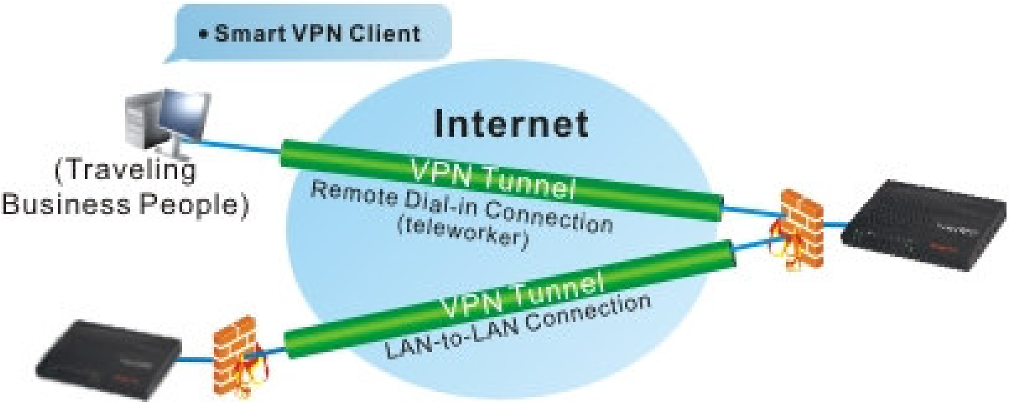
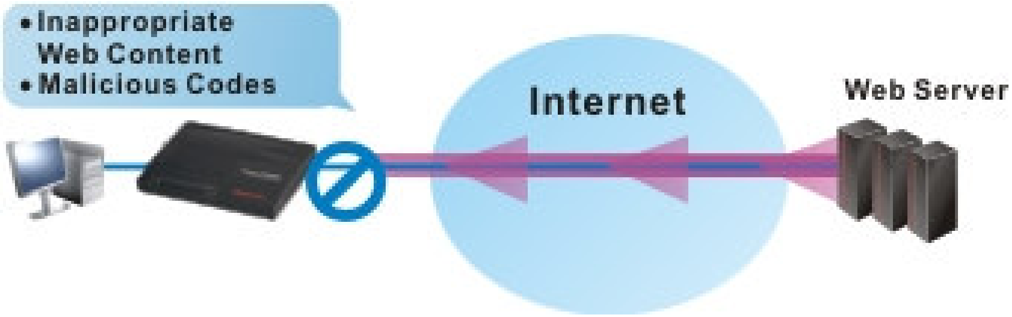
Preamble of Vigor2900 series Broadband Security Router

1. Introduction

- **Firewall contains SPI technique against intrusions, attacks and DOS**
- **VPN encryption enhances transmission privacy and security**
- **QoS optimizes bandwidth for mission-critical traffic**
- **URL content filtering blocks malicious codes and inappropriate webs**
- **High-speed 802.11g implements carefree wireless access**





1.1 Brief Overview

	Vigor2900	Vigor2900G	Vigor2900Gi	Vigor2900i
Security Broadband Router	*	*	*	*
802.11g WLAN AP	-	*	*	-
ISDN Backup	-	-	*	*

The Vigor2900 series router, an Internet access solution for your LAN, which provides you the shared web surfing and countless value-added features, such as Firewall / Security, VPN, USB interface printer server support, and 802.11g Wireless LAN (up to 54Mbps for Vigor2900G/Gi only). These are all in a reliable one-box solution.

1.2 Highlights

Firewall

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

Virtual Private Network (VPN)

- Up to 32 simultaneous VPN tunnels
- Dial-in or dial-out, LAN-to-LAN or Teleworker-to-LAN
- Protocol support for PPTP, IPSec, L2TP, L2TP over IPSec
- AES, MPPE, and hardware- based DES/3DES Encryption
- Authentication support for MD5 and SHA-1
- IKE key management
- Interoperable with other leading 3rd party vendor VPN devices or software

Bandwidth Management facilities

- Class-based bandwidth guarantee by user-defined traffic categories
- Provision of inbound/outbound bandwidth control
- Support of eight priority-levels
- Support of DiffServ-Codepoint marking

WAN

- One 10/100M Base-TX port with a RJ-45 connector
- DHCP client for cable service
- Static IP address assignment for fixed IP networks
- PPPoE/PPTP client for ADSL service

LAN

- 4 port 10/100 Base-TX Ethernet switch with VLAN
- DHCP server for IP assignment (up to 253 users)
- DNS cache and proxy
- NAT (Network Address Translation)
- Virtual server via port redirection or open port
- Port-based rate throttling capability
- Routing support: RIPv2, Static Route

Printer Server

- One USB port connector
- Built-in LPD printer server
- Support for Win98/98SE/ME LPR printer driver
- Compatible with Win2000/XP/MacOS 9/MacOS X built-in LPR printer driver

Wireless Access Point (Vigor2900VG/VGi only)

- 802.11g support (54Mbps data rate)
- Backward compatible with 802.11b device
- Wireless security:
  - .Secure VPN over WLAN
  - .WPA Support
  - .802.1x User Authentication
  - .64/128 bits WEP wireless encryption
  - .Client MAC-address locking
  - .SSID stealth

Flexible URL Content Filtering

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

Application Support

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

Router Management

- Web-based User Interface
- Command line interface (Telnet)
- Telnet remote access support
- SNMP agent with MIB-II
- Built-in diagnostic tools
- Remote firmware upgrade
- Quick Start Wizard
- Syslog Monitoring

ISDN Facilities (Vigor2900Gi/Vigor2900i only)

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

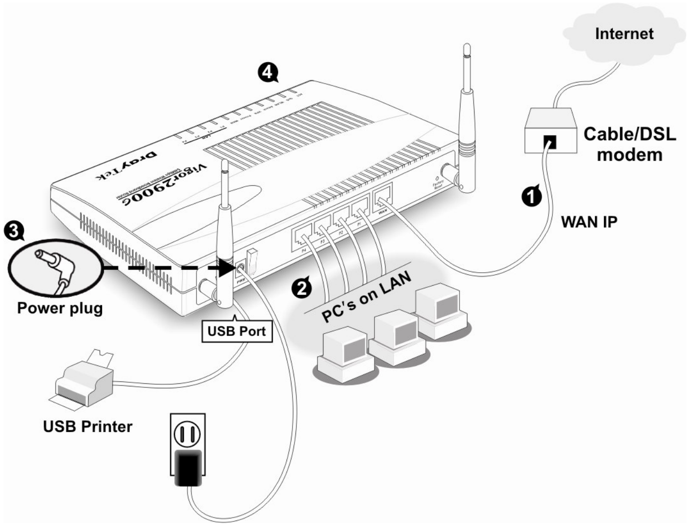
2. Hardware Connection

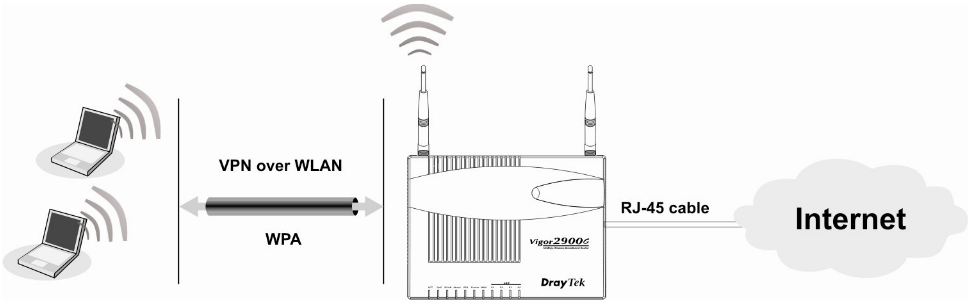
2.1 Hardware Connection

Before starting to configure the router, please ensure to connect your devices correctly.

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

Connection scenario is shown as below:





About This User's Manual

This manual is designed to assist users in using one of the Vigor2900 series of Broadband Security routers. Information in this document has been carefully checked for accuracy and, however, no guarantee is given as to the correctness of the contents. The information contained in this document is subject to change without notice. Should you have any inquiries, please feel free to contact our support via E-mail, Fax or phone. For the latest product information and features, please visit our website at **www.draytek.com**.

Copyright

Trademark

DrayTek Limited Warranty

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

During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or remanufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty.

We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

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

Safety Instructions

- Please read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic device that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range from +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Keep the package out of reach of children.
- When you would like to dispose of the router, please follow the local regulations on conservation of the environment.

European Community Declarations

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

Product: Vigor2900 Series Broadband Security Routers
[Vigor2900,Vigor2900G, Vigor2900Gi and Vigor2900i]

DrayTek Corp. declares that Vigor2900 series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 89/336/EEC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 73/23/EEC by complying with the requirements set forth in EN60950.

The ISDN interface of Vigor2900Gi and Vigor2900i is designed for the Euro-ISDN network throughout the EC-region and where Telcos/ISPs are also adopting Euro-ISDN to their ISDN services.

The Vigor2900G/Gi is designed for the WLAN 2.4GHz network throughput EC region, Switzerland, and the restrictions of France.

Commission (FCC) Interference Statement

The Vigor2900 and Vigor2900G have been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Class B limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is not guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Customer Support

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

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

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

Table of Contents

PART I Basic Setup

CHAPTER 1. Administration Password Setup

CHAPTER 2. LAN TCP/IP and DHCP Setup

CHAPTER 3. ISDN Setup

CHAPTER 4. Wireless LAN Setup

PART II Quick Setup

CHAPTER 5. Internet Access Setup

CHAPTER 6. Virtual TA (Remote CAPI) Setup

PART III Advanced Setup

CHAPTER 7. Dynamic DNS Setup

CHAPTER 8. Call Control and PPP/MP Setup

CHAPTER 9. Call Schedule Setup

CHAPTER 10. NAT Setup

CHAPTER 18. Online Status

CHAPTER 19. VPN Connection Management

CHAPTER 20. Configuration Backup/Restoration

CHAPTER 21. SysLog / Mail Alert Setup

CHAPTER 22. Time Setup

CHAPTER 23. Management Setup

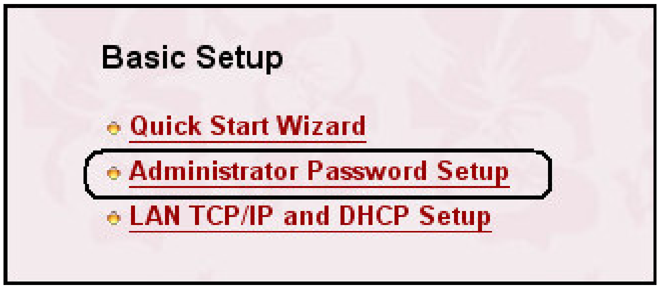
CHAPTER 24. Diagnostic Tools

CHAPTER 25. Reboot System and Firmware Upgrade(TFTP Server)

Chapter 1
Administrator Password Setup

1.1 Introduction

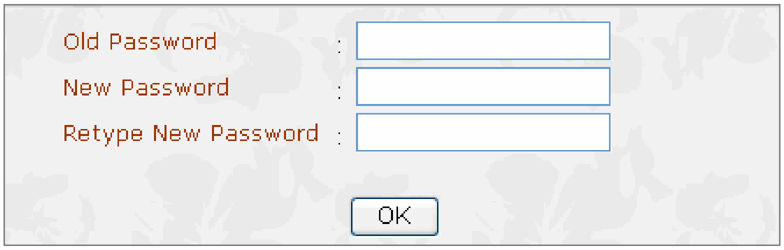
In the **Basic Setup** group, you can change the administrator password, IP configuration of LAN interface, local DHCP server, ISDN and Wireless LAN configuration. In this chapter, we focus on the explanation of the **Administrator Password Setup**



1.2 Changing the Administrator Password

For security reason, we strongly recommend that you should set an administrator password for the router. On the first setup, the router requires no password. If you don’t set a password, the router is free from any user in the local network or the Internet and, obviously, the user can log into the router and change the settings.

Click **Administrator Password Setup**, the following screen will open.



Old Password: Enter a current administrator password. If this is the first time to set a password, leave this field empty.

New Password: Enter a new administrator password.

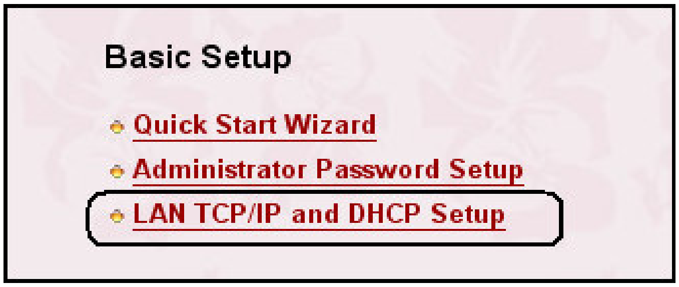
Retype New Password: Type the new password again for confirmation.

Click **OK**.

Chapter 2
LAN TCP/IP and DHCP Setup

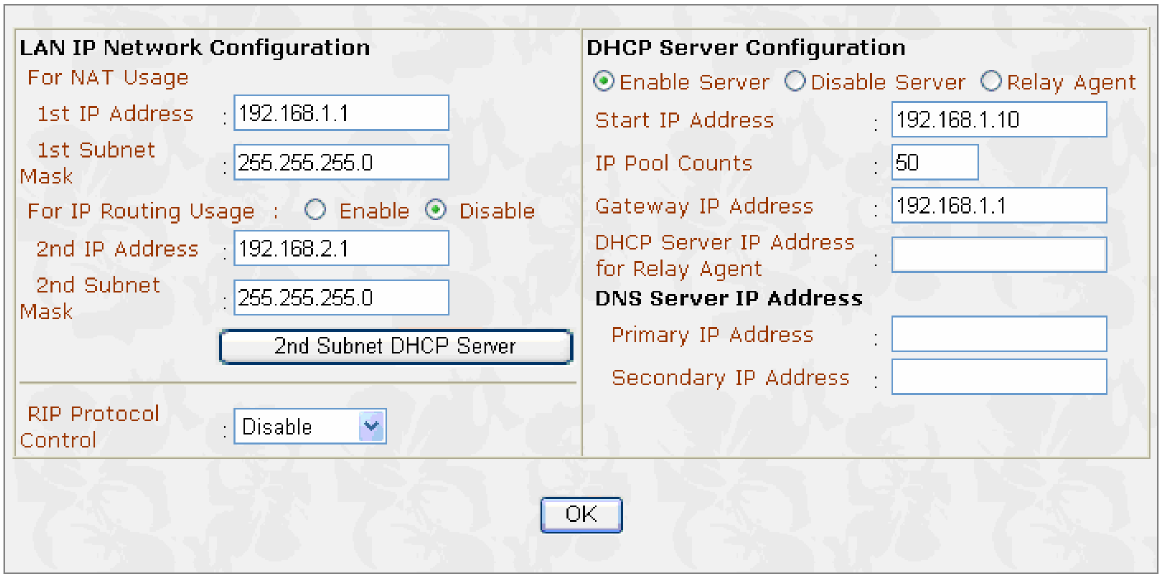
2.1 Introduction

In this chapter, we will explain in detail about the **LAN TCP/IP and DHCP Setup**.



2.2 LAN IP Network Configuration

In the router, there are two sets of IP address settings for the LAN interface, as shown below. The 1st IP address/subnet mask is for private users or NAT users, and the 2nd IP address/subnet mask is for public users. To allow public users, you need to have subscribed to a globally reachable subnet from your ISP. For example, for some DSL accounts, the ISP will assign a few public IP addresses for your local network. You could use one IP address for your router, and the 2nd IP address/subnet mask should be configured with the public IP address. Other local PCs should set the router IP address as the default gateway. When the DSL connection to the ISP has been established, each local PC will directly route to the Internet. Also, you could use the 1st IP address/subnet mask to connect to other private users (PCs). These IP addresses of the users will be translated to the 2nd IP address by the router and sent out via the DSL connection.



LAN IP Network Configuration

For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage : ○ Enable ● Disable

2nd IP Address : 192.168.2.1

2nd Subnet Mask : 255.255.255.0

RIP Protocol Control : Disable

DHCP Server Configuration

● Enable Server ○ Disable Server ○ Relay Agent

Start IP Address : 192.168.1.10

IP Pool Counts : 50

Gateway IP Address : 192.168.1.1

DHCP Server IP Address for Relay Agent :

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

For NAT Usage: (Default: Always Enable)

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

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

For IP Routing Usage: (Default: Disable)

Enable: Enable the 2nd IP address settings.

Disable: Disable the 2nd IP address settings.

2nd IP Address: Set a public IP address.

2nd Subnet Mask: Set a netmask for the public IP address.

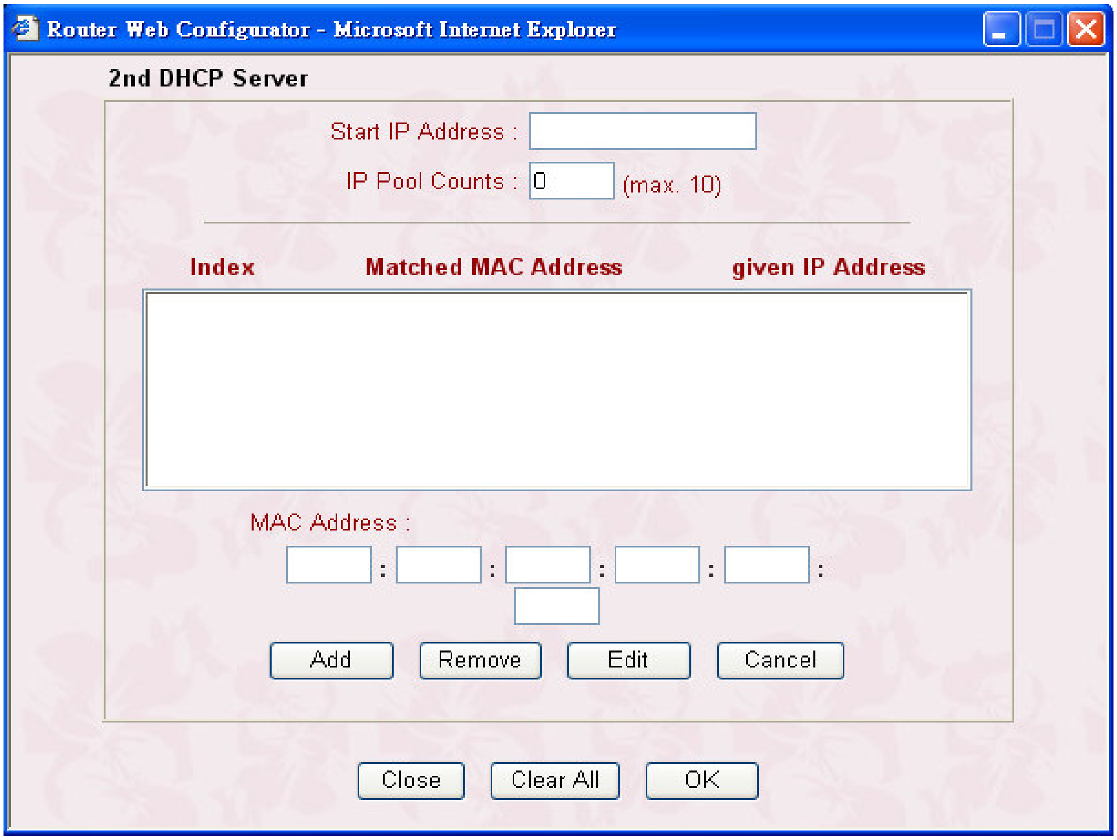
RIP Protocol Control:

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

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

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

2nd Subnet DHCP Server: The following picture is for 2nd subnet DHCP server of the router.



IP Pool Counts : 0

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

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

MAC Address: Type the specific MAC Address which could be added, removed or edited from the access listed above.

ADD: To add a MAC address on the list.

Remove: To delete the selected MAC address on the list.

Edit: To edit the selected MAC address on the list.

Cancel: Give up the MAC address access control setup.

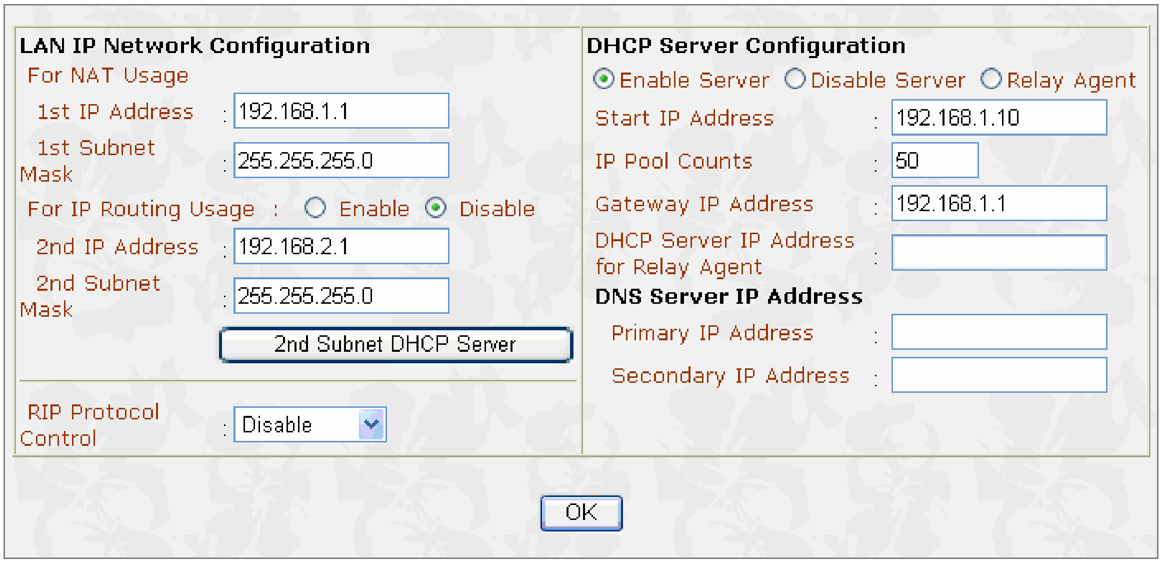
Close: Close this window.

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

OK: Save the access control list.

2.3 DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. It can automatically dispatch related IP settings to any local user configured as a DHCP client. Please refer to the following picture for DHCP Server Configuration.



LAN IP Network Configuration

For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage : ○ Enable ● Disable

2nd IP Address : 192.168.2.1

2nd Subnet Mask : 255.255.255.0

RIP Protocol Control : Disable

DHCP Server Configuration

● Enable Server ○ Disable Server ○ Relay Agent

Start IP Address : 192.168.1.10

IP Pool Counts : 50

Gateway IP Address : 192.168.1.1

DHCP Server IP Address for Relay Agent :

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

Enable Server: Assign IP address to LAN PC automatically.

Disable Server: Assign IP address to LAN PC manually.

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

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

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

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

DNS Server IP Address: (Default: None).

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: Sets the IP address of the primary DNS server.

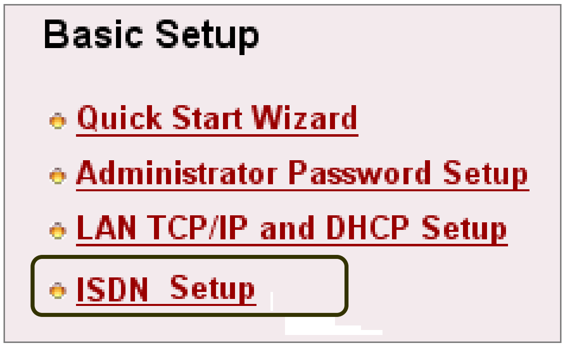
Secondary IP Address: Sets the IP address of the secondary DNS server.

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

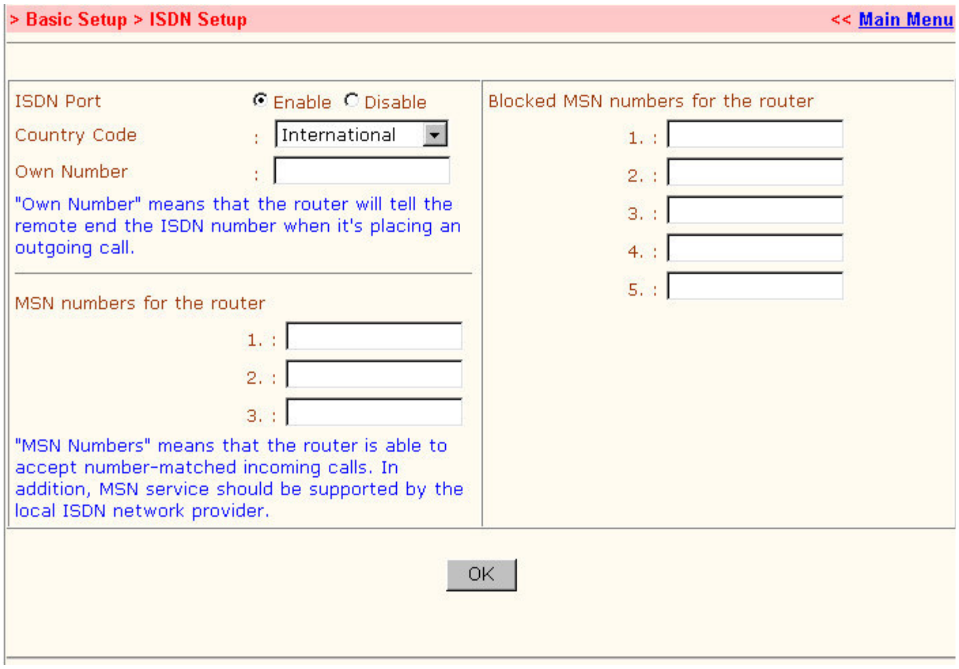
Chapter 3
ISDN Setup

3.1 Introduction

In this chapter, we focus on the explanation of the **ISDN Setup.** The following content is suitable for **Vior2900Gi/Vigor2900i** only.



3.2 Configuring the ISDN Interface



ISDN Port ● Enable ○ Disable
Country Code : International
Own Number :

"Own Number" means that the router will tell the remote end the ISDN number when it's placing an outgoing call.

MSN numbers for the router
1. :
2. :
3. :

"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.

Blocked MSN numbers for the router
1. :
2. :
3. :
4. :
5. :

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

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

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

Blocked MSN Numbers for the router: Sets the specified MSN number into the appropriate boxes in order to prevent the router from dialing to the specified MSN number

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

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

The ISDN interface on Vigor2900Gi and Vigor2900i supports the **VTA** (**Virtual Terminal Adapter**) facility. The VTA offers a “CAPI” software interface, similar to that which an actual ISDN terminal adapter installed on your PC. You can install CAPI-compliant software for dial-up networking, fax or voice activities – relying on the capabilities of your adopted CAPI software. To use the VTA facility, please download VTA drivers (available only for Windows 98SE/2000/XP) from http://www.draytek.com/english/support/download.php .

Chapter 4
Wireless LAN Setup

4.1 Introduction

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the face of the earth. Hundreds of millions of people exchange information every day using wireless communication products. Therefore, the Vigor2900G and Vigor2900Gi security routers are designed for increasing flexibility and efficiency of a small office/a home by deploying the WLAN network.

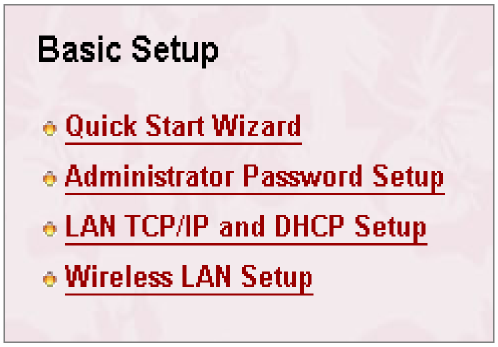
To elaborate one example, any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable.

One more example, parents can write E-mail at their studyoom and kids are also able to surf Internet at their bedrooms as the Vigor2900G is set up in some corner of a home. Parents do not need to drill any hole for installing LAN cable everywhere in the house.

The Vigor2900G and Vigor2900Gi are equipped with a wireless LAN interface compliant with the IEEE 802.11g protocol supporting data rate of 54Mbps. The wireless LAN capability enables high mobility of several users so that they can simultaneously access all LAN facilities just like on a wired LAN as well as Internet and WAN access.

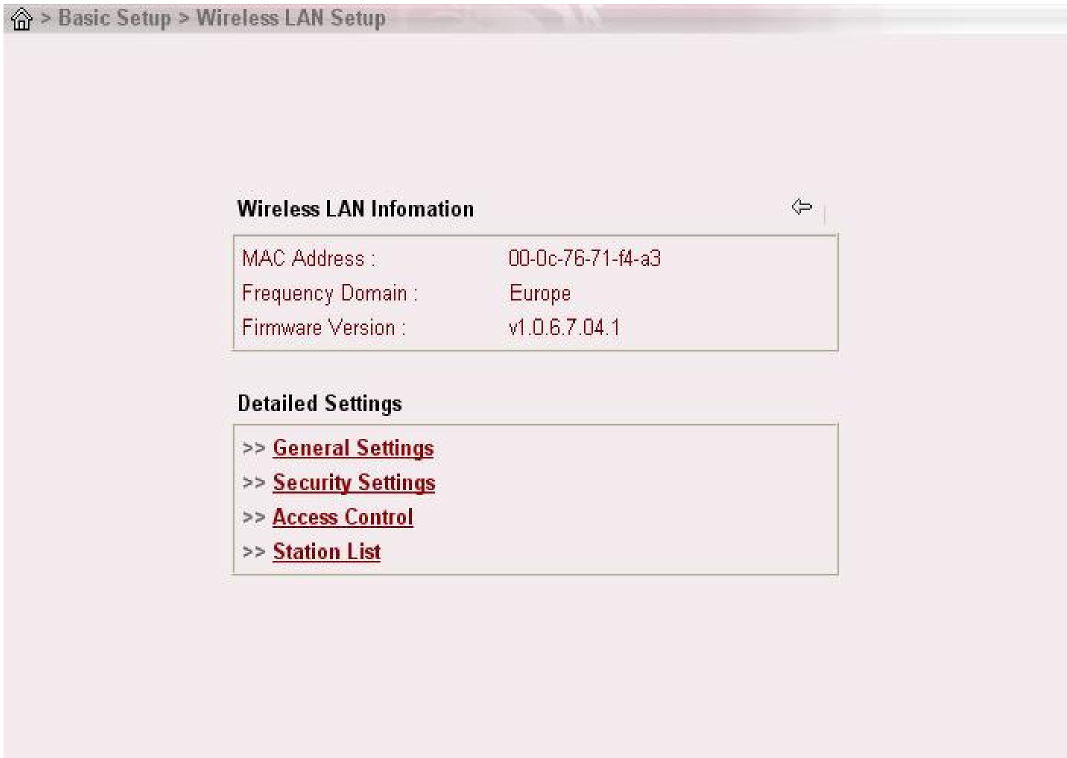
In this chapter, we explain the capabilities of the wireless LAN and its associated web configurations. Use the following setup path on the Setup Main Menu to configure the wireless LAN function.

Basic Setup > Wireless LAN Setup



4.2 Configuration

After clicking the "**Wireless LAN Setup**", you will see the following web page.



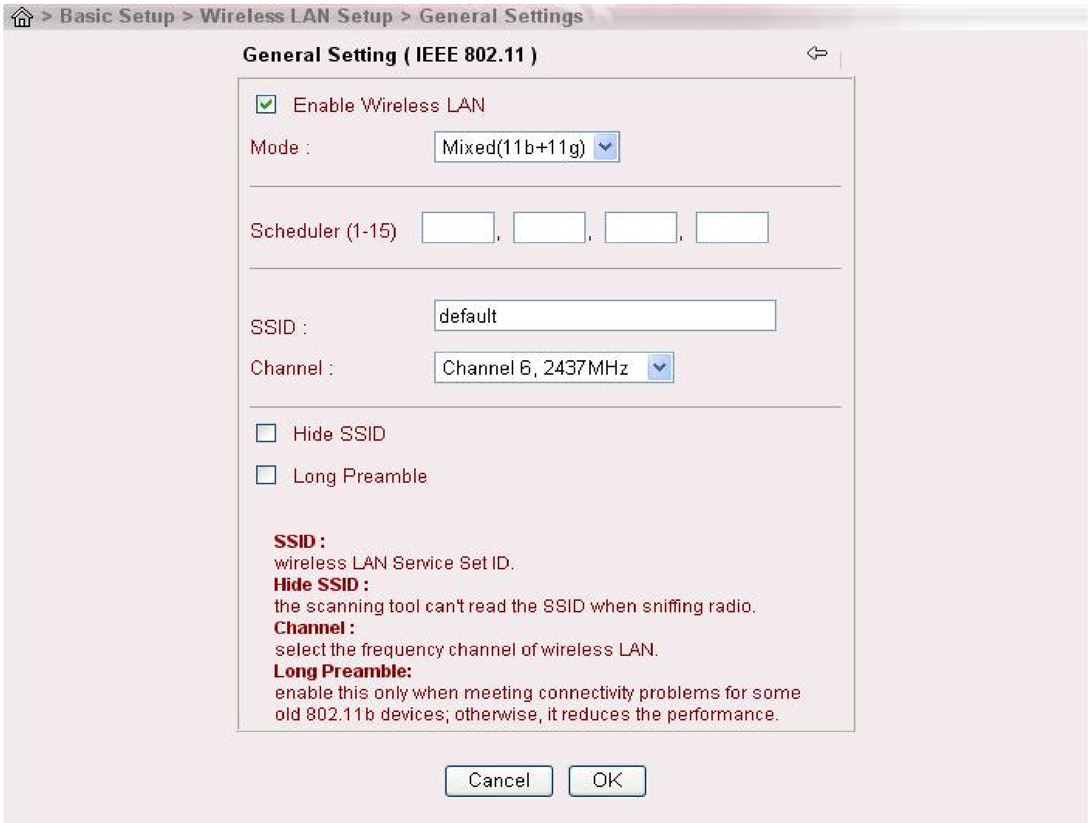
Wireless LAN Infomation

MAC Address : 00-0c-76-71-f4-a3
Frequency Domain : Europe
Firmware Version : v1.0.6.7.04.1

Detailed Settings

This web page will show the wireless LAN information including *MAC address* and *Frequency domain* and provide the **Detailed Setting** for advanced setting. For example, in this figure, the *Frequency Domain* is set as Europe and the *MAC address* is set as 00-60-b3-14-d1-e8. The **Detailed Settings** consists of **General Settings**, **WEP Settings**, and **Access Control**.

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



General Setting (IEEE 802.11)

☑ Enable Wireless LAN

Mode : Mixed(11b+11g)

Scheduler (1-15) ☐ , ☐ , ☐ , ☐

SSID : default

Channel : Channel 6, 2437MHz

☐ Hide SSID

☐ Long Preamble

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

Enable Wireless LAN: Click it to enable the wireless access activity for the wireless device.

Scheduler: You can set the wireless device to work at some time interval only. Four time internals are available for you to choose. The default setting is always active without any time limitation. The schedule can be specified through **Advanced Setup > Call Schedule Setup.**

SSID: SSID stands for Service Set Identification. You should set the SSID to be one that the wireless card in your notebook/desktop allows the client hosts to access the network via the wireless LAN interface. By default, the SSID is ***default*.**

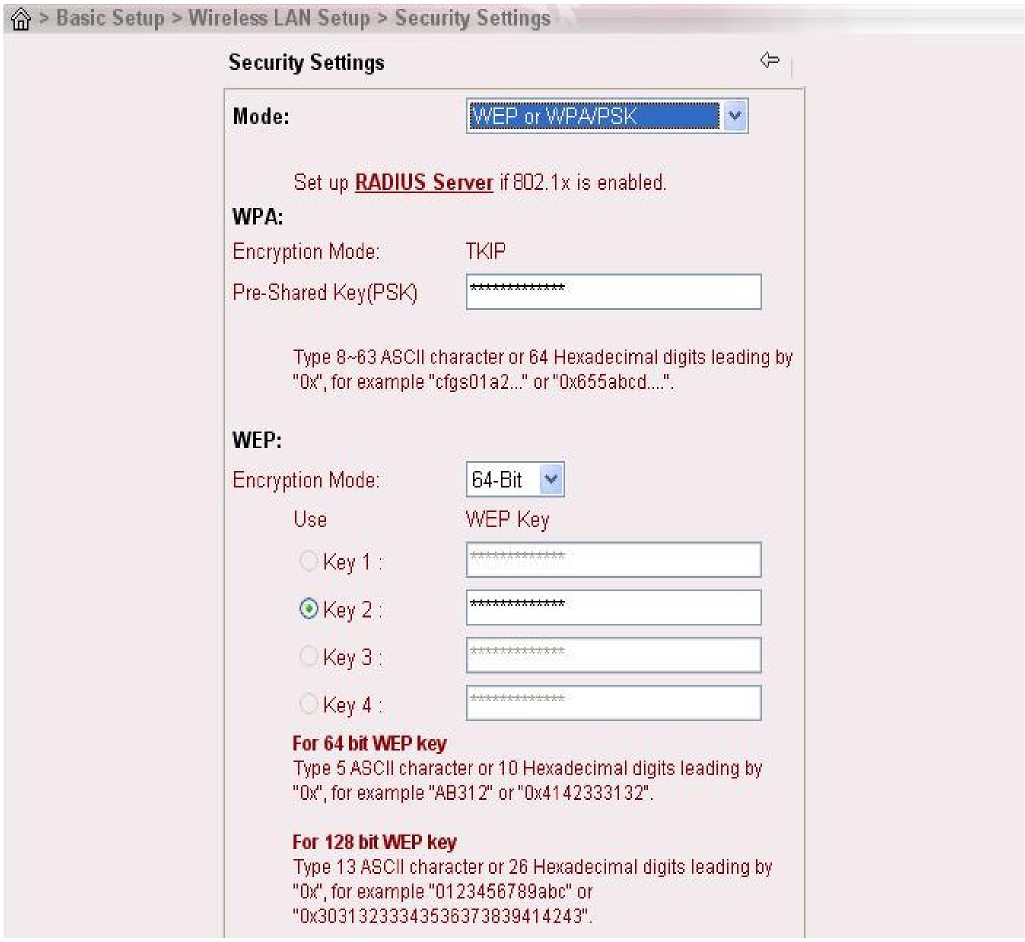
Channel: Select an adequate wireless channel the router. The default channel is 6.

Hide SSID: This term is used to increase the security level. Check it to hide SSID information against the wireless clients that are sniffing radio. By default, this option is inactive.

Long Preamble：This term is used to overcome the wireless connectivity problem for some older 802.11b station.

4.3 Configuring the WEP Security

To improve the security and privacy of your wireless data packets, the WEP and WPA encryption feature can be employed, where WEP stands for Wireless Equivalent Privacy. The WEP facility that uses a set of four *default keys* encrypts each frame transmitted from the radio using only one of the given keys. Default keys are shared between the Vigor wireless router and WEP station in a service set. Once a station has obtained the default keys for its service set, it may communicate using WEP. WPA (Wi-Fi Protected Access) uses the Temporal Key Integrity Protocol (TKIP) for encryption and employs 802.1X authentication. It greatly enhances the over-the-air data protection and access control on existing Wi-Fi networks. It addresses the weaknesses of WEP. By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.



Mode: WEP or WPA/PSK

Set up RADIUS Server if 802.1x is enabled.

WPA:

Encryption Mode: TKIP

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

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

WEP:

Encryption Mode: 64-Bit

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

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

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

Mode：To improve the security and privacy of your wireless data packets, one of the following encryption features can be used.

-Disable：Turn off the encryption mechanism.

-WEP Only：Only allow the access from WEP clients and the encryption key is given from WEP Keys.

-WEP/802.1x Only：Only allow the access from WEP clients and the encryption key is given dynamically through 802.1x.

-WEP or WPA/PSK：Allow the access from WEP and WPA clients simultaneously and the encryption keys are given from WEP Keys and PSK respectively.

-WEP/802.1x or WPA/802.1x：Allow the access from WEP and WPA clients simultaneously and the encryption keys are given dynamically through 802.1x.

-WPA/PSK Only：Only allow the access from WPA clients and the encryption key is given from PSK.

-WPA/802.1x Only：Only accept the access from WPA clients and the encryption key is given dynamically through 802.1x.

NOTE： You should also set RADIUS Server if **WEP/802.1x or WPA/802.1x** , **WEP/802.1x Only** or **WPA/802.1x Only** mode is selected.

WPA Encryption：The WPA encrypts each frame transmitted from the radio using the pre-shared key (PSK) entered from this panel or a key is given dynamically through 802.1x.

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

WEP Encryption：

- **Disable**：Turns off the WEP encryption mechanism.
- **WEP 64 Bit**：For 64bits WEP key, either 5 ASCII characters or 10 hexadecimal digitals leading by **0x** can be entered. For example, **ABCDE** or **0x4142434445.**
- **WEP 128 Bit**：For 128bits 13 ASCII characters or 26 hexadecimal digits leading by **0x** can be entered. For example, **ABCDEFGHIJKLM** or **0x4142434445464748494A4B4C4D.**

128 bits WEP is most secure, but has more encryption/decryption overhead.
Note that all wireless devices must support the same WEP encryption bit size and have the same key.

Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Choose one key from key 1 to key 4.

Click **OK,** the **Security Settings** is saved.

4.4 Configuring the Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address which has been configured can access the wireless LAN interface. By clicking the **Access Control** in the **Detailed Settings** group, 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: To check the **Enable Access Control** to enable the MAC Address access control feature.

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

ADD: Add a new MAC address into the list.

Remove: Delete the selected MAC address in the list.

Edit: Edit the selected MAC address in the list.

Cancel: Give up the access control set up.

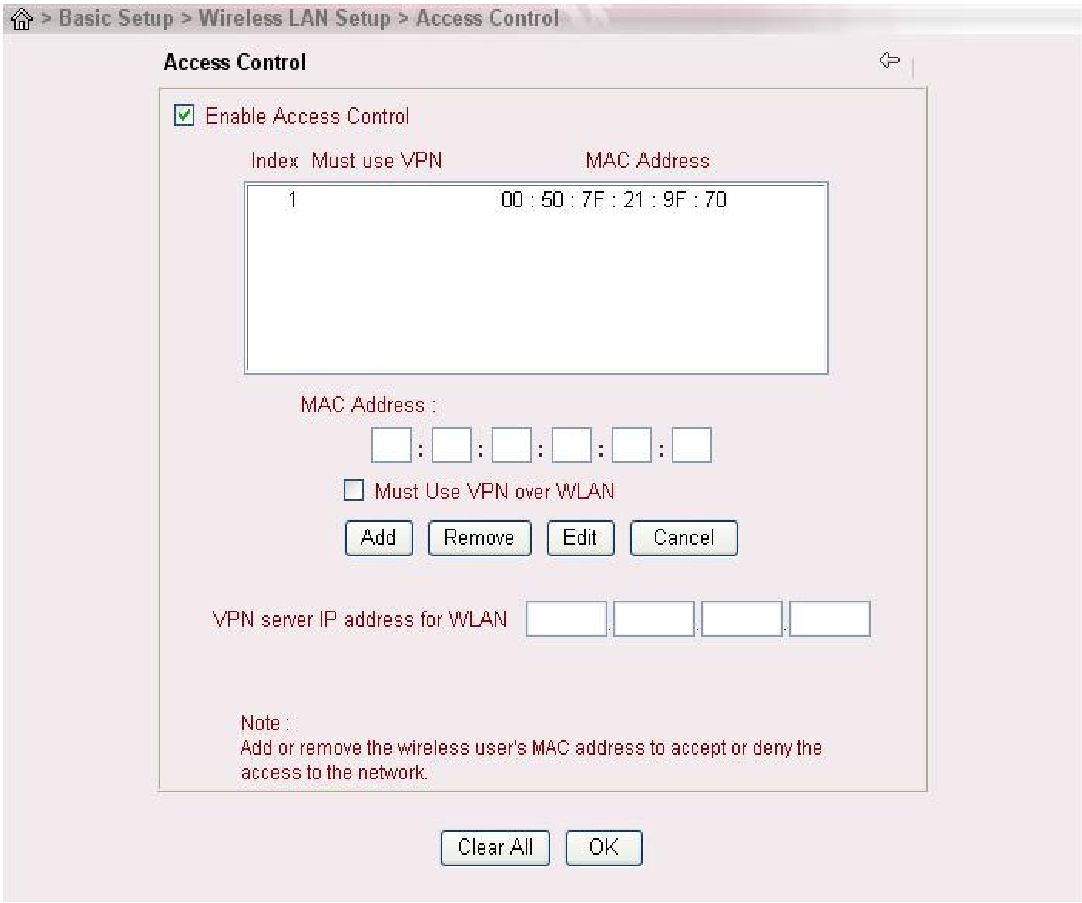
Clean All： Clean all entries in the MAC address list.

OK： Click it to save the access control list.

VPN over WLAN

The Vigor offers PPTP/L2TP/L2TP over IPSec VPN protocols over Wireless LAN. Assume that the wireless clients which are assigned IP address by DHCP are connected to Vigor wireless router through a protected and reliable type of VPN tunnels. For example, you can use 40-bit WEP as a further safe enhancement. i.e., WEP plus VPN. The detailed scenarios are explained in Tips section in the attached CD.

Note: You are recommended to apply the **L2TP** or the **L2TP with IPSec** Policy **to WLAN network** as their security level is higher than that of **PPTP**.

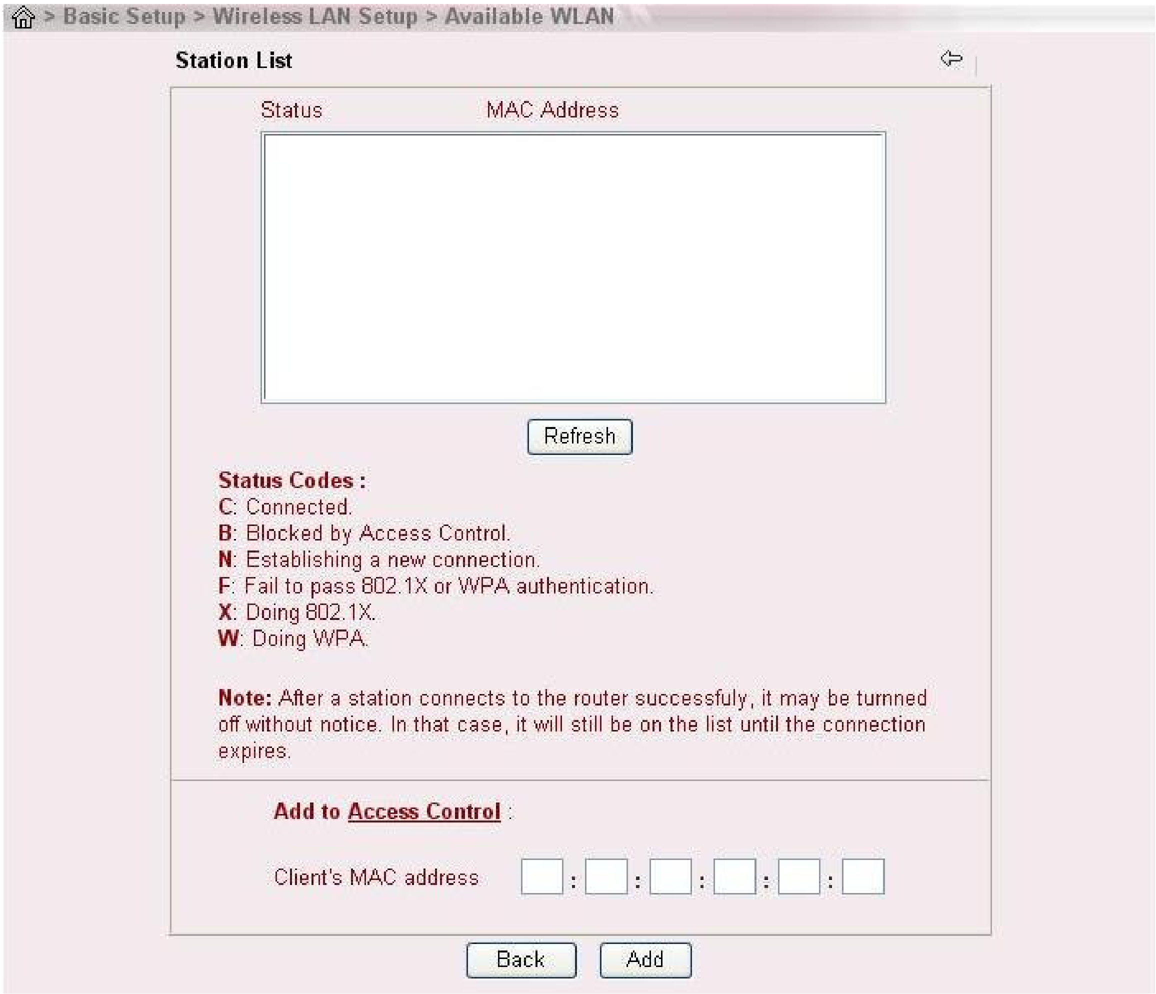


1 00 : 50 : 7F : 21 : 9F : 70

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

4.5 Configuring the Station List

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



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

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

Add to Access Control :

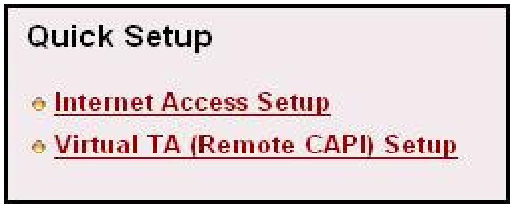
Client's MAC address ☐ : ☐ : ☐ : ☐ : ☐ : ☐

Chapter 5
Internet Access Setup

5.1 Introduction

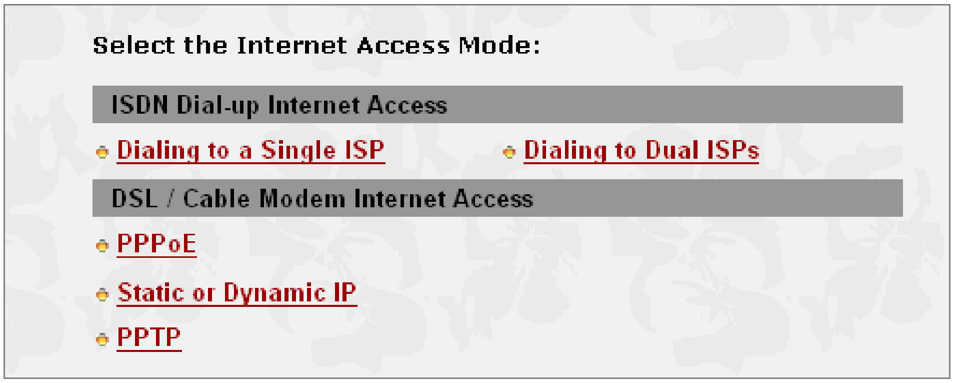
In the **Quick Setup** group, you can configure the router to access the Internet with different modes, for instance, ISDN, PPPoE, PPTP, Dynamic/Static IP or Broadband Access with ISDN dial backup. Notice that the modes of ISN and Broadband Access with ISDN dial backup are only available for Vigor routers having the ISDN interface (e.g. Vigor2900VGi). Use the following setup link on the Setup Main Menu to configure the Internet Access Setup.

Quick Setup > Internet Access Setup



For most users, Internet access is the primary application. The router supports the Ethernet WAN interface for Internet access. The following sections will explain more details of various broadband access setup. When you click **Internet Access Setup** within the **Quick Setup** group, the following setup page will appear.

Five modes are available for Internet Access, that is, Dialing to a Single ISP, Dialing to Dual ISPs, PPPoE, PPTP, and Static/Dynamic IP.


Select the Internet Access Mode:
ISDN Dial-up Internet Access
Dialing to a Single ISP
Dialing to Dual ISPs
DSL / Cable Modem Internet Access
PPPoE
Static or Dynamic IP
PPTP

Dialing to a Single ISP: If you access the Internet via a single ISP, click here.

Dialing to Dual ISPs: If you have more than one ISP, click here to set two ISP dialup profiles. 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 line to 128kbps data speed.

PPPoE: This is used for most DSL modem users. All local users can share one PPPoE connection to access the Internet.

Static or Dynamic IP: On this page you are able to configure the WAN interface by using a static (fixed) IP or dynamic (DHCP client) IP address. Most cable users will use the dynamic IP address mode to get a globally reachable IP address from the cable head-end system. Before you connect a broadband access device, e.g. a DSL/Cable modem, to the router, you need to know what kind of Internet access is provided by your ISP.

PPTP: Some DSL service providers supply a special DSL modem (e.g. Alcatel's DSL modem). This kind of modem only supports the PPTP tunnel to access the Internet. In these cases, you should create a PPTP tunnel that carries a PPP session and terminates on the DSL modem. Once the tunnel has been established, this kind of DSL modem will forward the PPP session to the ISP. As long as the PPP session is connected, all the local users will be able to share this PPP session to access to the Internet.

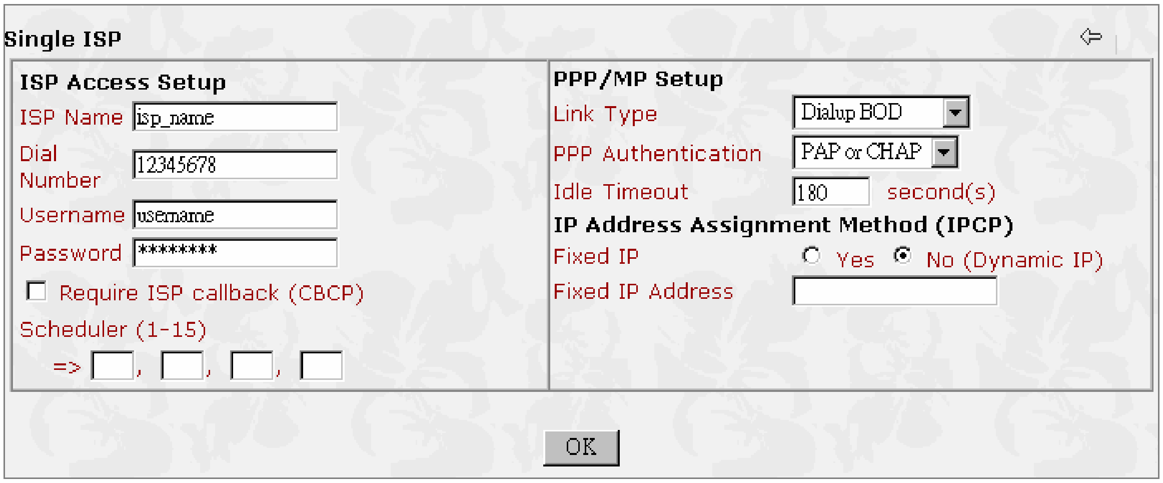
For ISDN Internet users, you should click **Dialing to a Single ISP** or **Dialing to Dual ISPs** for detailed Internet settings.

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

The following sections deal with four widely-used broadband access services. They are **PPPoE Client, PPTP Client, Static IP** for DSL, and **Dynamic IP (DHCP Client)** for Cable. In most cases, you will get a DSL or Cable modem from the broadband access service provider. The router is connected behind the broadband device (i.e. DSL/Cable modem) and works as a NAT or IP router for broadband connections.

5.2 Configuration

5.2.1 Connecting to a Single ISP



Single ISP

ISP Access Setup
ISP Name: isp_name
Dial Number: 12345678
Username: username
Password: ********
☐ Require ISP callback (CBCP)
Scheduler (1-15)
=> ☐, ☐, ☐, ☐

PPP/MP Setup
Link Type: Dialup BOD
PPP Authentication: PAP or CHAP
Idle Timeout: 180 second(s)
IP Address Assignment Method (IPCP)
Fixed IP: ○ Yes ● No (Dynamic IP)
Fixed IP Address:

ISP Access Setup

ISP Name**:** Enter your ISP name.

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

Username**:** Enter the username provided by your ISP.

Password**:** Enter the password provided by your ISP.

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

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

PPP/MP Setup

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

Link Disable: Disable the ISDN dial-out function.

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

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

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

PPP Authentication**:**

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

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

Idle Timeout**:**

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

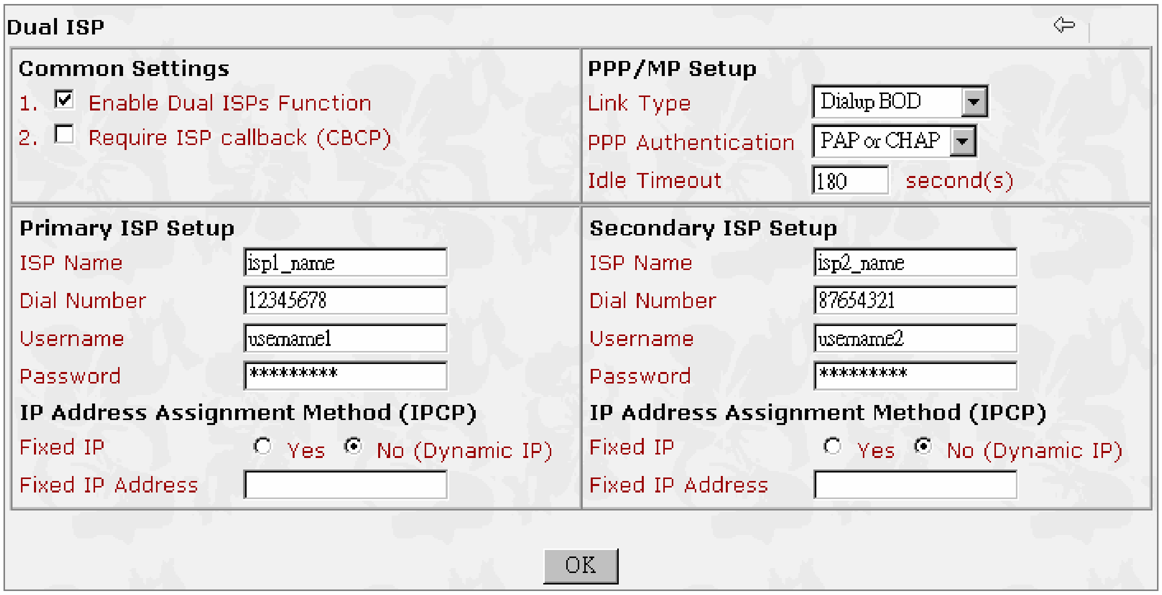
ISDN connection will remain always connected to the ISP.

<u>IP Address Assignment Method (IPCP)</u>

***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.

5.2.2 Connecting to Dual ISPs



Dual ISP

Common Settings

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

PPP/MP Setup

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

Primary ISP Setup

ISP Name: isp1_name
Dial Number: 12345678
Username: username1
Password: *********

IP Address Assignment Method (IPCP)

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

Secondary ISP Setup

ISP Name: isp2_name
Dial Number: 87654321
Username: username2
Password: *********

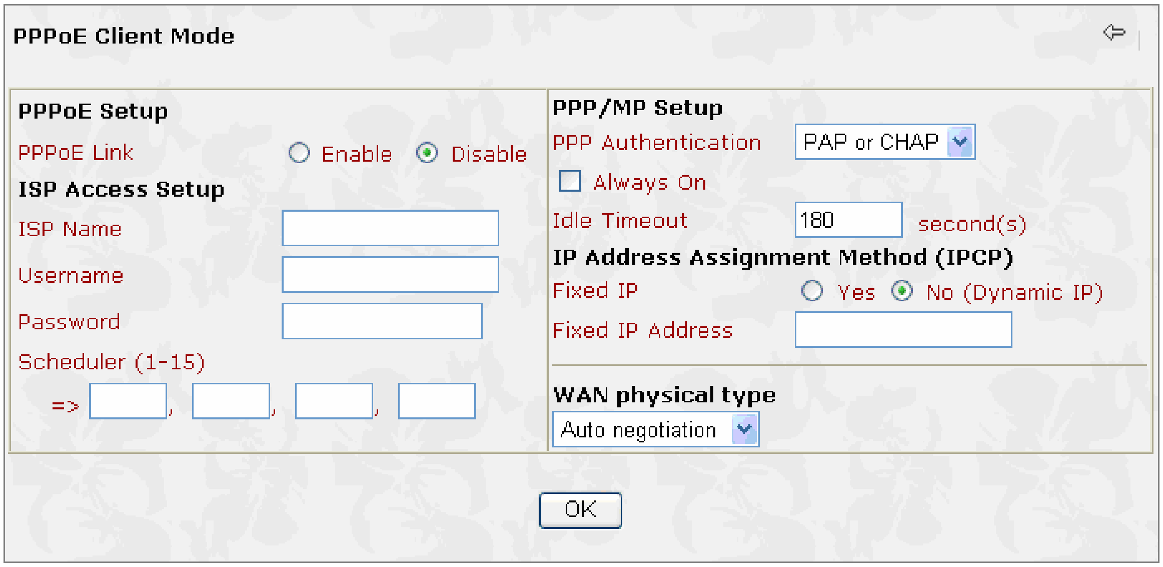
IP Address Assignment Method (IPCP)

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

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

5.2.3 Using PPPoE with a DSL Modem

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



PPPoE Client Mode

PPPoE Setup

PPPoE Link ○ Enable ● Disable

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

PPP/MP Setup

PPP Authentication: PAP or CHAP

☐ Always On

Idle Timeout: 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

WAN physical type: Auto negotiation

PPPoE Setup

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

ISP Access Setup

ISP Name**:** Enter the ISP name.

