Table of Contents

0

Preface

0.1 About This Manual

This manual is designed to assist users in using the Vigor2200USB. Information in this document has been carefully checked for accuracy; 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 latest product info and features, please visit our website.

0.2 Copyright Declarations

0.3 Trademarks

Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, and 2000 are trademarks of Microsoft Corp. Other trademarks and registered trademarks of products referred to in this manual are the properties of their respective owners.

0.4 How To Become A Registered Owner

Web registration 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.

0.5 Safety Instructions

• Read the installation guide thoroughly before you set up the Vigor2200USB.
•The Vigor2200USB is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
•Do not place the router in a damp or humid place, e.g. a bathroom.
•The Vigor2200USB should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
•Do not expose the Vigor2200USB to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
•Keep the packaging out of reach of children.
•When you to dispose of the Vigor2200USB, please follow local regulations on conservation of the environment.

0.6 Warranty

We warrant to the original end user (purchaser) that the Vigor2200USB will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase.

During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, re-

pair 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 re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

The warranty does not cover 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.

0.7 European Community Declarations

We hereby declare that the Vigor2200USB is in compliance with the essential requirements and other relevant provisions of R&TTE Directive 99/5/EC.

1 Getting Started

1.1 Introduction

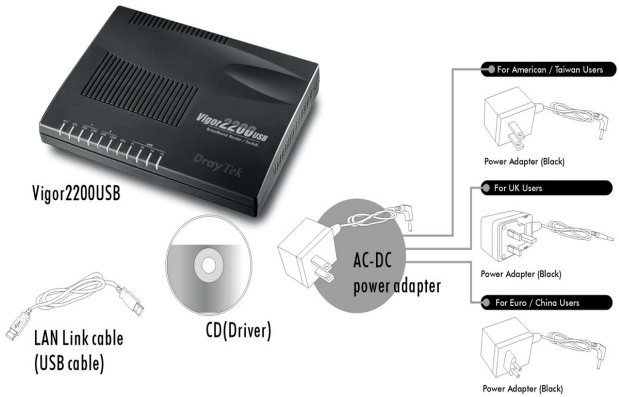
The Vigor2200USB provides multiple users with efficient and reliable access over a DSL line to the Internet and corporate LAN for using e-mail, sharing documents, Web surfing, file transfers, etc.

The broadband access protocol for the USB port supports PPPoE, PPPoA. These protocols comply with USB-based DSL Modem standards.

1.2 Unpacking Your Vigor2200USB

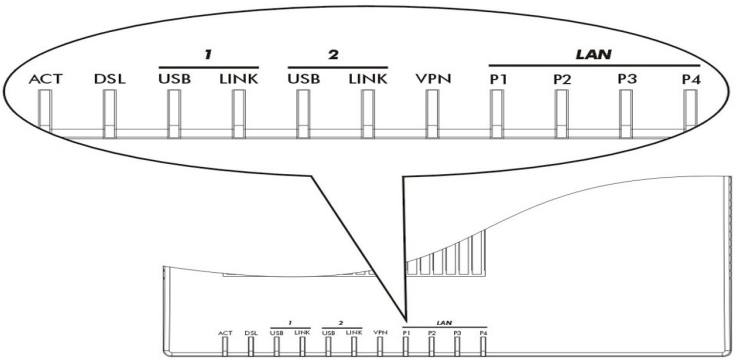
Your Vigor2200USB package should contain the items listed below. If any item is missing or damaged, contact your dealer or our Customer Service Department immediately.

- One Quick Start User Guide with warranty/registration card
- One CD-ROM; includes detailed User Manual in electronic form, latest released firmware, and utilities
- One AC/DC power adapter (black)
- One Ethernet LAN cable (blue) for connection to a computer or hub


Vigor2200USB
LAN Link cable
(USB cable)
CD(Driver)
AC-DC
power adapter
For American / Taiwan Users
Power Adapter (Black)
For UK Users
Power Adapter (Black)
For Euro / China Users
Power Adapter (Black)

1.3 LED Indicators & Rear Panel Description

LED Indicators



There are eleven LEDs on the front panel; ACT, DSL, USB, LNK, USB, LNK, VPN, P1, P2, P3 and P4.

