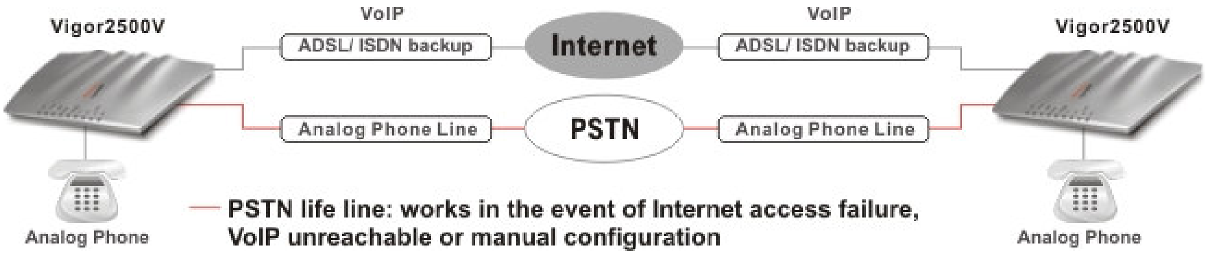
Brief Overview

	Vigor2500V	Vigor2500Vi
ADSL Router	*	*
VoIP	*	*
PSTN life line	*	*
ISDN loop through	-	*
ISDN backup	-	*

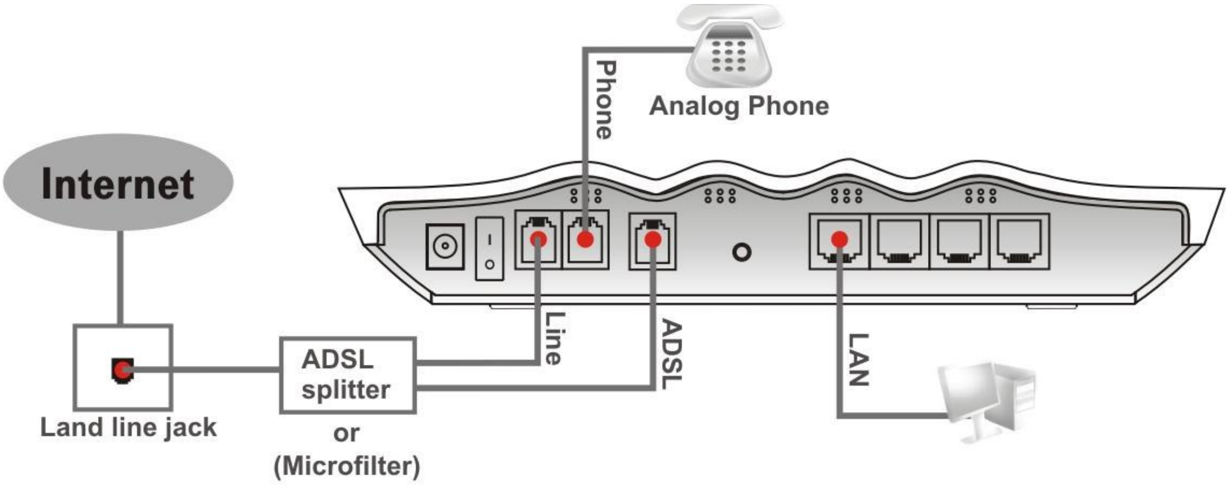
What does **"PSTN life line"** and **"ISDN loop through"** perform on Vigor2500V series**?**

The Vigor2500V has a “Line” port on the rear panel for connecting to a PSTN (regular analogue) line. The Loop Through option can be used to set an alternate telephone number for your contact on the PSTN, which the Vigor2500V will dial instead of the SIP account if you lose ADSL access or power to the Vigor2500V. Hence, the PSTN line can act as a lifeline (backup mechanism) for VoIP calls. The lifeline mechanism is activated automatically but can also be manually configured.

