DrayTek

Vigor2800 Series

User's Guide

Version 1.0

Preamble of Vigor2800 Series ADSL2/2+ Router

Highlights

- **Easy Internet-sharing of your broadband connection**
- **Robust firewall to help protect your network from external attacks**
- **Comprehensive VPN facilities provide deployment of linked branch offices and teleworkers**

For G models:

- **802.11g compliant Wireless LAN access with security features.**
- **Super G ^{TM} high speed wireless LAN up to 108Mbps data rate**

Brief Overview

Model comparison chart:

	ADSL2/2+ Router	VoIP	High Speed Wireless AP	ISDN
Vigor2800Gi	*	-	*	*
Vigor2800G	*	-	*	-
Vigor2800i	*	-	-	*
Vigor2800	*	-	-	-

Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor2800 series is an ADSL2/2+ enabled integrated access device. With downstream speed up to 12Mbps(ADSL2) or 24Mbps(ADSL2+), the Vigor2800 series provides exceptional bandwidth* for Internet access. (*note: the available bandwidth also depends on the Internet Service Provider)

Embedded with sophistic VPN firewall security features, the Vigor2800 series provides 32 dedicated virtual private data networks tunneling through public Internet. Powered by hardware-based DES/3DES engine, all the information transmitted is well encrypted, hence against any snooping without performance degraded when VPN is enabled.

The Vigor2800 G models are embedded 802.11g compliant wireless module which provides wireless LAN access with line rate as much as 54Mbps. The Vigor2800 G models feature WPA2(802.11i), wireless LAN isolation, WDS(Wireless Distribution System), and Universal VLAN™.

The Vigor2800 i models provide ISDN backup, which keep your internet access alive even when ADSL internet access fails.

Specifications

For Vigor2800G models

Wireless Access Point

- IEEE802.11b/g compliant
  - 64/128-bit WEP
  - WPA/WPA2(IEEE802.11i)
  - 802.1x authentication with RADIUS client
- VPN over WLAN
- Wireless client list
- Hidden SSID
- MAC address access control
- Access point discovery
- Wireless VLAN*
- Wireless LAN isolation
- Wireless client isolation
- Wireless rate-control*
- WDS(Wireless Distribution System)
- Super G ™
  - Up to 108 Mbps data rate**
  - Utilizing adaptive radio to automatically identify clear channels
  - Real-time hardware data compression

* *Actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

For Vigor2800 i models

ISDN

- Euro ISDN compatible
- Automatic ISDN backup
- Support 64/128Kbps(multilink-PPP)/BOD (Bandwidth on Demand)
- Remote Dial-In/LAN-to-LAN connection
- Remote activation
- Virtual TA

All models

ADSL Compliant

- ADSL
  - G.dmt (G.992.1)
  - G.lite (G.992.2)
  - ANSI T1.413 issue2
- ADSL2
  - G.dmt.bis(G.992.3)
  - G.lite.bis(G.992.4)
- ADSL2+(G.992.5)
- Up to 24Mbps downstream and 1Mbps upstream

ATM Protocols

- Multiple Protocol over AAL5 (RFC 2684)
- PPP over Ethernet and AAL5 (RFC 2516,2364)
- Up to 8 PVC
- PPPoE pass through LAN/WLAN
- Transparent bridge for MPoA

VPN
- Up to 32 VPN tunnels
- Supported protocol: PPTP, IPSec, L2TP, L2TP over IPSec
- DHCP over IPSec(*)
- Encryption: AES, MPPE and hardware-based DES/3DES
- Authentication: MD5, SHA-1
- IKE authentication: pre-shared key and digital signature(X.509)*
- LAN-to-LAN, Teleworker-to-LAN

Firewall Facilities
- IM/P2P blocking
- Multi-NAT, DMZ host, port-redirect/open port
- Rule-based packet filtering
- Stateful packet inspection
- DoS/DDoS protection
- IP address anti-spoofing
- E-mail alert and logging via syslog
- VPN pass through

QoS
- Class-based bandwidth guarantee by user-defined traffic categories
- Support 4 priority levels
- Support of DiffServ Code Point classifying

Printer Server
- One USB port connector
- Built-in LPR printer server
- Provide LPR printer for Windows 98/SE/ME
- Compatible with Windows 2000/XP/Server 2003/MAC OS 9/MAC OS X built-in LPR printer driver

Network Features
- DHCP client/relay/server
- Dynamic DNS
- SNTP client
- Call scheduling
- RADIUS client
- DNS cache/proxy
- UPnP
- Routing protocol:
  - Static routing
  - RIP V2

Router Management
- Web-based user interface (HTTP/HTTPS)
- Quick Start Wizard
- CLI (Command Line Interface, Telnet/SSH*)
- Administration access control
- Configuration backup/restore
- Built-in diagnostic function
- Firmware upgrade via TFTP/FTP
- Syslog
- SNMP management MIB-II

Content Filtering
- URL blocking
- Java Applet, Cookies, Active X, compressed, executable, multimedia
- Time schedule control

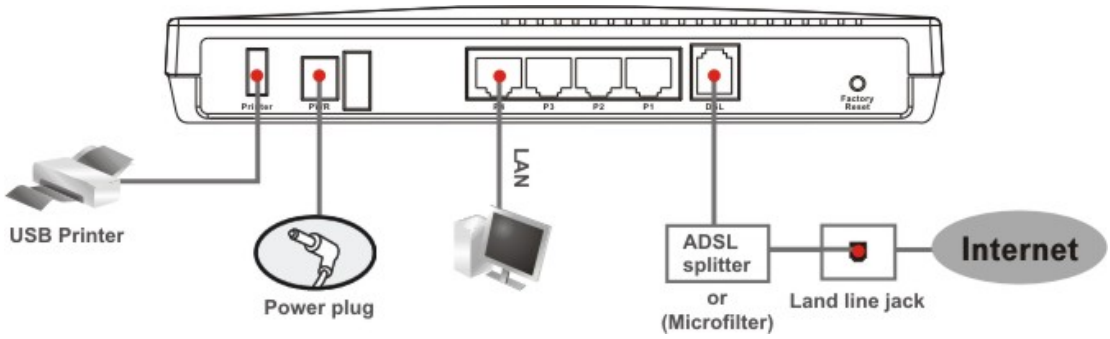
Power Consumption
- 15Watt Max.

*future release

Hardware Connection

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

1. Connect the DSL interface to the external ADSL splitter with an ADSL line cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
3. For G models, connect detachable antennas to the router.
4. Connect the attached power adapter to the power port.
5. Check the ACT and WAN, LAN LEDs to assure network connections.
   (Regarding the detailed LED status explanation, please refer to section 1.3)



About This User's Guide

This manual is designed to assist users in using one of the Vigor2800 series of ADSL2/2+ 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  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

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.
- Do not deploy Ethernet cable connecting to LAN ports outdoor to prevent electronic shock hazards.
- 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: Vigor2800 Series ADSL2/2+ Routers

DrayTek Corp. declares that Vigor2800 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 Vigor2800Gi/G are designed for the WLAN 2.4GHz network throughput EC region, Switzerland, and the restrictions of France.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

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

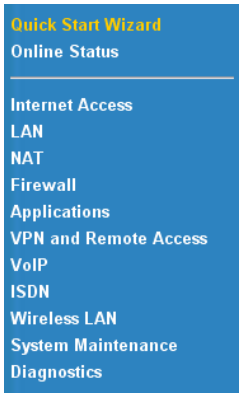
The Quick Start Wizard is designed to easily set up your broadband Internet access.

1.2 Configure Your Router via Quick Start Wizard

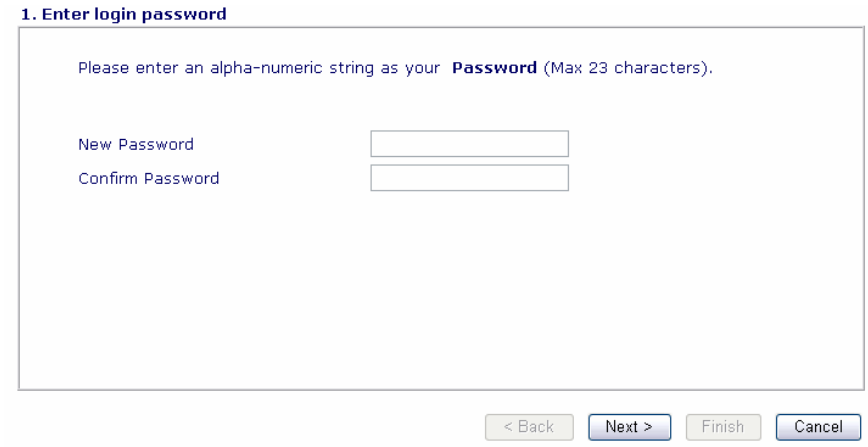
Step 1. Open the web browser on a PC which is connected to the router and then link to the gateway IP address of the router (the default setting is **192.168.1.1**). Once your link (**http://192.168.1.1**) is successful, a pop-up window will open to ask for username and password. Leave the default null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

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

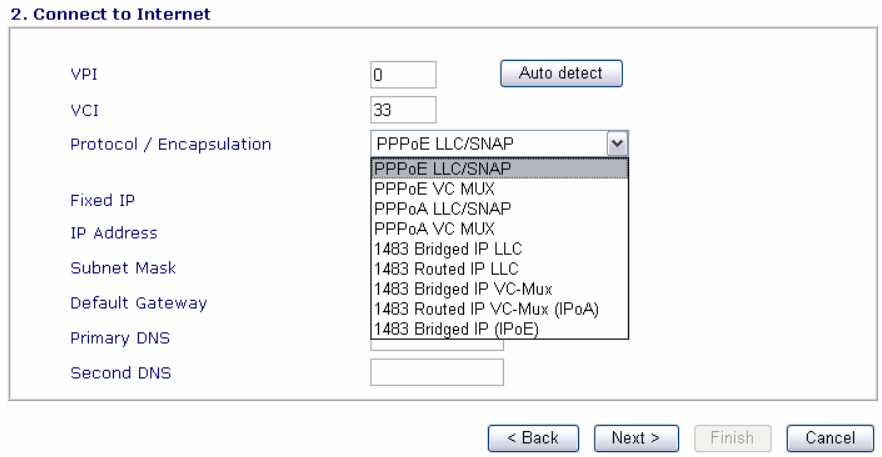
Step 2. The **Main Menu** will pop out after completing previous step.



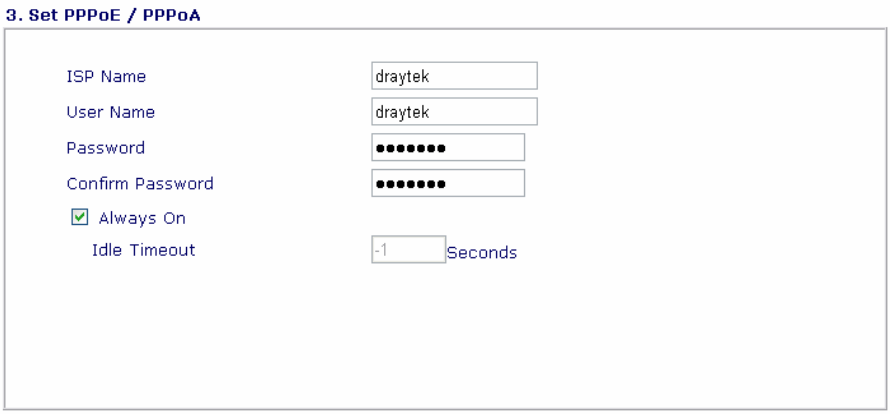
Step 3. Now Quick Start Wizard is switched on. Enter login password. Then click **Next** to continue.



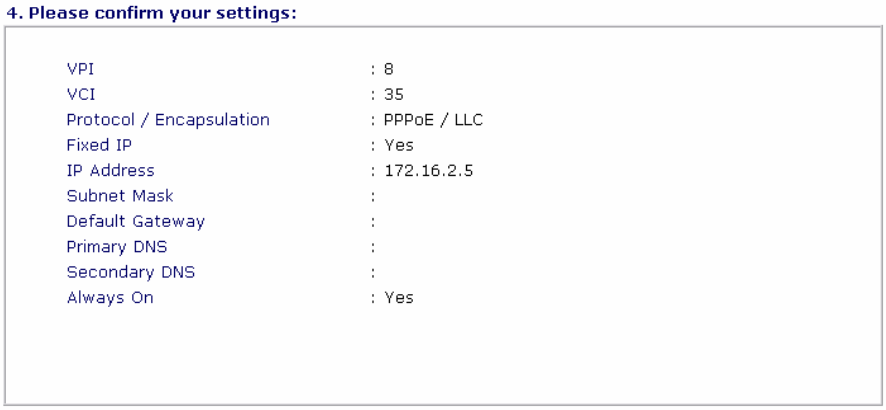
Step 4 Set up appropriate DSL parameters according the information provided by your Internet Service Provider(ISP). “Auto detect” can provide some of DSL parameters automatically. For more detail, see **Chapter 3**. Then click **Next** to continue.



Step 5 If PPPoE/PPPoA is selected, please manually enter the Username/Password provided by your ISP. Checking the **Always On** means Internet access is always on regardless of Internet usage.



Step 6 Review the summary of settings.



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

- "**Ready**" indicates the system is ready for you to input settings.
- "**Settings Saved**" means your settings are saved once you click "Finish" or "OK" button.

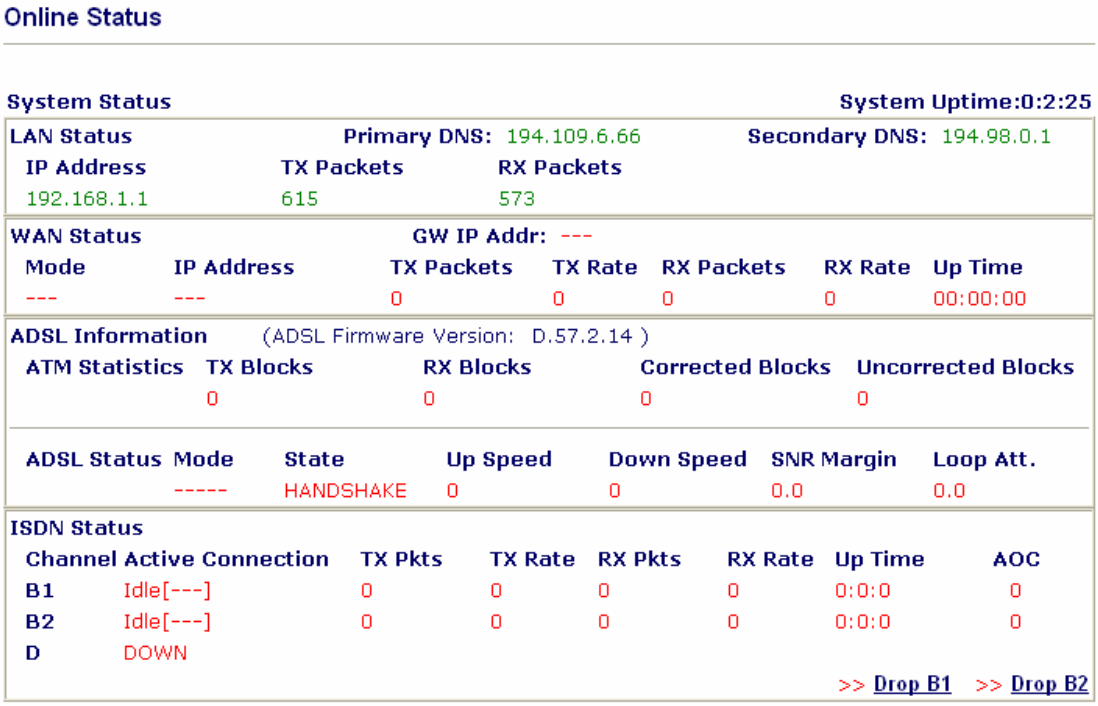
Chapter 2
Online Status

2.1 Introduction

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

2.2 Settings

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



2.2.1 System Status

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

2.2.2 LAN Status

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

2.2.3 WAN Status

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

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

2.2.4 ADSL Information

ADSL Firmware Version: Indicates the ADSL 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 corrupted but corrected.
Uncorrected Blocks	Total number of received ATM Blocks corrupted but uncorrected.

ADSL Status

Mode	Indicates which modulation mode is used: G.DMT, G.Lite, or T1.413.
State	Indicates the DSL line status.
Up Speed	Indicates Up Stream Speed (bits/ second).
Down Speed	Indicates Down Stream Speed (bits/ second).
SNR Margin	Indicates Signal Noise Ratio Margin (dB). The higher value has better signal quality.
Loop Att.	Indicates subscribed Loop Attenuation.

2.2.5 ISDN Status (for i models)

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 sent during this connection session.
TX Rate	Transmission rate for outgoing data. The unit is characters per

	second (cps).
RX Pkts	Total number of received IP packets received during this connection session.
RX Rate	Reception rate for incoming data. The unit is characters per second (cps).
Up Time	Connection time. The format is HH:MM:SS where HH means hours, MM means minutes, and SS means seconds.
Drop B1	Click to disconnect the B1 channel.
Drop B2	Click to disconnect the B2 channel.

Chapter 3
Internet Access

3.1 Introduction

Basics of Internet Protocol (IP) Network

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

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

Public IP Address and Private IP Address

As Vigor router plays a role to manage and further protect its LAN, it interconnects groups of host PCs each of which has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default private IP address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices with a public IP address. When data flow passing through, the Network Address Translation (NAT)

function of the Vigor router will dedicate to translate public/private addresses and packets will be delivered to the correct host PC in the local area network. Thus all host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

To acquire a public IP address from your ISP for Vigor router as a CPE, there are three common protocols: Point to Point Protocol over Ethernet (**PPPoE), PPPoA and MPoA**. **Multi-PVC** is provided for more advanced setup of the above.

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device, such as Vigor Pro DSL router, using ATM Permanent Virtual Circuit, to a remote access concentrator or aggregation concentrator. This implementation provides the end user with the significant ease of use and requires virtually no knowledge other than that of standard dial-up Internet access. Meanwhile it provides access control, billing, and type of service on a per user basis.

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

PPPoA, included in RFC1483, can be operated in either Logical Link Control-Subnetwork Access Protocol or VC-Mux mode. As an CPE device, Vigor router encapsulates the PPP session based for transport

across the ADSL loop and your ISP's Digital Subscriber Line Access Pultiplexer (SDLAM).

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

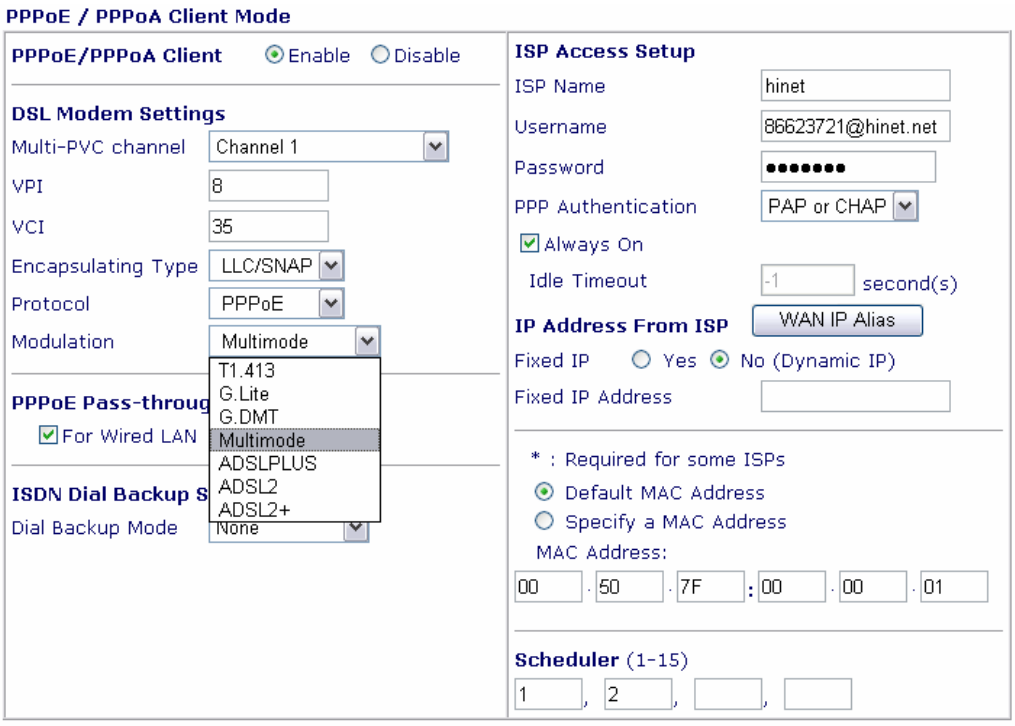
Once you already access Internet via the procedure of "Chapter 1 Quick Start Wizard", you do not need to re-set your settings for Internet connection unless you would like to change your configuration.

3.2 Settings

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

3.2.1 PPPoE/PPPoA

Click on **Enable** to activate this function.



DSL Modem Settings

Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.

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.

ISDN Dial Backup Setup (for i model only)

None	Disable this function
Packet trigger	Enable this function when packet
Always on	Always enable this function

ISP Access Setup

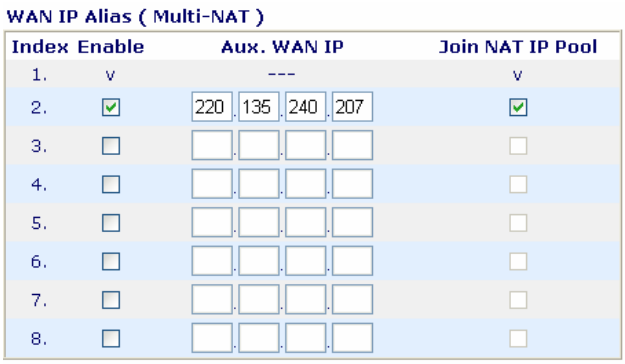
Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check 'Always On'.

Fixed IP:

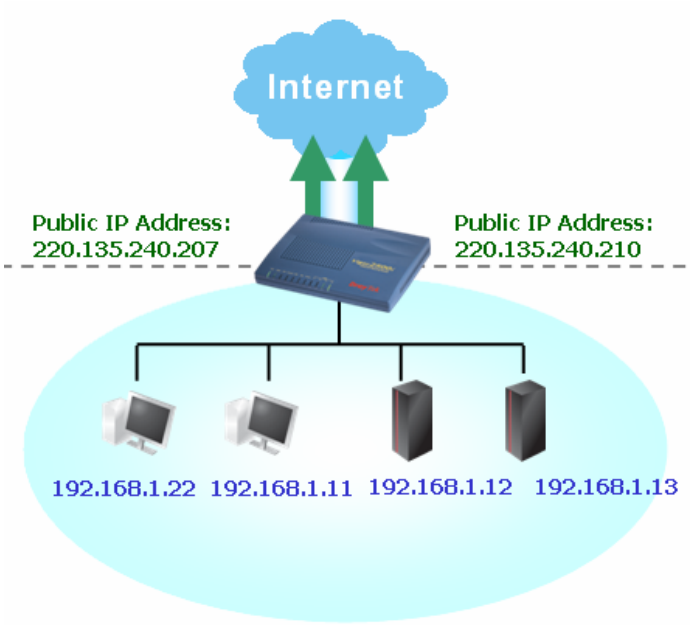
Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want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

WAN Alias:

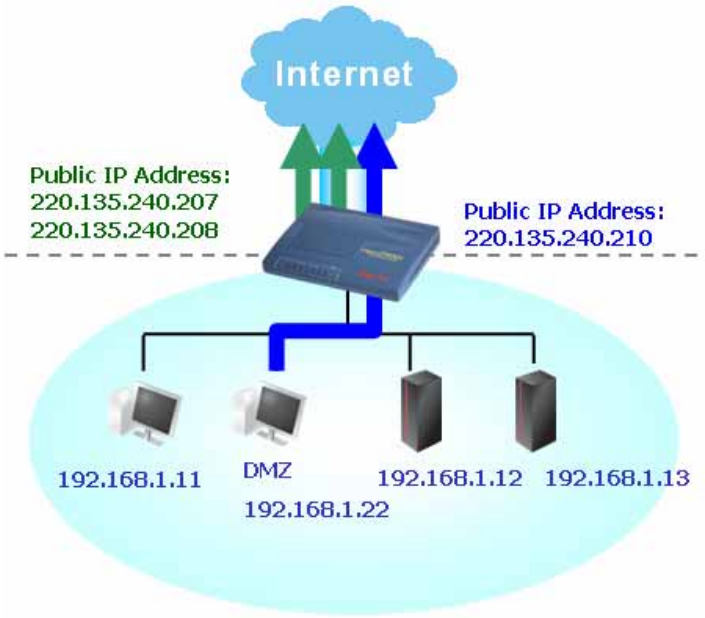
If you have multiple public IP addresses and would like to utilize them on the WAN interface, you can use **WAN IP Alias**. You may set up to 8 public IP addresses other than the current one you are using.



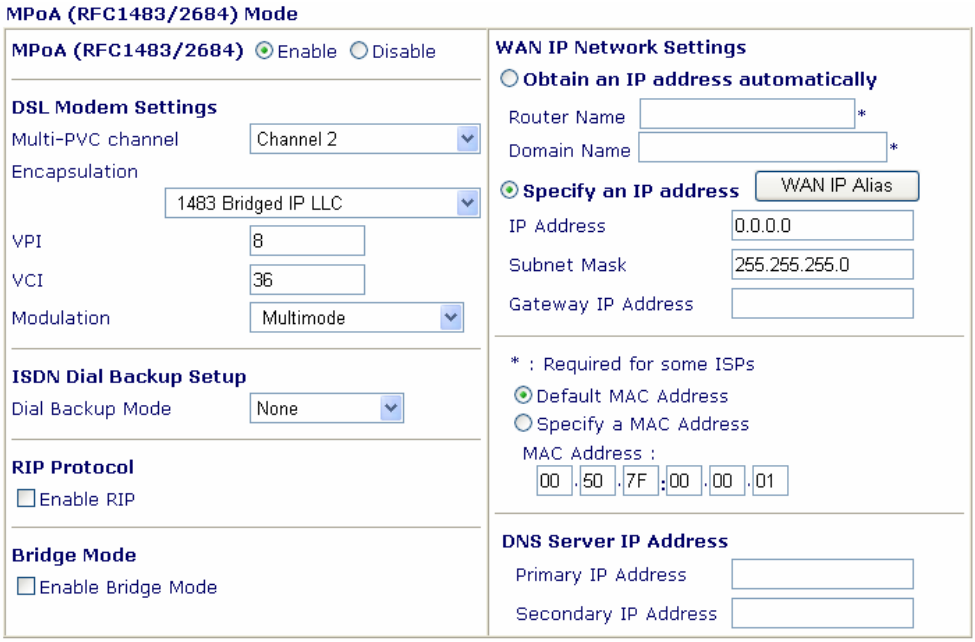
By checking the checkbox **Join NAT IP Pool**, data from NAT hosts will be round-robin forwarded on a per session basis.



If you don't check **Join NAT IP Pool**, you can still use these public IP addresses for other purpose, such as DMZ host, Open Ports. You may refer to Chapter 5 NAT for setting details.



3.2.2 MPoA



DSL Modem Settings

Set up the DSL parameters according to the information provided by your ISP.

ISDN Dial Backup Setup

None	Disable this function
Packet trigger	Enable this function when packet
Always on	Always enable this function

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.

WAN IP Network Settings

You can **Obtain an IP address automatically** by specifying Router Name and Domain Name which you get IP address from, or just **Specify an IP Address**.

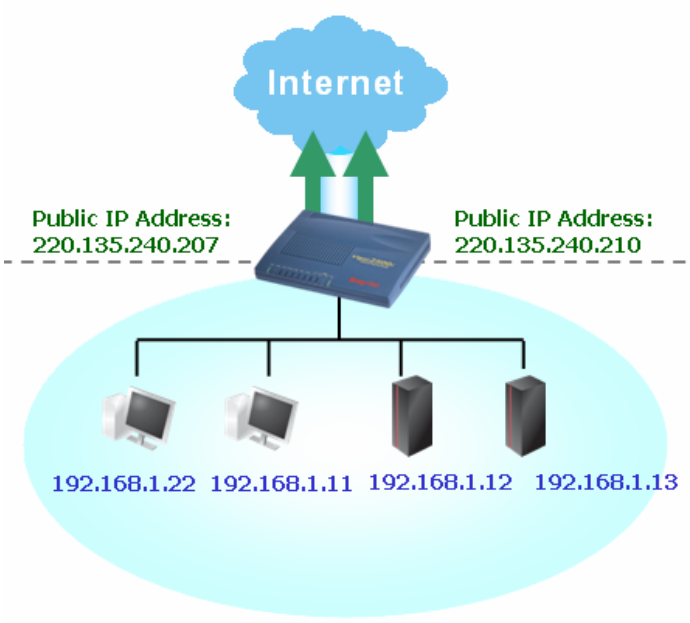
WAN IP Alias：

If you have multiple public IP addresses and would like to utilize them on the WAN interface, you can use WAN IP Alias. You may set up to 8 public IP addresses other than the current one you are using.

WAN IP Alias (Multi-NAT)

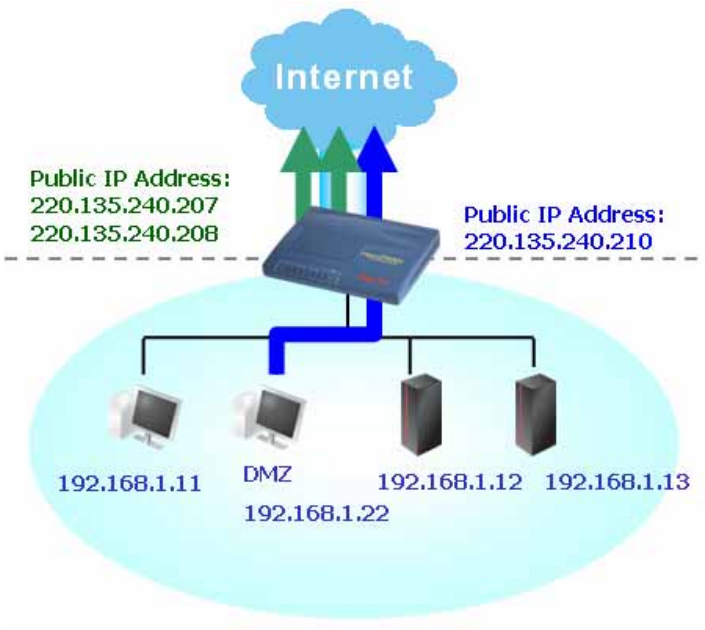
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	---	v
2.	☑	220 . 135 . 240 . 207	☑
3.	☐	. . .	☐
4.	☐	. . .	☐
5.	☐	. . .	☐
6.	☐	. . .	☐
7.	☐	. . .	☐
8.	☐	. . .	☐

By checking the checkbox **Join NAT IP Pool**, data from NAT hosts will be round-robin forwarded on a per session basis.



If you don’t check **Join NAT IP Pool**, you can still use these public IP

addresses for other purpose, such as DMZ host, Open Ports. You may refer to Chapter 5 NAT for setting details.



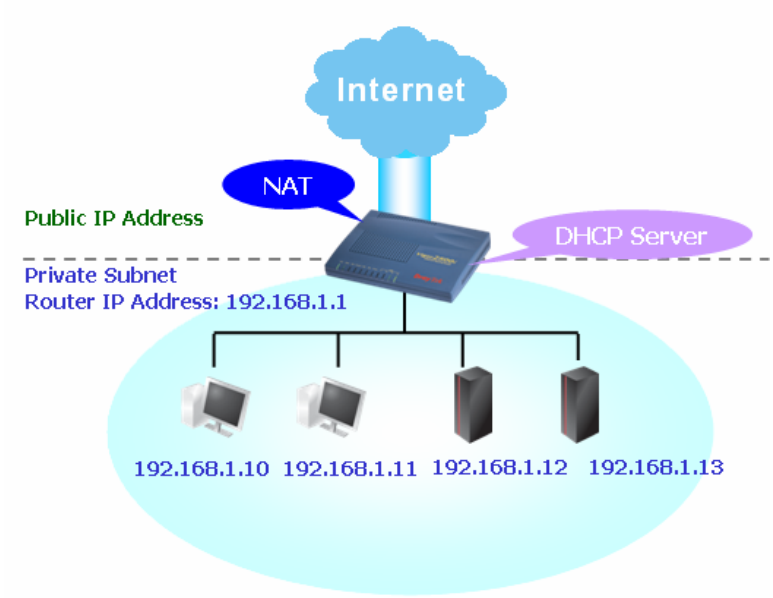
Chapter 4
LAN Setup

4.1 Introduction

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

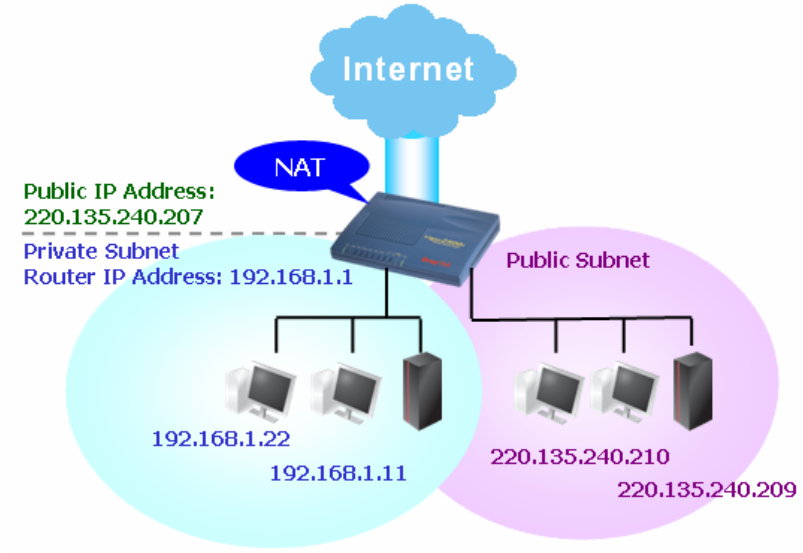
Basics for Creating Your LAN

The most generic function of Vigor router is NAT, which creates a private subnet of your own. As mentioned in Chapter 3.1, the router will talk to other public hosts on the Internet using public IP address while talking to local hosts using its private IP address. What NAT does is to translate from public IP address to private IP address in order to forward the right packets to the right host and vice versa. Besides, Vigor Router has a built-in DHCP server that assigns private IP address to each local host. Thus basically no effort is needed to create a LAN structure as shown below:



Advanced for Creating Your LAN

In some special case, you may own a public IP subnet from your ISP such as 220.135.240.0/24. This means you are able to set up a public subnet or we call 2nd subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing purpose to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



Routing Information Protocol (RIP)

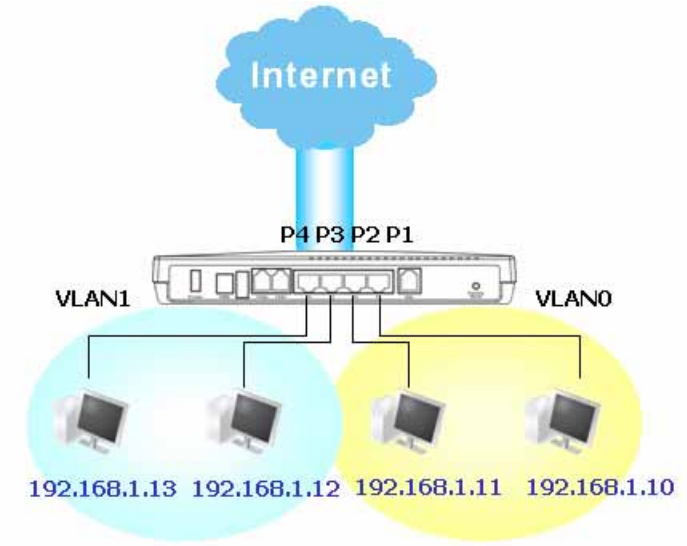
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address at will and the routers will automatically inform each other.