Username**:** Enter the ISP supplied username.

Password**:** Enter the ISP supplied password.

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

PPP/MP Setup

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

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

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

IP Address Assignment Method (IPCP)

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

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

Click **OK**.

5.2.4 Using PPTP with a DSL Modem

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

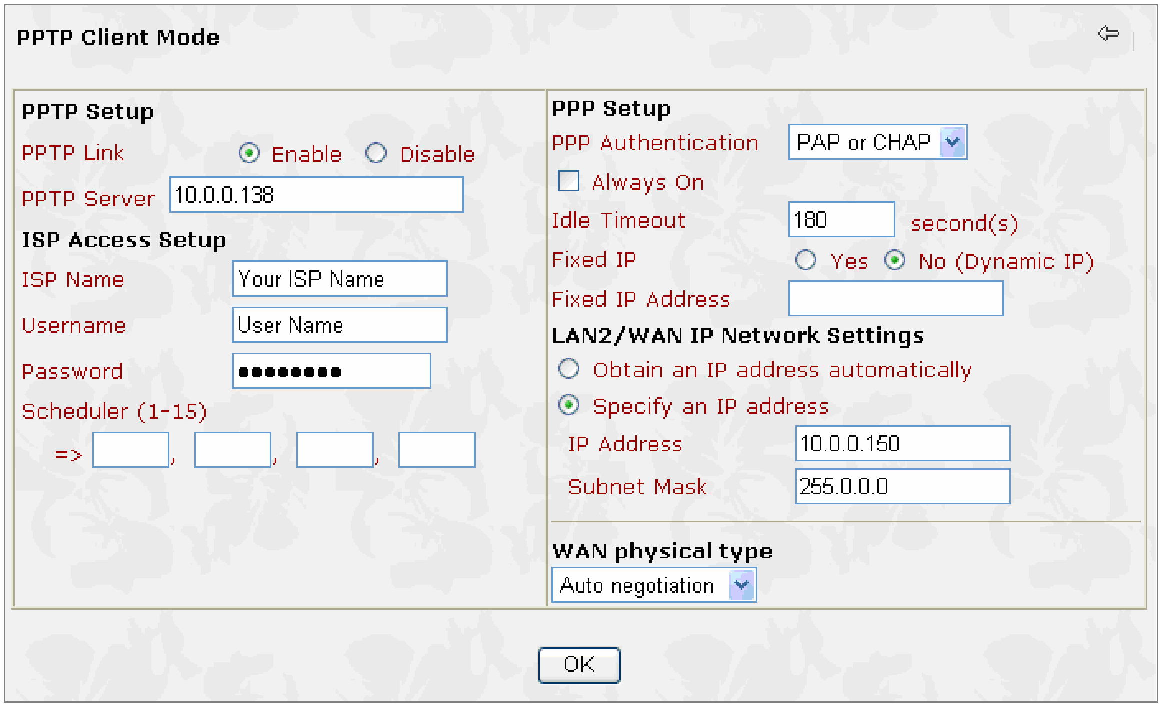
PPTP Setup

PPTP Link**:** Check **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.

PPTP Server IP Address**:** Specify the IP address of the PPTP-enabled DSL modem. Refer to the user manual of the PPTP-enabled DSL modem.

ISP Access Setup

ISP Name**:** Enter the ISP name.



PPTP Client Mode

PPTP Setup

PPTP Link ● Enable ○ Disable

PPTP Server: 10.0.0.138

ISP Access Setup

ISP Name: Your ISP Name

Username: User Name

Password: ●●●●●●●●●

Scheduler (1-15)

=> ___ , ___ , ___ , ___

PPP Setup

PPP Authentication: PAP or CHAP

☐ Always On

Idle Timeout: 180 second(s)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address:

LAN2/WAN IP Network Settings

○ Obtain an IP address automatically

● Specify an IP address

IP Address: 10.0.0.150

Subnet Mask: 255.0.0.0

WAN physical type

Auto negotiation

Username: Enter the ISP supplied username.

Password: Enter the ISP supplied password.

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

PPP/MP Setup

PPP Authentication: Select PAP or CHAP for widest compatibility.

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

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

IP Address Assignment Method (IPCP)

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

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

WAN IP Network Settings

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

Specify an IP address: If you are not sure whether there are any DHCP services on the LAN2/WAN interface, you can manually assign an IP address to the interface. Note that the IP Address and Subnet Mask should be assigned within the same network as the PPTP-enabled DSL modem.

Click **OK**.

5.2.5 Using a Static IP or multiple Static IPs with a DSL/Cable Modem

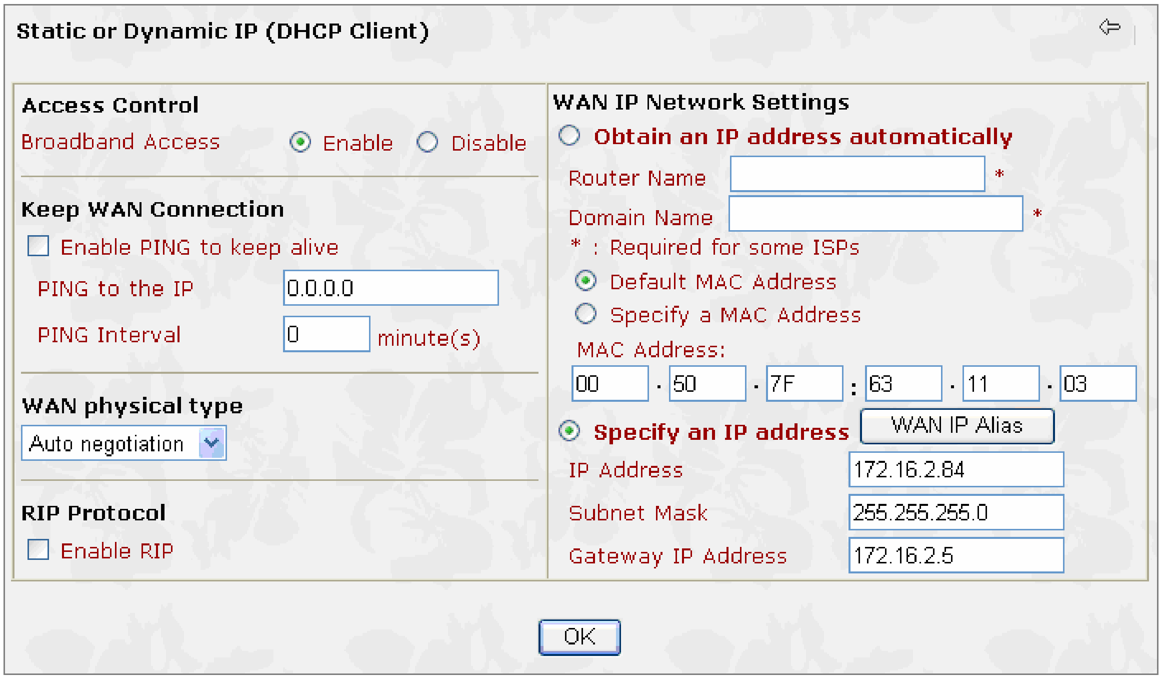
In this application, you receive a fixed public IP address or a public subnet (ie. Multiple public IP addresses) from your DSL or Cable ISP. In most cases, a Cable ISP will provide a fixed public IP, while a DSL ISP will provide a public subnet. If you have a public subnet, you could choose an IP address or many IP address to assign to the WAN interface. Click **Internet Access Setup > Static or Dynamic IP** to enter the setup page, which is depicted as follows.

Access Control

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

Keep WAN Connection

Enable PING to keep alive**:** Check to enable PING to keep alive function. Normally, this function is used for Dynamic IP environment. Here will ignore the settings.



Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

Keep WAN Connection

☐ Enable PING to keep alive

PING to the IP: 0.0.0.0

PING Interval: 0 minute(s)

WAN physical type

Auto negotiation

RIP Protocol

☐ Enable RIP

WAN IP Network Settings

○ Obtain an IP address automatically

Router Name: *

Domain Name: *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 - 50 - 7F : 63 - 11 - 03

● Specify an IP address [WAN IP Alias]

IP Address: 172.16.2.84

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.16.2.5

RIP Protocol

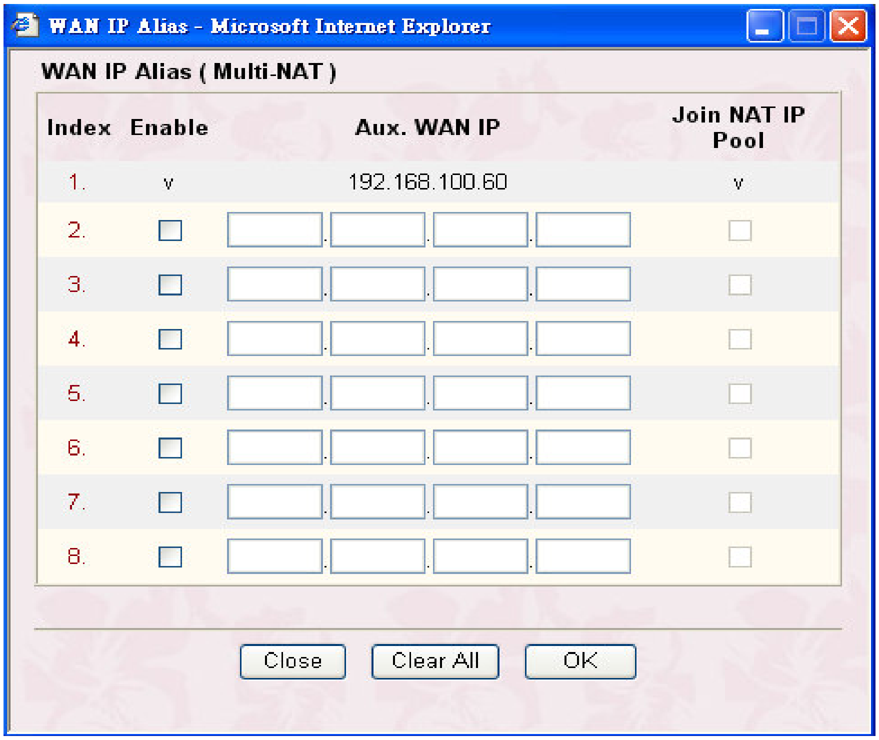
Enable RIP: Check to turn RIP packets exchange on WAN interface. For most Internet access, you don't need to check the option.

WAN IP Network Settings

Specify an IP address: As we are using a static IP, you have to select the option to specify an IP Address, Subnet Mask, and Gateway IP Address.

Click **OK**.

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



WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	192.168.100.60	v
2.	☐	. . .	☐
3.	☐	. . .	☐
4.	☐	. . .	☐
5.	☐	. . .	☐
6.	☐	. . .	☐
7.	☐	. . .	☐
8.	☐	. . .	☐

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

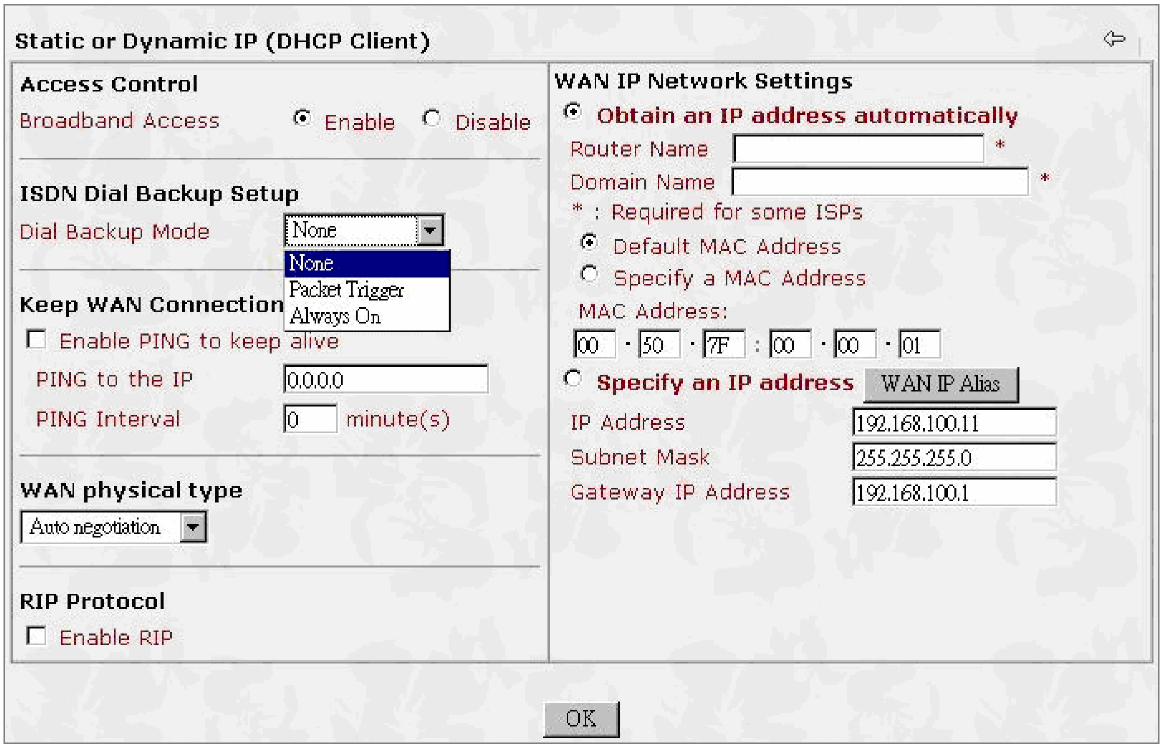
This application is mostly used by Cable ISPs. Click **Internet Access Setup > Static or Dynamic IP** to enter the setup page.

Access Control

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

Keep WAN Connection

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



Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

ISDN Dial Backup Setup

Dial Backup Mode: None

Keep WAN Connection

☐ Enable PING to keep alive

PING to the IP: 0.0.0.0

PING Interval: 0 minute(s)

WAN physical type

Auto negotiation

RIP Protocol

☐ Enable RIP

WAN IP Network Settings

● Obtain an IP address automatically

Router Name: *

Domain Name: *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

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

○ Specify an IP address

IP Address: 192.168.100.11

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.100.1

RIP Protocol

***Enable RIP*: Check to turn RIP packets exchange on WAN interface. For most Internet access, you don't need to check the option.

WAN IP Network Settings

Obtain an IP address automatically: The option must be enabled.

Router Name: Depending on your Cable ISP, this option may or may not be left blank. Some ISPs require this name for access authentication.

Domain Name: Depending on your Cable ISP this field may or may not be left blank.

Default MAC Address & Specify a MAC Address: These two options are mutually exclusive. Some Cable ISPs use a specific MAC address for access authentication. In such cases you need to check the **Specify a MAC Address box** and enter the MAC address in the MAC Address fields. Click **OK** and restart the router to allow the settings to take affect.

5.2.7 Configure ISDN dial backup for broadband access

Due to no ISDN interface in the Vigor2900 and Vigor2900G models, the ISDN dial backup facility and its associated setup options are not available for these models. Please refer to the previous figure, you can find out the ISDN Dial Backup Setup.

ISDN Dial Backup Setup

Dial Backup Mode**:** Three options are provided for dial backup mode.

None: Disable the backup function.

Packet Trigger**:** The backup line is disconnected until a packet from a local host triggers the router to establish a connection.

Always On**:** If the broadband connection is no longer available, the backup line will automatically connect and stay always-on until the broadband connection is recovered.

For ISDN dial backup function, you must create a dial backup profile. Please click **Internet Access Setup > Dialing to a Single ISP** to enter the backup profile setup page.

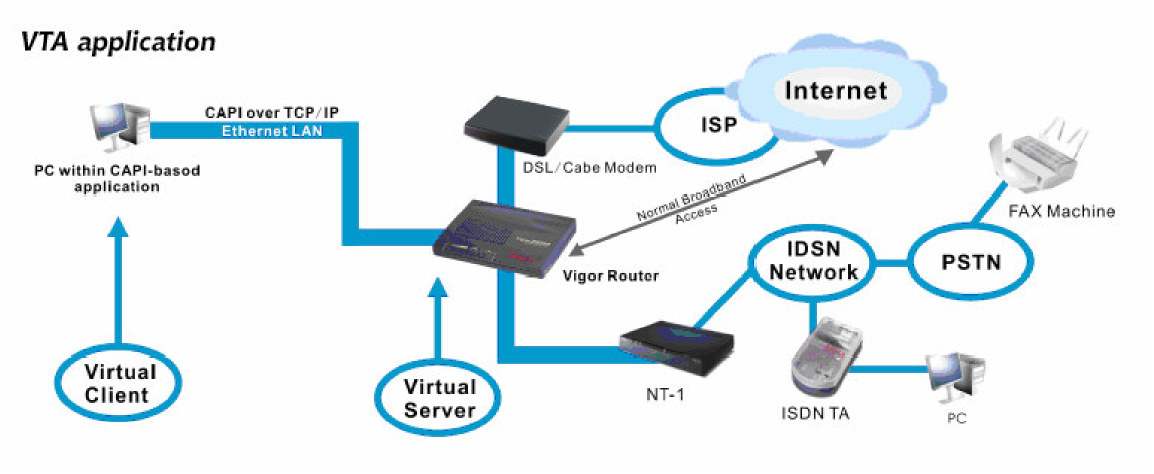
Chapter 6
Virtual TA (Remote CAPI) Setup

6.1 Introduction

This chapter is only applied to Vigor2900G and Vigor2900Gi models which have the **ISDN interface** and the **Virtual TA** facilities are available.

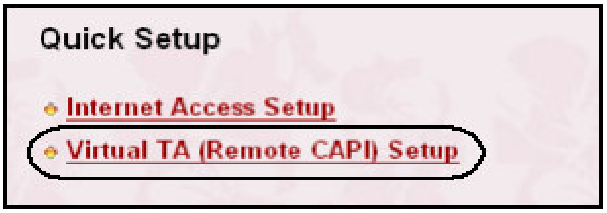
The term **Virtual TA** means the local Ethernet-connected hosts or PCs use popular CAPI-based software such as RVS-COM or BVRP etc. to access the router as a local ISDN TA for FAX sending or receiving via the ISDN line. Basically, it is a client/server network model. The Virtual TA server built into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

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



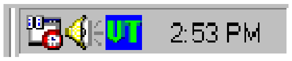
As depicted in the following application chart, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA etc. Use the following setup link on the Setup Main Menu to configure the Virtual TA facility.

Quick Setup > Virtual TA (Remote CAPI) Setup

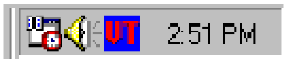


6.2 Install a Virtual TA Client

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



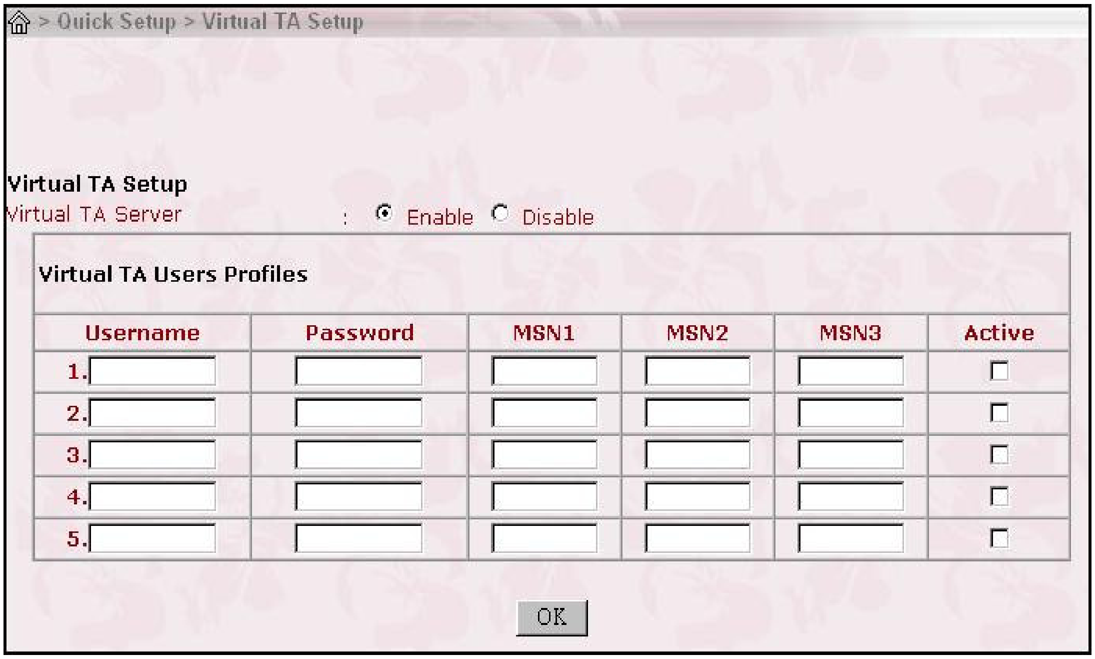
When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Read your software user guide for detailed configuration. If the icon text is RED, it means the client lost the connection with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



6.3 Configure a Virtual TA Client/ Server

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

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



Virtual TA Setup

Virtual TA Server : ● Enable ○ Disable

Virtual TA Users Profiles

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

Virtual TA Server

Enable: Check it to activate the server.

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

Virtual TA User Profiles

Username: Specify the username for a specific client.

Password: Specify the password for a specific client.

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

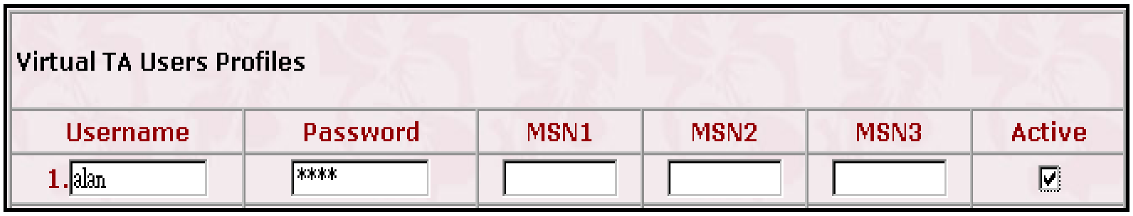
Active: Check it to enable the client for accessing the server.

Creating a User Profile

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

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

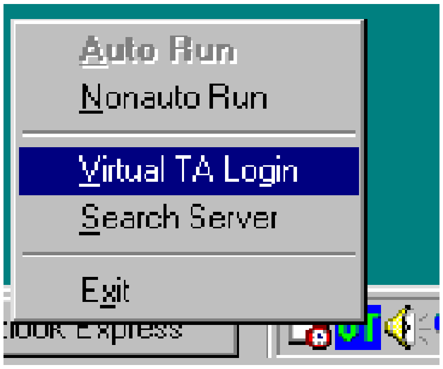
1. On the server: Click **Virtual TA (Remote CAPI) Setup**, and fill in the Username and Password fields. Click the **Active** checkbox to enable the account.



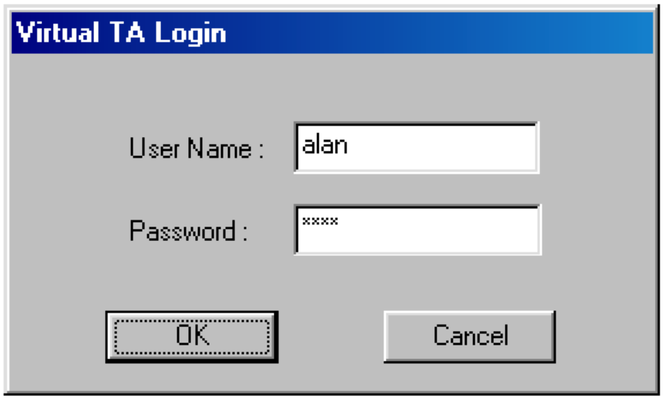
Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	****				☑

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



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



Virtual TA Login

User Name : alan

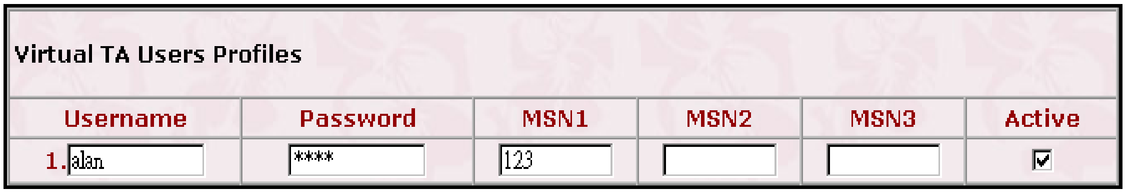
Password : ****

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

Configuring the MSN number

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

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



Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	****	123			☑

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

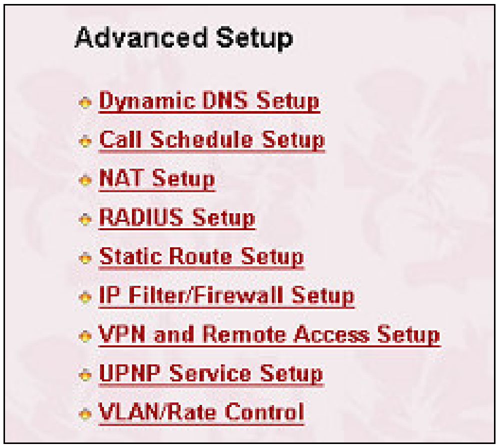
Chapter 7
Dynamic DNS Setup

7.1 Introduction

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

The Dynamic DNS function allows the router to update its online WAN IP address which assigned by ISP to the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. Use the following setup link on the Setup Main Menu to configure the Dynamic DNS Setup function.

Advanced Setup > Dynamic DNS Setup

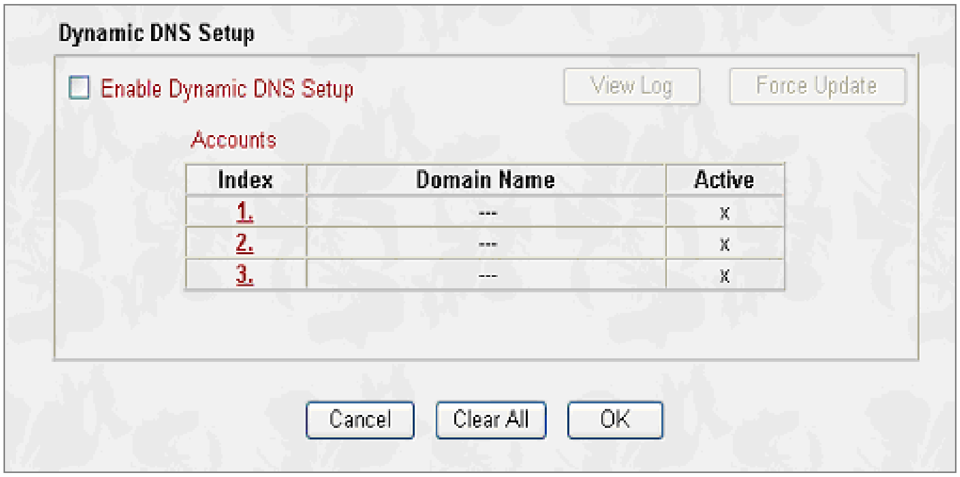


7.2 Configuration

Enable the Function and Add a Dynamic DNS Account

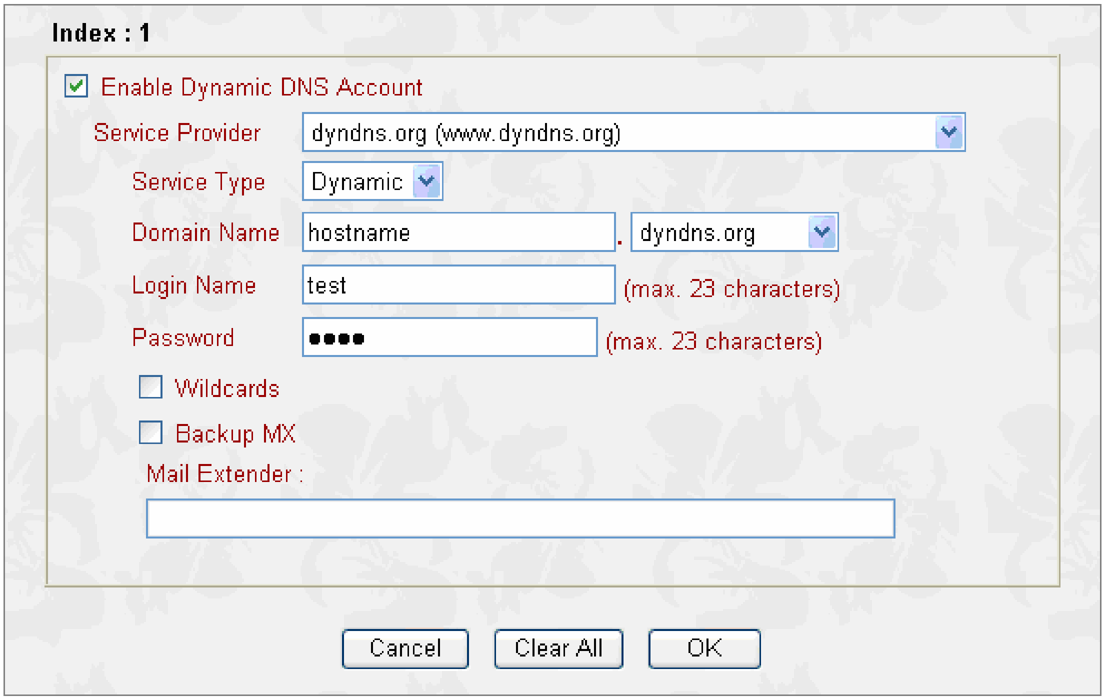
1. Assume you have a registered domain name from the DDNS provider, say ***hostname.dyndns.org***, and an account with username: ***test*** and password: ***test***.

2. Login **Main Menu > Dynamic DNS Setup** and then you will see the following web page.



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

3. Check **Enable Dynamic DNS Setup** and Index number **1** to add an account for the router. And now, you will see the following web page.



Index : 1

☑ Enable Dynamic DNS Account

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

Service Type: Dynamic

Domain Name: hostname . dyndns.org

Login Name: test (max. 23 characters)

Password: ●●●● (max. 23 characters)

☐ Wildcards

☐ Backup MX

Mail Extender :

4. 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***.

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

Note: 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

1. Login **Main Menu > Dynamic DNS Setup**.
2. 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

1. Login **Main Menu > Dynamic DNS Setup**.

2. Click the **Index** number you want to delete and then push **Clear All** button to delete the account.

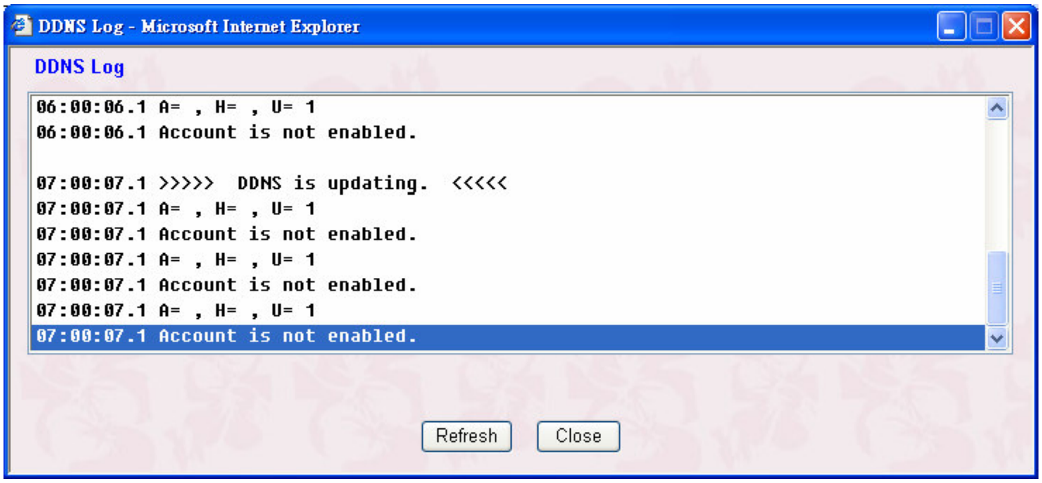
7.3 Validation and Troubleshooting

Ping the Registered Domain Name

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

View the DDNS Logs

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



```
06:00:06.1 A= , H= , U= 1
06:00:06.1 Account is not enabled.

07:00:07.1 >>>>>  DDNS is updating.  <<<<<
07:00:07.1 A= , H= , U= 1
07:00:07.1 Account is not enabled.
07:00:07.1 A= , H= , U= 1
07:00:07.1 Account is not enabled.
07:00:07.1 A= , H= , U= 1
07:00:07.1 Account is not enabled.
```

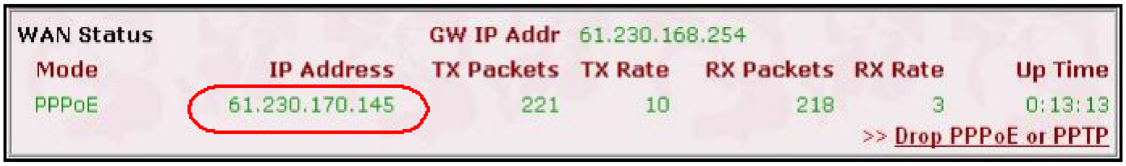
Where **A** : Login Name

H : Domain Name without suffix.

Return Code= good 61.230.170.145

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

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



WAN Status		GW IP Addr	61.230.168.254			
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.170.145	221	10	218	3	0:13:13

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

Chapter 8
Call Control and PPP/MP Setup

8.1 Introduction

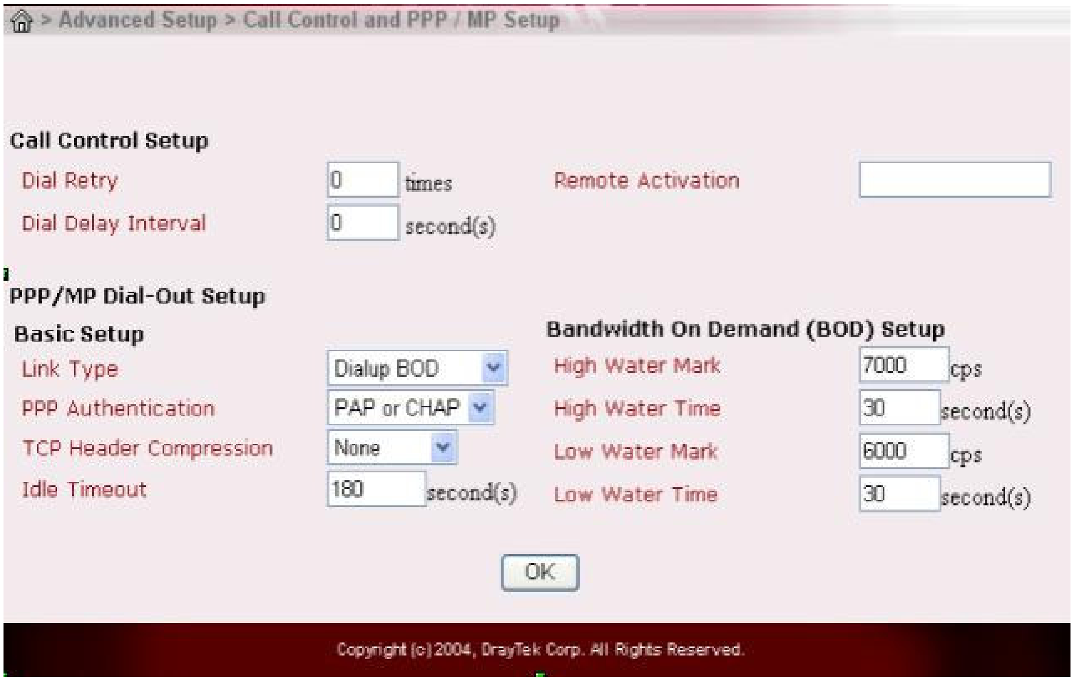
Some applications require that the router could be remotely activated, or dial up to the ISP using the ISDN interface. For instance, if you want to access the Internet via ISDN from home, usually the dialup connection is idle when you are not at home. It may be that, while working in the office, you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

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

Note: The Call Control and PPP/MP are only available on the ISDN interface of Vigor2900Gi and Vigor2900i. This chapter is not applied to Vigor2900 and Vigor2900G which do not have ISDN interface.

8.2 Configuration

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



> Advanced Setup > Call Control and PPP / MP Setup

Call Control Setup

Dial Retry: 0 times

Dial Delay Interval: 0 second(s)

Remote Activation:

PPP/MP Dial-Out Setup

Basic Setup

Link Type: Dialup BOD

PPP Authentication: PAP or CHAP

TCP Header Compression: None

Idle Timeout: 180 second(s)

Bandwidth On Demand (BOD) Setup

High Water Mark: 7000 cps

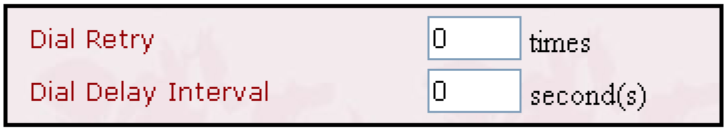
High Water Time: 30 second(s)

Low Water Mark: 6000 cps

Low Water Time: 30 second(s)

Call Control Setup:

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



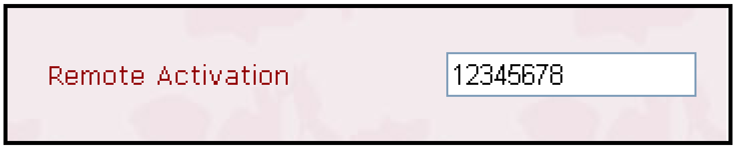
Dial Retry: 0 times

Dial Delay Interval: 0 second(s)

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

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

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



Remote Activation 12345678

Note that Internet Access Setup > Dialing to a Single ISP should be pre-set 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 or two B channels or BOD (Bandwidth on Demand).

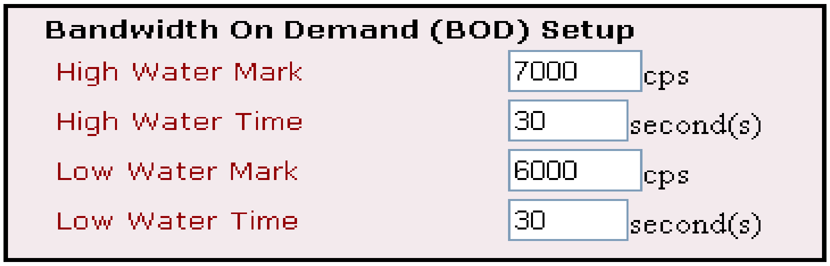
PPP Authentication: Specify the PPP authentication method for PPP/MP connection. Normally set to **PAP/CHAP** for the widest compatibility.

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

Idle Timeout: Because our IDSN facility is "Dial On Demand", we will drop ISDN line as there is no data traffic within the specified duration.

BOD Setup :

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



Bandwidth On Demand (BOD) Setup

High Water Mark 7000 cps

High Water Time 30 second(s)

Low Water Mark 6000 cps

Low Water Time 30 second(s)

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

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

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

Note: If you are not familiar with ISDN and ML-PPP's operations, please be wary of changing the default values.

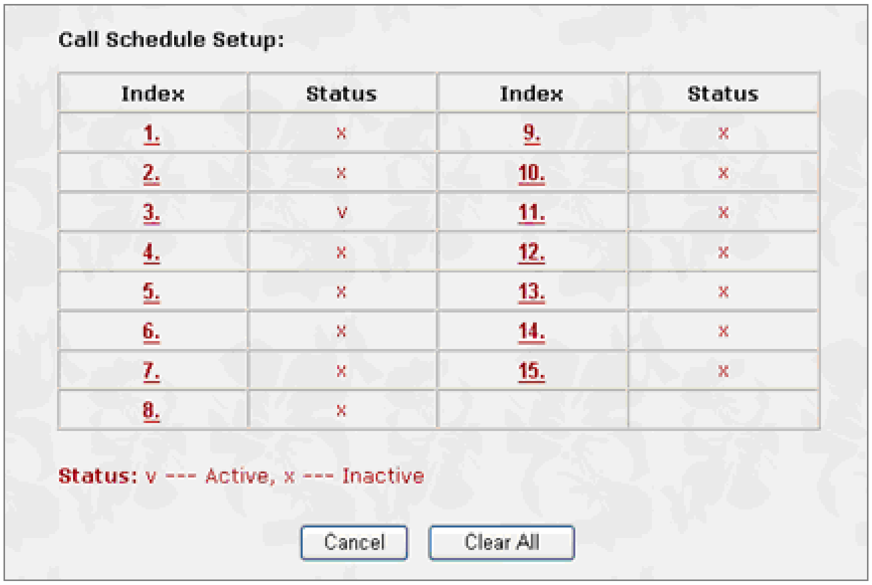
Click **OK**.

Chapter 9
Call Schedule Setup

9.1 Introduction

Call Schedule facility is used to control the router's dialer or connection manager what time should be up or down according to the pre-defined call schedule profiles. Before configuring the Call Schedule function, you have to set up time function properly and arrange schedules for specified Internet access profile or LAN-to-LAN profile.

The Vigor router supports up to 15 profiles for call schedule usage. Click **Call Schedule Setup** under **Advanced Setup** group, you will see the profiles as follows.



Call Schedule Setup:

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

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

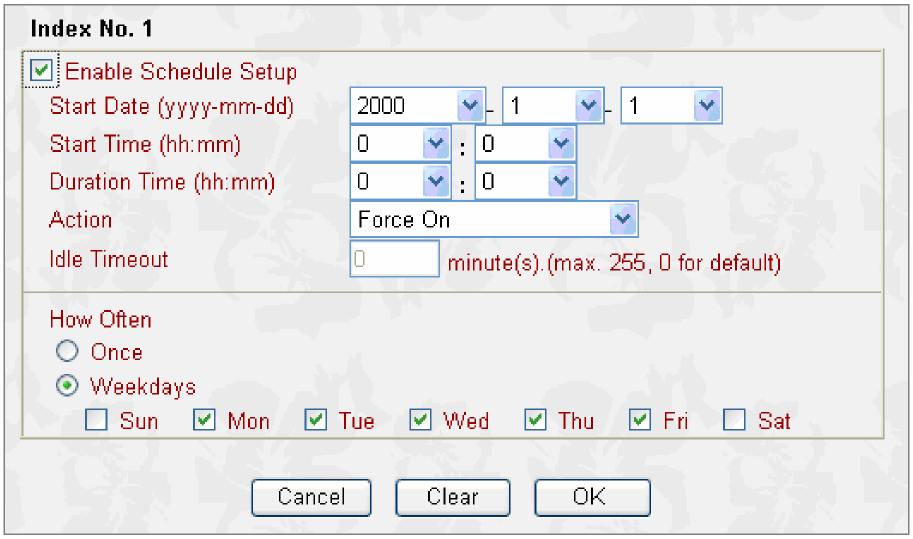
Click **Clear All** button to remove all schedules in the router.

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

9.2 Configuration

Add a Call Schedule

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



Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd): 2000 - 1 - 1

Start Time (hh:mm): 0 : 0

Duration Time (hh:mm): 0 : 0

Action: Force On

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

How Often

○ Once

● Weekdays

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

2. The detailed descriptions for each setting are:

Enable Schedule Setup: Check to enable the schedule.

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

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

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

Action: Specify which action should be applied by Call Schedule during the time period of the schedule.

Force On: Force the connection to be always-on.

Force Down: Force the connection to be always-down.

Enable Dial-On-Demand: Specify the connection to be dial-on-demand and the value of idle timeout should be specified as following **Idle**

Timeout field.

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

How Often: Specify how often the schedule will be applied.

Once*:* The schedule will be applied just once.

Weekdays*:* Specify which days in one week should perform the schedule.

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

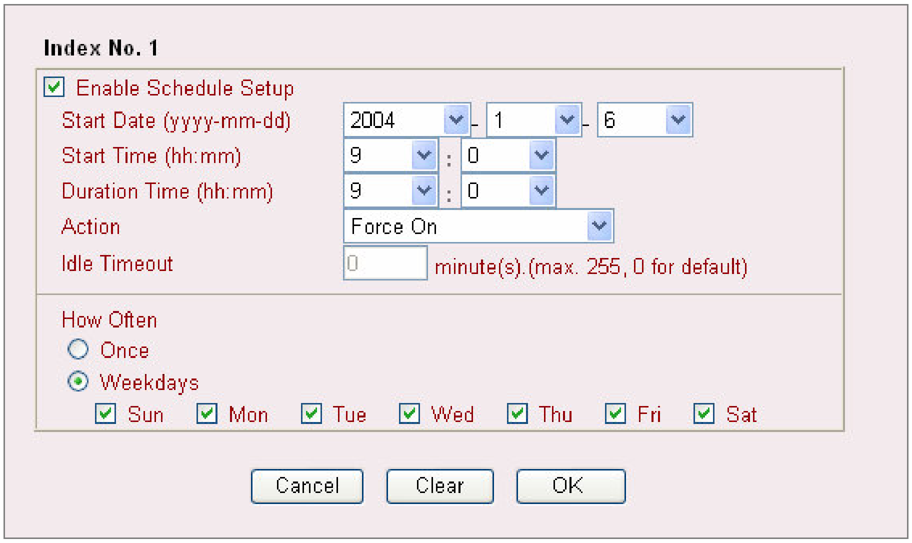
Delete a Call Schedule

1. Click **Call Schedule Setup** and the **Index** number which you want to remove.
2. Click **Clear** button to remove that profile.

9.3 An Example

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

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



Index No. 1

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd): 2004 - 1 - 6

Start Time (hh:mm): 9 : 0

Duration Time (hh:mm): 9 : 0

Action: Force On

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

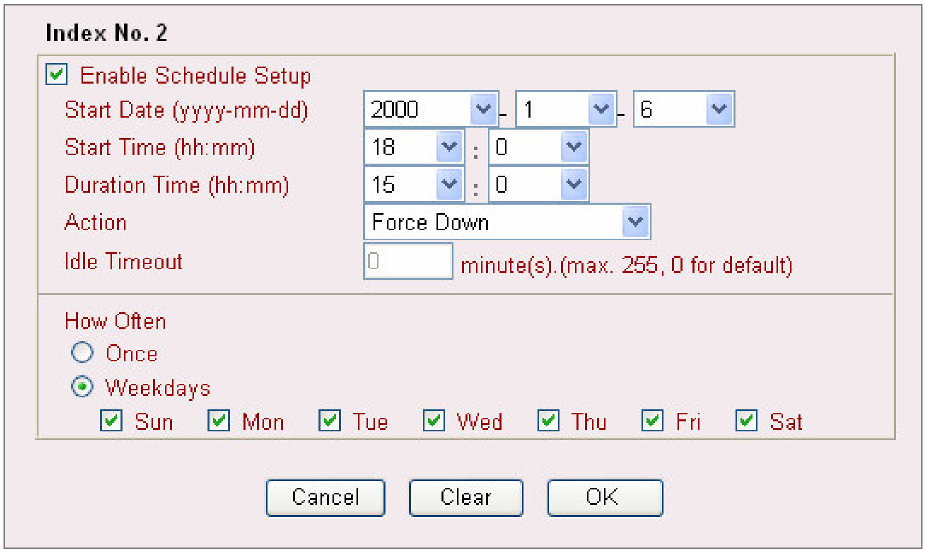
How Often

○ Once

● Weekdays

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

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



Index No. 2

☑ Enable Schedule Setup

Start Date (yyyy-mm-dd): 2000 - 1 - 6

Start Time (hh:mm): 18 : 0

Duration Time (hh:mm): 15 : 0

Action: Force Down

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

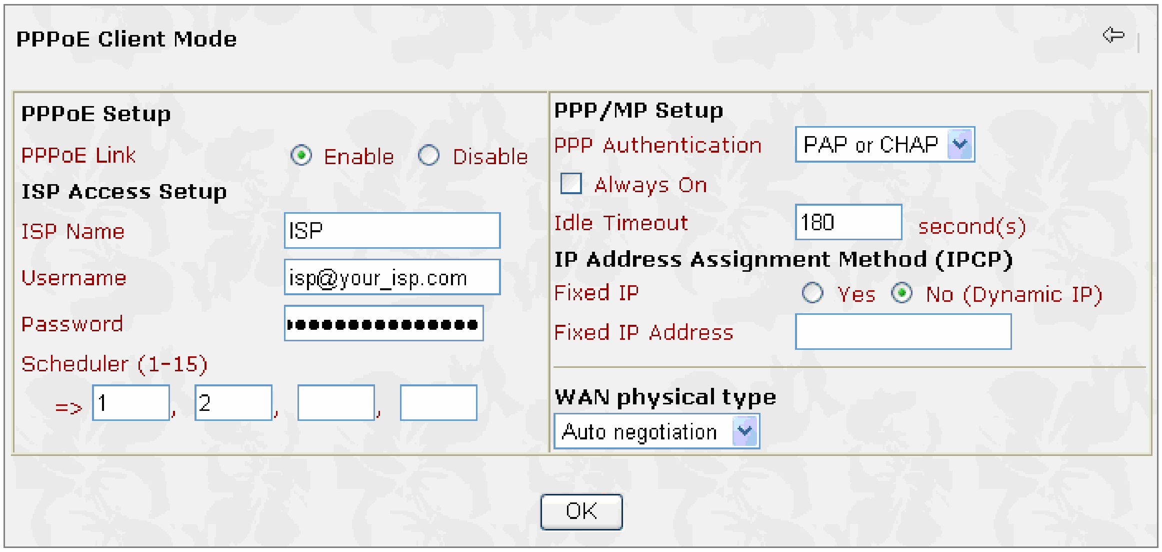
How Often

○ Once

● Weekdays

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

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



PPPoE Client Mode

PPPoE Setup

PPPoE Link ● Enable ○ Disable

ISP Access Setup

ISP Name: ISP

Username: isp@your_isp.com

Password: ••••••••••••••••

Scheduler (1-15) => 1, 2, ,

PPP/MP Setup

PPP Authentication: PAP or CHAP

☐ Always On

Idle Timeout: 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address:

WAN physical type

Auto negotiation

Chapter 10
NAT Setup

10.1 Introduction

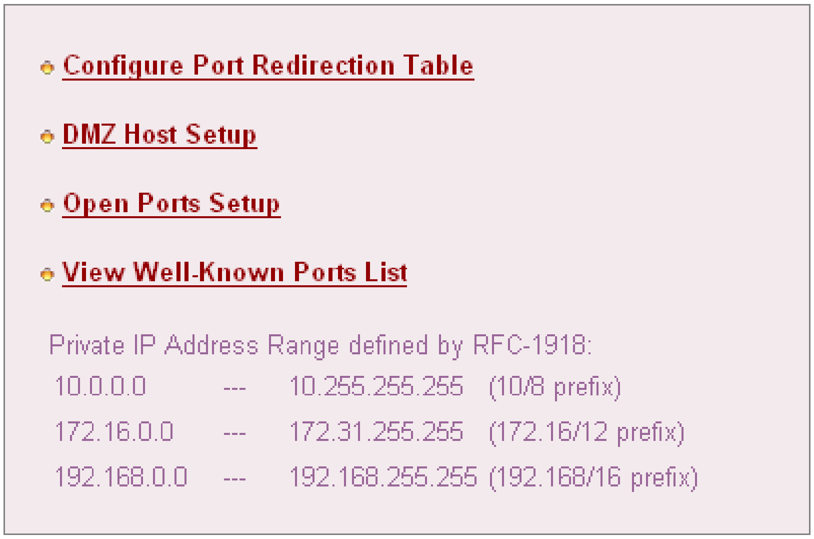
NAT is a method of mapping one or more IP addresses and/or service ports into different specified services, where NAT stands for Network Address Translation. It allows the internal IP addresses of many computers on a Local Area Network (LAN) to be translated to one public address, saving users' cost.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

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

The following sections describe the web configuration for setting up the NAT facility, including specific configuration information and any limitation it has. One can find the entrance of this setting, as depicted in the following figure, after clicking the **NAT Setup** in the Advanced Setup of the main menu.

10.2 NAT Setup

Click **NAT Setup** to open the setup page. On the page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. Also, as stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping method. In the Vigor routers, we support three variants of port mapping methods: **Port Redirection**, **Open Ports**, and **DMZ host**.



Private IP Address Range defined by RFC-1918:

```
10.0.0.0     ---  10.255.255.255  (10/8 prefix)
172.16.0.0   ---  172.31.255.255  (172.16/12 prefix)
192.168.0.0  ---  192.168.255.255 (192.168/16 prefix)
```

Port Redirection: The packet is forwarded to a specific local host if the port number matches that defined in the table. A user can also translate the port to another port locally.

Open Ports: Similar to the Port Redirection, the Open Ports facility also supports users to define a range of ports.

DMZ host: This opens up a single host completely. All incoming packets will be forwarded to the host with the local IP address you designated. The only exception is packets received in response to outgoing requests from other local computers or incoming packets which match rules in the other two methods.

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

Port Redirection > Open Ports > DMZ

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

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

10.3 Configure Port Redirection Table

The **Port Redirection Table** may be used to expose internal servers to the public domain or open a specific port number for internal hosts. Internet hosts can use the WAN IP address to access internal network services, such as FTP, WWW, etc.

The following example shows how to expose an internal FTP server to the public domain. Assume that the internal FTP server is running on the local host with IP address of 192.168.1.10.

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

Service Name: Specify the name for the specific network service.

Protocol: Specify the transport layer protocol (TCP or UDP).

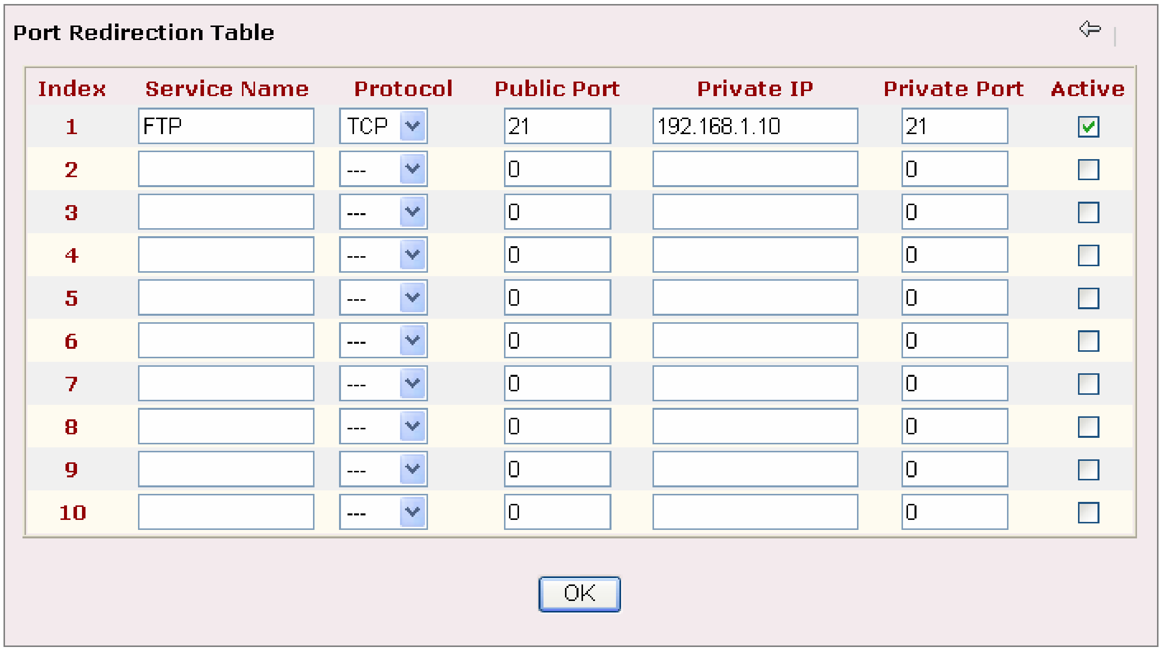
Public Port: Specify which port should be redirected to the internal host.

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

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

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

Click **OK**



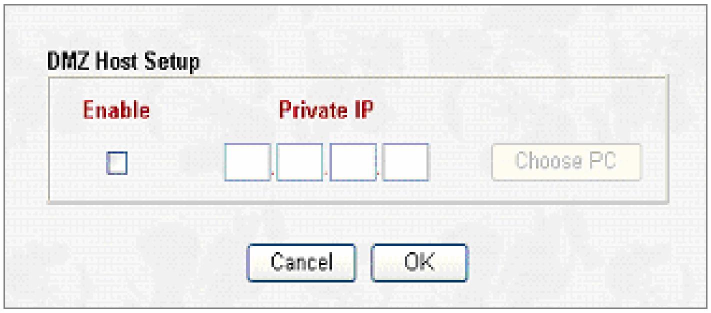
Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	FTP	TCP	21	192.168.1.10	21	☑
2		---	0		0	☐
3		---	0		0	☐
4		---	0		0	☐
5		---	0		0	☐
6		---	0		0	☐
7		---	0		0	☐
8		---	0		0	☐
9		---	0		0	☐
10		---	0		0	☐

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

10.4 DMZ Host Setup

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



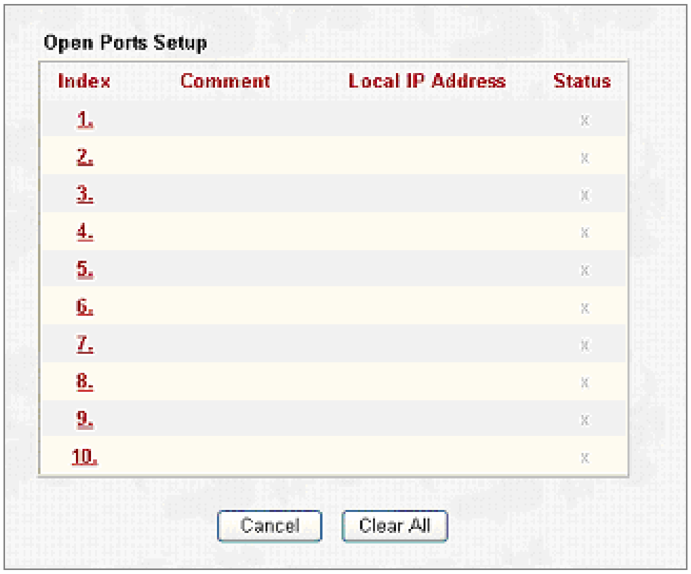
Enable: Check to enable the DMZ Host function.

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

Choose PC: 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.