ACT (Activity)
Blinks when power is supplied to the router and the router is running normally.

DSL
ON when the DSL modem is active.

USB1 Group:

USB
ON when the DSL modem is ready.
Blinking when there is data transferring between the Vigor2200USB and the DSL modem.

LNK
ON when the PPP connection of the DSL modem is active.

USB2 Group:

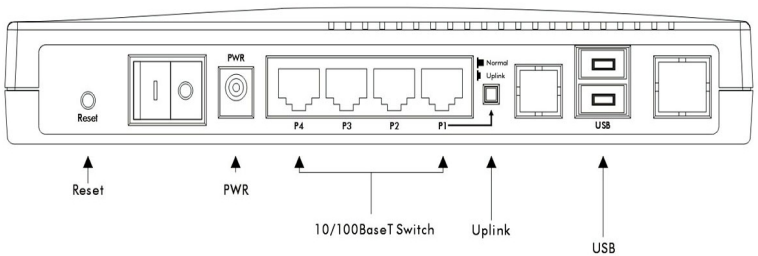
USB
ON when the DSL modem is ready.
Blinking when there is data transferring between the Vigor2200USB and the DSL modem.

LNK
ON when the PPP connection of the DSL modem is active.

VPN
ON when the VPN function is active.

P1, P2, P3, P4 (LAN)
ON when a network card or hub is connected.

Rear Panel Description



The Vigor2200USB has a reset button, a power jack, four 10/100Base-T RJ-45 switch ports, an Uplink button, and 2 USB ports on the rear panel:

Reset

For firmware upgrades: Press and hold the button, then power ON. The ACT and DSL LEDs will blink simultaneously (see section 5.5). To restore default settings: While the device is running, press the button and hold for more than five seconds. When the ACT LED begins to blink rapidly, release the Reset button. The router will restart with the default configuration

PWR

Only the supplied power adapter should be connected to the power jack.

P1, P2, P3, P4
These are 10/100Base-TX Ethernet Switch ports. Connect your PCs to these ports.

Uplink
For connecting to another hub/switch, press the Uplink button and connect the other hub/switch to the P1 port.

USB

The DSL USB modem (Alcatel Speed Touch USB, or DynaMite USB Modem) should be connected to one of these USB ports. For an interoperable USB DSL modem list, contact DrayTek or your dealer.

1.4 Detailed Features

The Vigor2200USB provides many built-in server and software features to provide a convenient comprehensive solution for your SOHO network.

1. **Network Address Translation (NAT)**: NAT allows multiple SOHO users to concurrently connect to an Internet Service Provider (ISP) using a single Internet access account.

2. **Firmware Upgrade (TFTP) Server**: Using this server and the **Firmware Upgrade Utility** software, you may easily upgrade to the latest firmware whenever enhanced features are added.

3. **Web (HTTP) Server**: A Web browser is the most common tool used to surf the Internet. You may use Microsoft's **Internet Explorer** or a **Netscape** browser etc, to configure the router as easily as surfing a website.

4. **Domain Name Server (DNS) Proxy**: The DNS proxy maintains a DNS cache, including a mapping table of domain names and IP addresses. The proxy also remembers DNS query packets sent through the router and saves them into its own DNS cache. For enhanced speed, when a DNS query packet enters the Vigor2200USB, the proxy searches its local DNS cache. If matched, the Vigor2200USB sends an answer to the host that sent the DNS query packet. Only umatched DNS queries require querying a WAN Domain Name Server.

5. **Telnet Terminal Server**: The Telnet User Interface (TUI) is an efficient method of configuring and managing routers. It utilizes a traditional command-line user interface and is mainly for advanced configuration, management, and troubleshooting.