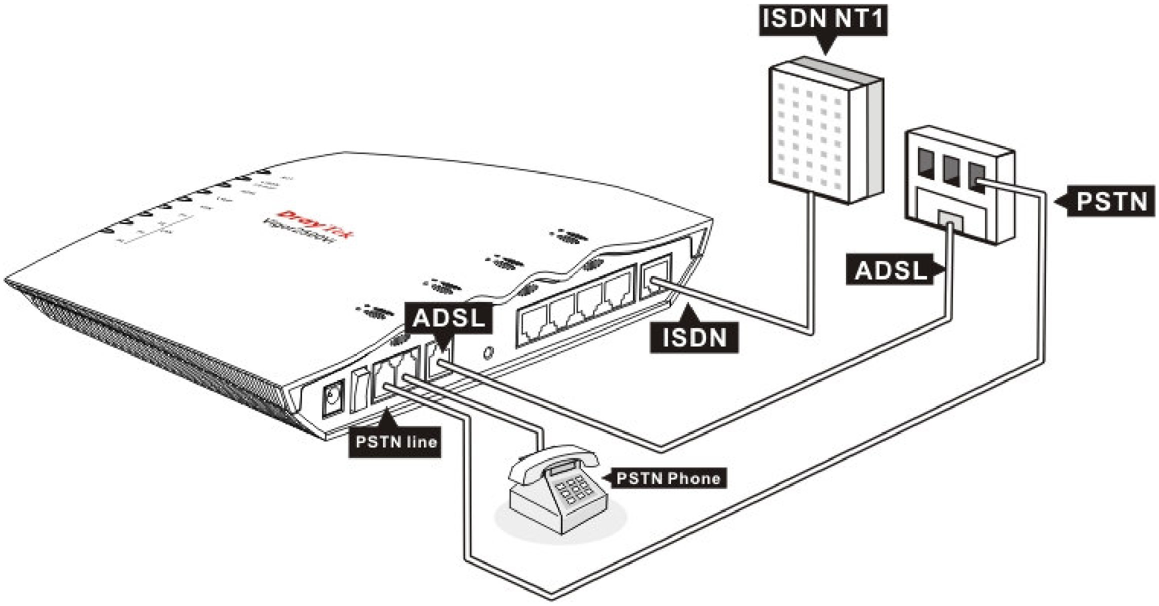
Because there is ISDN interface on the Vigor2500Vi series, you can use the ISDN line as phone line as well as Internet remote access/dial back-up for ADSL. You will be able to still make ISDN phone calls if the router loses power or the VoIP calls can not make as Internet access is broken. Hence, the ISDN line can also be lifeline (backup mechanism) for VoIP calls.



Annex- A countries:



Annex – B countries



Highlights

VoIP

- G.168 Line Echo-cancellation
- Gain Control
- Jitter Buffer (250ms)
- Voice CODEC: G.711 A/u law, G.729 A/B, VAD/CNG
- Tone Generation and Detection: DTMF, Dial, Busy, Ring Back
- Protocol: SIP, RTP/RTCP

ADSL

- Compatible with ADSL lines up to 8 Mbps.
- Support PPPoE, PPPoA, MPoA

LAN

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

Network Features

- DHCP server / relay
- Dynamic DNS
- Call Scheduling

Firewall

- Stateful Packet Inspection
- Selectable DoS/DDoS protection
- IP address anti-spoofing
- User-configurable packet filtering
- NAT/PAT with Port Forwarding/Redirection & DMZ
- E-mail alerting mechanism

E-mail Detection

- Detect user-defined e-mails and hold them in mail server (POP3).