10.5 Open Port Setup

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



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

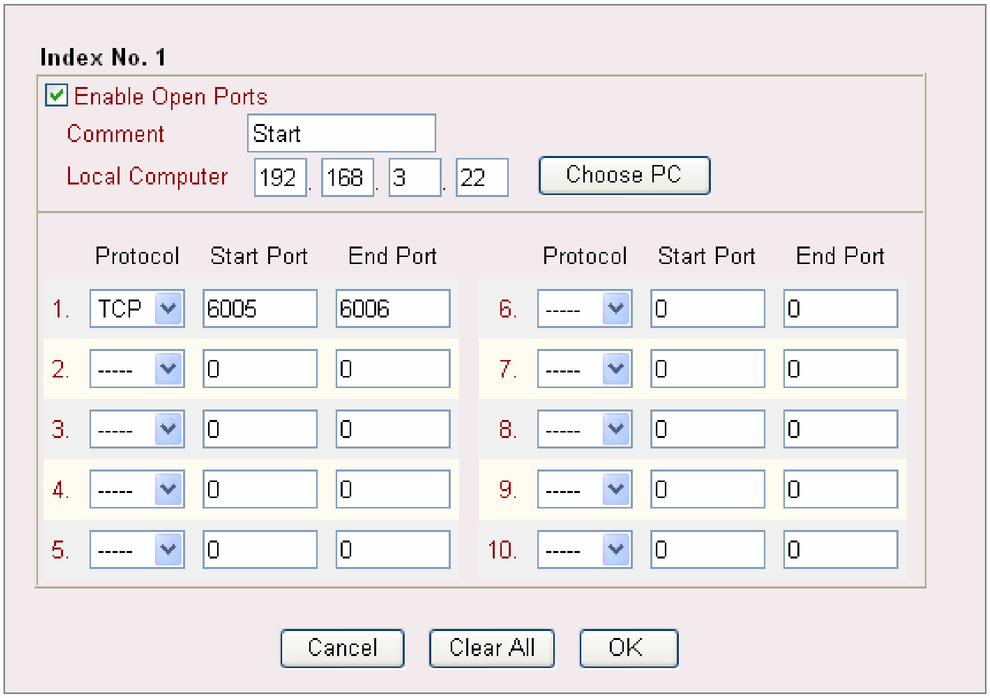
Index: Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

Comment: Display the name for the specified network service.

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

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

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



Index No. 1

☑ Enable Open Ports

Comment: Start

Local Computer: 192 . 168 . 3 . 22

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

Enable Open Ports: Check to enable the Open Port function for this entry.

Comment: Specify the name for the defined network service.

Local Computer: Enter the private IP address of the local host.

Choose PC: Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select one appropriate IP address of the local host in the list.

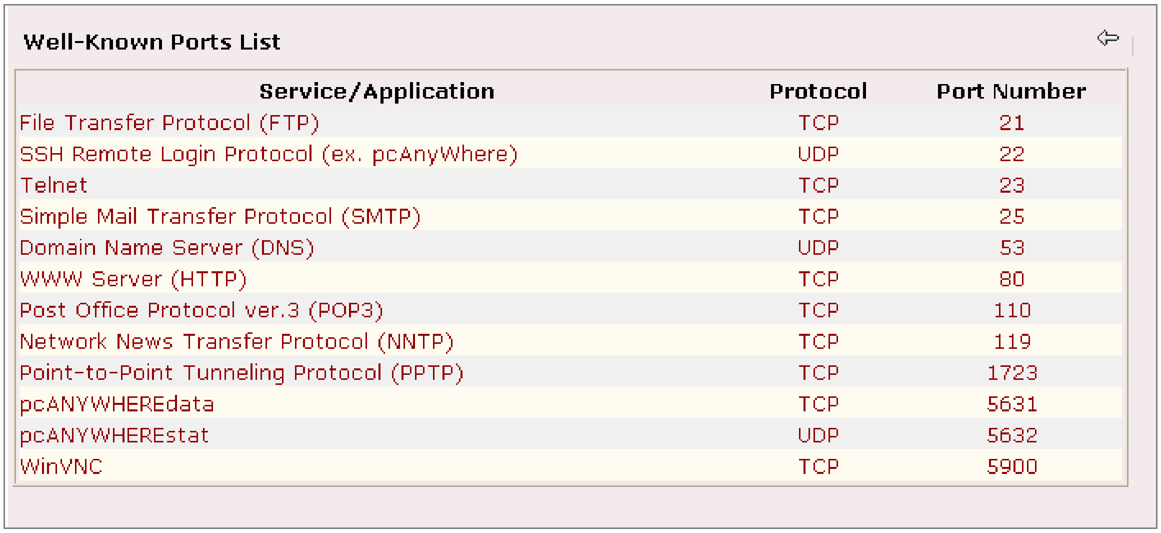
Protocol: Specify the transport layer protocol. It could be TCP, UDP, or NONE for selection.

Start Port: Specify the starting port number of the service offered by the local host.

End Port: Specify the ending port number of the service offered by the local host.

10.6 Well-known Port Number List

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



Well-Known Ports List

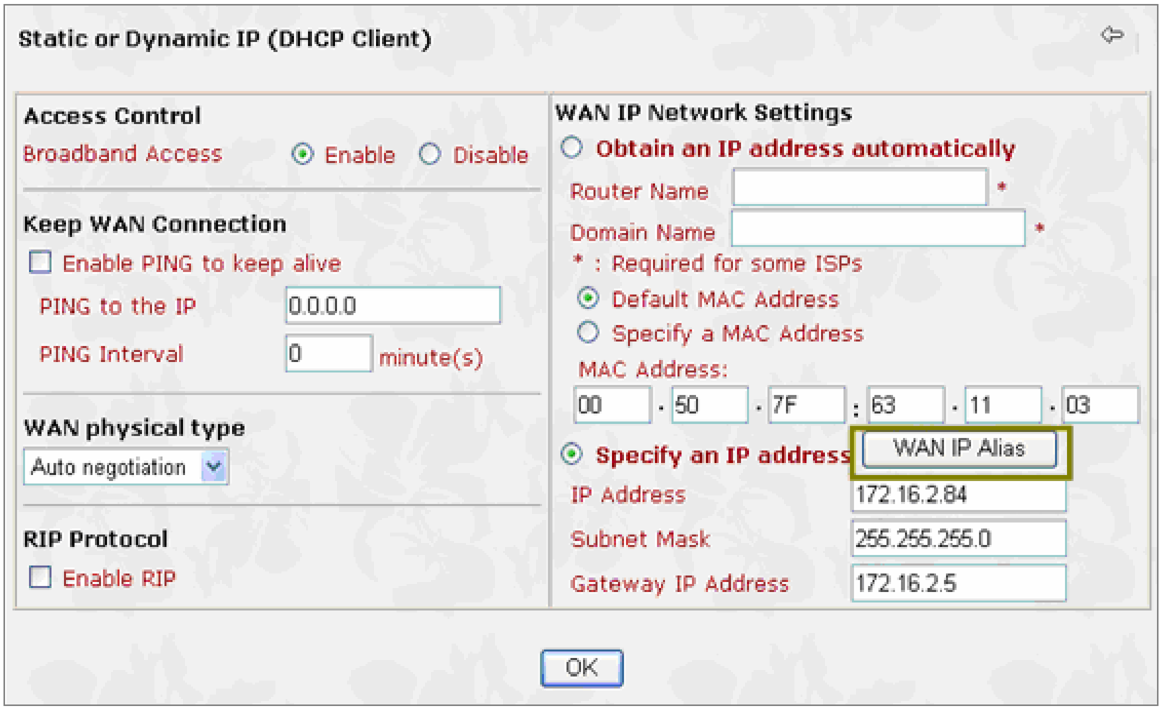
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer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

10.7 Multi-NAT Setup

If you have a group of static IP addresses, then you can use the Multi-NAT features to set up multiple DMZ hosts or multiple open ports hosts in your Vigor routers.

The following session shows you how to setup Multi-NAT feature.

To achieve it, you should find the path to click the button of **WAN IP Alias**. The path is **Main Menu > Quick Setup > Internet Access Setup**. Herein, you will see the following page.



Static or Dynamic IP (DHCP Client)

Access Control
Broadband Access ● Enable ○ Disable

Keep WAN Connection
☐ Enable PING to keep alive
PING to the IP 0.0.0.0
PING Interval 0 minute(s)

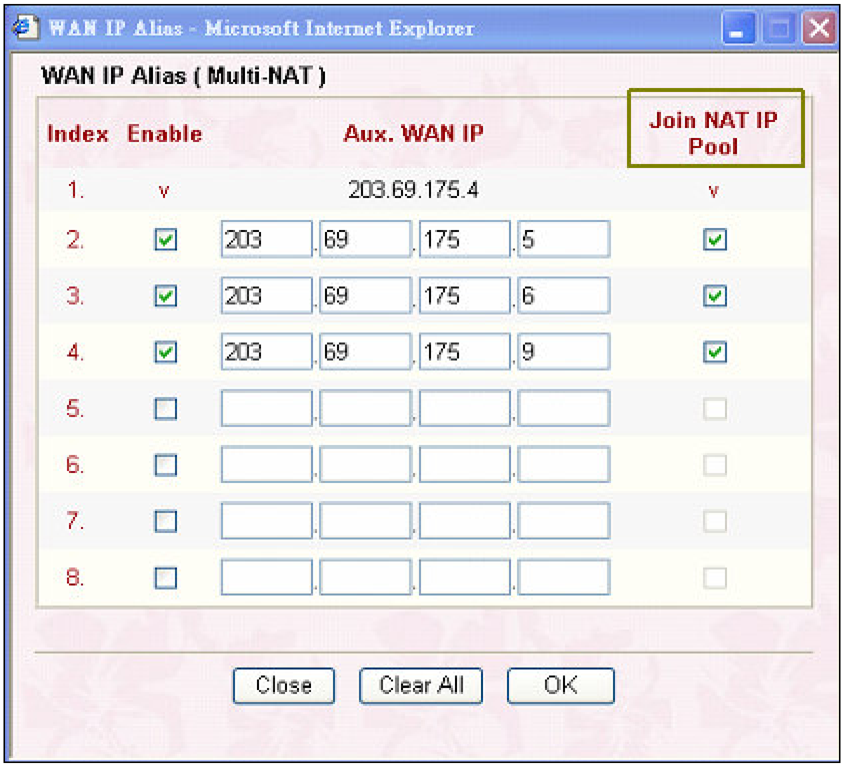
WAN physical type
Auto negotiation

RIP Protocol
☐ Enable RIP

WAN IP Network Settings
○ Obtain an IP address automatically
Router Name *
Domain Name *
* : Required for some ISPs
● Default MAC Address
○ Specify a MAC Address
MAC Address: 00 . 50 . 7F : 63 . 11 . 03
● Specify an IP address
IP Address 172.16.2.84
Subnet Mask 255.255.255.0
Gateway IP Address 172.16.2.5

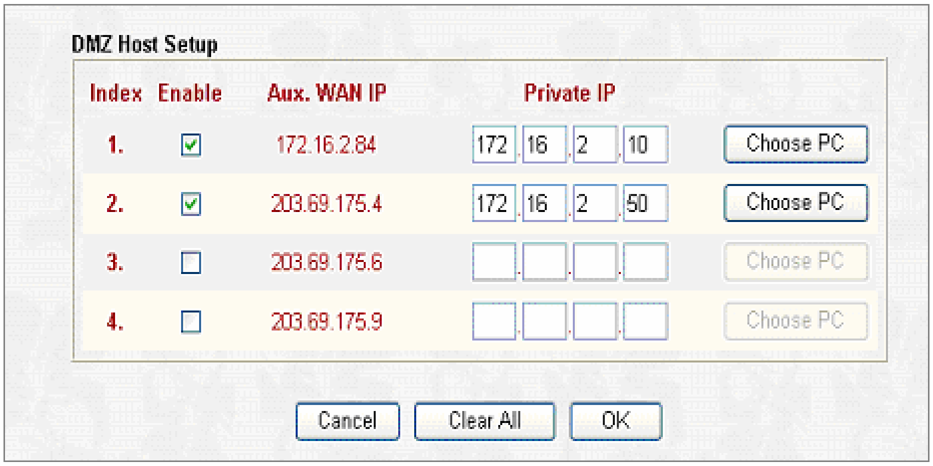
When you click the **WAN IP Alias** button, it will open a window for you to input your public IPs, as shown below. The **Join NAT IP Pool** check box indicates that the local user can use this IP to connect to the Internet. If you do not chick this check box, then the local user can not use this IP address.

After you set up the **WAN IP Alias**, then you can setup multiple DMZ and/or multiple open ports, as shown below.



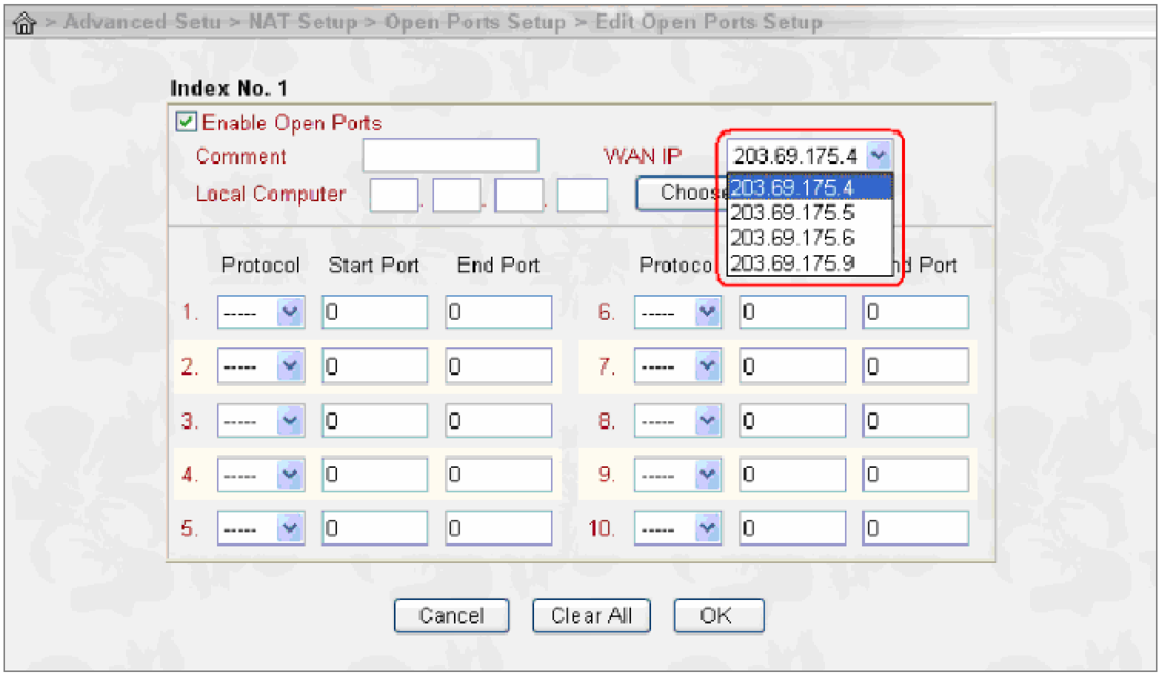
WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	203.69.175.4	v
2.	☑	203 . 69 . 175 . 5	☑
3.	☑	203 . 69 . 175 . 6	☑
4.	☑	203 . 69 . 175 . 9	☑
5.	☐	. . .	☐
6.	☐	. . .	☐
7.	☐	. . .	☐
8.	☐	. . .	☐



DMZ Host Setup

Index	Enable	Aux. WAN IP	Private IP	
1.	☑	172.16.2.84	172 . 16 . 2 . 10	Choose PC
2.	☑	203.69.175.4	172 . 16 . 2 . 50	Choose PC
3.	☐	203.69.175.6	. . .	Choose PC
4.	☐	203.69.175.9	. . .	Choose PC



> Advanced Setu > NAT Setup > Open Ports Setup > Edit Open Ports Setup

Index No. 1

☑ Enable Open Ports

Comment

WAN IP 203.69.175.4

203.69.175.4
203.69.175.5
203.69.175.6
203.69.175.9

Local Computer . . .

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

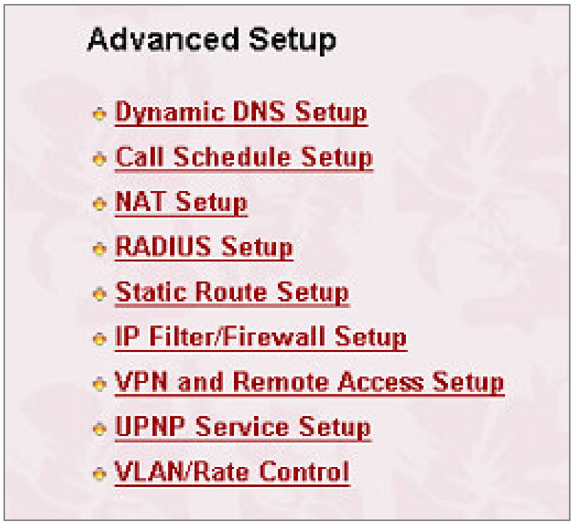
Chapter 11
RADIUS Setup

11.1 Introduction

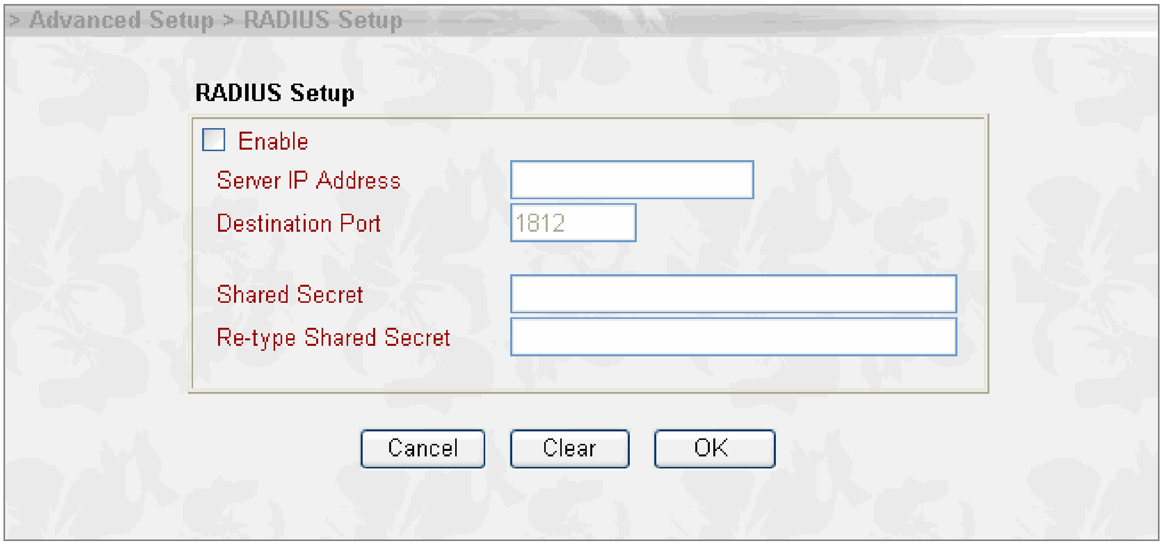
Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol widely used by Internet service providers on other remote access service. RADIUS is the most common means of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client function allows you to extend the remote dial-in user accounts to the RADIUS server. Your user accounts will not be limited by built-in accounts. It also lets you centralize remote access authentication for network management. Use the following setup link on the Setup Main Menu to configure the RADIUS function.

Advanced Setup > RADIUS Setup



11.2 Configuration



Destination Port: 1812

Check the **Enable** box to enable RADIUS client function

Server IP Address: The IP address of RADIUS server

Destination Port: The UDP port number that the RADIUS server is listening. The default value of 1812 is based on RFC 2138.

Shared Secret: The RADIUS server and client share a secret that is used to authenticate the messages sent between them. You must configure both sides to use the same shared secret.

Re-type Shared Secret: Confirm the Shared Secret.

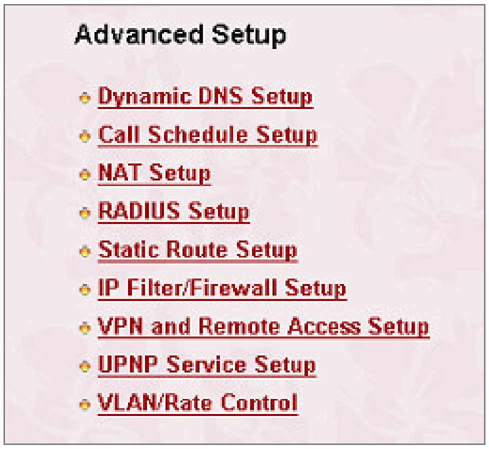
Chapter 12
Static Route Setup

12.1 Introduction

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

The router also has RIP (Routing Information Protocol) built-in by default. If the neighbor routers have the same protocol, the RIP will be used for exchanging routing information. Here, the **Static Route Setup** just provides a way to guide specified IP packets through specified routers in a static manner. This chapter shows you how to configure static routes within your Vigor routers. Use the following setup link on the Setup Main Menu to configure the Static Route Setup.

Advanced Setup > Static Route Setup



Advanced Setup

- Dynamic DNS Setup
- Call Schedule Setup
- NAT Setup
- RADIUS Setup
- Static Route Setup
- IP Filter/Firewall Setup
- VPN and Remote Access Setup
- UPNP Service Setup
- VLAN/Rate Control

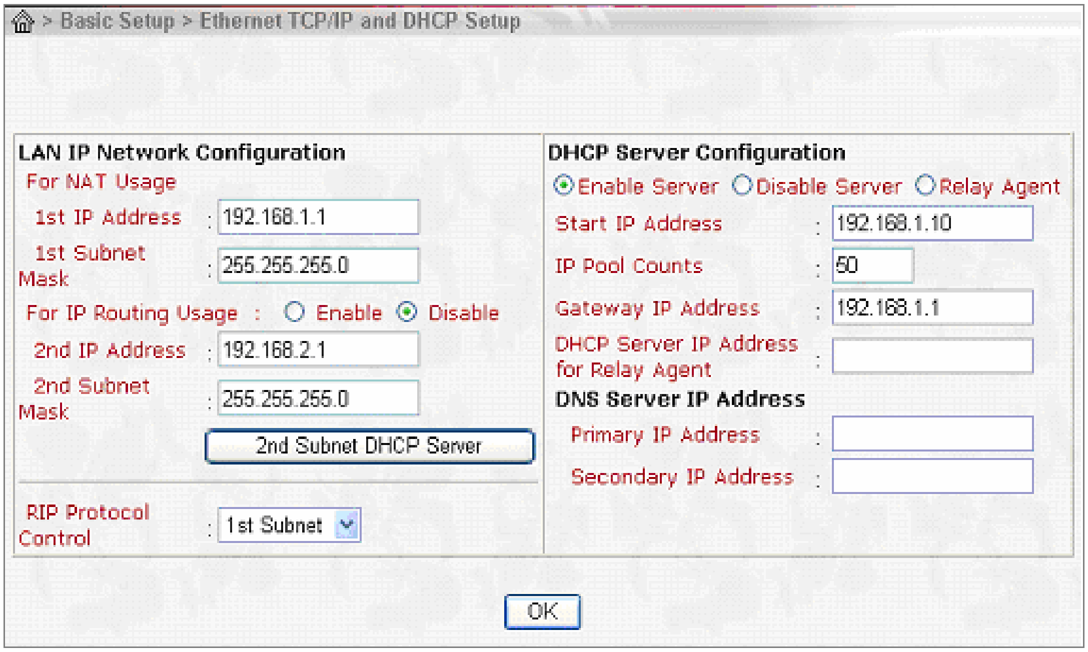
12.2 Configuration

Add Static Routers to Inside Private and Public Networks

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

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

Note: To set **RIP Protocol Control** as **1st Subnet** has two different meanings. The first one is that the LAN interface could be exchanged RIP packets with neighbor routers via 1st subnet (192.168.1.0/24). The second one is that those inside private subnets (ex. 192.168.10.0/24) could be NATed by the router to the Internet, but do IP routing for each other as well.



> Basic Setup > Ethernet TCP/IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage : ○ Enable ● Disable

2nd IP Address : 192.168.2.1

2nd Subnet Mask : 255.255.255.0

RIP Protocol Control : 1st Subnet

DHCP Server Configuration

● Enable Server ○ Disable Server ○ Relay Agent

Start IP Address : 192.168.1.10

IP Pool Counts : 50

Gateway IP Address : 192.168.1.1

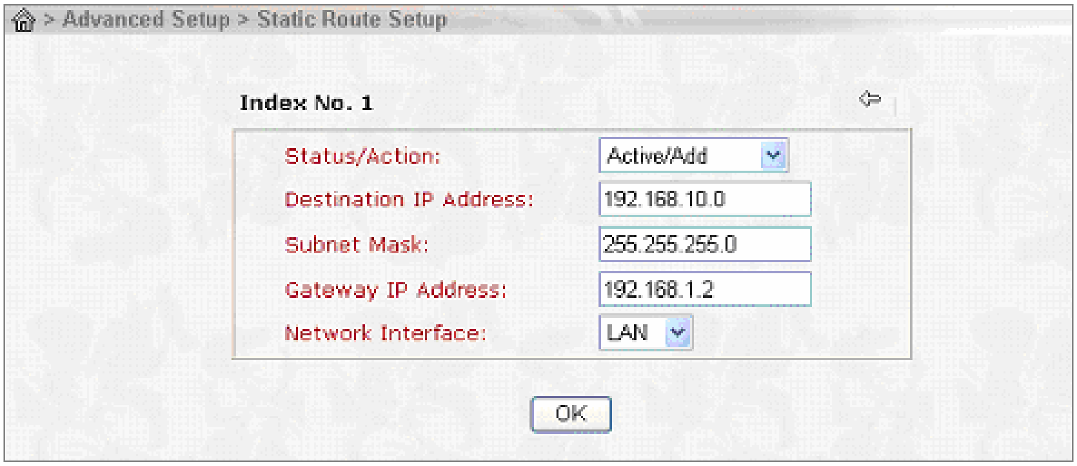
DHCP Server IP Address for Relay Agent :

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

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



> Advanced Setup > Static Route Setup

Index No. 1

Status/Action: Active/Add

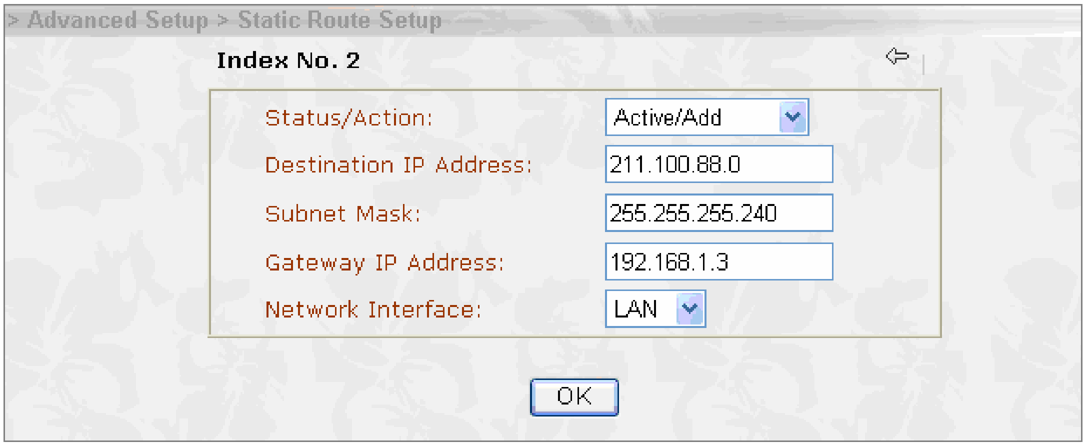
Destination IP Address: 192.168.10.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.2