Static Routes

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

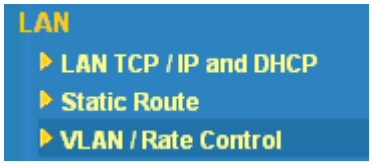
Virtual LANs and Rate Control

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



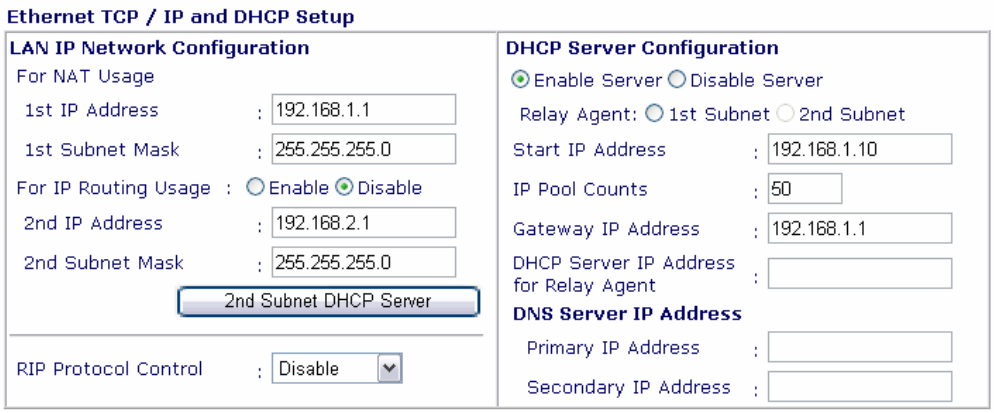
4.2 Settings

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



4.2.1 LAN TCP/IP and DHCP

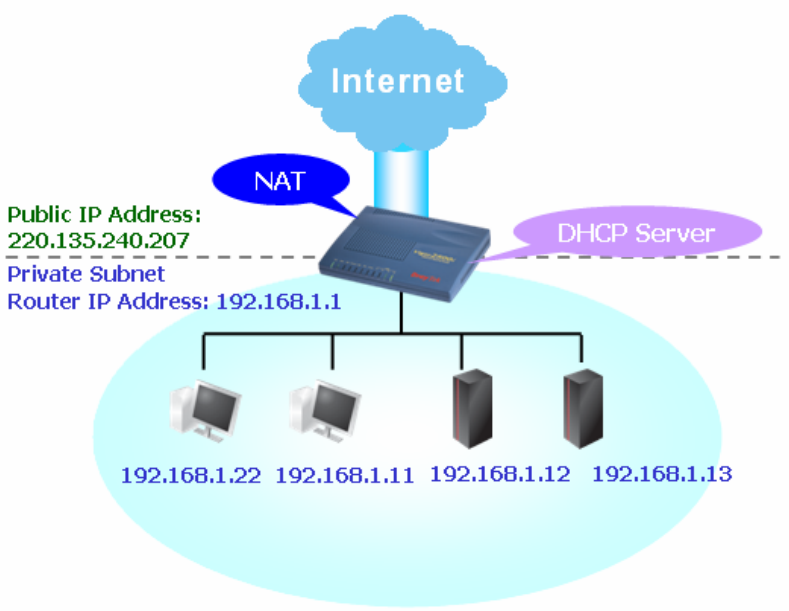
Click on **LAN TCP/IP and DHCP**, and you will see as show below.

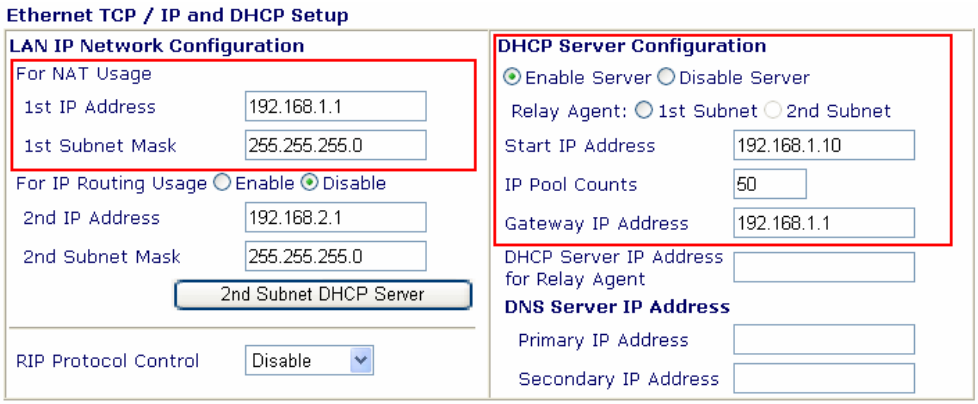


Here we will provide two common scenarios and followed by detail explanation of each field.

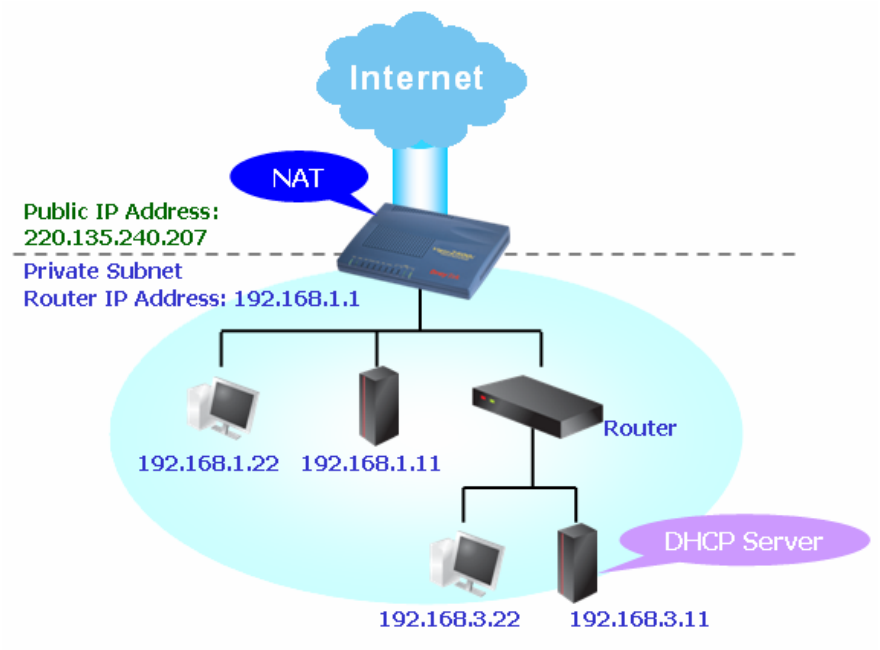
Settings of 1st subnet – A Subnet Created Using NAT

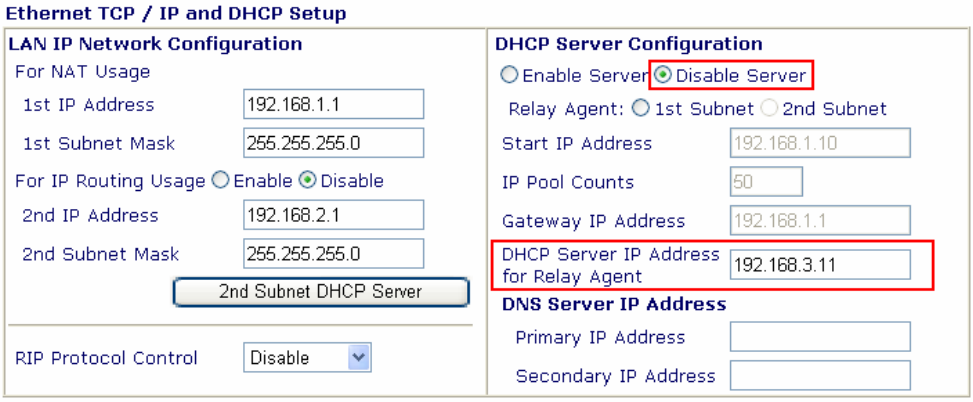
An example of default setting and the corresponding deployment are as shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host a 192.168.1.x IP address starting from 192.168.1.10.





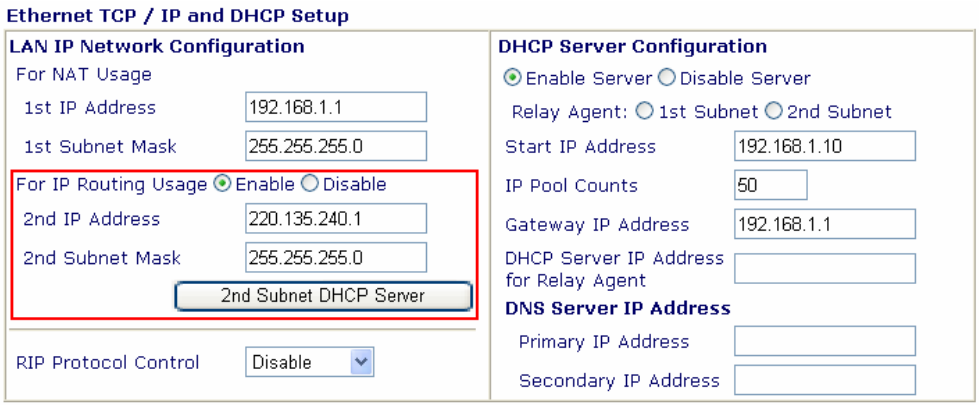
To using another DHCP server in the network rather than the built-in one of Vigor Router, you may have to change the settings as show below.

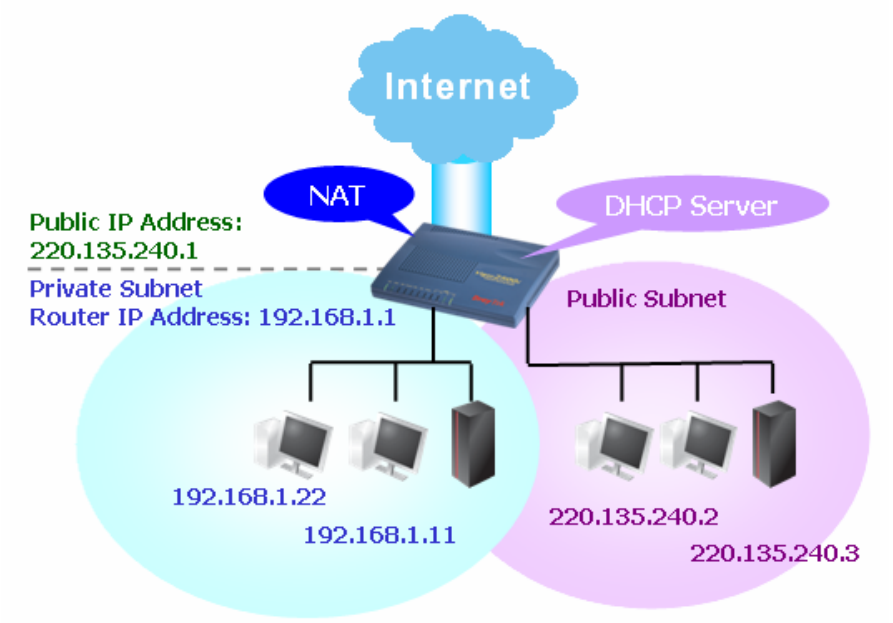




Settings of 2nd subnet – A Public Subnet

An example of setting Vigor router for IP routing of public subnet and the corresponding deployment are as shown below.





LAN IP Network Configuration

Here we provide explanation of each field.

For NAT Usage:

1st IP Address	Private IP address for connecting to a local private network (Default: 192.168.1.1).
1st Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/ 24)

For IP Routing Usage: (Default: Disable)

2nd IP Address	Secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24)
2nd Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/ 24)
2nd DHCP Server	You can configure the router to serve as a DHCP server for the 2nd subnet. **Start IP Address:** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254. **IP Pool Counts:** Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, The range of IP address issuance by the DHCP server will be from 220.135.240.2 to 220.135.240.11. **MAC Address:** Enter the MAC Address of the hosts to create a list of hosts to be assigned, deleted or edited IP address from above pool.  Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control

Disable	Deactivate the RIP protocol. This will lead to a stoppage of the exchange of routing information between routers. (Default)
1st Subnet	Select the router to change the RIP information of the 1st

	subnet with neighboring routers.
2nd Subnet	Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP Server Configuration

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

If you wan to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

Enable Server	Let the router assign IP address to every host in the LAN
Disable Server	You manually assign IP address to every host in the LAN
Relay Agent **1st subnet/2nd subnet**	Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts	Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address	Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default

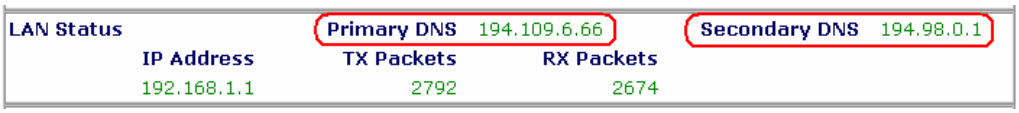
	gateway.
DHCP Server IP Address for Relay Agent	Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

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

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



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.

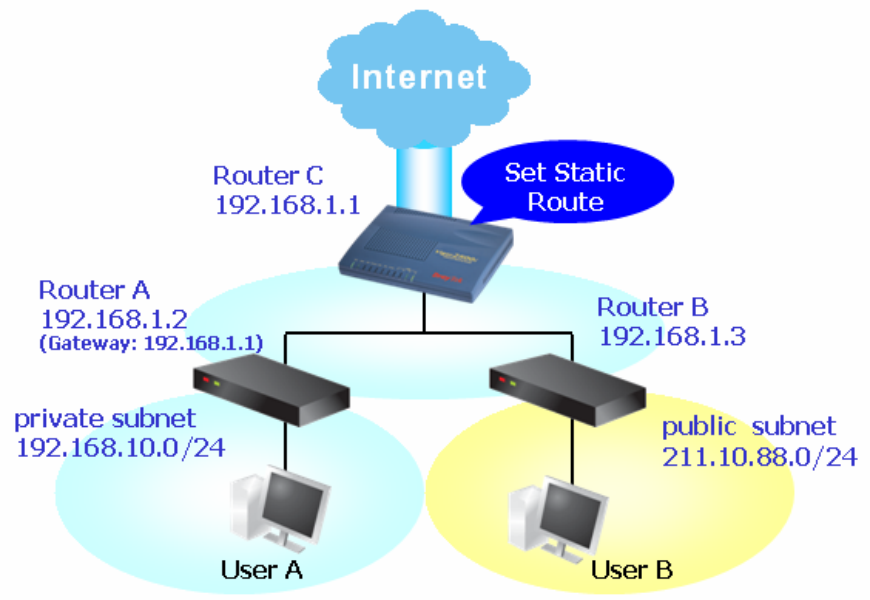
4.2.2 Static Route

Add Static Routers to Private and Public Networks

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

- You use the Main Router to surf the Internet.
- You create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- You create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- You have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before we set Static Route, User A cannot talk to User B because the Router A can only forward recognized packets to its default gateway Main Router.



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

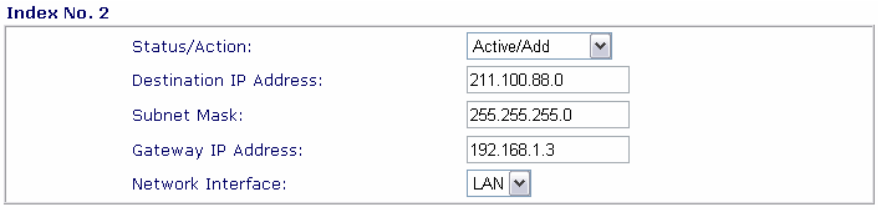
   We apply RIP Protocol Control to the 1st Subnet for two reasons. The first one is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second one is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

2. Click the **Static Route Setup** tab and click on the **Index Number.** You now add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2.

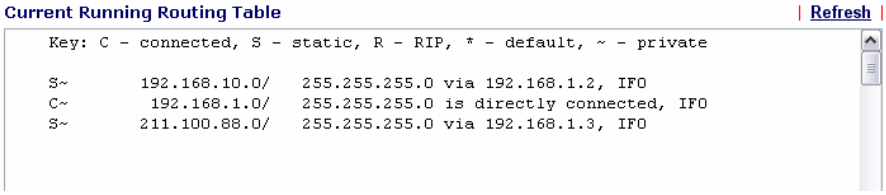
Index No. 1

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. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.2.

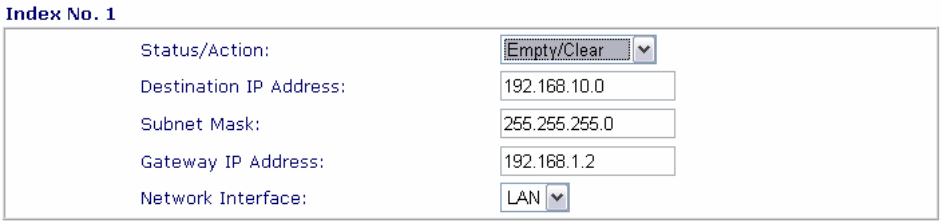


4. Click **Diagnostics >>Routing Table** to verify the current routing table.



Delete or Deactivate Static Route

1. Click the **Static Route Setup** tab and in the Index Number screen, select the index number you would like to delete.
2. Select **Empty/Clear** from the drop-down menu, and then click the **OK** button to delete the route.



4.2.3 VLAN/Rate Control

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port.

Click on **VLAN/Rate Control** and you will see the below.

VLAN Configuration

☐ Enable

	P1	P2	P3	P4
VLAN0	☐	☐	☐	☐
VLAN1	☐	☐	☐	☐
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

Rate Control

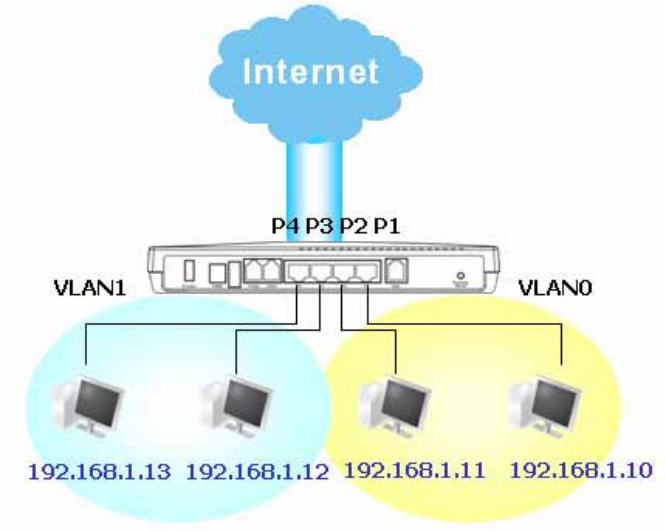
☐ Enable

	Out		In	
	Enable	Rate	Enable	Rate
P1	☐	640Kbps	☐	640Kbps
P2	☐	640Kbps	☐	640Kbps
P3	☐	640Kbps	☐	640Kbps
P4	☐	640Kbps	☐	640Kbps

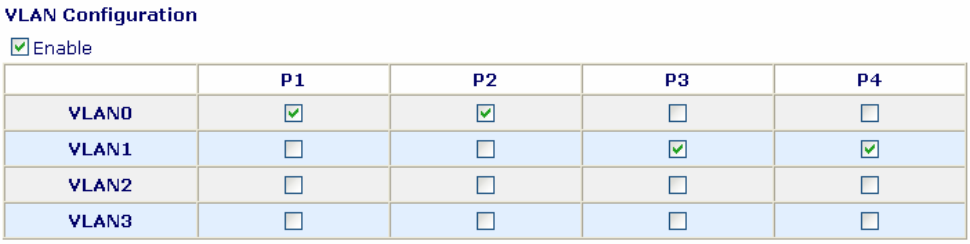
Add/Remove VLANs

Here is an example of setting VLANs.

- VLAN 0 is consisted of hosts linked to P1 and P2
- VLAN 1 is consisted of hosts linked to P3 and P4



So after check the box to enable VLAN function, you will check the table according to the needs as shown below.

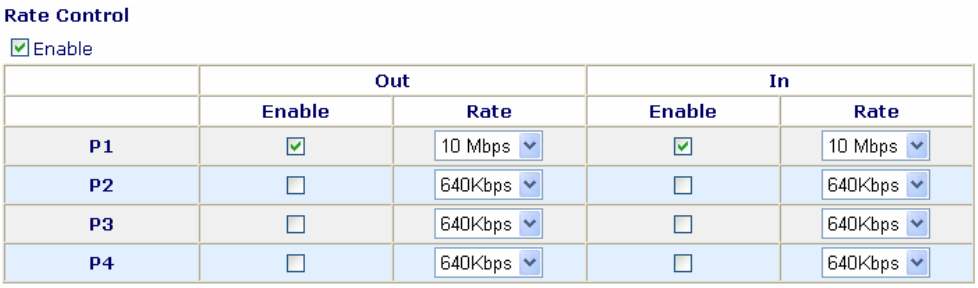


To remove VLAN, uncheck the needed box and click OK to save.

Rate Control

You may manage the in and out rate of one physical port. There are 4 level of speed: 650Kbps, 1.5Mbps, 3Mbps, 5.5Mbps and 10Mbps.

To set the in and out rate of P1 to 10Mbps, you can set as shown below.



Chapter 5
NAT Setup

5.1 Introduction

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

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

The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

5.2 Settings

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

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

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

Port Redirection	For the packets destined to specific public port from the external network, the router will forward them to a specific private port of a specific local host.
Open Ports	Similar to port redirection, it also enables users to define a range of ports to be opened and forward the traffic to the same port of internal hosts.
DMZ host	It allows one local host to be completely exposed to the Internet by opening all its ports for the purpose of some special services. All incoming packets will be forwarded to the designated PC.

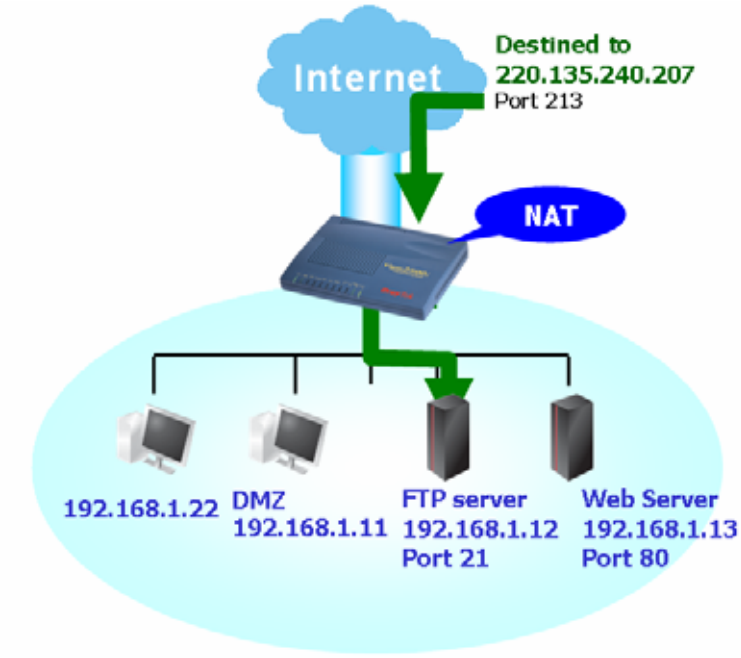
Note that if you enable these options simultaneously, a priority scheme will be adopted to avoid the possible conflicts. The precedence order is defined : **Port Redirection > Open Ports > DMZ host**

Check Status

Click **Diagnostics** to check the detail information of address/port mapping table in the router.

5.2.1 Port Redirection Table

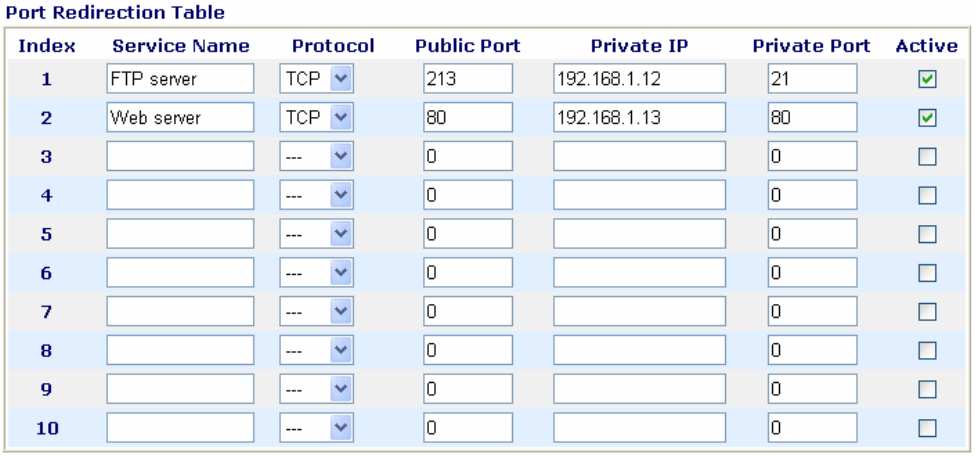
Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually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



The port redirection can only apply to incoming traffic. The server users inside the LAN can not access public IP address of the server. The correct route is to access the server using the local private IP address of the server, or you should 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.

The **Port Redirection Table** provides 10 port-mapping entries for the internal hosts.



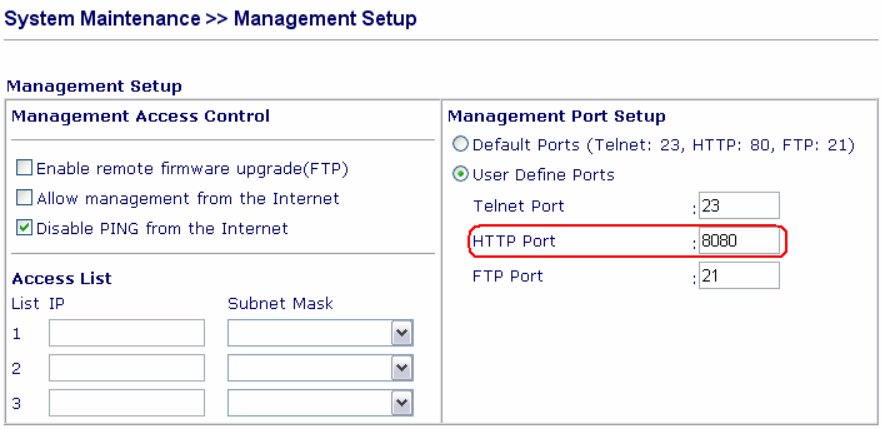
Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	FTP server	TCP	213	192.168.1.12	21	☑
2	Web server	TCP	80	192.168.1.13	80	☑
3		---	0		0	☐
4		---	0		0	☐
5		---	0		0	☐
6		---	0		0	☐
7		---	0		0	☐
8		---	0		0	☐
9		---	0		0	☐
10		---	0		0	☐

Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
Public Port	Specify which port can be redirected to the specified **Private IP and Port** of the internal host.
Private IP	Specify the private IP address of the internal host providing the service.
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

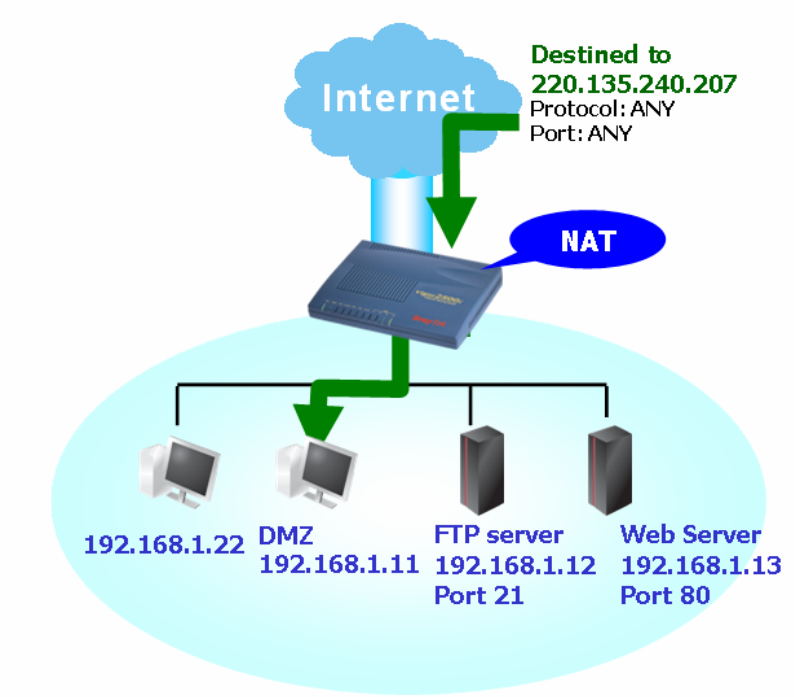
Note that because the router has its own built-in services(servers), such as Telnet, HTTP and FTP etc. Since the common port numbers of these services(servers) are all the same, you may need to reset the router's in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://92.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g.http://192.168.1.1:8080 instead of port 80.



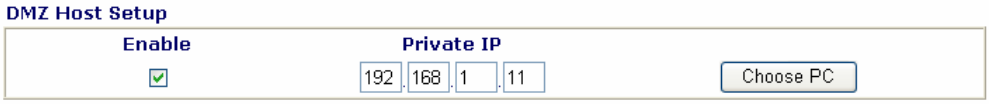
5.2.2 DMZ Host Setup

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



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

Click **DMZ Host Setup** to open the setup page, as shown below. Each item in the setup page is described below.



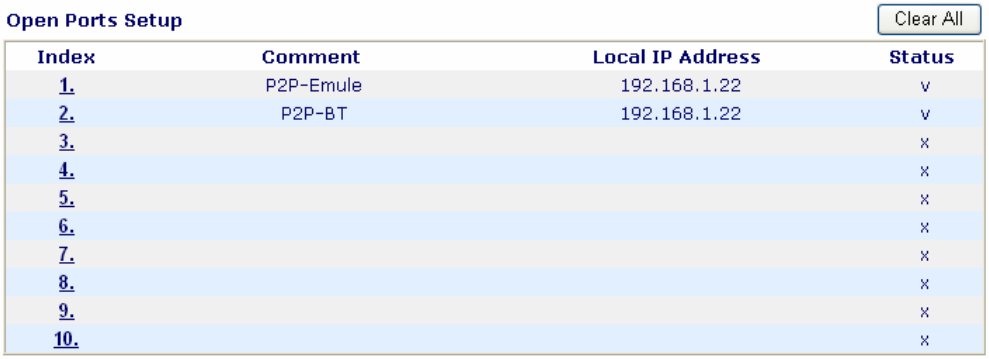
If you previously has set up a set of **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find them in **Aux. WAN IP list** for your selection.

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

5.2.3 Open Ports

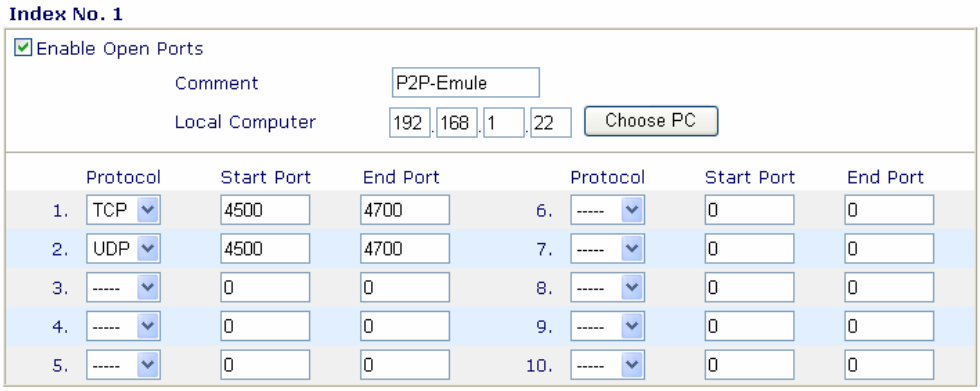
Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application(BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any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

In the Vigor router, the **Open Ports** facility provides 10 entries for internal hosts. Below is the table of the setup summary.

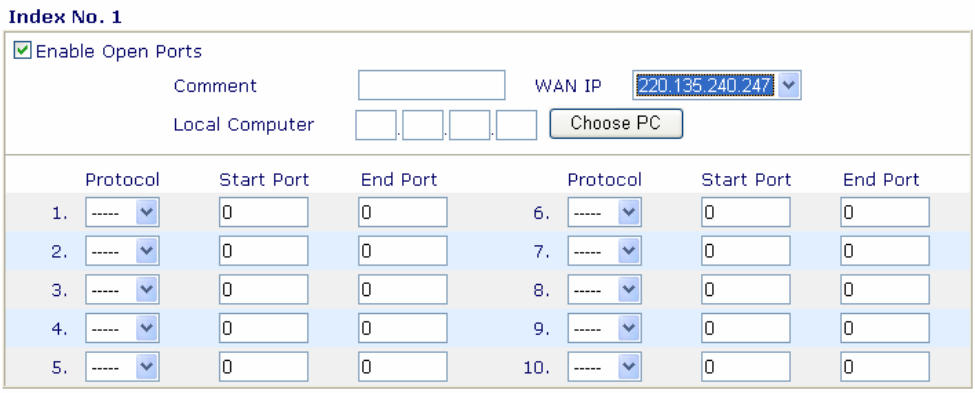


Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

Click one index number. The index entry setup page will pop up. In each index entry, you can specify 10 port ranges for diverse services.



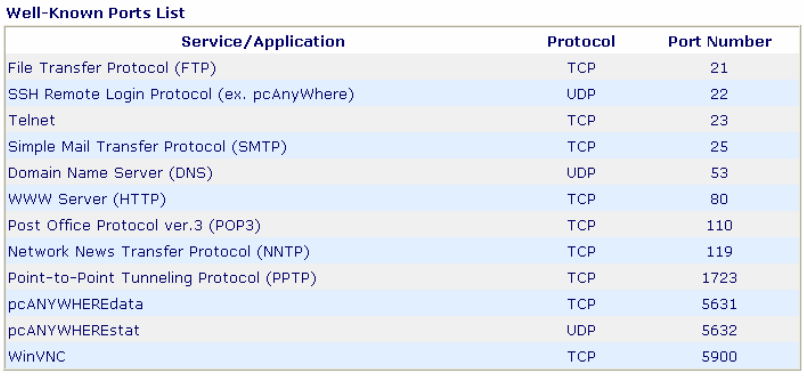
If you previously has set up a set of **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find them in **WAN IP** for your selection.



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

5.2.4 Well-known Port Number List

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



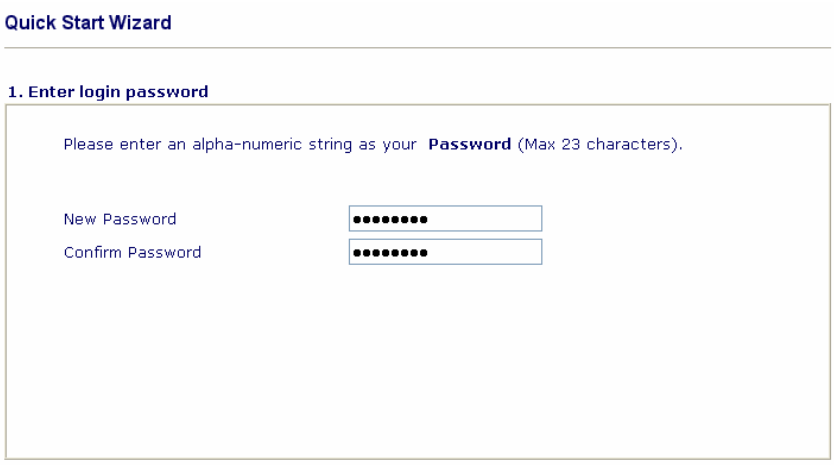
Chapter 6
Firewall Setup

6.1 Introduction

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

Before you start

Before introducing the advanced security firewall, we would like to remind you the most basic security concept is to set user name and password while you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.