6. **Dynamic Host Configuration Protocol (DHCP) Server**: This server provides an easy-to-configure function for your local IP network. It automatically assigns IP network configurations to local PCs, such as IP address, IP netmask, gateway IP address, and Domain Name Server etc.

7. **Built-in Flash ROM**: The Flash ROM memory saves the Vigor2200USB firmware and configurations, even after power down.

8. **Point-to-Point Protocol over Ethernet (PPPoE) Client Support**: The Vigor2200USB has a built-in PPPoE client for establishing a DSL link connection with the ISP. There is no need to install a further PPPoE driver on your computers.

9. **Firewall**: In addition to the built-in NAT mechanism, the Vigor2200USB features another powerful firewall to protect your local network, or to deny specified local users access to unauthorized network services.

10. **VPN**: The Vigor2200USB supports to establish a private network of computers that's partially connected over the internet. The IPSec protocol is used for VPN (Virtual Private Network).

2 Installation & Setup

2.1 Before You Begin

1. Use only the power adapter supplied by us. Using an incorrectly rated power adapter will result in damage to the router.

2. In case of emergency, unplug the power adapter first.

3. Locate the device in a clean location. Do not block the ventilation slots on the rear panel.

4. Cables must be attached to the correct ports; to do otherwise may result in damage to the router. Keep cables away from walkways.

5. If you are a DSL user with USB ADSL modem, check that if your USB ADSL modem is **Alcatel Speed Touch USB** or **DynaMite USB Modem**. For other USB ADSL modem, please check the information on web to see if the router support it.

6. Before you set up the router, you need to know the router default settings as shown on the next page:

Factory Default Settings:

Router' s Default IP Network Settings:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server: Enabled

Start IP Address: 192.168.1.10

IP Pool Counts: 50

Web Configurator:

Username: admin

Password: <blank>

Note: Blank means no password required.

Telnet Console:

Password: <blank>

Note: Blank means no password required.

Management from the Internet:

Not allow.

2.2 Hardware Installation

2.2.1 Connecting the Power Adapter

1. Connect the power adapter to the power outlet on the wall and to the PWR power jack on the rear panel of the router.

2. The **ACT** LED should be blinking once every 2 seconds.

2.2.2 Connecting to the Ethernet

A. Connecting to a PC:

1. Attach the Ethernet cable (blue color cable) to any P1 ~ P4 port.

2. Connect the other end of the Ethernet cable to your PC's installed network interface card (NIC).

3. The LED indicators at both the Ethernet port and the NIC should be ON.

Note:
If the Ethernet cable is not long enough to reach your PCs, purchase a longer straight-through CAT. 5 UTP or STP Ethernet cable.

B. Connecting to an External Ethernet Hub or Switch:

1. Attach the Ethernet cable (blue color cable) to any P1~ P4 port.

2. Connect the other end of the Ethernet cable to the external Ethernet hub or switch.

3. The LED indicators on both the Ethernet port and the external Ethernet hub or switch should be ON.

Note:
If the Ethernet cable is not long enough to reach the external hub/switch, purchase a longer straight-through 10Base-T Ethernet cable.

2.2.3 Installing USB ADSL Modem firmware

The following document describes how to install and configure the router with your Alcatel Speedtouch USB modem or DynaMite USB modem. Please follow the instructions closely, step-by-step:

Preparation

Do not connect the USB modem to the router yet.

1. Connect the router to the PSU(Power supply unit) and an Ethernet cable between a PC and any one of the router's four Ethernet sockets.

2. If the PC is set to obtain IP address automatically (recommended), reboot the PC and ensure that it has obtained an IP address from the router (you can use Windows *winipcfg.exe* or *ipconfig.exe* to check). You can use windows ping.exe to check that your PC can see the router successfully (ping 192.168.1.1).