Network Interface: LAN

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



Index No. 2

Status/Action: Active/Add

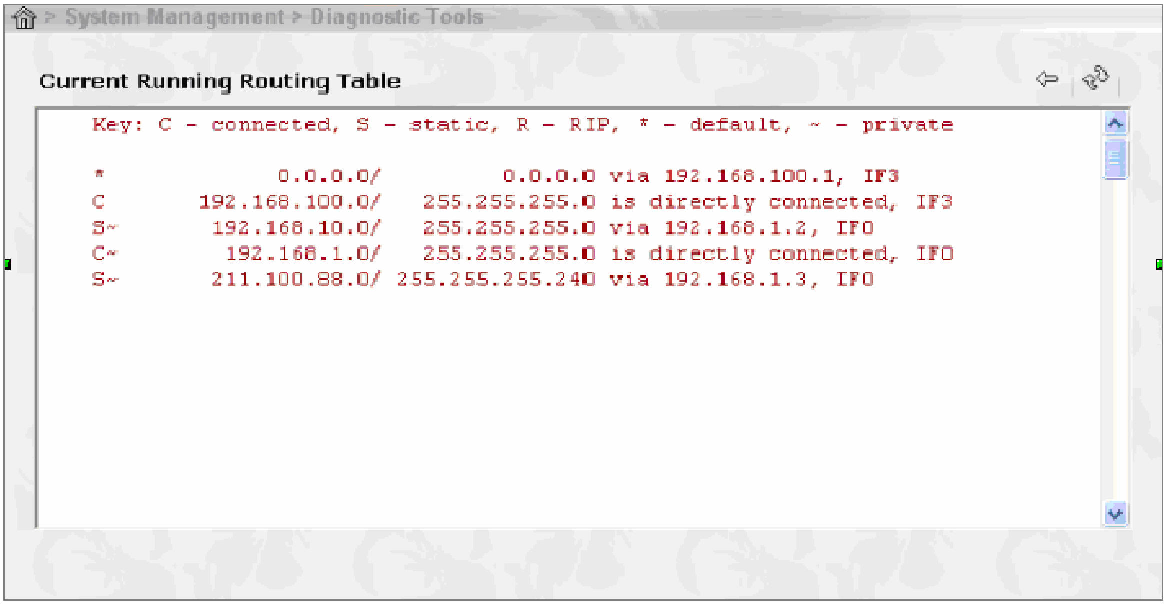
Destination IP Address: 211.100.88.0

Subnet Mask: 255.255.255.240

Gateway IP Address: 192.168.1.3

Network Interface: LAN

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

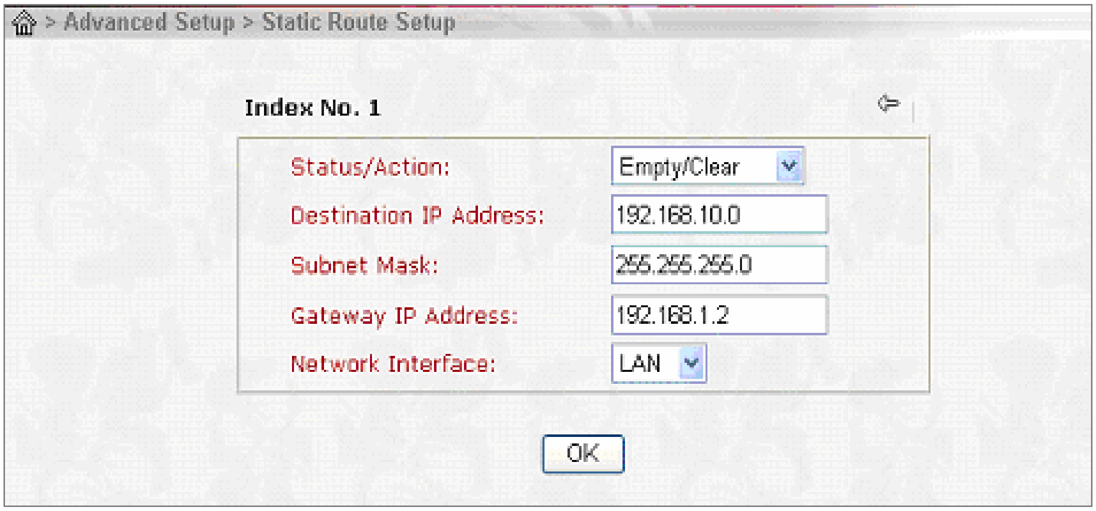


Current Running Routing Table

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

*            0.0.0.0/         0.0.0.0 via 192.168.100.1, IF3
C        192.168.100.0/   255.255.255.0 is directly connected, IF3
S~        192.168.10.0/   255.255.255.0 via 192.168.1.2, IF0
C~         192.168.1.0/   255.255.255.0 is directly connected, IF0
S~        211.100.88.0/ 255.255.255.240 via 192.168.1.3, IF0
```

Delete or Deactivate a Static Route

1. Click **Static Route Setup > Index Number** which you want to delete.
2. Select **Status/Action** to **Empty/Clear**. Click **OK** button to delete the route.



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

Chapter 13
IP Filter / Firewall Setup

13.1 Introduction

The IP Filter/Firewall function helps protect your local network against attack from outside. It also provides a way of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

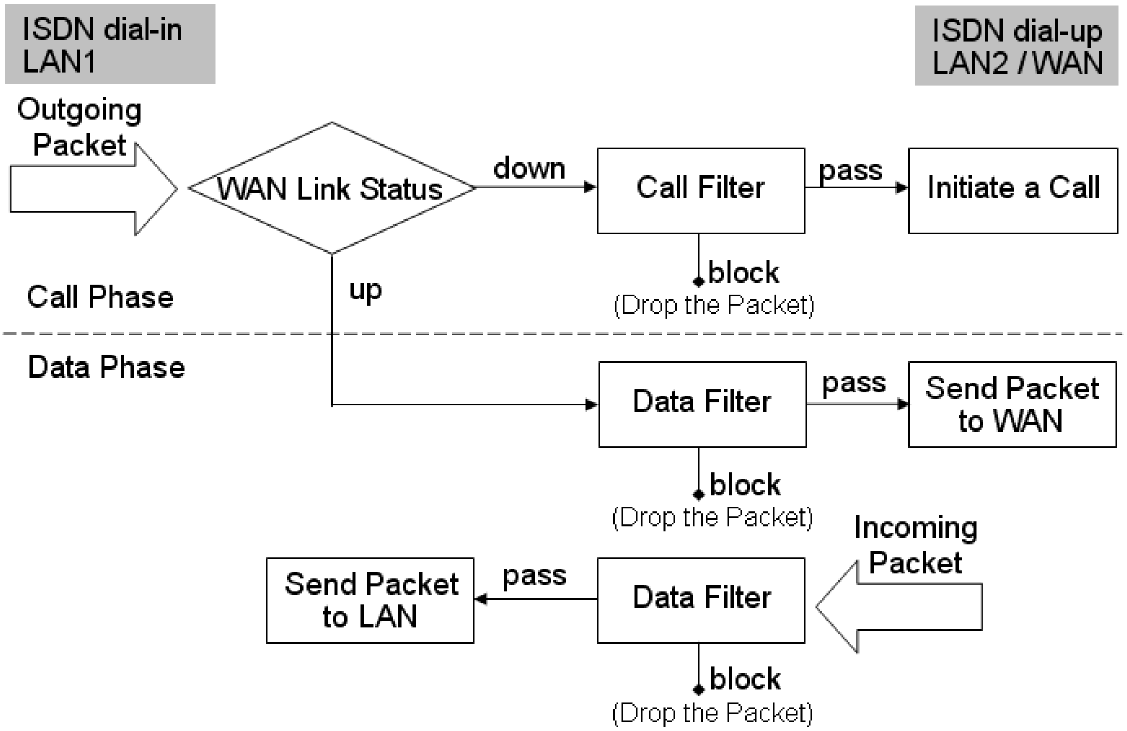
13.2 An Overview of the IP Filter/Firewall

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

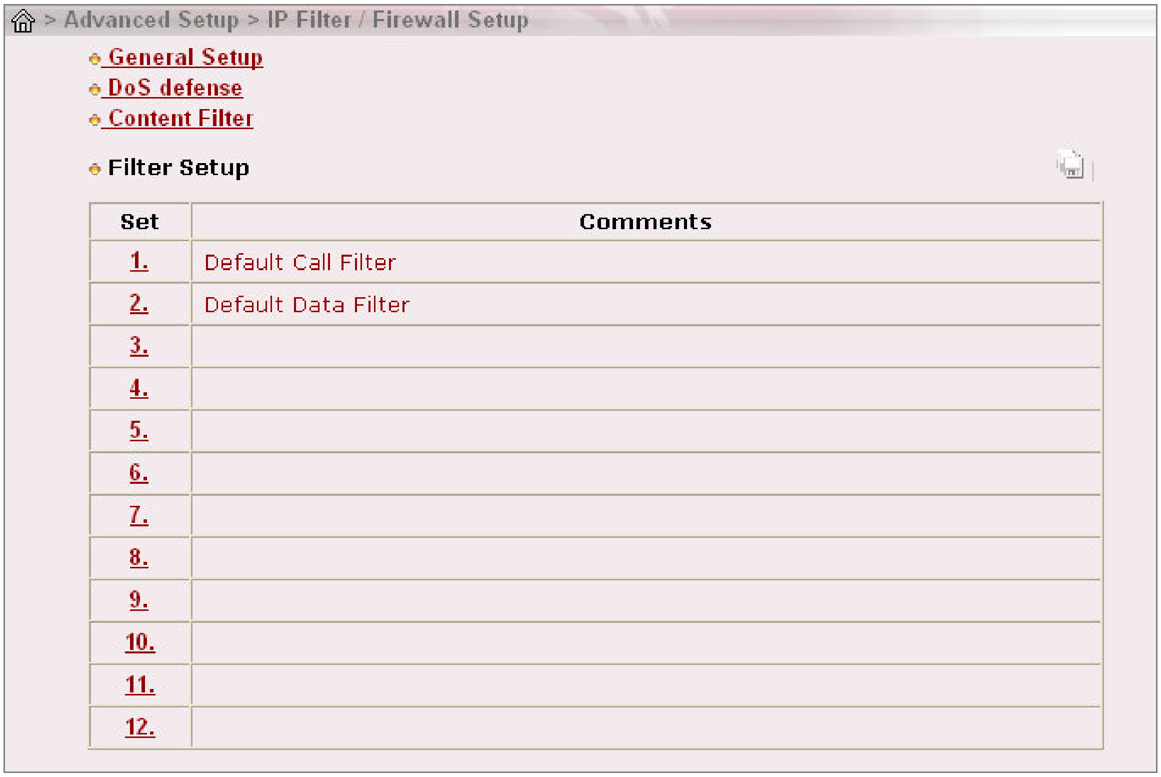
The packet filtering function contains, by default, two types of filter sets: Call Filter set and Data Filter set. The Call Filter is used for users that attempt to establish a connection from LAN side to the Internet. The Data Filter set is used to determine what kind of IP packets is allowed to pass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

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

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



The following sections will explain more about the **General Setup** and **Filter Setup** in the **IP Filter/Firewall Setup** section using the Web Configurator. The Vigor router provides 12 filter sets with 7 filter rules for each set. As a result, there are a total of 84 filter rules for the **Filter Setup**. By default, the Call Filter rules are defined in Filter Set 1 and the Data Filter rules are defined in Filter Set 2.



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

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

DoS defense: Click it to set up the DoS defense facility for detecting and mitigating the DoS attacks. The more details can be found in Chapter 13-A.

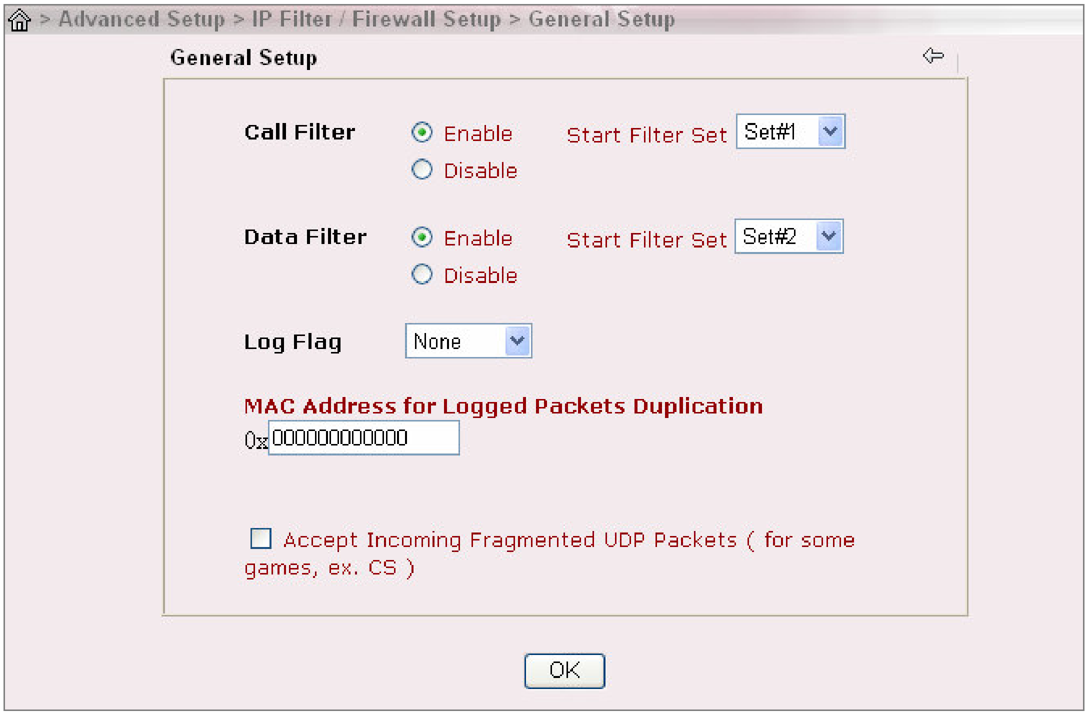
Content Filter: Here provides the capability of blocking inappropriate web sites to protect child in school or at home. The more details can be found in Chapter 13-B.

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

(Set to Factory Default): Click here to restore the filter rules to default values.

13.3 General Setup

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


> Advanced Setup > IP Filter / Firewall Setup > General Setup
General Setup
OK

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

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

Log Flag None

MAC Address for Logged Packets Duplication

0x 000000000000

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

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

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

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

None: The log function is inactive.

Block: All blocked packets will be logged.

Pass: All passed packets will be logged.

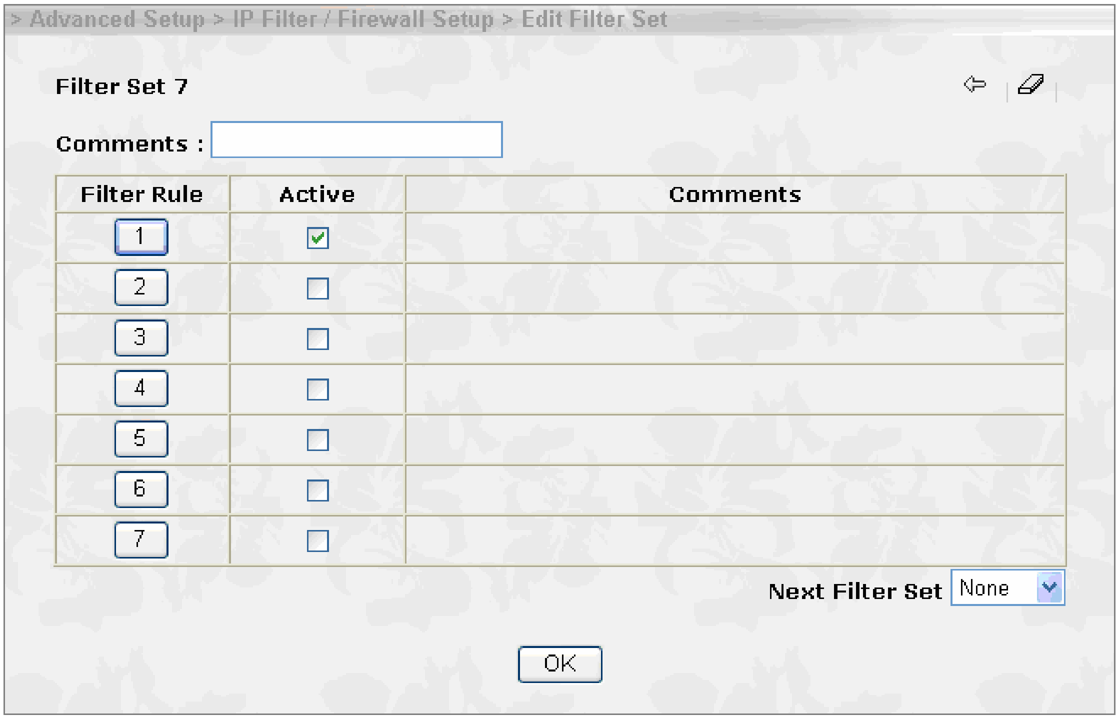
No Match: The log function will record all packets which are matched.

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

MAC Address for Packet Duplication: Logged packets may also be logged to another location via Ethernet. If you want to duplicate logged packets from the router to another network device, you must enter the other devices' MAC

Address (HEX Format). Type “0” to disable the feature. The feature will be helpful under Ethernet environments.

13.4 Editing the Filter Sets



> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set

Filter Set 7

Comments :

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

Next Filter Set: None

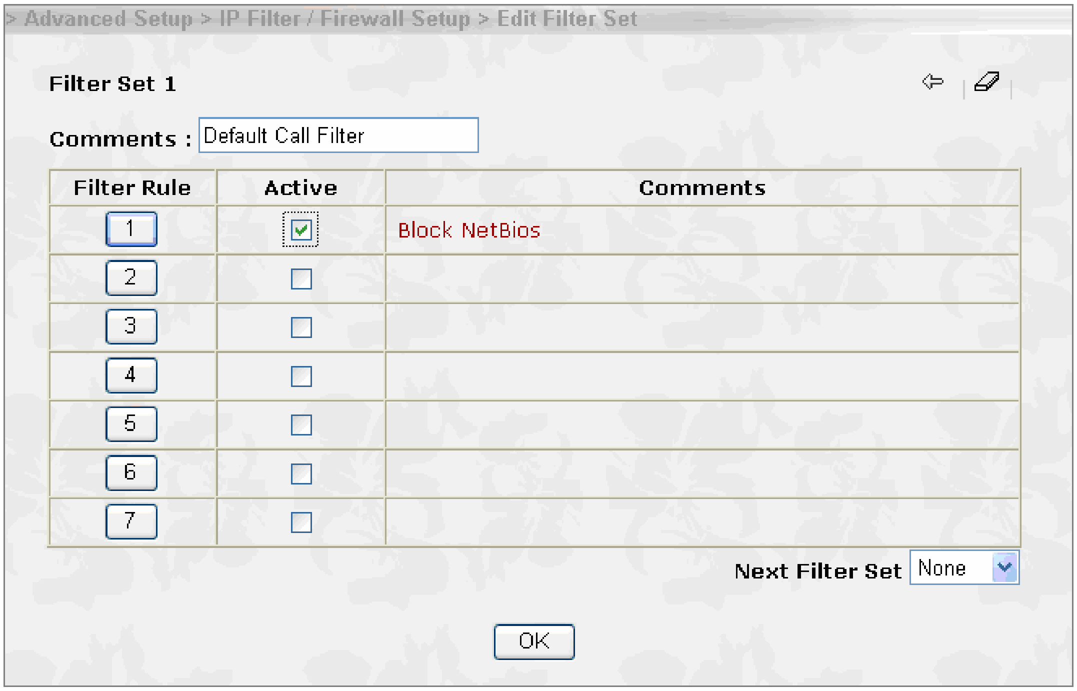
Comments: Enter filter set comments/description. Maximum length is 23 characters.

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

Active: Enable or disable the filter rule.

Next Filter Set: Specifies the next filter set to be linked behind the current filter set. The filters cannot be looped.

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



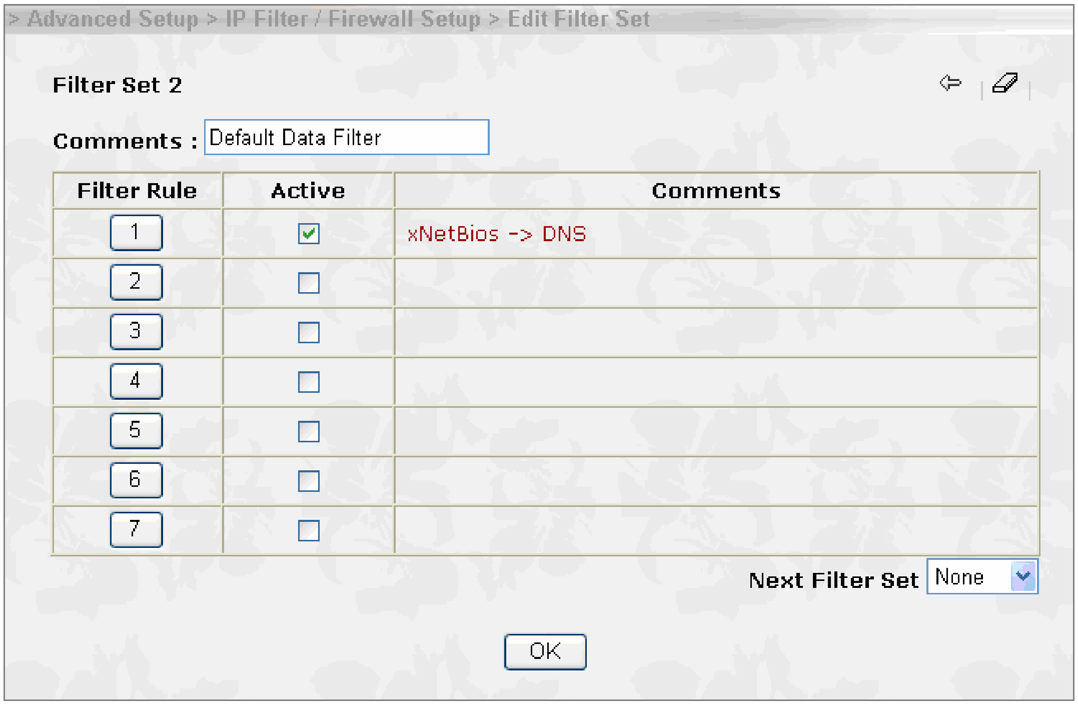
> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set

Filter Set 1

Comments : Default Call Filter

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

Next Filter Set None



> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set

Filter Set 2

Comments : Default Data Filter

Filter Rule	Active	Comments
1	☑	xNetBios -> DNS
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	

Next Filter Set None

13.5 Editing the Filter Rules

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

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

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

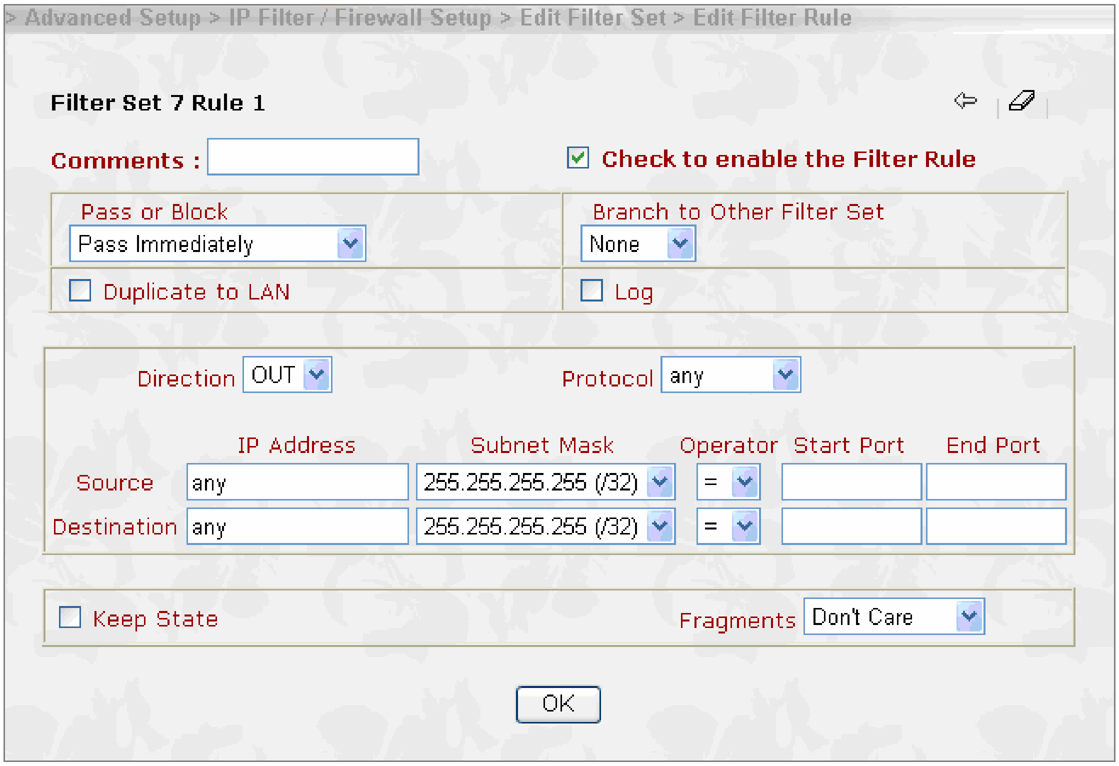
Pass or Block: Specifies the action to be taken when packets match the rule.

***Block Immediately*:** Packets matching the rule will be dropped immediately.

***Pass Immediately*:** Packets matching the rule will be passed immediately.

***Block If No Further Match*:** A packet matching the rule, and that does not match further rules, will be dropped.

***Pass If No Further Match*:** A packet matching the rule, and that does not match further rules, will be passed through.



> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set > Edit Filter Rule

Filter Set 7 Rule 1

Comments :

☑ Check to enable the Filter Rule

Pass or Block: Pass Immediately

Branch to Other Filter Set: None

☐ Duplicate to LAN

☐ Log

Direction: OUT

Protocol: any

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

☐ Keep State

Fragments: Don't Care

Branch to Other Filter Set: If the packet matches the filter rule, the next filter rule will branch to the specified filter set.

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

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

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

<u>For the Data Filter:</u>

IN: Specify the rule for filtering incoming packets.

OUT: Specify the rule for filtering outgoing packets.

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

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

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

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

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

!= : If the **End Port** is empty, the port number is not equal to the value of the

Start Port. Otherwise, this port number is not between the **Start Port** and the **End Port** (including the **Start Port** and **End Port**).

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

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

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

Fragments: Specify a fragmented packets action.

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

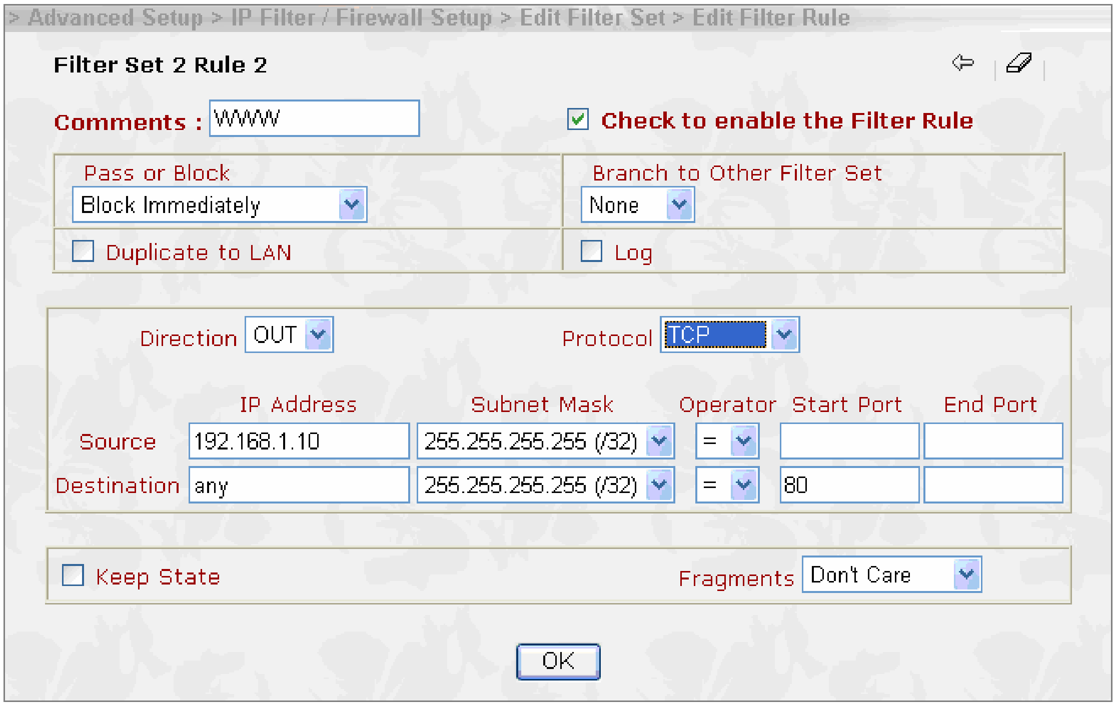
Unfragmented: Apply the rule to unfragmented packets.

Fragmented: Apply the rule to fragmented packets.

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

13.6 An Example of Restricting Unauthorized Internet Services

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


> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set > Edit Filter Rule

Filter Set 2 Rule 2

Comments : WWW

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

☐ Duplicate to LAN

☐ Log

Direction: OUT

Protocol: TCP

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

☐ Keep State

Fragments: Don't Care

Port 80 is the HTTP protocol port number for WWW services.

Supplement A

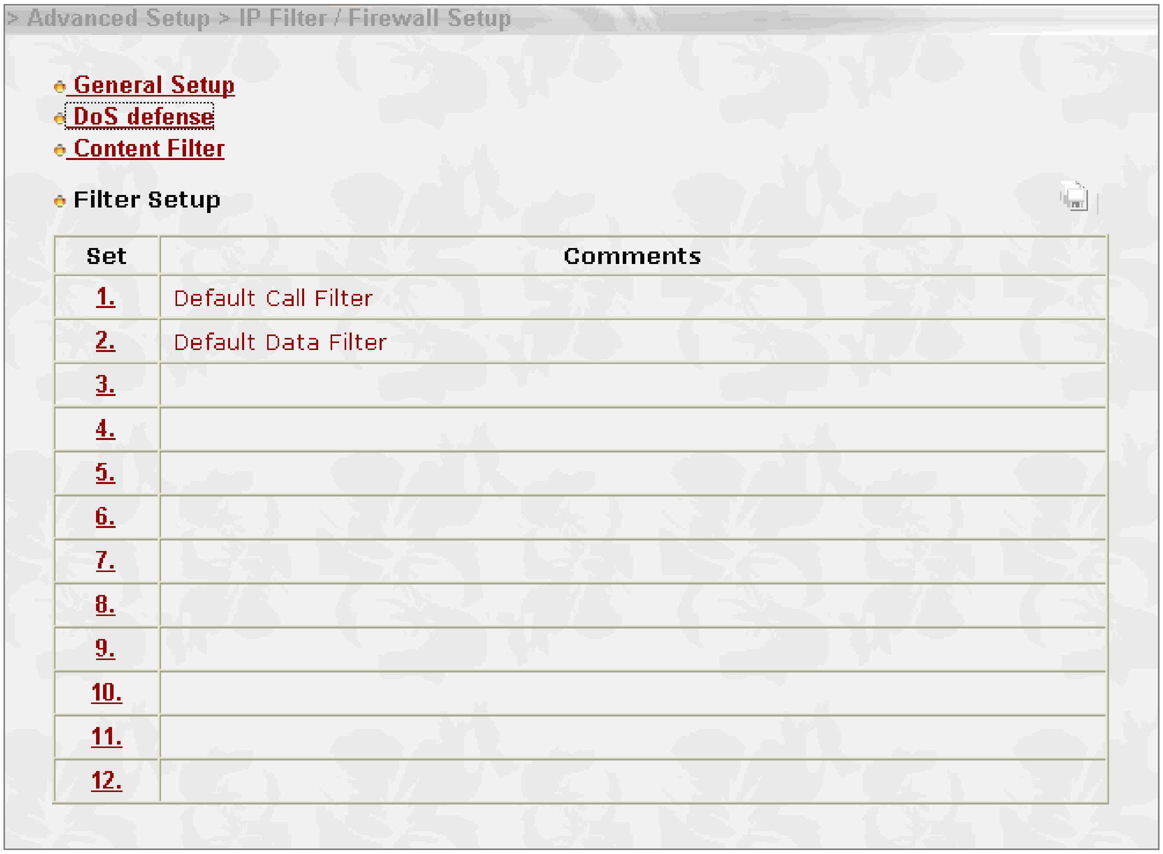
Prevention of Denial of Service Attacks

A.1 Introduction

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

A.2 An Overview of DoS Defense Functionality

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



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

A.3 Configuration

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

Enable DoS Defense: Click the checkbox to activate the DoS Defense Functionality.

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

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

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

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

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

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

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

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

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

Enable Block fraggle Attack: Click the checkbox to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

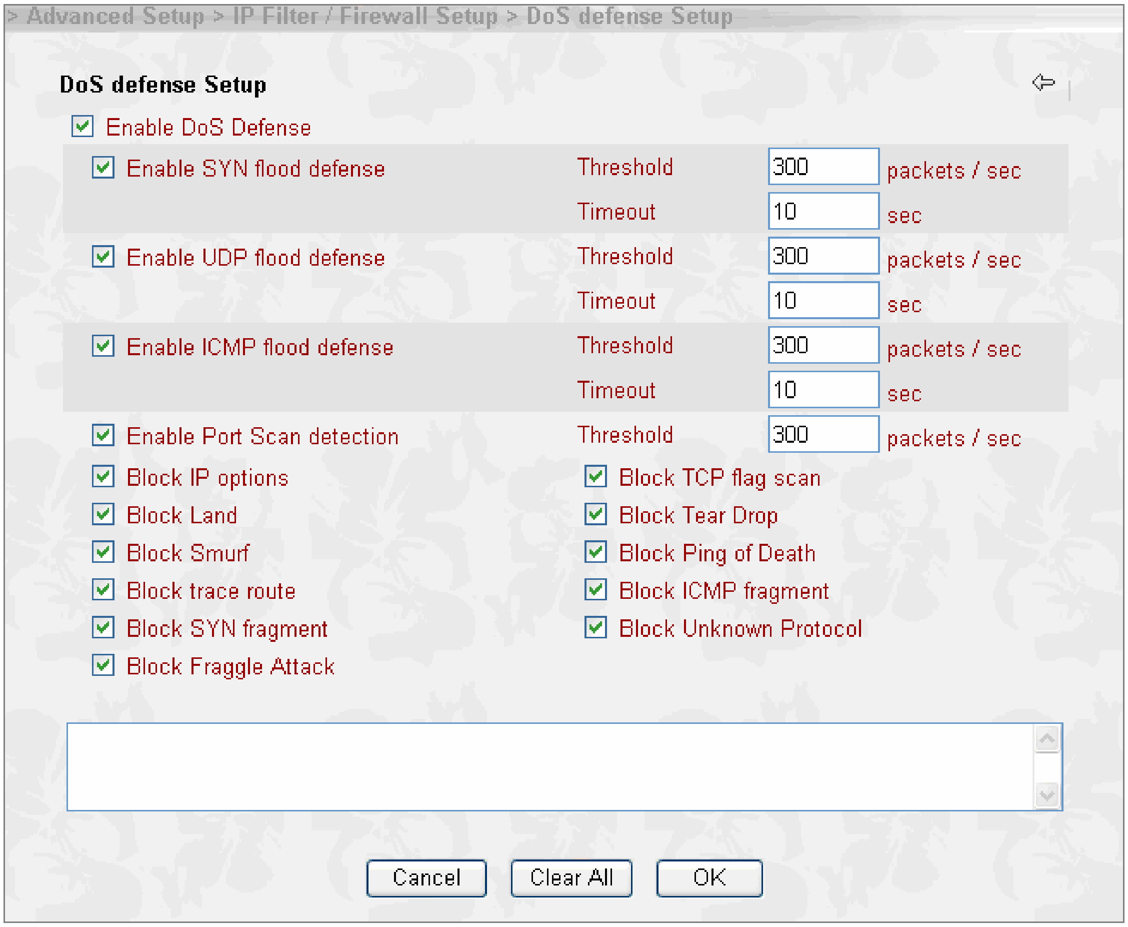
Enable TCP flag scan: Click the checkbox to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include ***no flag scan***, ***FIN without ACK scan***, ***SYN FINscan***, ***Xmas scan*** and ***full Xmas scan***.

Enable Tear Drop: Click the checkbox to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. Any packets realizing this attacking activity will be blocked by the Vigor routers.

Enable Ping of Death: 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.

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

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


> Advanced Setup > IP Filter / Firewall Setup > DoS defense Setup
Cancel
Clear All
OK

DoS defense Setup

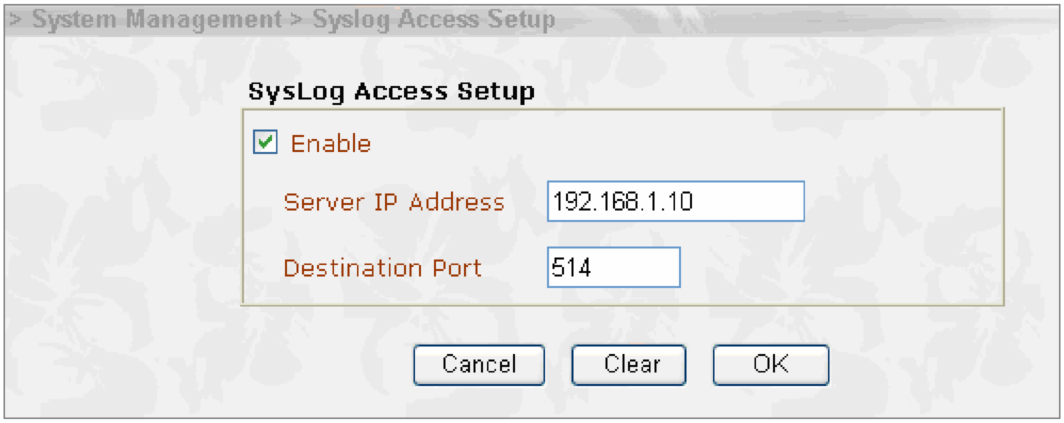
☑ Enable DoS Defense

☑ Enable SYN flood defense	Threshold	300	packets / sec
	Timeout	10	sec
☑ Enable UDP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
☑ Enable ICMP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
☑ Enable Port Scan detection	Threshold	300	packets / sec

☑ Block IP options
☑ Block Land
☑ Block Smurf
☑ Block trace route
☑ Block SYN fragment
☑ Block Fraggle Attack
☑ Block TCP flag scan
☑ Block Tear Drop
☑ Block Ping of Death
☑ Block ICMP fragment
☑ Block Unknown Protocol

A.4 Warning Message

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



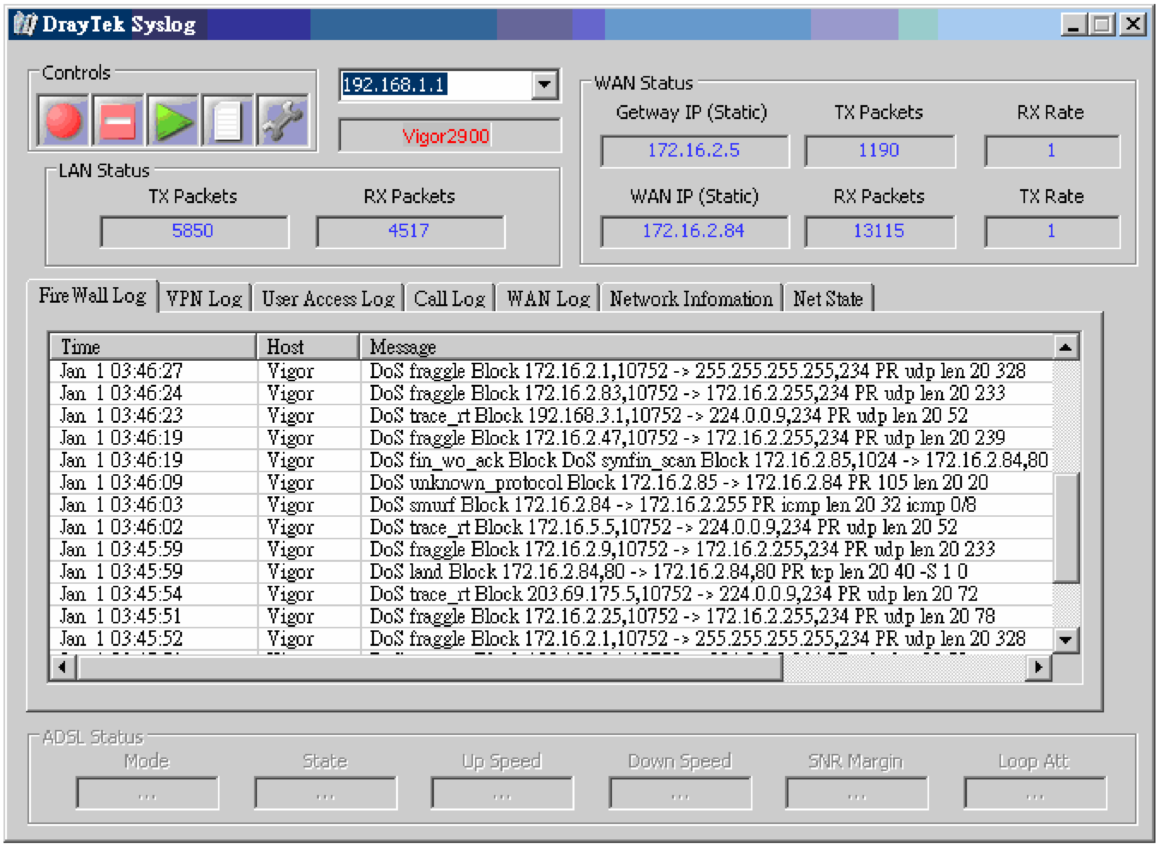
> System Management > Syslog Access Setup

SysLog Access Setup

☑ Enable

Server IP Address: 192.168.1.10

Destination Port: 514



192.168.1.1

Vigor2900

LAN Status

TX Packets	RX Packets
5850	4517

WAN Status

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

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

ADSL Status

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

Supplement B

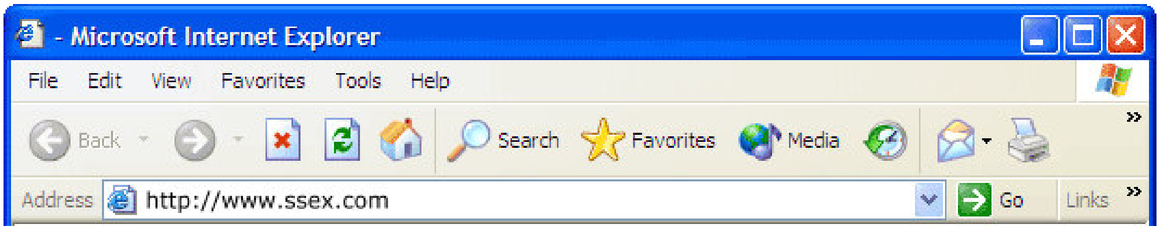
URL Content Filtering

B.1 Introduction

The Internet contains a wide range of materials, some of which may be offensive or even illegal in many countries. Unlike traditional media, the Internet does not have any obvious tools to segregate materials based on URL strings or content. URL content filtering systems are seen as tools that would provide the cyberspace equivalent of the physical separations that are used to limit access to some particular materials. In rating a site as objectionable, and refusing to display it on the user's computer screen, URL content filtering facilities can be used to prevent children from seeing material that their parents find objectionable. In preventing access, the URL content filtering facility acts as an automated version of the convenience-store clerk who refuses to sell adult magazines to high-school students. The URL content filtering facilities are also used by businesses to prevent employees from accessing Internet resources that are either not work related or otherwise deemed inappropriate.

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

B.2 An Overview of URL Content Filtering



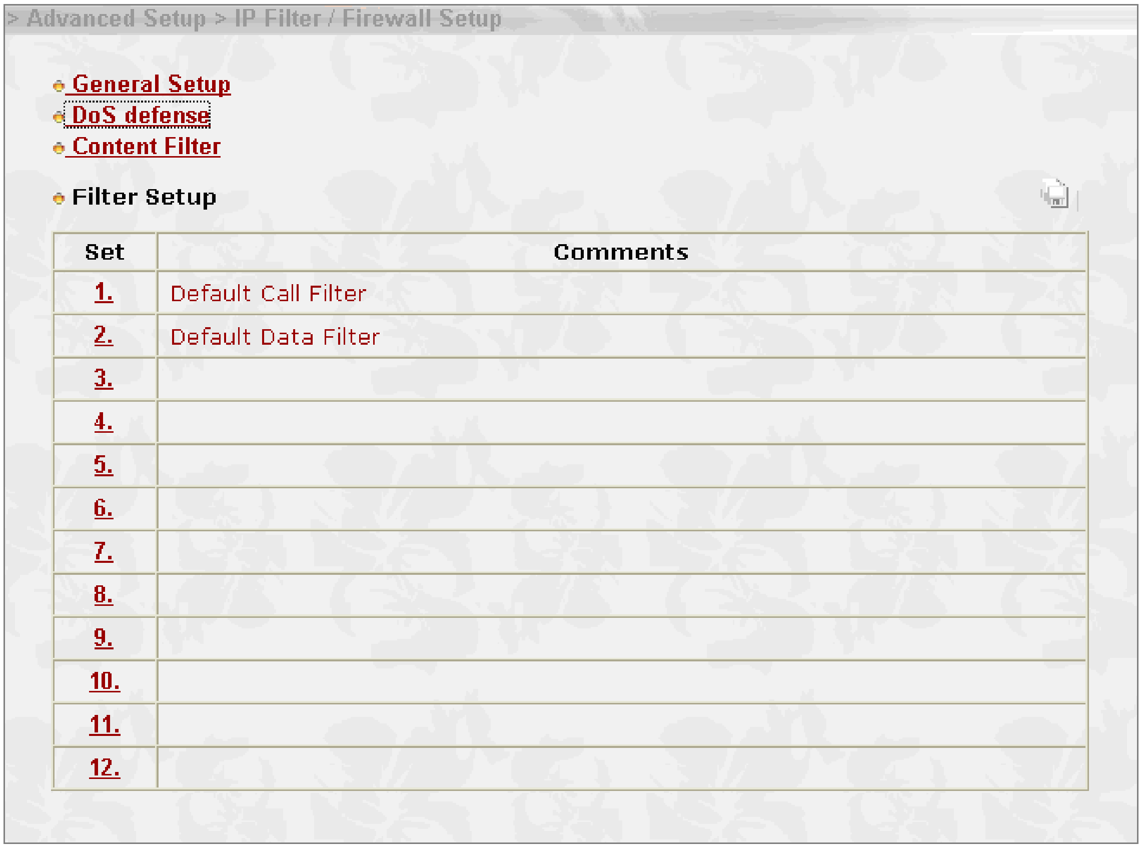
The URL content filtering facility in Vigor routers inspects every URL string in the HTTP request initiated inside against the keyword list. If the entire or part of the URL string (for instance, http://www.ssex.com as shown above) matches any activated keyword, the Vigor router will block its associated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

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

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

B.3 Configuration

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



> Advanced Setup > IP Filter / Firewall Setup

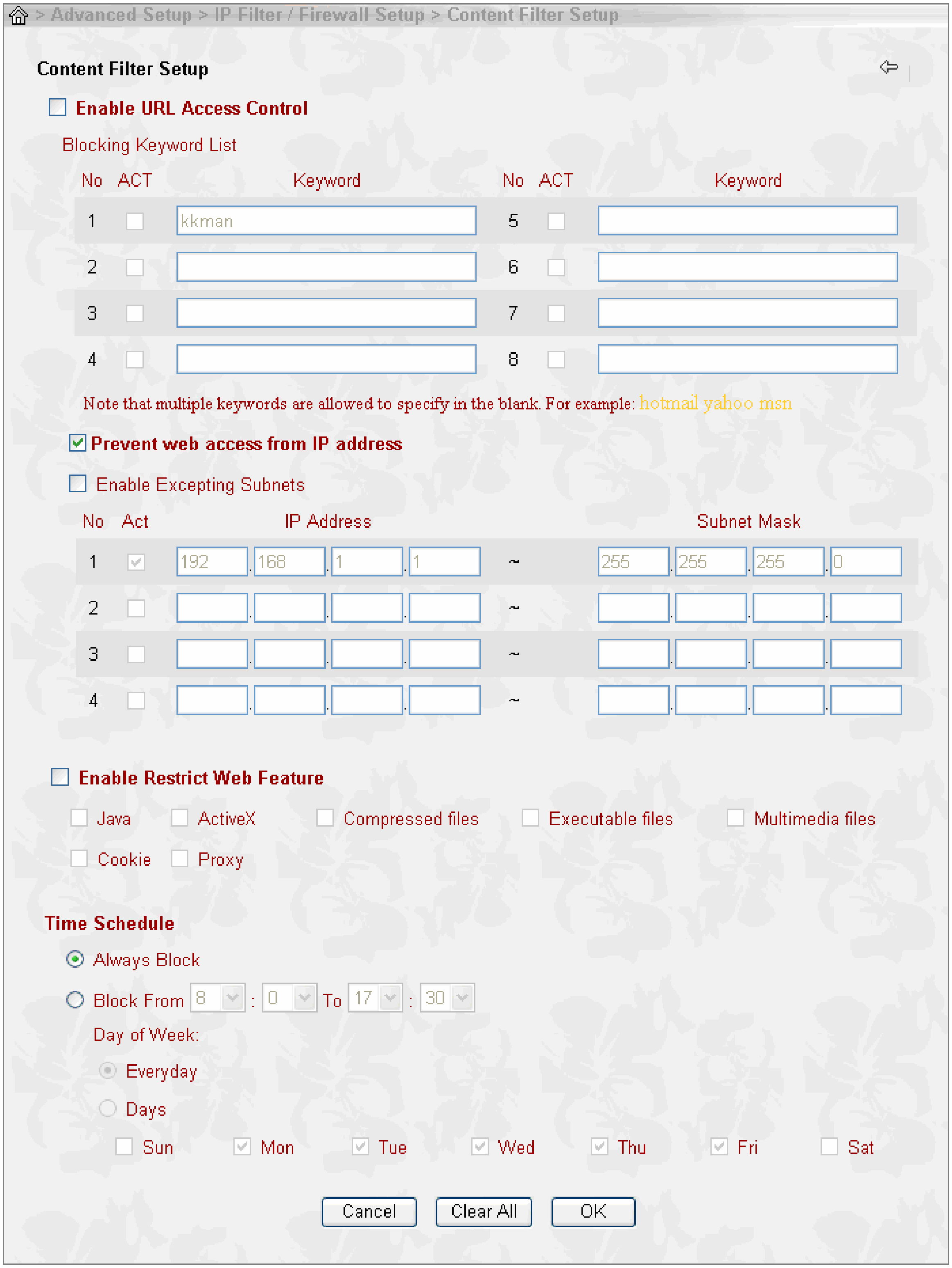
- General Setup
- DoS defense
- Content Filter

Filter Setup

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

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

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



> Advanced Setup > IP Filter / Firewall Setup > Content Filter Setup

Content Filter Setup

☐ **Enable URL Access Control**

Blocking Keyword List

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

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

☑ **Prevent web access from IP address**

☐ Enable Excepting Subnets

No	Act	IP Address		Subnet Mask
1	☑	192 . 168 . 1 . 1	~	255 . 255 . 255 . 0
2	☐	. . .	~	. . .
3	☐	. . .	~	. . .
4	☐	. . .	~	. . .

☐ **Enable Restrict Web Feature**

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

☐ Cookie ☐ Proxy

Time Schedule

● Always Block

○ Block From 8 : 0 To 17 : 30

Day of Week:

● Everyday

○ Days

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

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

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

Example: If you want to filter any website whose URL string contains "sex", "fuck", "gun", or "drug", you should add these words into the frames. Thus, your Vigor router will automatically deny any web surfing that its associated URL string contains any one of the list's keywords. Considering that the user tries to access www.backdoor.net/images/sex /p_386.html, the Vigor router will cut the connection because this website is prohibited. But, the user is able to access the website www.backdoor.net/firewall/forum/d_123.html. Further, the URL content filtering facility also allows you to specify either a complete URL string (e.g., "www.whitehouse.com" and "www.hotmail.com") or a partial URL string (e.g., "yahoo.com") in the blocking keyword list. Accordingly, the Vigor router will identify the forbidden URL and perform the blocking action for these websites by cutting the associated connections.

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

Enable Excepting Subnets: 4 entries are available for users to specify some specific IP addresses or subnets so that they can be free from the *URL Access Control*. To enable an entry, click on the empty checkbox, named as "**ACT**", in front of the appropriate entry. The hook image (√) appears to indicate the entry is active. To disable an entry, click on the hook image (√).

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

***Java*: **Click the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.

***ActiveX*: **Click the checkbox to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.

***Compressed file*: **One checkbox appears giving the choice to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router.

.zip **.rar** **.arj** **.ace** **.cab** **.sit**

To enable it, click on the empty box image and, subsequently, the hook image (√) will appear.

***Executable file*: **Similar to the above function, click the checkbox to enable the Block Executable file function to reject any downloading behavior of the executable file from the Internet. To enable it, click on the empty box image and, subsequently, the hook image (√) will appear. Accordingly, files with the following extensions will be blocked by the Vigor router.

.exe **.com** **.scr** **.pif** **.bas** **.bat** **.inf** **.reg**

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

Cookie: Click the checkbox to activate the Block Cookie transmission. The Vigor router will filter out the cookie transmission from inside to outside world in order to protect the local user's privacy.

Proxy: One checkbox appears giving the choice to activate this function to reject any proxy transmission. To enable it, click on the empty box image and, subsequently, the hook image ( ) will appear.

To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. To enable it, click on the empty box image and, subsequently, the hook image (√) will appear. Accordingly, files with the following extensions will be blocked by the Vigor router.

.mov **.mp3** **.rm** **.ra** **.au** **.wmv**
.wav **.asf** **.mpg** **.mpeg** **.avi** **.ram**

Time Schedule: Specify what time should perform the URL content filtering facility.

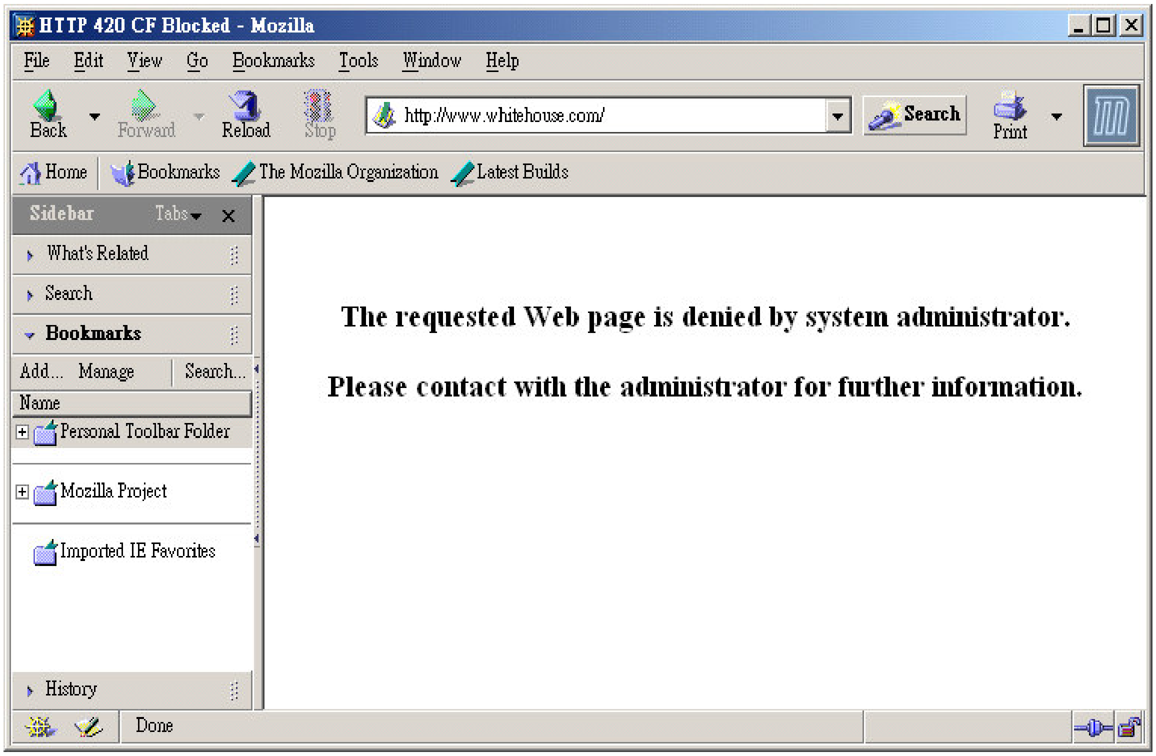
Always Block: Click it so that the URL content filtering facility can be executed on the Vigor router anytime.

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.

B.4 Warning Message

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

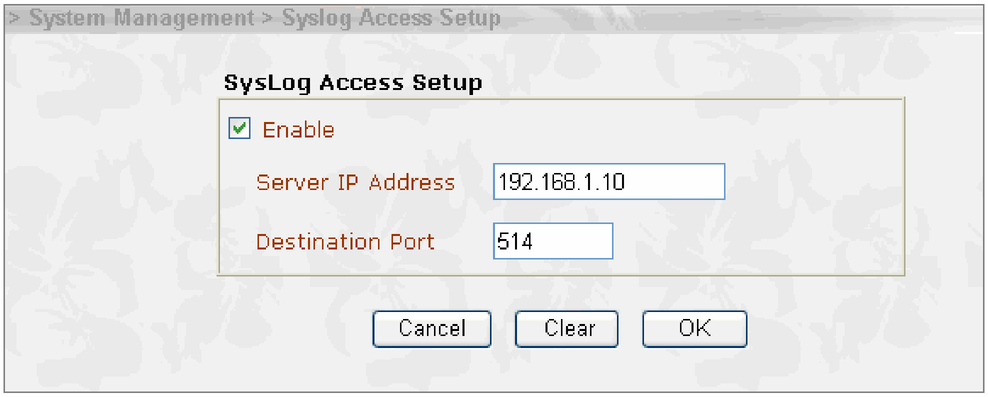


http://www.whitehouse.com/

The requested Web page is denied by system administrator.

Please contact with the administrator for further information.

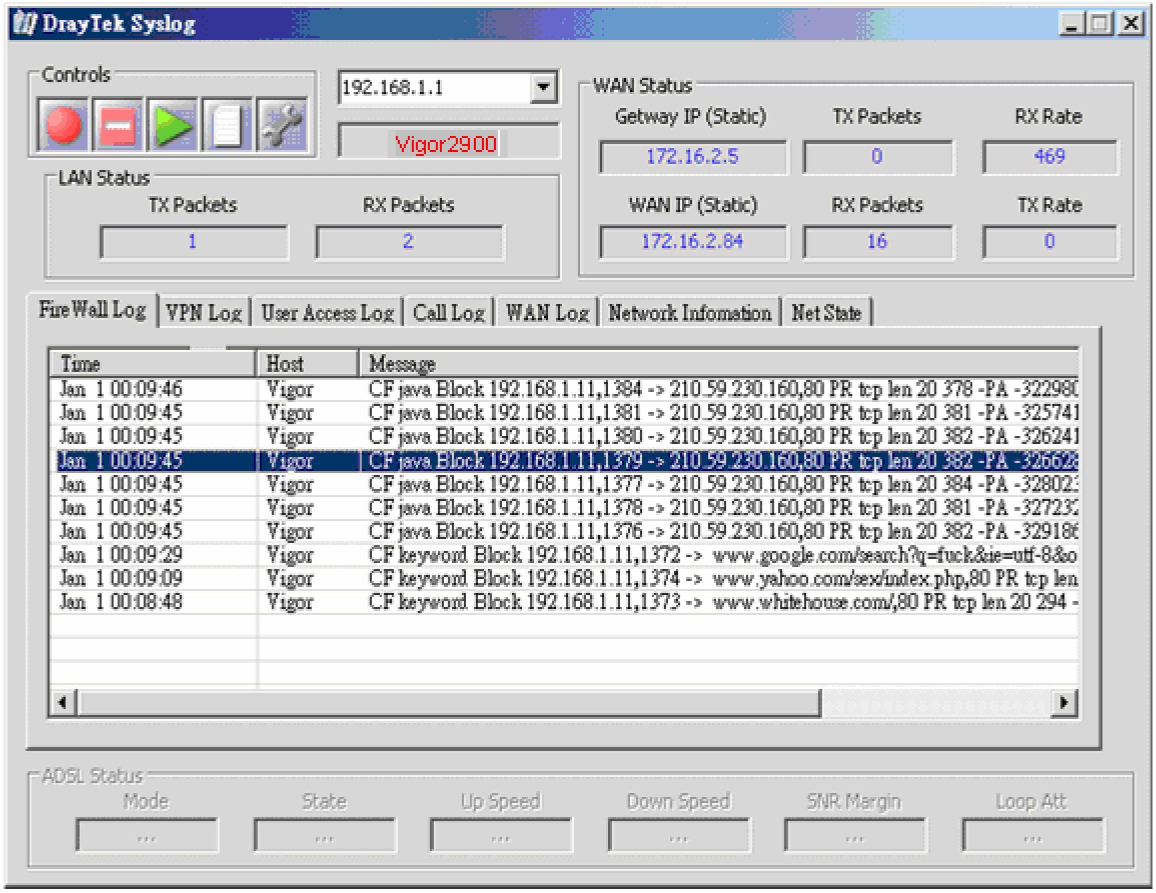
Also, the warning message will be automatically sent to the syslog client after you enable the syslog function. The administrator can setup the syslog client in the **Syslog Setup** by using Web Configurator. Thus, the administrator can view the warning messages from the **URL Content Filtering** functionality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



☑ Enable

Server IP Address 192.168.1.10

Destination Port 514



LAN Status

TX Packets: 1

RX Packets: 2

WAN Status

Getway IP (Static): 172.16.2.5

TX Packets: 0

RX Rate: 469

WAN IP (Static): 172.16.2.84

RX Packets: 16

TX Rate: 0

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

Appendix of Chapter 13
Log Event Disposition for IP Filter / Firewall Setup

Appendix: Log Event Disposition

The syslog messages in the Vigor routers consist of three parts: ***Time*** field, ***Host*** field and ***Message body*** filed. Time field states the time epoch when an event happens. Host field stands for describing the device that sends the log message. By default, Vigor routers fill this field with “Vigor”. The Message body field describes what kind of events occurs and its associated information, say source/destination IP addresses, source/destination port number, and so on.

Basically, all firewall-related messages in Vigor routers can be classified into five categories. They are Startup, Alarm, Authentication, Access, and URL filtering messages. In the following, we will give a full detail of their formats or syntaxs.

1. Startup message

System startup log: The Vigor router will send a "SYSBOOT" message to the specified management host whenever system starts up successfully and the connection to the syslog utility on management host is available.

2. Alarm message

ARP alarm messages: Possible messages are described below.

“Arp address mismatch - Ethernet destination address doesn't match ARP target adress”.

“Arp address mismatch - Ethernet source address doesn't match ARP sender address”.

"Directed ARP request - ARP request directly directed to a host (not broadcasted)".

"ARP address mismatch - Ethernet source address doesn't match ARP sender address".

"LAN IP conflict - lan ip conflict with the one whose MAC is XX:XX:XX:XX: XX:XX, please contact with the administrator".

DoS attack detection messages**:** When your Vigor router suffers from some type of Denial of Service (DoS) attacks, the Vigor router will activate the defense mechanism and in turn send the corresponding log message for administrator to trace what happens. According to protocol type of received DoS-attack packets, possible messages are described below.

For TCP/UDP packets, the message is shown as

DoS *type action src_addr*[,*src_port*] -> *dst_addr*[,*dst_port*] [CD *option*] PR *protocol* len *ipheader iplen* [-*tcpflag th_seq th_ack*]

For ICMP packets, the message is

DoS *type action* *src_addr* -> *dst_addr* [CD *option*] PR icmp len *ipheader iplen* icmp *icmp_type*/*icmp_code*

For other protocol packets, the message is illustrated as

DoS *type action* *src_addr* -> *dst_addr* [CD *option*] PR *protocol* len *ipheader iplen*

where

DoS/PR/CD: stand for Denial of Service/Protocol/IP option CoDe , respectively,

type: indicate the reason why a packet is dropped. The reason can be:

ip_option: belonging to bad ip_option attack,

Portscan: belonging to portscan behavior,

icmp_flood (*timeout value*): belonging to the ICMP flooding attack (notice that the timeout value appears for the setting of the blocking period.),

syn_flood (*timeout value*): belonging to the TCP SYN flooding attack (the timeout value also be displayed for the setting of the blocking period.),

udp_flood Block (*timeout value*): belonging to the UDP flooding attack (the timeout represents the blocking period.),

tcp_short_packet: saying an attack which uses a TCP packet with too short length,

land: indicating a land attack,

syn-fragment: representing a type of attacks which uses a TCP SYN packet with “more fragemnt” flag set,

fin_wo_ack: saying an attack issued by a TCP packet with flag FIN set without ACK set,

synfin_scan: similar to above case, representing an attack by using a TCP packet with flag SYN and FIN set,

xmas_scan: indicating a TCP xmas scan attack, *full_xmas*: indicating a TCP full xmas scan attack,

no_flags: saying an attack which employs a TCP packet without any flag set,

teardrop: indicating a teardrop attack,

fraggle: saying a fraggle attack,

teardrop_mod: representing a teardrap modified attack,

trace_rt: showning a packet to perform the trace route,

smurf : indicating a smurf attack,

icmp_fragment: being an attack activated by a ICMP packet with more fragment set,

pingofdeath: indicating a ping of death attack, *unknown_protocol*: being a type of attacks which sends a packet with unknown protocol field in the IP header,

action: indicate the operation of your Vigor router in a response to an attack. The action could be "Block", if an attacking packet is dropped, or " " only for information.

src_addr: be the source IP address of that packet.

src_port: be the source port number of that packet.

dst_addr: be the destination IP address of the packet.

dst_port: be the destination port number of that packet.

option: be the ip option value consisting of the following cases:

no: No Option,

eol: End of Option list,

rr: Recod Route,

ts: Timestamp,

lsr: Loose Source Routing,

ssr: Strict Source Routing,

si: Stream Identifier,

ra: Router Alert,

dbs: DoD Basic Security,

des: DoD Extended Security,

protocol : indicate the protocol number and may contain the protocol name, such as icmp, tcp, or udp.

ipheader: represent the IP header length. For a IP packet without option fields, this value is 20.

iplen: be the value of length field in the IP header.

tcpflag: indicate the TCP flag field and may contain zero or more than one characters which are defined as follows.

'A': ACK,

'R': RST,

'S': SYN,

'F': FIN,

'U': URG,

'P': PUSH,

th_seq: indicate the TCP sequence number of the packet.

th_ack: be the TCP acknowledge number of the packet.

icmp_type: be the type field in ICMP packet header.

icmp_code: be the code field in the ICMP packet header.

FTP PORT and PASV commands messages: Possible messages are described below.

FTP bounce attack *disposition src_addr,src_port -> dst_addr,dst_port cmd arg* Add data channel for FTP *src_addr,src_port -> dst_addr,dst_port cmd arg*

where

disposition: The default disposition is " Block" which means drop without response to sender.

src_addr: be the source IP address of that packet.

src_port: be the source port number of that packet.

dst_addr: be the destination IP address of the packet.

dst_port: be the destination port number of that packet.

cmd: " PORT" or "PASV"

arg: Arguments(ip address and port) of PORT and PASV commands.

3. Authentication message

***Authentication log*:** Any attempt to authenticate at an Administrative interface will be logged in the syslog utility with the following syntax.

ADMIN *if src_addr,src_port -> dst_addr,dst_port* PR 6(tcp) len *ipheader iplen -tcpflag th_seq th_ack*

where

ADMIN and ***PR*** stand for administaration and protocol.

if: can be "lan" (from a lan port) or "wan" (from wan port) interface,

src_addr: be the source IP address of that packet,

src_port: be the source port number of that packet and may contain service name (for example, ftp, telnet, smtp, www, and so on.),

dst_addr: be the destination IP address of the packet,

dst_port: be the destination port number of that packet and may contain service name (e.g. ftp, telnet, smtp, www, and so on.).

ipheader: represent the length of the IP header. For a IP packet without option field, this value is 20.

iplen: be the value of length field in the IP header.

tcpflag: indicate the TCP flag field and may contain zero or more than one characters which are defined as follows,

'A': ACK,

'R': RST,

'S': SYN,

'F': FIN,

'U': URG, and

'P': PUSH.

th_seq: be the TCP sequence number of the packet, and

th_ack: represent the TCP acknowledge number of the packet.

In addition to above information, we also provide other messages to state the success or failure of authentication at an Administration interface. Basically, there are four possible messages.

"AUTH Success (web)": indicate the success of authentication when you access the web configurator.

"AUTH Fail (web), password incorrect": indicate the failure of authentication and display the password is incorrect if you access the web configurator.

"AUTH Success (ftp)": indicate the success of authentication for remote firmware upgrade via ftp functionality.

"AUTH Fail (ftp), password incorrect": represent the failure of authentication and display that the required password is incorrect if you intend to use ftp facility to upgrade firmware remotely.

4. Access message

With regarding to any access request through the Vigor router, the Vigor router will log its associated access message according on the protocol and fragment types of the inspected packets. Possible messages are described as follows.

For fragemented packets, the message format is:

hour:*min*:*sec*.*ms* *if* @Group:Rule=*group*:*rule* *disposition* *src_addr* -> *dst_addr* PR *protocol* len *ipheader* *iplen* frag [*ip_mf*][*ip_df*]*f_len*@*offset*[K-S][K-F][*dir*]

For TCP and UDP packets, the message format is shown below:

hour:*min*:*sec*.*ms* *if* @Group:Rule=*group*:*rule* *disposition* *src_addr*[,*src_port*] -> *dst_addr*[,*dst_port*] PR *protocol* len *ipheader* *iplen*[-*tcpflag* *th_seq* *th_ack* *th_win*][K-S][K-F][*dir*]

For ICMP packets, the message format is defined based on the following syntax.

hour:*min*:*sec.ms* *if* @Group:Rule=*group*:*rule* *disposition* *src_addr* -> *dst_addr* PR 1(icmp) len *ipheader* *iplen* icmp *icmp_type*/*icmp_code*[for *ic_src_addr*,*ic_src_port* - *ic_dst_addr*,*ic_dst_port* PR *ic_protocol* len *ic_ipheader* *ic_iplen*][K-S][K-F][*dir*]

For other protocol type packets, the message format is defined as follows.

hour:*min*:*sec.ms* *if* @Group:Rule=*group*:*rule* *disposition* *src_addr* -> *dst_addr* PR *protocol* len *ipheader* *iplen* [K-S][K-F][*dir*]

where

hour*:*min*:*sec*:*ms: stand for the system up time in hour: minute: second: microsecond unit,

if: its value can be "lan" (from either lan or wan port), "wan" (from ISDN port), "dialin" (from VPN tunnel), or "-".

group: be either -1 or any positive number,

rule: can be either -1 or any positive number,

disposition:

'n': indicate that inspected packet doesn't match any pre-defined rule and thus is dropped without any response to the sender,

'p': indicate that the packet matches a filter rule and subsequently is passed through the Vigor router,

'b': represent that packet matches a filter rule but is dropped without any response to the sender.

src_addr: be the source IP address of that packet.

src_port: be the source port number of that packet and may contain service name (for instance, ftp, telnet, smtp, www, and so on.).

dst_addr: be the destination IP address of the packet.

dst_port: be the destination port number of that packet and may contain service name (for example, ftp, telnet, smtp, www, and so on.).

protocol: indicate the protocol number and may contain the protocol name, such as ip, igmg, icmp, tcp, or udp. eg: 17(udp).

ipheader: represent the IP header length. For a IP packet without option fields, this value is 20.

iplen: be the value of length field in the IP header.

ip_mf: it will be filled with “+” if More Fragement is set, else this field is empty.

ip_df: it will filled with “-” if Don't Fragement is set, else this field is empty.

f_len: indicate the length of the data payload, e.g. Iplen-ipheader.

offset: show the fragement offset.

tcpflag: it is the TCP flag field and may contain zero or more than one characters defined below.

'A': ACK,

'R': RST,

'S': SYN,

'F': FIN,

'U': URG, and

'P': PUSH.

th_seq: be the TCP sequence number of the packet.

th_ack: indicate the TCP acknowledge number of the packet.

th_win: show the TCP window size.

icmp_type: be the type field in the ICMP packet header.

icmp_code: show the code field in the ICMP packet header.

ic_src_addr: be the source IP address of the packet that triggers this ICMP packet.

ic_src_port: be the source port number of that packet that triggers this ICMP packet.

ic_dst_addr: be the destination IP address of the packet that triggers this ICMP packet.

ic_dst_port: be the destination port number of that packet.that triggers this ICMP packet.

ic_protocol: show the protocol number of the packet that triggers this ICMP packet.

ic_ipheader: indicate the IP header length of the packet that triggers this ICMP packet.

ic_iplen: be the value of length field in IP header of the packet that triggers this ICMP packet.

dir: can be "IN" (an incoming filter rule is matched) or "OUT" (an outgoing filter rule is matched)

5. URL Filtering message

The URL filtering facility has been employed in Vigor routers to inspect each outgoing HTTP request. Once the HTTP request issued by a local user is not allowed by the administrator, the Vigor router will prohibit the associated website (specified by its URL string) surfing and in turn send a warning page to the user's browser (i.e. IE or Netscape). In addition, a syslog message is also generated to appear at the syslog utility. The syslog message may have following formats:

For an inspected HTTP request matching a user pre-defined keyword (a URL keyword or a URL string), the syslog message format is shown below:

CF *type* Block *src_addr*[,*src_port*] -> *url*[,*dst_port*] PR tcp len *ipheader iplen* [-*tcpflag th_seq th_ack*]

For other HTTP requsts, such as an attempt to download java/ActiveX object, proxy, cookie, compressed files, multimedia files, or any executable files, that are blocked by Vigor router, the syslog message will appear according to the following syntax:

CF *type* Block *src_add*[,*src_port*] -> *dst_addr*[,*dst_port*] PR tcp len *ipheader iplen*

where

type: indicate what kind of reasons to deny the HTTP request by the Vigor router. All possible reasons are listed below.

keyword: indicate that the denied HTTP request matches a user pre-defined URL keyword.

ip: indicate that the blocked HTTP request appears in the IP-address form.

java: indicate that the blocked HTTP request attepmts to download java object code.

activeX: indicate that the prohibited HTTP request attemps to download active-X object.

proxy: indicate that the denied HTTP request is destined to a proxy server.

cookie: indicate that the blocked HTTP request will bring cookie information within it.

zip: indicate that the blocked HTTP request attempts to download a compressed file.

mms: indicate that the denied HTTP request attempts to download a multimedia file.

exe: indicate that the blocked HTTP request attempts to download an executable file.

url: be the destination website (specified by the url form) of the HTTP request.

src_addr: be the source IP address to issue the specific HTTP request.

src_port: be the source port number to initiate the specific HTTP request.

dst_addr: be the destination IP address of the destined website.

dst_port: be the destination port number of the destined website.

ipheader: be the IP header length. For a IP packet without option fields, this value is 20.

iplen: be the value of length field in the IP header.

tcpflag: be the TCP flag field and may contain zero or more than one characters whose meanings are defined below:

'A': ACK,

'R': RST,

'S': SYN,

'F': FIN,

'U': URG, and

'P': PUSH.

th_seq: be the TCP sequence number of the inspected packet.

th_ack: be the TCP acknowledge number of the inspected packet.

Chapter 14

VPN and Remote Access Setup

14.1 Introduction

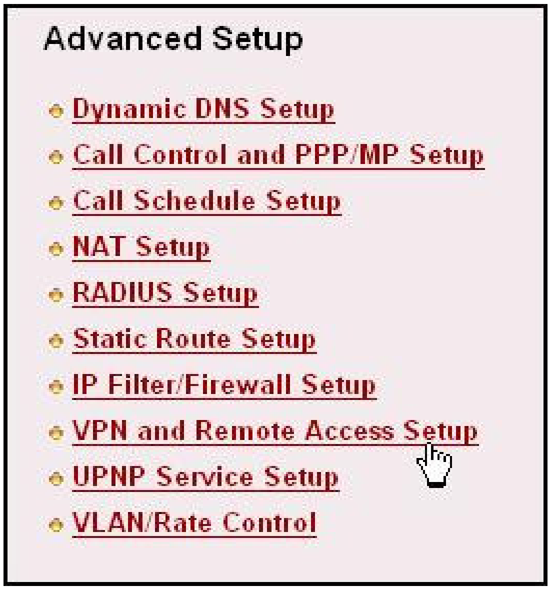
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private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

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

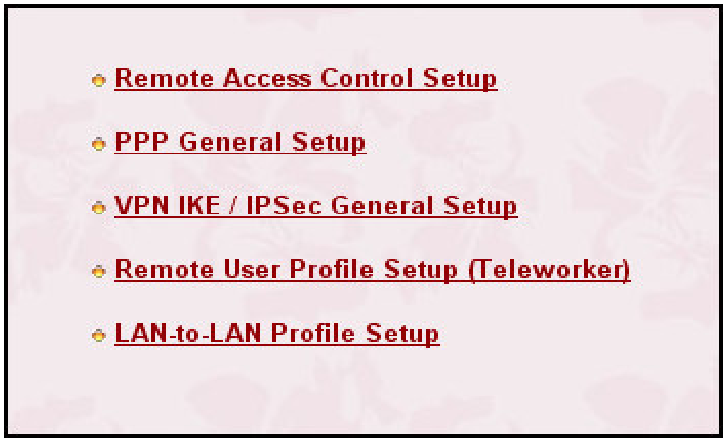
The VPN technology employed in the Vigor routers supports Internet-industry standard to provide customers with interoperable VPN solutions, such as Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP).

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

Advanced Setup > VPN and Remote Access Setup



The **VPN and Remote Access Setup** has five main functions, as shown below. You may set up **Remote Access Control**, **PPP**, **VPN IKE/IPSec**, **Remote Dial-in**, and **LAN-to-LAN Profile** on demand.


Remote Access Control Setup
PPP General Setup
VPN IKE / IPSec General Setup
Remote User Profile Setup (Teleworker)
LAN-to-LAN Profile Setup

The **Remote Access Control Setup** allows you to enable each type of VPN service or disable it for VPN pass-through purpose. For example, you can enable IPSec and L2TP VPN service on your router and disable PPTP VPN service if you intend running a PPTP server inside your LAN. Further, you also can enable or disable the ISDN remote access including remote dial-in and LAN-to-LAN access.

Use the **PPP General Setup** to configure your router's PPP authentication method as well as IP assignment range for remote dial-in user. This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec, and ISDN-based remote access. .

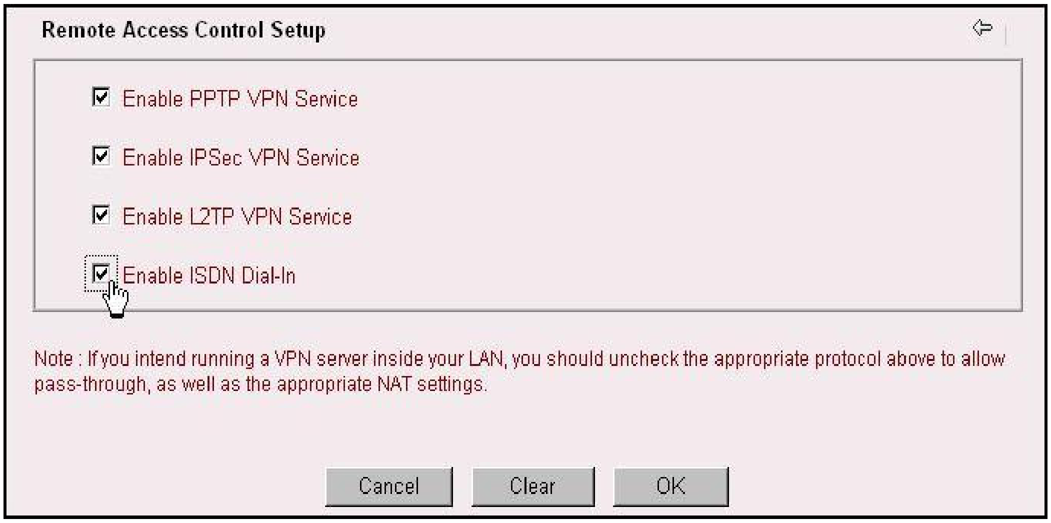
The **VPN IKE / IPSec General Setup** let you configure a common Pre-shared key and security method for remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address.

Use **Remote User Profile Setup(Teleworker)** to create dial-in user accounts. Vigor router supports three types of dial-in methods, PPTP, L2TP, and L2TP over IPSec and ISDN. The PPTP VPN connection is compatible with all Windows platforms which have built-in PPTP protocol. The L2TP and L2TP over IPSec are compatible with Window 2000 and XP.

Use **The LAN-to-LAN Profile Setup** to create profiles for LAN to LAN VPNs. The Vigor router supports four types of LAN-to-LAN VPN, IPSec Tunnel, PPTP, L2TP, and L2TP over IPSec and ISDN. You can establish simultaneously up to 32 VPN tunnels including remote dial-in users.

14.2 Remote Access Control Setup

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



☑ Enable PPTP VPN Service

☑ Enable IPSec VPN Service

☑ Enable L2TP VPN Service

☑ Enable ISDN Dial-In

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

14.3 PPP General Setup

PPP/MP Protocol

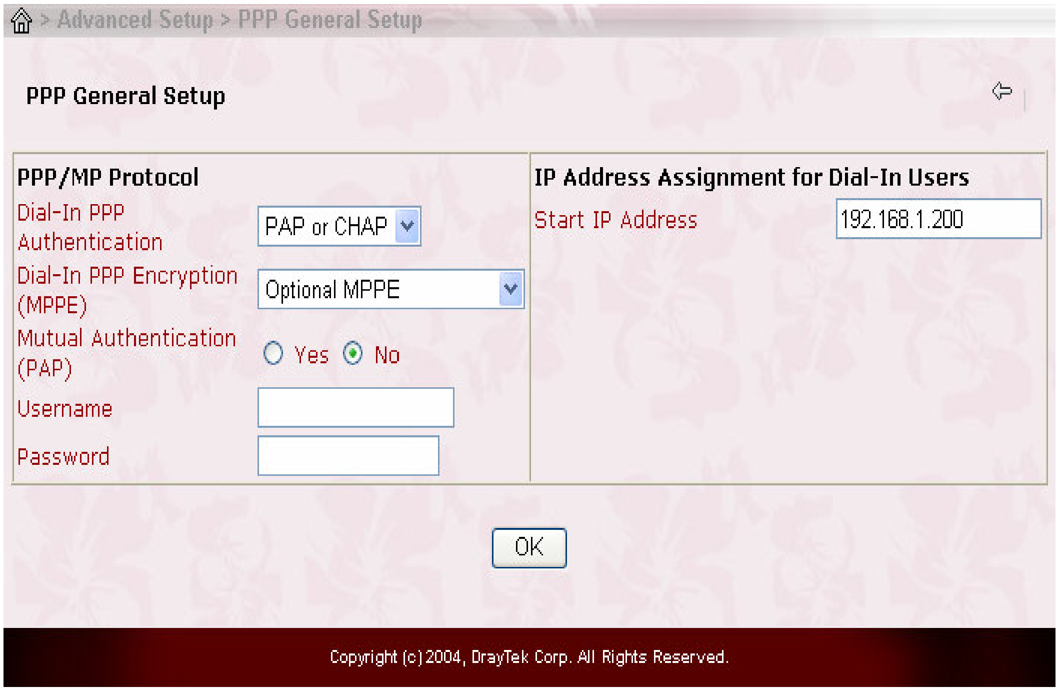
Dial-In PPP Authentication:

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


> Advanced Setup > PPP General Setup
PPP General Setup
OK
Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

PPP/MP Protocol

Dial-In PPP Authentication	PAP or CHAP
Dial-In PPP Encryption (MPPE)	Optional MPPE
Mutual Authentication (PAP)	○ Yes ● No
Username	
Password	

IP Address Assignment for Dial-In Users

Start IP Address	192.168.1.200

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

Username: Specify the username for the purpose of the Mutual Authentication.

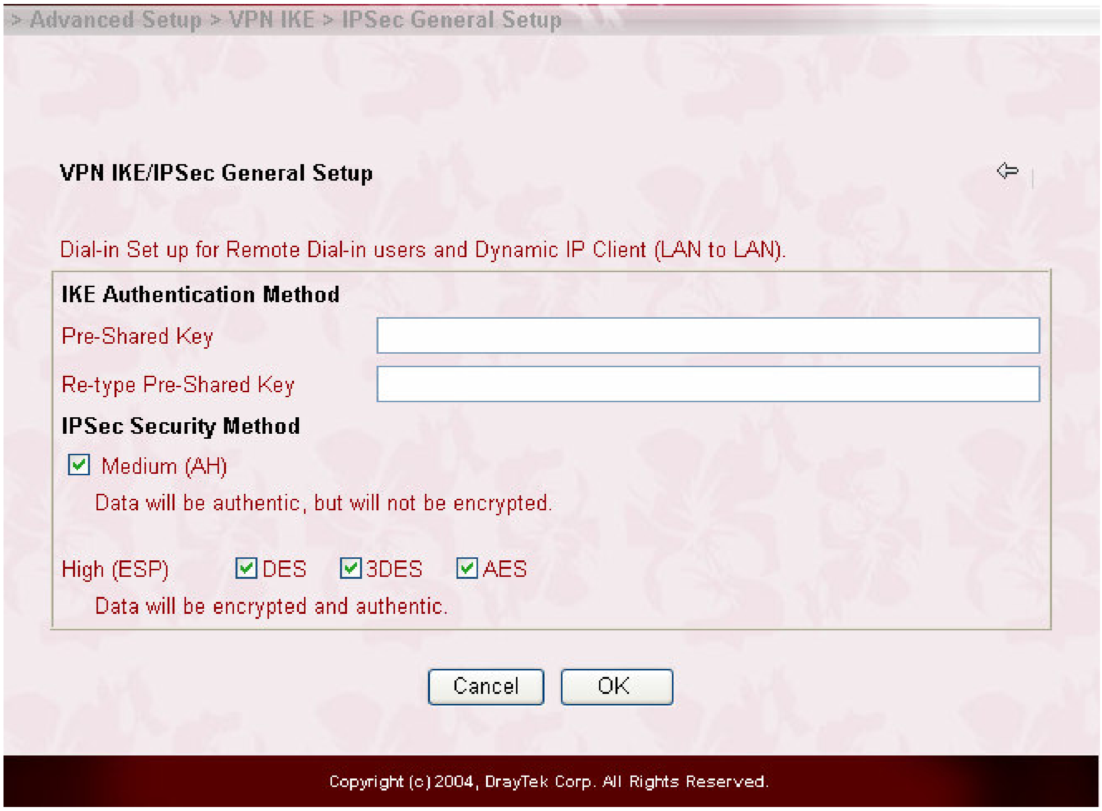
Password: Specify the password for the purpose of the Mutual Authentication.

IP Address Assignment for Dial-In Users

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

14.4 VPN IPSec / IKE General Setup

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


> Advanced Setup > VPN IKE > IPSec General Setup

VPN IKE/IPSec General Setup

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

IKE Authentication Method

Pre-Shared Key

Re-type Pre-Shared Key

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

Cancel
OK
Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

IKE Authentication Method: 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: Select allowed IPSec security methods.

***Medium* (*AH*):** Data will be authenticated, but not be encrypted. By default, this option is active.

***High* (*ESP*):** Data will be encrypted and authenticated. Herein, we support DES, 3DES, and AES encryption methods. By default, these methods are available to support.

14.5 Creating an Access Account for a Remote Dial-in User

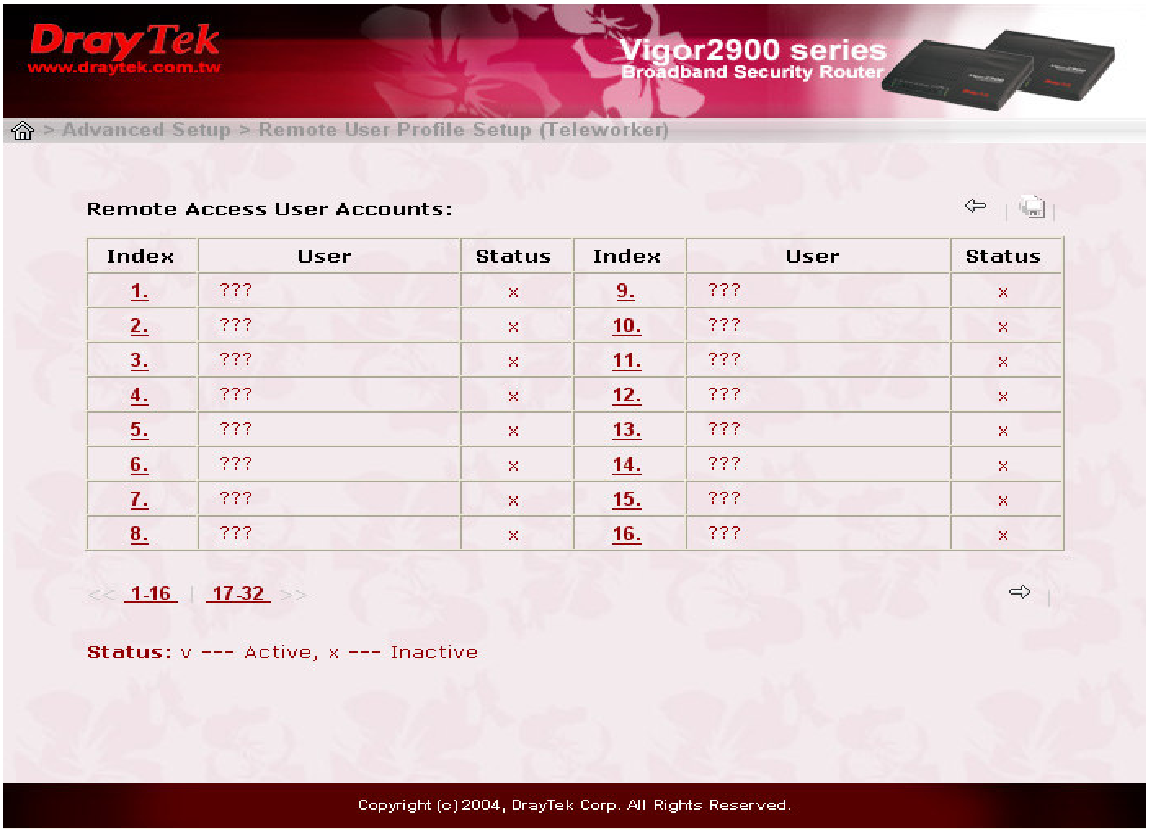
After completing the general setup, you must create an access account for each remote dial-in user. The router provides 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the *Remote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

(Set to Factory Default): Click here to clear all dial-in user accounts.

User: Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

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

Index: Click the index number to open an individual setup page for a dial-in user account, as shown below.



> Advanced Setup > Remote User Profile Setup (Teleworker)

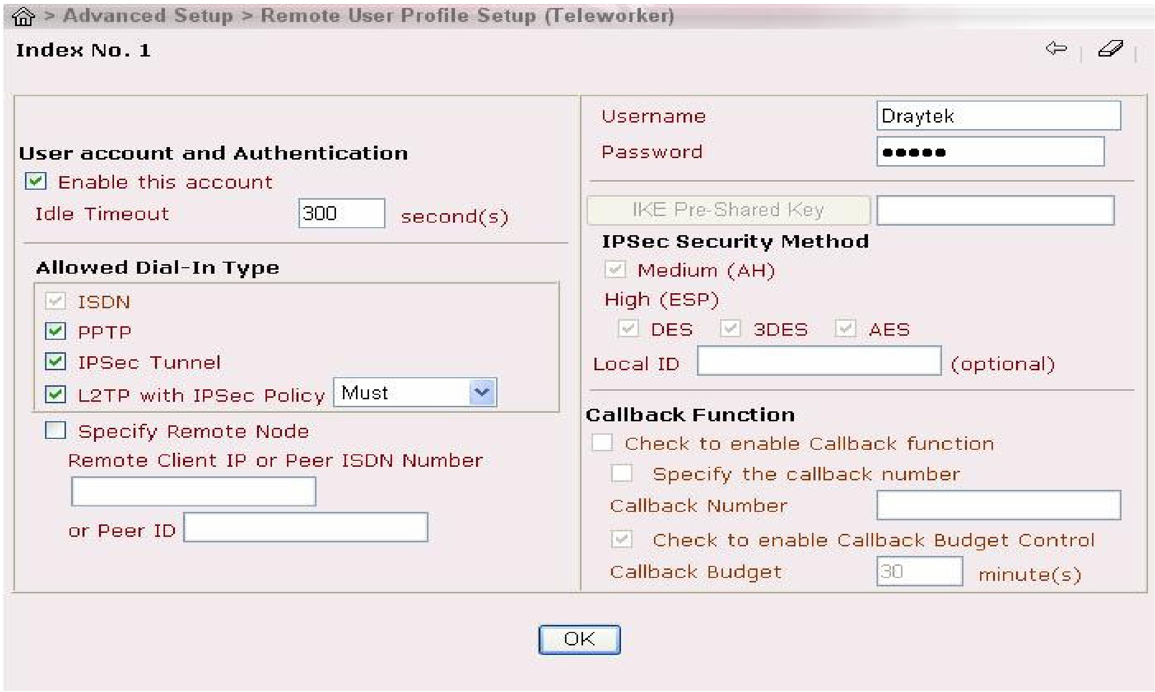
Remote Access User Accounts:

Index	User	Status	Index	User	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 >>

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

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.



> Advanced Setup > Remote User Profile Setup (Teleworker)

Index No. 1

User account and Authentication

☑ Enable this account

Idle Timeout: 300 second(s)

Allowed Dial-In Type

☑ ISDN
☑ PPTP
☑ IPSec Tunnel
☑ L2TP with IPSec Policy: Must

☐ Specify Remote Node

Remote Client IP or Peer ISDN Number:

or Peer ID:

Username: Draytek

Password: ●●●●●

IKE Pre-Shared Key:

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Local ID: (optional)

Callback Function

☐ Check to enable Callback function

☐ Specify the callback number

Callback Number:

☑ Check to enable Callback Budget Control

Callback Budget: 30 minute(s)

User Account and Authentication

Enable this account: Check this item to activate the individual dial-in user account.

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

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

PPTP: Allow the remote dial-in user to make a PPTP VPN connection through the Internet.

IPSec Tunnel: Allow the remote dial-in user to trigger a IPSec VPN connection through Internet.

L2TP: Allow the remote dial-in user to make a L2TP VPN connection through the Internet. Specify the IPSec policy to be "*None*", "*Nice to Have*", or "*Must*".

None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the *L2TP without IPSec Policy* can be viewed as one pure L2TP connection.

Nice to Have: Apply the IPSec policy first, if it is available. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.