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

Firewall Facilities

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

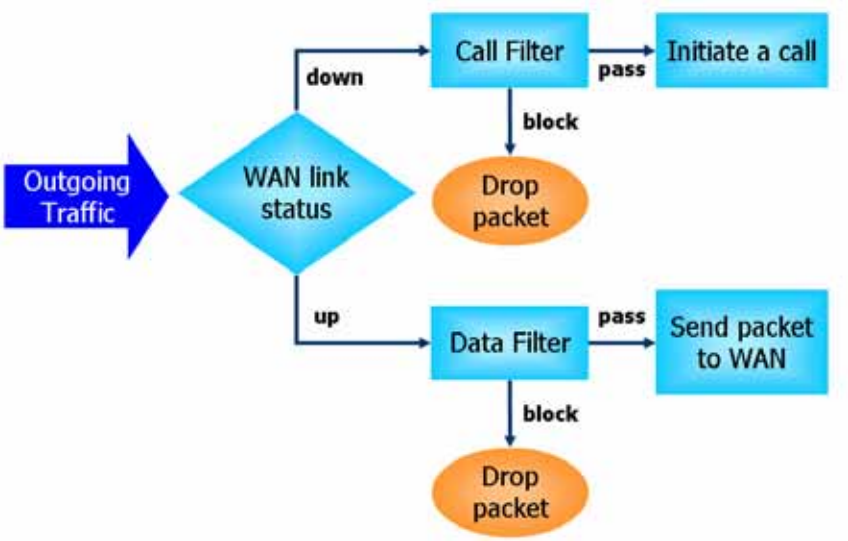
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

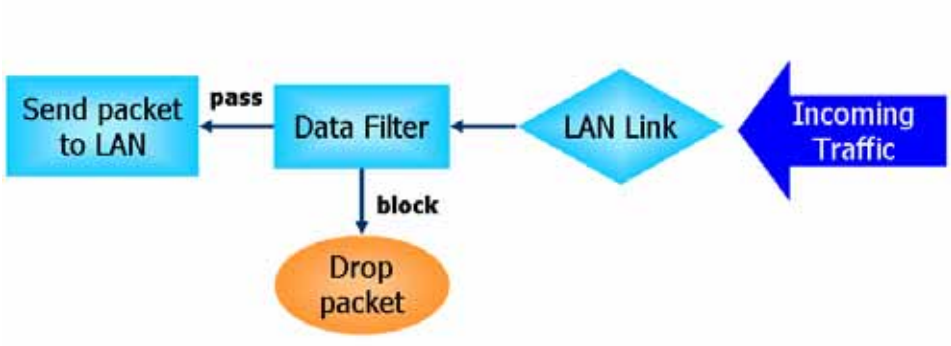
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

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

Application Blocking

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

Denial of Service (DoS) Defense

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

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

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

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

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

Content Filtering

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

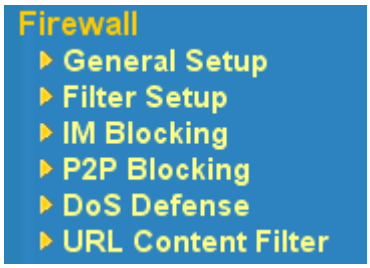
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines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

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX,

Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

6.2 Settings

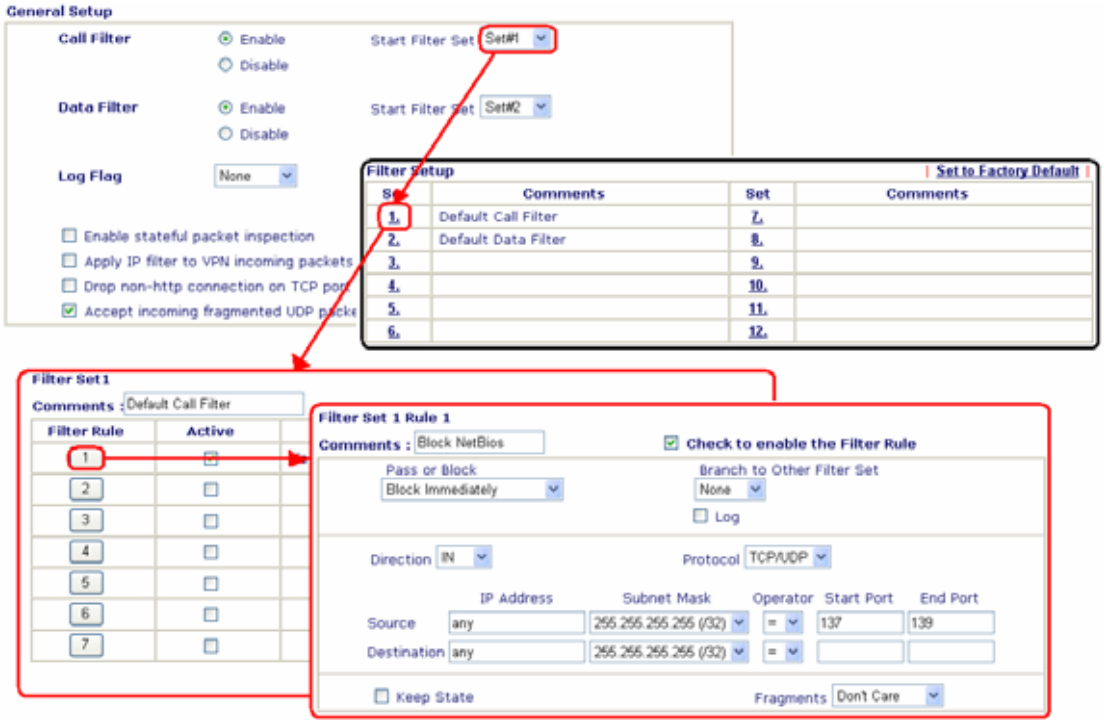
Click **Firewall Setup** to open the setup page.



General Setup	General settings of IP Filter and common options.
Filter Setup	Set up to 12 filter sets for IP Filter configurations.
IM Blocking	Blocking function for common instant messenger applications. Setup time schedule if needed.
P2P Blocking	Blocking function for common peer to peer applications. Setup time schedule if needed.
DoS Defense	Set up the DoS defense facility for detecting and mitigating the DoS attacks.
URL Content Filter	Set up filter to block inappropriate URL to protect children at home or prevent employee's misusages. Block web feature that might carry malicious codes.

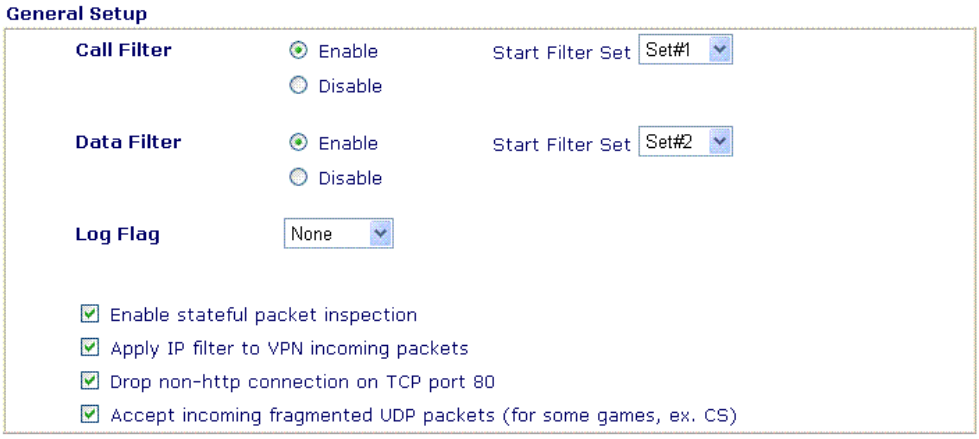
The following will explain how to accomplish settings in conjunction with the **General Setup** and **Filter Setup.**

As stated before, all the traffic will be separated and arbitrated using one out of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



6.2.1 General Setup

Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the Log Flag settings, Enable Stateful packet inspection, Apply IP filter to VPN incoming packets, Drop non-http connection on TCP port 80, and Accept incoming fragmented UDP packets (for some games, ex. CS).



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

Call Filter

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

Data Filter

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

Log Flag

For troubleshooting needs you can specify the filter log here.

None	The log function is not activated.
Block	All blocked packets will be logged.
Pass	All passed packets will be logged.
No Match	The log function will record all packets that are not matched.

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

6.2.2 Filter Setup

Filter Sets Summary

As soon as you click Filter Setup, first you will find the filter sets summary table. It will list all filters including two factory default filters. The comments field shows the Click on the set number to edit the individual set.

Filter Setup | Set to Factory Default |

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

Editing Filter Sets

Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check Active to enable the rule.

Filter Set 1

Comments : Default Call Filter

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

Next Filter Set None

Filter Rules

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

Active

Enable or disable the filter rule.

Comments

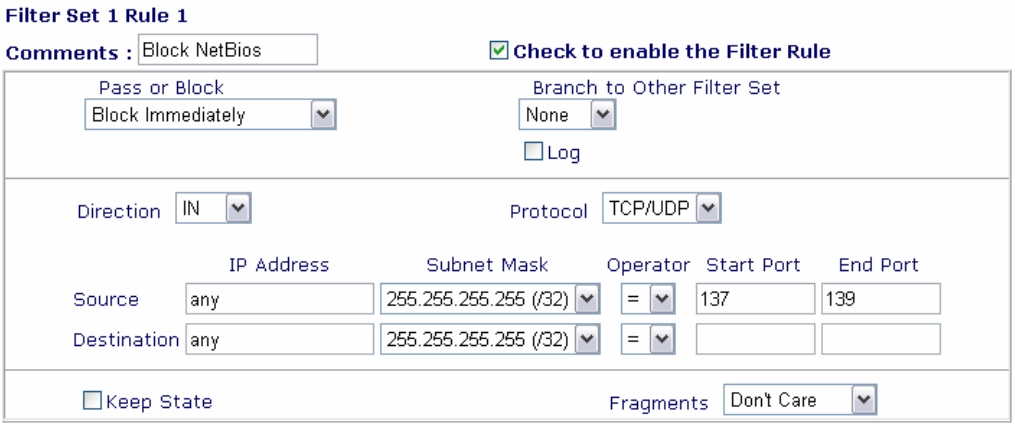
Enter filter set comments/description. Maximum length is 23–character long.

Next Filter Set

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

Editing Filter Rules

Click the Filter Rule index button to enter the Filter Rule setup page.



Comments

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

Check to enable the Filter Rule

Enables the filter rule.

Pass or Block

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

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

Branch to other Filter Set

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

Log

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

Direction (for Data Filter only)

Sets the direction of packet flow.

For the Call Filter, this setting is not available since Call Filter is only applied to outgoing traffic.

Protocol

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

IP Address

Specify a source and destination IP address for this filter rule to apply to. Place the symbol "**!**" before a specific IP Address will prevent this rule from being applied to that IP address. It is equal to the logical NOT operator. To apply the rule to all IP address, enter "any" or leave the field blank.

Subnet Mask

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

Operator, Start Port and End Port

The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number.

=	If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port).
!=	If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port).
>	Specify the port number is larger than the Start Port (includes the Start Port).
<	Specify the port number is less than the Start Port (includes the Start Port).

Keep State (for Data Filter only)

This function should work along with **Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port** settings.

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

Fragments (for Data Filter only)

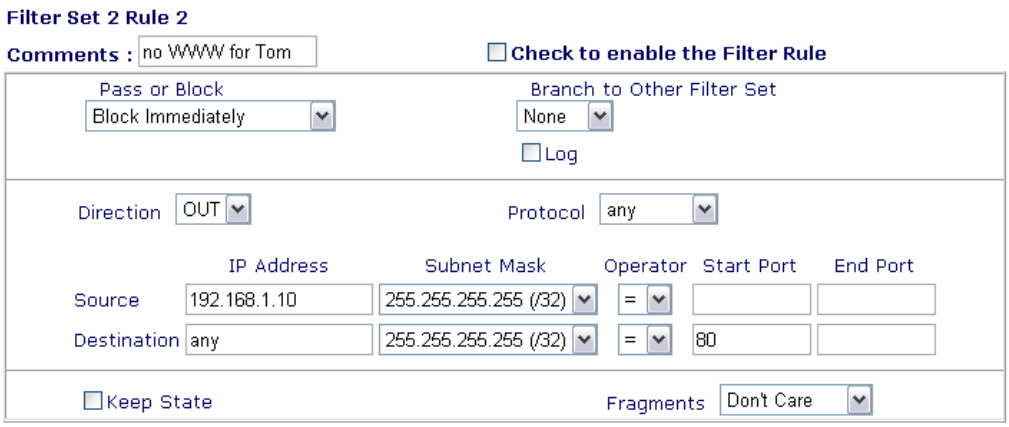
Specify the action for fragmented packets.

Don't care	No action will be taken towards fragmented packets.

Unfragmented	Apply the rule to unfragmented packets.
Fragmented	Apply the rule to fragmented packets.
Too Short	Apply the rule only to packets that are too short to contain a complete header.

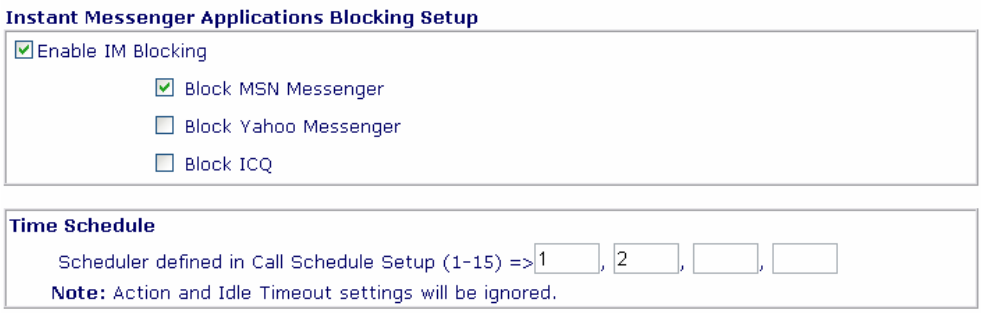
Example

This section will show a simple example to always restrict a user from accessing WWW services. Assume the IP address of the user is 192.168.1.10. In the Filter Set 2 - Data Filter, you can create a rule as shown below. Port 80 is the HTTP protocol port number for WWW services.



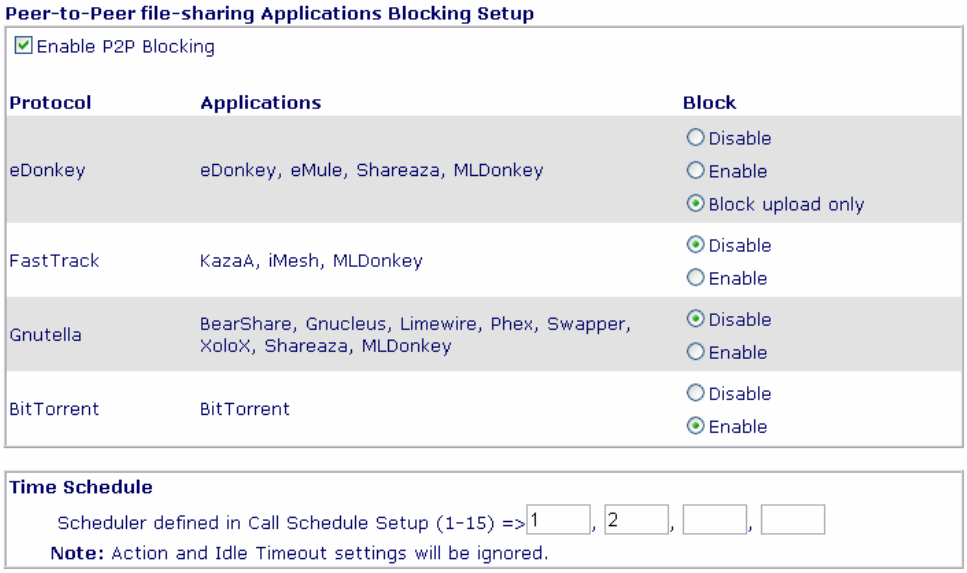
6.2.3 Instant Messenger(IM) Blocking

Click **IM Blocking** to view the setup window. You will see a list of common IM applications. Check to select the one(s) to block. To block selected IM applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.



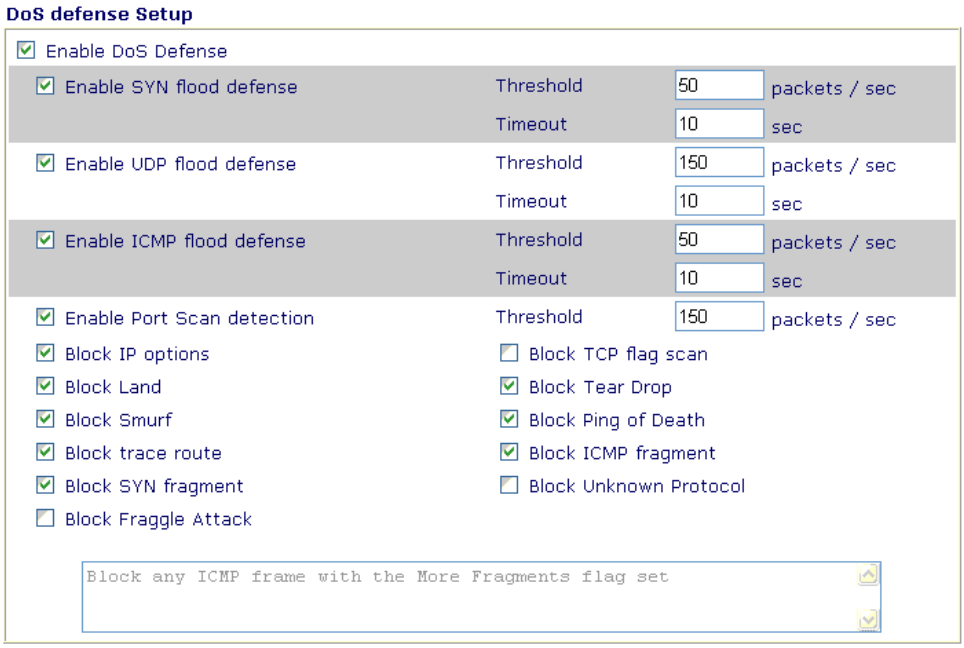
6.2.4 Peer-to-Peer(P2P) Blocking

Click **P2P Blocking** to view the setup window. You will see a list of common P2P applications. Check to select the one(s) to block. To block selected P2P applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.



6.2.5 DoS (Denial of Service) Defense

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



Enable Dos Defense

Click the checkbox to activate the DoS Defense Functionality.

Enable SYN flood defense

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

Enable UDP flood defense

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

second and 10 seconds, respectively.

Enable ICMP flood defense

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

Enable PortScan detection

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

Block IP options

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

Block Land

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

Block Smurf

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

Block trace router

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

Block SYN fragment

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

Block Fraggle Attack

Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.

Block TCP flag scan

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

Block Tear Drop

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

Block Ping of Death

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

Block ICMP Fragment

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

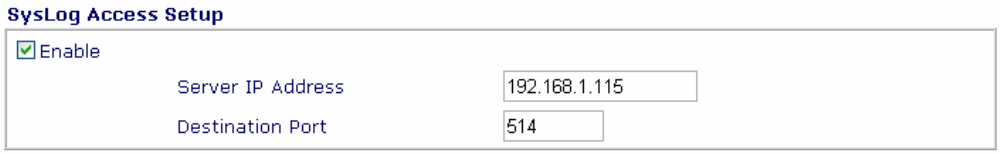
Block Unknown Protocol

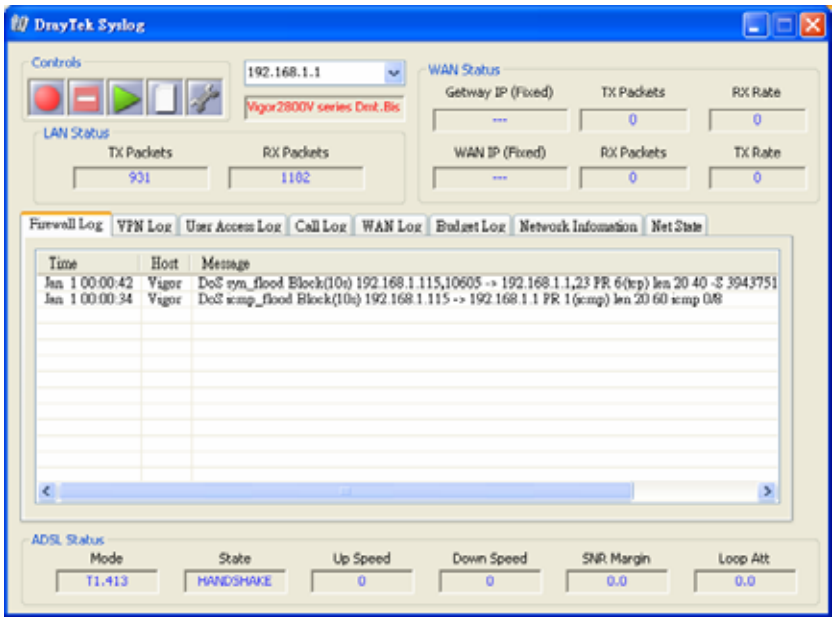
Click the checkbox to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router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

Warning Messages

We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. (Refer to Chapter 13 System Maintenance Syslog Access Setup for detail information.)

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





6.2.6 URL Content Filter

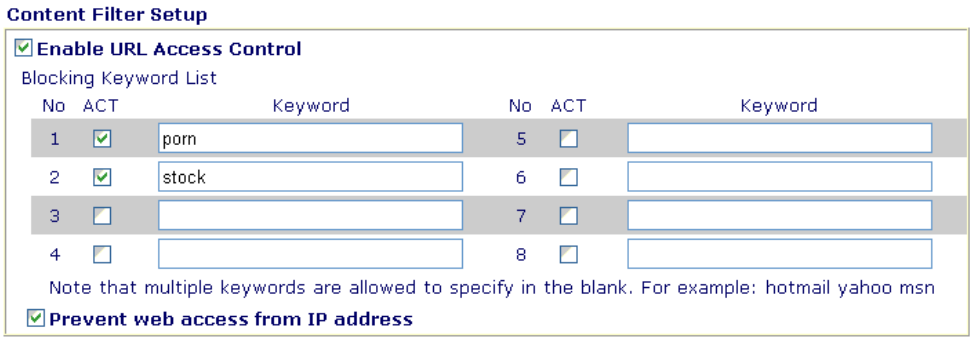
Based on the list of user defined keywords, the **URL Content Filter** facility in Vigor router inspects the URL string in every outgoing HTTP request. No matter the URL string is found full or partial matched with a keyword, the Vigor router will block the associated HTTP connection.

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

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

Enable URL Access Control

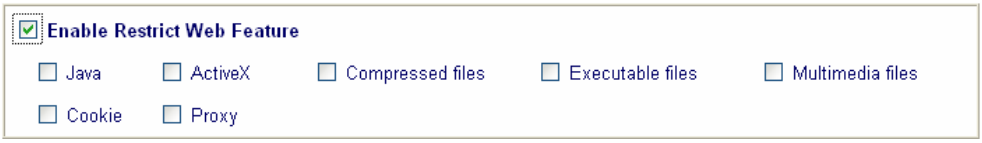
To enable **URL Access Control**, check the checkbox.



Keyword	The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.
Prevent web access from IP address	Check this checkbox to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control.

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

Enable Restrict Web Feature



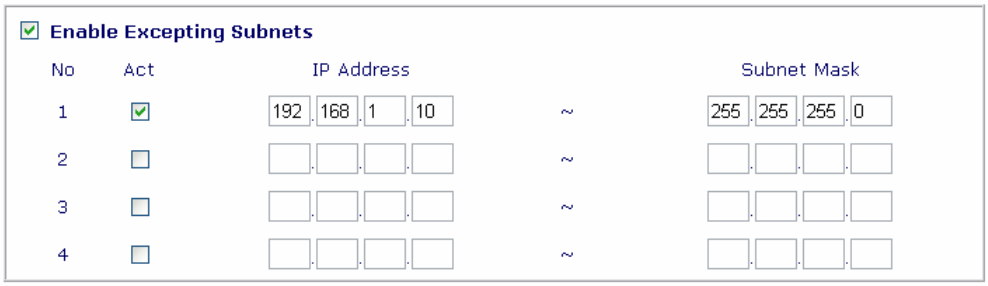
Java	Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.
ActiveX	Check the checkbox to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.
Compressed file	Check the checkbox to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router. **.zip, .rar,.arj,.ace,.cab,.sit**
Executable file	Check the checkbox to reject any downloading behavior of the executable file from the Internet. **.exe,.com,.scr,.pif,.bas,.bat,inf,.reg**

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

Cookie	Check the checkbox to filter out the cookie transmission from inside to outside world in order to protect the local user's privacy.
Proxy	Check the checkbox to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router. **.mov .mp3 .rm .ra .au .wmv** **.wav .asf .mpg .mpeg .avi .ram**

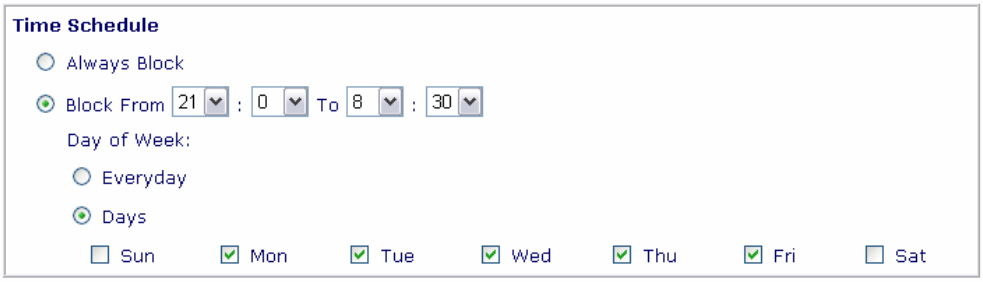
Enable Excepting Subnets

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.



Time Schedule

Specify what time should perform the URL content filtering facility.

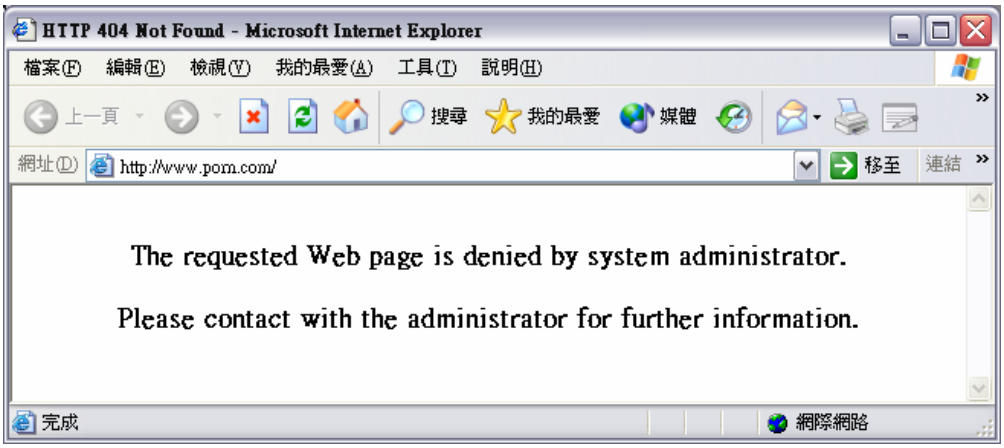


Always Block	Click it so that the URL content filtering facility can be executed on the Vigor router anytime.
Block from H1:M1 To H2:M2	Specify the appropriate time duration from H1:M1 to H2:M2 in one day, where H1 and H2 indicate the hours. M1 and M2 represent the minutes.
Days of Week	Specify which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

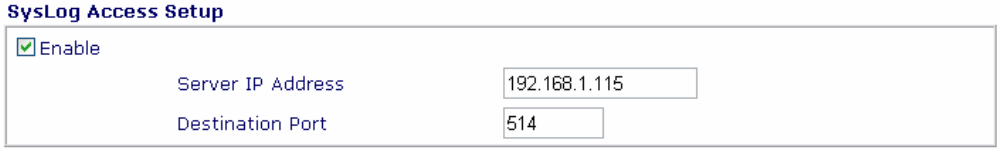
	Monday to Wednesday, then you should click the appropriate checkboxes (Monday, Tuesday, and Wednesday). Other days the URL content filtering facility will be silent.

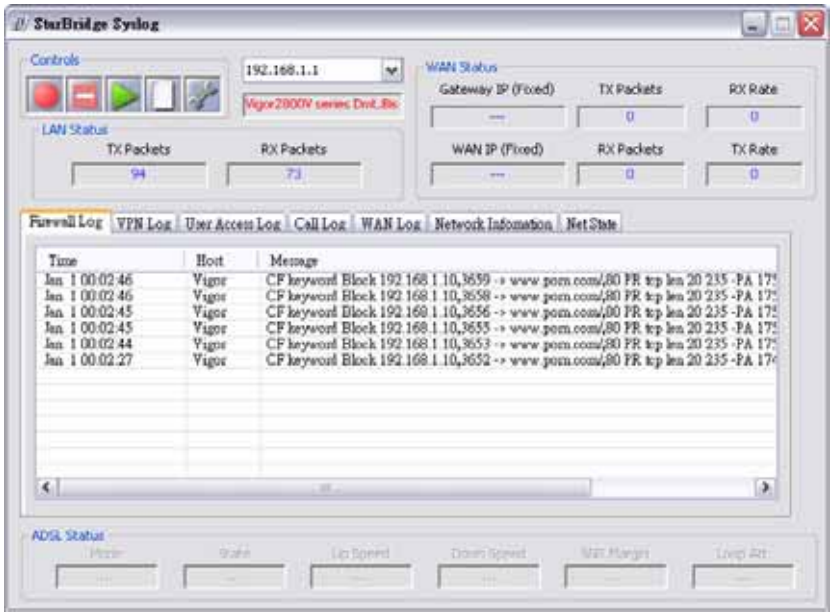
Warning Messages

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 Syslog daemon. The format for this kind of the warning messages is similar to those in the **IP Filter/Firewall** except for the preamble keyword "**CF**", followed by a name to indicate what kind of the HTTP request is blocked.




StarBridge Syslog
Controls
192.168.1.1
LAN Status
TX Packets
RX Packets
94
73
WAN Status
Gateway IP (Fixed)
TX Packets
RX Rate
WAN IP (Fixed)
RX Packets
TX Rate
Firewall Log
VPN Log
User Access Log
Call Log
WAN Log
Network Information
Net State
Time
Host
Message
Jan 1 00:02:46 Vigor CF keyword Block 192.168.1.10,3659 -> www.porn.com/,80 PR tcp len 20 235 -PA 175
Jan 1 00:02:46 Vigor CF keyword Block 192.168.1.10,3658 -> www.porn.com/,80 PR tcp len 20 235 -PA 175
Jan 1 00:02:45 Vigor CF keyword Block 192.168.1.10,3656 -> www.porn.com/,80 PR tcp len 20 235 -PA 175
Jan 1 00:02:45 Vigor CF keyword Block 192.168.1.10,3655 -> www.porn.com/,80 PR tcp len 20 235 -PA 175
Jan 1 00:02:44 Vigor CF keyword Block 192.168.1.10,3653 -> www.porn.com/,80 PR tcp len 20 235 -PA 175
Jan 1 00:02:27 Vigor CF keyword Block 192.168.1.10,3652 -> www.porn.com/,80 PR tcp len 20 235 -PA 176
ADSL Status

Chapter 7
Application Setup

7.1 Introduction

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

Dynamic DNS

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

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

Call Schedule

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

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they

need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. UPnP is available on Windows XP and the router provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

QoS Control

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

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

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

There are two components within Primary configuration of QoS deployment:

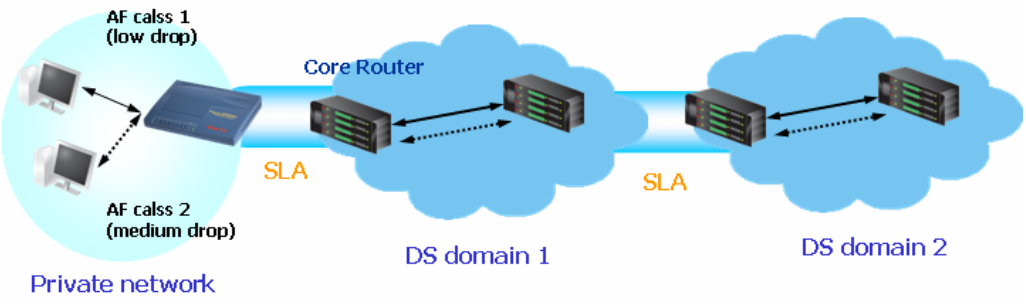
- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

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

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

Vigor routers as edge routers of DS domain shall check the marked

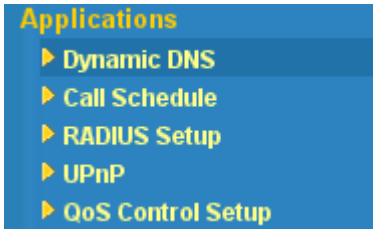
DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the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



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

7.2 Settings

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



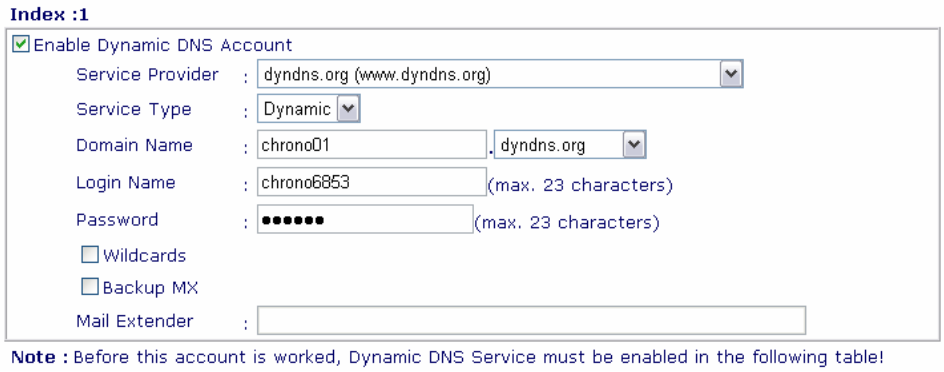
Dynamic DNS	Settings of domain names you subscribe from up to three Dynamic DNS service providers.
Call Schedule	Settings of a real time clock that update automatically from an Internet time server (NTP).
RADIUS Setup	Settings of RADIUS server
UPnP	Settings of UPnP protocol available for directly connected

	PC peripherals with the existing Windows 'Plug and Play' system.
QoS Control Setup	Settings of QoS control related information, such as address, DiffServ CodePoint, Service Type etc.

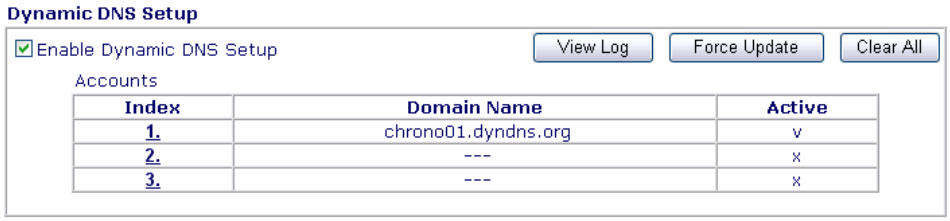
7.2.1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say ***hostname.dyndns.org***, and an account with username: ***test*** and password: ***test***.
2. In the DDNS setup menu, check **Enable Dynamic DNS Setup.**
3. Select Index number **1** to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct **Service Provider**: **dyndns.org,** type the registered hostname: ***hostname*** and domain name suffix: **dyndns.org** in the **Domain Name** block. The following two blocks should be typed your account **Login Name**: ***test*** and **Password**: ***test***.



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



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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

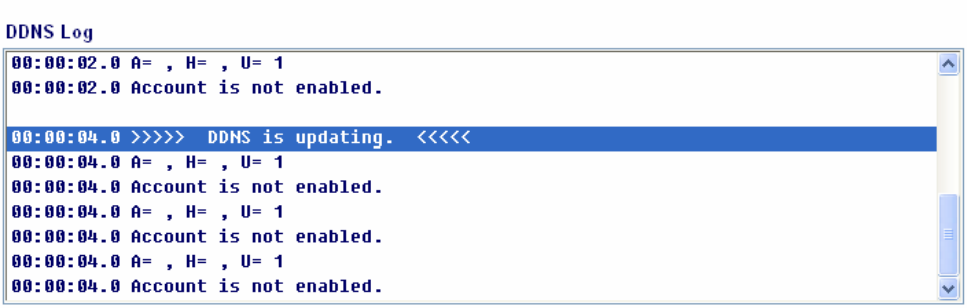
Validation and Troubleshooting

Ping the Registered Domain Name

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

View the DDNS Logs

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



Where A : Login Name

H : Domain Name without suffix.

Return Code= good 61.230.170.145

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

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

Check if the IP address in the circle is the same as the Return Code in the DDNS logs. This indicates that the update is successful.

7.2.2 Call Schedule

Before you start

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

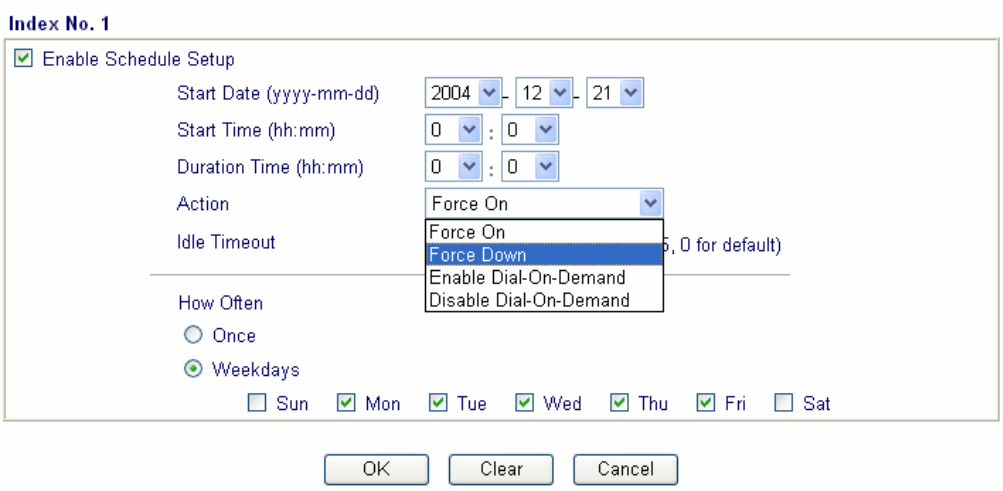
Set up call schedules

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN and Remote Access >> LAN-to-LAN**

settings

Add a Call Schedule

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



Enable Schedule Setup

Check to enable the schedule.

Start Date (yyyy-mm-dd)

Specify the starting date of the schedule.

Start Time (hh:mm)

Specify the starting time of the schedule.

Duration Time (hh:mm)

Specify the duration (or period) for the schedule.

Action:

Specify which action Call Schedule should apply during the period of the schedule.