3. Insert the supplied DrayTek CD into your PC, and install the Router Tools.

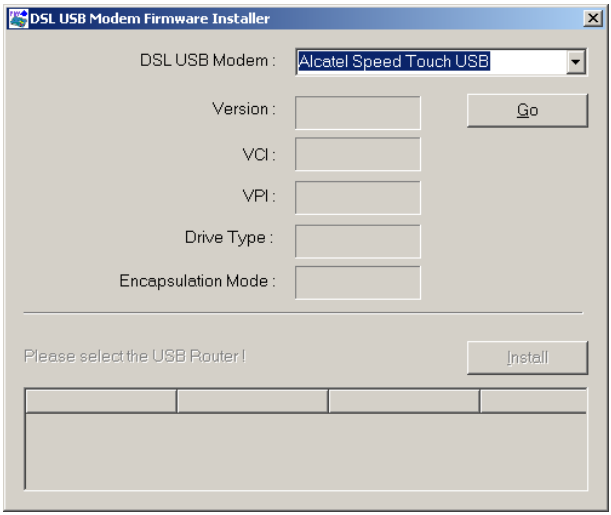
Step 1 - Upload ADSL modem firmware into router

The USB modem is designed in such a way that its own firmware is loaded from the host device (PC or Vigor2200USB) every time it is initialised or restarted.

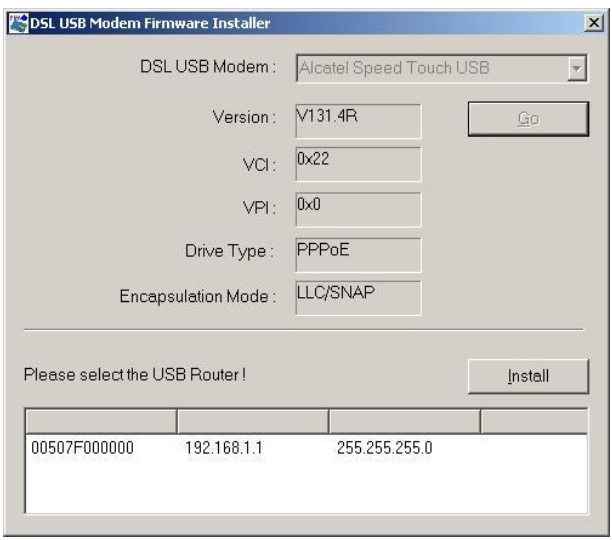
You must upload the modem's firmware into the Vigor2200USB's memory so that it's available to the modem. This only ever needs to be done once; the firmware is then stored in the Vigor2200USB's non-volatile memory.

From your Windows Start Button, run the USB Modem Firmware utility :

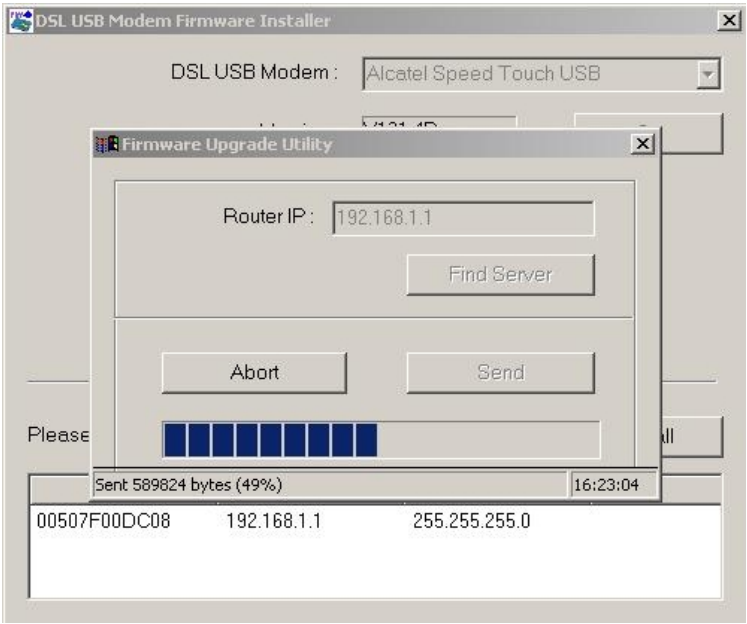
Firstly, the utility will detect your modem type. Currently only the "Alcatel SpeedTouch USB" and "DynaMite USB" are supported. Support for other models will be added later; please check with your dealer. If you have more than one USB modem installed, you may need to select it in the list :