Must: Specify the IPSec policy to be definitely applied on the L2TP connection.

Note: when you choose either the **PPTP** or the **L2TP with IPSec Policy** for the dial-in VPN type, you should specify the ***Username*** and ***Password***. Other functions including ***IKE Pre-Shared Key***, ***IPSec Security Method***, ***Remote Client***

IP or Peer ID* and optional *Local ID are reserved for the option of the **IPSec Tunnel** and will be disabled for the **PPTP** or the **L2TP with IPSec Policy** option. One exception for the **L2TP with IPSec Policy** option is that policy sets to ***Nice to Have*** or ***Must***. In this exception, you should move on the setting of ***IKE Pre-Shared Key***, ***IPSec Security Method***, ***Remote Client IP or Peer ID***, and optional ***Local ID***.

Hence, if you enable the **PPTP** or **L2TP without IPSec Policy** option for the remote dial-in VPN type, you should move on the following setting

Username: Specify a username for the specific dial-in user.

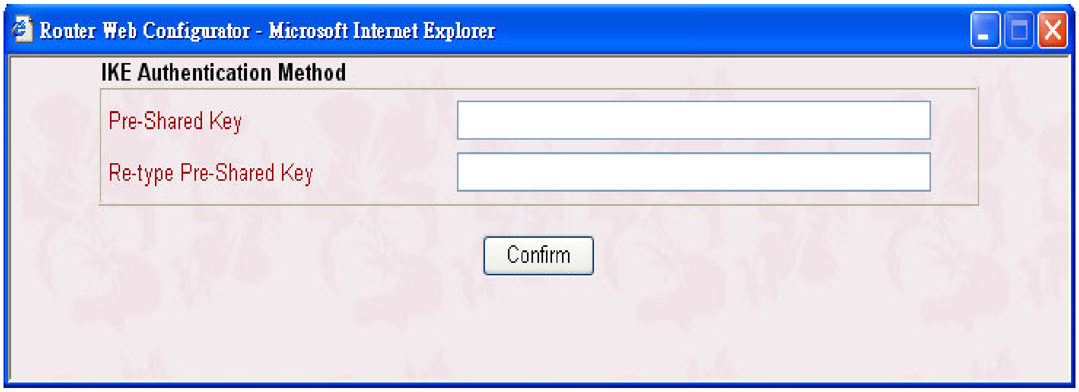
Password: Specify a password for the specific dial-in user.

Once you enable the **IPSec Tunnel** or **L2TP with IPSec Policy** with selection of ***Nice to Have*** or ***Must*** for the remote dial-in setting, you should move on the following setting.

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

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

IKE Pre-shared Key: Click it and a window will be automatically poped up for you, as depicted below. Please fill a Pre-shared Key and confirm it for this specific node.


Router Web Configurator - Microsoft Internet Explorer
IKE Authentication Method
Pre-Shared Key
Re-type Pre-Shared Key
Confirm

IPSec Security Method: Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one.

***Medium*(*AH*):** Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted.

***High* (*ESP*):** Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are DES, 3DES, and AES. By default, these three algorithms are available.

Local ID: Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional.

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

Callback Function（2900i,2900Gi only）

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 the 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 ISDN number defined in the next parameter,

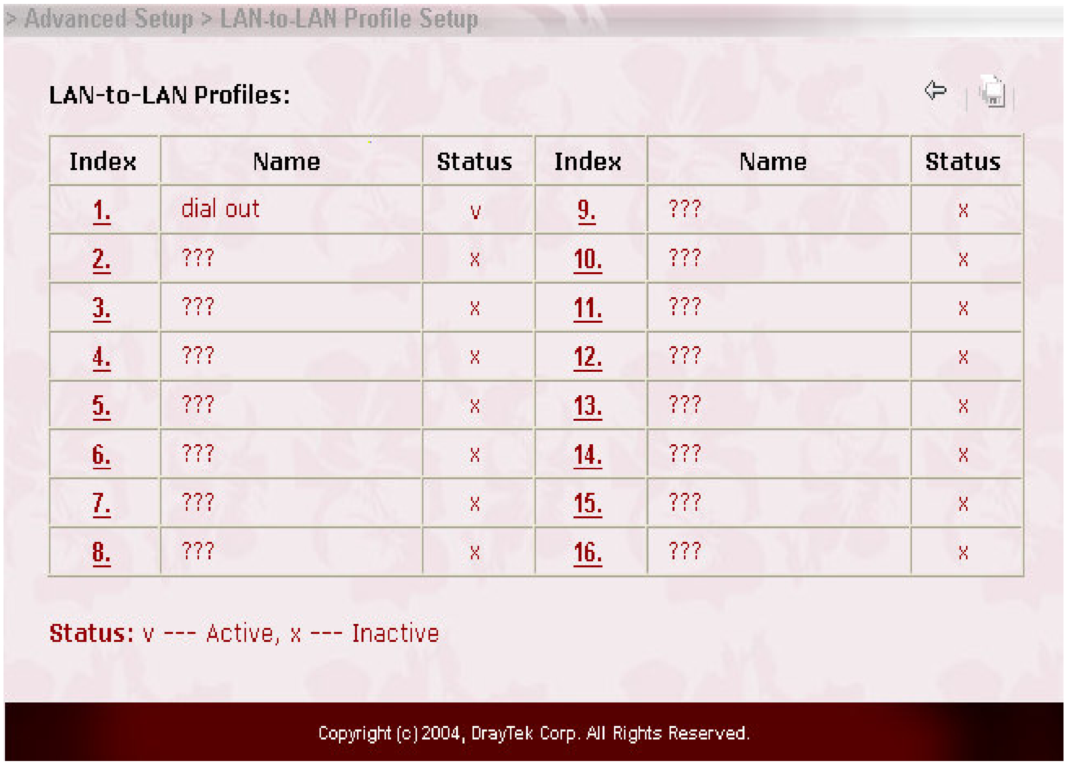
Callback Number：Callback Number: If the previous option has been enabled, enter the dial-in ISDN line number of the user here.

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.

14.6 Creating a LAN-to-LAN Profile

In this section, we will explain how to set up the **LAN-to-LAN Profile** in more detail. The path to configure it in the Web configurator is **Advanced Setup > VPN and Remote Access Setup > LAN-to-LAN Profile Setup**. The web page is shown below. Herein, you can create up to 32 LAN-to-LAN profiles.



> Advanced Setup > LAN-to-LAN Profile Setup

LAN-to-LAN Profiles:

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

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

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

(Set to Factory Default): Click here will clear all the LAN-to-LAN profiles.

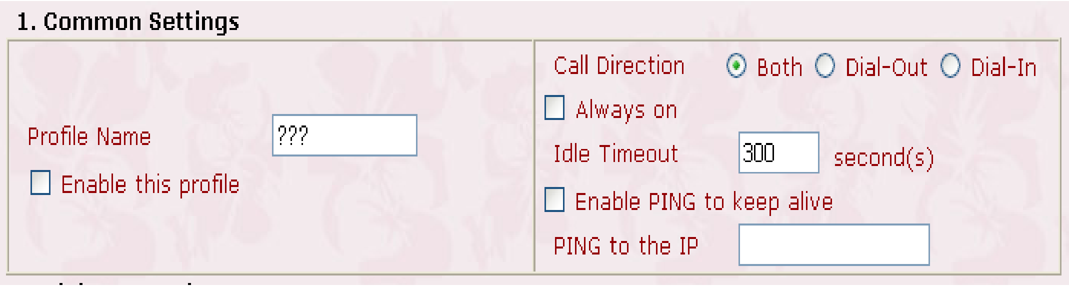
Index: Click a number to open a detailed setting page for each profile.

Name: Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

Status: Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

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

◆ Common Settings



1. Common Settings

Profile Name ???

☐ Enable this profile

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

☐ Always on

Idle Timeout 300 second(s)

☐ Enable PING to keep alive

PING to the IP

Profile Name: Specify a name for the remote network.

Enable this profile: Check here to activate this profile.

Call Direction: Specify the call direction for this profile. ***Both*** means it can be used for outgoing and incoming access. ***Dial-Out*** means it can only be used for outgoing access. ***Dial-In*** allows only incoming access.

Always on: Click it to always activate this profile. The field of ***Idle Timeout*** will be grayed to disallow any input.

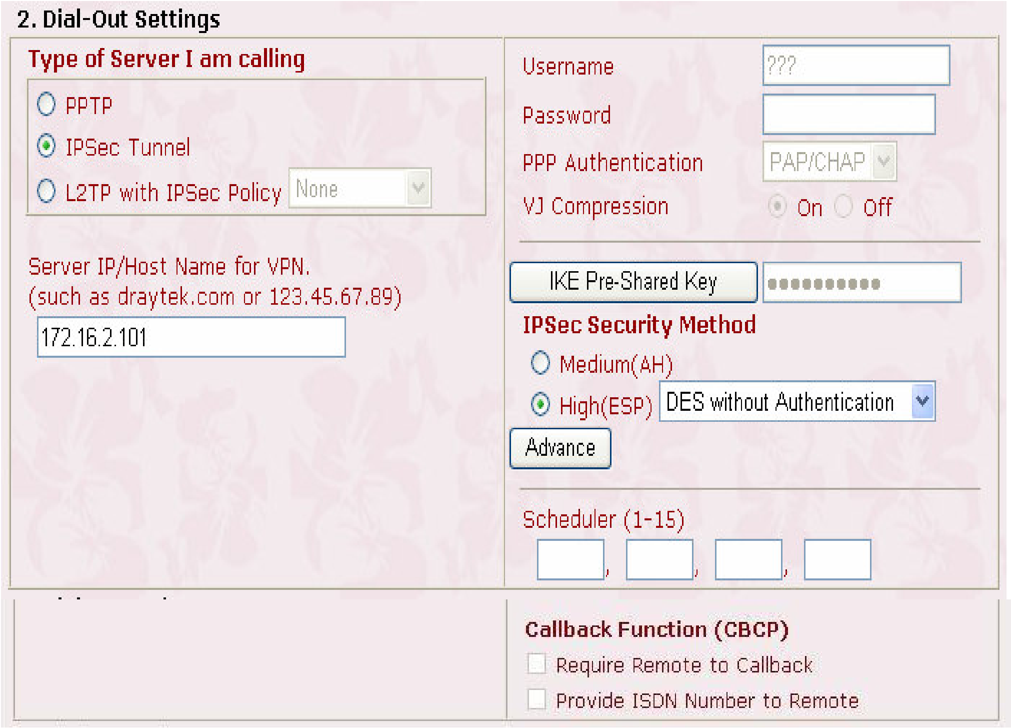
Idle Timeout: By default, set as 300 seconds. If the profiles connection is idle over the limitation of the timer, the router will drop the connection.

Enable PING to keep alive: Click this item to enable the transmission of PING packets to an IP address defined in the field of "***PING to the IP***".

***PING to the IP*:** Specify the IP address of the remote host that located at the other-end of the VPN tunnel.

Note: this function is useful to determine the state of a specific VPN connection. Normally, when the remote host wants to disconnect the VPN connection, this host should send some necessary packets to inform the Vigor router. Accordingly, the Vigor router will drop the designated VPN connection and clear its associated parameters, for example, key for encryption. However, once the remote host *abnormally* disconnects a VPN connection, say VPN *k*, the Vigor router has no ideal about VPN *k* at this moment due to its abnormal behavior. Hence, the Vigor router will regard this VPN *k* to be alive, which results in *no more packets to send within the* VPN *k and no more chance to trigger the VPN k again*. To resolve this dilemma, this function (***Enable PING to keep alive***) is designed to determine of the status of the VPN *k*. By continuously sending PING packets to the remote host, the Vigor router can know the existence of this VPN *k*. If there is no response for PING packets, the Vigor router will consider the state of the VPN *k* as disconnection. In this way, the Vigor router will clear all related parameters of the VPN *k* so that the VPN *k* can be triggered again.

◆ Dial Out Settings



2. Dial-Out Settings

Type of Server I am calling

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
172.16.2.101

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ••••••••••

IPSec Security Method

○ Medium(AH)

● High(ESP): DES without Authentication

Scheduler (1-15): , , ,

Callback Function (CBCP)

☐ Require Remote to Callback

☐ Provide ISDN Number to Remote

Type of Server I am calling: Indicate the dial-out VPN type. Herein, three options are available and only one option can be activated. These options are ***PPTP***, ***IPSec Tunnel***, and ***L2TP with IPSec Policy***. For the ***L2TP with IPSec Policy***, you have other three choices (*None*, *Nice to Have*, and *Must*) to set up the dial-out VPN type.

PPTP: Specify the dial-out VPN connection to be the PPTP connection.

IPSec Tunnel: Specify the dial-out VPN connection to be the IPSec Tunnel connection.

L2TP with IPSec Policy: Specify the IPSec policy for the L2TP connection.

None: Do not apply IPSec. Accordingly, the VPN connection employed the *L2TP without IPSec Policy* can be viewed as one pure L2TP connection.

Nice to Have: Apply the IPSec policy first, if it is available. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.

Must: Specify the IPSec policy to be definitely applied on the L2TP connection.

Note: when you choose either the **PPTP** or the **L2TP with IPSec Policy** for the dial-out VPN type, you should specify the ***Username*, *Password***, ***PPP Authentication***, and ***VJ Compression***. Other functions including ***IKE Pre-Shared Key***, ***IPSec Security Method***, ***Server IP/Host Name for VPN***, ***Scheduler***, **and *Advance Setting*** are reserved for the option of the **IPSec Tunnel** and will be disabled for the **PPTP** or the **L2TP with IPSec Policy** option. One exception for the **L2TP with IPSec Policy** option is that policy sets to ***Nice to Have*** or ***Must***. In this exception, you should move on the setting of ***IKE Pre-Shared Key***, ***IPSec Security Method***, and ***Server IP/Host Name for VPN***.

Hence, if you enable the **PPTP** or **L2TP without IPSec Policy** option for the dial-out VPN type, you should move on the following setting.

Username: Specify a username for authentication by the remote router.

Password: Specify a password for authentication by the remote router.

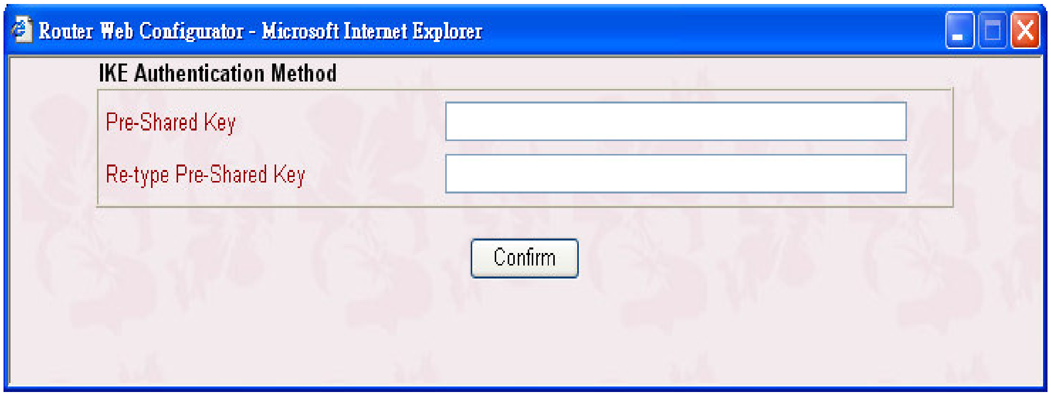
PPP Authentication: Specify the PPP authentication method for PPTP, and L2TP over IPSec. Normally set to **PAP/CHAP** for the widest compatibility.

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

Once you enable the **IPSec Tunnel** or the **L2TP with IPSec Policy (**applying ***Nice to Have*** or ***Must*** option**)** for the dial-out VPN type, you should move on the following setting.

Server IP/Host Name for VPN: Specify the IP address of the destination VPN server or the Host Name for dialup.

IKE Pre-shared Key: Click it and a window will be automatically pop out for you, as depicted below. Please fill a Pre-shared Key and confirm it for this specific node.


Router Web Configurator - Microsoft Internet Explorer
IKE Authentication Method
Pre-Shared Key
Re-type Pre-Shared Key
Confirm

IPSec Security Method: Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one.

***Medium*(*AH*):** Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted.

***High* (*ESP*):** Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are listed below.

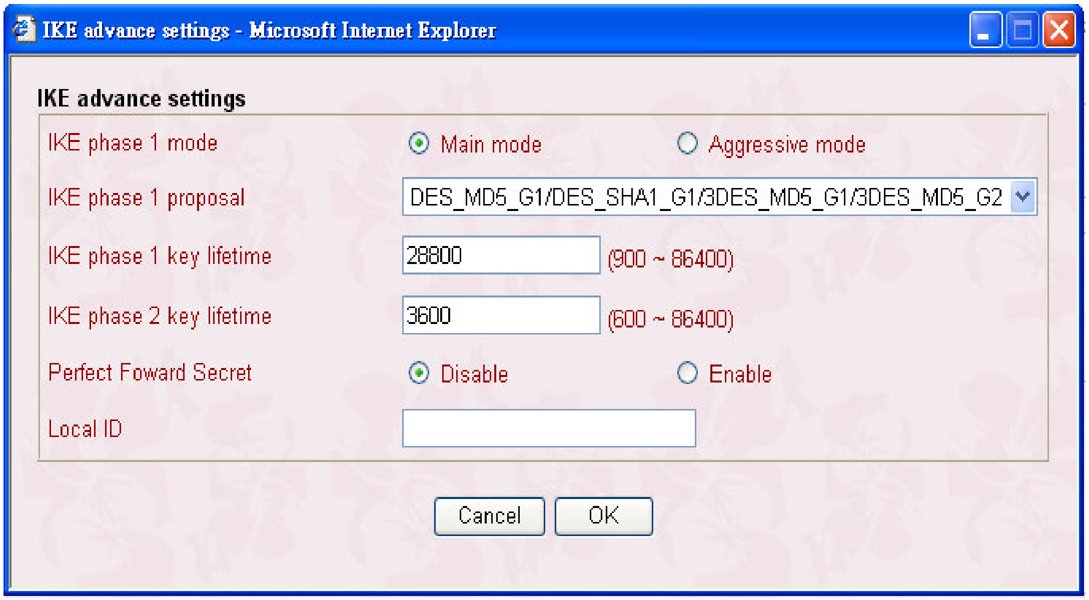
***DES without Authentication*:** Use DES encryption algorithm and not apply any authentication scheme.

***DES with Authentication*:** Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

***3DES without Authentication*:** Use triple DES encryption algorithm and not apply any authentication scheme.

***3DES with Authentication*:** Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced Setting: Click it and a window will automatically pop out for advanced setting, as shown below. In this window, you need to decide which mode (Main mode or Aggressive Mode) to be used for Phase 1 IKE negotiation process, specify the authentication and encryption algorithms, fill the lifetime for the IKE phase 1 and phase 2, enable or disable the "Perfect Forward Secret", and provide the Local ID for remote VPN gateway.



IKE advance settings

IKE phase 1 mode: ● Main mode ○ Aggressive mode

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

IKE phase 1 key lifetime: 28800 (900 ~ 86400)

IKE phase 2 key lifetime: 3600 (600 ~ 86400)

Perfect Foward Secret: ● Disable ○ Enable

Local ID:

IKE phase 1 mode: ***Main mode*** and ***Aggressive mode*** are provided in the Vigor routers. Basically, both modes are two kinds of Phase 1 IKE negotiation process. Most VPN servers support Main mode and so does the Vigor routers. Aggressive mode is a more recent implementation to speed up the negotiation process, but may incur less security. The Vigor routers also support this Aggressive mode. By default, Main mode is active for consideration of greatest compatibility.

IKE phase 1 proposal: As stated above, you should specify authentication scheme, encryption algorithm, or their combinations. Then the router will deliver the specified algorithm to the remote VPN server and ask whether it supports such an algorithm. Two options are available for selection in Aggressive mode and nine choices are provided for Main mode. For Main mode, you have better to choose the latest term, i.e. "DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2". This is because that more selections are available, more consistent algorithm is.

IKE phase 1 key lifetime: In order to increase the security level, the router should limit the key lifetime. By default, the key lifetime is set to the standard value, i.e. 28800 seconds. You are able to specify a value in between 900 and 86400 seconds on demand.

IKE phase 2 key lifetime: By default, the phase 2 key lifetime is set to the standard value, i.e. 3600 seconds. You also are able to specify a value in between 600 and 86400 seconds according to your demand.

Perfect Forward Secret: If you enable this term, then the Phase 1 key will be reused to reduce the computation complexity in phase 2. Otherwise, a new key will be generated for phase 2 key. By default, this option is inactive.

Local ID: This term is mainly used in Aggressive mode and is on behalf of the IP address to perform identity authentication with remote VPN server. It is not necessary for Main mode.

Scheduler (1-15): Specify the index of the call schedule.

Callback Function (CBCP)

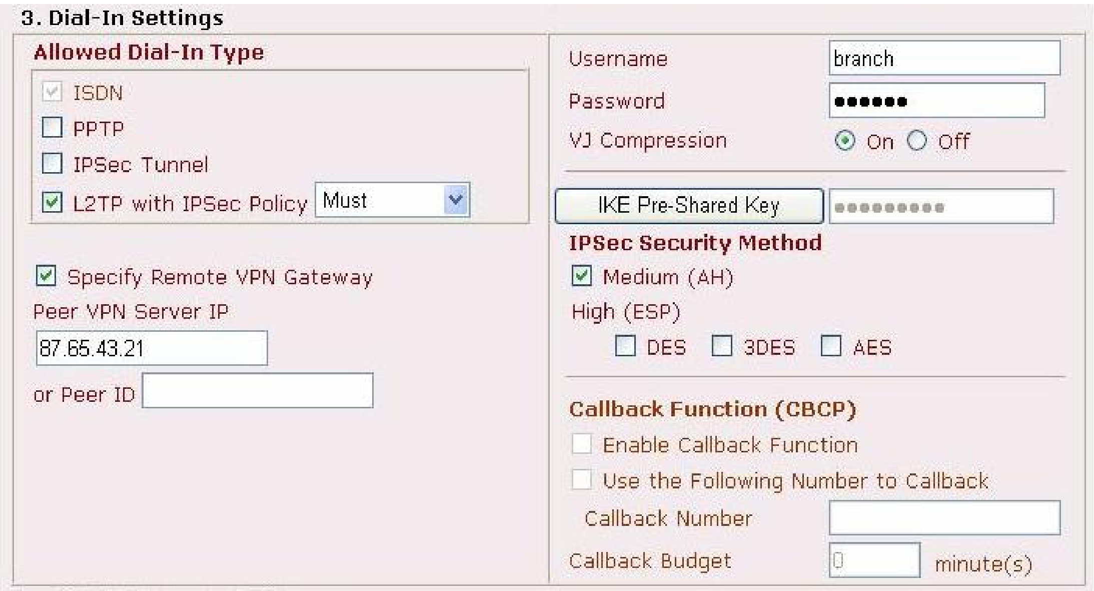
The callback function is implemented by the CBCP protocol which is part of the PPP protocol suite. It only works for ISDN LAN-to-LAN connection.

Require Remote to Callback：Inactive by default. When active, the router

exchanges connection information with the remote router and requires the remote router to call back to make a connection.

Provide ISDN Number to Remote：In some cases, the remote router requires the ISDN number for calling back. Check here to allow the local router to send the ISDN number to the remote router.

◆ Dial-In Settings



3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN
☐ PPTP
☐ IPSec Tunnel
☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway
Peer VPN Server IP: 87.65.43.21
or Peer ID:

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

IKE Pre-Shared Key: ●●●●●●●●●

IPSec Security Method
☑ Medium (AH)
High (ESP)
☐ DES ☐ 3DES ☐ AES

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

Allowed Dial-In Type: Indicate the allowed dial-in connection type. In the Vigor routers, we provide three options: ***PPTP***, ***IPSec Tunnel***, and ***L2TP with IPSec Policy***. By default, these three options are active.

PPTP: Check to allow the PPTP dial-in connection.

IPSec Tunnel: Click it to allow the IPSec tunnel dial-in connection.

L2TP with IPSec Policy: Specify the IPSec policy for the L2TP connection.

None: Do not apply the IPSec policy.

Nice to Have: Apply the IPSec policy first. If it fails, the dial-in VPN connection will be the L2TP connection without employing the IPSec policy.

*Must***:** Specify the IPSec policy to be definitely applied on the L2TP connection.

Note : It is similar to the settings for dial-out users, when you choose either the **PPTP** or the **L2TP with IPSec Policy** for dial-in setting, you should specify the **Username, Password**, **PPP Authentication**, and **VJ Compression**. Other functions including **IKE Pre-Shared Key**, **IPSec Security Method**, and **Peer VPN Server IP or Peer ID** are reserved for the option of **IPSec Tunnel** and will be disabled for the **PPTP** or **L2TP with IPSec Policy** option. One exception for the **L2TP with IPSec Policy** option is that policy sets to ***Nice to Have*** or ***Must***. In this exception, you should move on the setting of **IKE Pre-Shared Key**, **IPSec Security Method**, and **Peer VPN Server IP or Peer ID**.

Hence, if you enable the **PPTP**, **L2TP**, or **L2TP with IPSec Policy** option for dial-in setting, you should move on the setting of the following fields.

Username: Specify a username to authenticate the dial-in router.

Password: Specify a password to authenticate the dial-in router.

PPP Authentication: Specify the PPP authentication method for PPTP, L2TP, and L2TP over IPSec. Normally set to PAP/CHAP for the widest compatibility.

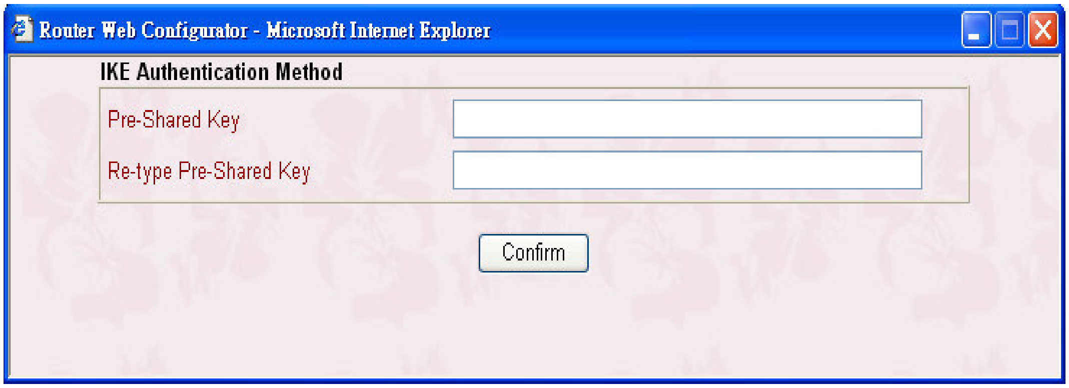
VJ Compression: VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.

Once you enable the **IPSec Tunnel** or **L2TP with IPSec Policy** with selection of ***Nice to Have*** or ***Must*** for dial-in setting, you should move on the following setting.

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

Peer VPN Server IP or Peer ID: Specify the IP address of the remote VPN server or the peer ID in the field. Afterward, you should fill a Pre-Shared Key for this specific node.

IKE Pre-shared Key: Click it and a window will be automatically popped up for you, as depicted below. Please fill a Pre-shared Key for this specific node.


Router Web Configurator - Microsoft Internet Explorer
IKE Authentication Method
Pre-Shared Key
Re-type Pre-Shared Key
Confirm

IPSec Security Method: Specify the IPSec security method, either authentication or encryption algorithm, to determine the security level. You can only select one.

***Medium*(*AH*):** Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted.

***High* (*ESP*):** Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted. Supported algorithms are DES, 3DES, and AES. By default, these three algorithms are available.

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

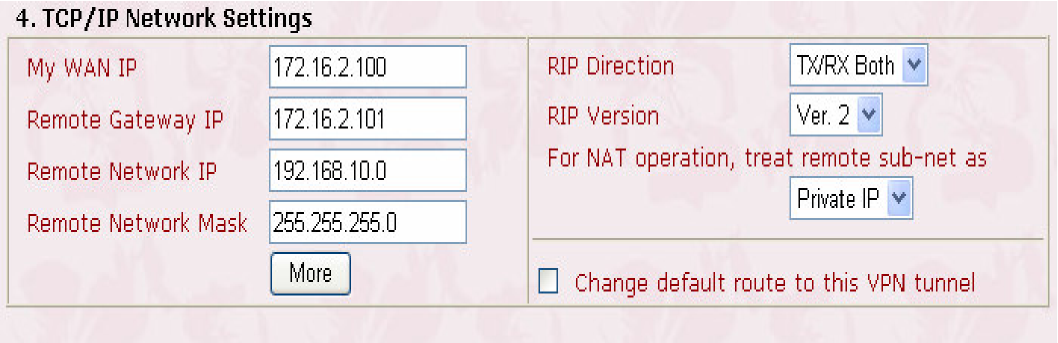
Callback Function (CBCP)

Enable Callback Function：Check to allow this router to accept requests from a remote router for call back.

Use Following Number to Callback & Callback Number：Check here and enter a callback number for the router to call.

Callback Budget：Specifies a time budget for the callback function. By default the value is zero, which means there is no time limitation on call backs.

◆ TCP/IP Network Settings



4. TCP/IP Network Settings

My WAN IP: 172.16.2.100
Remote Gateway IP: 172.16.2.101
Remote Network IP: 192.168.10.0
Remote Network Mask: 255.255.255.0
RIP Direction: TX/RX Both
RIP Version: Ver. 2
For NAT operation, treat remote sub-net as: Private IP
☐ Change default route to this VPN tunnel

The following settings are required for proper LAN-to-LAN operations.

My WAN IP: In most cases, you may accept the default value of 0.0.0.0 in this field. The router will then get a WAN IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.

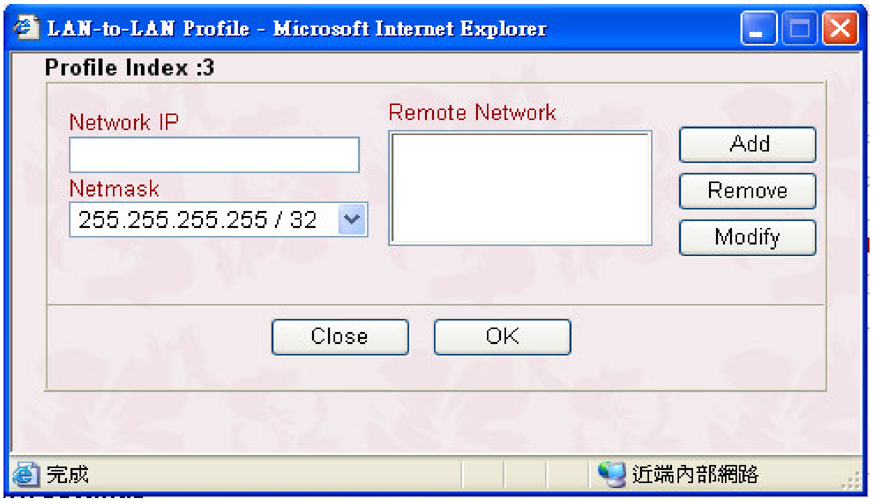
Remote Gateway IP: In most cases, you may accept the default value of 0.0.0.0 in this field. The router will then get a Remote Gateway IP address from the remote router during the IPCP negotiation phase. If the Remote Gateway IP address is fixed, specify the fixed IP address here.

Note: if you are not familiar with IPCP protocol, please set these two fields as 0.0.0.0.

Remote Network IP: Specify the network identification of the remote network. For example, 192.168.1.0 is a network identification of a class-C subnet with subnet mask of 255.255.255.0 (/24).

Remote Network Mask: Specify the subnet mask of the remote network.

More: This button let you add a static route when this connection is up. Clicking it will pop up a window for more setting, as depicted below.



LAN-to-LAN Profile - Microsoft Internet Explorer

Profile Index :3

Netmask: 255.255.255.255 / 32

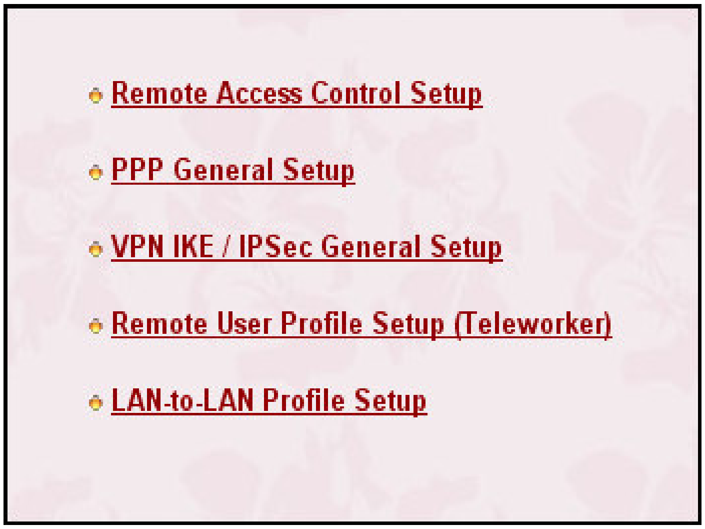
RIP Direction: The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: **TX/RX Both**, **TX Only**, **RX Only**, and **Disable**.

RIP Version: Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.

For NAT operation, treat remote sub-net as: The Vigor router supports two local IP networks: the 1st subnet and 2nd subnet. Thus, you can set which subnet will be used as the local network for VPN connection and exchange RIP packets with the remote network. Usually set to **Private IP** for routing between the 1st subnet and the remote network.

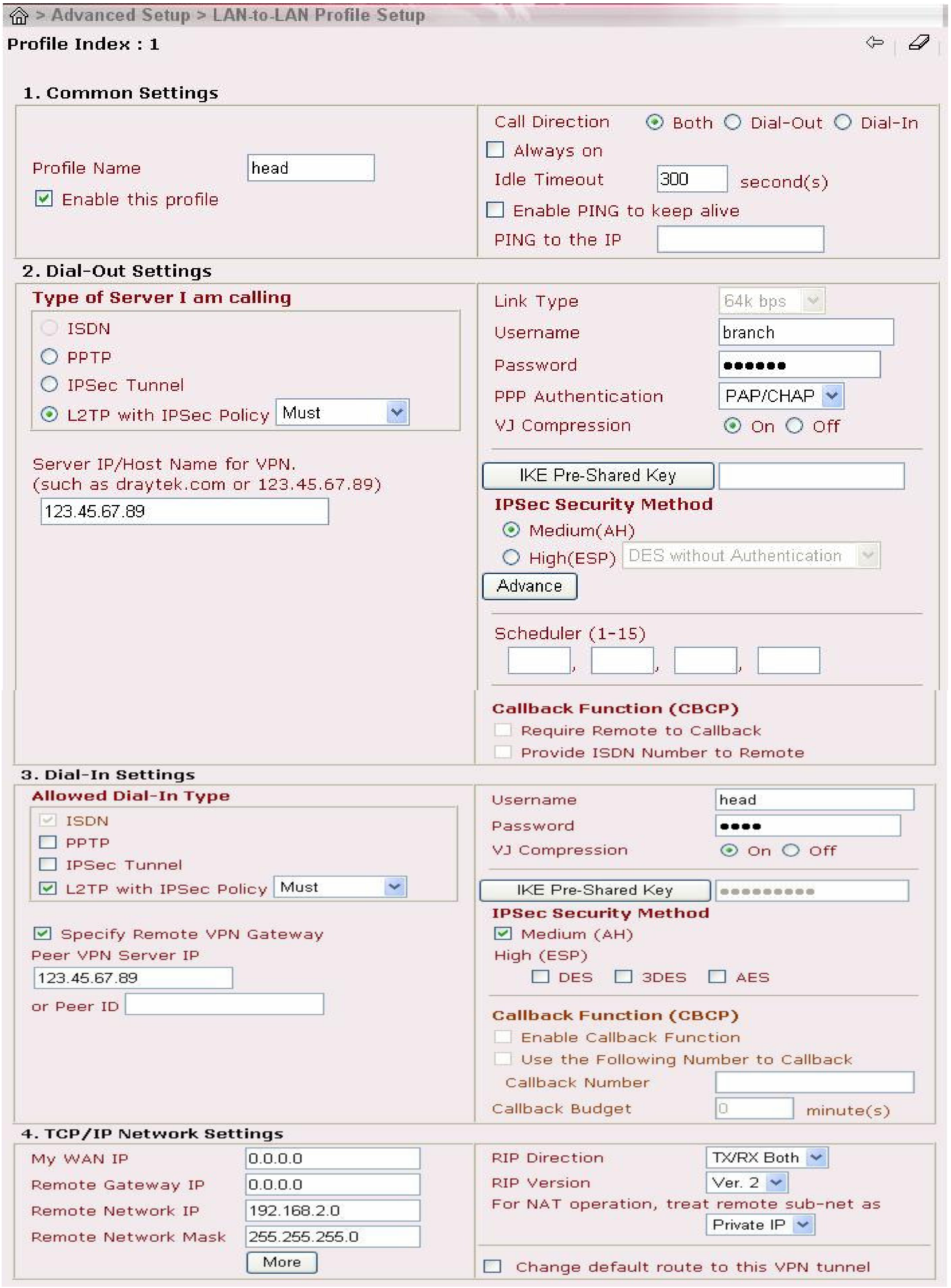
14.7 An example of LAN-to-LAN VPN connection

This example is based on the network configuration shown in the following table to describe how to set up a LAN-to-LAN profile to connect two private networks through Internet. As shown in the table, the private network 192.168.1.0/24 is located at head office, the network of off-site branch office is 192.168.2.0/24.


Remote Access Control Setup
PPP General Setup
VPN IKE / IPSec General Setup
Remote User Profile Setup (Teleworker)
LAN-to-LAN Profile Setup

Before configuring the LAN-to-LAN profile for each site, you should click **VPN and Remote Access Setup > VPN IKE/IPSec Setup** to configure the pre-shared key **ABC123** in advance.

Creating a LAN-to-LAN profile at Head Office



Profile Index : 1

1. Common Settings

Profile Name: head

☑ Enable this profile

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

☐ Always on

Idle Timeout: 300 second(s)

☐ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

○ IPSec Tunnel

● L2TP with IPSec Policy: Must

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

Link Type: 64k bps

Username: branch

Password: ●●●●●●

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key:

IPSec Security Method

● Medium(AH)

○ High(ESP): DES without Authentication

Advance

Scheduler (1-15): , , ,

Callback Function (CBCP)

☐ Require Remote to Callback

☐ Provide ISDN Number to Remote

3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN

☐ PPTP

☐ IPSec Tunnel

☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 123.45.67.89

or Peer ID:

Username: head

Password: ●●●●

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ●●●●●●●●●●

IPSec Security Method

☑ Medium (AH)

High (ESP): ☐ DES ☐ 3DES ☐ AES

Callback Function (CBCP)

☐ Enable Callback Function

☐ Use the Following Number to Callback

Callback Number:

Callback Budget: 0 minute(s)

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.2.0

Remote Network Mask: 255.255.255.0

More

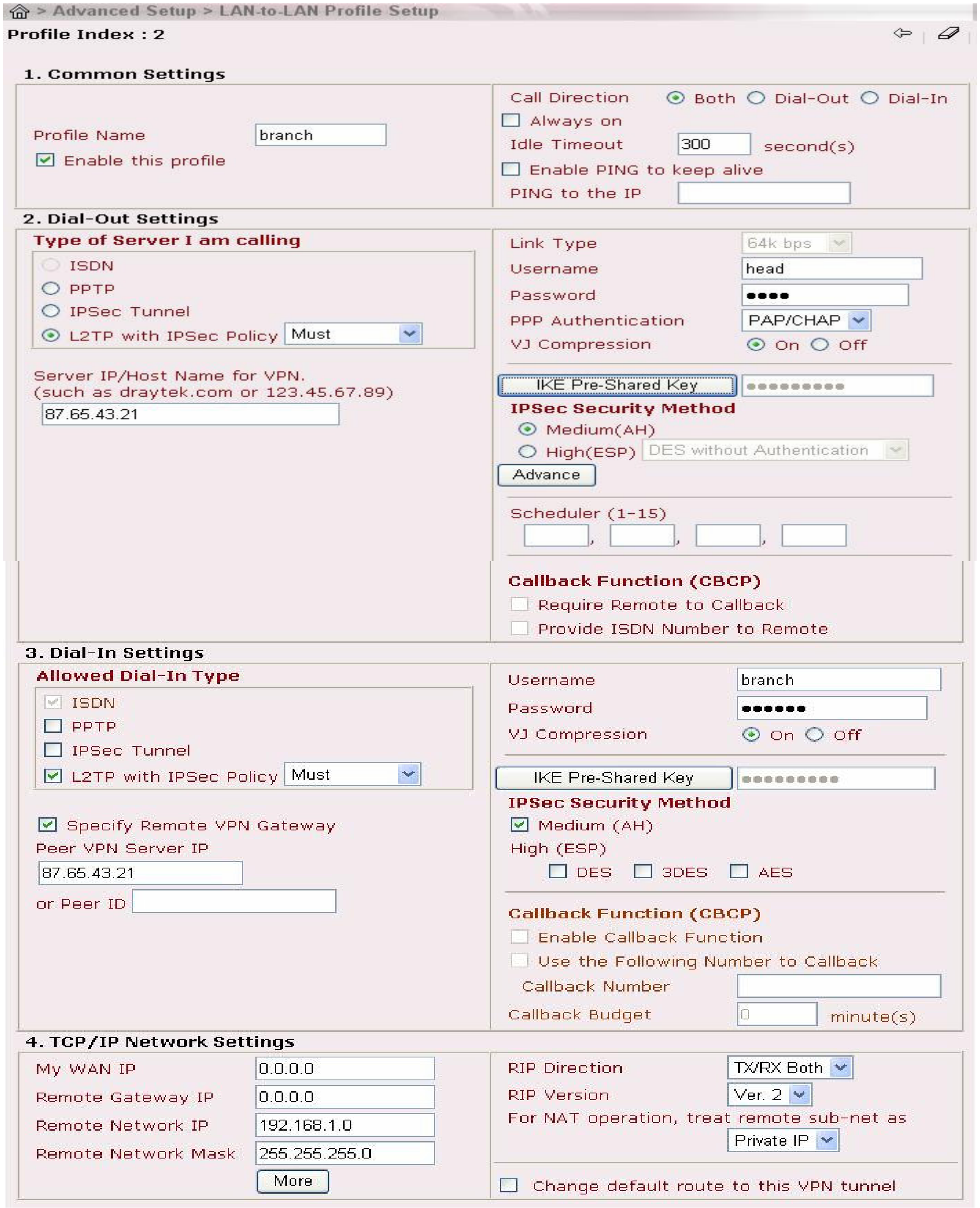
RIP Direction: TX/RX Both

RIP Version: Ver. 2

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

☐ Change default route to this VPN tunnel

Creating a LAN-to-LAN profile at Branch Office



Profile Index : 2

1. Common Settings

Profile Name: branch

☑ Enable this profile

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

☐ Always on

Idle Timeout: 300 second(s)

☐ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

○ IPSec Tunnel

● L2TP with IPSec Policy: Must

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
87.65.43.21

Link Type: 64k bps

Username: head

Password: ●●●●

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ●●●●●●●●●

IPSec Security Method

● Medium(AH)

○ High(ESP): DES without Authentication

Advance

Scheduler (1-15): , , ,

Callback Function (CBCP)

☐ Require Remote to Callback

☐ Provide ISDN Number to Remote

3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN

☐ PPTP

☐ IPSec Tunnel

☑ L2TP with IPSec Policy: Must

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 87.65.43.21

or Peer ID:

Username: branch

Password: ●●●●●●

VJ Compression: ● On ○ Off

IKE Pre-Shared Key: ●●●●●●●●●

IPSec Security Method

☑ Medium (AH)

High (ESP): ☐ DES ☐ 3DES ☐ AES

Callback Function (CBCP)

☐ Enable Callback Function

☐ Use the Following Number to Callback

Callback Number:

Callback Budget: 0 minute(s)

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.1.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: TX/RX Both

RIP Version: Ver. 2

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

☐ Change default route to this VPN tunnel

Appendix: *Log Event Disposition*

Any syslog message in the Vigor routers consists of three parts: ***Time*** field, ***Host*** field and ***Message body*** filed. Time field states the time epoch when an event happens. Host field stands for describing the device that sends the log message. By default, the Vigor routers fill this field with "Vigor" which can be configured through the following web configuration

Internet Access Setup > Static or Dynamic IP > Router Name.

The Message body is used to describe what kind of events occurs and its associated information, say source/destination IP addresses, source/destination port number, and so on.

In this section, we describe the log event disposition for VPN function, mainly for IKE (Internet Key Exchange) and IPSec protocol. Basically, the Vigor router classify them into four categories: IKE Negotiate Status Messages (IPSec), IKE Negotiate Packet Messages (IPSec), Rejected IKE Messages, and Discard ESP Packet Messages. In the following, we move on giving a full detail of their formats or syntaxs.

1. IKE Negotiate Status Messages (IPSec)

Before successfully establishing an IPSec VPN connection, the user should employ the IKE protocol to securely negotiate and provide authenticated keying material for security associations. Accordingly, the Vigor router will record the status during the IKE negotiation process and send its related syslog messages to your syslog utility for tracing. The format in the syslog message is shown below.

For a security association initiated from remote side

Action *p_index* (*p_name*) *remote_addr*

where

Action: indicate the behavior (action) performed by the received node of a security association once receiving some messages sent by a remote access IPSec client. The behavior could be

Responding to Main Mode from: Suppose that a remote access IPSec client initiates a IPSec VPN connection operating in IKE Main Mode to your Vigor router. Once receiving such a message, the Vigor router will display such a message.

Responding to Aggressive Mode from: Suppose that a remote access IPSec client initiates a IPSec VPN connection operating in IKE Aggressive Mode to your Vigor router. Once receiving such a message, the Vigor router will display such a message.

Responding to Quick Mode from: Suppose that a remote access IPSec client initiates a IPSec VPN connection operating in IKE Quick Mode to your Vigor router. Once receiving such a message, the Vigor router will display such a message.

p_index (*p_name*): indicate the profile index # in the "LAN-to-LAN profile" or "Remote User profile" and its associated profile name.

remote_addr: specify the IP address of a remote VPN Gateway that triggers a security association.

For a security association initiated from local side

Action local_addr

where

Action: indicate the initiating IKE behavior (action) performed by the local node of a security association. The action could be

Initiating IKE Main Mode to: Show a local VPN node commences to initiate a VPN connection operating in IKE Main Mode with remote access IPSec client.

Initiating IKE Aggressive Mode to: Show a local VPN node commences to initiate a VPN connection operating in IKE Aggressive Mode.

Start IKE Quick Mode to: Show a local VPN node commences to initiate a VPN connection operating in IKE Quick Mode.

ISAKMP SA established with: Describe a local VPN client has established successfully a ISAKMP SA with another VPN peer. (Phase 1)

IPsec SA established with: Describe a local VPN client establishes a IPSec SA (Security Association) with another VPN peer. (Phase 2)

local_addr: specify the IP address of the local VPN Gateway triggering a VPN connection.

For a dialing-out behavior from a local side

Dialing Node *p_index* (*p_name*) *remote_addr*

where

Dialing Node: Show a local VPN node which triggers a VPN connection based on a "LAN-to-LAN" or "Remote-Dialin" profile.

p_index (*p_name*): Indicate the profile index # in the "LAN-to-LAN profile" or "Remote User profile" and its associated profile name.

remote_addr: Specify the IP address of a remote VPN Gateway (another VPN peer).

For example: *Suppose a local user intends to establish an IPSec VPN tunnel with a remote node having the IP address of 140.113.13.101 by using an IKE Main Mode. At the starting phase of the IKE negotiation process, the Vigor router will record the status and, accordingly, send the syslog message as "Initiating IKE Main Mode to 140.113.13.101".*

2. Rejected IKE Messages

During the IKE negotiation process, some abnormal activities of the VPN peer will cause the Vigor router to reject its requests which attempt to establish a IPSec VPN connection. To effectively know the failures on establishing a VPN connection, the Vigor routers provides the following log messages to record the rejection reasons. Each log entry includes minimally *Date/Time*, *Source and Destination IP address*, *Cookie pair* (i.e *Initiator cookie* and *Responder cookie*), *Payload responsible for rejection*, and *Reason for Rejection*. The corresponding syntax of the log messages is shown below.

(Rejected IKE Message) => Source IP = *src_addr,* **Destination IP =** *dst_addr,* **I_Cookie =** *Initial_cookie,* **R_Cookie =** *Response_cookie,* **Rejection Payload =** *payload_name* **=> Failed:** *Reason for Rejection*

where

(Rejected IKE Message)/Source IP/Destination IP/I_Cookie/R_Cookie/ Rejection Payload/Failed: All of them are reserved words appearing in the syslog messages.

src_addr: Show the IP address of the sender which is a VPN peer to initiate a VPN connection.

dst_addr: Show the IP address of the recipient which is another VPN peer.

Initial_cookie: Show the Initiator's cookie.

Response_cookie: Specify the Responder's cookie.

payload_name: Display the payload responsible for rejection. The payload_name could be

NULL,

ISAKMP Header Payload,

Security Association Payload,

Proposal Payload,

Transform Payload,

Key Exchange Payload,

Identification Payload,

Certificate Payload,

Certificate Request Payload,

Hash Payload,

Signature Payload,

Nonce Payload,

Notification Payload,

Delete Payload, and

Vendor ID Payload.

Reason for Rejection: Show the reason for rejection when some error occurs at the IKE negotiation phase or at the establishment phase of a SA (Security Association). For any error occurred at the IKE negotiation phase, this filed will use the following format for illustration purpose.

IKE Error Message

On the other hand, for any error occuring at the establishment phase of a SA, the reason for rejection will use the following format to explain it.

IKE State status =>Notify Error Message

Now, let us describe them in more detail.

IKE Error Message: Show the error messages during the IKE negotiation process and the error message could be one of the following reasons.

"**ISAKMP Header Failed!**",

"**The packet size *packet_size* differs from the size specified in ISAKMP HDR *packet_len_ isakmp***"

"**Message ID was *Msg_id* but should be zero in Main Mode**"

"Initiator Cookie must not be zero in Main Mode message"

"Without default dial-in pre-shared key, Dial-in function is disabled for dynamic ip client"

"Initial Main Mode message is invalid: its Encrypted Flag is on"

"This is a duplicate packet"

"Main Mode message is a part of an unknown exchange"

"Message ID was *Msg_id* but should be zero in Aggressive Mode"

"Initiator Cookie must not be zero in Aggressive Mode message"

"Aggressive Mode message is a part of an unknown exchange"

"Informational Exchange is for an unknown (expired?) SA"

"Encrypted Informational Exchange message is invalid! because it is for incomplete ISAKMP SA"

"Informational Exchange message is invalid! because it has a Message ID of 0"

"Informational Exchange message is invalid! because it has a previously used Message ID (*Msg_id*)"

"Informational Exchange message for an established ISAKMP SA must be encrypted"

"Quick Mode message is invalid because it has an Initiator Cookie of 0"

"Quick Mode message is invalid because it has a Responder Cookie of 0"

"Quick Mode message is invalid because it has a Message ID of 0"

"Quick Mode message is for a non-existent (expired?) ISAKMP SA"

"Quick Mode message is unacceptable because it is for an incomplete ISAKMP SA"

"Quick Mode I1 message is unacceptable because it uses a previously used

Message ID *Msg_id* (perhaps this is a duplicated packet)"

"Unsupported exchange type *Exchange_type* in message"

"Retransmitting in response to duplicate packet; already *IKE State status*"

"Discarding duplicate packet -- exhausted retransmission; already *IKE State status*"

"Discarding duplicate packet; already *IKE State status*"

"Discarding encrypted message for an unknown ISAKMP SA"

"Discarding encrypted message because we haven't yet negotiated keying material"

"Malformed message: not a multiple of encryption block size"

"Packet rejected: should have been encrypted"

"More than *max_payload* payloads in the message; ignored"

"Message ignored because it contains an unknown or unexpected payload type (*Payload_type*:) at the outermost level"

"Message ignored because it contains a payload type (*Payload_type*:) unexpected in this message"

"Malformed payload in packet"

"Message for *IKE State status* is missing payloads"

"Malformed Phase 1 message: does not start with an SA payload"

"Malformed Quick Mode message: does not start with a HASH payload"

"Malformed Quick Mode message: SA payload is in a wrong position"

"Malformed Quick Mode message: if any ID payload is present, there must be exactly two"

"Malformed Quick Mode message: the ID payloads are not adjacent"

"State transition function for *IKE State status* had internal error".

where

packet_size: Show the received packet size.

packet_len_isakmp: Show the packet length in the ISAKMP Header.

Msg_id: Indicate the Unique Message Identifier.

Exchange_type: Show the exchange type of the ISAKMP Header.

max_payload: Show the maximum number of payloads.

Payload_type: Show the Next Payload type of the ISAKMP Header.

IKE State status: Display the phase and mode of the IKE negotiation process. One of the following messages may appear in the field of *IKE State status*.

STATE_MAIN_R0

STATE_MAIN_I1

STATE_MAIN_R1

STATE_MAIN_I2

STATE_MAIN_R2

STATE_MAIN_I3

STATE_MAIN_R3

STATE_MAIN_I4

STATE_QUICK_R0

STATE_QUICK_I1

STATE_QUICK_R1

STATE_QUICK_I2

STATE_QUICK_R2

STATE_INFO

STATE_INFO_PROTECTED

STATE_AGGR_R0

STATE_AGGR_I1

STATE_AGGR_R1

STATE_AGGR_I2

STATE_AGGR_R2

Notify Error Message: Notify the error message to specify why an SA can not be established successfully. The error message could be one of the following forms.

"INVALID_PAYLOAD_TYPE"

"DOI_NOT_SUPPORTED"

"SITUATION_NOT_SUPPORTED"

"INVALID_COOKIE"

"INVALID_MAJOR_VERSION"

"INVALID_MINOR_VERSION"

"INVALID_EXCHANGE_TYPE"

"INVALID_FLAGS"

"INVALID_MESSAGE_ID"

"INVALID_PROTOCOL_ID"

"INVALID_SPI"

"INVALID_TRANSFORM_ID"

"ATTRIBUTES_NOT_SUPPORTED"

"NO_PROPOSAL_CHOSEN"

"BAD_PROPOSAL_SYNTAX"

"PAYLOAD_MALFORMED"

"INVALID_KEY_INFORMATION"

"INVALID_ID_INFORMATION"

"INVALID_CERT_ENCODING"

"INVALID_CERTIFICATE"

"CERT_TYPE_UNSUPPORTED"

"INVALID_CERT_AUTHORITY"

"INVALID_HASH_INFORMATION"

"AUTHENTICATION_FAILED"

"INVALID_SIGNATURE"

"ADDRESS_NOTIFICATION"

"NOTIFY_SA_LIFETIME"

"CERTIFICATE_UNAVAILABLE"

"UNSUPPORTED_EXCHANGE_TYPE"

"UNEQUAL_PAYLOAD_LENGTHS"

For example: Suppose a VPN peer with the IP address of 172.16.2.220 intends to establish an IPSec VPN tunnel with another VPN peer having the IP address of 172.16.2.110 by using an IKE Main Mode. However, it fails to establish such a VPN connection due to lack of proposal chosen. Thus, the Vigor router will show the following log message in response to the rejection reason.

(Rejected IKE Messages) => Source IP = 172.16.2.220, Destination IP = 172.16.2.110, I_Cookie = 0x00 80 40 a0 d0 e8 f4 fa, R_Cookie = 0x9a 65 e4 6f 00 45 26 a8, Error Payload = ISAKMP Header Payload => Failed: STATE_MAIN_I1 => NO_PROPOSAL_CHOSEN.

3. Discarded ESP packets

With regarding to discarded ESP (Encapsulating Security Payload) packets, the

Vigor router also log the corresponding messages. Similar to the messages mentioned in the previous section, each log entry includes minimally *Date/Time*, *SPI (Security Parameter Index) value, Soure and Destination IP address*, *Sequence Number,* and *Reason for Discard*. The format of the log messages is shown below.

(Discarded ESP packets) => SPI = *spi*, **Source IP =** *src_addr*, **Destination IP =** *dst_addr*, **Sequence number =** *seq_num* **=>** *Reason for Discard*

where

Discarded ESP packets/SPI/Source IP/Destination IP/Sequence number: All of them are reserved words in the log messages.

spi: Show the security parameter index of the packet.

src_addr: Show the source IP address of a VPN Gateway which triggers a VPN connection.

dst_addr: Indicate the destination IP address of a VPN Gateway.

seq_num: Show the sequence nember of the received packet.

Reason for Discard: Display the reason for discarded Encapsulating Security Payload packet. The reason could be

"Authenticator length error"

"Event To Cypher failed, free buffer"

"Got packet with content length = ***content_length*** **-- should be on 4-octet boundary, packet dropped"**

"Source address of pkt does not agree with expected SA source address policy"

"Replay window counter rolled, expiring SA"

"Duplicate frame from ***sender_ip***, **packet dropped"**

"Authentication failed on incoming packet from *sender_ip*: dropped"

"Got packet with ESP Payload length = *esp_length* -- should be on 8 octet boundary, packet dropped"

"Decryption fail!"

"Got packet with ESP Payload length(AES Encryption) = *esp_length* -- should be on 16 octet boundary, packet dropped"

"Warning, decrypted packet from *sender_ip* has bad padding...may be bad decryption – dropped"

Parameters used for the Reason for Discard are defined below.

content_length: Show the content length of the received packet.

sender_ip: Show the source IP address of the packet from sender.

esp_length: Show the length of the Encapsulating Security Payload (ESP) packet.

For example: Suppose a VPN peer with the IP address of 172.16.2.220 has established successfully an IPSec VPN tunnel with another VPN peer having the IP address of 172.16.2.110. However, it fails to transmit packets through such a VPN tunnel due to failed decryption at the packet with sequence number 0x1. As a result, the Vigor router will show the following log message in response to the discarded ESP packet.

(Discarded ESP packets) => SPI = *0x*13c32319, Source IP = 172.16.2.220, Destination IP = 172.16.2.110, Sequence number = 0x1 => Decryption fail!

4. IKE Negotiate Packet Messages (IPSec)

The administrator may be interested in understanding some information regarding to the IKE negotiation packets, for instance cookie pair, payload type of the ISAKMP header, the exchange type number of the ISAKMP header, and so forth. Hence, the Vigor router further provides the following log messages to record the related status. The format of the log messages is defined as follows.

IKE *direction* **I Cookie =** *Initial_cookie* **, R Cookie =** *Response_cookie* **, Next Payload =** *Payload_type* **, Exchange Type =** *Exchange_type_no,* **Message ID =** *Msg_id*

where

IKE/I Cookie/R Cookie/Next Payload/Exchange Type/Message ID: All of them are reserved words in the log messages and stand for Internet Key Exchange/Initial Cookie/Response Cookie/Next Payload type/ Exchange Type/Message Identity, respectively,

direction: Indicate the direction of the IKE packet. Use "==>" to represent the outbound packet and employ "<==" to illustrate the inbound packet.

Initial_cookie: Show the initiator cookie.

Response_cookie: Display the responder cookie.

Payload_type: Show the Next Payload type of the ISAKMP Header. There are several payload types which are described below.

ISAKMP_NEXT_NONE: indicate "No Other Payload Followed".

ISAKMP_NEXT_SA: represent the "Security Association Payload".

ISAKMP_NEXT_P: be the "Proposal Payload".

ISAKMP_NEXT_T: indicate the "Transform Payload".

ISAKMP_NEXT_KE: indicate the "Key Exchange Payload".

ISAKMP_NEXT_ID: indicate the "Identification Payload".

ISAKMP_NEXT_CERT: indicate the "Certificate Payload".

ISAKMP_NEXT_CR: indicate the "Certificate Request Payload".

ISAKMP_NEXT_HASH: indicate the "Hash Payload".

ISAKMP_NEXT_SIG: indicate the "Signature Payload".

ISAKMP_NEXT_NONCE: indicate the “Nonce Payload”.

ISAKMP_NEXT_N: indicate the “Notification Payload”.

ISAKMP_NEXT_D: indicate the “Delete Payload”.

ISAKMP_NEXT_VID: indicate the “Vendor ID Payload”.

Exchange_type_no: Show the exchange type number of the ISAKMP Header. The possible number and its associated meanning is shown below.

0x0: ISAKMP_XCHG_NONE

0x1: ISAKMP_XCHG_BASE

0x2: ISAKMP_XCHG_IDPROT (for ID Protection)

0x3: ISAKMP_XCHG_AO (for Authentication Only)

0x4: ISAKMP_XCHG_AGGR (for Aggressive mode)

0x5: ISAKMP_XCHG_INFO (for Informational)

0x20: ISAKMP_XCHG_QUICK (for Oakley Quick Mode)

0x21: ISAKMP_XCHG_NGRP (for Oakley New Group Mode)

0x22: ISAKMP_XCHG_ACK_INFO (for Oakley Acknowledged Informational)

Msg_id: Show the Unique Message Identifier.

***For example*:** Herein, we use a log message to trace the outbound IKE negotiation packet, as shown below.