Force On	Force the connection to be always on.
Force Down	Force the connection to be always down.

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

Idle Timeout

Specify the duration (or period) for the schedule.

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

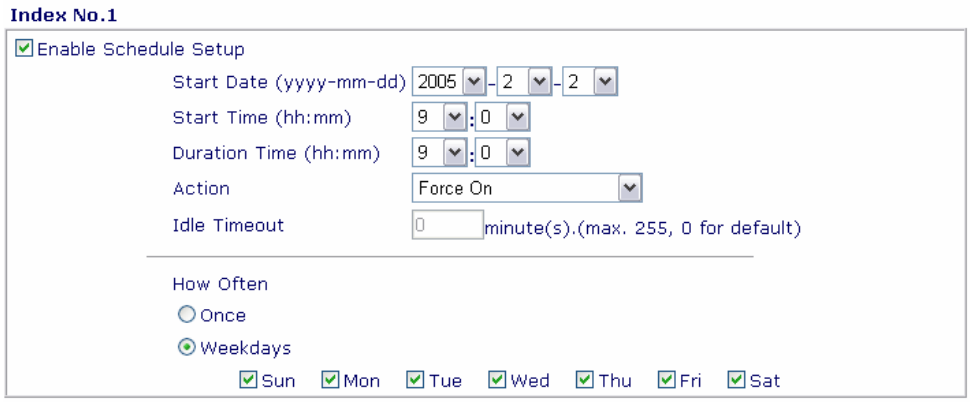
Example

Suppose you want to control the PPPoE Internet access connection to stay connected (Force On) from 9:00 to 18:00 in a whole week. From 18:00 to next 9:00 the Internet access should be disconnected (Force Down).

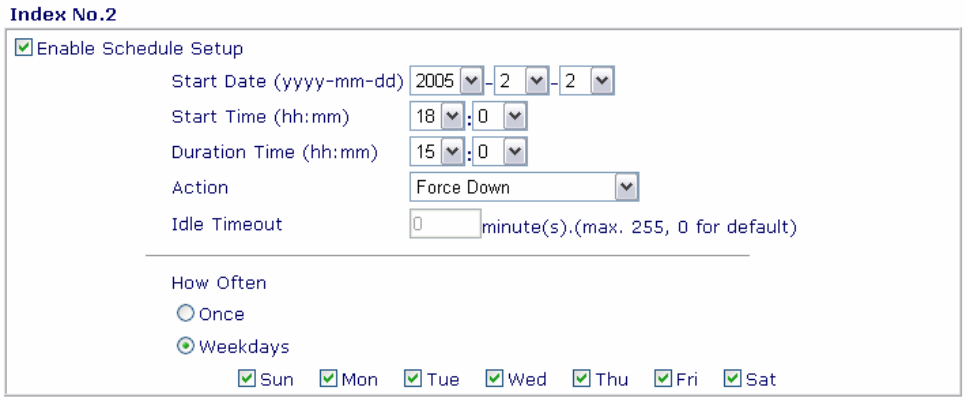
Office Hour:

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

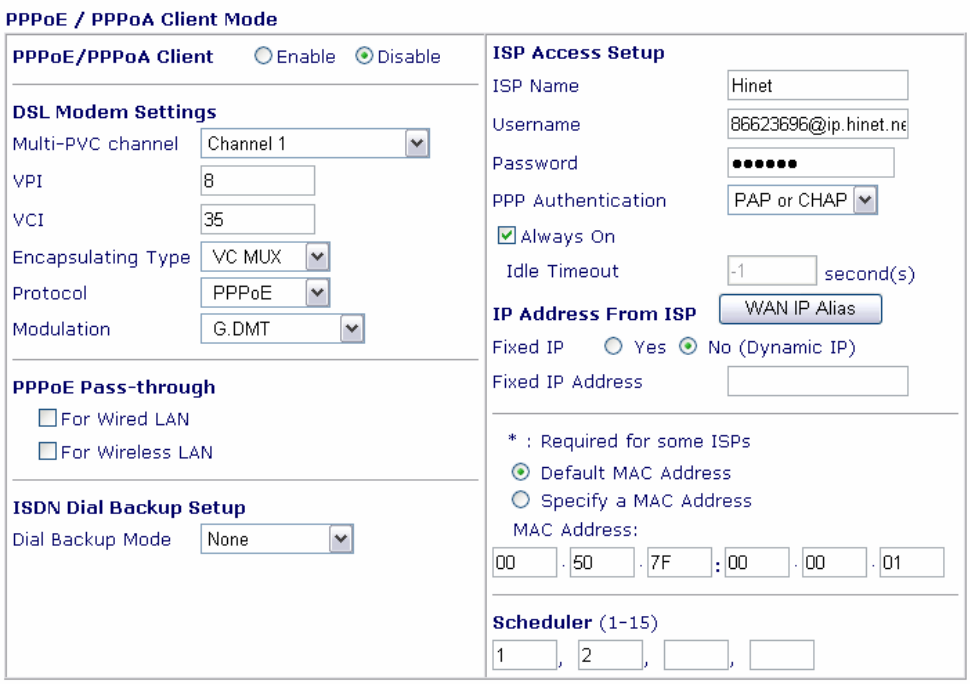
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.



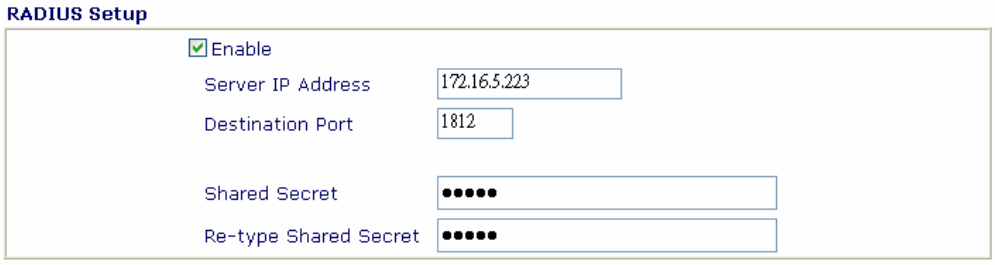
3. Configure the Force Down from 18:00 to next day 9:00 for whole week.



4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform “Force On” or “Force Down” action according to the time plan that has been pre-defined in the schedule profiles.



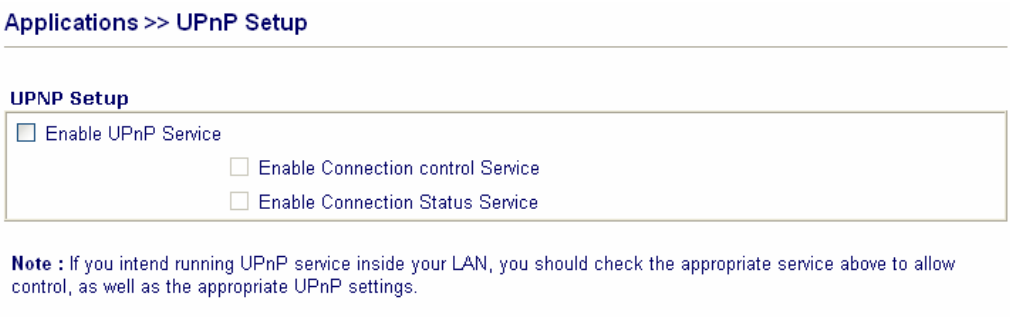
7.2.3 RADIUS



Enable	Check to enable RADIUS client feature
Server IP Address	Enter the IP address of RADIUS server
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812 , based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Re-type Shared Secret	Re-type the Shared Secret for confirmation.

7.2.4 UPnP

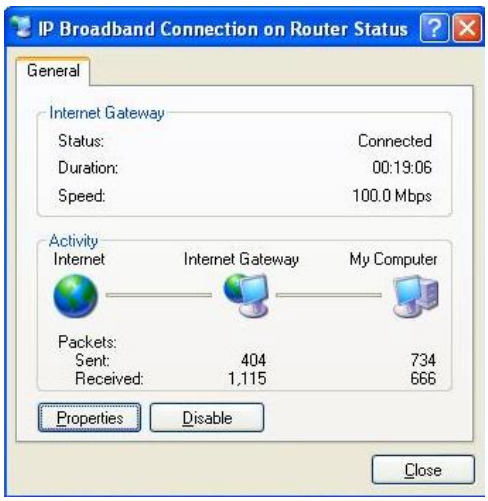
You can enter the **UPNP Setup** as below as below picture shown.



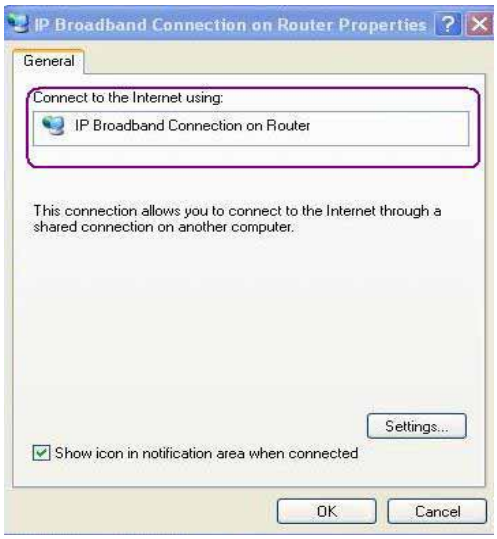
Enable UPNP Service:

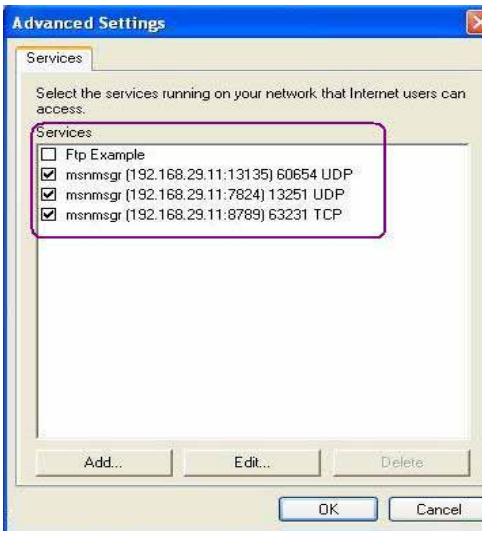
Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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



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





The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

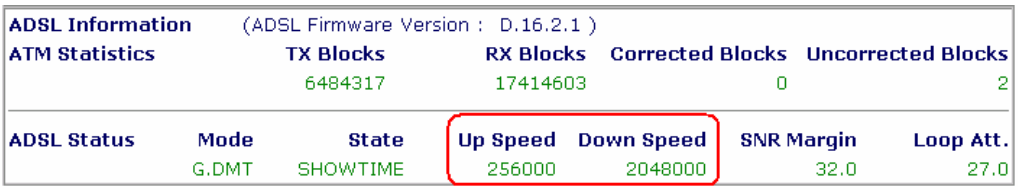
1. Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
2. Non-privileged users can control some router functions, including removing and adding port mappings.

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

7.2.5 QoS Control

Before you start

For more effective QoS deployment, you should check the available ADSL upstream and downstream speed in **Online Status** as indicated below.

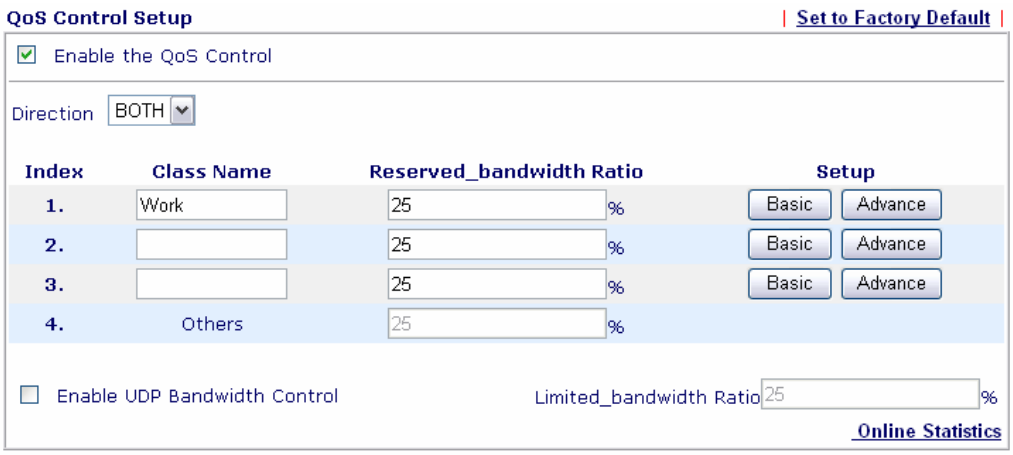


ADSL Information	(ADSL Firmware Version : D.16.2.1)					
ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks		
	6484317	17414603	0	2		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	32.0	27.0

The following QoS policies will be defined in the form of ratio of upstream/downstream speed. We will also provide application QoS requirement as reference to help you accomplish this task. The setting values will vary depending on the network condition.

Configuration

You Click on **Application >>QoS Control Setup** to see the below window.



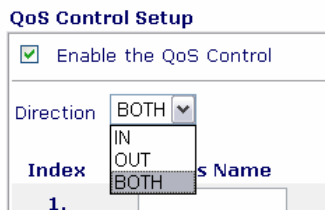
Enable the QoS Control	For V models, the factory default for this is checked to enable.

Direction	Define which traffic the QoS Control settings apply to. **IN:** apply to incoming traffic only. **OUT:** apply to outgoing traffic only. **BOTH:** apply to both incoming and outgoing traffic.
Index	The group index number of QoS Control settings. There are total 4 groups.
Class Name	Define the name for the group index.
Reserved Bandwidth Ratio	The bandwidth that is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.
Setup	There are two-level of settings: **Basic:** setup Reserved Bandwidth Ratio according to the traffic service type. We provide a list of common service types. **Advance:** custom setting of Reserved Bandwidth Ratio based on the source address, destination address, DiffServ CodePoint, and service type.
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.

Example

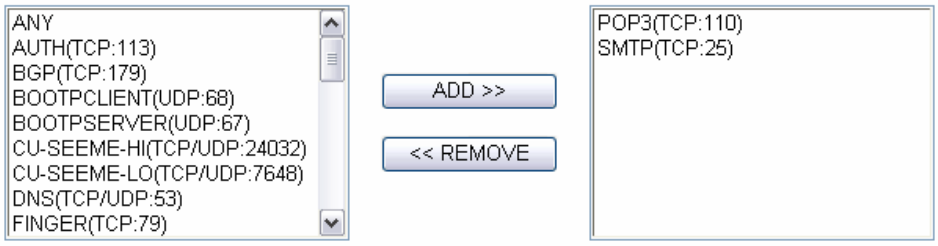
Jane is a teleworker who sometimes works at home and takes care of children. When working time, she would use Vigor router at home to connect to the server in the headquater office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

1. Make sure the QoS Control on the left corner is checked. And select BOTH in **Direction**.

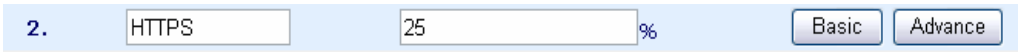


2. Enter the Class Name of Index 1. In this index, she will set reserve bandwidth for Email using protocol POP3 and SMTP. Click Basic button on the right.

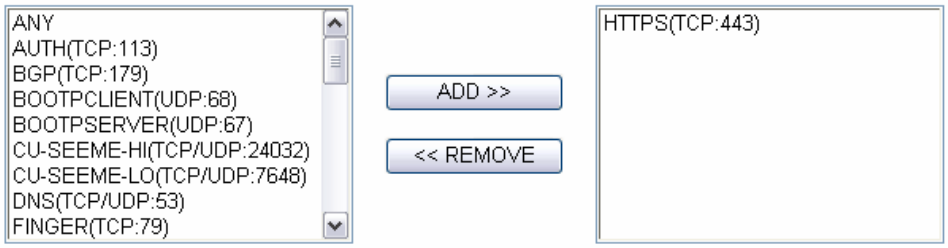
3. Select POP3 and SMTP on the left column and add to right column. Click OK to exit.



4. Enter the Class Name of Index 2. In this index, she will set reserve bandwidth for HTTPS. And click Basic button on the right.



5. Select HTTPS in the list on the left column and click on ADD to add to right column. Click OK to exit.

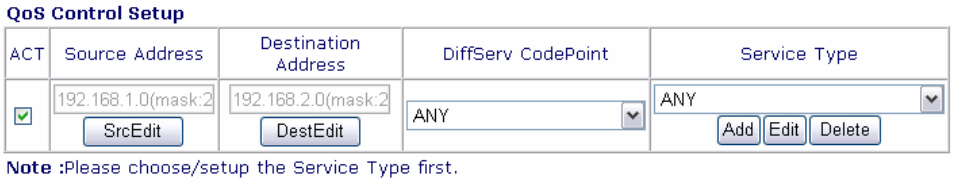


6. Check the Enable UDP Bandwidth Control on the bottom to prevent enormous UDP traffic influent other application.

7. If Jane has connected to the headquater using host to host VPN tunnel. (Please refer to Chapter 8 VPN for detail instruction),

she may set up an index for it. Enter the Class Name of Index 3. In this index, she will set reserve bandwidth for 1 VPN tunnel. And click Advance button on the right.

8. Click edit to open a new window. First, check the ACT box. Then click SrcEdit to set a Jane's subnet address. Click DestEdit to set headquarter's subnet address. Leave other fields and click OK.



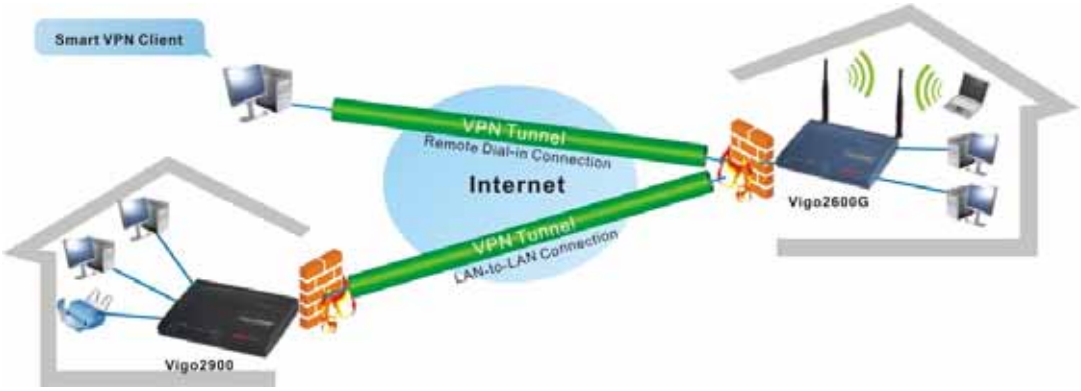
Chapter 8
VPN and Remote Access Setup

8.1 Introduction

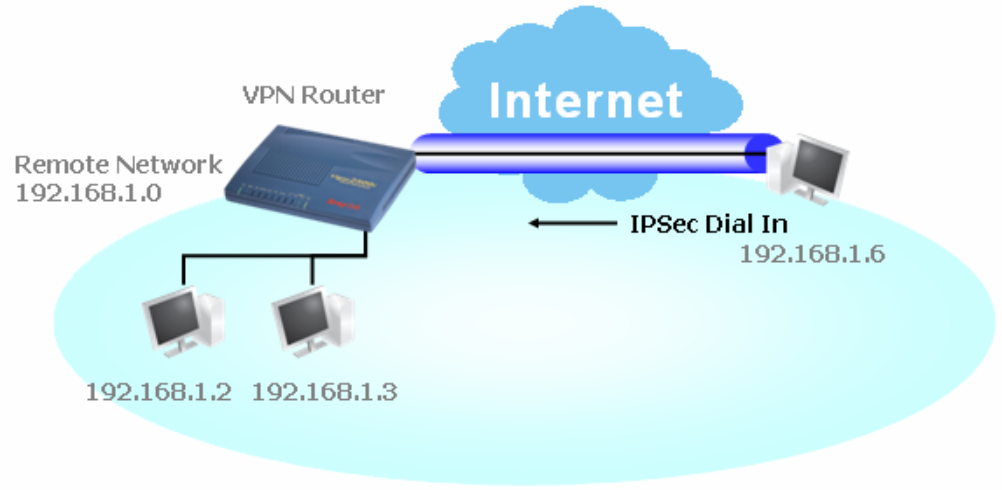
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Categories of VPN: Remote Dial-In and LAN-to-LAN

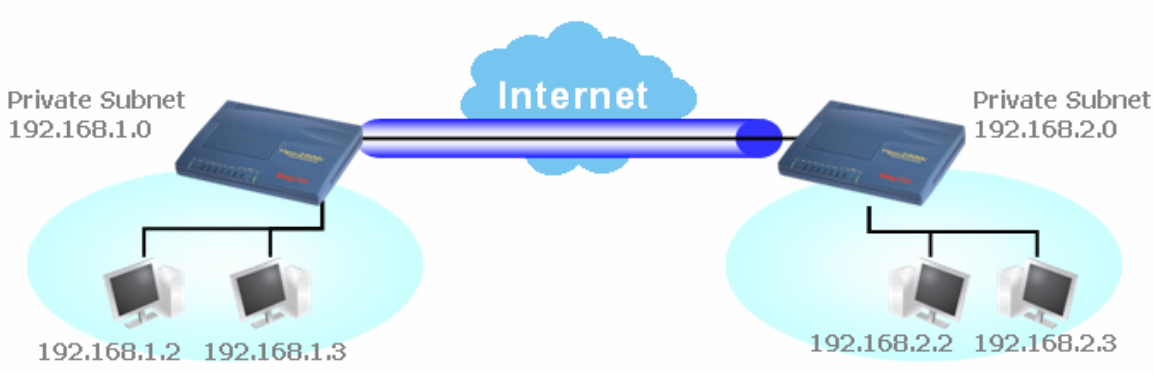
VPNs fall into two categories, as illustrated below.



- **Remote-access** VPN connection allows a remote access node, a NAT router or a single mobile user/telecommuter, to dial into a VPN router through the Internet to access the remote enterprise network resources. The dialer may get an IP address belonging to remote network after a serial of authentication process and VPN tunnels built up, so it will be treated as a member of the private network.



- **LAN-to-LAN Access** VPN connection allows two independent LANs in different fixed locations to share the resource mutually, such as the interconnection between the head office network and the branch/home offices.



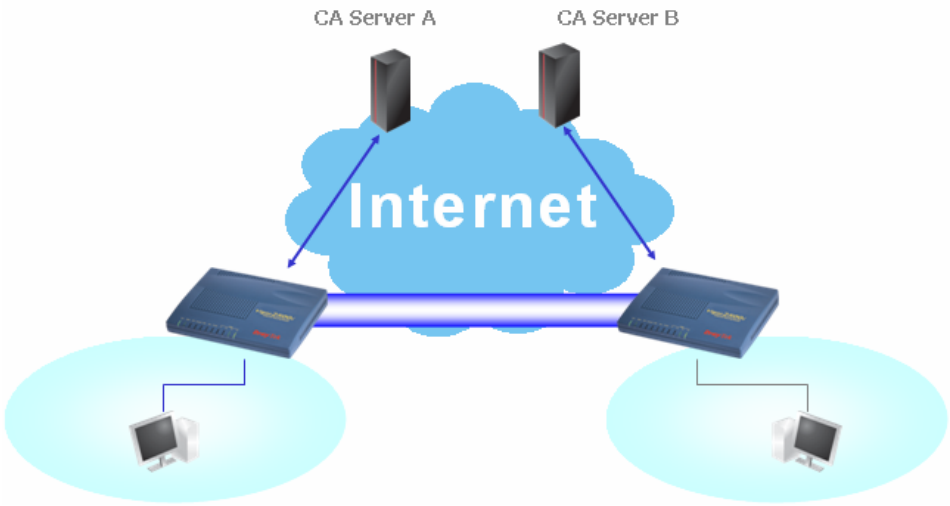
Protocols Used to Enable Each Type of VPN

The Vigor router supports several VPN technology standards in industry. Each of them has different characteristics that enable specific VPN features.

- **Internet Protocol Security (IPSec)** is a set of protocols developed by the IETF to support secure exchange of packets at the network layer between endpoints in a shared IP-based network. It applies a hybrid protocol called **Internet Key Exchange (IKE)** that provides

services including authentication of the IPSec peers, negotiation of IKE and IPSec security association parameters, and establishment of keys for encryption algorithms used by IPSec. Authentication cab be further separated into categories depending on the methods:

- **Pre-Shared Key** is manually configured on each IPSec peer. Each peer will compute and send a keyed hash of data. If the receiving peer can independently create the same hash using its pre-shared key, which proves that it has the same with the sending peer, so it can authenticate the peer.
- **Digital Signatures (X.509 certificates)** are used with the IKE protocol when authentication requires public keys. This certificate provides digital ID to each device by Certificate Authorities (CA) servers. Thus two devices will exchange digital certificates to prove their identity before starting communication.



- **Point-to-Point Tunneling Protocol (PPTP)** is a Point-to-Point (PPP)–based protocol developed by Microsoft. In a transport level session (TCP/IP or NetBIOS), the tunneling technique is used to send the PPP packets to the legacy Remote Access Service (RAS) server over the Internet. Authentication of users is done using the existing protocols: PAP and CHAP. MS-CHAP supports MD4 hash as

well as the DES scheme. Data encryption is performed using the encryption protocols RSA RC4. PPTP provides secure access across the Internet with the shared secret, a hashed form of the user credentials, is validated by both ends. The PPTP VPN connection is compatible with all Windows platforms which have built-in PPTP protocol.

- **Layer 2 Tunneling Protocol (L2TP)** is another Point-to-Point (PPP)-based tunneling protocol developed by Microsoft and Cisco. It merges the best features of two existing tunneling protocols: PPTP from Microsoft and L2F from Cisco. Like PPTP, L2TP requires that the ISP's routers support the protocol.
- **L2TP over IPSec** is to apply L2TP with IPSec policy. The L2TP and L2TP over IPSec are compatible with Window 2000 and XP.

VPN Pass Through

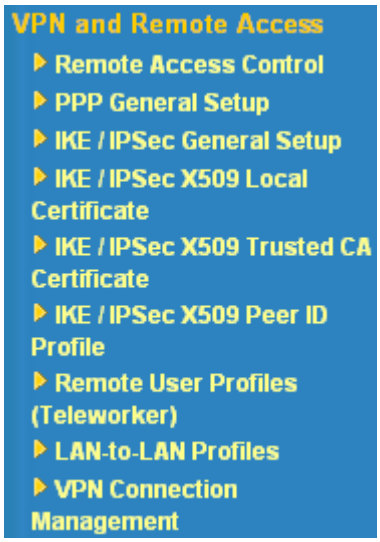
In the case that you may add a Vigor router to an existing structure in which there is a router dedicated for VPN, you should let those VPN tunnels pass through the Vigor router. You may add control based on the type of VPN tunnels. For example, you can enable IPSec and L2TP VPN service pass through and deny PPTP VPN service.

ISDN Related Features (for I models)

For those who have ISDN connections, ISDN related features including remote ISDN dial-in, dial-in and dial-out in LAN-to-LAN access can be set up. ISDN applies also PPP-based connection for authentication and billing purpose. Vigor router also provides Callback function that allows company Vigor router to share the connection fee.

8.2 Settings

This chapter explains the capabilities of the VPN facility and the remote access on the router. Use the link on the menu to configure the VPN and remote access functions.



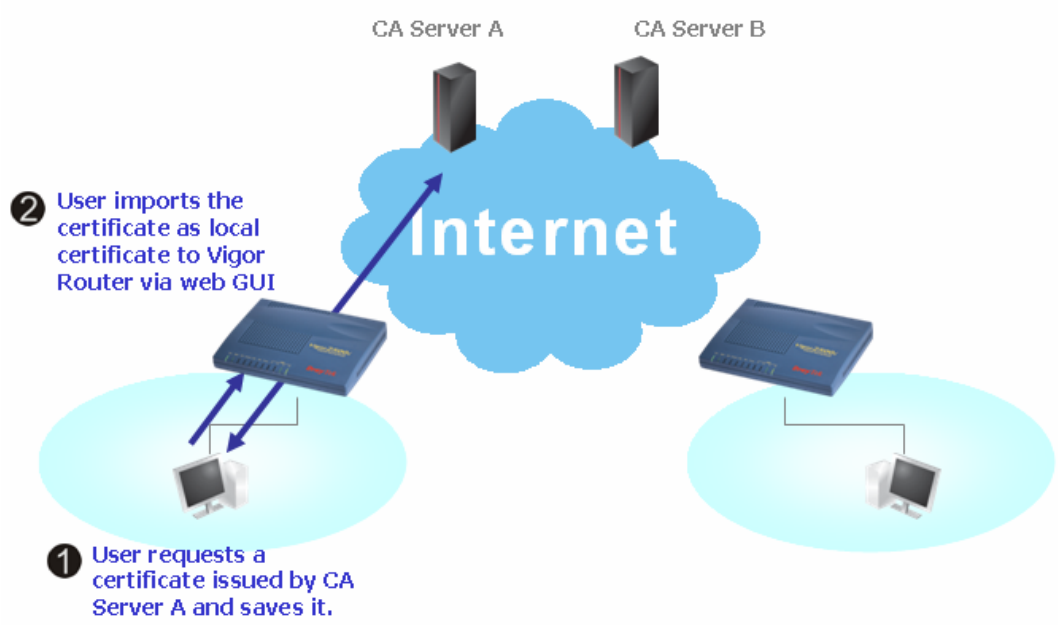
8.2.1 Certificate Management and Peer ID Profiles

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

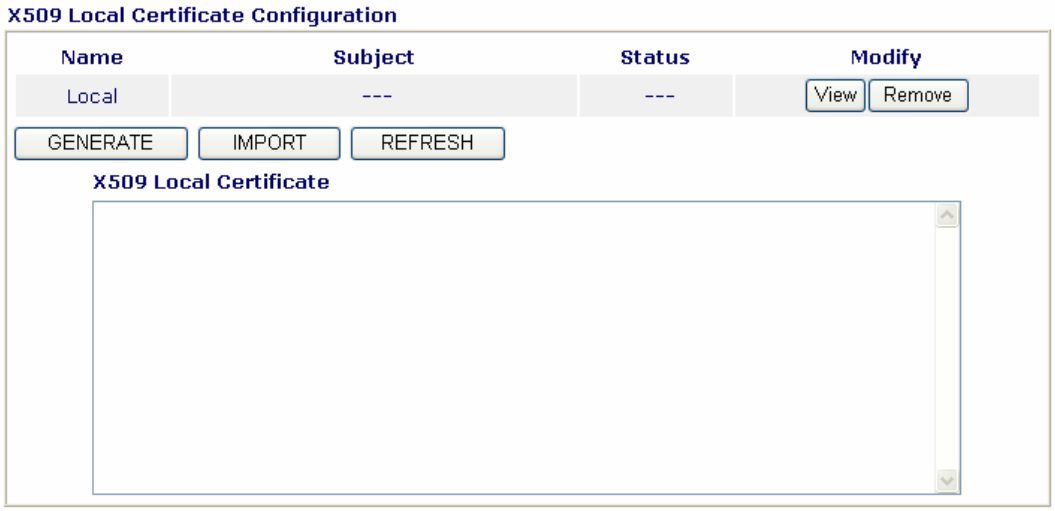
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates.

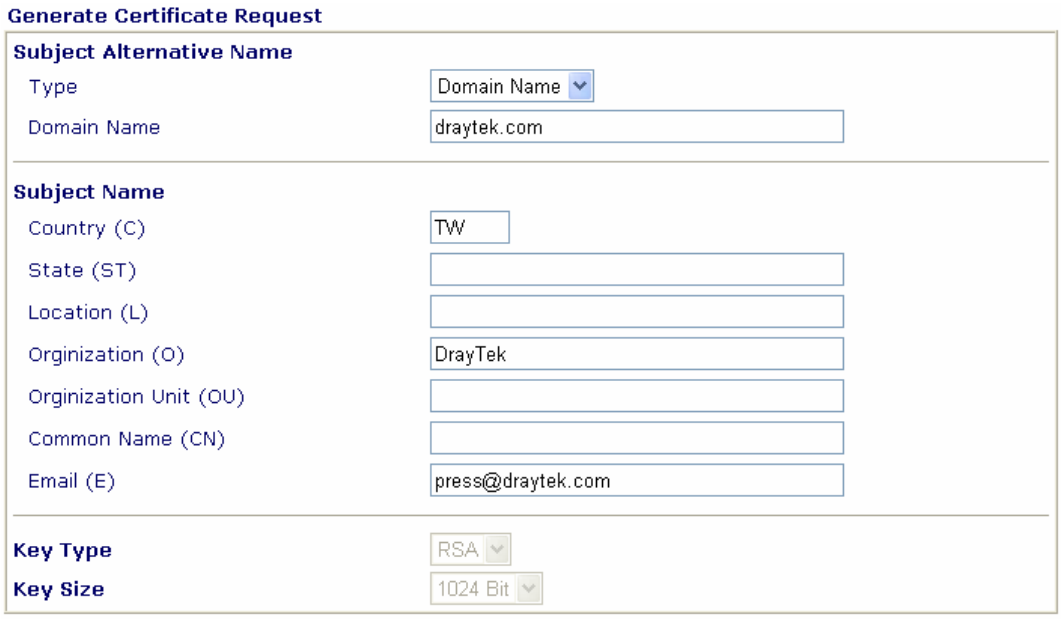
Request a certificate from a CA server



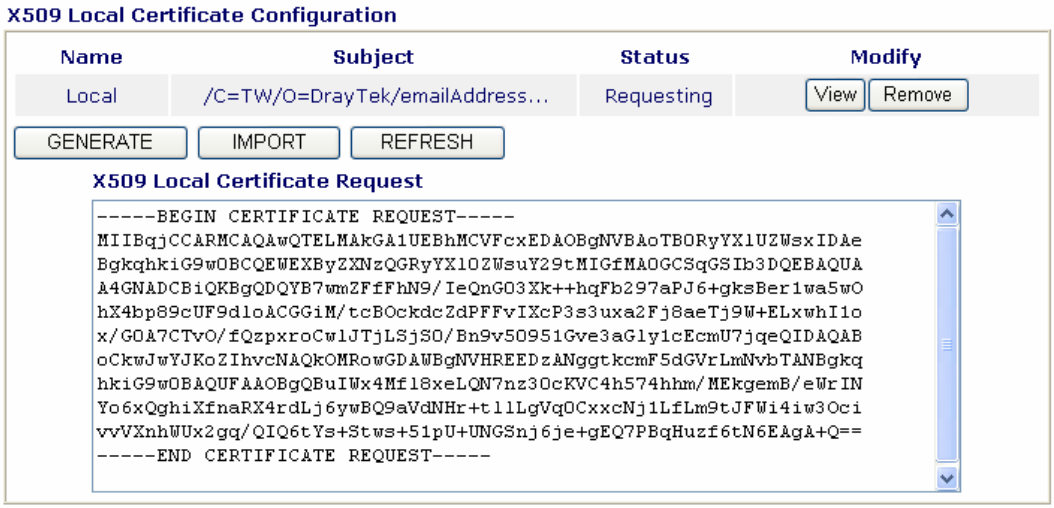
Step 1: Go to **Local Certificate**, as shown below. You can click **GENERATE** button to start to edit a certificate request.



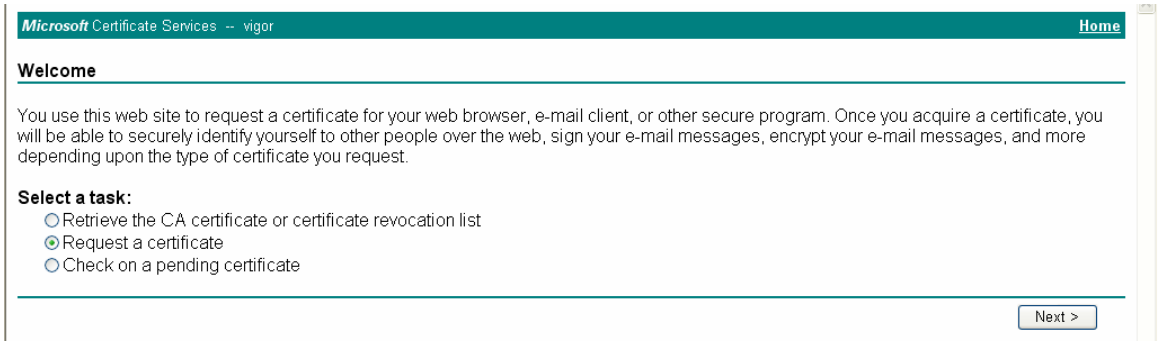
Step 2: Enter the information in the certificate request.