After the correct modem is selected, click "**Go**" and you should see some information relating to ATM settings, firmware version and the IP address of the router :



Then, press "**Install**" and the firmware will be uploaded to the router :

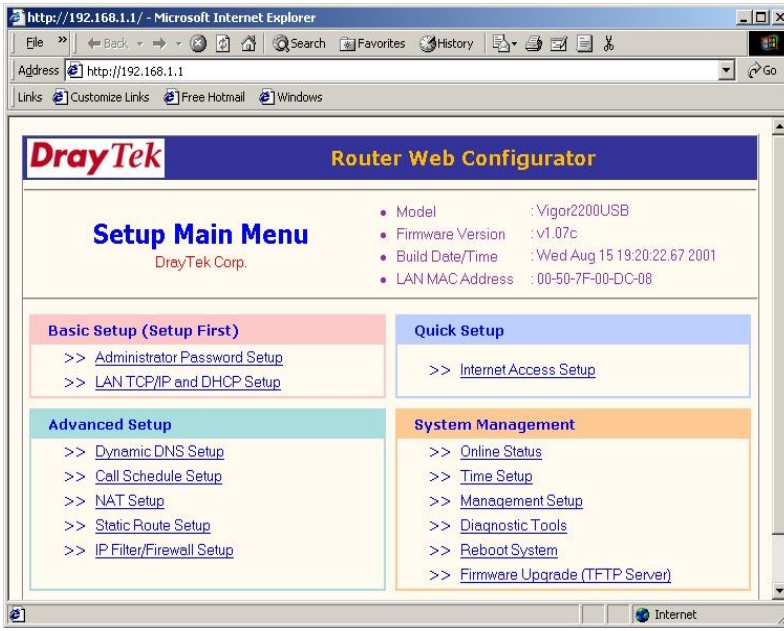


Step 2 - Configure your ISP details

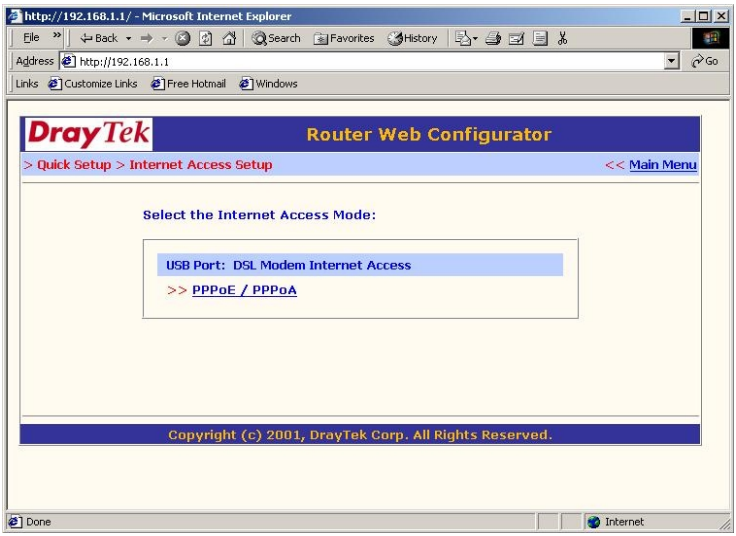
Where as your log-in name and password was previously stored on your PC (in Dial-up networking), these details now need to be stored in the Vigor2200USB so that it can automatically log into your ISP when required.

Open you web browser (e.g. MSIE or Netscape) and enter the Vigor2200USB's IP address into the address bar (http://192.168.1.1). The Vigor2200USB will ask for a username and password. There is none by default, so just click "**OK**".