```
IKE ==> I Cookie = 0x00 80 40 a0 d0 e8 f4 fa, R Cookie = 0x00 00 00 00 00 00 00 00, Next Payload = ISAKMP_NEXT_SA, Exchange Type = 0x2, Message ID = 0x0
```

Appendix of Chapter 14

Appendix: Log Event Disposition for VPN and Remote Access Setup

Appendix: *Log Event Disposition*

Any syslog message in the Vigor routers consists of three parts: ***Time*** field, ***Host*** field and ***Message body*** filed. Time field states the time epoch when an event happens. Host field stands for describing the device that sends the log message. By default, the Vigor routers fill this field with “Vigor” which can be configured through the following web configuration

Internet Access Setup > Static or Dynamic IP > Router Name.

The Message body is used to describe what kind of events occurs and its associated information, say source/destination IP addresses, source/destination port number, and so on.

In this section, we describe the log event disposition for VPN function, mainly for IKE (Internet Key Exchange) and IPSec protocol. Basically, the Vigor router classify them into four categories: IKE Negotiate Status Messages (IPSec), IKE Negotiate Packet Messages (IPSec), Rejected IKE Messages, and Discard ESP Packet Messages. In the following, we move on giving a full detail of their formats or syntaxs.

1. IKE Negotiate Status Messages (IPSec)

Before successfully establishing an IPSec VPN connection, the user should employ the IKE protocol to securely negotiate and provide authenticated keying material for security associations. Accordingly, the Vigor router will record the status during the IKE negotiation process and send its related syslog messages to your syslog utility for tracing. The format in the syslog message is shown below.

For a security association initiated from remote side

Action   *p_index* (*p_name*)   *remote_addr*

where

Action: indicate the behavior (action) performed by the received node of a security association once receiving some messages sent by a remote access IPSec client. The behavior could be

Responding to Main Mode from: Suppose that a remote access IPSec client initiates a IPSec VPN connection operating in IKE Main Mode to your Vigor router. Once receiving such a message, the Vigor router will display such a message.

Responding to Aggressive Mode from: Suppose that a remote access IPSec client initiates a IPSec VPN connection operating in IKE Aggressive Mode to your Vigor router. Once receiving such a message, the Vigor router will display such a message.

Responding to Quick Mode from: Suppose that a remote access IPSec client initiates a IPSec VPN connection operating in IKE Quick Mode to your Vigor router. Once receiving such a message, the Vigor router will display such a message.

p_index (*p_name*): indicate the profile index # in the “LAN-to-LAN profile” or “Remote User profile” and its associated profile name.

remote_addr: specify the IP address of a remote VPN Gateway that triggers a security association.

For a security association initiated from local side

Action local_addr

where

Action: indicate the initiating IKE behavior (action) performed by the local node of a security association. The action could be

Initiating IKE Main Mode to: Show a local VPN node commences to initiate a VPN connection operating in IKE Main Mode with remote access IPSec client.

Initiating IKE Aggressive Mode to: Show a local VPN node commences to initiate a VPN connection operating in IKE Aggressive Mode.

Start IKE Quick Mode to: Show a local VPN node commences to initiate a VPN connection operating in IKE Quick Mode.

ISAKMP SA established with: Describe a local VPN client has established successfully a ISAKMP SA with another VPN peer. (Phase 1)

IPsec SA established with: Describe a local VPN client establishes a IPSec SA (Security Association) with another VPN peer. (Phase 2)

local_addr: specify the IP address of the local VPN Gateway triggering a VPN connection.

For a dialing-out behavior from a local side

Dialing Node   *p_index* (*p_name*)   *remote_addr*

where

Dialing Node: Show a local VPN node which triggers a VPN connection based on a "LAN-to-LAN" or "Remote-Dialin" profile.

p_index (*p_name*): Indicate the profile index # in the "LAN-to-LAN profile" or "Remote User profile" and its associated profile name.

remote_addr: Specify the IP address of a remote VPN Gateway (another VPN peer).

For example**:** *Suppose a local user intends to establish an IPSec VPN tunnel with a remote node having the IP address of 140.113.13.101 by using an IKE Main Mode. At the starting phase of the IKE negotiation process, the Vigor router will record the status and, accordingly, send the syslog message as "Initiating IKE*

Main Mode to 140.113.13.101".

2. Rejected IKE Messages

During the IKE negotiation process, some abnormal activities of the VPN peer will cause the Vigor router to reject its requests which attempt to establish a IPSec VPN connection. To effectively know the failures on establishing a VPN connection, the Vigor routers provides the following log messages to record the rejection reasons. Each log entry includes minimally *Date/Time*, *Source and Destination IP address*, *Cookie pair* (i.e *Initiator cookie* and *Responder cookie*), *Payload responsible for rejection*, and *Reason for Rejection*. The corresponding syntax of the log messages is shown below.

(Rejected IKE Message) => Source IP = *src_addr,* **Destination IP =** *dst_addr,* **I_Cookie =** *Initial_cookie,* **R_Cookie =** *Response_cookie,* **Rejection Payload =** *payload_name* **=> Failed:** *Reason for Rejection*

where

(Rejected IKE Message)/Source IP/Destination IP/I_Cookie/R_Cookie/ Rejection Payload/Failed: All of them are reserved words appearing in the syslog messages.

src_addr: Show the IP address of the sender which is a VPN peer to initiate a VPN connection.

dst_addr: Show the IP address of the recipient which is another VPN peer.

Initial_cookie: Show the Initiator's cookie.

Response_cookie: Specify the Responder's cookie.

payload_name: Display the payload responsible for rejection. The payload_name could be

NULL,

ISAKMP Header Payload,

Security Association Payload,

Proposal Payload,

Transform Payload,

Key Exchange Payload,

Identification Payload,

Certificate Payload,

Certificate Request Payload,

Hash Payload,

Signature Payload,

Nonce Payload,

Notification Payload,

Delete Payload, and

Vendor ID Payload.

Reason for Rejection: Show the reason for rejection when some error occurs at the IKE negotiation phase or at the establishment phase of a SA (Security Association). For any error occurred at the IKE negotiation phase, this filed will use the following format for illustration purpose.

IKE Error Message

On the other hand, for any error occuring at the establishment phase of a SA, the reason for rejection will use the following format to explain it.

IKE State status =>Notify Error Message

Now, let us describe them in more detail.

IKE Error Message: Show the error messages during the IKE negotiation process and the error message could be one of the following reasons.

“ISAKMP Header Failed!”,

“The packet size *packet_size* differs from the size specified in ISAKMP HDR *packet_len_ isakmp*”

“Message ID was *Msg_id* but should be zero in Main Mode”

“Initiator Cookie must not be zero in Main Mode message”

“Without default dial-in pre-shared key, Dial-in function is disabled for dynamic ip client”

“Initial Main Mode message is invalid: its Encrypted Flag is on”

“This is a duplicate packet”

“Main Mode message is a part of an unknown exchange”

“Message ID was *Msg_id* but should be zero in Aggressive Mode”

“Initiator Cookie must not be zero in Aggressive Mode message”

“Aggressive Mode message is a part of an unknown exchange”

“Informational Exchange is for an unknown (expired?) SA”

“Encrypted Informational Exchange message is invalid! because it is for incomplete ISAKMP SA”

“Informational Exchange message is invalid! because it has a Message ID of 0”

“Informational Exchange message is invalid! because it has a previously used Message ID (*Msg_id*)”

“Informational Exchange message for an established ISAKMP SA must be encrypted”

“Quick Mode message is invalid because it has an Initiator Cookie of 0”

“Quick Mode message is invalid because it has a Responder Cookie of 0”

“Quick Mode message is invalid because it has a Message ID of 0”

"Quick Mode message is for a non-existent (expired?) ISAKMP SA"

"Quick Mode message is unacceptable because it is for an incomplete ISAKMP SA"

"Quick Mode I1 message is unacceptable because it uses a previously used Message ID *Msg_id* (perhaps this is a duplicated packet)"

"Unsupported exchange type *Exchange_type* in message"

"Retransmitting in response to duplicate packet; already *IKE State status*"

"Discarding duplicate packet -- exhausted retransmission; already *IKE State status*"

"Discarding duplicate packet; already *IKE State status*"

"Discarding encrypted message for an unknown ISAKMP SA"

"Discarding encrypted message because we haven't yet negotiated keying material"

"Malformed message: not a multiple of encryption block size"

"Packet rejected: should have been encrypted"

"More than *max_payload* payloads in the message; ignored"

"Message ignored because it contains an unknown or unexpected payload type (*Payload_type*:) at the outermost level"

"Message ignored because it contains a payload type (*Payload_type*:) unexpected in this message"

"Malformed payload in packet"

"Message for *IKE State status* is missing payloads"

"Malformed Phase 1 message: does not start with an SA payload"

"Malformed Quick Mode message: does not start with a HASH payload"

"Malformed Quick Mode message: SA payload is in a wrong position"

“**Malformed Quick Mode message: if any ID payload is present, there must be exactly two**”

“**Malformed Quick Mode message: the ID payloads are not adjacent**”

“**State transition function for *IKE State status* had internal error**”.

where

packet_size: Show the received packet size.

packet_len_isakmp: Show the packet length in the ISAKMP Header.

Msg_id: Indicate the Unique Message Identifier.

Exchange_type: Show the exchange type of the ISAKMP Header.

max_payload: Show the maximum number of payloads.

Payload_type: Show the Next Payload type of the ISAKMP Header.

IKE State status: Display the phase and mode of the IKE negotiation process. One of the following messages may appear in the field of *IKE State status*.

STATE_MAIN_R0

STATE_MAIN_I1

STATE_MAIN_R1

STATE_MAIN_I2

STATE_MAIN_R2

STATE_MAIN_I3

STATE_MAIN_R3

STATE_MAIN_I4

STATE_QUICK_R0

STATE_QUICK_I1

STATE_QUICK_R1

STATE_QUICK_I2

STATE_QUICK_R2

STATE_INFO

STATE_INFO_PROTECTED

STATE_AGGR_R0

STATE_AGGR_I1

STATE_AGGR_R1

STATE_AGGR_I2

STATE_AGGR_R2

Notify Error Message: Notify the error message to specify why an SA can not be established successfully. The error message could be one of the following forms.

"INVALID_PAYLOAD_TYPE"

"DOI_NOT_SUPPORTED"

"SITUATION_NOT_SUPPORTED"

"INVALID_COOKIE"

"INVALID_MAJOR_VERSION"

"INVALID_MINOR_VERSION"

"INVALID_EXCHANGE_TYPE"

"INVALID_FLAGS"

"INVALID_MESSAGE_ID"

"INVALID_PROTOCOL_ID"

"INVALID_SPI"

"INVALID_TRANSFORM_ID"

"ATTRIBUTES_NOT_SUPPORTED"

"NO_PROPOSAL_CHOSEN"

"BAD_PROPOSAL_SYNTAX"

"PAYLOAD_MALFORMED"

"INVALID_KEY_INFORMATION"

"INVALID_ID_INFORMATION"

"INVALID_CERT_ENCODING"

"INVALID_CERTIFICATE"

"CERT_TYPE_UNSUPPORTED"

"INVALID_CERT_AUTHORITY"

"INVALID_HASH_INFORMATION"

"AUTHENTICATION_FAILED"

"INVALID_SIGNATURE"

"ADDRESS_NOTIFICATION"

"NOTIFY_SA_LIFETIME"

"CERTIFICATE_UNAVAILABLE"

"UNSUPPORTED_EXCHANGE_TYPE"

"UNEQUAL_PAYLOAD_LENGTHS"

For example: Suppose a VPN peer with the IP address of 172.16.2.220 intends to establish an IPSec VPN tunnel with another VPN peer having the IP address of 172.16.2.110 by using an IKE Main Mode. However, it fails to establish such a VPN connection due to lack of proposal chosen. Thus, the Vigor router will show the following log message in response to the rejection reason.

(Rejected IKE Messages) => Source IP = 172.16.2.220, Destination IP = 172.16.2.110, I_Cookie = 0x00 80 40 a0 d0 e8 f4 fa, R_Cookie = 0x9a 65 e4 6f 00

45 26 a8, Error Payload = ISAKMP Header Payload => Failed: STATE_MAIN_I1 => NO_PROPOSAL_CHOSEN.

3. Discarded ESP packets

With regarding to discarded ESP (Encapsulating Security Payload) packets, the Vigor router also log the corresponding messages. Similar to the messages mentioned in the previous section, each log entry includes minimally *Date/Time*, *SPI (Security Parameter Index) value, Soure and Destination IP address*, *Sequence Number,* and *Reason for Discard*. The format of the log messages is shown below.

(Discarded ESP packets) => SPI = *spi*, **Source IP =** *src_addr*, **Destination IP =** *dst_addr*, **Sequence number =** *seq_num* **=>** *Reason for Discard*

where

Discarded ESP packets/SPI/Source IP/Destination IP/Sequence number: All of them are reserved words in the log messages.

spi: Show the security parameter index of the packet.

src_addr: Show the source IP address of a VPN Gateway which triggers a VPN connection.

dst_addr: Indicate the destination IP address of a VPN Gateway.

seq_num: Show the sequence nember of the received packet.

Reason for Discard: Display the reason for discarded Encapsulating Security Payload packet. The reason could be

"Authenticator length error"

"Event To Cypher failed, free buffer"

"Got packet with content length = ***content_length*** **-- should be on 4-octet boundary, packet dropped"**

"Source address of pkt does not agree with expected SA source address policy"

"Replay window counter rolled, expiring SA"

"Duplicate frame from *sender_ip*, packet dropped"

"Authentication failed on incoming packet from *sender_ip*: dropped"

"Got packet with ESP Payload length = *esp_length* -- should be on 8 octet boundary, packet dropped"

"Decryption fail!"

"Got packet with ESP Payload length(AES Encryption) = *esp_length* -- should be on 16 octet boundary, packet dropped"

"Warning, decrypted packet from *sender_ip* has bad padding...may be bad decryption – dropped"

Parameters used for the Reason for Discard are defined below.

content_length: Show the content length of the received packet.

sender_ip: Show the source IP address of the packet from sender.

esp_length: Show the length of the Encapsulating Security Payload (ESP) packet.

For example: Suppose a VPN peer with the IP address of 172.16.2.220 has established successfully an IPSec VPN tunnel with another VPN peer having the IP address of 172.16.2.110. However, it fails to transmit packets through such a VPN tunnel due to failed decryption at the packet with sequence number 0x1. As a result, the Vigor router will show the following log message in response to the discarded ESP packet.

(Discarded ESP packets) => SPI = *0x*13c32319, Source IP = 172.16.2.220, Destination IP = 172.16.2.110, Sequence number = 0x1 => Decryption fail!

4. IKE Negotiate Packet Messages (IPSec)

The administrator may be interested in understanding some information regarding to the IKE negotiation packets, for instance cookie pair, payload type of the ISAKMP header, the exchange type number of the ISAKMP header, and so forth. Hence, the Vigor router further provides the following log messages to record the related status. The format of the log messages is defined as follows.

IKE *direction* **I Cookie =** *Initial_cookie* , **R Cookie =** *Response_cookie* , **Next Payload =** *Payload_type* , **Exchange Type =** *Exchange_type_no,* **Message ID =** *Msg_id*

where

IKE/I Cookie/R Cookie/Next Payload/Exchange Type/Message ID: All of them are reserved words in the log messages and stand for Internet Key Exchange/Initial Cookie/Response Cookie/Next Payload type/ Exchange Type/Message Identity, respectively,

direction: Indicate the direction of the IKE packet. Use "==>" to represent the outbound packet and employ "<==" to illustrate the inbound packet.

Initial_cookie: Show the initiator cookie.

Response_cookie: Display the responder cookie.

Payload_type: Show the Next Payload type of the ISAKMP Header. There are several payload types which are described below.

ISAKMP_NEXT_NONE: indicate "No Other Payload Followed".

ISAKMP_NEXT_SA: represent the "Security Association Payload".

ISAKMP_NEXT_P: be the "Proposal Payload".

ISAKMP_NEXT_T: indicate the "Transform Payload".

ISAKMP_NEXT_KE: indicate the "Key Exchange Payload".

ISAKMP_NEXT_ID: indicate the "Identification Payload".

ISAKMP_NEXT_CERT: indicate the “Certificate Payload”.

ISAKMP_NEXT_CR: indicate the “Certificate Request Payload”.

ISAKMP_NEXT_HASH: indicate the “Hash Payload”.

ISAKMP_NEXT_SIG: indicate the “Signature Payload”.

ISAKMP_NEXT_NONCE: indicate the “Nonce Payload”.

ISAKMP_NEXT_N: indicate the “Notification Payload”.

ISAKMP_NEXT_D: indicate the “Delete Payload”.

ISAKMP_NEXT_VID: indicate the “Vendor ID Payload”.

Exchange_type_no: Show the exchange type number of the ISAKMP Header. The possible number and its associated meanning is shown below.

0x0: ISAKMP_XCHG_NONE

0x1: ISAKMP_XCHG_BASE

0x2: ISAKMP_XCHG_IDPROT (for ID Protection)

0x3: ISAKMP_XCHG_AO (for Authentication Only)

0x4: ISAKMP_XCHG_AGGR (for Aggressive mode)

0x5: ISAKMP_XCHG_INFO (for Informational)

0x20: ISAKMP_XCHG_QUICK (for Oakley Quick Mode)

0x21: ISAKMP_XCHG_NGRP (for Oakley New Group Mode)

0x22: ISAKMP_XCHG_ACK_INFO (for Oakley Acknowledged Informational)

Msg_id: Show the Unique Message Identifier.

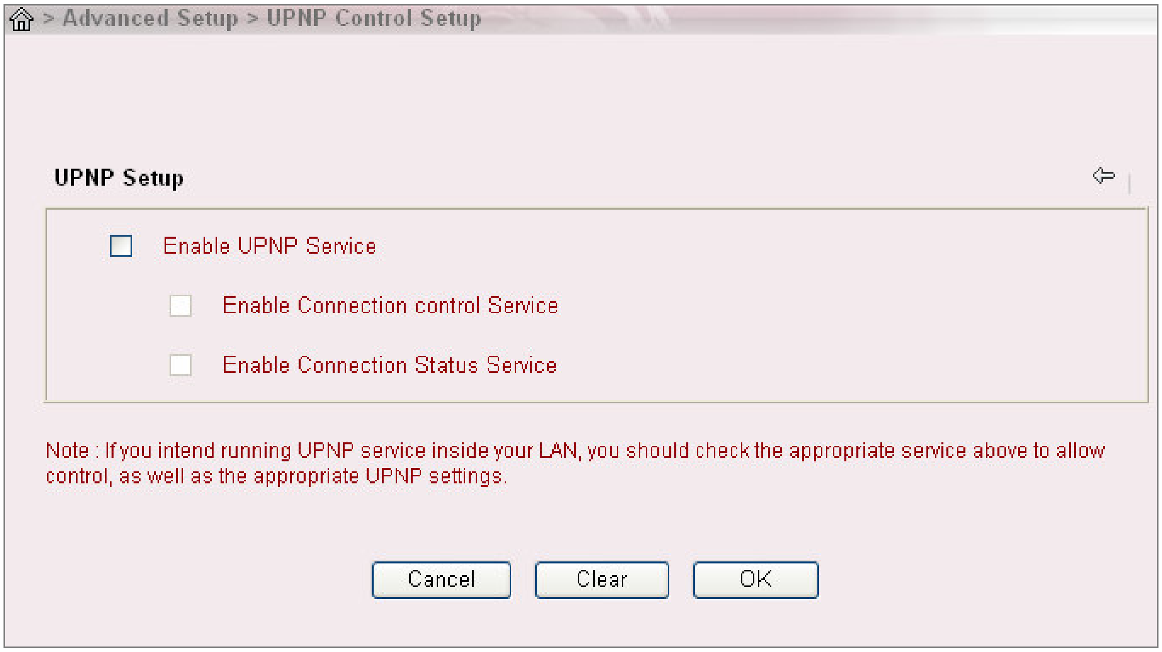
For example**:** Herein, we use a log message to trace the outbound IKE negotiation packet, as shown below.