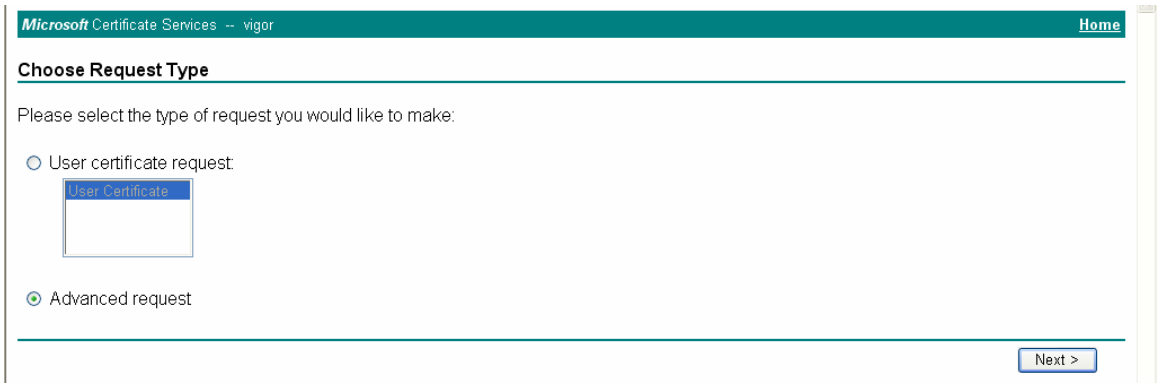
Step 3: Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



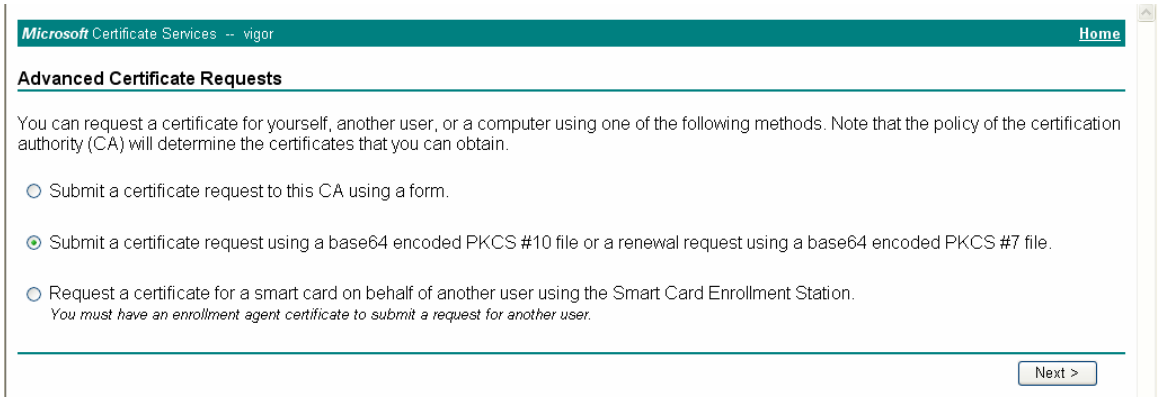
Step 4: Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



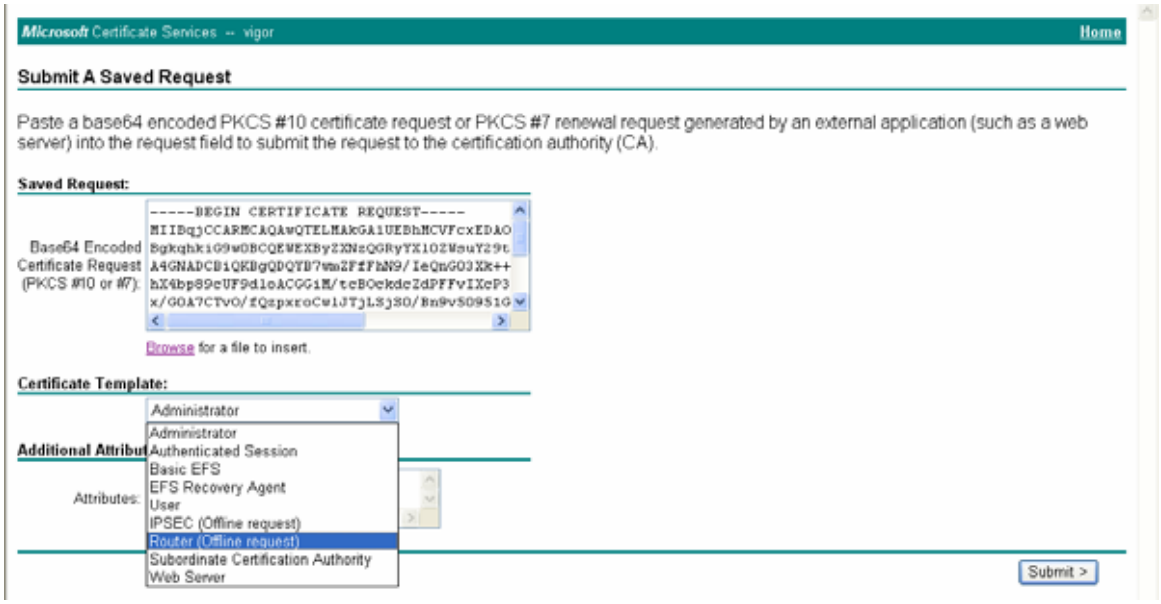
Select **Advanced request**.



Select **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**.



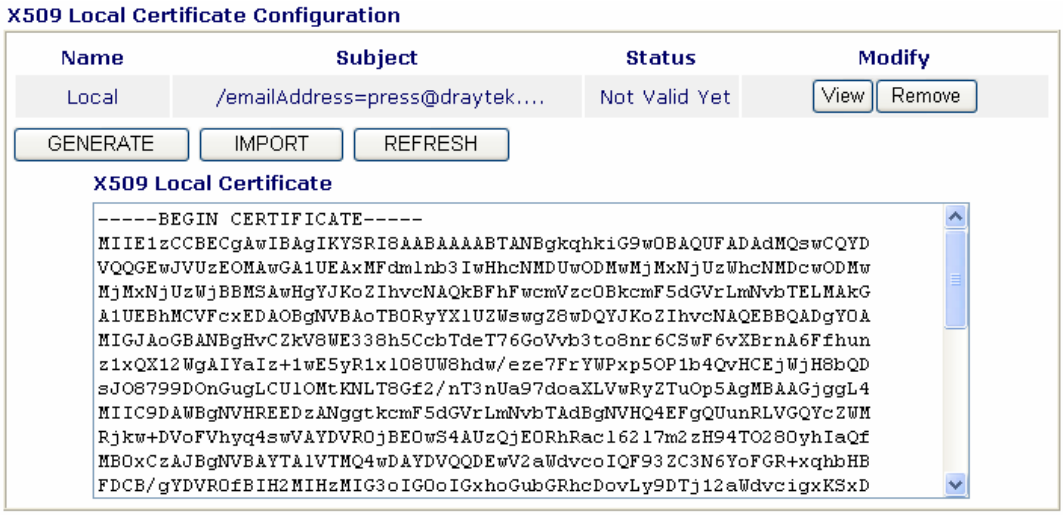
Import the X509 Local Certificate Requet text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



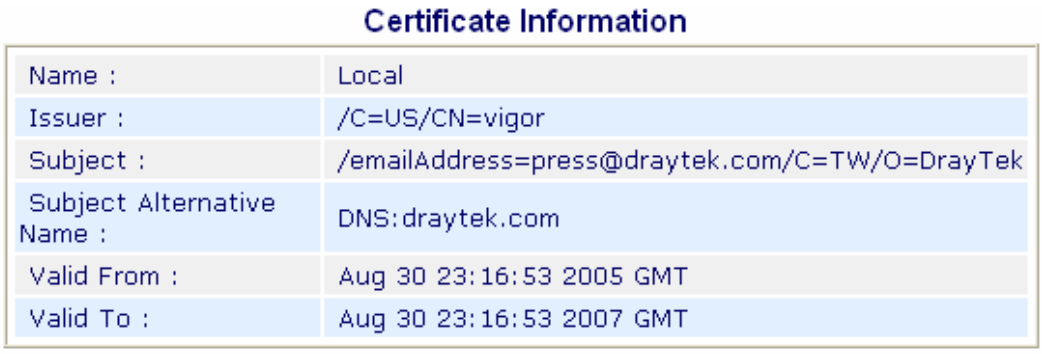
Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**.

Now you should get a certificate (.cer file) and save it.

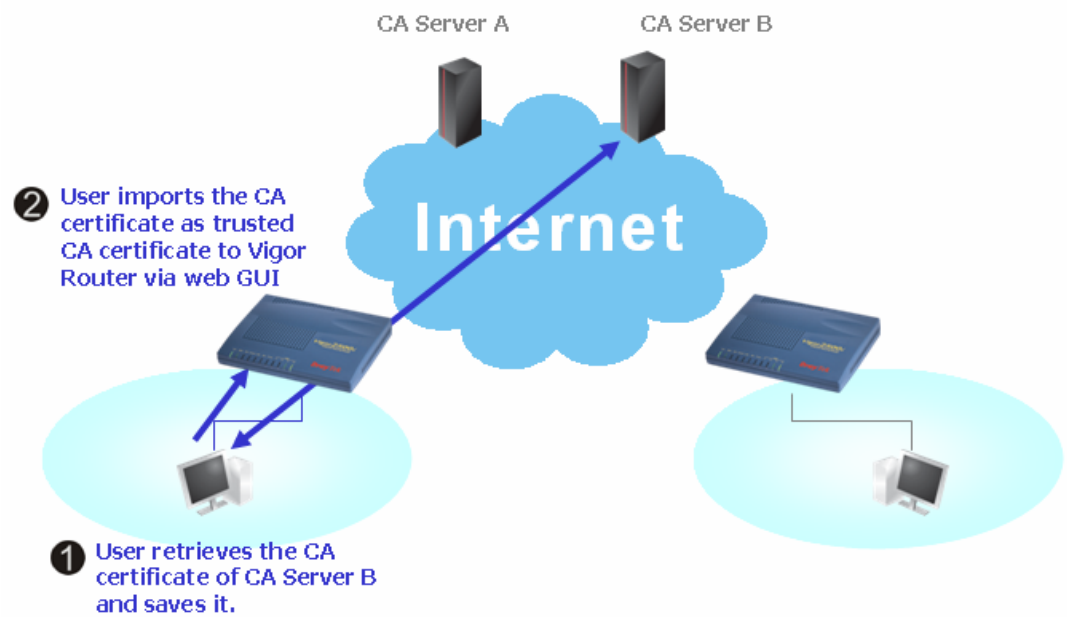
Step 5: Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below window showing “------BEGINE CERTIFICATE------.....”.



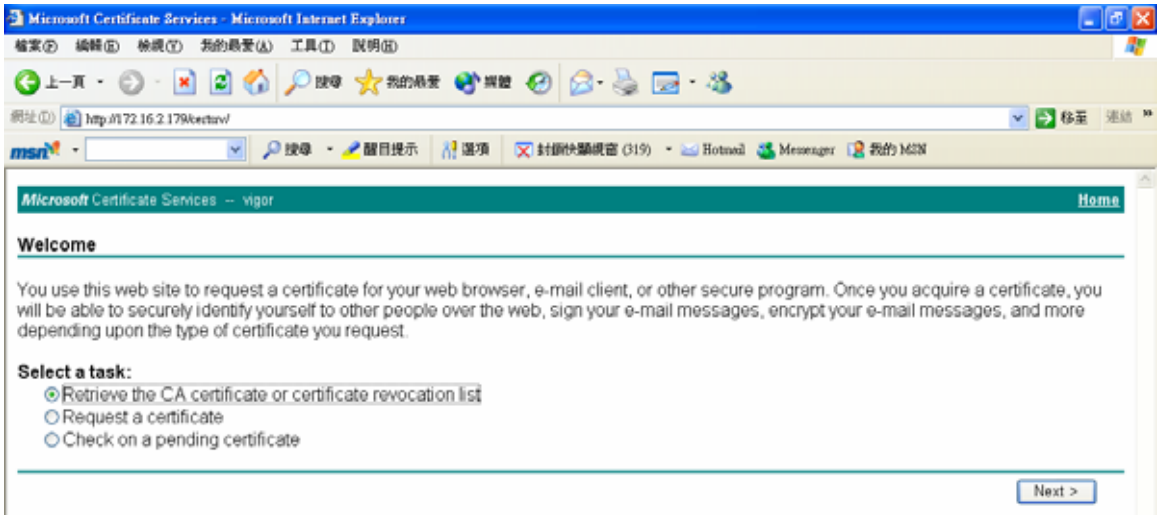
You may review the detail information of the certificate by clicking **View** button.



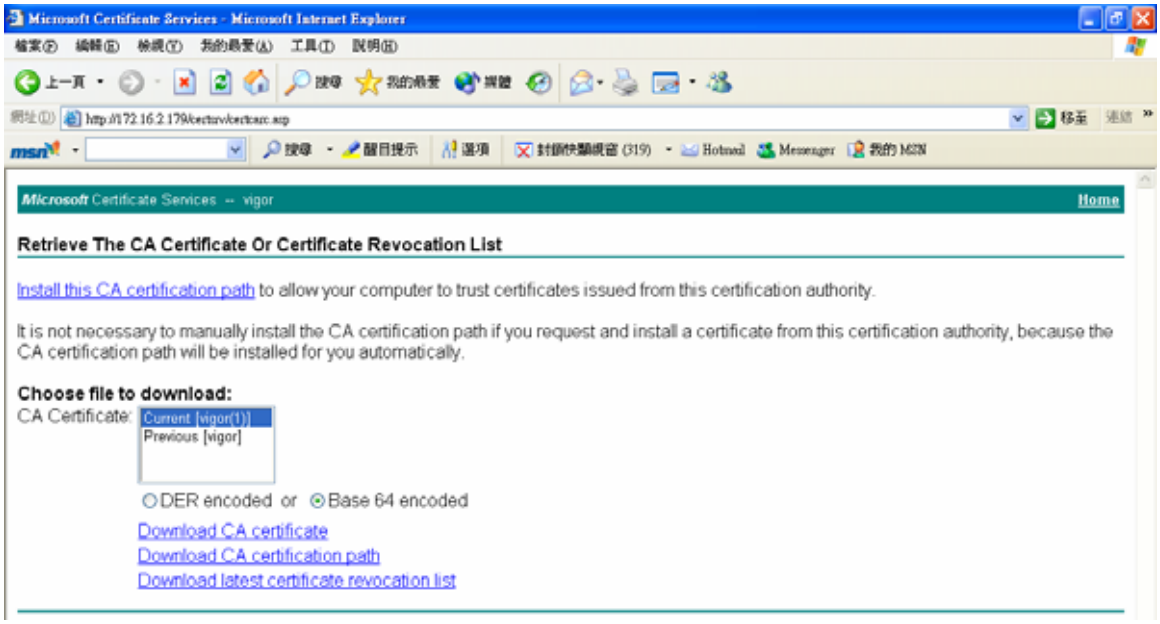
Request a CA certificate and set as trusted



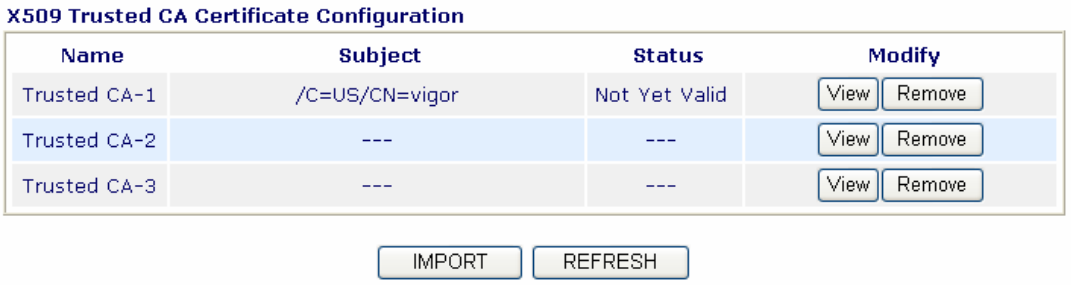
Step 1: Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.



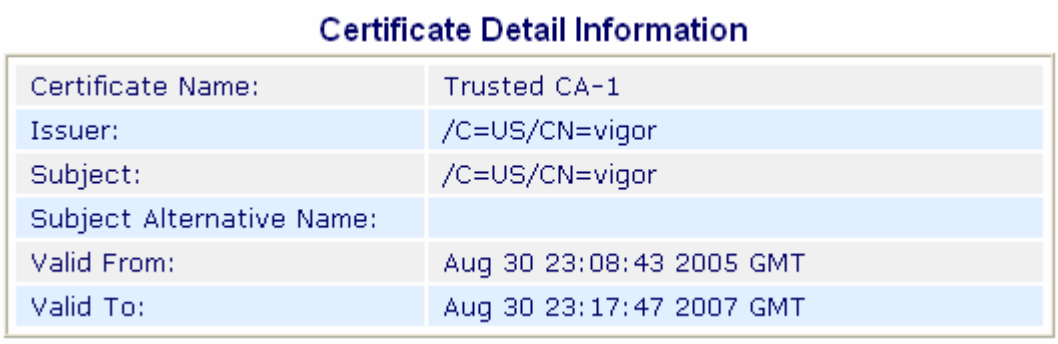
Step 2: In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.



Step 5: Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

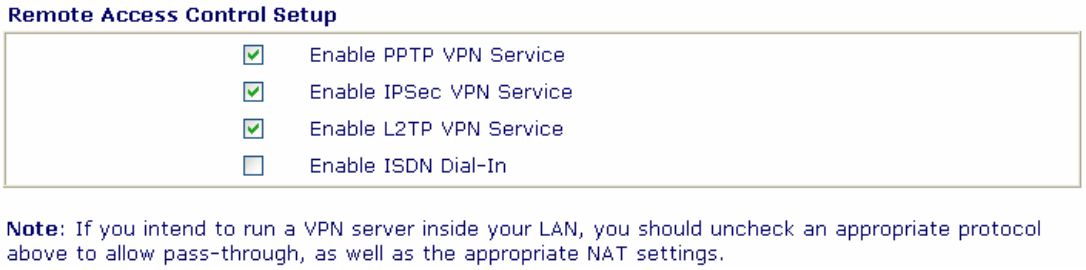


You may review the detail information of the certificate by clicking **View** button.



8.2.2 Remote Access Control Setup

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port. Enable ISDN Dial-In service if necessary.



8.2.3 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

PPP/MP Protocol

Dial-In PPP Authentication	**PAP Only:** Select this option to force the router to authenticate dial-in users with the PAP protocol. **PAP or CHAP:** Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall

	back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE	**Optional MPPE:** This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the **Require MPPE (40/128bits):** Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 40-bit MPPE encryption method is not available, then 128-bit encryption scheme will be applied to encrypt the data. **Maximum MPPE:** This option indicates that the router will use the MPPE encryption scheme with maximum bits (128 bits) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security. For example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer

IP Address Assignment for Dial-In Users

Start IP Address	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 to be the Start IP Address. 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user

8.2.4 IPSec General Setup

In **IPSec General Setup,** there are two major parts of configuration.

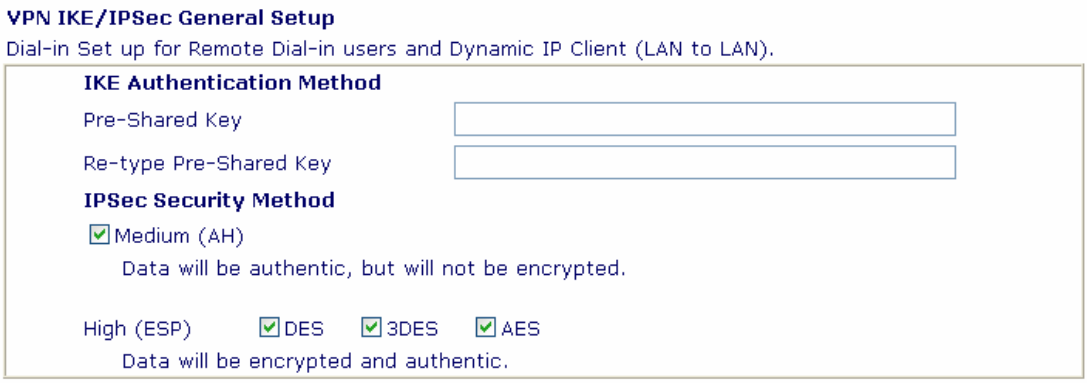
There are two phases of IKE/IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) and/or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service. Vigor supports IPSec used ESP to encrypt the data payload. There are two encryption methods in IPSec: Transport and Tunnel. Transport mode encrypts only the data portion, a.k.a. payload, of each packet, but not the header. Transport mode is used in L2TP over IP Sec. The more secure Tunnel mode encrypts both the header and the payload. Tunnel mode is used in IPSec. ESP can be used alone or in

conjunction with AH.



IKE Authentication Method

This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.

Pre-Shared Key	Currently only support Pre-Shared Key authentication **Pre-Shared Key:** Specify a key for IKE authentication **Re-type Pre-Shared Key:** Confirm the pre-shared key

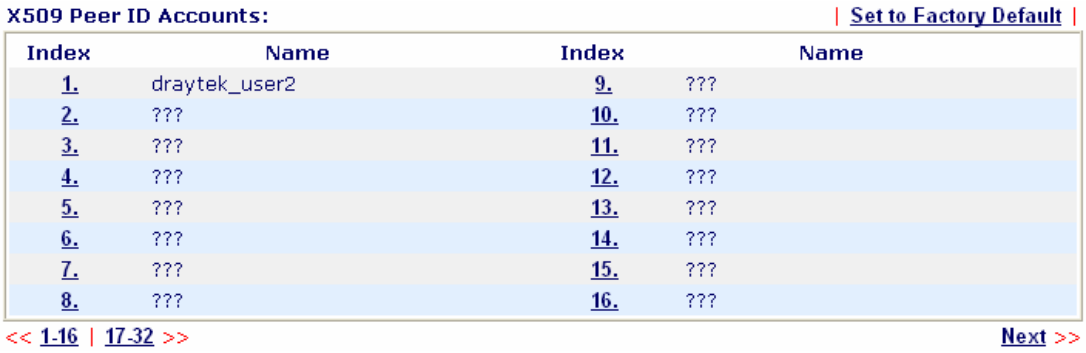
IPSec Security Method

Medium	**Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is active.
High	**Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

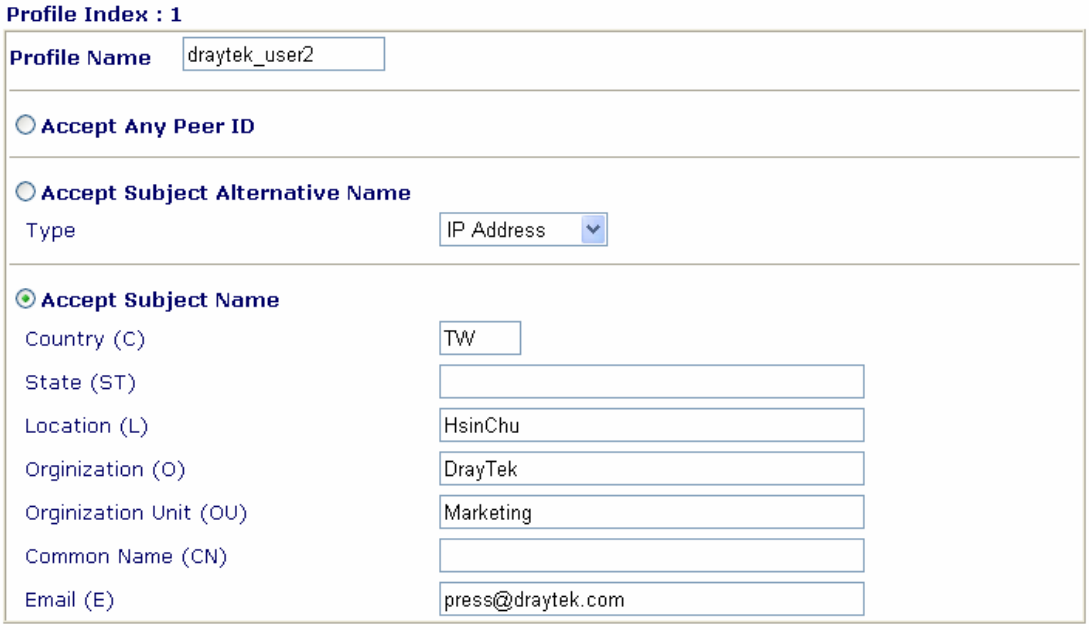
8.2.5 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table

of peer certificate for selection. As shown below, the router provides 32 entries of digital certificates for peer dial-in users.



Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.



Profile Index

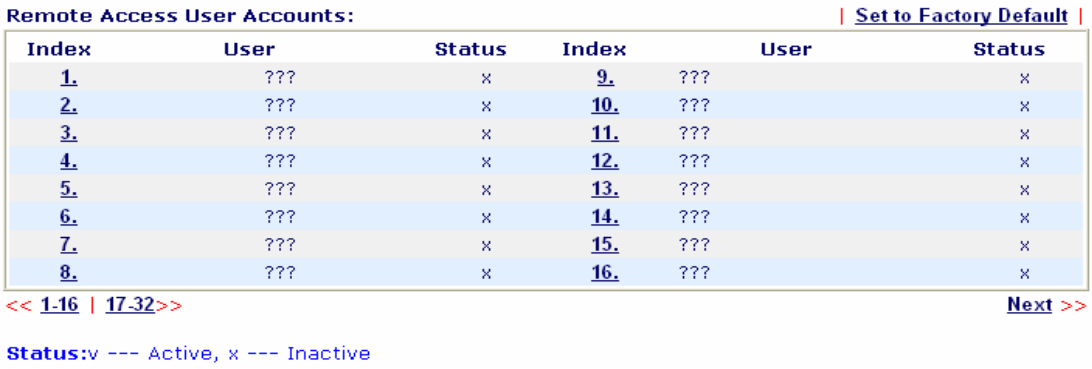
Accept Any Peer ID	Click to accept all peer regardless of its identity
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP**

	Address, Domain, or **E-mail Address**.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN),** and **Email (E)**.

8.2.6 Remote User Profile (Teleworkers)

Here you can manage remote access by maintaining a table of remote user profile so that user can be authenticated to dial-in or build the VPN connection. You may set parameters including specified connection peer ID, connection type (ISDN, VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

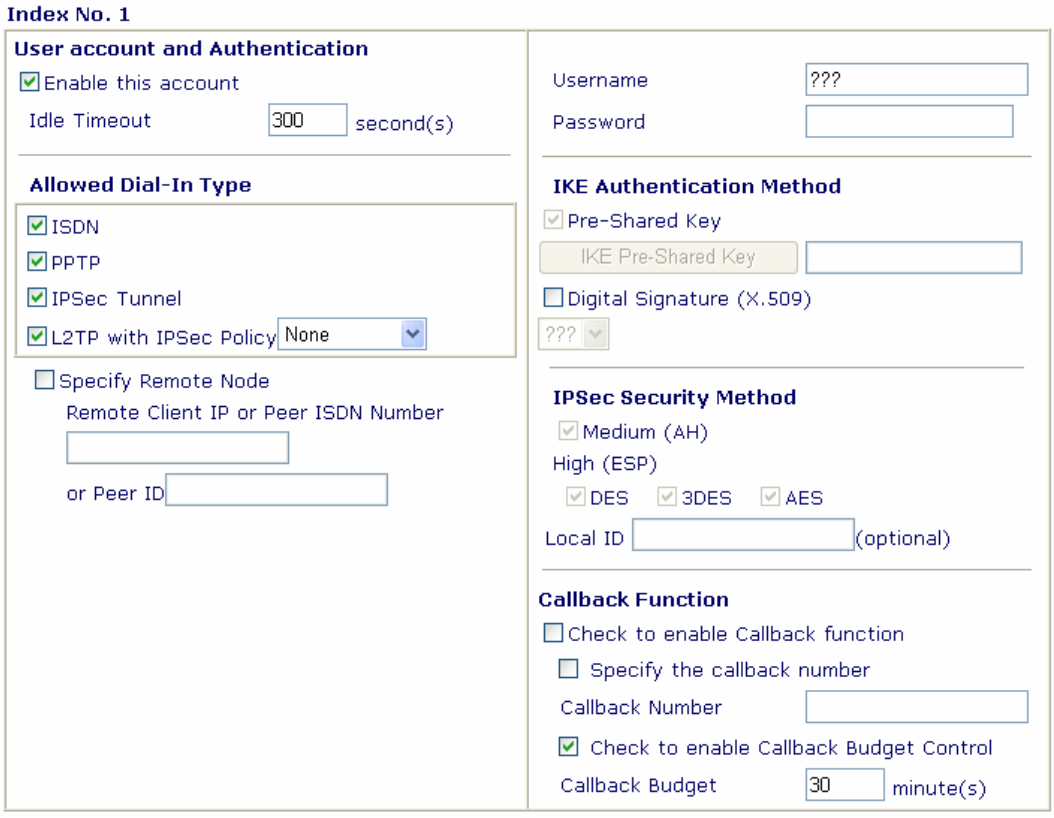


Remote Access User Accounts

Set to Factory Default	Click to clear all indexes.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the

	profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.



User Account Authentication

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

Allowed Dial-In Type

Type	**ISDN:** Allow the remote ISDN dial-in connection You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below **PPTP:** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below **IPSec Tunnel:** Allow the remote dial-in user to trigger a IPSec VPN connection through Internet. **L2TP:** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ➢**None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ➢N**ice to Have:** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ➢**Must:** Specify the IPSec policy to be definitely applied on the L2TP connection. You should set the User Name and Password of the remote dial-in user below
User Name	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Specify Remote Node	**Check the checkbox:** You can specify the IP address of the remote dial-in user or peer ID. Enter Peer ISDN number if you select ISDN above. Also, you should further specify the corresponding security methods on the right side. **Uncheck the checkbox:** This means the connection type you

	select above will apply the authentication methods and security methods in the **general settings**.

IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy **when you specify the IP address of the remote node**. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either w/ or w/o specify the IP address of the remote node.

Pre-Shared Key	Input 1-63 characters as pre-shared key.
Digital Signature (X.509)	Select one predefined in the X.509 Peer ID Profiles

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.

Medium	**Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is active.
High	**Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Local ID	Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional.

Callback Function

The callback function provides a callback service only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Check to enable Callback function	Enables the callback function.

Specify the callback number	The option is for extra security. Once enabled, the router will ONLY call back to the specified **Callback Number**.
Check to enable callback budget control	By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. **Callback Budget (Unit: minutes):** Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

8.2.7 Creating a LAN-to-LAN Profile

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (ISDN, VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides up to 32 profiles, which also means supporting 32 VPN tunnels simultaneously. The following figure shows the summary table.

LAN-to-LAN Profiles: | Set to Factory Default |

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

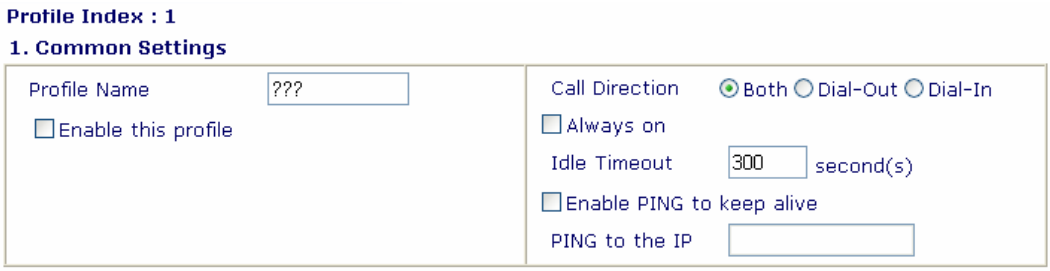
<< 1-16 | 17-32 >> Next >>

LAN-to-LAN Profiles

Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit a LAN-to-LAN profile. Each LAN-to-LAN profile includes 4 subgroups. The Dial-In Type subgroup requires you to fill the different corresponding fields on the right. If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

Common Settings



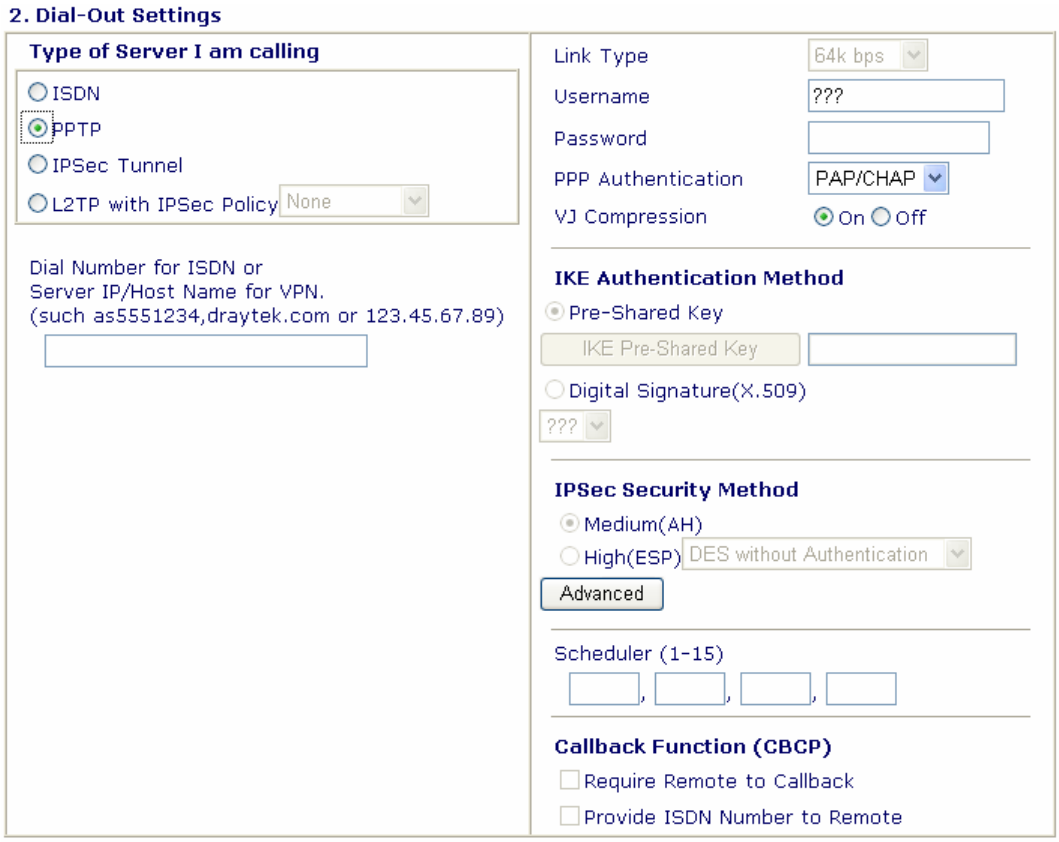
Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. **Both**: outgoing and incoming access. **Dial-Out**: outgoing access only. **Dial-In:** incoming access only.
Always On or Idle Timeout	**Always On:** Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of VPN connection, especially useful in the case of abnormal VPN

	IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address. **PING to the IP:** Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial.

Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly.

Dial-Out Settings



Type of Server I am calling	Select one out of four types. **ISDN:** build ISDN dial-out connection to the server. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. **PPTP:** build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server. **IPSec Tunnel:** build a IPSec VPN connection to the server through Internet. **L2TP:** build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ➢ **None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ➢ N**ice to Have:** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN

	connection becomes one pure L2TP connection. ➢ **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection. You should set the User Name and Password below as your identity for the authentication of remote server.
User Name	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
PPP Authentication	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.
Dial Number for ISDN or Server IP/Host Name for VPN	You must specify the IP address of the remote VPN server/host name. Enter Peer ISDN number if you select ISDN above. Also, you should further specify the corresponding security methods on the right side.

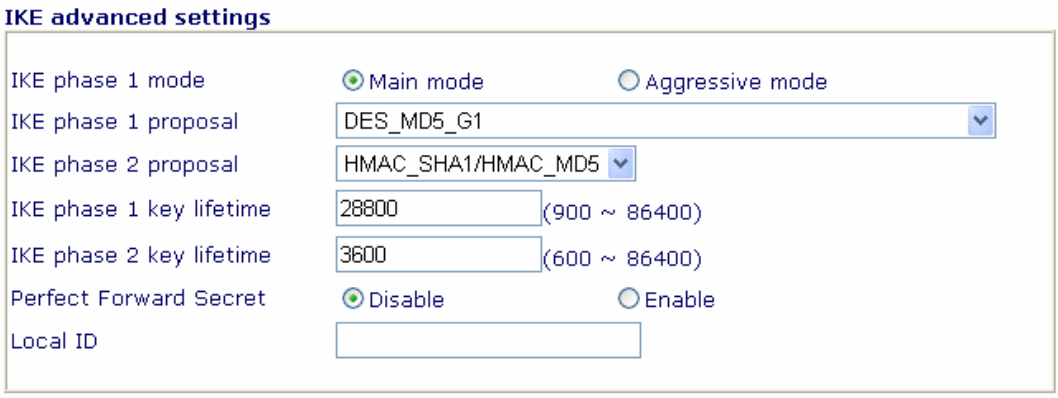
IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.

Pre-Shared Key	Input 1-63 characters as pre-shared key.
Digital Signature (X.509)	Select one predefined in the X.509 Peer ID Profiles

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy. The window of Advance setup is as show below.