Flexible URL Content Filtering

- URL blocking by user-defined keywords
- Preclude web surfing from using directly IP address
- Java/ActiveX/cookies/proxy blocking
- Executable/compressed/multimedia files blocking
- Time schedule support

Application Support

- Windows Messenger, Yahoo Messenger, MSN Messenger V6.0, NetMeeting, ICQ2001b/2002a, most online gaming, and other multimedia applications
- UPnP protocol support

Router Management

- Web-based User Interface
- Command line interface (Telnet)
- Telnet remote access support
- Built-in diagnostic tools
- Quick Start Wizard
- Attack alert by e-mail
- Syslog Monitoring

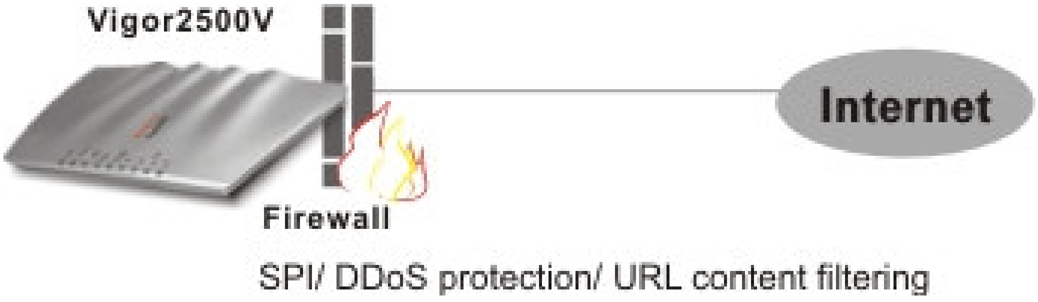
ISDN Facilities (for Vigor2500Vi only)

- Compatible with Euro ISDN
- Automatic ISDN backup
- Support for 64/128kbps (multilink-PPP)
- Bandwidth on demand (automatically switches between 64kbps and 128kbps)
- LAN-to-LAN connectivity
- Remote Activation
- Virtual TA

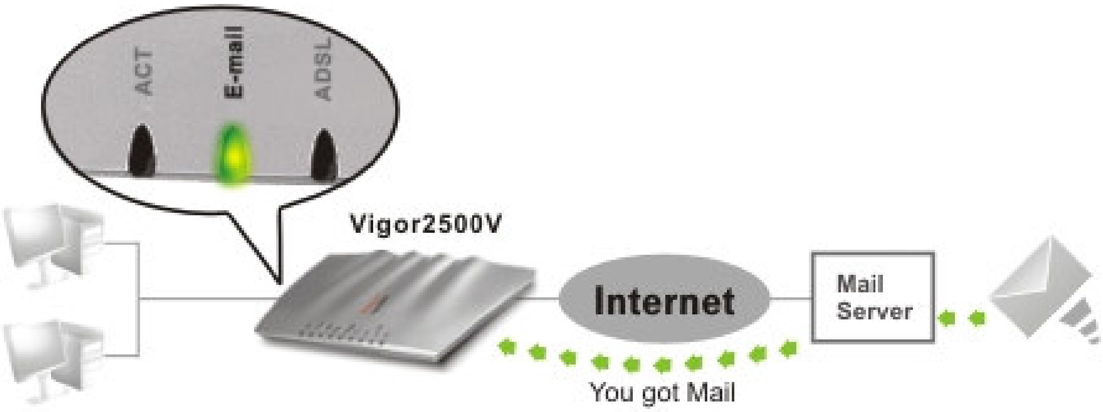
Routing Support

- RIPv2 **(not applicable to the UK)**
- Static Route **(not applicable to the UK)**