```
IKE ==> I Cookie = 0x00 80 40 a0 d0 e8 f4 fa, R Cookie = 0x00 00 00 00 00 00
00 00, Next Payload = ISAKMP_NEXT_SA, Exchange Type = 0x2, Message ID
= 0x0
```

Chapter 15
UPnP Service Setup

15.1 Introduction

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.


> Advanced Setup > UPNP Control Setup
UPNP Setup
☐ Enable UPNP Service
☐ Enable Connection control Service
☐ Enable Connection Status Service
Cancel
Clear
OK

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

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.

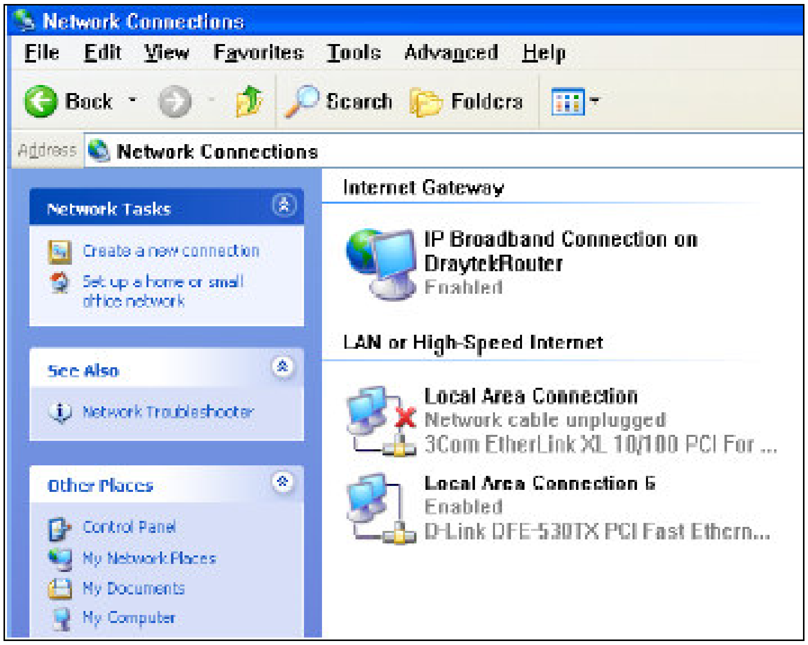
UPnP is available on Windows XP and the router provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

15.2 Configuration

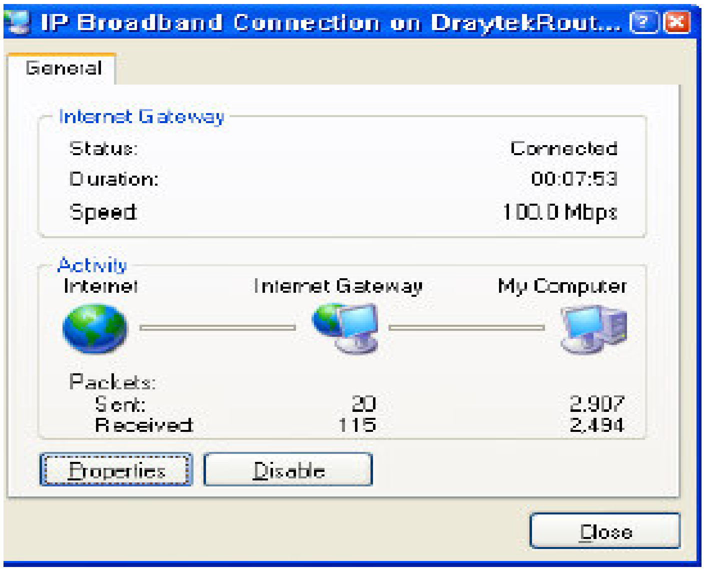
You can enter the **UPNP Setup** via **Advanced Setup > UPNP Service Setup** on the Web Configurator in your router.

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.



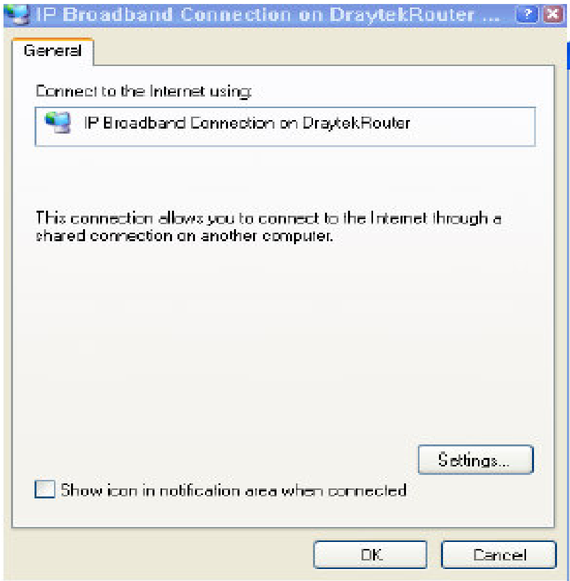
The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots above show examples of this facility.



Status: Connected
Duration: 00:07:53
Speed: 100.0 Mbps

Packets:
Sent: 20 2,907
Received: 115 2,494

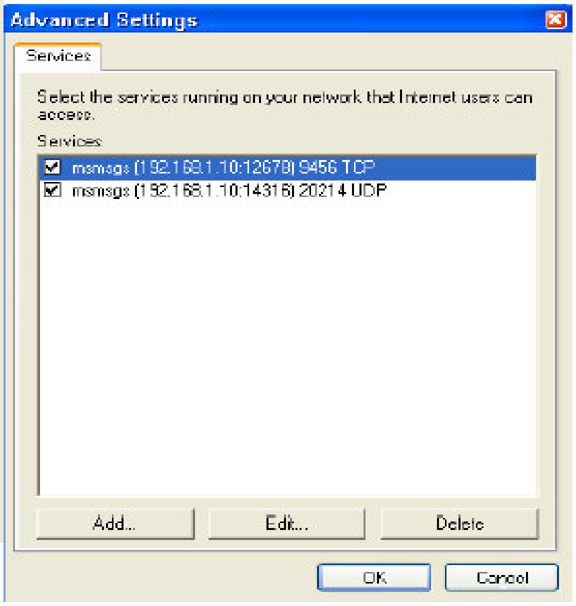
The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router, learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal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



Connect to the Internet using:
IP Broadband Connection on DraytekRouter

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

☐ Show icon in notification area when connected



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

Services
☑ msmsgs (192.168.1.10:12679) 9456 TCP
☑ msmsgs (192.168.1.10:14316) 20214 UDP

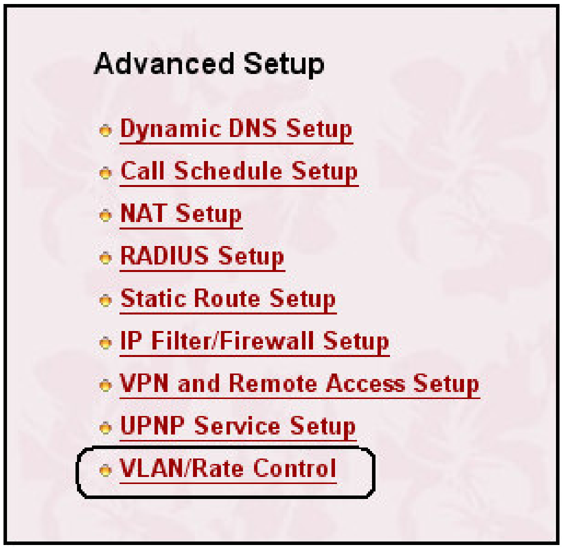
Chapter 16
VLAN / Rate Control

16.1 Introduction

VLAN stands for **Virtual Local Area Network** and, conceptually, represents a broadcast domain. In the switched networks, a broadcast packet or a packet with an unknown destination MAC (Medium Access Control) address will be forwarded to all other ports in a broadcast fashion. This leads to significant reduction of the whole network performance. To increase the router performance and support stronger security, the Vigor2900 series security router provides the **VLAN Control** facility. By grouping some ports into one VLAN, broadcast packets will only be sent to the ports within the same VLAN without affecting the traffic of other ports outside the VLAN. This is because the broadcast domains are independent for different VLANs. All packets from individual ports can't cross different VLANs. Further, any port can be grouped as one VLAN, and one port can be shared among different VLANs. Thus, the VLAN facility improves the efficiency of network resource usage and network security.

Rate Control facility allows you to set the upper bound of the port forwarding rate, also called “bandwidth throttling rate”. In other words, this facility allows you to set a maximum inbound and/or outbound bandwidth available for each LAN port. It will be of great value to minimize the impact on other users from one user who would otherwise monopolize the network transmission bandwidth (e.g. playing games or downloading large files).

The following sections describe the web configuration for setting up the VLAN/Rate Control facility, including specific configuration information and any limitation they have. One can find the entrance of this setting, named as **VLAN/Rate Control**, in the main menu, as depicted in the following figure.



16.2 VLAN Configuration

After clicking the VLAN/Rate Control in the main menu, the associated web configuration appears as shown below.

Enable: One checkbox appears giving the choice to activate the *VLAN function* or not. To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear.

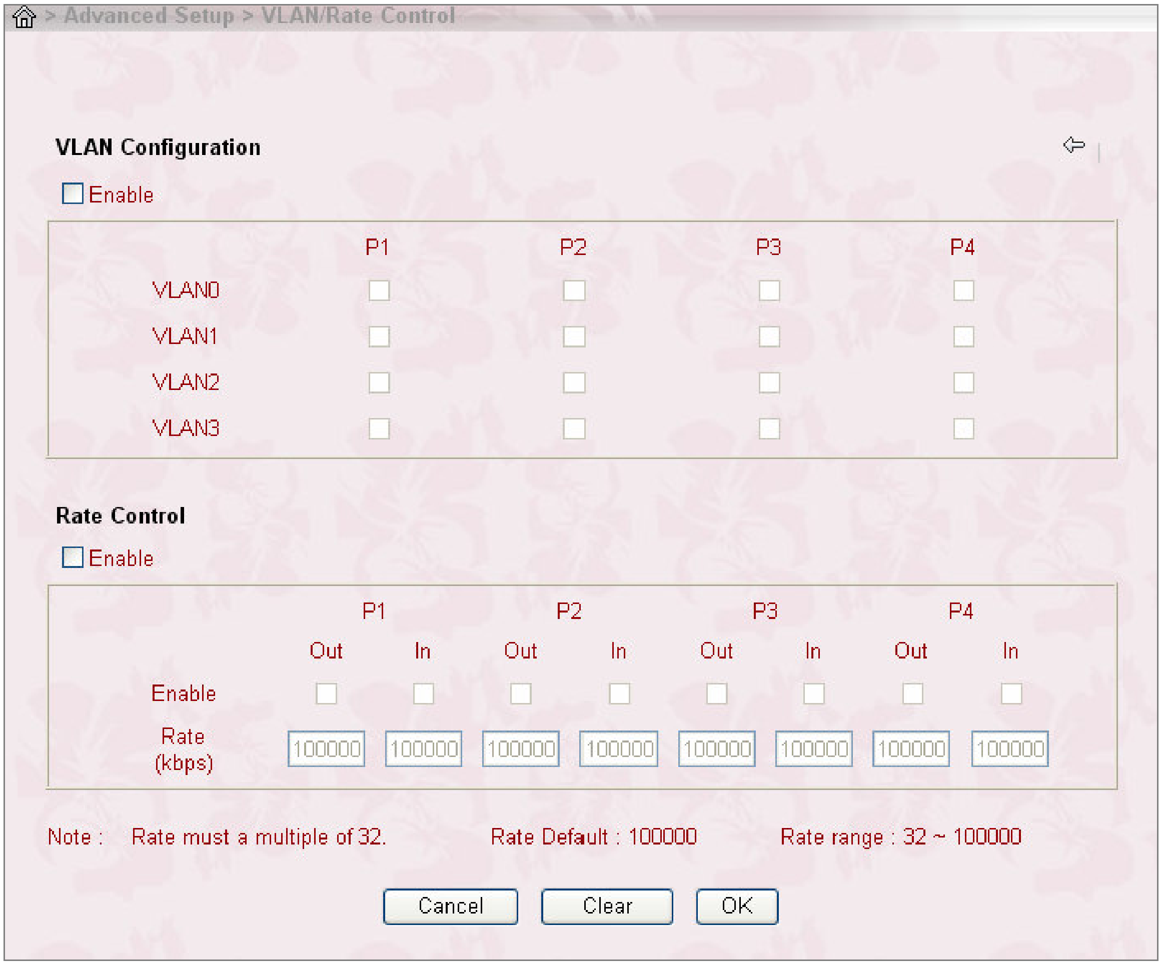
In the Vigor2900 series security router, there are 4 VLAN groups available for users. They are called **VLAN0**, **VLAN1**, **VLAN2**, and **VLAN3**, respectively. Select the ports that you want to cluster them in one VLAN group by clicking the appropriate checkboxes. Other unchecked ports will be automatically arranged as one VLAN, say non-visible VLAN group. It should be noticed that, if only one port is arranged as a VLAN, then this port only could communicate with WAN port.

P1: Specify LAN port 1.

P2: Specify LAN port 2.

P3: Specify LAN port 3.

P4: Specify LAN port 4.



> Advanced Setup > VLAN/Rate Control

VLAN Configuration

☐ Enable

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

Rate Control

☐ Enable

	P1		P2		P3		P4	
	Out	In	Out	In	Out	In	Out	In
Enable	☐	☐	☐	☐	☐	☐	☐	☐
Rate (kbps)	100000	100000	100000	100000	100000	100000	100000	100000

Note : Rate must a multiple of 32. Rate Default : 100000 Rate range : 32 ~ 100000

16.3 Rate Control Configuration

Now, let us continue to introduce the **Rate Control** configuration. Again, we use the same figure shown above.

Enable: One checkbox is available to activate this function that will control the upper bound of the port forwarding rate. To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear.

For each LAN ports (named **P1**, **P2**, **P3** and **P4**), the router provides two options for users to limit the incoming and/or outgoing bandwidth. Simply click the checkbox

"In" or "Out" under the appropriate LAN port index and then enter the rate under that "In" or "Out" checkbox. Accordingly, the **Rate Control** facility will apply on selected LAN ports. To turn off a Rate Control setting for a particular port, simply click on the appropriate checkbox to disable it.

Out: Click it to enable the outbound (upload) Rate Control for the selected LAN port.

In: Click it to enable the inbound (download) Rate Control for the selected LAN port.

Rate: Enter a number that is multiple of 32 (i.e. 32, 64, 96, 128...) and less than 100,000. This number indicates the maximum granted-rate (in kbps) for the selected LAN port in the selected direction.

Chapter 17
QoS (Quality of Service) Control Setup

17.1 Introduction

The Vigor router normally distribute the available Internet bandwidth equally between all local users and all applications. In the case of a file download, it's quite reasonable to merely receive the file as soon as resources allow, taking the demands and needs of other into account, equally important users and applications while downloading, you can get on with other work.

If Jane's E-mail attachment is an important contract and David's file download is a computer game, it is obvious that David can wait for more than 1 hour as it is **very low priority** for the company. On the other hand, it is very essential for Jane to quickly download her E-mail attachment which she needs to review with her attorney within certain time frame. Jane's E-mail is **very high priority** for the company. This is what QoS is all about – giving different priorities to different types of data of users and allocating them with the most appropriate Internet bandwidth.

DrayTek's Quality of Service Assurance (QoS) lets you select sets of traffic types and give each type a guaranteed percentage of the available bandwidth. Using the earlier example again, the http downloads have been limited to a very low priority of 10%, and the E-mail downloads a high priority of 90%. If David is the only person using the Internet, his http file download will come in at 1Mb/s, but as soon as Jane starts her E-mail download, David's download speed will drop to 0.1Mbps, whilst Jane gets 0.9Mb/s –90% of the bandwidth.

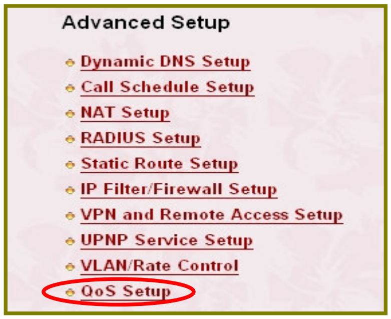
Without QoS-guaranteed control, there is virtually no way to prioritize users/services or to guarantee allocation of finite bandwidth resources to network or servers for supporting timing-sensitive and mission-critical network applications, such as VoIP (Voice over IP) and online gaming applications. The VoIP applications carry person to person voice calls across your Internet connection. You cannot wait for VoIP packets as they have to be received at re-assembled at a constant rate in order for the voice to be intelligible. It is extremely vital for VoIP traffic to be assured with the immediacy by using QoS. As such, SIP VoIP traffic is always allocated as much bandwidth as it needs if your Vigor router supports QoS.

Although priority for applications will depend on your own specific requirements, you still have plenty of other bandwidth available on a typical broadband line while the 8-32Kb/s-bandwidth-consumed VoIP traffic will be proritised and sent immediately

Moreover, in the Vigor routers, we also take the support of DSCP (Differentiated Service Code Point) code into consideration in the design of our QoS-guaranteed control module. We have already implemented **High Priority to Vigor built-in VoIP traffic and hence please do not disable "QoS" settings in order to assure your Vigor built-in VoIP calls be with High Priority.**

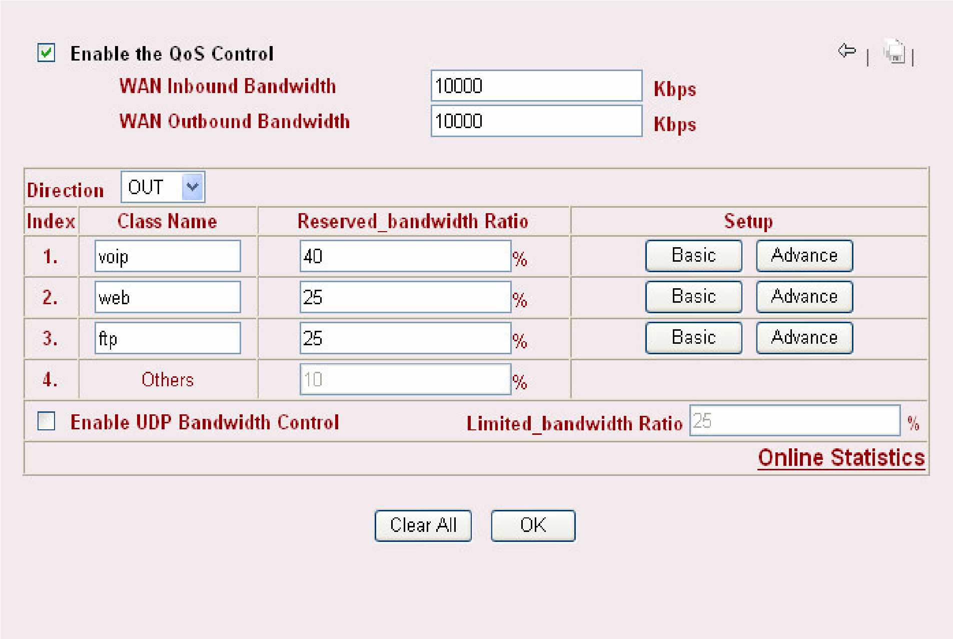
The Vigor's QoS facility provides you with differentiating traffic types on the following criteria and more detailed instructions are explained as below:

- Recognized TDP/UDP Protocols
- TCP/UDP Port Numbers
- Internet Client IP address
- Remote IP address/Subnet (e.g. a mail server, or branch office)
- Direction - Inbound or Outbound



17.2 QoS Control Setup

After clicking the **QoS Control Setup** in the **Setup Main Menu**, the following web configuration will appear on your browser. Essentially, the QoS facility consists of two types of settings for user, as shown in the following figure. One is for "**Basic**" setting and the other one is for "**Advance**" setting.



☑ Enable the QoS Control

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

Direction OUT

Index	Class Name	Reserved_bandwidth Ratio	Setup
1.	voip	40 %	Basic Advance
2.	web	25 %	Basic Advance
3.	ftp	25 %	Basic Advance
4.	Others	10 %	

☐ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

Note that the real throughput depends on the local network environment or quality of infrastructure. **The inbound/outbound bandwidths are recommended to set 80-85% of physical network speed to maximum the QoS performance.**

The **Basic setting** for QoS control function provides a convenience way for users to classify the different applications into individual groups with different guaranteed-bandwidths by *only choosing pre-defined services*.

The **Advance setting** for QoS control function provides users another way to classify applications into individual groups after *defining your own services* based on protocol type (for example TCP or UDP), source IP address/destination IP address, source port number/destination port number, and so on. More detail information about **Basic** and **Advance** setting can be found in next two sections.

Note: the QoS control function needs to perform packet classification, buffer management, scheduling, flow measurement, and so on to achieve the bandwidth guarantees on user demand. Thus, after enabling the QoS Control function, the router performance will degrade significantly.

Now, let us describe each item involved in the **QoS Control Setup** in more detail.

Enable the QoS Control: One checkbox appears to activate the QoS control function or not. Click it to force the router to perform QoS control over traffic flows. By default, it is enabled.

Note that the whole QoS control facility does not work without enabling this checkbox.

WAN Inbound Bandwidth: According to the actual incoming transmission rate offered by Internet service, please set the appropriate value in this field. If the inputted value is not proper, that could reduce the QoS function performance.

WAN Outbound Bandwidth: According to the actual outgoing transmission rate offered by Internet service, please set the appropriate value in this field. If the inputted value is not proper, that could reduce the QoS function performance.

Note : **The inbound/outbound bandwidths are recommended to set 80-85% of physical network speed to maximum the QoS performance.**

Direction: Three options ("***IN***", "***OUT***", "***BOTH***") are provided for users to apply the QoS control function on incoming, outgoing traffic flows, or both direction traffic flows. Please select the pull-down menu "***IN***","***OUT***" or "***BOTH***" for the appropriate flow direction. By default, the "***Direction***" is set as "***OUT***".

IN: All incoming flows (from WAN to LAN side) are under control of QoS functionality.

OUT: All outgoing packets (from LAN to WAN side) are under the control of QoS functionality.

BOTH: The QoS functionality will be applied simultaneously on incoming and outgoing flows.

Index: Each index number represents a particular traffic class. The Vigor router provides up to four traffic classes for users to apply the QoS control facility.

Class Name: As mentioned above, four traffic classes are provided and only first three class names can be defined by users. The forth class name is reserved as "Others" which means other traffic flows not being defined or classified in the first three traffic classes. The maximum length for each class name is 12 characters. By default, first three class names are empty.

Reserved-bandwidth Ratio: Each class has one blank for the user to specify the bandwidth ratio that he wants. By default, all blanks are empty. With each reserved-bandwidth ratio, the allowed maximum and minimum values are 97 and 1, respectively. Supposed that the first three classes have been specified their own reserved-bandwidth ratios (and sum of individual ratios are less than 100%), the web configurator will automatically compute the remaining bandwidth ratio for "Others" class (i.e. the fourth class) and then display the result in the field of the reserved-bandwidth ratio for "Others" class.

Note: when the reserved-bandwidth ratio of a class is not in between 1 and 97, the web configurator will automatically detect this error and pop up a warning message, ***"Reserved-bandwidth ratio for each class should be in between 1***

***and 97.*"** In addition, if sum of reserved-bandwidth ratios for all classes exceeds 100%, then the web configurator is also capable of detecting this error and in turn pop up the warning message, ***"Sum of reserved-bandwidth ratios for all classes can not exceed 100%*"**. For example, assume that the reserved-bandwidth ratios for the first two classes are 50% and 60%, respectively, it is clear that the sum of their reserved-bandwidth ratios exceeds 100%, resulting in that the warning message, ***"Sum of reserved-bandwidth ratios for all classes can not exceed 100%.*"** appears in your browser.

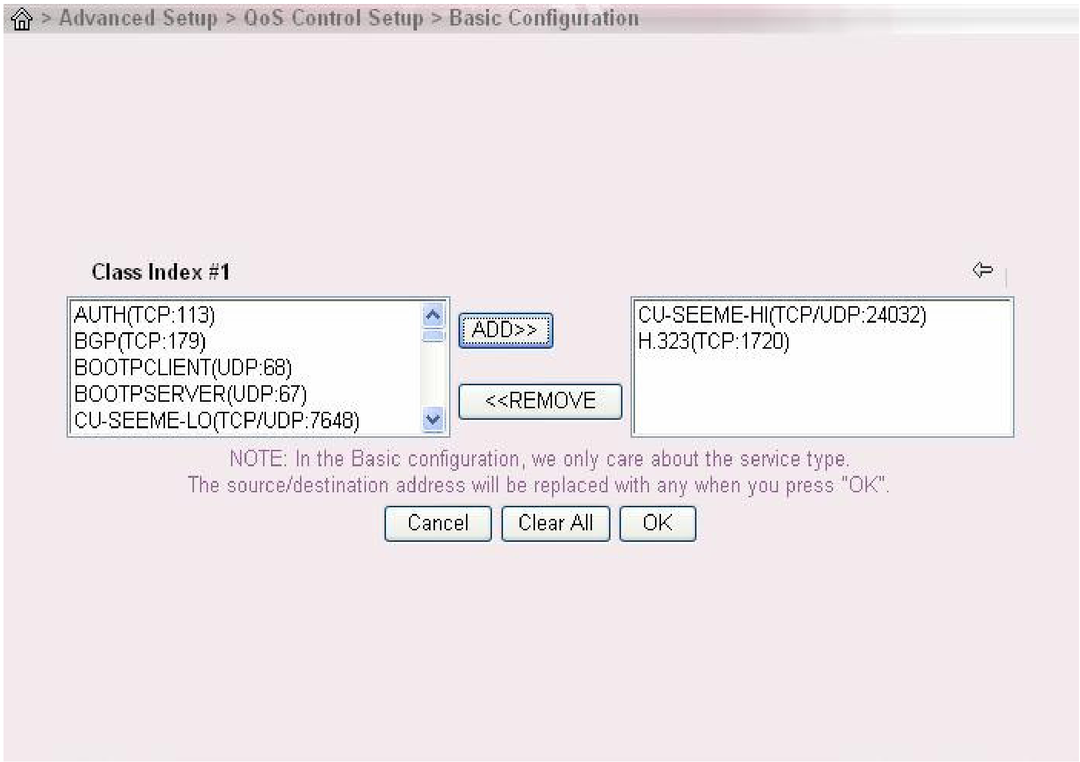
Basic and Advance: For each class, the Vigor router provides two ways to set up the QoS control function. One way is to classify Internet applications into individual groups by *only choosing pre-defined services*. Users can click the "**Basic**" button for such settings. Another way is to classify applications into individual groups by *defining your own services based on protocol type (for example TCP or UDP), source IP address/destination IP address, source port number/destination port number, and so on*. Users can check the "**Advance**" to know how to setup. More detail information about **Basic** and **Advance** configurations can be found in next two sections.

Enable UDP Bandwidth Control: If the flag is enabled, bandwidth usage of all defined UDP packets in each class can not exceed the **limited bandwidth ratio** of total throughput. It prevents low priority UDP packets consuming all the bandwidth and also guarantees bandwidth will be available for critical TCP services.

Online Statistics: After click it, the web configuration will switch to another scene which shows the instant bandwidth usages of individual traffic classes.

***For example*:** *As shown in the following figure, the option of "**Direction**" is chosen as "**OUT**" and, accordingly, the QoS control facility will be applied on all outbound packets (i.e. all packets from LAN to WAN side). Four classes are named as "voip", "web", "ftp", and "Others", respectively. Their associated reserved-bandwidth ratios are 45%, 25%, 25%, and 10%, respectively.*

17.3 Basic Configuration



NOTE: In the Basic configuration, we only care about the service type.
The source/destination address will be replaced with any when you press "OK".

After clicking the “**Basic**” button in the QoS Control Setup page, the web configuration, as shown above, will appear. Clearly, two frames are provided and, by default, the right frame is empty. The left frame is filled with pre-defined services. The pre-defined services are listed as follows.

“ANY”,

“AUTH(TCP:113)”,

“BGP(TCP:179)”,

“BOOTP_CLIENT(UDP:68)”,

“BOOTP_SERVER(UDP:67)”,

“CU-SEEME-HI(TCP/UDP:24032)”,

“CU-SEEME-LO(TCP/UDP:7648)”,

“DNS (TCP/UDP:53)”,

“FINGER(TCP:79)”,

"FTP(TCP:20~21)",

"H.323(TCP:1720)",

"HTTP(TCP:80)",

"HTTPS(TCP:443)",

"IKE(UDP:500)",

"IPSEC-AH(IP:51)",

"IPSEC(IP:50)",

"IRC(TCP/UDP: 6667)",

"L2TP(UDP:1701)",

"NEWS(TCP:144)",

"NFS(UDP:2049)",

"NNTP(TCP:119)",

"PING(IP:1)",

"POP3(TCP: 110)",

"PPTP(TCP:1723)",

"RCMD(TCP:512)",

"REAL-AUDIO(TCP:7070)",

"RTSP (TCP/UDP:554)",

"SFTP(TCP:115)",

"SMTP(TCP:25)",

"SNMP(TCP/UDP: 161)",

"SNMP-TRAPS(TCP/UDP:162)",

"SQL-NET(TCP:1521)",

"SSH(TCP/UDP:22)",

"SYSLOG(UDP:514)",

"TELNET(TCP:23)", and

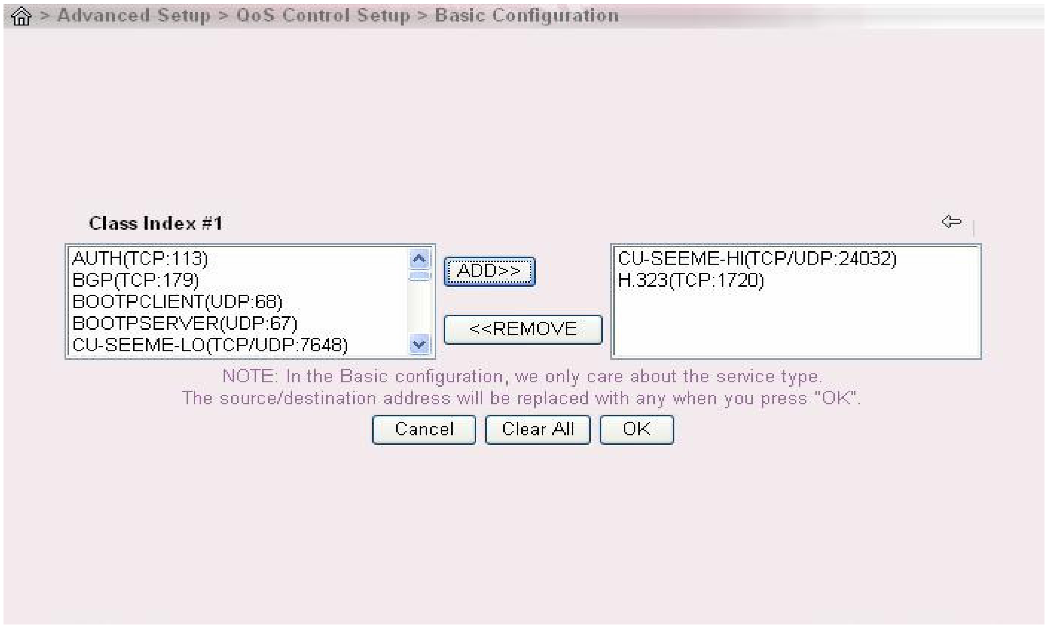
"TFTP(UDP:69)".

ADD >>: If one selects a service, say H.323 (TCP: 1720), in the left frame and presses the "***ADD>>***" button, then this H.323 (TCP: 1720) service (application) will be moved from left frame to the right frame.

REMOVE<<: In contrast to "***ADD>>***" button, clicking the "***<<REMOVE***" button will move one service selected in the right frame to the left frame.

For example: *Consider the basic setting for class index #1 whose reserved-bandwidth ratio is 40% and the QoS control function on all outgoing packets. As depicted in the following figure, one can easily find that two services (applications), H.323 (TCP: 1720) and CU-SEEME (TCP/UDP: 7648, 24032), have been moved from the left frame to the right frame. This means that the Vigor router will only allow the outbound packets of "Class index #1" coming from (TCP port 1720) or (TCP/UDP ports 7648, 24032) to utilize at most 40% outgoing bandwidths.*

Notice that, in this example, the set of services in the left frame for all Classes no longer includes H.323 (TCP: 1720) and CU-SEEME (TCP/UDP: 7648, 24032) applications.



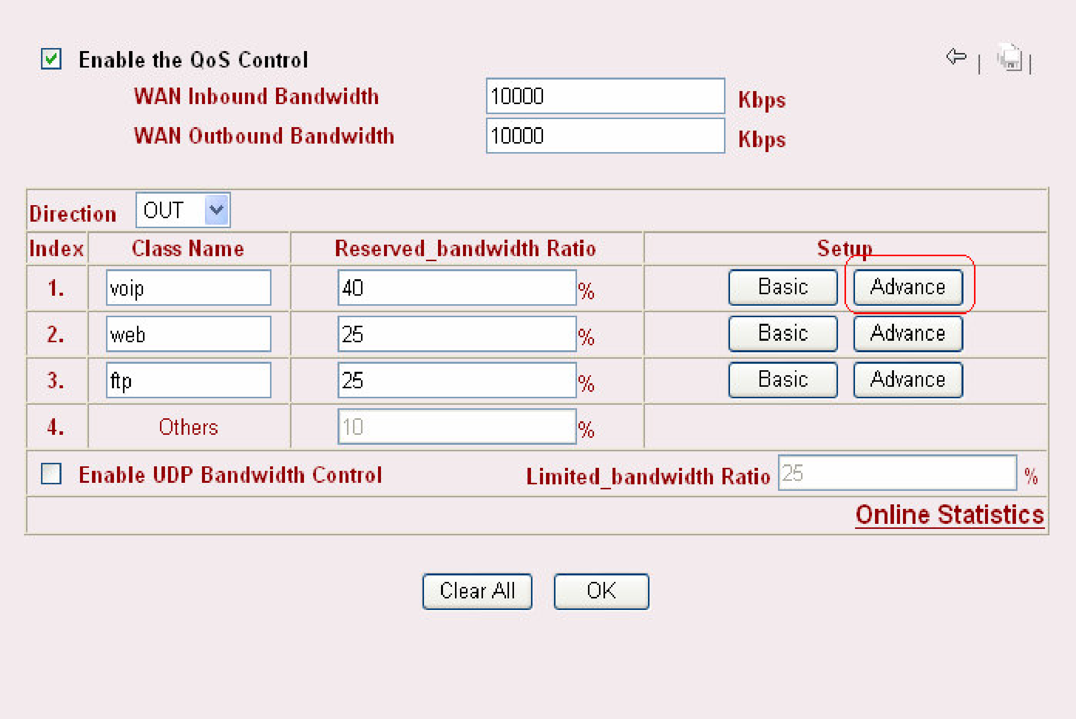
Class Index #1

AUTH(TCP:113)
BGP(TCP:179)
BOOTPCLIENT(UDP:68)
BOOTPSERVER(UDP:67)
CU-SEEME-LO(TCP/UDP:7648)

CU-SEEME-HI(TCP/UDP:24032)
H.323(TCP:1720)

NOTE: In the Basic configuration, we only care about the service type.
The source/destination address will be replaced with any when you press "OK".

17.4 Advanced Configuration



☑ Enable the QoS Control

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

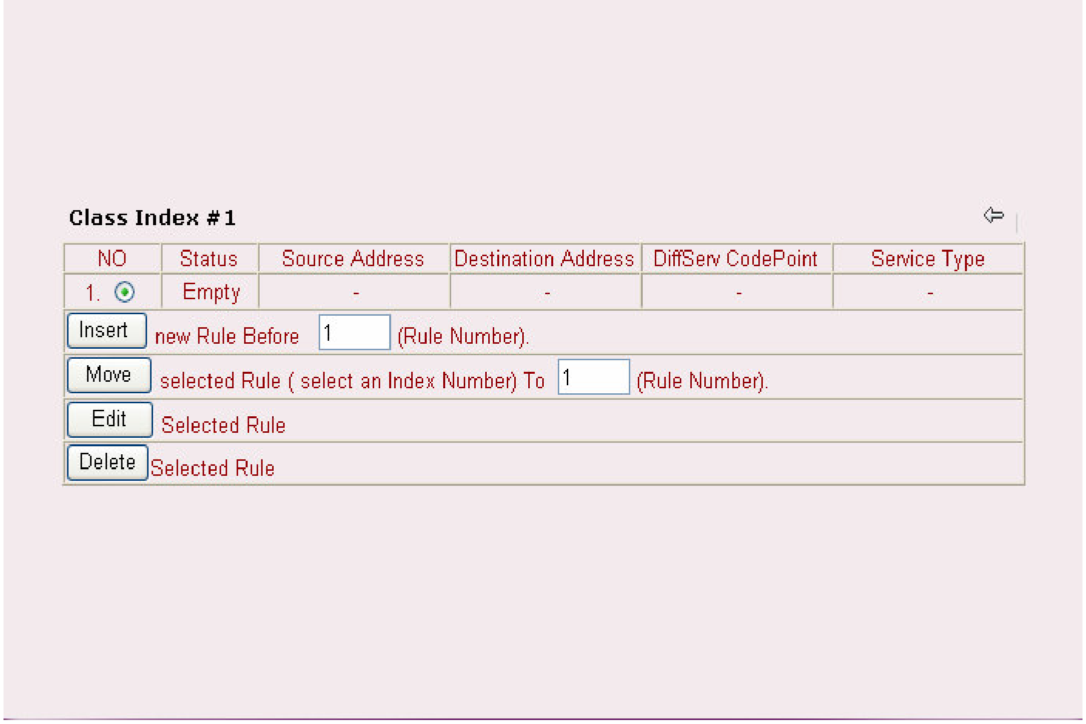
Direction OUT

Index	Class Name	Reserved_bandwidth Ratio	Setup
1.	voip	40 %	Basic Advance
2.	web	25 %	Basic Advance
3.	ftp	25 %	Basic Advance
4.	Others	10 %	

☐ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

As illustrated in the above figure, the ***QoS control Setup*** page also provides users another way to classify applications (service) into individual groups by *defining their own services based on protocol type (for example TCP or UDP), source IP address/destination IP address, source port number/destination port number, and so on*. Click the "**Advance**" button for a particular class, say Class Index #1, and subsequently the web page will change to another one, as shown below.

In this figure, one can easily find that this configuration allows users to define their own applications based on source IP address, destination IP address, and service type. For each class (excluding "**Others**" class), the maximum number of allowed user-defined applications is 20. For each user-defined application, the Vigor router provides four commands, such as "***Insert***", "***Move***", "***Edit***", and "***Delete***" to manage it. Each command and other items involved in this configuration are described as follows.



Class Index #1

NO	Status	Source Address	Destination Address	DiffServ CodePoint	Service Type
1. ●	Empty	-	-	-	-

[Insert] new Rule Before 1 (Rule Number).

[Move] selected Rule (select an Index Number) To 1 (Rule Number).

[Edit] Selected Rule

[Delete] Selected Rule

Index Number/Check circle: One circle is created for each rule and clicking it allows the user to edit the selected rule.

Status: Indicate if the specific rule is active. If one rule is activated, this field will show *Active*. Otherwise, "Inactive" will be displayed. By default, this field is filled with "Empty" representing no rule.

Source Address: Show the source IP address of a specific application.

Destination Address: Display the destination IP address of a specific application.

DiffServ CodePoint: For experienced users, they can set priority criteria basing on the service level which is defined by a specific application and thus the subsequent routers in the Internet will also decide its transmission precedence depended on what kind of a service level.

Service Type: Show the protocol type and port number over which a specific application runs.

Insert: This button provides users to insert a rule prior to another rule whose index number is specified in the blank. By default, the blank is filled with 1 (Rule Index Number).

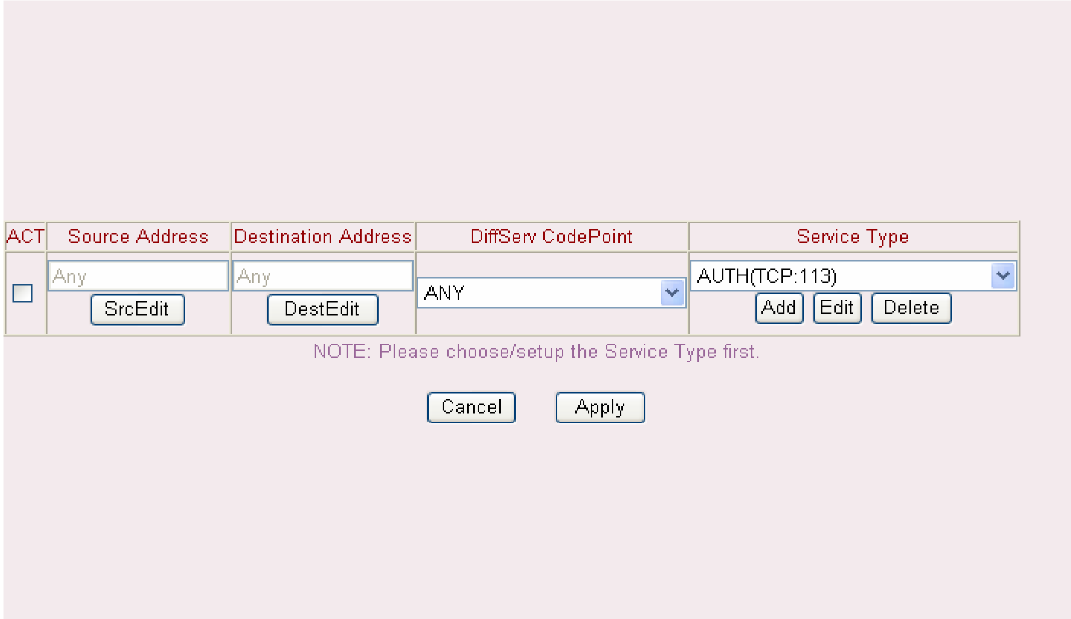
Edit: Similar to button "**Insert**", this button provides users to edit a specific rule. Before performing the edition operation, the user should choose the rule by enabling its corresponding check circle.

Move: Allow users to move the selected rule into a position with Index number *n*, which is specified in the blank. By default, the blank is filled with 1.

Delete: Allow users to remove the selected rule by enabling its corresponding check circle. By default, the selected rule will stay at Rule 1.

Advanced Configuration - Insert

As mentioned above, the "***Insert***" button allows the user to insert a rule prior to another rule whose index number is specified in the blank. For example, assuming the blank is filled with position *i*. When the insertion action is completed, the new rule will be inserted in front of rule *i* and original rules with number *j* (*j* > *i*) will move down one position in sequence. Of course, the web configuration will reflect this change.



ACT	Source Address	Destination Address	DiffServ CodePoint	Service Type
☐	Any SrcEdit	Any DestEdit	ANY	AUTH(TCP:113) Add Edit Delete

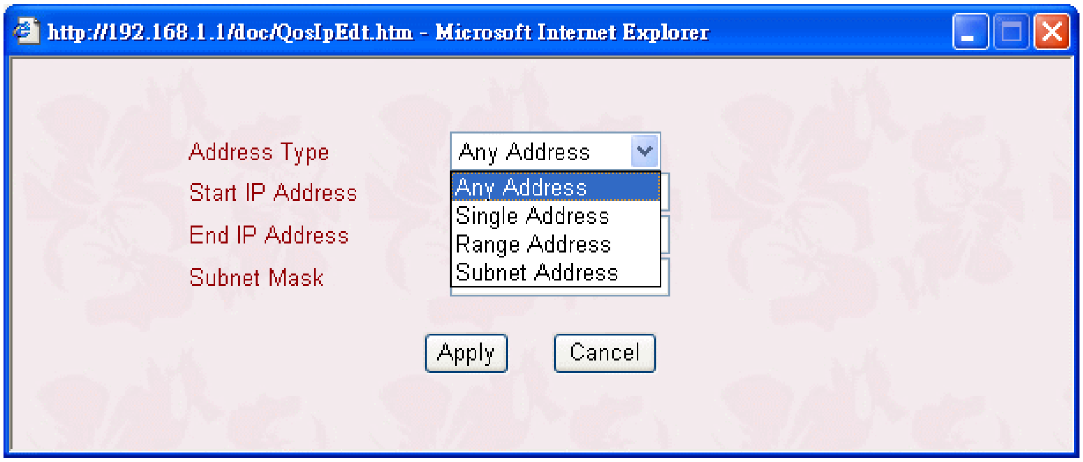
NOTE: Please choose/setup the Service Type first.

After clicking the "***Insert***" button, the web configuration will switch to another one, as shown above. Each item involved in such web configuration is described below in more detail.

ACT: Check it to enable the rule.

Source Address: Specify the source IP address of the user-defined application. By default, this field is filled with "Any".

SrcEdit button: Allow the user to edit the source IP address of the user-defined application. After clicking it, your browser will pop up a window, as shown below, for more setting.



In this figure, there is one pull-down menu to provide four options for "***Address Type***" and three blanks to specify associated addresses. The options for "***Address Type***" including "***Any Address***", "***Single Address***", "***Range Address***", and "***Subnet Address***".

Any Address: If it is selected, all remaining entries in this figure (i.e. "*Start IP Address*", "*End IP Address*", and "*Subnet Mask*") will be disabled.

Single Address: If it s selected, entries of "*End IP Address*" and "*Subnet Mask*" are disabled and only one entry of "*Start IP Address*" is available for users to specify their single source IP address.

Range Address: If it is selected, the "*Subnet Mask*" entry will be disabled and other entries are available for users to specify a group of source IP addresses. Such a group IP addresses is delimited by both values specified in fields of "*Start IP Address*" and "*End IP address*".

Subnet Mask: If this option is selected, the "*End IP Address*" entry will be disabled and other entries are available. In this case, we allow users to define a subnet by assigning values in fields of "*Start IP Address*" and "*Subnet Mask*".

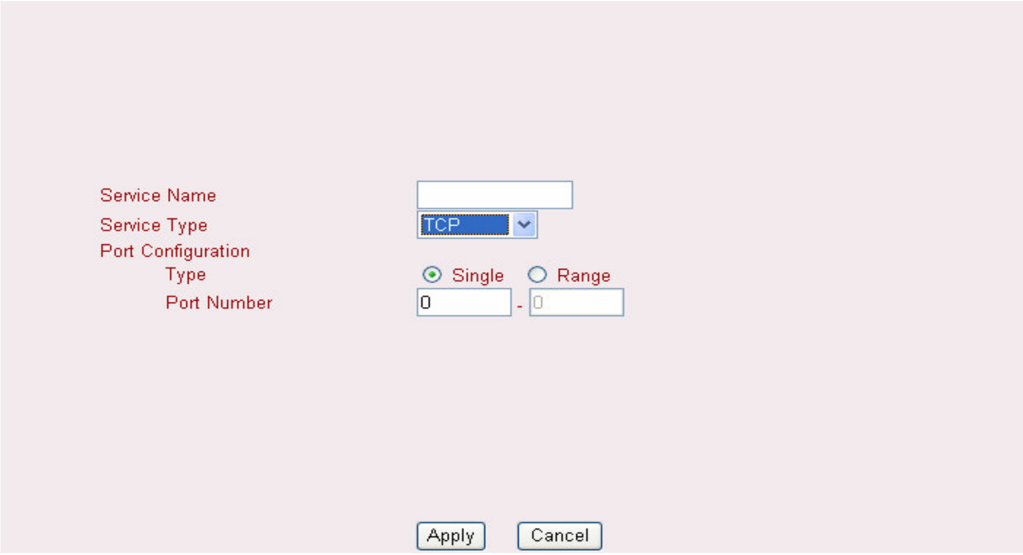
Destination Address: Specify the destination IP address of the user-defined application. By default, this field is filled with "Any".

DestEdit button: Allow the user to edit the destination IP address of the user-defined application. After clicking it, your browser will pop up a window, as shown above. All operations and their associated web configurations after clicking "***DesEdit***" button are identical to those after clicking "***SrcEdit***" button.

DiffServ CodePoint: Prioritize the service level by selecting the predefined precedence during the QoS management. However, the default value stays at "ANY".

Service Type: Show the selected or defined service type for the user-defined application. You can choose a service type through the pull-down menu and then perform edition or deletion operation. This is achieved by clicking the "***Edit***" or "***Delete***" button. In addition, you can create a new service type by clicking the "***Add***" button and then specify all necessary information. For example, this field is filled with "AUTH(TCP: 113)".

Add: After clicking this button, the web page will change to the following one so that the user is able to add a user-defined application (herein called Service Type). After the new service type is defined completely and the "***Apply***" button is pressed, the new service type will be automatically added into the pull-down menu. Several options for service type configuration is described below.



Service Name

Service Type TCP

Port Configuration

Type ● Single ○ Range

Port Number 0 - 0

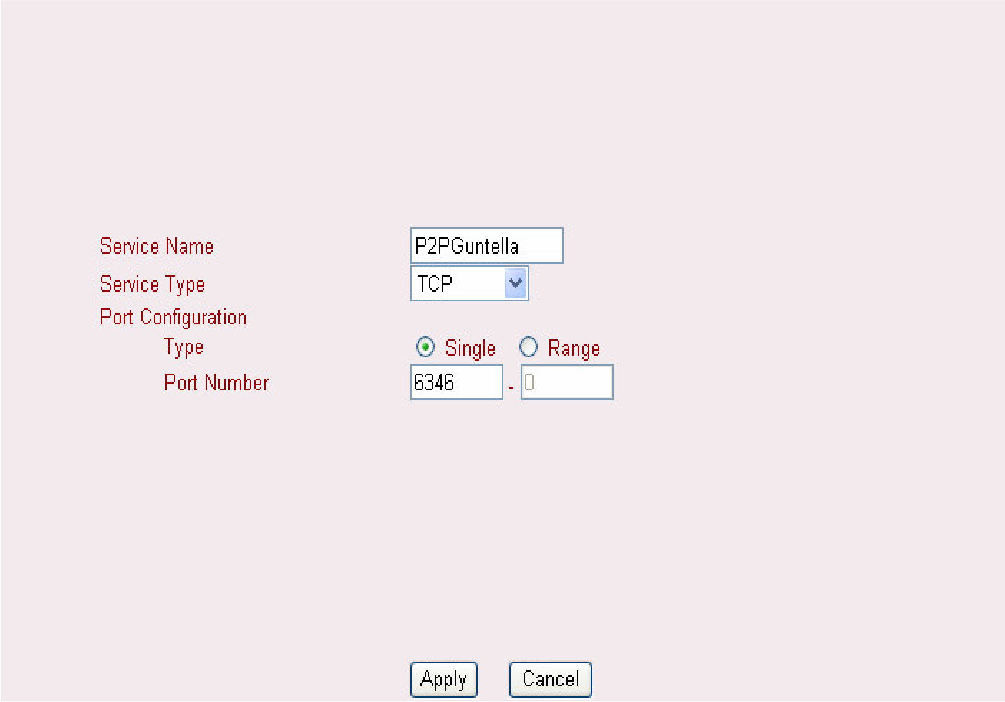
Service Name: Specify a service name whose maximum length is 12 characters. By default, this filed is empty.

Service Type: Select a protocol that the service type will carry out.

Port Configuration: Specify which port or port range will be opened for this service type.

- **Type:** Click one option for port type which could be "*Single*" port or "*Range*" ports.
- **Port Number:** If the "*Single*" port is chosen, the user could specify the single port number in the left field and the right field will be automatically disabled. If the "*Range*" type is activated, the user should define a range of ports delimited by both values of the left and right fields respectively.

Edit: After clicking this button, the user can modify any selected service type, excluding any default service type. After modification, it becomes a new user-defined service type. Please refer to the following figure to see that the selected service type P2PGnutella(TCP: 6346) is allowed to be modified.



Service Name: P2PGuntella
Service Type: TCP
Port Configuration
Type: ● Single ○ Range
Port Number: 6346 - 0

Delete: After clicking this button, the user can remove the selected service type from the pull-down menu.

Note: the default service type cannot be edited or deleted, but any user-defined service type does.

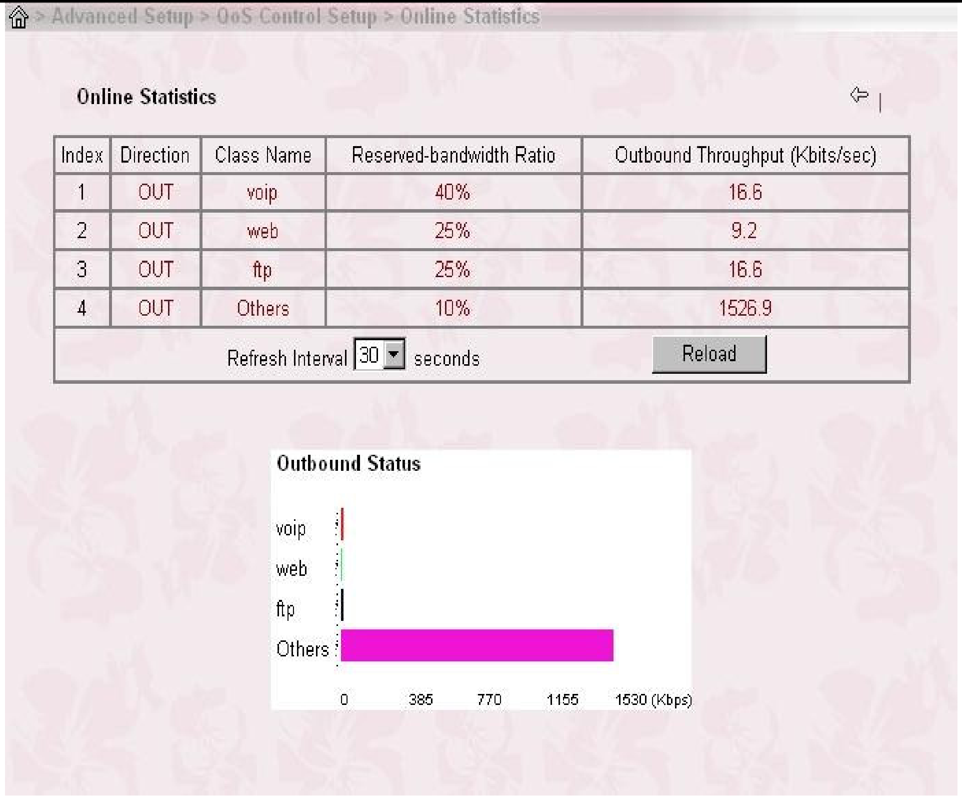
Advance Setting - Edit

Similar to button "**Insert**" in the ***Advance Setting***, this button provides users to edit a specific service. Before performing the edition operation, the user should choose one service by enabling its corresponding check circle at the left-most side. Assume the first service is selected, i.e. AUTH (TCP: 113) with service level of best effort. After clicking the "***Edit***" button, the web configuration will change to the following figure. Since all operations and their associated web configurations are identical to those after clicking "***Insert***" button in ***Advanced Configuration***, the user could refer to the explanation mentioned in the previous section.

17.5 Online Statistics

Before introducing the ***Online Statistics*** in more detail, let us go back to the ***QoS Control Setup*** page. In the ***QoS Control Setup***, user can easily find the link labeled with ***Online Statistics***. After clicking it, the web page will be changed to another scene to show the instant bandwidth usage of individual classes.

Herein, we use as an example to explain the ***Online Statistics***. Assume that the QoS control function applies on all outbound packets (from LAN to WAN side) and traffic flows are classified into “voip”, “web”, “ftp”, and “Others” groups with reserved-bandwidth ratios of 40%, 25%, 25%, and 10%, respectively. Since we only transfer a little data belonging to the first three classes through the Vigor router, the reserved-bandwidth for these classes is enough to carry them, leading to the remaining bandwidth of the first three classes will be totally given to the forth class (i.e. “Others” Class). The result is shown in the following figure.



Index	Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Kbits/sec)
1	OUT	voip	40%	16.6
2	OUT	web	25%	9.2
3	OUT	ftp	25%	16.6
4	OUT	Others	10%	1526.9

Refresh Interval 30 seconds

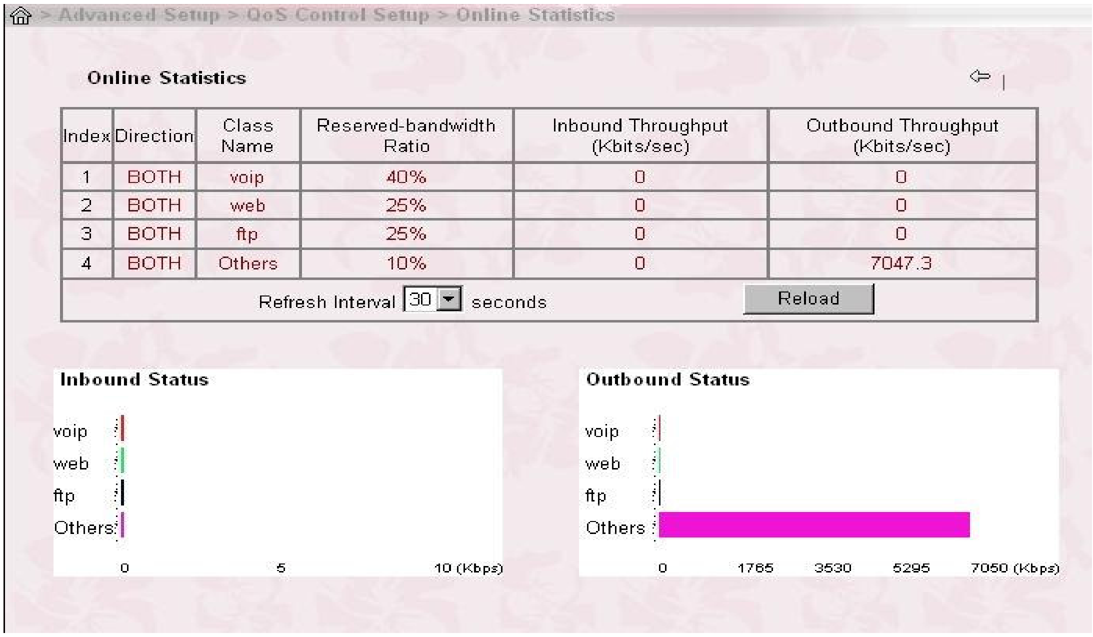
In this figure, we provide a table to reveal all necessary information consisting of "***Index***", "***Direction***", "***Class Name***", "***Reserved-bandwidth Ratio***", and "***Outbound Throughput (Kbits/sec)***". Also, we use a graph to reflect the instant outbound throughput of individual classes. The *Direction* field shows "***OUT***" to indicate the QoS control function is applied on all outbound packets. *Class name* and their associated *Reserved-bandwidth Ratio*s are displayed as those mentioned above. *Outbound throughput* (in Kbits/sec) for each class in text and graphic formats shows the instant throughput in Kbits per second. One button ("**Reload**") and one selection item ("**Refresh Interval**") involved in this web page are described below.

Reload: Click it to refresh the web page on demand.

Refresh Interval (**in second**): Specify a value to this field and then the browser will refresh automatically the result every *refresh time interval*. The Vigor router only supports 5, 10, and 30 seconds to fill the *Refresh Interval* field. .

Notice that, as mentioned before, the activation of the QoS control facility depends on enabling the check box "***Enable the QoS Control***". If this checkbox is not enabled, the QoS control function will not work and the ***Online Statistics*** will disappear in that web page.

Now, consider the previous example again with a little change. Assume the QoS control function is applied on both-direction packets (i.e. inbound and outbound packets) and no traffic for the first three classes is transferred. Class name and its reserved-bandwidth ratio for each class keeps the same. After running a time period, the ***Online Statistics*** is shown below. In this figure, Inbound throughput for each class in text and graphic format is also provided for users.



> Advanced Setup > QoS Control Setup > Online Statistics

Online Statistics

Index	Direction	Class Name	Reserved-bandwidth Ratio	Inbound Throughput (Kbits/sec)	Outbound Throughput (Kbits/sec)
1	BOTH	voip	40%	0	0
2	BOTH	web	25%	0	0
3	BOTH	ftp	25%	0	0
4	BOTH	Others	10%	0	7047.3

Refresh Interval 30 seconds

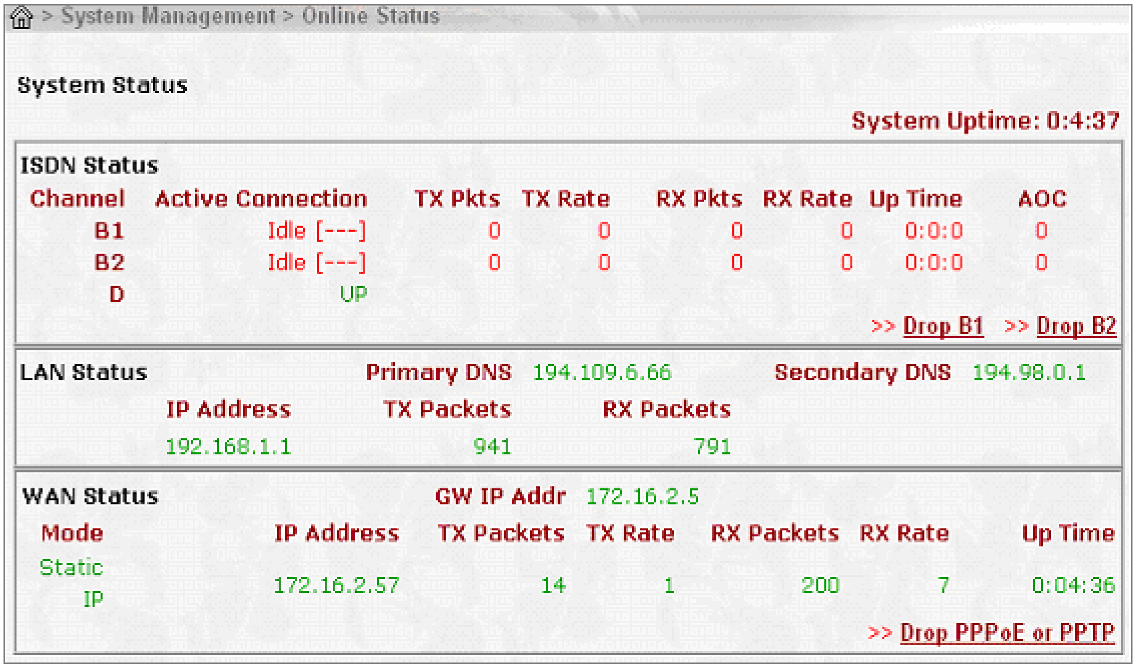
Chapter 18
Online Status

18.1 Introduction

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

18.2 Online Status Descriptions

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



System Status

System Uptime: 0:4:37

ISDN Status

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

LAN Status

Primary DNS 194.109.6.66

Secondary DNS 194.98.0.1

IP Address	TX Packets	RX Packets
192.168.1.1	941	791

WAN Status

GW IP Addr 172.16.2.5

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
Static IP	172.16.2.57	14	1	200	7	0:04:36

One may find that the Online Status page contains three basic subgroups. That is System Status, LAN Status and WAN Status. However, for the Vigor2900i and Vigor2900Gi, the Online Status page also displays the status of ISDN connection.

18.2.1 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.

18.2.2 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.

18.2.3 WAN Status

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

GW IP Addr: The gateway IP address.

IP Address: IP address of the WAN interface.

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

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

RX Packets: Total number of received IP packets during this connection session.

RX Rate: Reception rate in characters per second (cps) for incoming data.
Up Time: Connection time. The format is HH:MM:SS, where HH, MM, and SS, indicate hours, minutes, and seconds, respectively.

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

18.2.4 ISDN Status (for Vigor2900Vi / VGi only)

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

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

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

RX Pkts: Total number of received IP packets during this connection session.

RX Rate: Reception rate in characters per second (cps) for incoming data.

Up Time: Connection time. The format is HH:MM:SS, where HH, MM, and SS represent hours, minutes, and seconds, respectively.

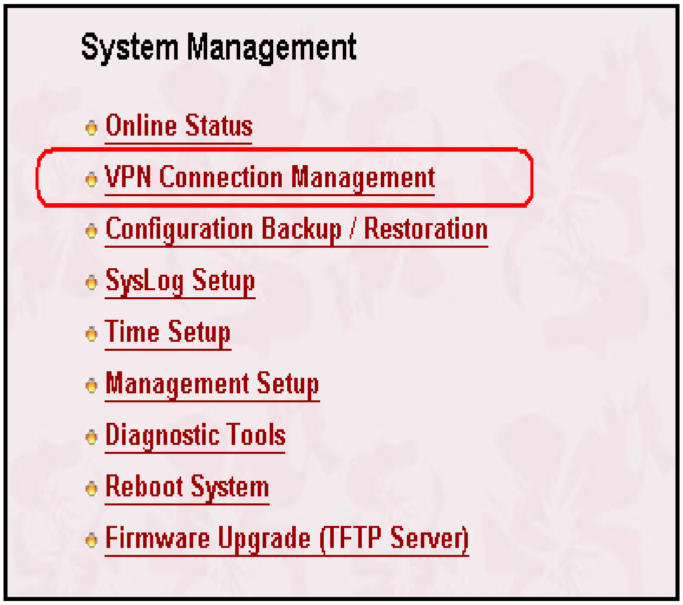
Drop B1: Click to disconnect the B1 channel.

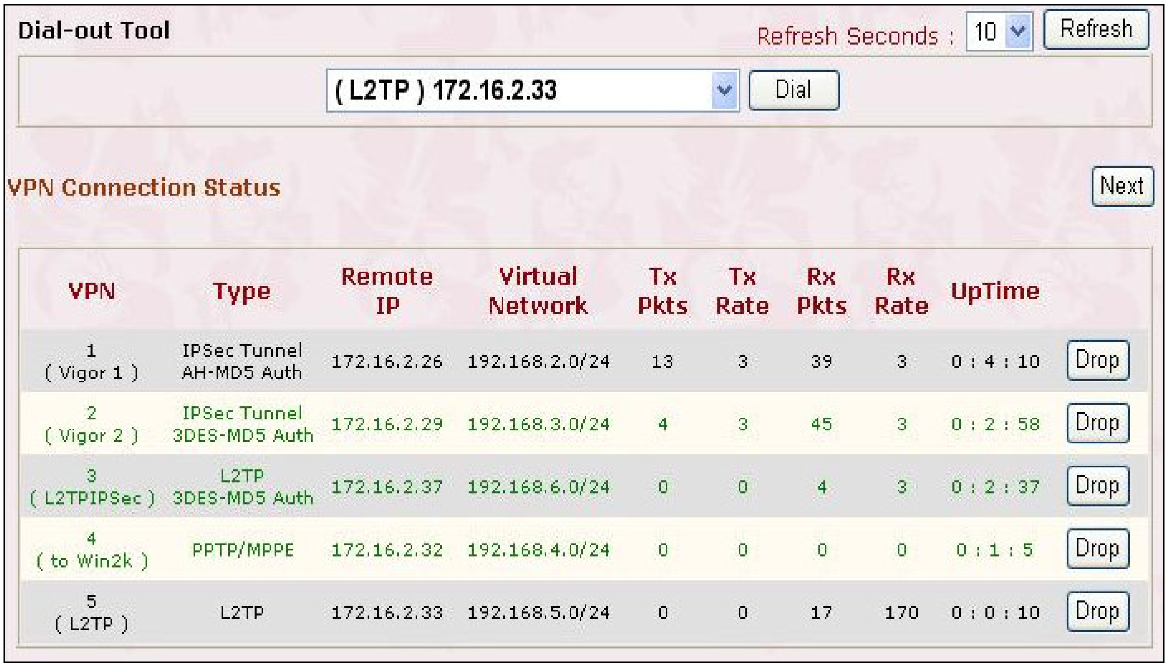
Drop B2: Click to disconnect the B2 channel.

Chapter 19
VPN Connection Management

19.1 Initiate a VPN connection

Once the VPN configuration is completed, any traffic from local LAN to remote LAN will trigger the VPN connection. Or you can use VPN Connection Management in System Management to direct "Dial" or connect a VPN from dial-out router. Once the link is up the VPN connection status/information will also show in VPN Connection Management page. A "Drop" button will let you to disconnect the link.





VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	
1 (Vigor 1)	IPSec Tunnel AH-MD5 Auth	172.16.2.26	192.168.2.0/24	13	3	39	3	0 : 4 : 10	Drop
2 (Vigor 2)	IPSec Tunnel 3DES-MD5 Auth	172.16.2.29	192.168.3.0/24	4	3	45	3	0 : 2 : 58	Drop
3 (L2TPIPSec)	L2TP 3DES-MD5 Auth	172.16.2.37	192.168.6.0/24	0	0	4	3	0 : 2 : 37	Drop
4 (to Win2k)	PPTP/MPPE	172.16.2.32	192.168.4.0/24	0	0	0	0	0 : 1 : 5	Drop
5 (L2TP)	L2TP	172.16.2.33	192.168.5.0/24	0	0	17	170	0 : 0 : 10	Drop

Chapter 20
Configuration Backup and Restoration

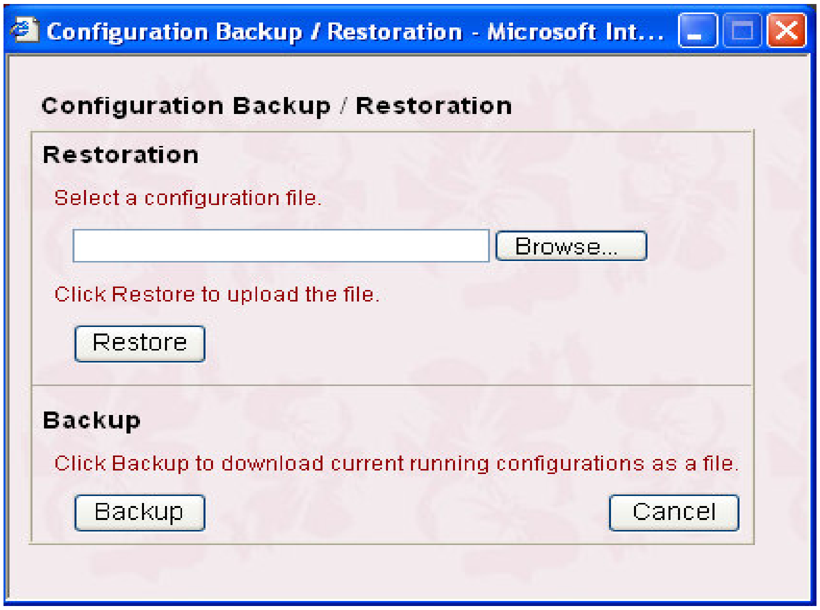
20.1 Introduction

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

20.2 Usage

20.2.1 Backup the Running Configuration

1. Login **Web Configurator**, and then click **Configuration Backup/Restoration**. The following windows will be popped-up, as shown below.



Configuration Backup / Restoration - Microsoft Int...

Configuration Backup / Restoration

Restoration

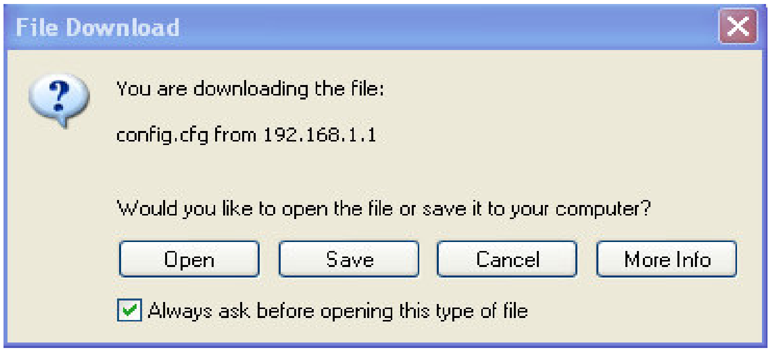
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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



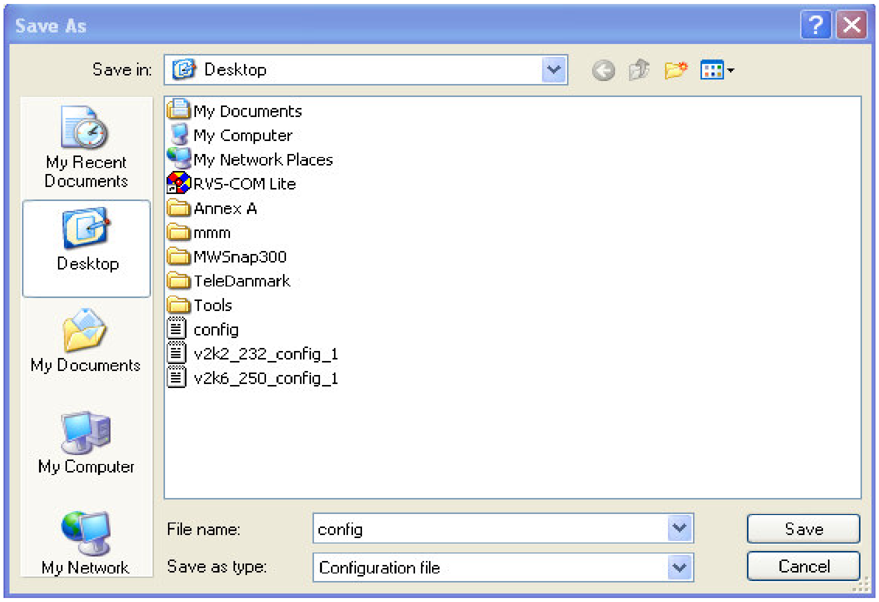
You are downloading the file:

config.cfg from 192.168.1.1

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

☑ Always ask before opening this type of file

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



Save in: Desktop

File name: config

Save as type: Configuration file

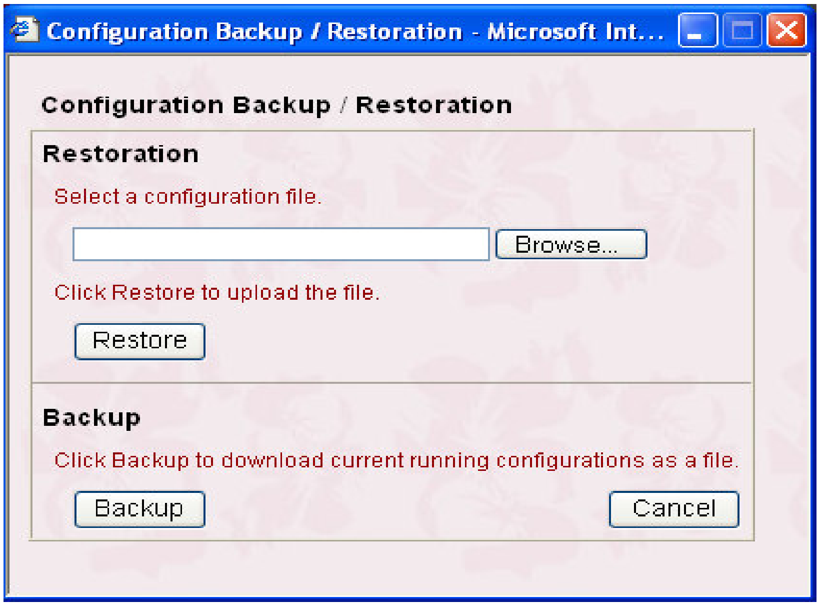
4. Push **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

20.2.2 Restore the Configuration with a Configuration File

1. Login **Web Configurator** and then click **Configuration Backup/ Restoration**. The following windows will be popped-up, as shown below.

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

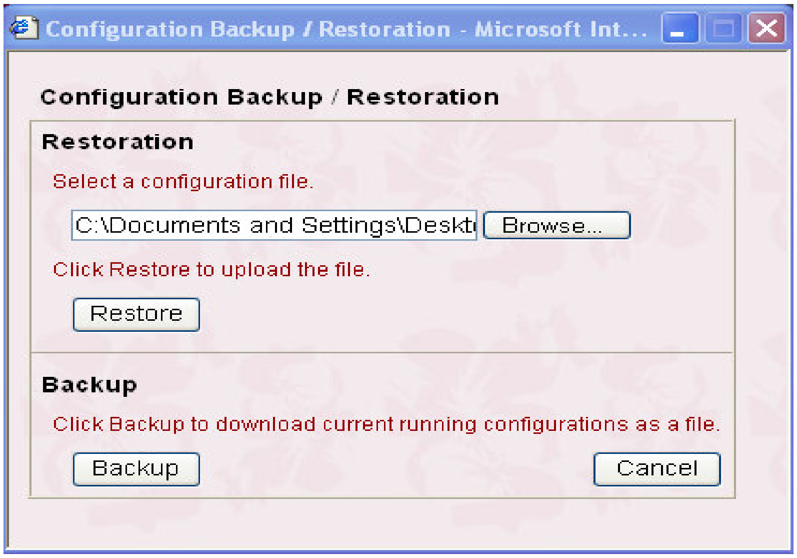

Configuration Backup / Restoration - Microsoft Int...
Configuration Backup / Restoration
Restoration
Browse...
Restore
Backup
Backup
Cancel

Select a configuration file.

Click Restore to upload the file.

Click Backup to download current running configurations as a file.

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



Configuration Backup / Restoration

Restoration

Select a configuration file.

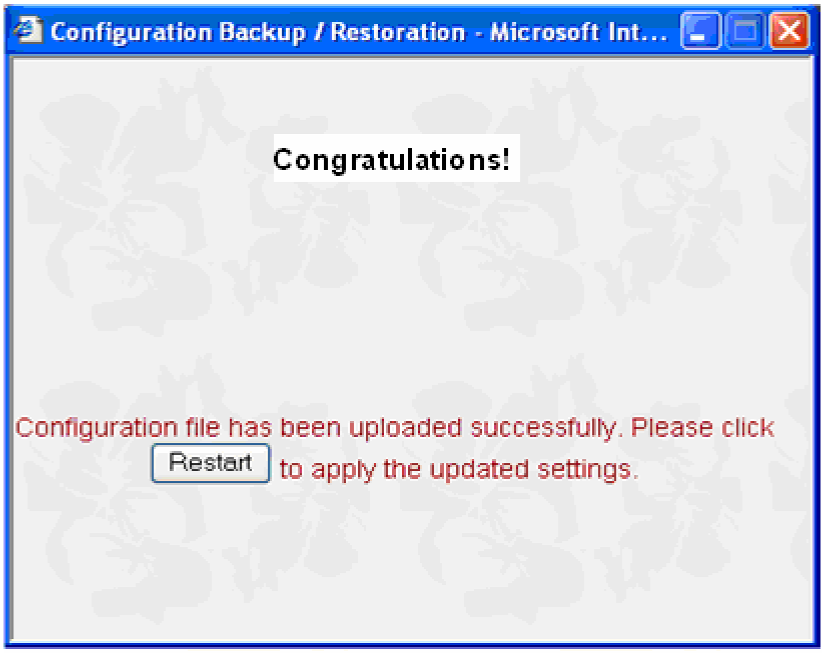
C:\Documents and Settings\Deskt

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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



Congratulations!

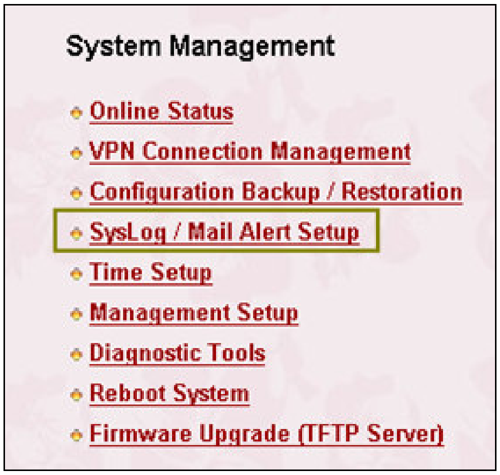
Configuration file has been uploaded successfully. Please click Restart to apply the updated settings.

Chapter 21
SysLog / Mail Alert Setup

21.1 Introduction

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

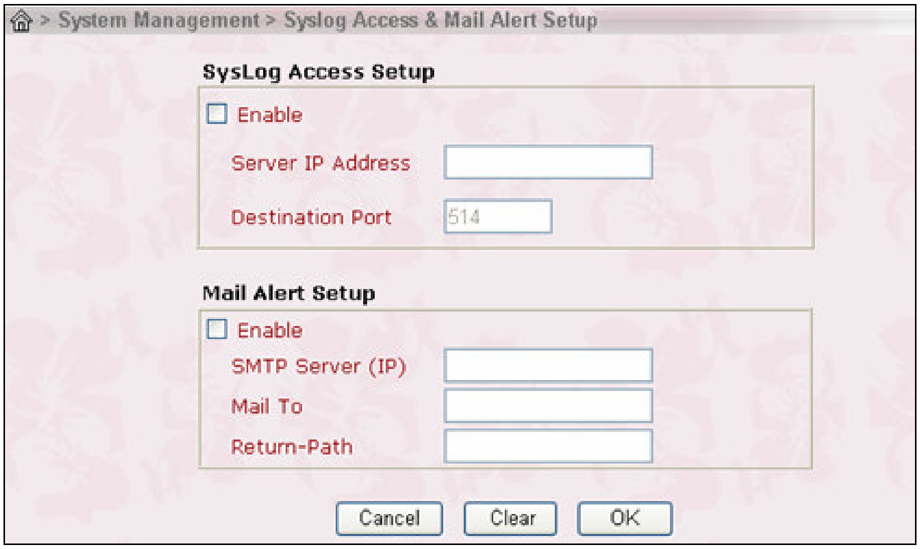
System Management > SysLog/Mail Alert Setup


System Management
Online Status
VPN Connection Management
Configuration Backup / Restoration
SysLog / Mail Alert Setup
Time Setup
Management Setup
Diagnostic Tools
Reboot System
Firmware Upgrade (TFTP Server)

21.2 Configuration

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

SysLog access setup and another one for mail alert setup.



SysLog Access Setup

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

Mail Alert Setup

1. Check the **Enable** box to activate the mail alert service.
2. **SMTP Server (IP)**: Specify an IP address of the SMTP server which can send mails from your Vigor router to the recipients' mailboxes directly.
3. **Mail To**: Specify an e-mail address of the recipient's mailbox to which all SysLog messages will be sent. The recipient could be an administrator who intends to view or analyze the SysLog messages.
4. **Return-Path**: Specify an e-mail address of another mailbox to accept all

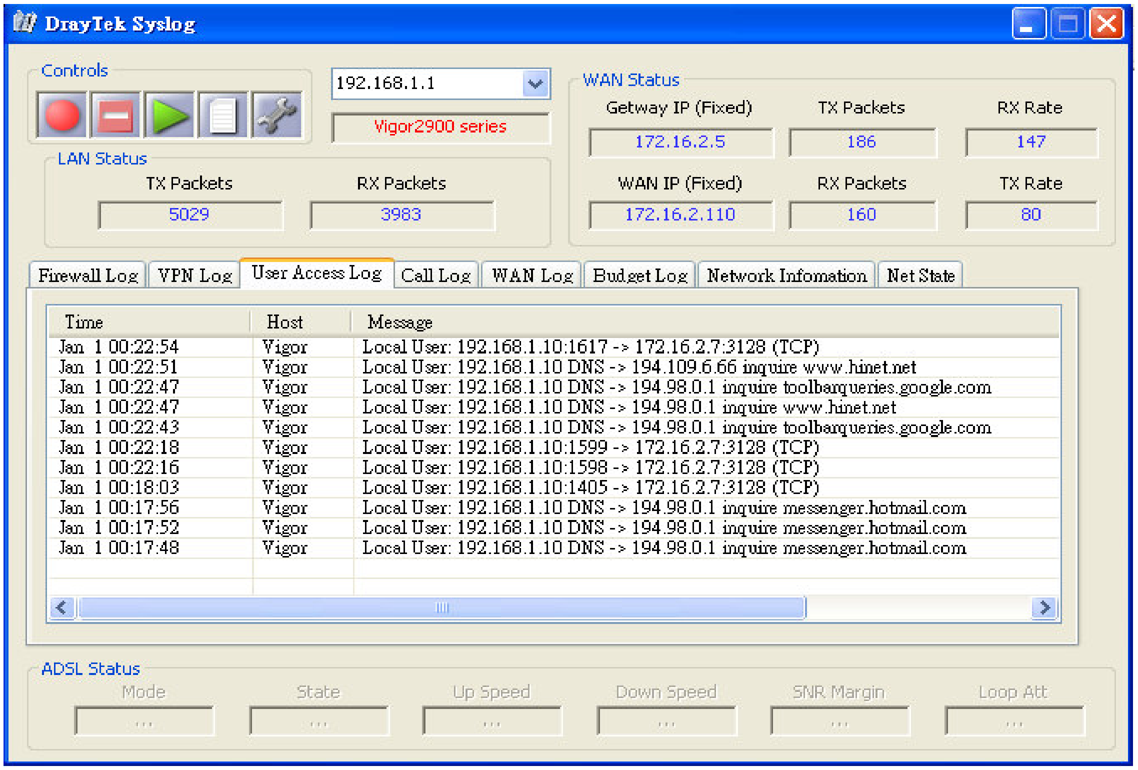
returned messages if some fatal problems occur at the recipient mailbox.

Notice that the current mail alert function is only used to send SysLog messages related to Denial-of-Service (DoS) defense behaviors while you have activated the DoS defense facility.

21.3 Example

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

An example of User Access log message:



192.168.1.1

Vigor2900 series

LAN Status

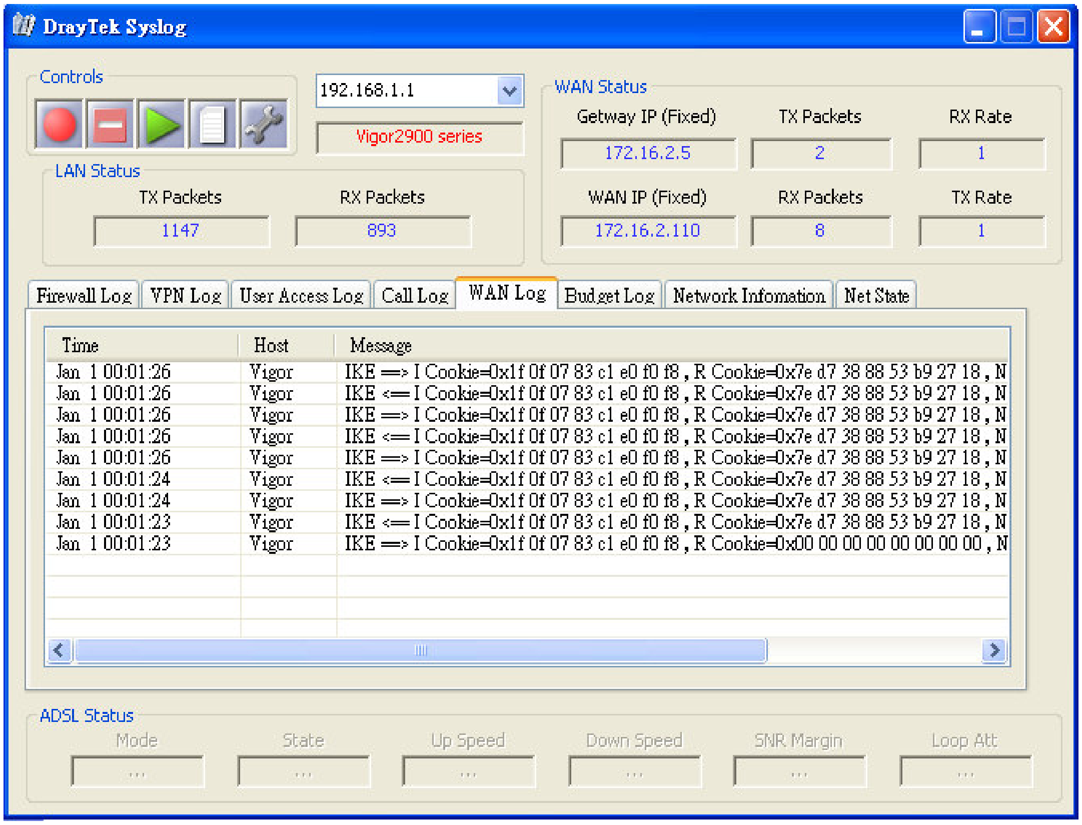
TX Packets	RX Packets
5029	3983

WAN Status

Getway IP (Fixed)	TX Packets	RX Rate
172.16.2.5	186	147
WAN IP (Fixed)	**RX Packets**	**TX Rate**
172.16.2.110	160	80

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

An example of WAN log message to record the status of VPN/IPSec tunnel:



192.168.1.1

Vigor2900 series

WAN Status

Getway IP (Fixed)	TX Packets	RX Rate
172.16.2.5	2	1
WAN IP (Fixed)	**RX Packets**	**TX Rate**
172.16.2.110	8	1

LAN Status

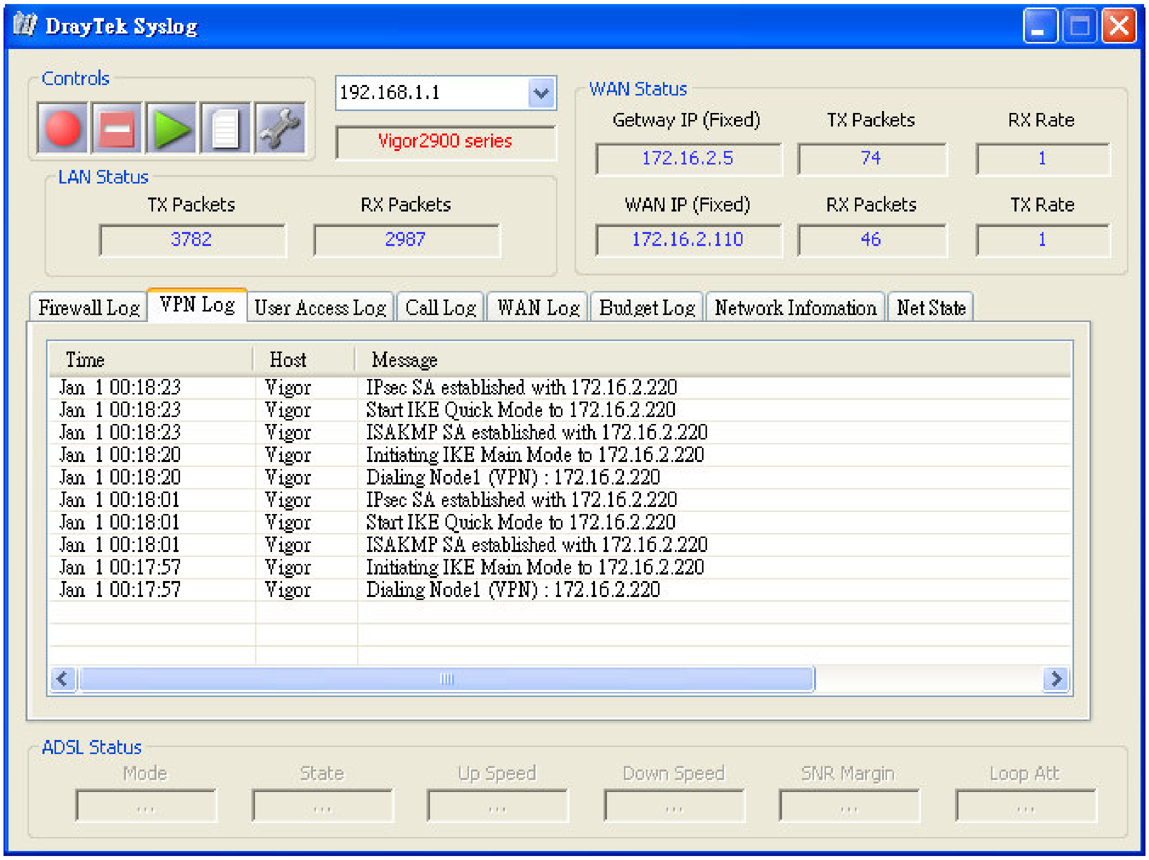
TX Packets	RX Packets
1147	893