Medium	**Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is active.
High	**Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. Select from below: **DES without Authentication:** Use DES encryption algorithm and not apply any authentication scheme. **DES with Authentication:** Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. **3DES without Authentication:** Use triple DES encryption algorithm and not apply any authentication scheme. **3DES with Authentication:** Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
Advanced	Specify mode, proposal and key life of each IKE phase. Gateway etc. **IKE phase 1 mode:** Select from Main mode and Aggressive mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPSec session. However, the Aggressive mode is faster. The default value in Vigor router is

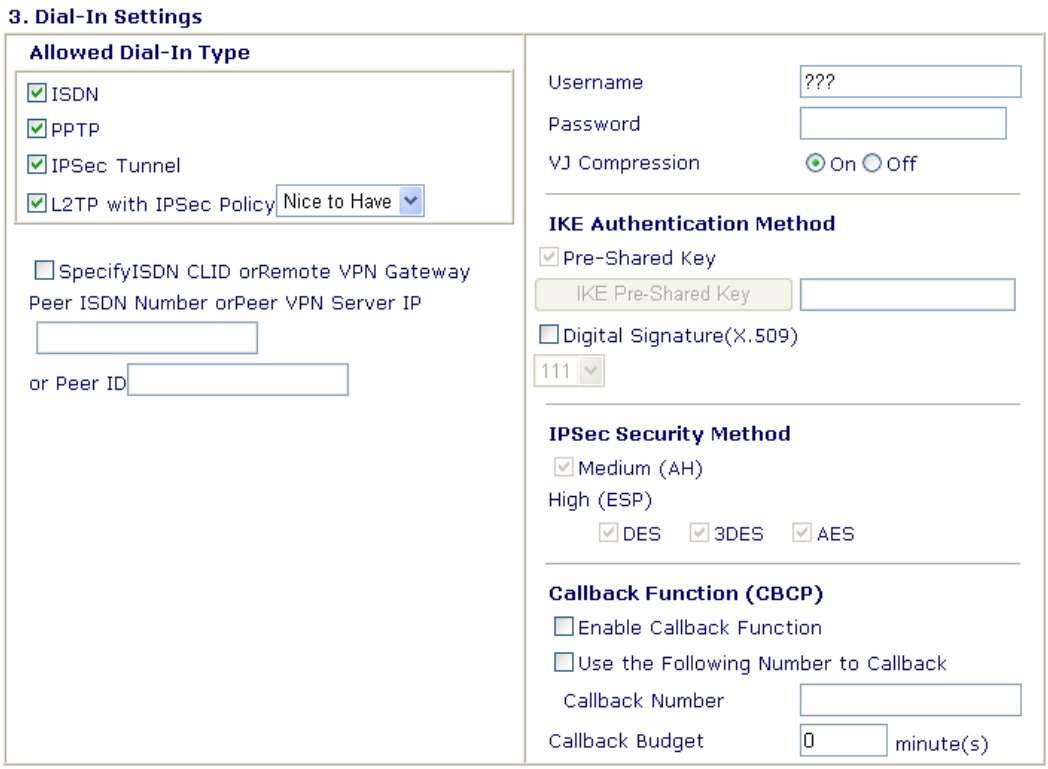
	Main mode. **IKE phase 1 proposal:** To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for Main mode. We suggest you select the combination that covers the most schemes. **IKE phase 2 proposal:** To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms. **IKE phase 1 key lifetime:** For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds **IKE phase 2 key lifetime:** For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds **Perfect Forward Secret (PFS):** The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function **Local ID:** In Aggressive mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server.

Callback Function (for I models)

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Require Remote to Callback	Enable this to let the router to require the remote peer to callback for the connection afterwards.
Provide ISDN Number to Remote	In the case that the remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router.

Dial-In Settings



Allowed Dial-In Type	**ISDN**: Allow the remote ISDN dial-in connection You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below **PPTP:** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below **IPSec Tunnel:** Allow the remote dial-in user to trigger a IPSec VPN connection through Internet. **L2TP:** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ➢**None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.

	➢**Nice to Have**: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ➢**Must:** Specify the IPSec policy to be definitely applied on the L2TP connection. You should set the User Name and Password of the remote dial-in user below
User Name	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP	**Check the checkbox:** You can specify the IP address of the remote dial-in user or peer ID. Enter Peer ISDN number if you select ISDN above. Also, you should further specify the corresponding security methods on the right side. **Uncheck the checkbox:** This means the connection type you select above will apply the authentication methods and security methods in the general settings.

IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy **when you Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP**. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either w/ or w/o specify the CLID or IPaddress of the remote node.

Pre-Shared Key	Input 1-63 characters as pre-shared key.
Digital Signature (X.509)	Select one predefined in the X.509 Peer ID Profiles

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.

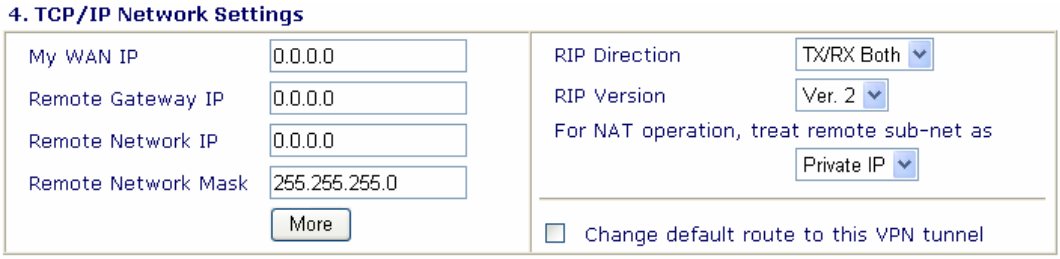
Medium	**Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is active.
High	**Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

Callback Function

The callback function provides a callback service only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Check to enable Callback function	Enables the callback function.
Callback number	The option is for extra security. Once enabled, the router will ONLY call back to the specified **Callback Number**.
Callback budget	By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically. **Callback Budget (Unit: minutes):** Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period

TCP/IP Settings

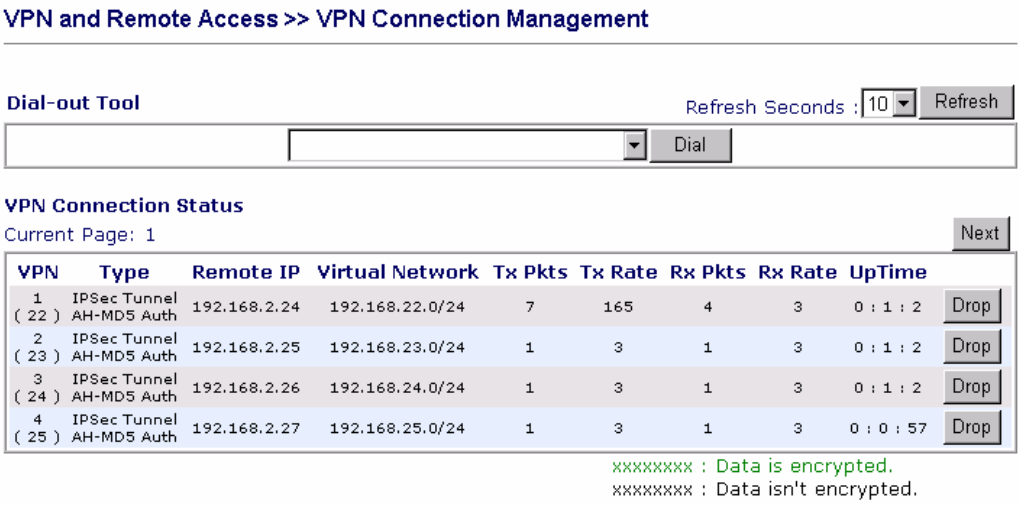


My WAN IP	The default value is 0.0.0.0, which means the Vigor router will get a WAN IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
Remote Gateway IP	The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
Remote Network IP/ Remote Network Mask	Add a static router to direct all traffic destined to this Remote Network IP Address/ Remote Network Mask through the VPN connection.
More	Add a static router to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
For NAT operation, treat remote sub-net	The Vigor router supports two local IP networks: the 1st subnet and 2nd subnet. Thus, you can set which subnet

as	will be used as the local network for VPN connection and exchange RIP packets with the remote network. Usually set to Private IP for routing between the 1st subnet and the remote network.

8.2.8 VPN Connection Management

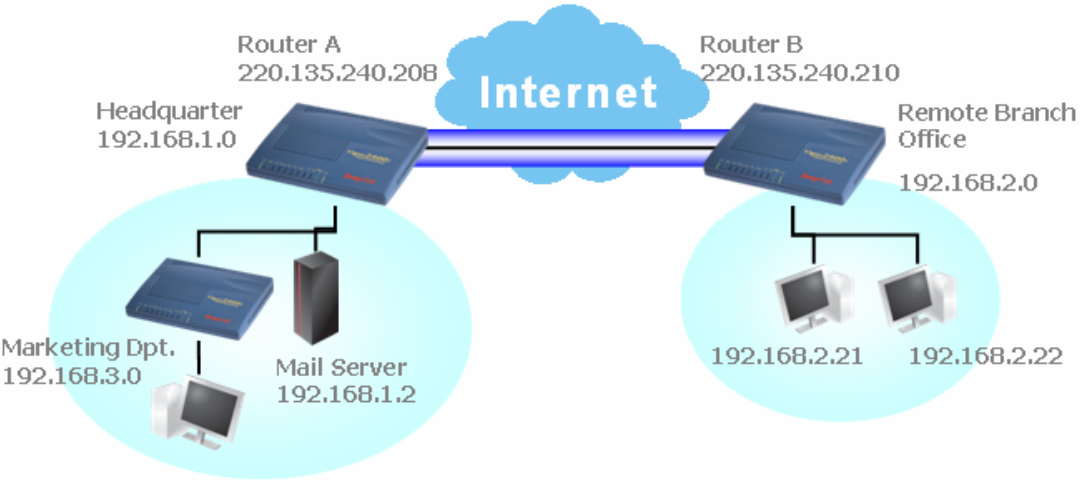
Here you can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking Drop button. You may also aggressively Dial-out by using Dial-out Tool and clicking Dial button.



8.2.9 Examples

Create a LAN-to-LAN connection between remote office and headquarter

The most common case is you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.

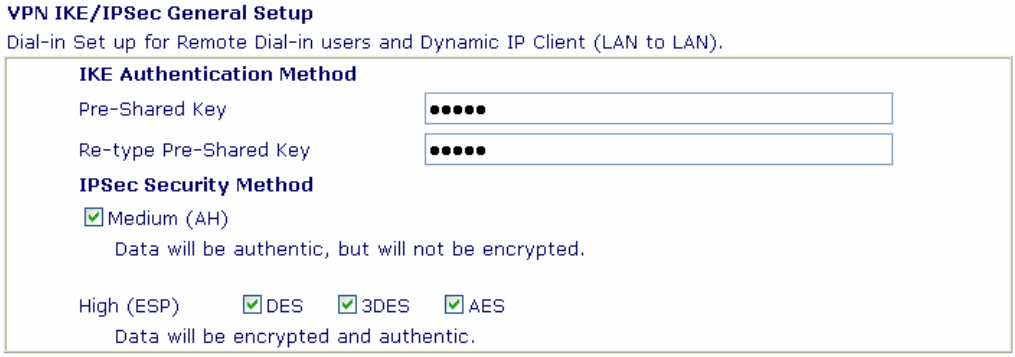


Settings in Router A in headquarter:

1. Go to **Remote Access Control** to enable the necessary VPN service.
2. Then,

➢ To use PPP based services, such as PPTP, L2TP, or ISDN, you have to set general settings in **PPP General Setup**.

➢ To use IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

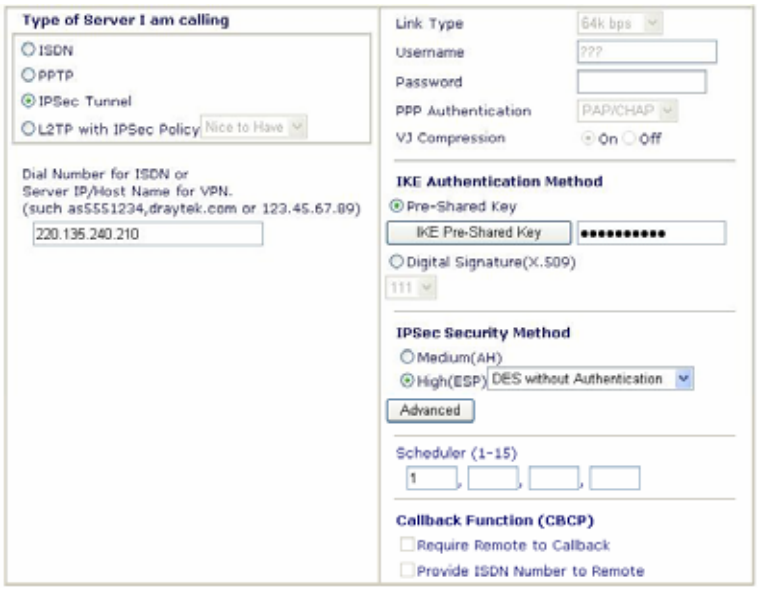


3. Go to **LAN-to-LAN Profiles**. Click on one index number to edit a profile.

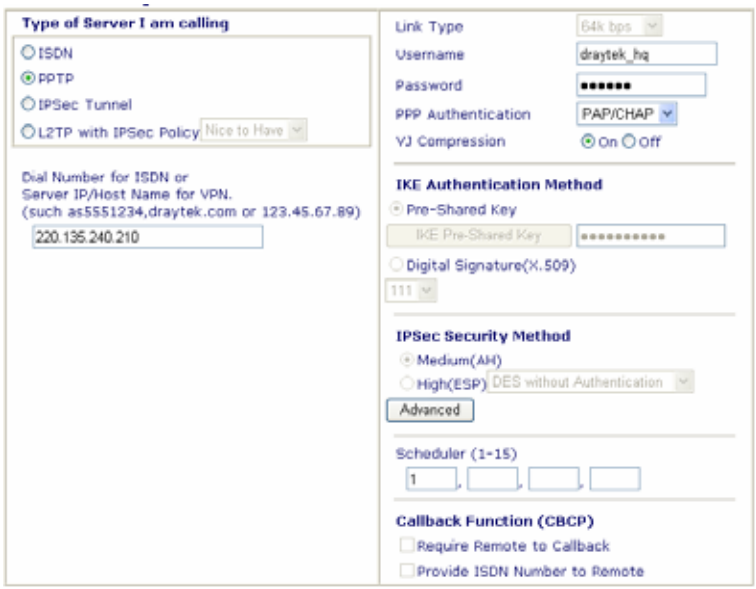
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

5. Set Dial-Out Settings as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

➢ If an IPSec-based service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.



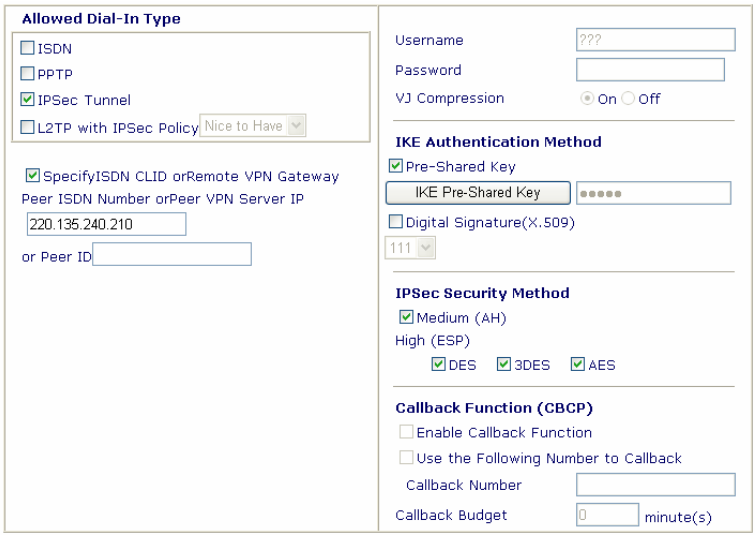
- If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.



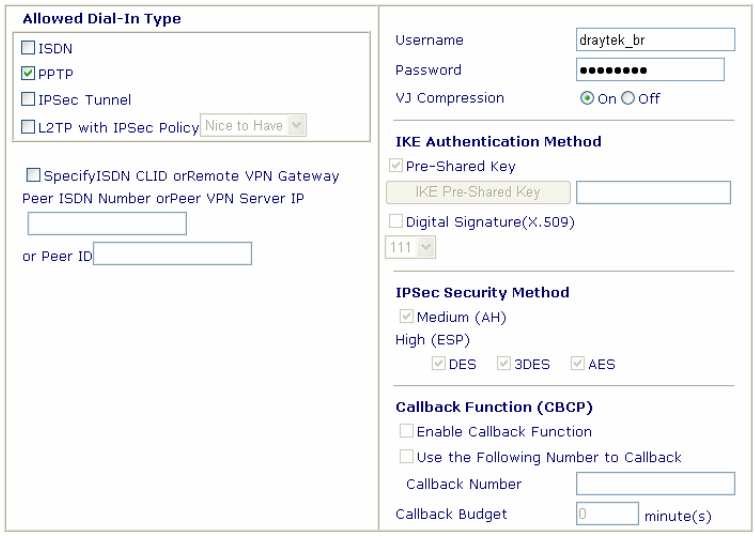
6. Set Dial-In settings to as shown below to allow Router B dial-in to build VPN connection.

- If an IPSec-based service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply

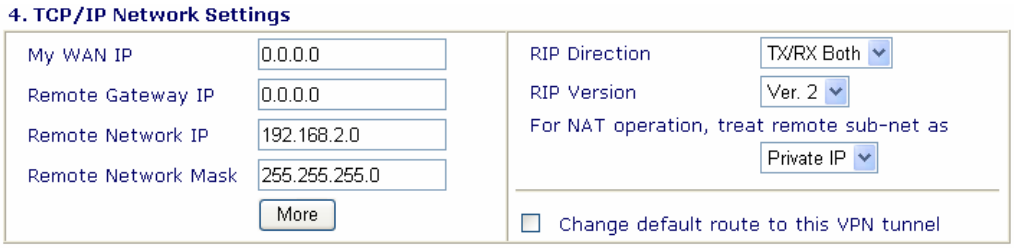
the settings defined in **IPSec General Setup** above.



- If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.



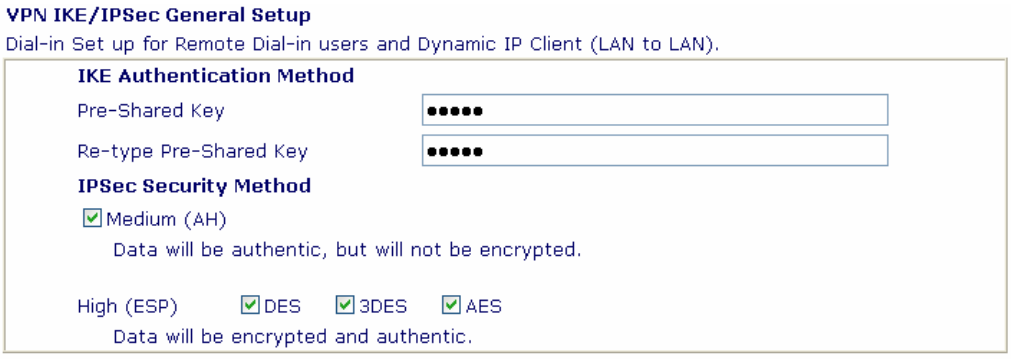
Settings in Router B in the remote office:

8. Go to **Remote Access Control** to enable the necessary VPN service.

9. Then,

➢ To use PPP based services, such as PPTP, L2TP, or ISDN, you have to set general settings in **PPP General Setup**.

➢ To use IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

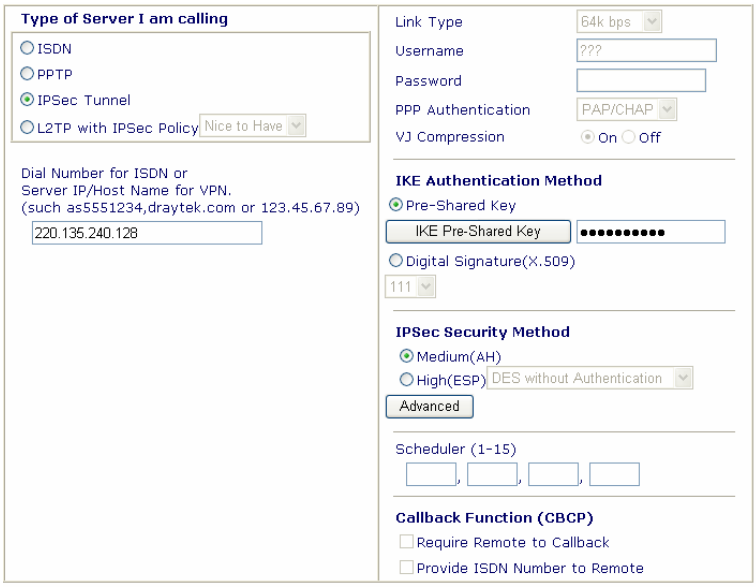


10. Go to **LAN-to-LAN Profiles**. Click on one index number to edit a profile.

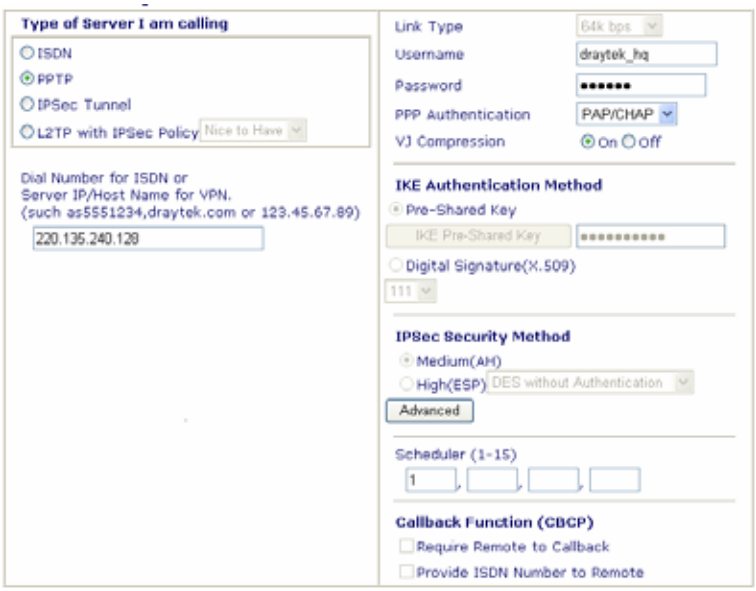
11. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

12. Set Dial-Out Settings as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

- If an IPSec-based service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

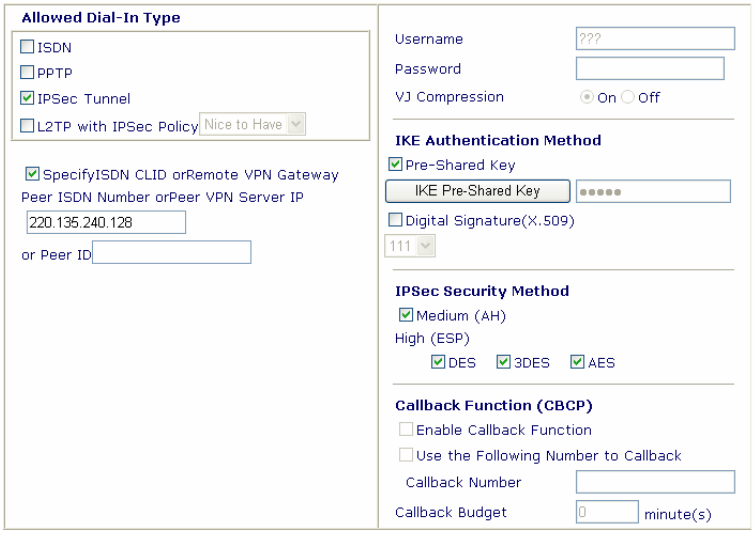


- If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

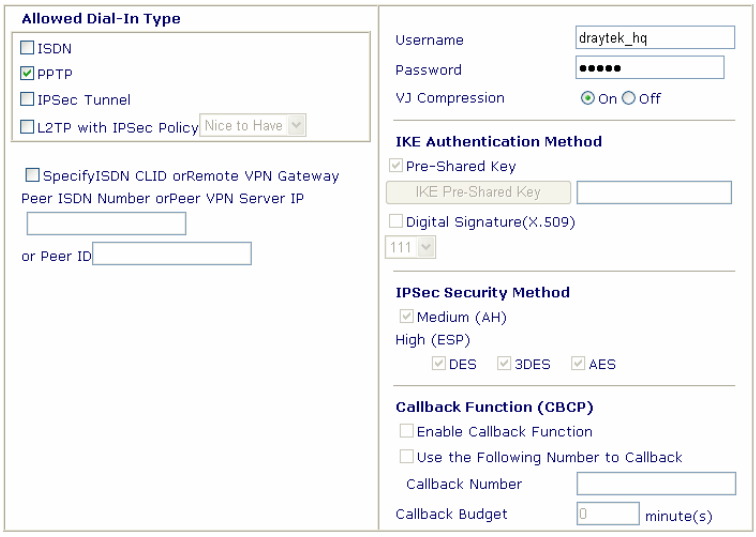


13. Set Dial-In settings to as shown below to allow Router A dial-in to build VPN connection.

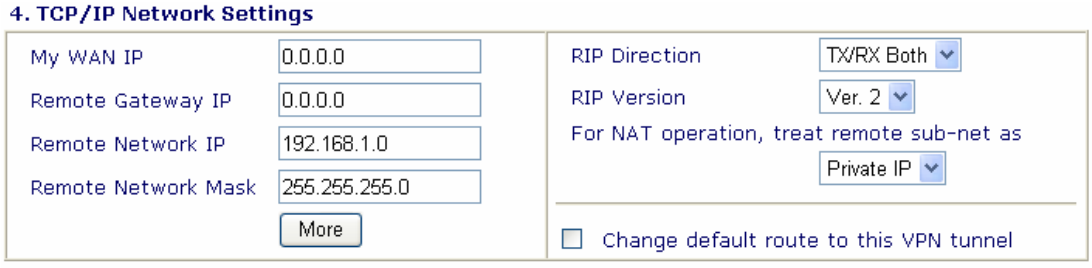
➢ If an IPSec-based service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

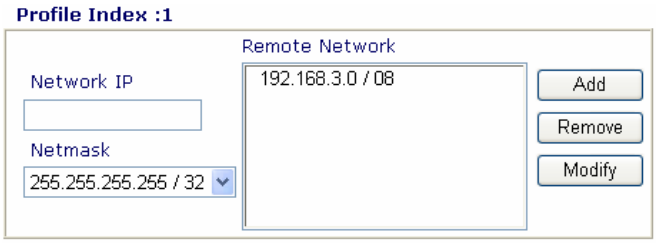


➢ If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



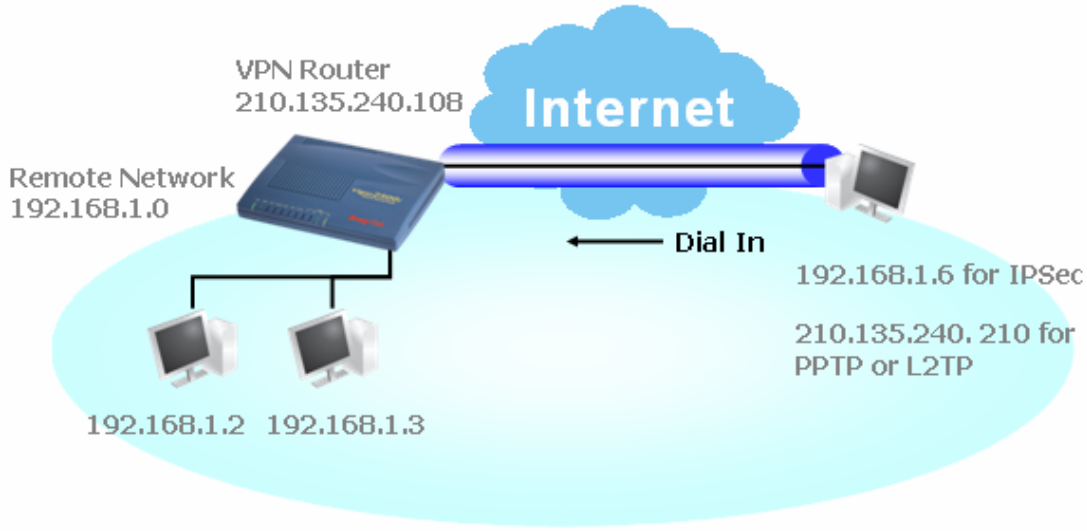
14. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.





Create a Remote Dial-in teleworker connection between the teleworker and headquarter

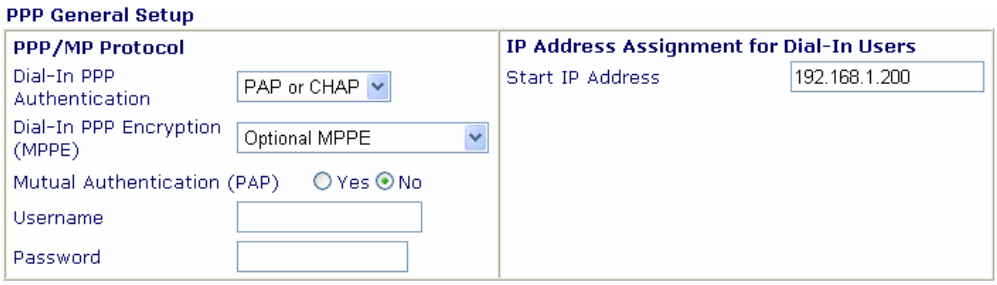
The other common case is that you as a teleworker may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



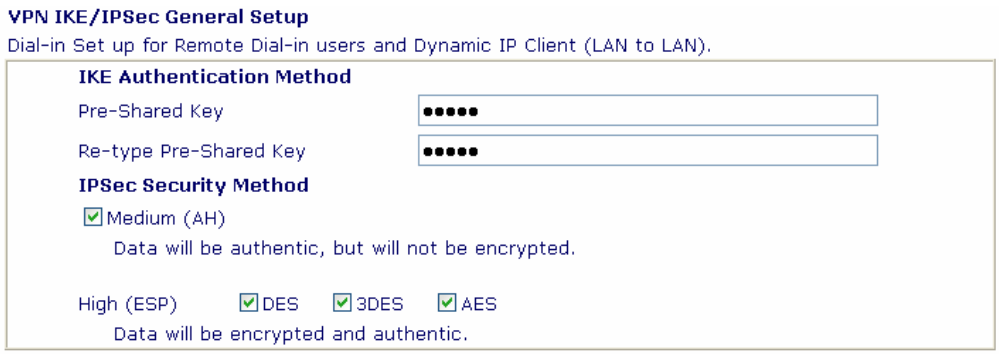
Settings in VPN Router in the enterprise office:

1. Go to **Remote Access Control** to enable the necessary VPN service.
2. Then,

➢ To use PPP based services, such as PPTP, L2TP, or ISDN, you have to set general settings in **PPP General Setup**.

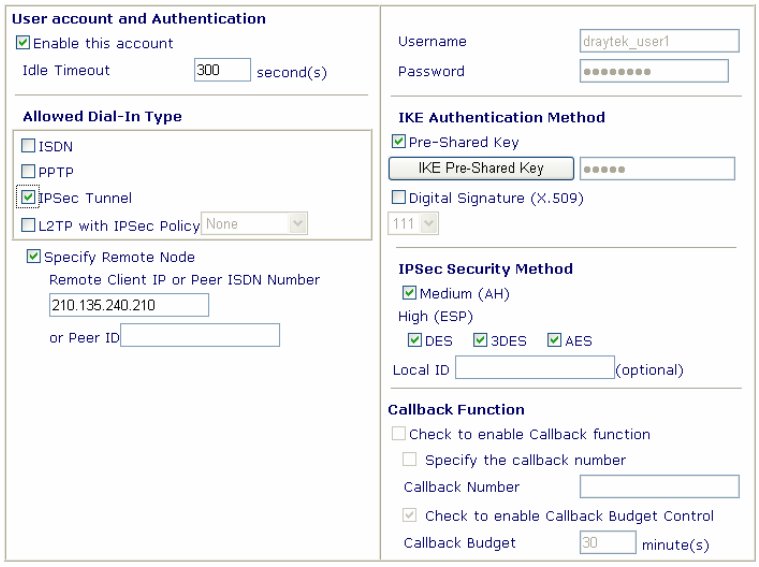


➢ To use IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

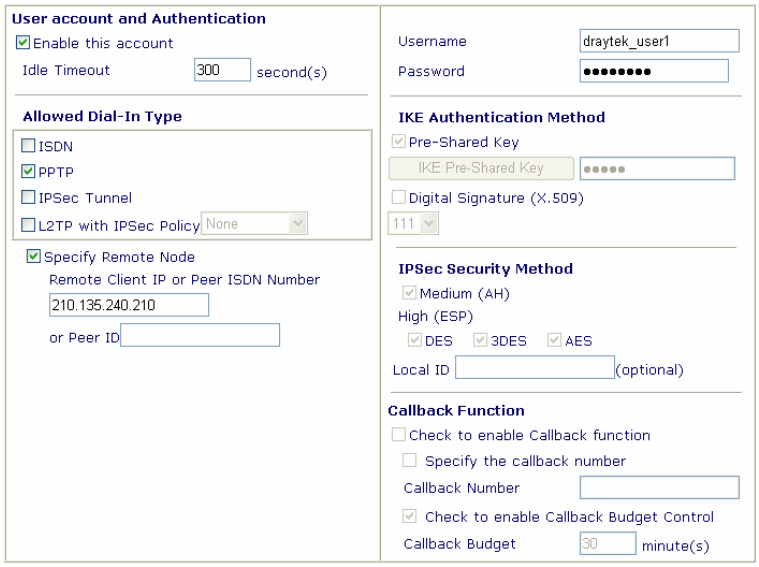


3. Go to **Remote Users Profiles (Teleworkers)**. Click on one index number to edit a profile.
4. Set Dial-In settings to as shown below to allow the remote user dial-in to build VPN connection.

➢ If an IPSec-based service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

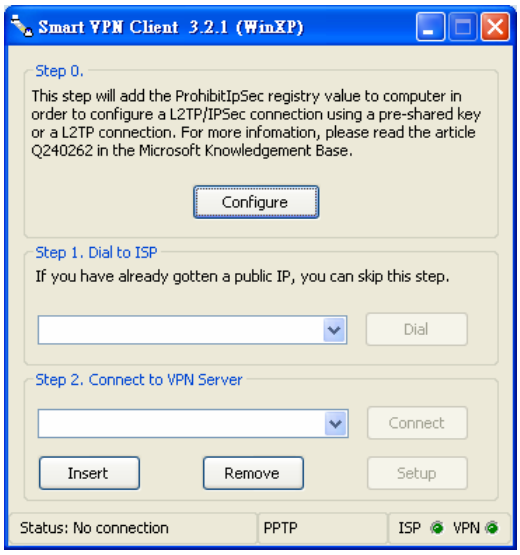


➢ If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



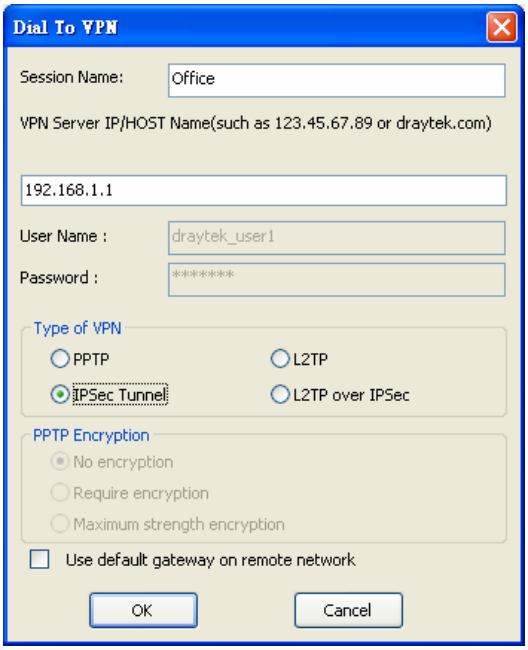
Settings in the remote host:

5. Find the complimentary software Smart VPN client or go to www.draytek.com download center. Install as instructed.
6. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.