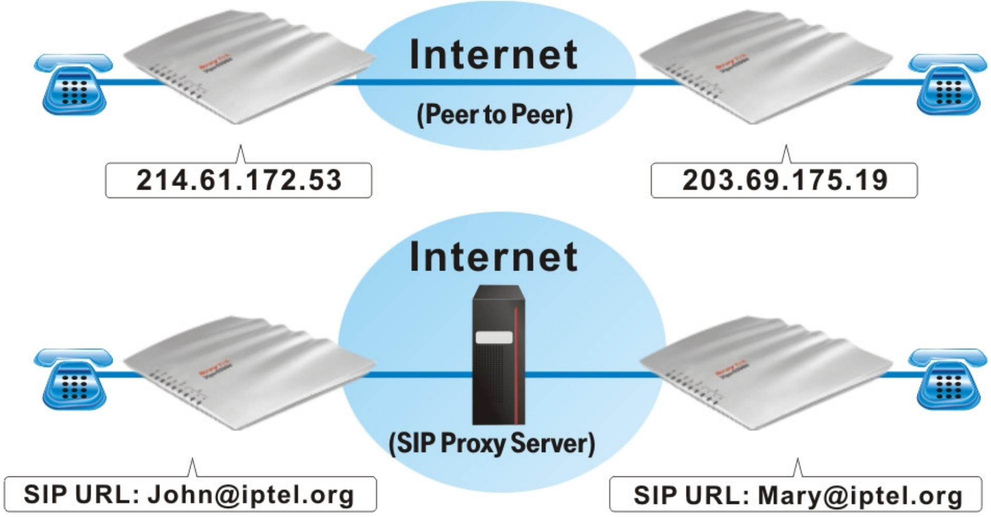
Robust Firewall:



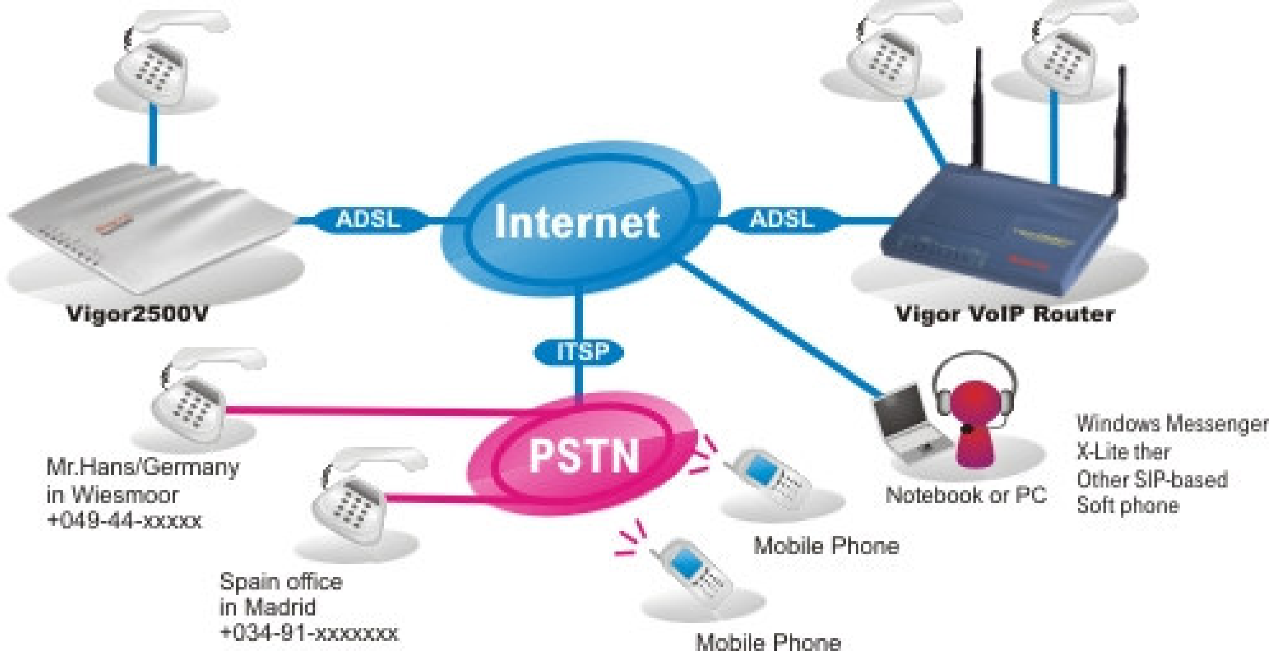
E-mail Detection:



Peer to Peer VoIP communications:



Vigor2500V series with the services of ITSP:



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)].