```
Time            Host    Message
Jan  1 00:01:26 Vigor   IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26 Vigor   IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26 Vigor   IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26 Vigor   IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26 Vigor   IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:24 Vigor   IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:24 Vigor   IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:23 Vigor   IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:23 Vigor   IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x00 00 00 00 00 00 00 00 , N
```

ADSL Status

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

An example of VPN (IPSec) log message to record the status of the VPN/IPSec tunnel:



192.168.1.1

Vigor2900 series

LAN Status

TX Packets	RX Packets
3782	2987

WAN Status

Getway IP (Fixed)	TX Packets	RX Rate
172.16.2.5	74	1

WAN IP (Fixed)	RX Packets	TX Rate
172.16.2.110	46	1

```
Time              Host    Message
Jan  1 00:18:23   Vigor   IPsec SA established with 172.16.2.220
Jan  1 00:18:23   Vigor   Start IKE Quick Mode to 172.16.2.220
Jan  1 00:18:23   Vigor   ISAKMP SA established with 172.16.2.220
Jan  1 00:18:20   Vigor   Initiating IKE Main Mode to 172.16.2.220
Jan  1 00:18:20   Vigor   Dialing Node1 (VPN) : 172.16.2.220
Jan  1 00:18:01   Vigor   IPsec SA established with 172.16.2.220
Jan  1 00:18:01   Vigor   Start IKE Quick Mode to 172.16.2.220
Jan  1 00:18:01   Vigor   ISAKMP SA established with 172.16.2.220
Jan  1 00:17:57   Vigor   Initiating IKE Main Mode to 172.16.2.220
Jan  1 00:17:57   Vigor   Dialing Node1 (VPN) : 172.16.2.220
```

ADSL Status

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

Chapter 22
Time Setup

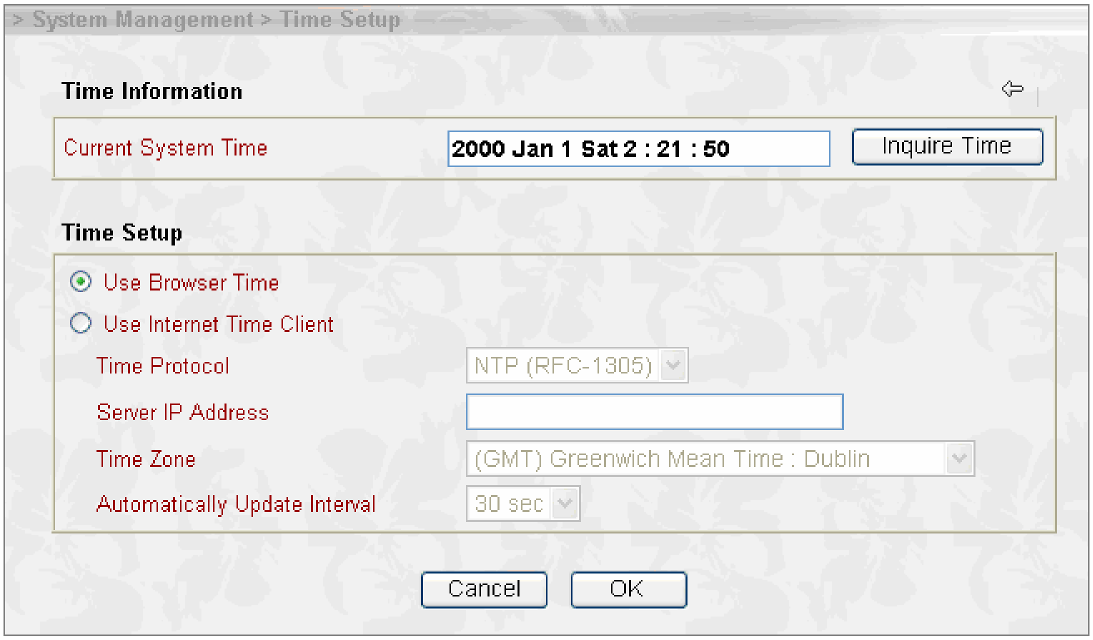
22.1 Introduction

The router has two different ways to set up time base: one is using computer time base via HTTP protocol and another is using NTP (Network Time Protocol) client to get time base from the time server. If you want to use any time-based function (for example, Call Schedule and URL Content filtering), the system time function should be worked properly in advance.

22.2 Configuration

22.2.1 Set Time Base Using Web Browser

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



> System Management > Time Setup

Time Information

Current System Time: 2000 Jan 1 Sat 2 : 21 : 50

Time Setup

● Use Browser Time

○ Use Internet Time Client

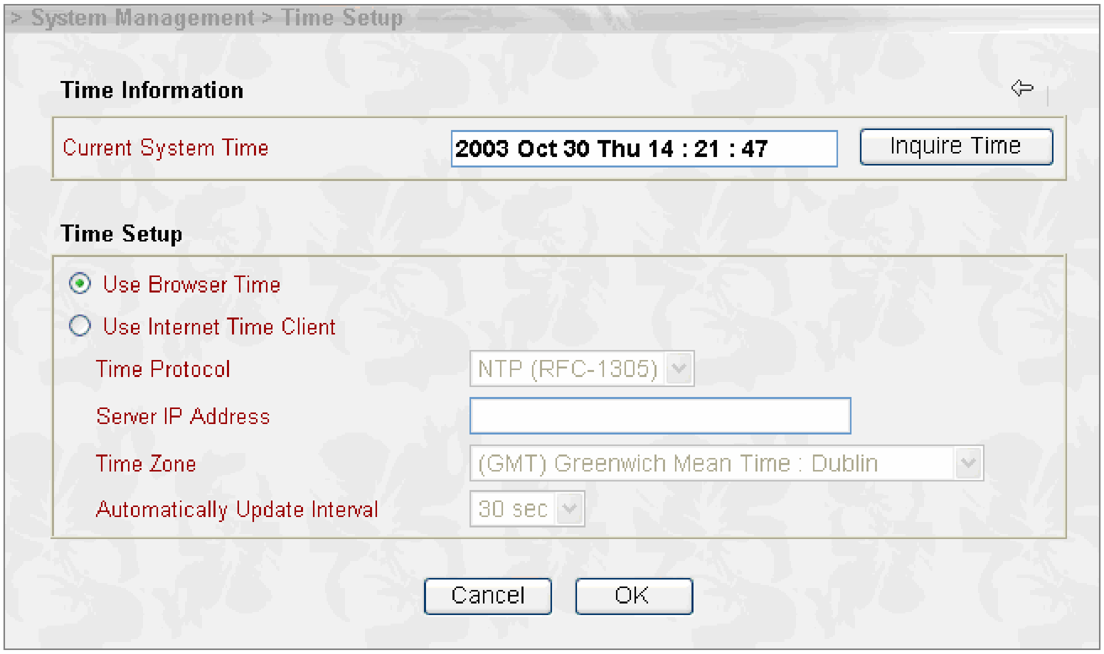
Time Protocol: NTP (RFC-1305)

Server IP Address:

Time Zone: (GMT) Greenwich Mean Time : Dublin

Automatically Update Interval: 30 sec

2. Select **Use Browser Time** and click **OK** button. Click **Time Setup** again and push **Inquire Time** to set time base to the router.



> System Management > Time Setup

Time Information

Current System Time: 2003 Oct 30 Thu 14 : 21 : 47

Time Setup

● Use Browser Time

○ Use Internet Time Client

Time Protocol: NTP (RFC-1305)

Server IP Address:

Time Zone: (GMT) Greenwich Mean Time : Dublin

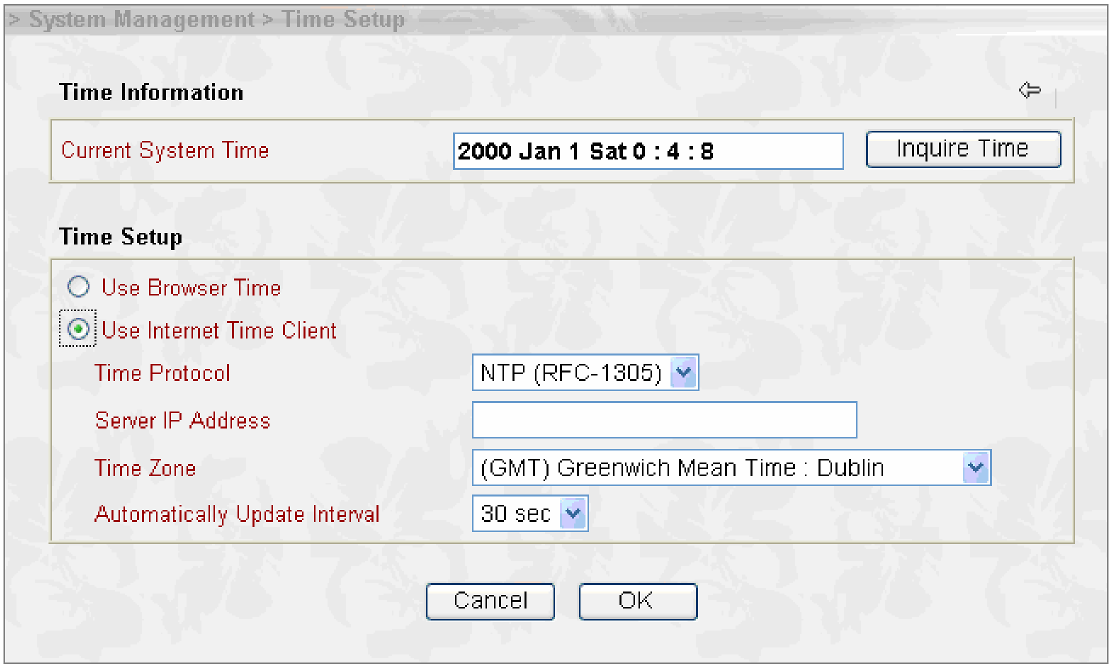
Automatically Update Interval: 30 sec

3. The **Current System Time** block will display exact time information as your computer.

22.2.2 Set Time Base Using Time Client

1. Before setting up the time base through the time client, you have to make sure if the time server is working properly. If the time server is located at the Internet, you should also make sure the router has Internet access capability. Login **Web Configurator** and then click **Time Setup**.

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



Time Information

Current System Time: 2000 Jan 1 Sat 0 : 4 : 8

Time Setup

○ Use Browser Time

● Use Internet Time Client

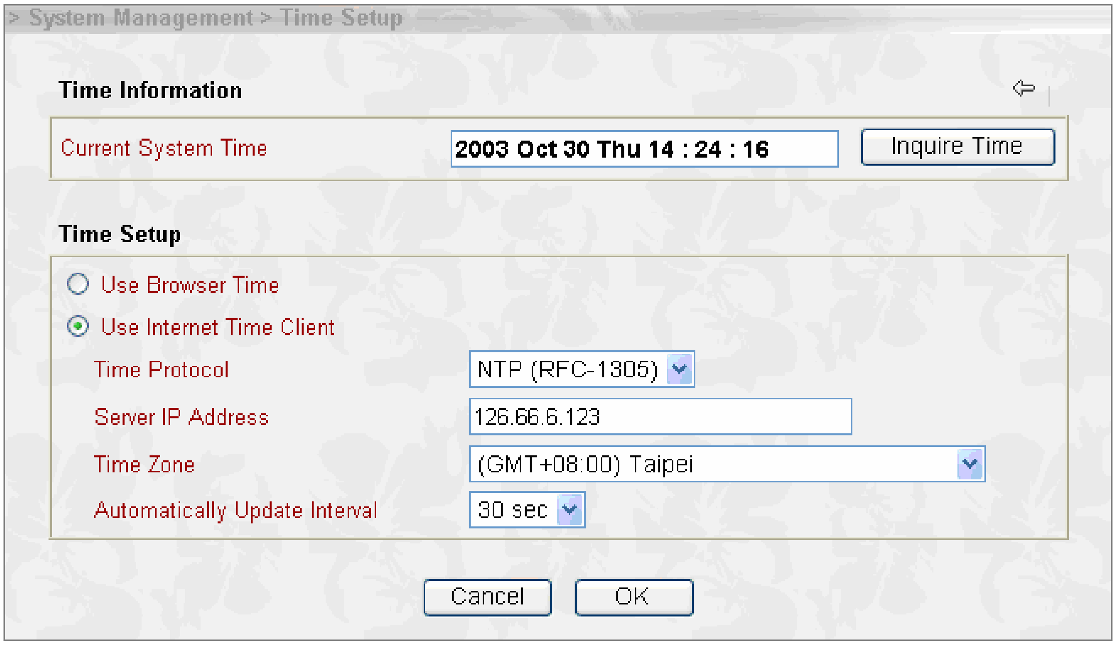
Time Protocol: NTP (RFC-1305)

Server IP Address:

Time Zone: (GMT) Greenwich Mean Time : Dublin

Automatically Update Interval: 30 sec

3. Click **OK** button, wait for few seconds, and then the time client will get time base from the specified time server. Click **Time Setup** again to check **Current System Time** information as shown below.



Time Information

Current System Time: 2003 Oct 30 Thu 14 : 24 : 16

Time Setup

○ Use Browser Time

● Use Internet Time Client

Time Protocol: NTP (RFC-1305)

Server IP Address: 126.66.6.123

Time Zone: (GMT+08:00) Taipei

Automatically Update Interval: 30 sec

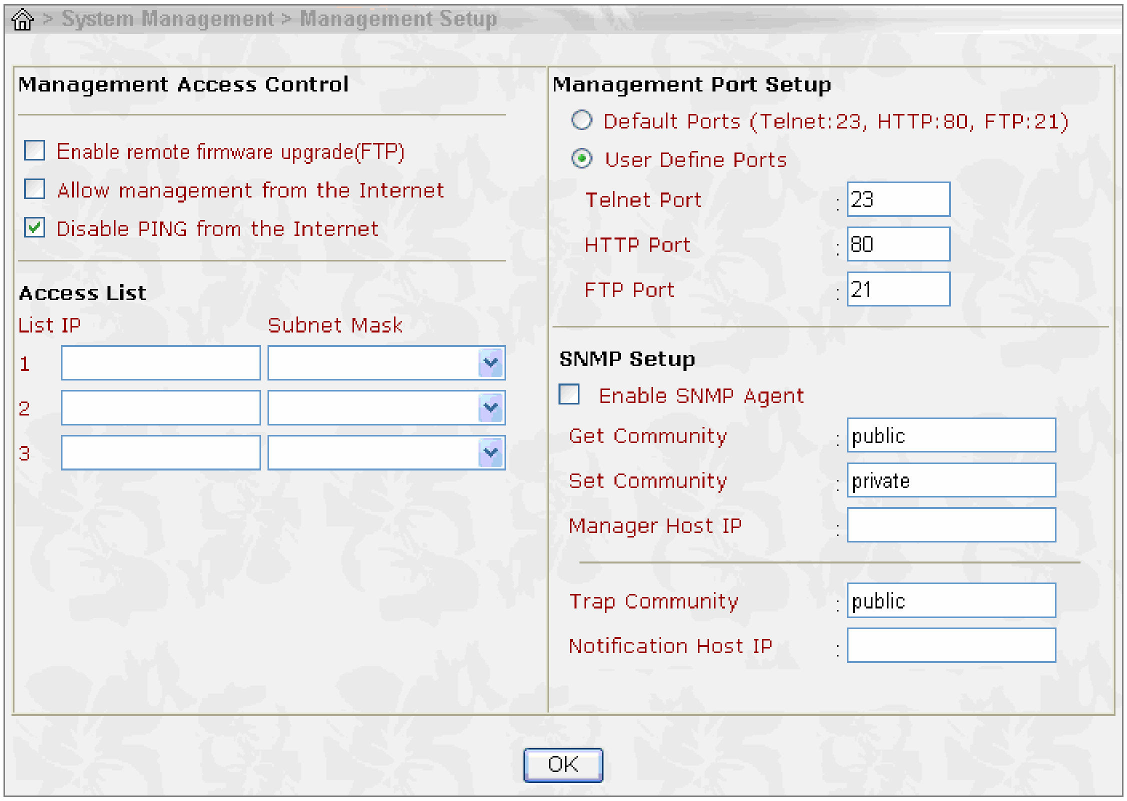
Chapter 23
Management Setup

23.1 Introduction

By default, the router may be configured and managed through any Telnet client or Web browser running on any operating system. There is no requirement for additional software or utilities. However, for some specific environments, you may want to 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.

23.2 Configuration

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



Management Access Control

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

Access List

List IP		Subnet Mask
1		
2		
3		

Management Port Setup

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

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

SNMP Setup

☐ Enable SNMP Agent

Get Community : public
Set Community : private
Manager Host IP :

Trap Community : public
Notification Host IP :

23.2.1 Management Access Control

Enable remote firmware update (FTP): Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).

Allow management from the Internet: Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.

Disable PING from the Internet: Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.

23.2.2 Access List

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

IP: Indicate an IP address allowed to login to the router.

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

23.2.3 Management Port Setup

Default Ports: Check to use standard port numbers for the Telnet and HTTP servers.

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

23.2.4 SNMP Setup

Enable SNMP Agent: Chick the checkbox to enable built-in SNMP agent.

Get Community: Specify a string to identify the management communities for the SNMP GET command.

Set Community: Specify a string to identify the management communities for the SNMP SET command.

Manager Host IP: Specify the IP address of the SNMP manager station.

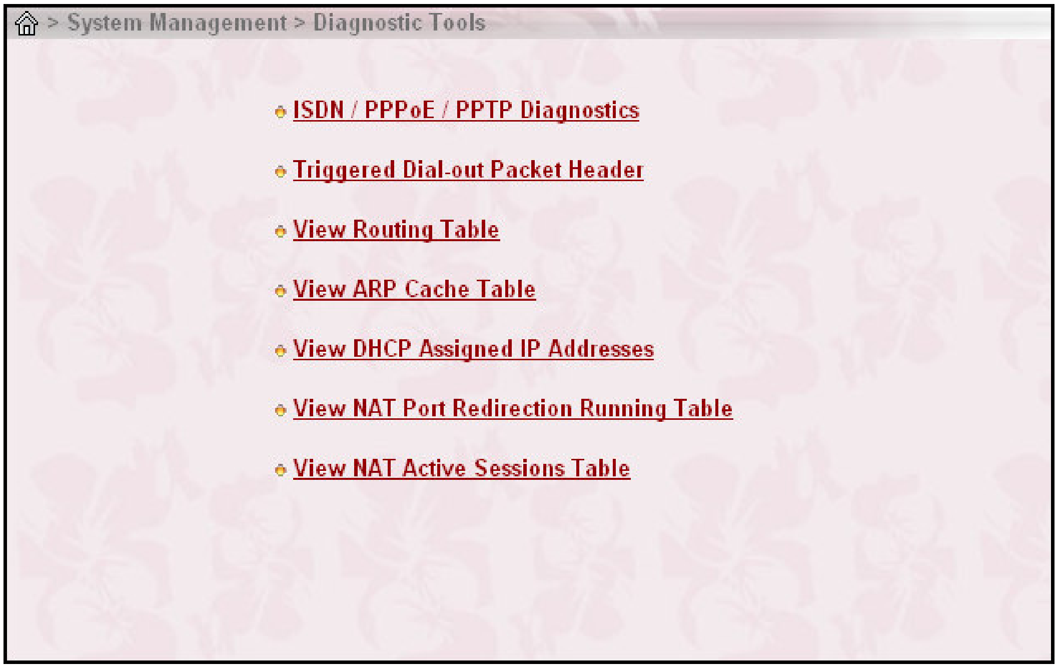
Trap Community: Specify a string to identify the management communities for the SNMP TRAP notifications.

Notification Host IP: Specify the IP address of the station that wants to receive the TRAP notifications.

Chapter 24
Diagnostic Tools

24.1 Introduction

Diagnostic Tools provide a useful way to view or diagnose the status of you Vigor router. Please click the link “**System Management > Diagnostic Tools Diagnostic Tools**” in the Setup Main Menu to enter the following page. More details for each tool will be explained below.

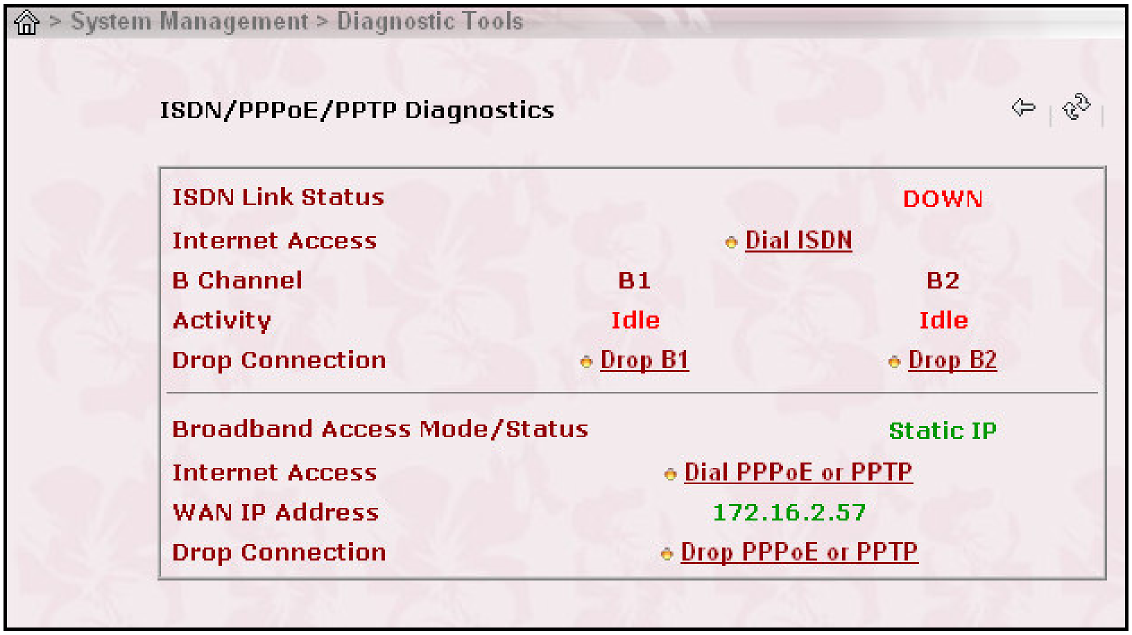

> System Management > Diagnostic Tools
ISDN / PPPoE / PPTP Diagnostics
Triggered Dial-out Packet Header
View Routing Table
View ARP Cache Table
View DHCP Assigned IP Addresses
View NAT Port Redirection Running Table
View NAT Active Sessions Table

24.2 Descriptions

24.2.1 ISDN/PPPoE / PPTP Diagnostics

Click here to open the following page. The page shown here is for reference only and individual networks will show different results.

The page has been grouped into two subgroups, the upper is for ISDN link status, and the lower is for broadband access status.


> System Management > Diagnostic Tools
ISDN/PPPoE/PPTP Diagnostics

ISDN Link Status		DOWN
Internet Access	Dial ISDN	
B Channel	B1	B2
Activity	Idle	Idle
Drop Connection	Drop B1	Drop B2
Broadband Access Mode/Status		Static IP
Internet Access	Dial PPPoE or PPTP	
WAN IP Address	172.16.2.57	
Drop Connection	Drop PPPoE or PPTP	

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

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

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

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

Drop B1: Click it to disconnect the B1 channel.

Drop B2: Click it to disconnect the B2 channel.

Broadband Access Mode/Status: Display the broadband access mode and status. If the broadband connection is active, it will show **PPPoE**, **PPTP**, **Static IP,** or **DHCP Client** depending on which access mode is enabled. If the connection is idle, it will show "**---**".

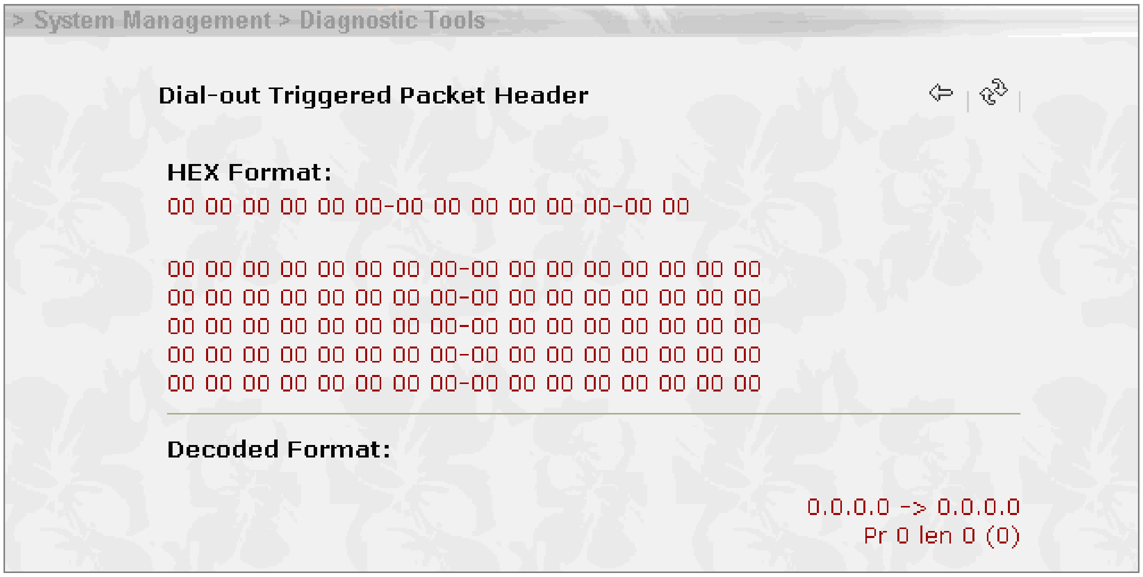
WAN IP Address: The WAN IP address for the active connection.

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

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

24.2.2 Triggered Dial-out Packet Header

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



Dial-out Triggered Packet Header

HEX Format:

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

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

Decoded Format:

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

(Refresh): Click to reload the page.

24.2.3 View Routing Table

Click **View Routing Table** to view the routing table of your Vigor router.

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

C --- Directly connected.

S --- Static route.

R --- RIP.

* --- Default route.

~ --- Routes for private routing domain.

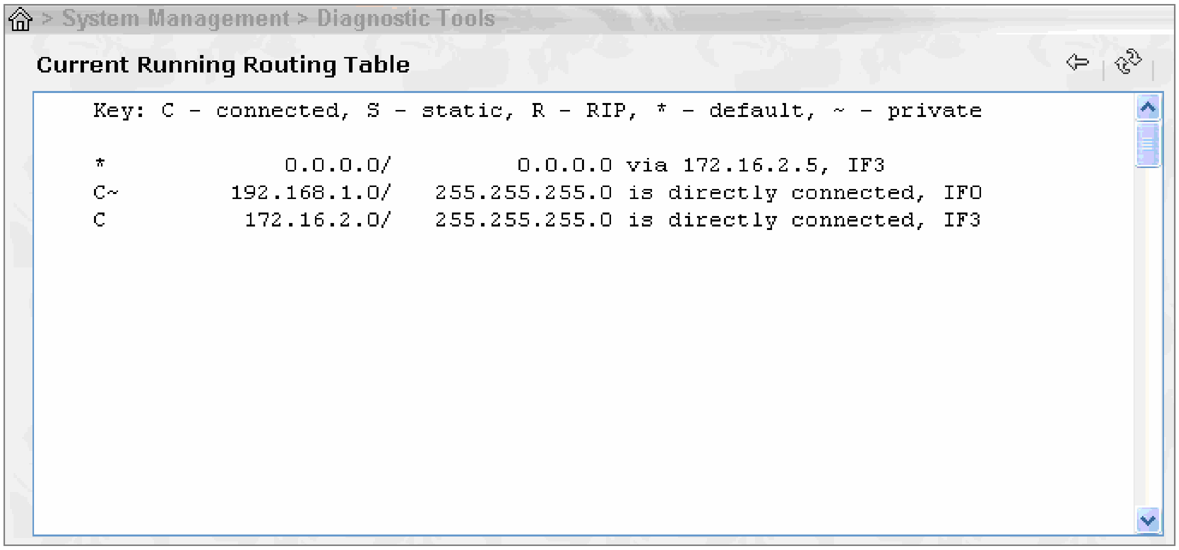
In the right of each routing rule, you will see an interface identifier which are defined as follows.

IF0 --- Local LAN interface.

IF1 --- ISDN B1 channel.

IF2 --- ISDN B2 channel.

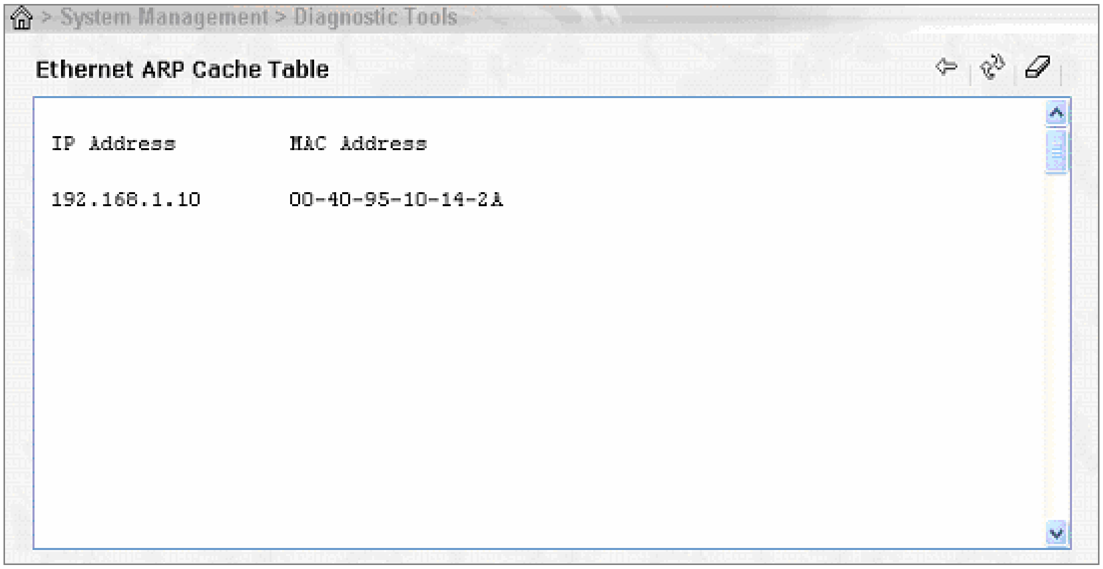
IF3 --- WAN interface.


> System Management > Diagnostic Tools
Current Running Routing Table

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

*            0.0.0.0/          0.0.0.0 via 172.16.2.5, IF3
C~         192.168.1.0/   255.255.255.0 is directly connected, IF0
C           172.16.2.0/   255.255.255.0 is directly connected, IF3
```

24.2.4 View ARP Cache Table

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



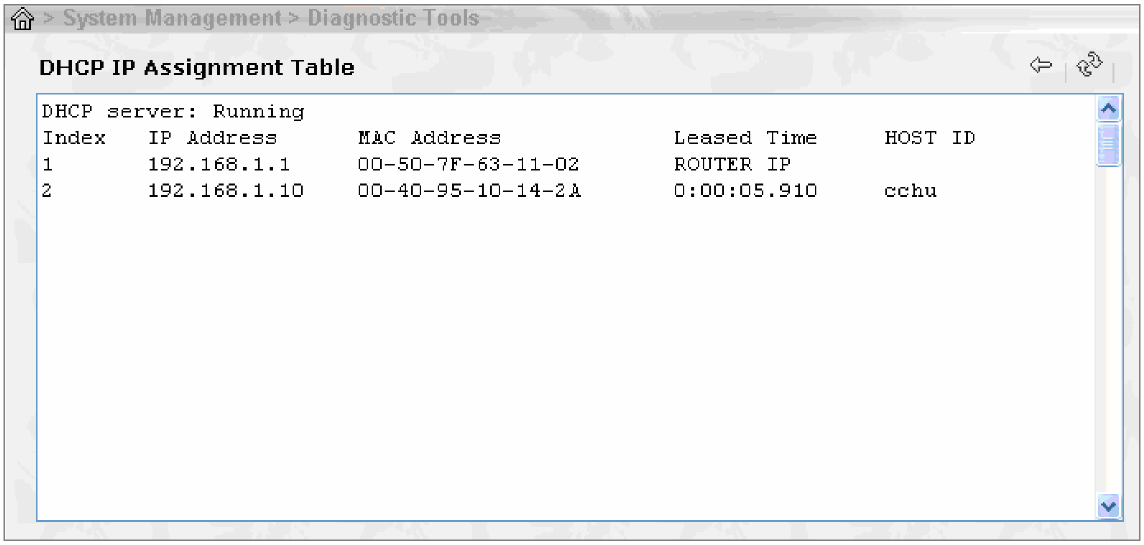
Ethernet ARP Cache Table

```
IP Address          MAC Address

192.168.1.10        00-40-95-10-14-2A
```

⟳ **(Refresh):** Click it to reload the page.

24.2.5 View DHCP Assigned IP Addresses

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.

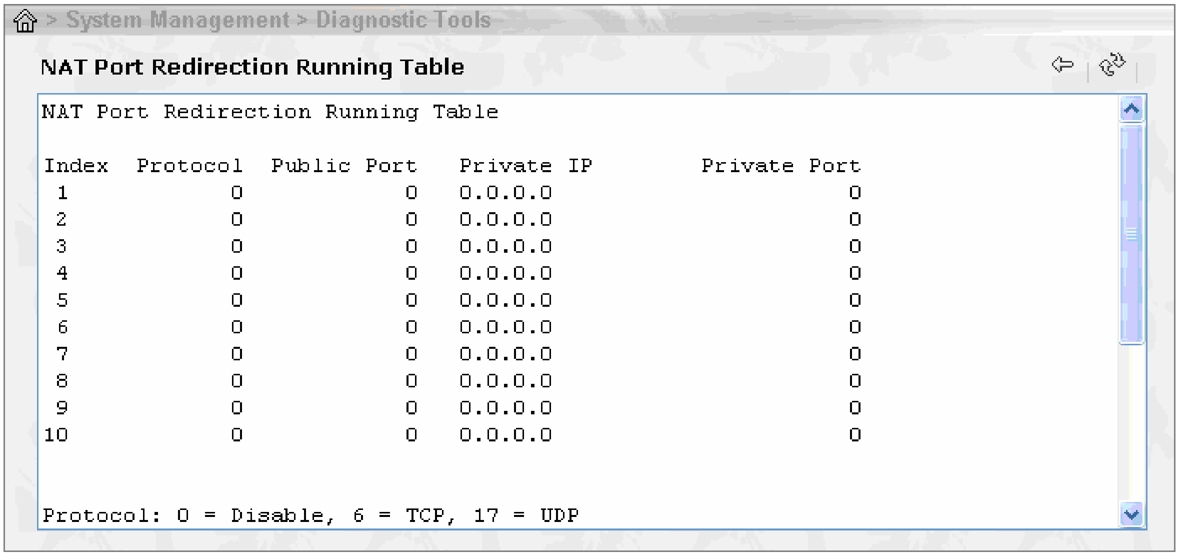


DHCP IP Assignment Table

```
DHCP server: Running
Index   IP Address      MAC Address             Leased Time     HOST ID
1       192.168.1.1     00-50-7F-63-11-02       ROUTER IP
2       192.168.1.10    00-40-95-10-14-2A       0:00:05.910     cchu
```

24.2.6 View NAT Port Redirection Running Table

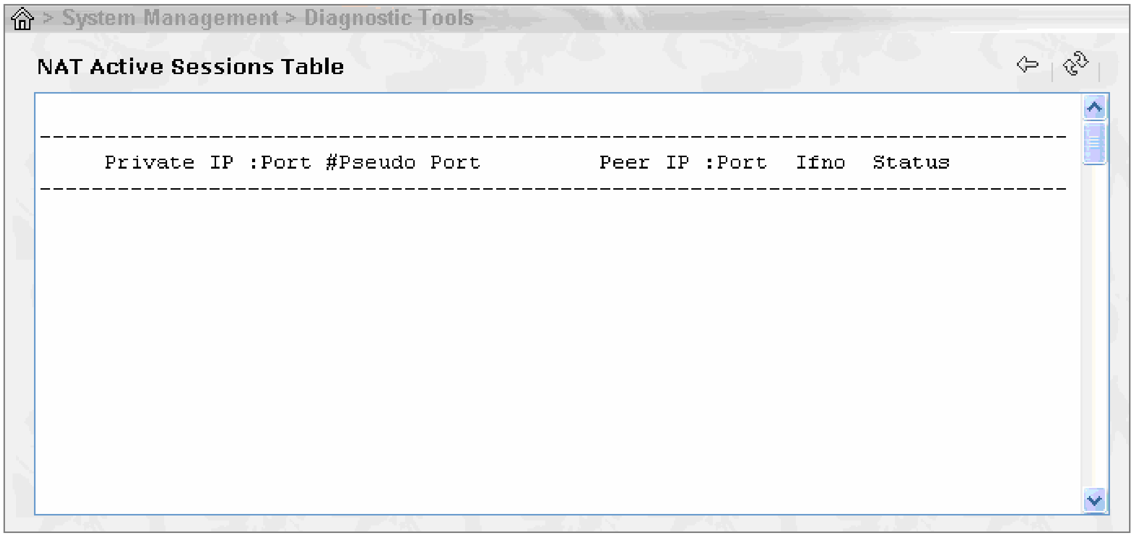
If you have configured **Port Redirection** (under **NAT Setup**), click it to verify that your settings are correct for redirecting specific port numbers to specified internal users.


> System Management > Diagnostic Tools
NAT Port Redirection Running Table

```
NAT Port Redirection Running Table

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


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

24.2.7 View NAT Active Sessions Table

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


> System Management > Diagnostic Tools
NAT Active Sessions Table

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

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

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

#Pseudo Port: The public port number.

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

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

0 --- LAN interface.

1 --- B1 interface.

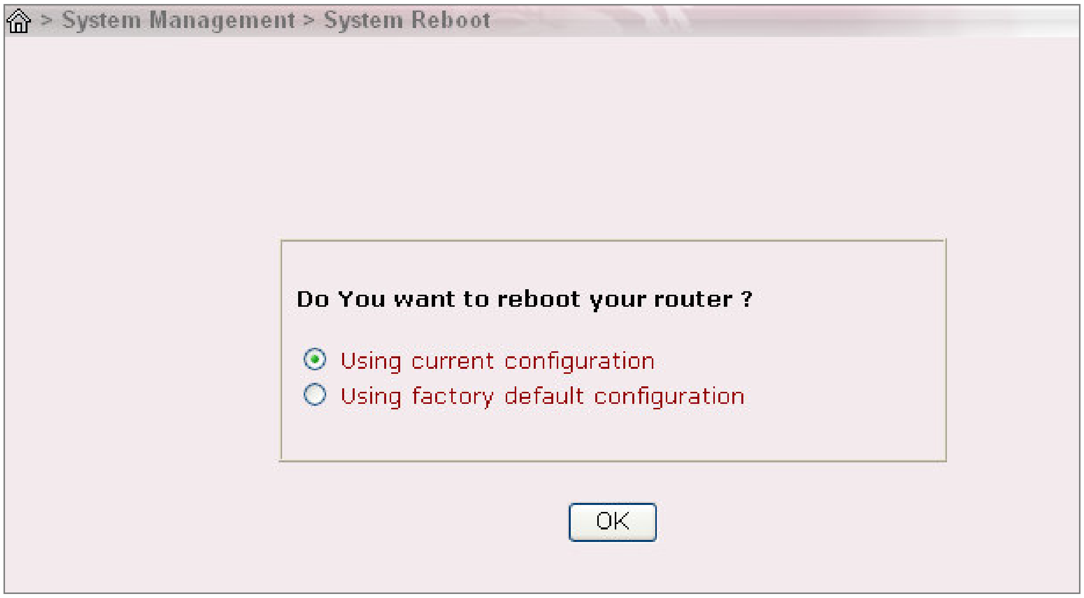
2 --- B2 interface.

3 --- WAN interface.

Chapter 25
Reboot System and Firmware Upgrade TFTP Server

25.1 Reboot System

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


> System Management > System Reboot
Do You want to reboot your router ?
OK

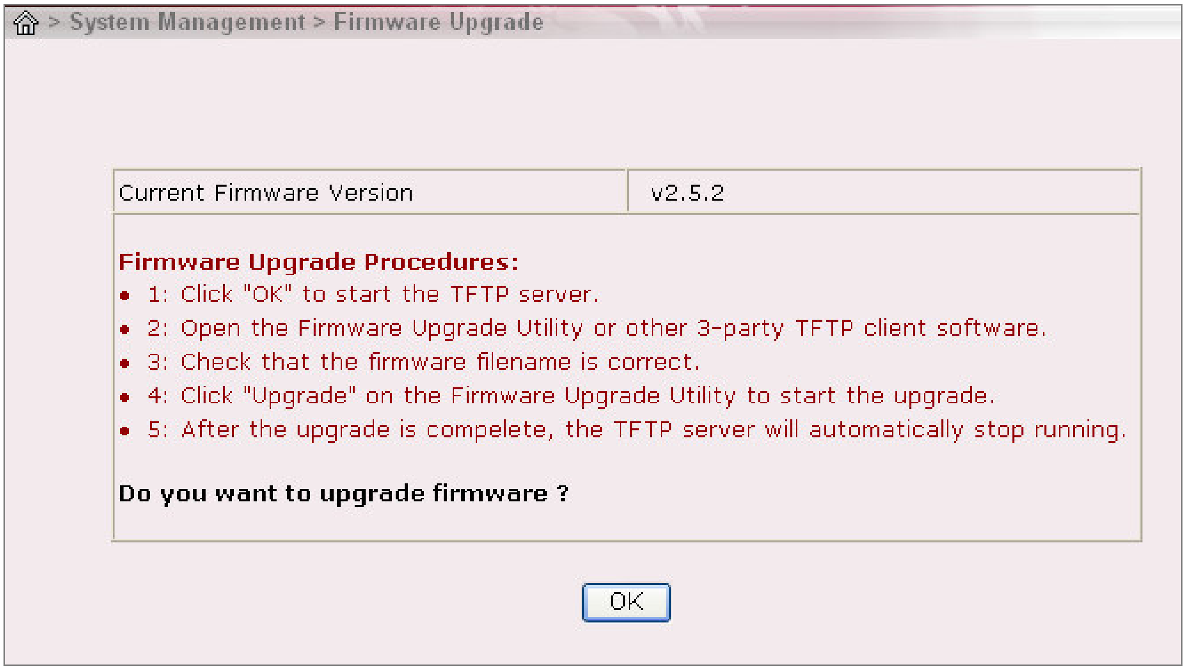
● Using current configuration
○ Using factory default configuration

There are two reboot options: **Using current configuration** and **Using factory default configuration**. If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 3 to 5 seconds to reboot the system.

25.2 Firmware Upgrade (TFTP Server)

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

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



Current Firmware Version	v2.5.2

Firmware Upgrade Procedures:

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

Do you want to upgrade firmware ?

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

Trouble Shooting Guide of Vigor2900 series
Broadband Security Router

1. Introduction

- **Firewall contains SPI technique against intrusions, attacks and DOS**
- **VPN encryption enhances transmission privacy and security**
- **QoS optimizes bandwidth for mission-critical traffic**
- **URL content filtering blocks malicious codes and inappropriate webs**
- **High-speed 802.11g implements carefree wireless access**

1.1 Brief Overview

	Vigor2900	Vigor2900G	Vigor2900Gi	Vigor2900i
Security Broadband Router	*	*	*	*
Wireless AP	-	*	*	-
ISDN Backup	-	-	*	*

The Vigor2900 series router, an Internet access solution for your LAN, which provides you the shared web surfing and countless value-added features, such as Firewall / Security, VPN, USB interface printer server support, and 802.11g Wireless LAN (up to 54Mbps for Vigor2900G/Gi only). These are all in a reliable one-box solution.

1.2 Highlights

Firewall

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

Virtual Private Network (VPN)

- Up to 32 simultaneous VPN tunnels
- Dial-in or dial-out, LAN-to-LAN or Teleworker-to-LAN
- Protocol support for PPTP, IPSec, L2TP, L2TP over IPSec
- AES, MPPE, and hardware- based DES/3DES Encryption
- Authentication support for MD5 and SHA-1
- IKE key management
- Interoperable with other leading 3rd party vendor VPN devices or software

Bandwidth Management facilities

- Class-based bandwidth guarantee by user-defined traffic categories
- Provision of inbound/outbound bandwidth control
- Support of eight priority-levels
- Support of DiffServ-Codepoint marking

WAN

- One 10/100M Base-TX port with a RJ-45 connector
- DHCP client for cable service
- Static IP address assignment for fixed IP networks
- PPPoE/PPTP client for ADSL service

LAN

- 4 port 10/100 Base-TX Ethernet switch with VLAN
- DHCP server for IP assignment (up to 253 users)
- DNS cache and proxy
- NAT (Network Address Translation)
- Virtual server via port redirection or open port
- Port-based rate throttling capability
- Routing support: RIPv2, Static Route

Printer Server

- One USB port connector
- Built-in LPD printer server
- Support for Win98/98SE/ME LPR printer driver
- Compatible with Win2000/XP/MacOS 9/MacOS X built-in LPR printer driver

Wireless Access Point (Vigor2900VG/VGi only)

- 802.11g support (54Mbps data rate)
- Backward compatible with 802.11b device
- Wireless security:
  - .Secure VPN over WLAN
  - .WPA Support
  - .802.1x User Authentication
  - .64/128 bits WEP wireless encryption
  - .Client MAC-address locking
  - .SSID stealth

Flexible URL Content Filtering

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

Application Support

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

Router Management

- Web-based User Interface
- Command line interface (Telnet)
- Telnet remote access support
- SNMP agent with MIB-II
- Built-in diagnostic tools
- Remote firmware upgrade
- Quick Start Wizard
- Syslog Monitoring

ISDN Facilities (Vigor2900G/Vigor2900i only)

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

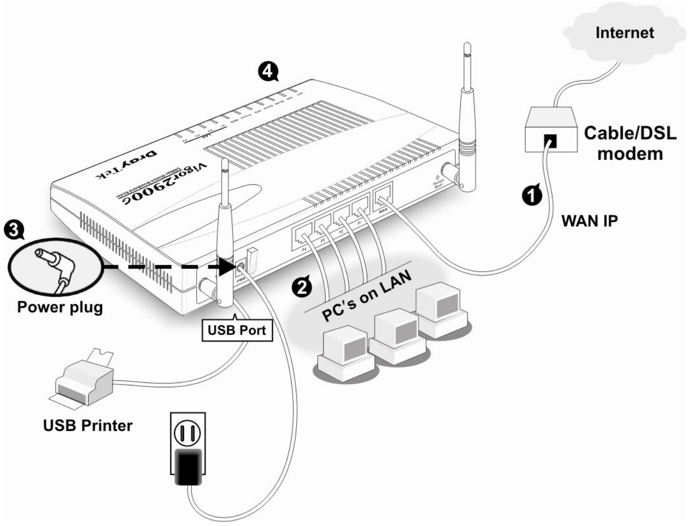
2. Hardware Connection

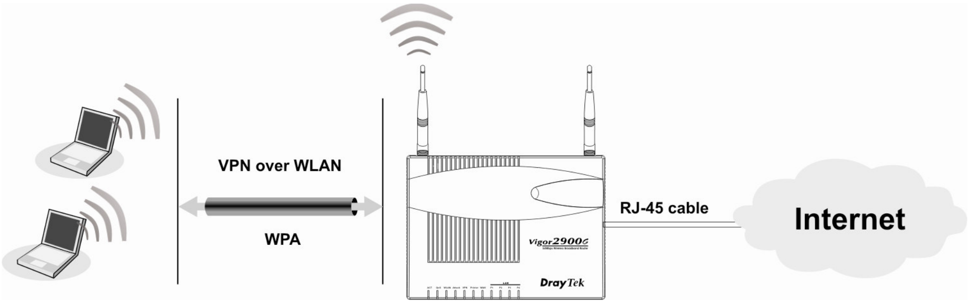
2.1 Hardware Connection

Before starting to configure the router, please ensure to connect your devices correctly.

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

Connection scenario is shown as below:



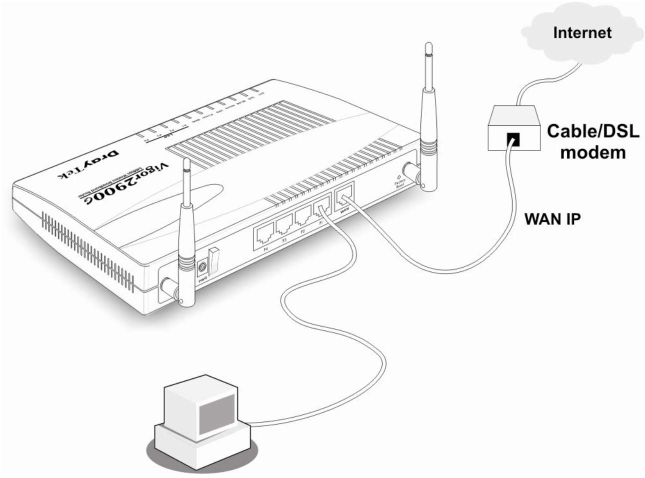


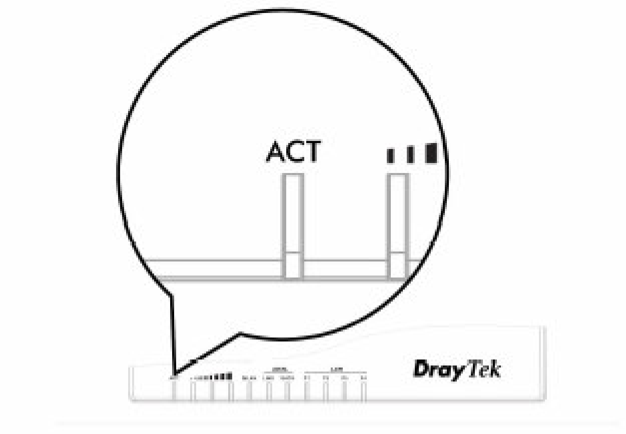
3. Trouble Shooting

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

3.1 Is the Hardware Status OK?

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

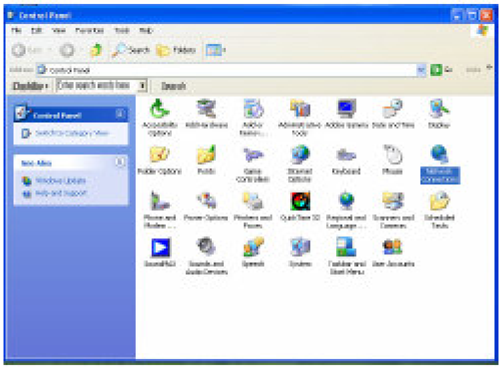




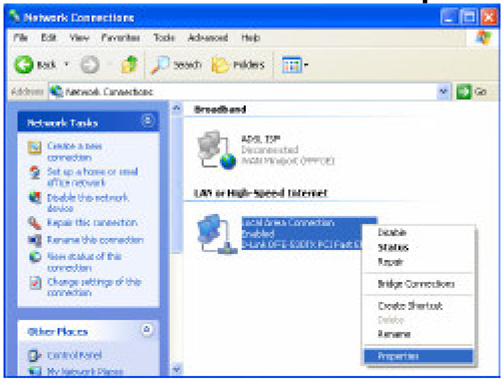
3.2 Are the Network Connection Settings on Your PC OK?

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

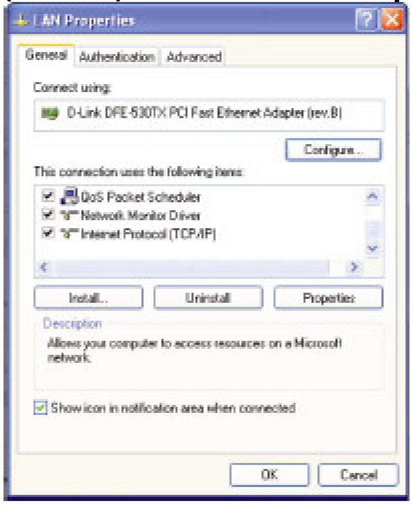
1. Go to **Control Panel** and then double-click on **Network Connections.**



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



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



Connect using:

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

This connection uses the following items:

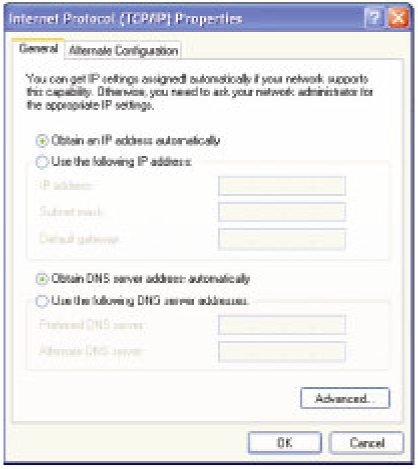
☑ QoS Packet Scheduler
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

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



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

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

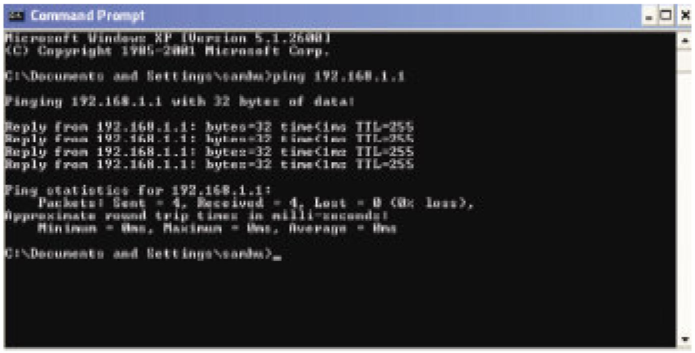
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

3.3 Can You Ping the Router from PC?

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

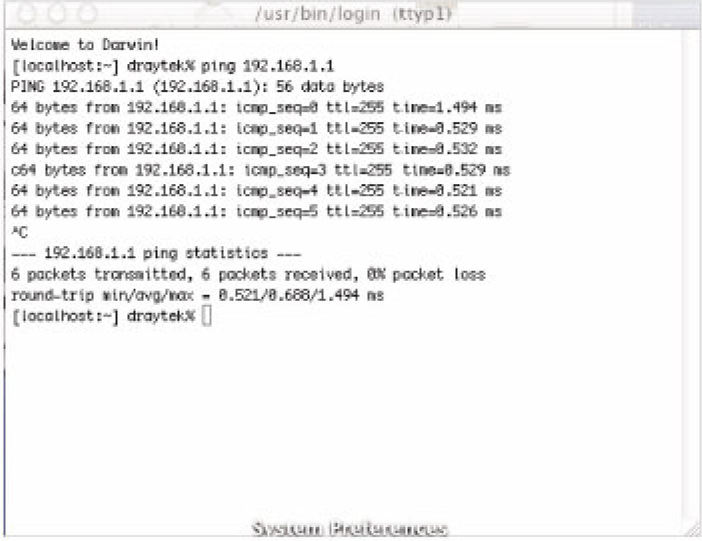
A. For Windows

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



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

C:\Documents and Settings\sandw>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

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

B. For Mac (Terminal)

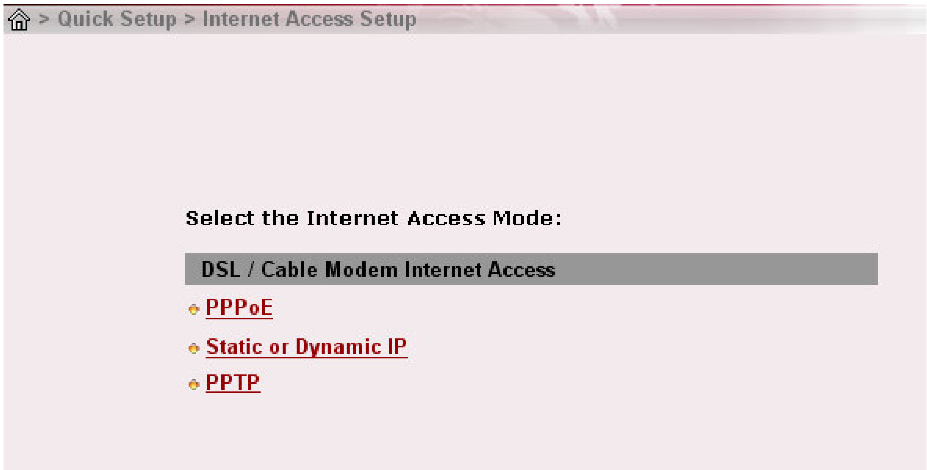


```
Welcome to Darwin!
[localhost:~] draytek% ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=1.494 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.529 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.532 ms
c64 bytes from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

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

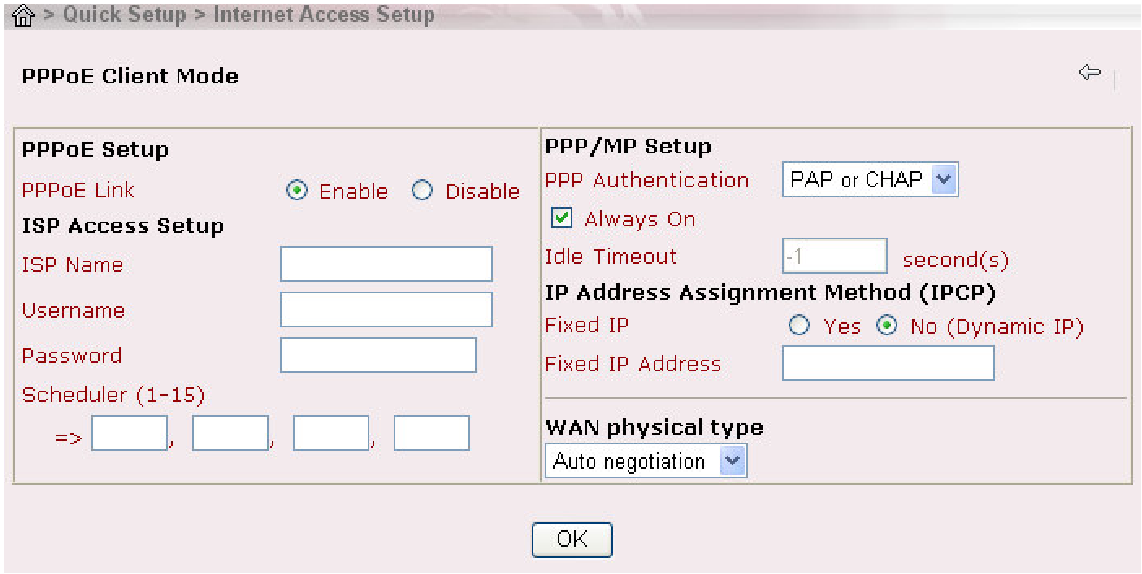
3.4 Are the ISP Settings OK?

1. Enter the web configuration UI to check your ISP settings (please refer to section2.2 setp1).
2. Click **Internet Access Setup** item in the “Quick Setup” group and then the UI will switch to the following window.


> Quick Setup > Internet Access Setup
Select the Internet Access Mode:
DSL / Cable Modem Internet Access
PPPoE
Static or Dynamic IP
PPTP

A. For PPPoE Users

1. Check that if the **Enable** option is selected.
2. Check that if the **Username** and **Password** are entered with correct value given by your ISP.



PPPoE Setup

PPPoE Link ● Enable ○ Disable

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

PPP/MP Setup

PPP Authentication: PAP or CHAP

☑ Always On

Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

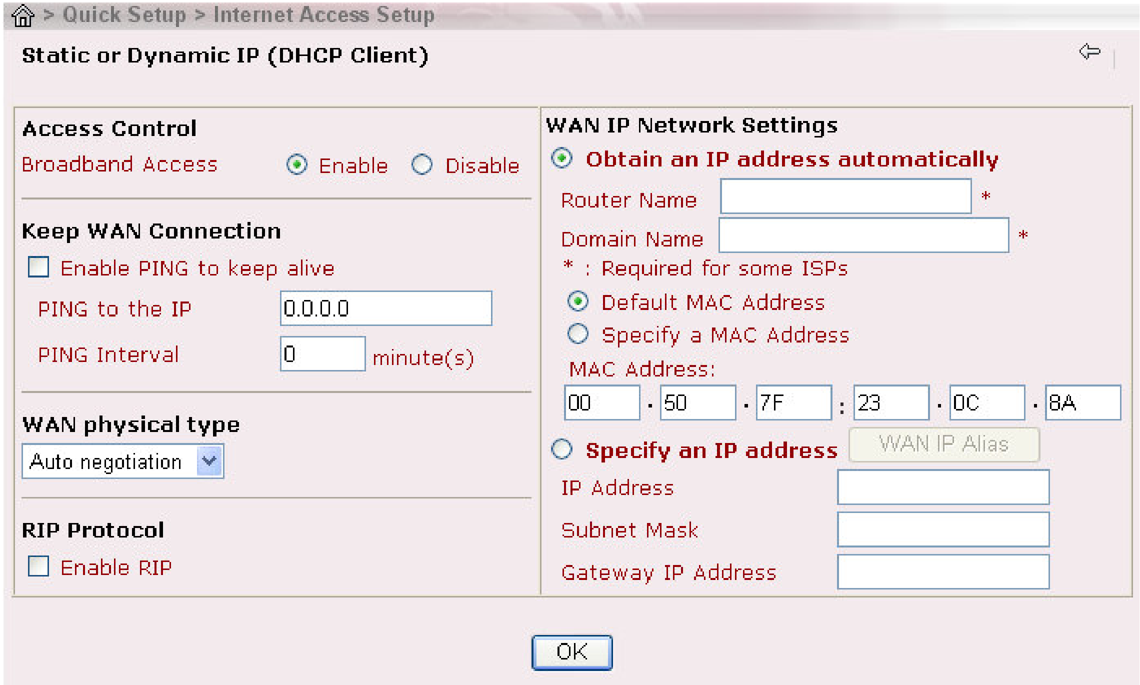
WAN physical type

Auto negotiation

B. For Static or Dynamic Users

1. Check that if the **Enable** option is selected.
2. Check that if **WAN IP Network Settings** is set appropriately. If you select “Specify an IP address”, **IP Address, Subnet Mask,** and **Gateway IP**

Address have to be entered with the correct value.



> Quick Setup > Internet Access Setup

Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

Keep WAN Connection

☐ Enable PING to keep alive

PING to the IP: 0.0.0.0

PING Interval: 0 minute(s)

WAN physical type

Auto negotiation

RIP Protocol

☐ Enable RIP

WAN IP Network Settings

● **Obtain an IP address automatically**

Router Name: *

Domain Name: *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F : 23 . 0C . 8A

○ **Specify an IP address**

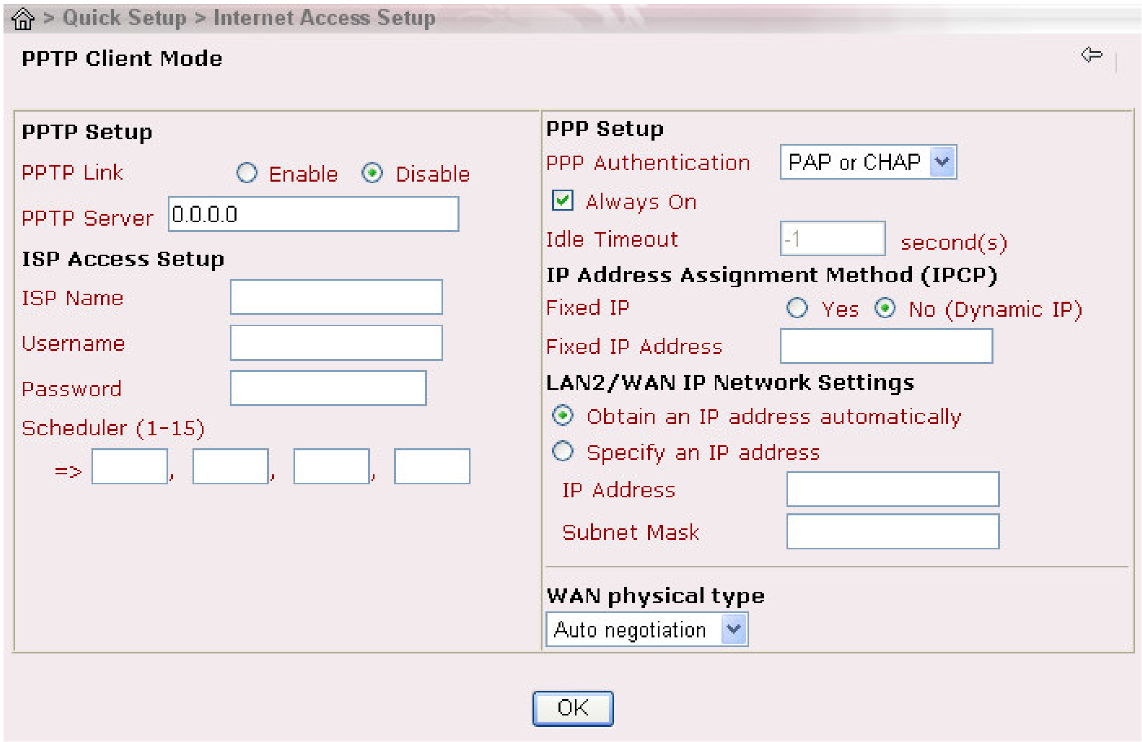
IP Address:

Subnet Mask:

Gateway IP Address:

C. For PPTP Users

1. Check that if the **Enable** option is selected.
2. Check that if **PPTP Server, Username, Password** is entered the correct value given by your ISP.
3. Check that if **LAN2/WAN IP Network Settings** is set appropriately. If you select “Specify an IP address”, **IP Address** and **Subnet Mask** have to be entered with the correct value.


> Quick Setup > Internet Access Setup

PPTP Client Mode

PPTP Setup

PPTP Link ○ Enable ● Disable

PPTP Server 0.0.0.0

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

PPP Setup

PPP Authentication PAP or CHAP

☑ Always On

Idle Timeout -1 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

LAN2/WAN IP Network Settings

● Obtain an IP address automatically

○ Specify an IP address

IP Address

Subnet Mask

WAN physical type

Auto negotiation

3.5 Report to ISP and Dealer for Further Technical Support

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