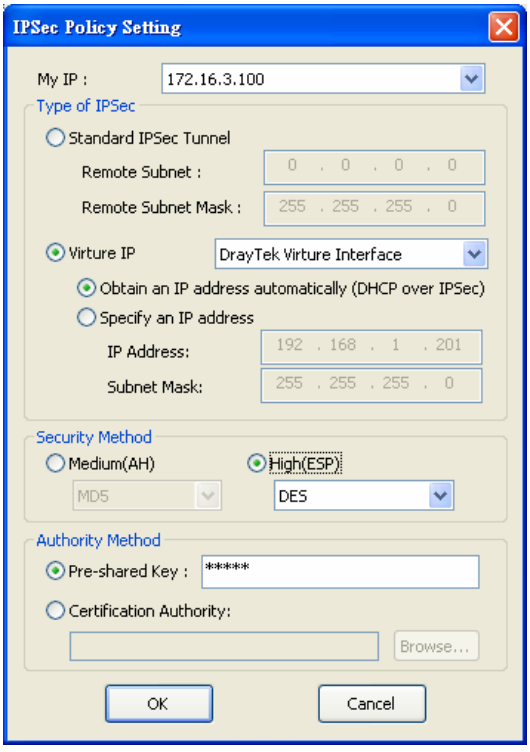


7. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

➢ If an IPSec-based service is selected as shown below,

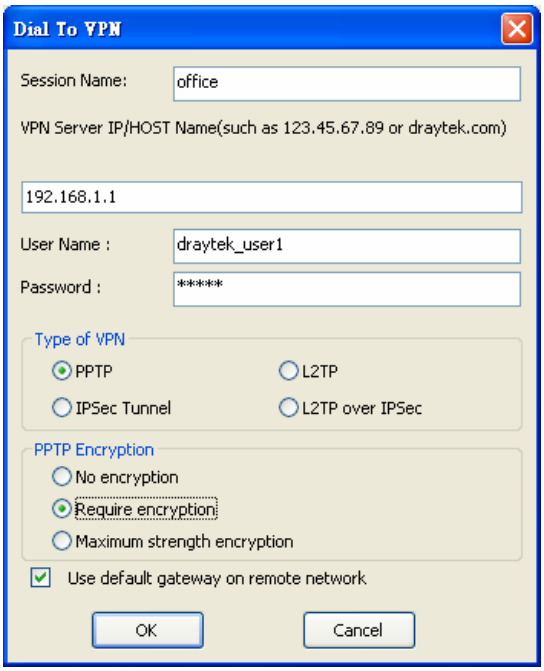


You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.



- If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and

encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.



8. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

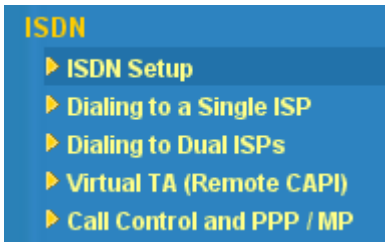
Chapter 9
ISDN Setup

9.1 Introduction

This section includes **ISDN Setup, Dialing to Single ISP, Dialing to Dual ISPs, Virtual TA (CAPI), and Call Control and PPP/MP** settings**.**

9.2 Settings

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



Dialing to single or dual ISP

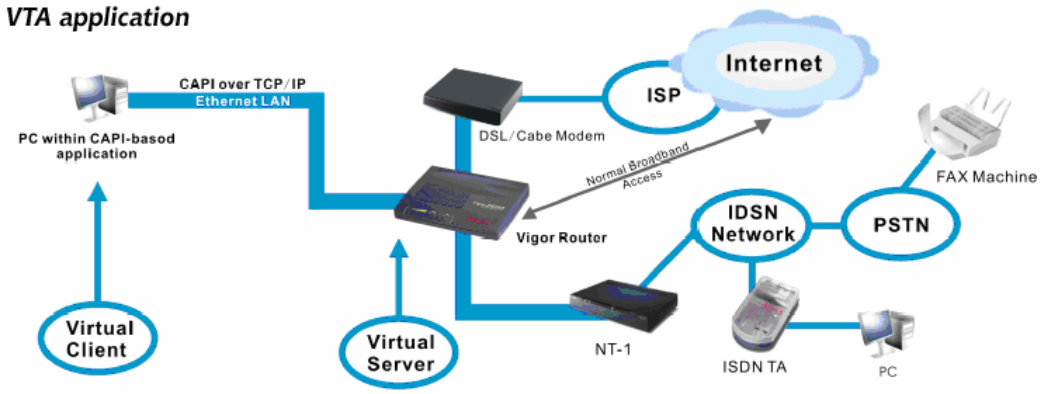
Select **Dialing to a Single ISP** if you access the Internet via a single ISP. Select **Dialing to Dual ISPs** if you have more than one ISP. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs that do not support Multiple-Link PPP (ML-PPP). In such cases, dialing to two ISPs can increase the bandwidth utilization of the ISDN channels to 128kbps data speed.

Virtual TA

Virtual Terminal Adapter (VTA) is actually a “CAPI” software, which can

simulate a real ISDN terminal adapter installed on your computer. You can install the CAPI-compliant software for dial-up networking, fax or voice applications, which depends on the functionality of the CAPI software you installed. To employ the VTA feature, please download the VTA drivers (available only to Windows 98SE/2000/XP) from http://www.draytek.com/english/support/download.php .

When a local host or PC in the network uses popular CAPI-based software such as RVS-COM or BVRP to access the router, it can act as a local ISDN TA to send or receive FAX messages over the ISDN line. Basically, there is a client/server network model. The built-in Virtual TA server handles the establishment and release of connections. The Virtual TA client, who is the local hosts or PCs, creates a CAPI-based driver to relay all CAPI messages between the applications and the router CAPI module.

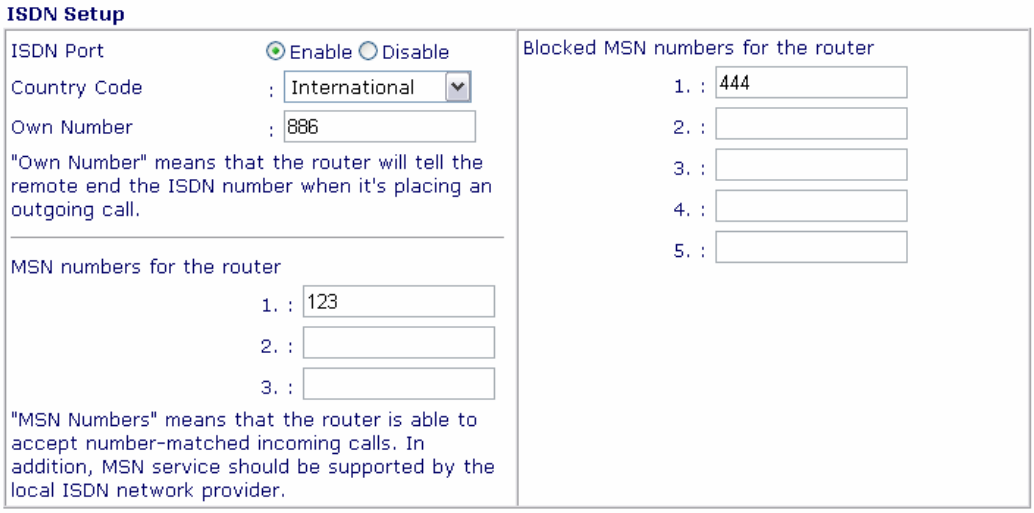


As depicted in the above application scenario, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA, etc. Click the **Virtual TA(Remote CAPI) Setup** tab in the **Quick Setup** field to configure the Virtual TA features.

Call Control and PPP/MP

Some applications require that the router (only for the ISDN models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature by allowing user to make a phone call to the router and then ask it to dial up to the ISP. Accordingly, a teleworker can access the remote network to retrieve resources. Of course, a fixed IP address is required for WAN connection and some internal network resource has to be exposed for remote users, such as FTP, WWW.

9.2.1 ISDN Setup



ISDN Port

Click **Enable** to open the ISDN port and **Disable** to close it.

Country Code

For proper operation on your local ISDN network, you should choose the correct country code.

Own Number

Enter your ISDN number. Every outgoing call will carry the number to the receiver.

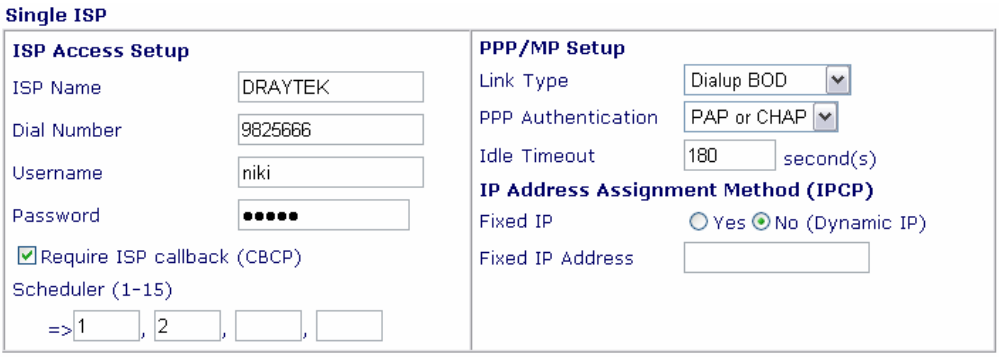
Blocked MSN Numbers for the router

Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN number

MSN Numbers for the Router

MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, local ISDN network provider should support MSN services. The router provides three fields for MSN numbers. Note that MSN services must be acquired from your local telecom operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching.

9.2.2 Dialing to Single ISP and Dialing to Dual ISPs



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, check this box to activate the Callback Control Protocol during the PPP negotiation.

Scheduler (1-15)	Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules.

PPP/MP Setup

Link Type	Enter your ISP name. **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 in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the Advanced Setup field > Call Control and PPP/MP Setup.
PPP Authentication	**PAP Only:** Configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP:** Configure 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 be 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 to the ISP will always remain on.

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**.

9.2.3 Virtual TA (Remote CAPI)

Before describing the configuration of Virtual TA in the Vigor routers, please heed the following limitations.

1. The Virtual TA client only supports MicrosoftTM 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 has two B channels. The maximum number of active clients is also 2.
4. Before you configure the Virtual TA, you must set the correct country code in **ISDN Setup**.

Install a Virtual TA Client

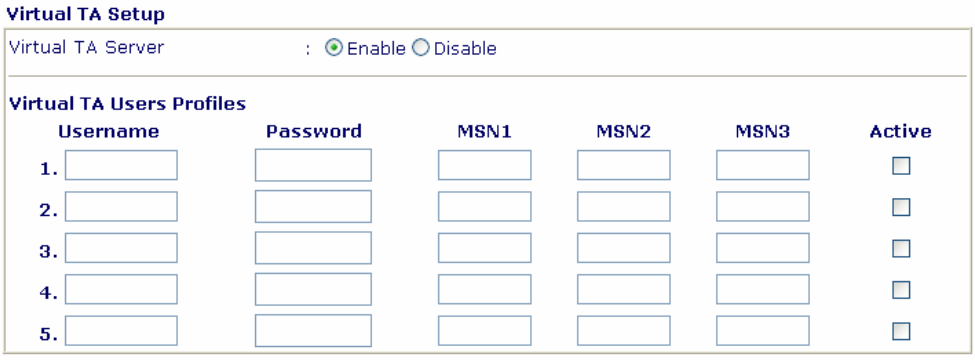
1. Insert the CD-ROM bundled with your Vigor router. Find **VTA Client** tool in the Utility menu and click on the Install button.
2. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.
3. After the computer restarts, you will see a VT icon in 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. If the icon text is RED, it means the client has lost the connection to the server. This time, please check the physical Ethernet connection.

Configure a Virtual TA Client/ Server

Since the Virtual TA application is a client/server network model, you must configure it on both ends to run properly your Virtual TA application.

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



Virtual TA Server

Enable	Select it to activate the server.
Disable	Select it to deactivate the server. All Virtual TA applications will be terminated.

Virtual TA User Profiles

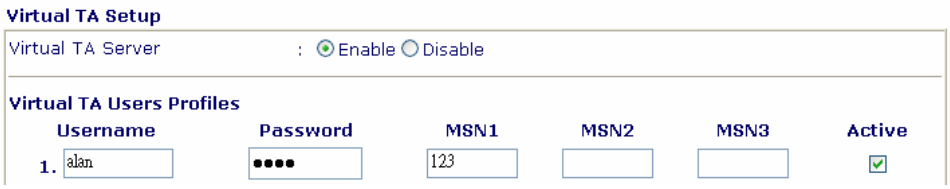
Username	Enter the username of a specific client.
Password	Enter the password of a specific client.

MSN 1/2/3	MSN stands for Multiple Subscriber Number. It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank.
Active	Check it to enable the client to access the server.

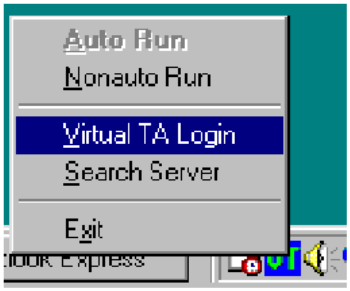
An example of VTA Client and Server connection

Note that creating a single user access account will confine the access to the Virtual TA server to only the specified account holders. In this example, we assume you did not acquire MSN service from your ISDN network provider.

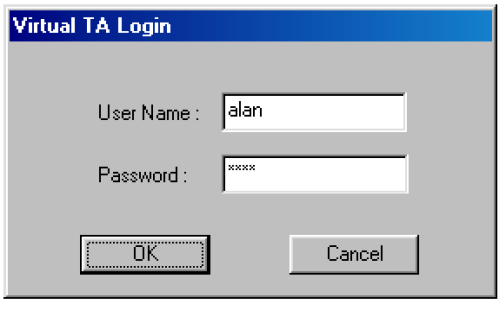
1. On the server: Click **Virtual TA (Remote CAPI) Setup** tab, and fill in the Username and Password fields. Check the **Active** box to enable the account.



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 tab to launch the login box.



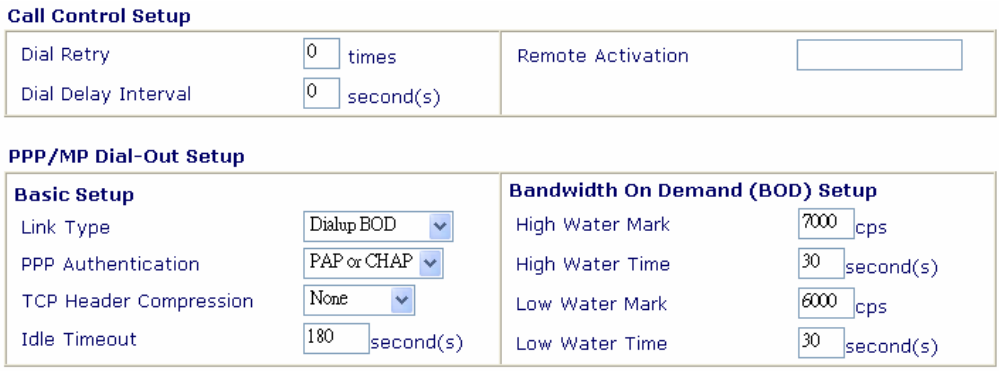
4. Enter the Username/Password and then click **OK**. After a short time, the VT icon text will turn green.

5. If you have applied to an MSN number service, the Virtual TA server can assign which client has the specified MSN number. When an incoming call arrives, the server will inform the appropriate client. Now if we have typed the specified MSN number”123” in the VTA client, when the Virtual TA server sends an alert signal to the VTA 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.

9.2.4 Call Control and PPP/MP

In this chapter, we will focus on the steps of configuration of call control and PPP/MP.

After you click the **Call Control and PPP/MP Setup** tab. The following screen will appear.



Call Control Setup

Dial Retry	It specifies the dial retry counts per triggered packet. A triggered packet is the 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	It specifies the interval between dialup retries. By default, the interval is 0 second.
Remote Activation	It specifies 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 terminate the incoming call immediately and dial to the ISP.

Note that **Dialing to a Single ISP** should be preconfigured properly.

PPP/MP Dial-Out Setup

Basic Setup

Link Type	Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.
PPP Authentication	It specifies the PPP authentication method for PPP/MP connections. Normally you can set it to PAP/CHAP for better compatibility.
TCP Header Compression	**VJ Compression**: It is used for TCP/IP protocol header compression. Normally it is set to Yes to improve bandwidth utilization.
Idle Timeout	Because our IDSN link type is “Dial On Demand”, the connection will be initiated only when needed.

Bandwidth-On-Demand (BOD) Setup

Bandwidth-On-Demand is for Multiple-Link PPP (ML-PPP or MP). The parameters are only applied when you set the **Link Type** to

Dialup BOD. The ISDN usually use one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide 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 situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being 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 situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).

Chapter 10
Wireless LAN Setup(for G models)

10.1 Introduction

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

Boost Up Your Wireless Speed

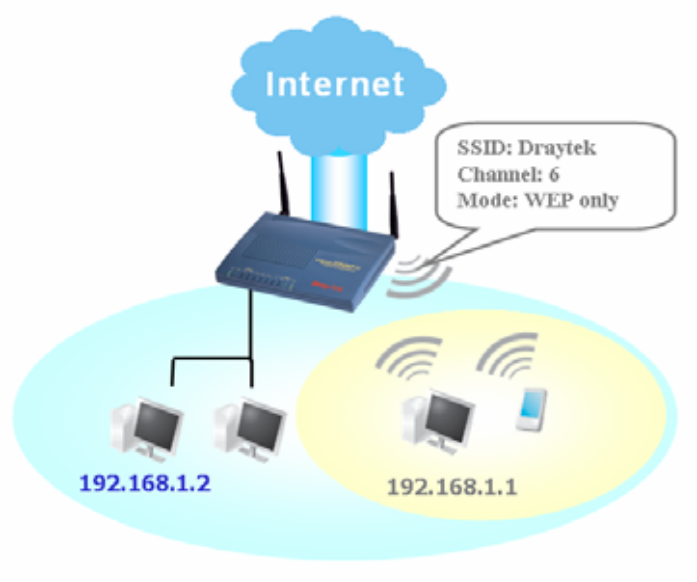
The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11g protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology Super G ^{TM} to lift up data rate up to 108 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

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

Basic Wireless LAN Concept

In an Infrastructure Mode of wireless network, Vigor wireless router plays

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



Securer than Ever

Real-time Hardware Encryption

Vigor Router is equipped with hardware 3DES encryption engine so it can apply highest standard to your data without influencing user experience.

Complete Security Standard Selection

To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

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

WPA (Wi-Fi Protected Access), including the first generation WPA and the latest WPA2, is the most dominating security mechanism in industry. There are two modes in WPA standard: WPA Pre-Share Key (WPA/PSK) and complete WPA. WPA Pre-Share Key (WPA/PSK) is to use a pre-defined key(PSK) for encryption during data transmitting. For PSK format, the first generation WPA applies Temporal Key Integrity Protocol (TKIP) while WPA2 applies AES.

The complete WPA standard combines not only encryption but also authentication. IEEE 802.1x is the most common implementation by setting up an RADIUS server in your network. The RADIUS server acts as a third party authenticator between the Vigor router and its stations to certify the station's identity before both parties start data communication. RADIUS server also helps to negotiate the key using for data encryption afterwards so neither of the access point and the station need to define a pre-shard key in advance. IEEE 802.1x can be used along with WEP as well.

In brief, the comparison of complexity above:

- WPA2 > WPA > WEP
- WPA2/802.1x > WPA/802.1x > WEP/802.1x

Since WEP has been proved to be vulnerable, you may consider use WPA for the most secure connection. Nevertheless, the more complex security mechanism is applied, the less efficient your network communication may be. You should select the appropriate security mechanism according to your needs.

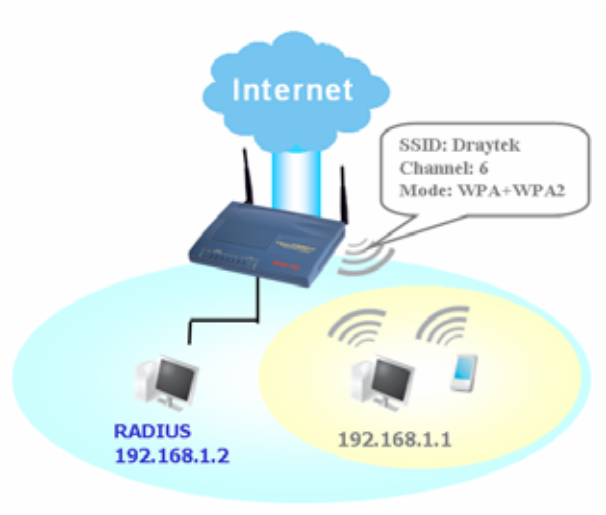
No matter which security suite you select, they all will enhance the

over-the-air data protection and /or privacy on your wireless networks. The Vigor wireless router is very flexible and can support multiple secure connections with either WEP or WPA at the same time.

Example 1

Example 2

Example 3



Separate the Wireless and the Wired

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

Manage Wireless Stations

Station List will display all the station in your wireless network and the status of their connection. Besides, you can allow the connection of only trusted user with the function **MAC Access control**. **Station Rate Control** can assign specific download/upload rate to each STA.

Extend You Network Wirelessly– WDS (Wireless Distribution System)

WDS enables single-radio Access Points (APs) to be wirelessly connected instead of using a wired Ethernet connection. The major benefit of it includes

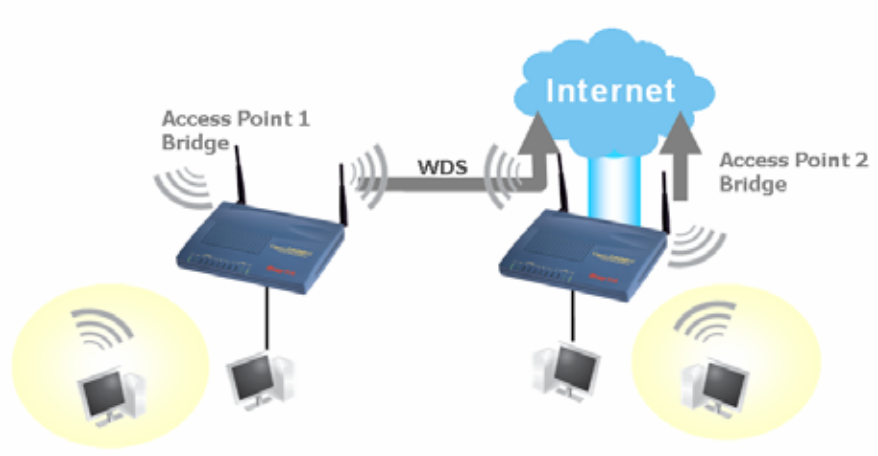
- bridge traffic between two LANs through the air
- extend the coverage range of a WLAN.

To achieve the goals of wireless AP-to-AP connectivity above, the Vigor wireless router can be configured to two modes accordingly, **Bridge Mode** and **Repeater Mode**.

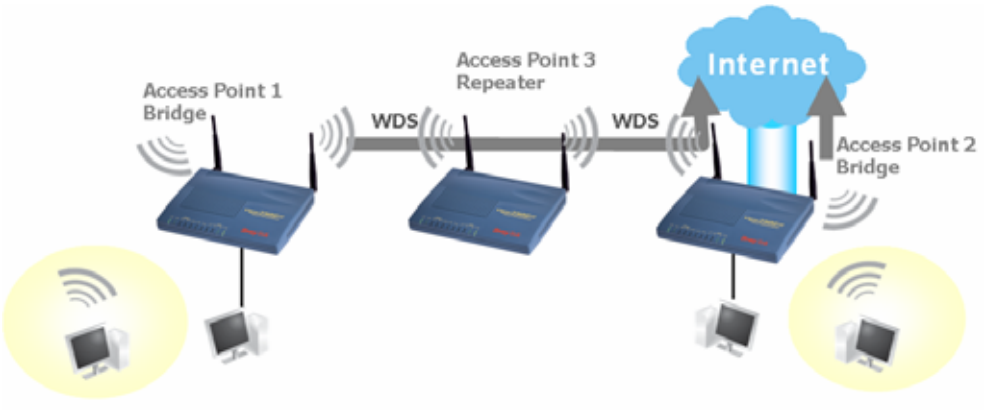
We provide two deploy examples to explain the major difference between these two modes:

- WDS Bridge Mode: the router can forward WDS packets of its local wireless/wired hosts to peer APs. It can act as a bridge between several wireless LAN and wired LAN.
- WDS Repeater Mode: the router can forward (or repeat) one peer AP's WDS packets to another peer AP wirelessly.

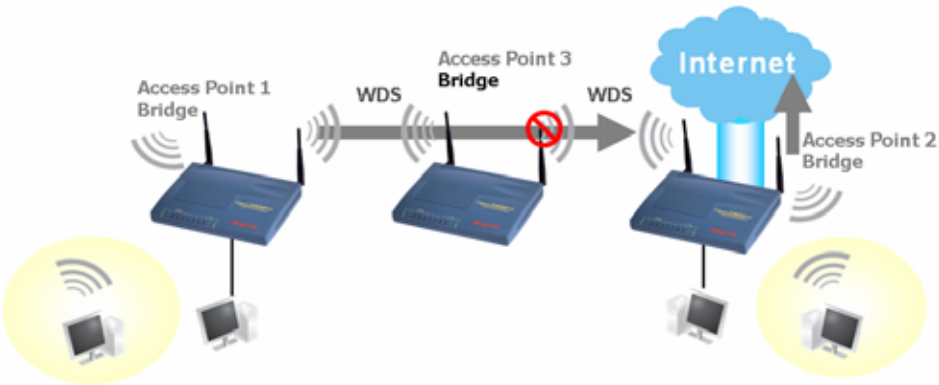
Example 1



Example 2



According the definition of WDS modes, note that the deployment in the illustration below will **NOT** work:



As long as you enable the WDS function, no matter what mode you set, Vigor wireless router can always work as an access point that has its own network unless you manually disable it. Please refer to the **WDS>>Access Point Function**.

To complete our security solution for all wireless network, Vigor wireless router provides WEP and WPA Pre-Shared Key (TKIP or AES) for your WDS security selection. Since the WDS standard doesn't define the mandatory encryption methods, not all the products on the market support the most secured WPA/PSK for WDS link. Unless you are connecting two

Vigor wireless routers, you may need to check whether if 3rd party access point support WPA/PSK.

All the WDS peer access points should use the same channel.

Discover Access Point in the Neighborhood

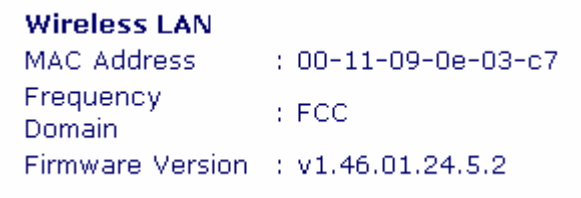
Access Point Discovery is a function usually provided in wireless client utility in order to find an Access Point to connect. The Vigor wireless router also leverages this functionality to ensure quality and safe wireless experience. Via scanning result, you may select the least crowded or interfered channel to set up your wireless network. You can select the WDS peer AP based on the MAC address here as well

10.2 Settings

In this chapter, we explain the capabilities of the wireless LAN and its associated web configurations. Use the link on the menu to configure the wireless LAN function.

Check Wireless Status

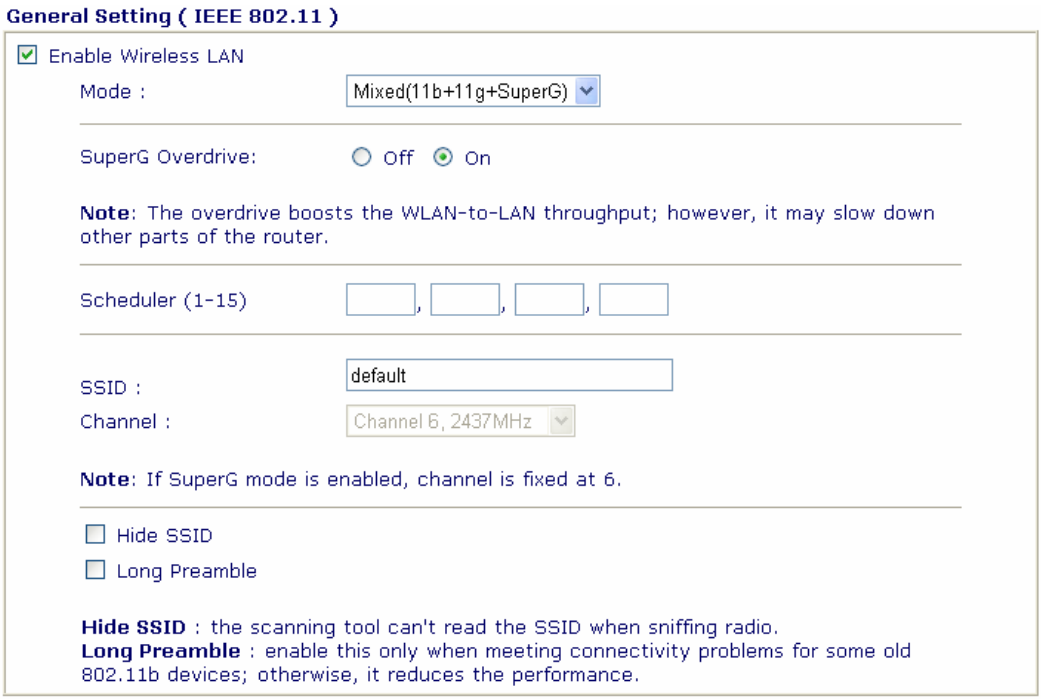
Also, click the "**System maintenance>>System status**". You will see the Wireless LAN status:



This web page will show the Wireless LAN information including **MAC Address**, **Frequency Domain** and **Firmware Version**. **Frequency Domain** can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various. The **Firmware Version** indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi card.

10.2.1 General Settings

Click on **General Settings** and you will see the bellowed window.



Enable Wireless LAN

Check the box to enable wireless function.

Mode

Select an appropriate wireless mode.

Mixed (11b+11g+SuperG)	The router communicates with standard 802.11b, standard 802.11g and Super G STAs simultaneously.
Mixed (11b+11g)	The router communicates with standard 802.11b and standard 802.11g STAs simultaneously.
Super G only	The router only communicates with Super G STAs.
11g only	The router communicates with standard 802.11b STAs.
11b only	The router communicates with standard 802.11b STAs.

Scheduler

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

SSID(Service Set Identifier) and Channel

The default SSID is "default". We suggest you to change it.

SSID	The identification of the wireless LAN. SSID can be any text numbers or various special characters.
Channel	The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.

Hide SSID

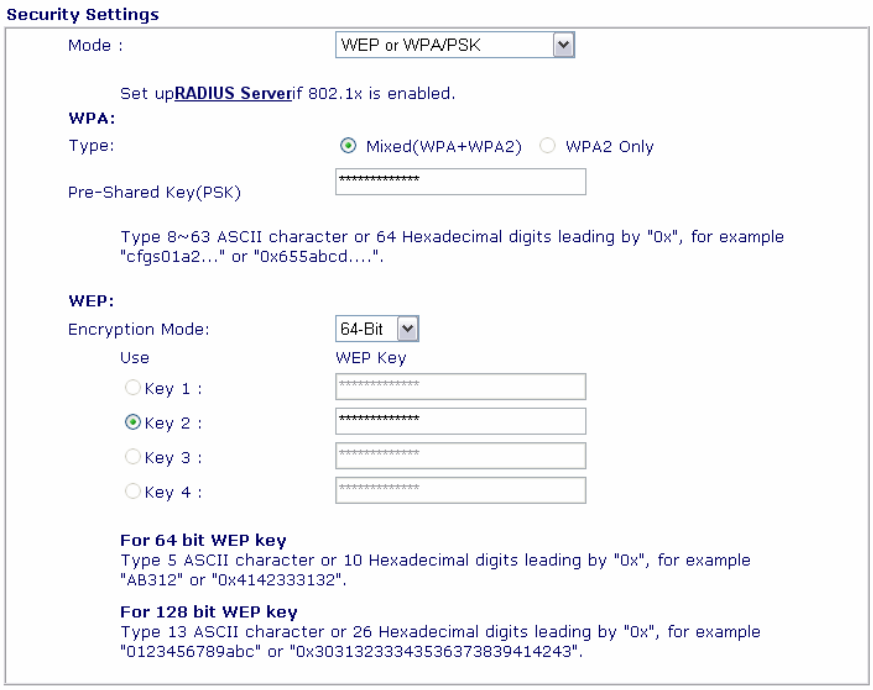
Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying

Long Preamble

This option is to define the length of the sync field in the preamble. In the intend to improve the efficiency of the wireless network for more “real-time” applications, streaming video and Voice-over-IP telephony applications, most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network device still keep using long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

10.2.2 Security

Clicking the **Security Settings**, and a new window will pop-up.



Mode

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

Disable	Turn off the encryption mechanism.
WEP Only	Accepts only WEP clients and the encryption key should be entered in WEP Key.
WEP/802.1x Only	Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.
WEP or WPA/PSK	Accepts WEP and WPA clients with legal key accordingly. Remember to select WPA type to define either Mixed or WPA2 only in the field below.
WEP/802.1x or WPA/802.1x	Accept WEP or WPA clients with 802.1x authentication. Remember to select WPA type to define either Mixed or WPA2 only in the field below. Since the key will be auto-negotiated during authentication, the field of key

	setting below will be not available for input.
WPA/PSK Only	Accepts WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.
WPA/802.1x Only	Accept WPA clients with 802.1x authentication. Remember to select WPA type to define either Mixed or WPA2 only in the field below. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK entered manually in this field below or automatically negotiated via 802.1x authentication.

Type	Select from **Mixed (WPA+WPA2)** or **WPA2 only**.
Pre-Shared Key(PSK)	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...")

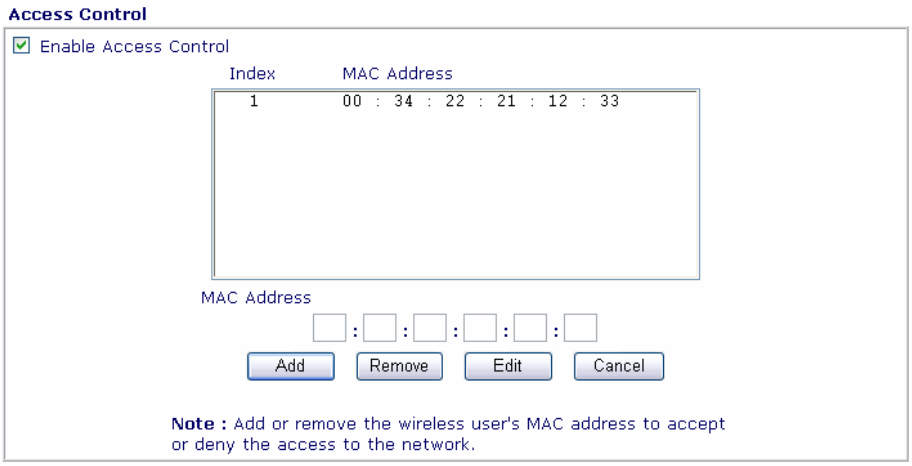
WEP

64-Bit	For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
128-Bit	For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM. (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D)

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

10.2.3 Access Control

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



Enable Access Control

Select to enable the MAC Address access control feature.

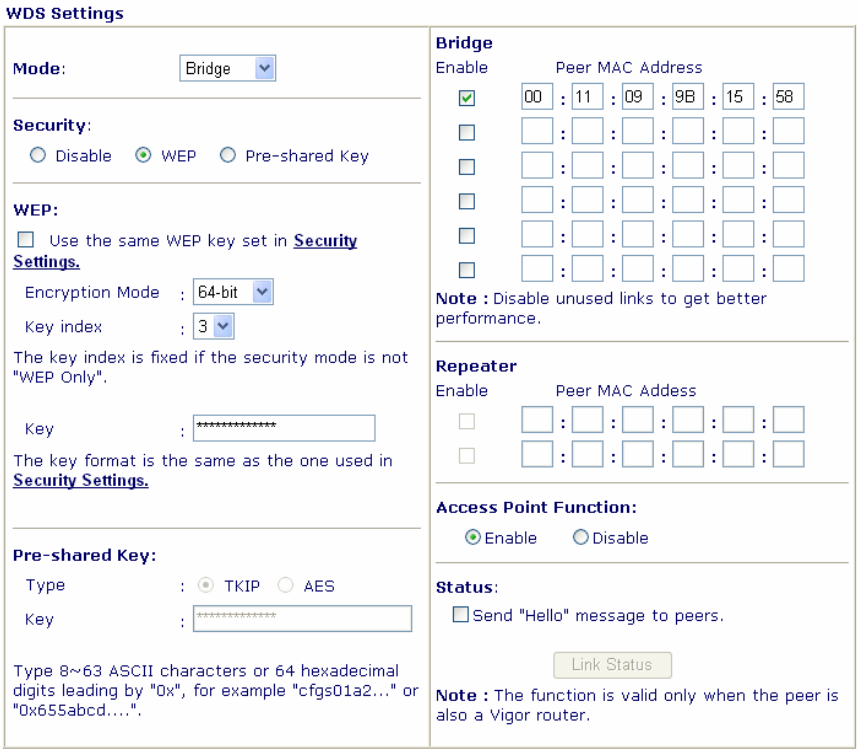
MAC Address

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

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

10.2.4 WDS

Click on the **WDS Settings** to see the window below.



Mode

Disable	Disable WDS function.
Bridge	Set Vigor router in Bridge mode.
Repeater	Set Vigor router in Repeater mode.

Security

Before you set up encryption method for WDS link, you may need to check the below table for the available WDS encryption options bound with encryption of WLAN in **Wireless>>Security**.

Mode for WLAN Security	Available WDS Encryption Option
Disable	Disable
WEP Only	WEP
WEP/802.1x Only	WEP

WEP or WPA/PSK	WEP, Pre-Shard Key
WEP/802.1x or WPA/802.1x	WEP, Pre-Shard Key
WPA/PSK only	Pre-Shard Key
WPA/802.1x only	Pre-Shard Key

Once decide what to use for WDS encryption, fill or check the fields needed.

Disable	Disable security function for WDS link.
WEP	Define the WEP key to use for WEP encryption of WDS link. You may select from one of the below: **Use the same WEP key set in Security**: For WDS link, use the defined key index already used for WLAN in **Wireless>>Security>>WEP**. **Settings**: Set the exclusive key used for WDS link. Select key length (64-bit or 128-bit). Select key index if the **Mode** is not WEP only in **Wireless>>Security**.
Pre-Shared Key	**Type**: Select encryption type. **Key**: Set the key used for WDS link.

Bridge or Repeater

Enable	Build WDS link with the WDS peer according to the **Peer MAC Address**.
Peer MAC Address	The MAC address of the WDS peer. To have the list shown here, go to **Access Point Discovery>>Scan** and add selected **AP's MAC Address** to WDS settings. Otherwise, manually type the MAC address of the peer access point that you wish to connect to.

Access Point Function

Check **Enable** to indicate that the Vigor router will work as an

access point for its WLAN while work as a WDS compliance building WDS link with other APs. Check **Disable** to indicate that the Vigor router will dedicate to work as a WDS compliance, either in Bridge or Repeater mode.

Status

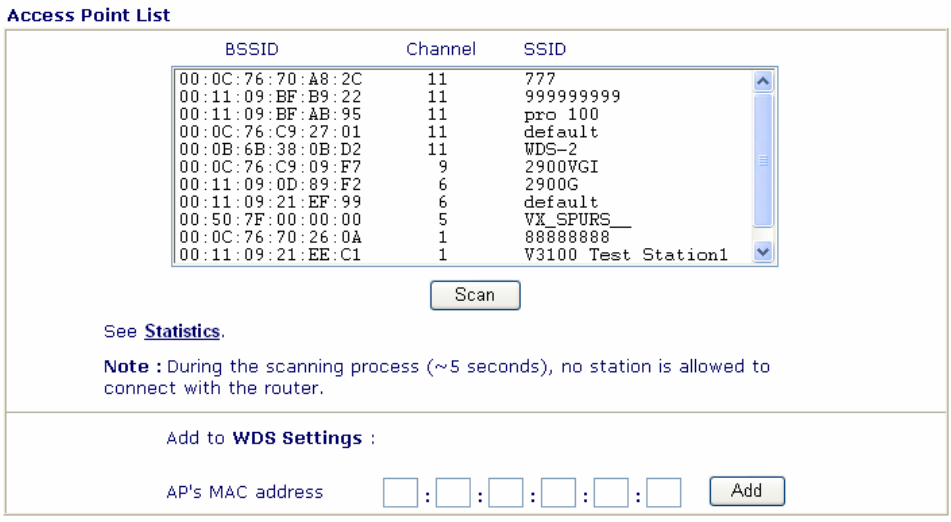
A complimentary test among the Vigor wireless routers by sending "Hello" message to the peers. Click the **Link Status** to check who receive the message.

The status will only be available among Vigor wireless routers.

U (Up)	Link is active.
D (Down)	No traffic from this link.
O (Off)	Link is disabled. No packet will be sent to this link.

10.2.5 AP Discovery

To discover all access point in your neighborhood, click on **Scan**.



Access Point list

Display all access points in the neighborhood.

BSSID	Add a new MAC address into the list.
Channel	Delete the selected MAC address in the list.
SSID	Edit the selected MAC address in the list.

Statistics

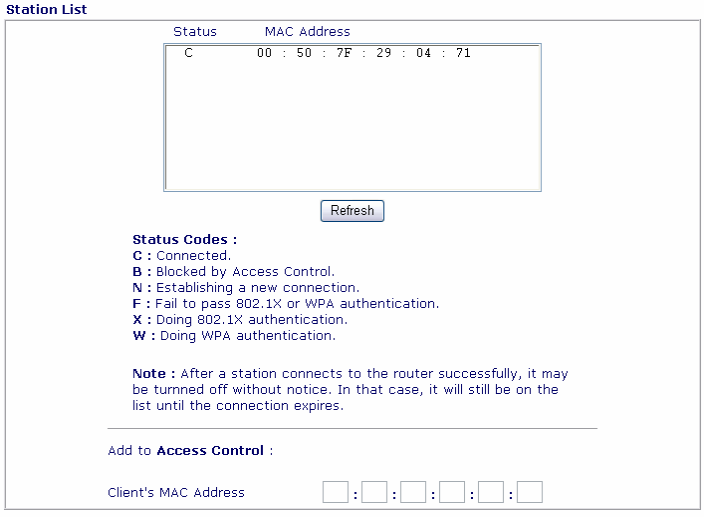
Account access points in the neighborhood based in each channel.

Add to WDS

Here you can specify the MAC address of the access point with which you want to build WDS link.

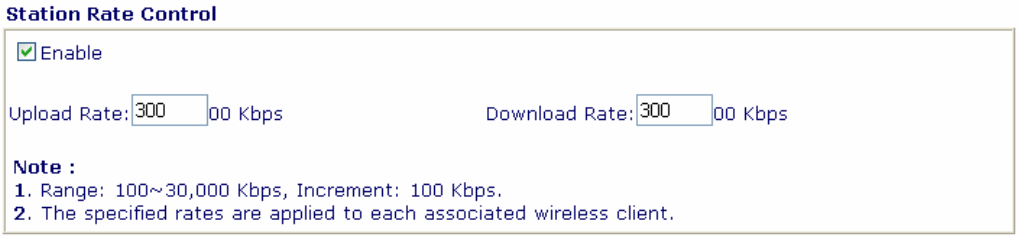
10.2.6 Station List

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



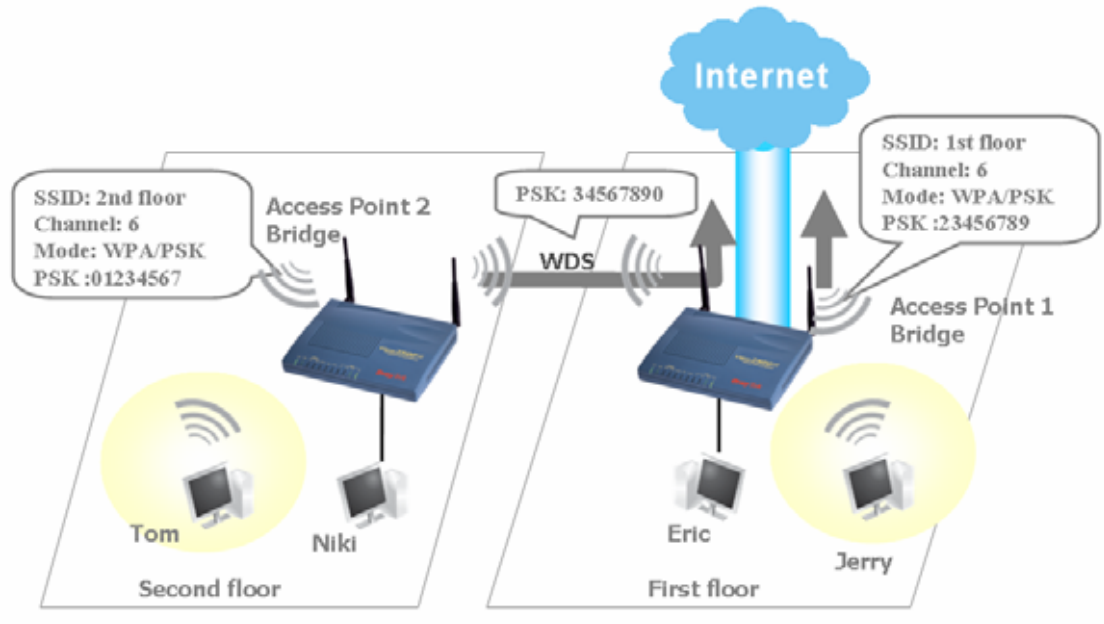
10.2.7 Station Rate Control

To specify the limitation of upload or download speed, fill the field below. The rate is for a single client and will be applied to all clients in the network.



Application Scenario: Step by Step

Assume you have two Vigor wireless routers at home. Access Point 2 on the second floor will build its WLAN and LAN and connect to Internet via Access Point 1 using WDS PSK–encrypted link.

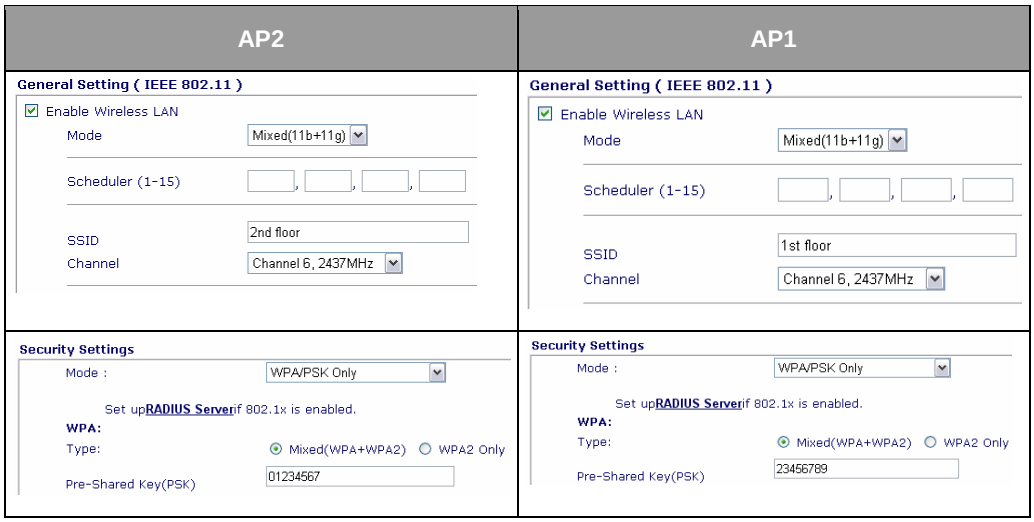


Step 1: Set Internet Access in AP 1

- Set up **Internet Access** according to the information you got from your ISP. Ensure Eric can access Internet.

Step 2: Set WLAN in AP 1 and AP 2

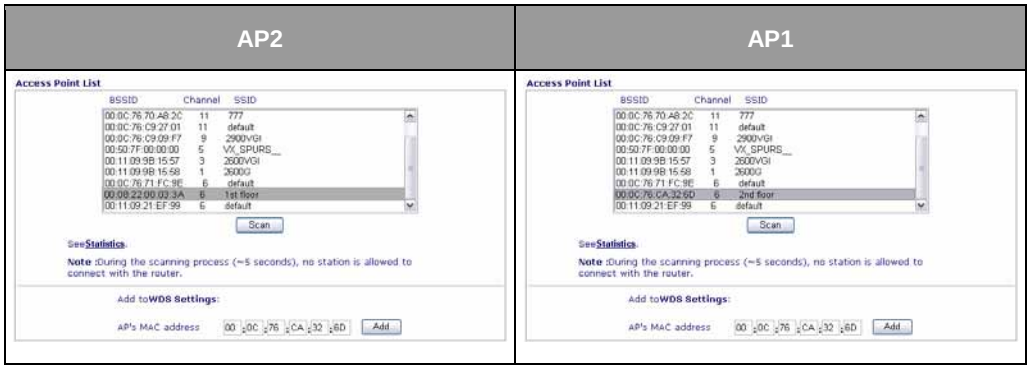
- Go to **Wireless>>General Settings** or **>>Security** to set its WLAN information, including SSID, Channel, Mode and encryption key.



- Ensure that STAs connects to AP by checking **Wireless>>Station List**. Jerry can connect to AP1. Tom and Niki can connect to AP 2.

Step 3: Set WDS link between AP 1 and AP 2

- Go to **Wireless>>AP Discovery>>Scan** searching for peer AP. Find its BSSID (MAC address) and click **ADD** to WDS settings.



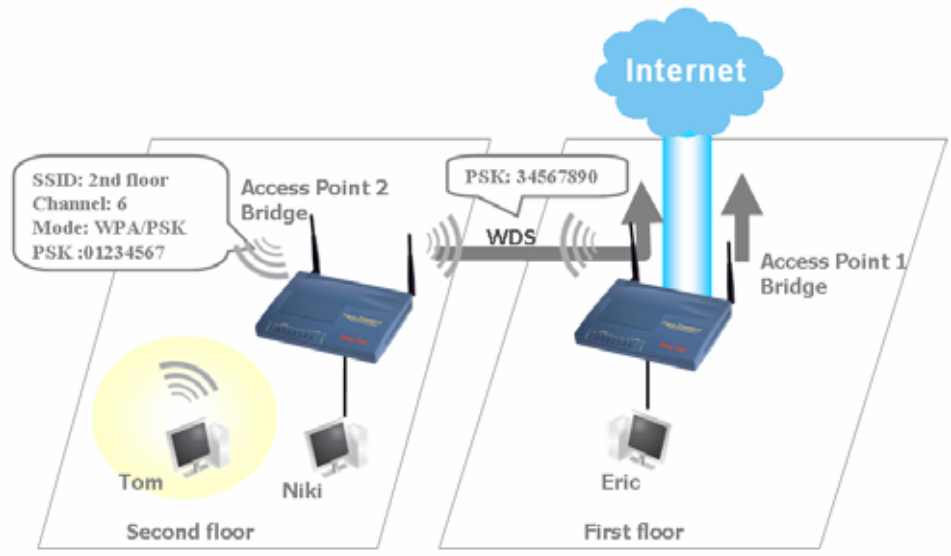
- The window will then switch to **Wireless>>WDS**. Here select **Bridge** in **Mode** and set **PSK** in **Security.** The peer MAC address added above will be shown in the list.

AP2	AP1
	

Others:

- To close AP1 WLAN, go to **Wireless>>WDS** and check on **Disable** in Access Point Function.

The application scenario will be as shown below:



Chapter 11
System Maintenance Setup

11.1 Introduction

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

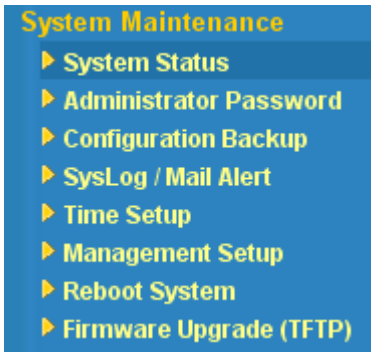
The **Configuration Backup** enables you to keep running configurations of your current router as a file or restore the configurations with the file. The router provides a web-based way to let you backup or restore the configuration very simple.

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

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

11.2 Settings

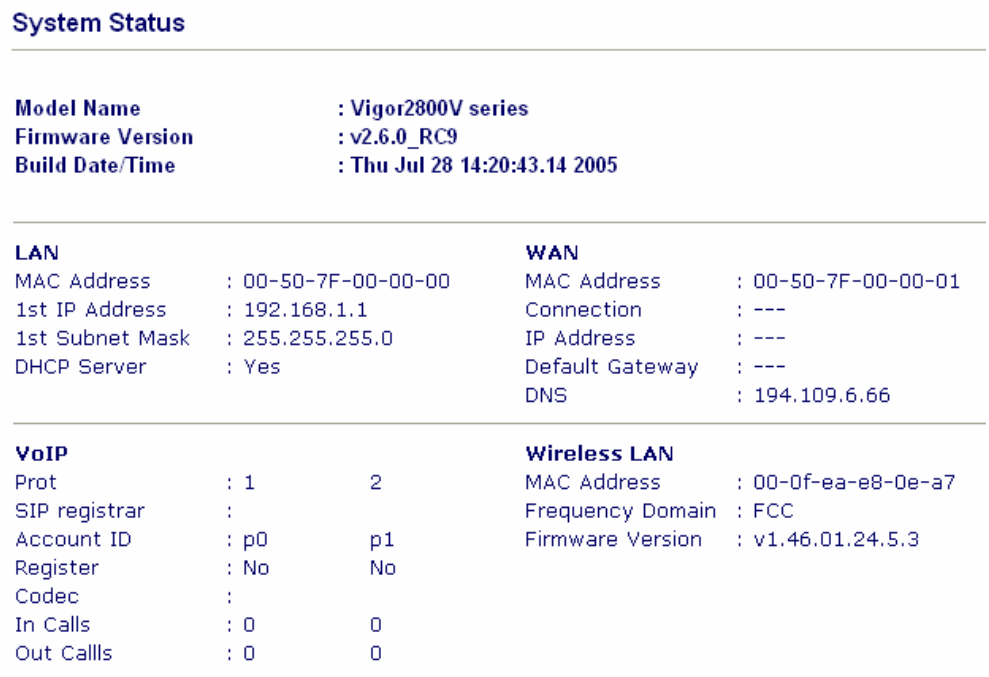
Click **System Maintenance Setup** to open the setup page.



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

11.2.1 System Status

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



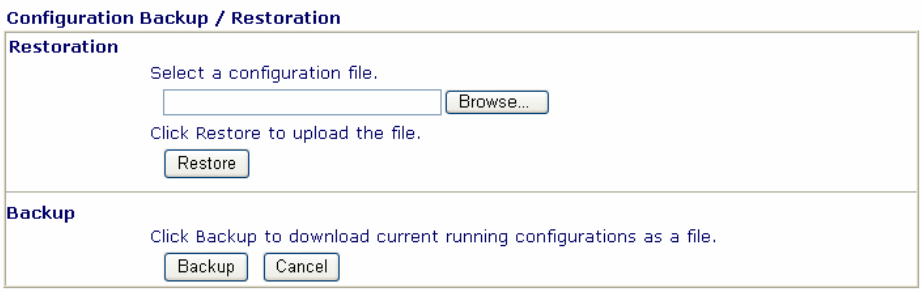
11.2.2 Administrator Password

Here you can reset administrator password.

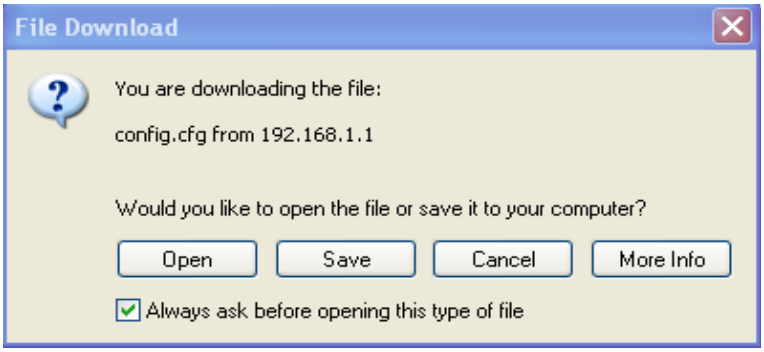
11.2.3 Configuration Backup

Backup the Running Configuration

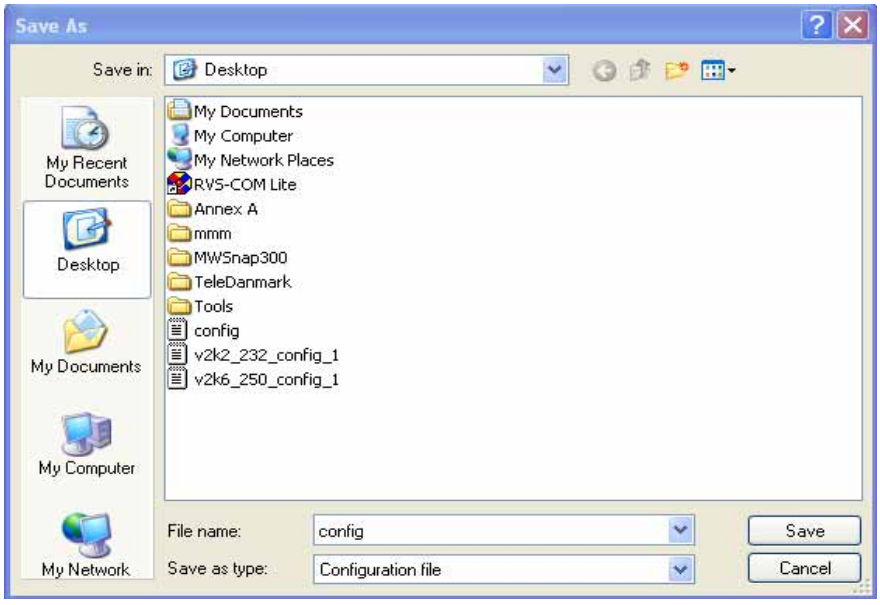
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click Backup button to get configurations.



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

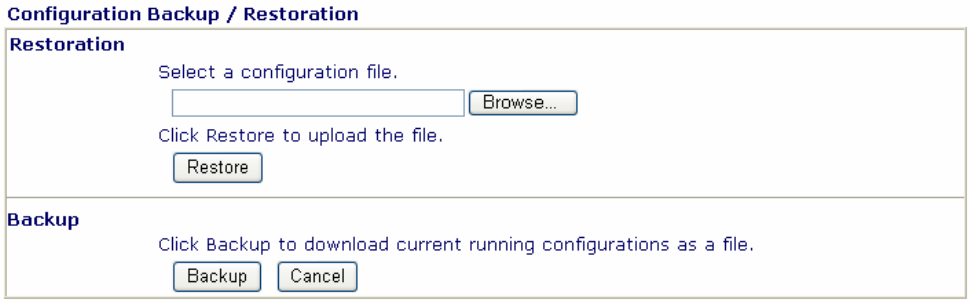


4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

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.



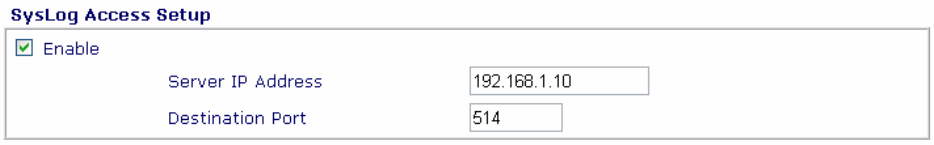
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

11.2.4 SysLog/Mail Alert

SysLog

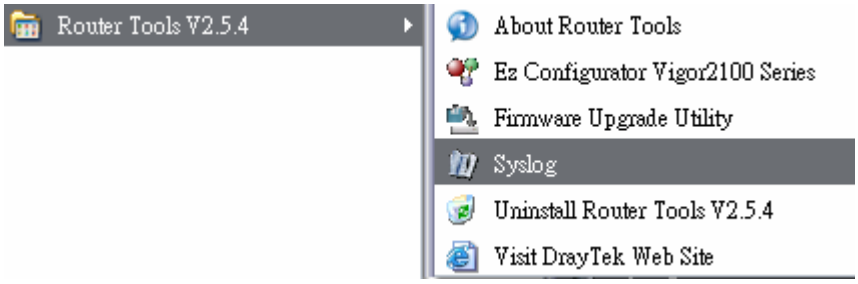
SysLog function is provided to help users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

1. Just set your monitor PC's IP address in this field.

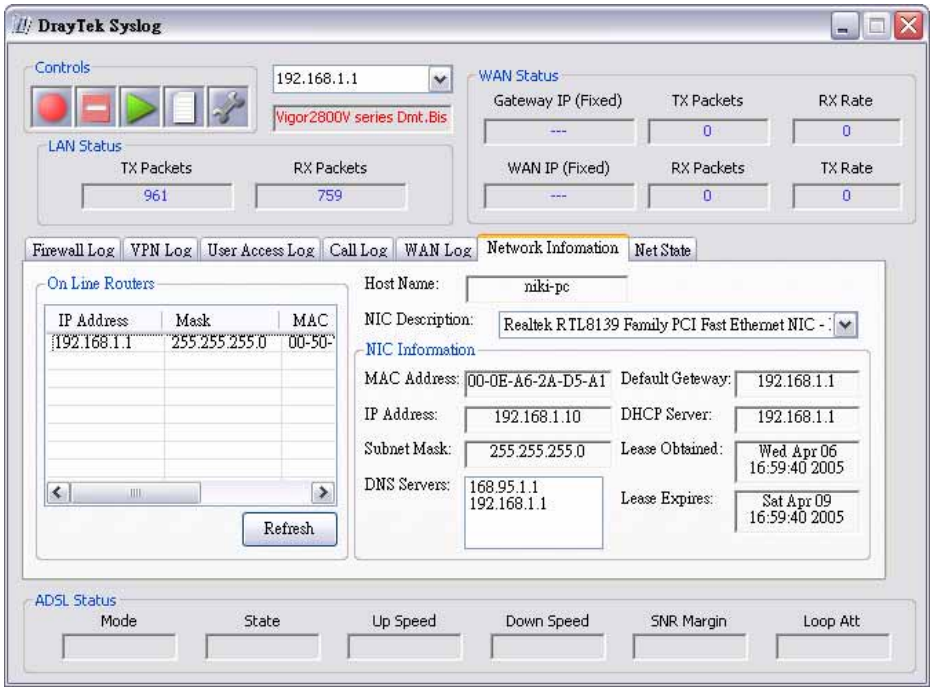


2. Install the Router Tools in the **Utility** within provided CD. In

program menu, click on the **Router Tools>>Syslog**.



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



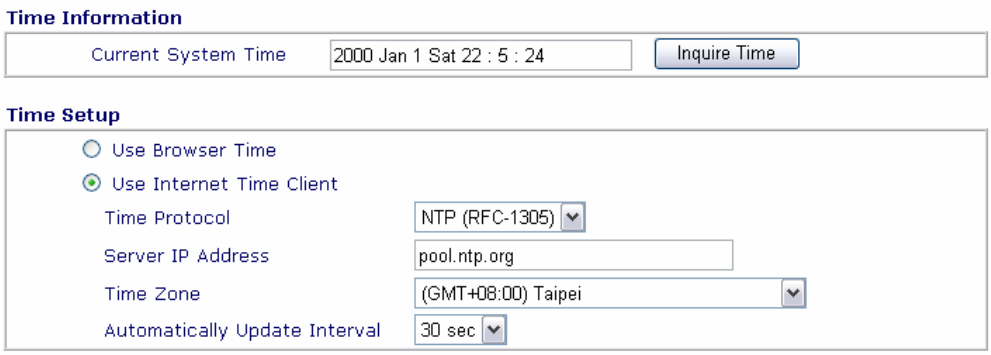
Mail Alert

Mail Alert function is provided to warn when designated events happen.

1. Just set your monitor PC's IP address in this field.

11.2.5 Time Setup

To specify where should the time of the router to be inquired from.



Time Information

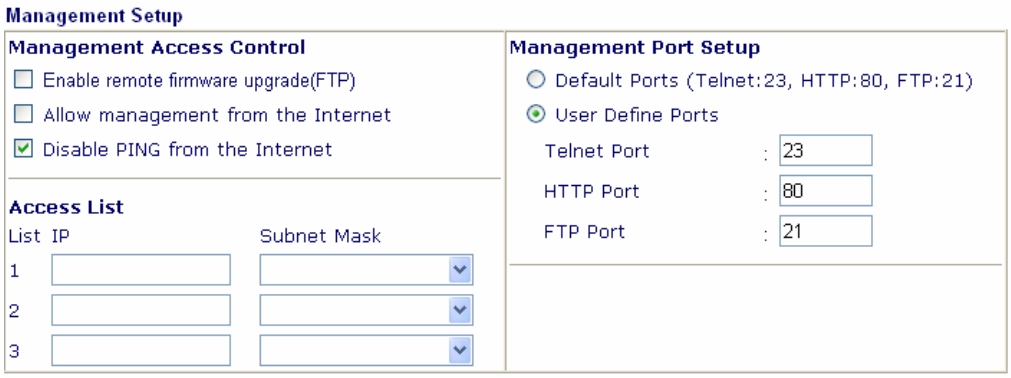
Click on Inquire Time to get the current time.

Time Setup

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

11.2.6 Management

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



Management Setup

The port number used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

Enable remote firmware update	Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.

Access List

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

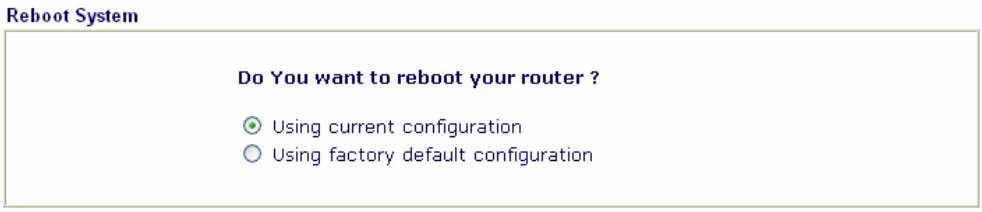
IP	Indicate an IP address allowed to login to the router
Subnet Mask	Represent a subnet mask allowed to login to the router.

Management Port Setup

Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet and HTTP servers.

11.2.7 Reboot System

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



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

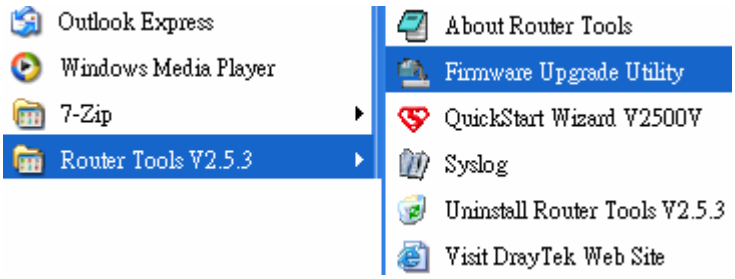
11.2.8 Firmware Upgrade

You can always find the latest firmware from

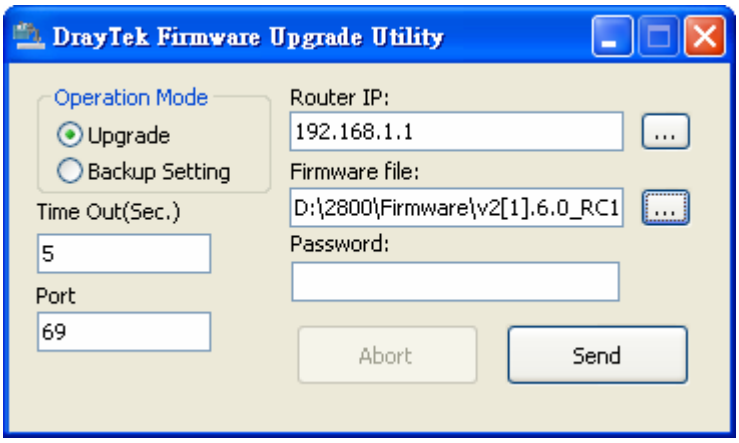
- Web site www.draytek.com (or local DrayTek web site)
- FTP site ftp://ftp.draytek.com

To easily upgrade the firmware of Vigor router, you need to install the Router Tools. It is a complimentary application software included in the product CD-ROM. You can also find it on the DrayTek web site.

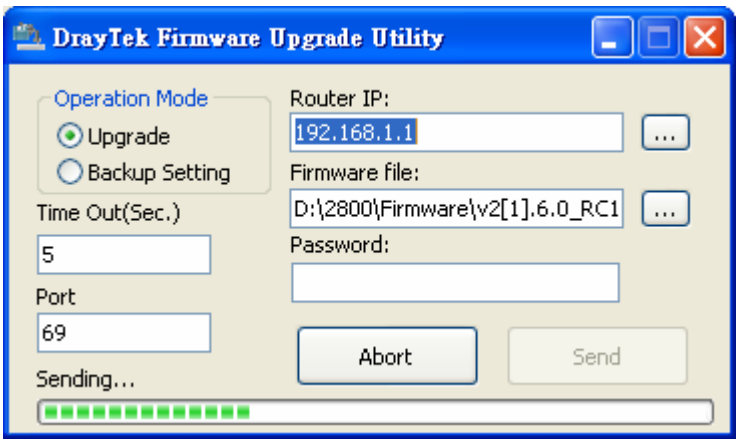
1. Make sure you connect to Vigor router and being able to browse the web GUI.
2. Install the Router Tools and when finished, you should find the below screen in the control panel. (*Windows OS Screen*)



3. Then you will find the pop-up window as shown below. You should fill in the IP address of the router in the field **Router IP**. Click "…" on the right to let the program auto survey any Vigor routers for your selection. Also you have to specify the firmware file location on your PC. The field **Password** should be filled if you have set up password when login your router.



The upgrade action will start and the status will be shown on the progress bar.



Once the upgrade operation has completed, wait approximately 30 seconds and the router will be ready (ACT light in the front panel of your router will resume flashing normally).

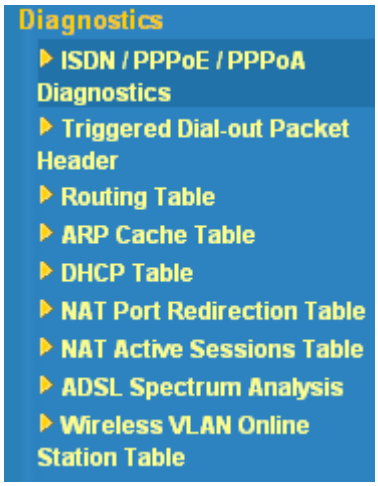
Chapter 12
Diagnostics Setup

12.1 Introduction

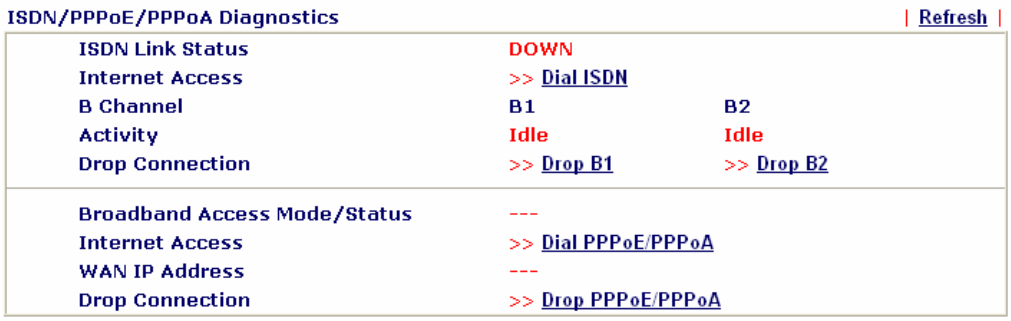
Diagnostic Tools provide a useful way to view or diagnose the status of you Vigor router.

12.2 Settings

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



12.2.1 PPPoE/PPPoA Diagnostics (ISDN is for i models)

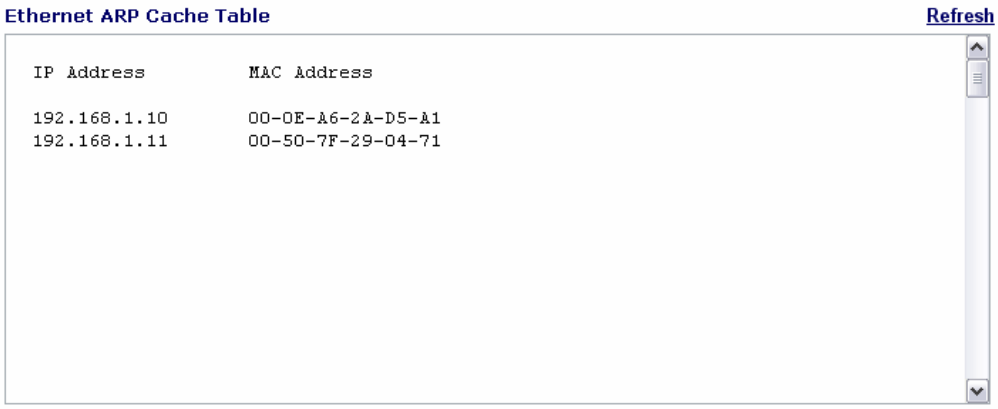


Refresh	To obtain the latest information, click here to reload the page.

Broadband Access Mode/Status	Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show "**---**".
WAN IP Address	The WAN IP address for the active connection.
Dial PPPoE or PPPoA	Click it to force the router to establish a PPPoE or PPPoA connection.
Dial PPPoE or PPPoA	Click it to force the router to establish a PPPoE or PPPoA connection.

12.2.2 ARP Cache Table

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



Refresh: Click it to reload the page.

12.2.3 DHCP Assigned IP Address

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

DHCP IP Assignment Table Refresh

DHCP server: Running

Index	IP Address	MAC Address	Leased Time	HOST ID
1	192.168.1.1	00-50-7F-27-E5-41	ROUTER IP	
2	192.168.1.11	00-50-7F-29-04-71	20:50:19.690	niki-pc