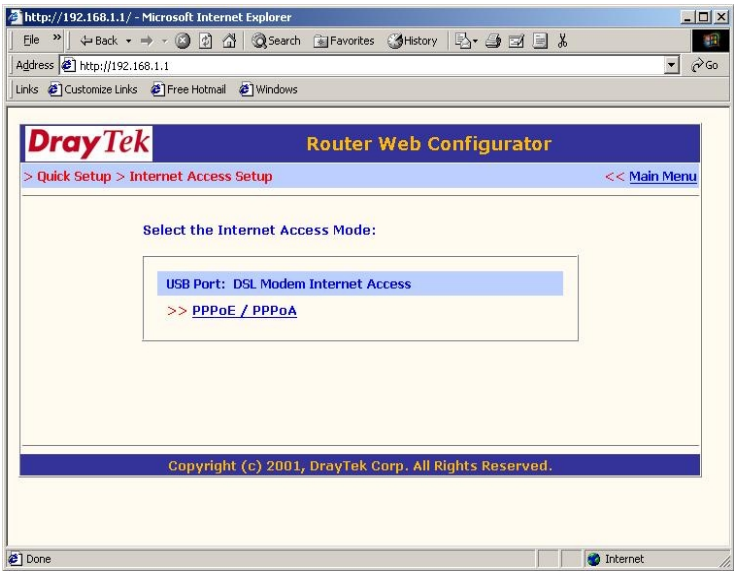
Once past the password prompt, you will now see the router's main menu :



Click on Internet Access Setup on the top right-hand menu.



Click **PPPoE/PPPoA** :



Enter ISP's Name and your allocated username and password according to the information provided by your ISP. Then click "**OK**".

Step 3 - Connect the USB ADSL Modem to your Vigor2200USB

Connect your USB ADSL modem to either of the USB ports on the rear panel of the router. After the firmware successfully is downloaded from the router to the modem, the USB LED on the front panel should light. This procedure will take few seconds to complete.

Connect the your ADSL line to your modem. The modem should start to handshake with the central site modem and once it has connected, the DSL LED on the front of the modem should light. This will take about 10-15 seconds to complete.

From your web browser, access the Internet - type in a web address. This will trigger the router to log-in to your ISP. Once the router has successfully logged in, the LNK LED will light on the front of the router. You now access to Internet from any PC. The router will stay connected to the ISP indefinitely. If you would prefer that it ends the connection after a fixed period of inactivity, you can select that in the ISP options.

2.3 Setting Up a Management PC

The router has a built-in HTTP (Web) server for configuration. Before you use the router to access the Internet, you should set up a management PC to log into the router for further configuration. The management PC may be configured with a fixed or dynamically assigned IP address.

For a fixed IP address, use an IP address from a 192.168.1.0/24 network, such as 192.168.1.2.

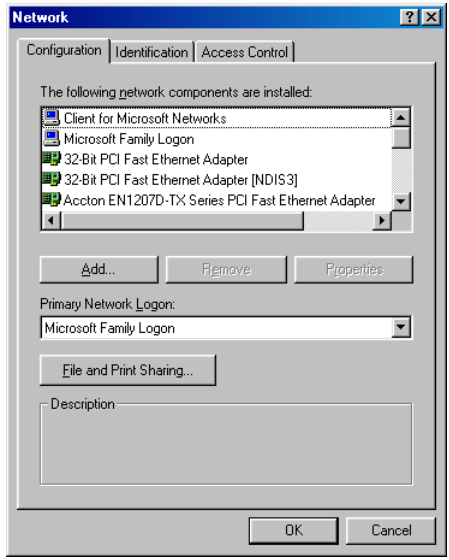
For a dynamic IP address, you need to set the PC as a DHCP client, and then restart or renew the network settings. The DHCP server of the router is enabled by default so the PC will then be assigned an IP address and related settings by the router.

The following examples are for a Microsoft™ Windows 95/98 machine set to use a dynamic IP address. For other operating systems, please refer to the OS user manuals.

2.3.1 Checking the Network IP Configuration

The following explains how to setup the Transmission Control Protocol/Internet Protocol (TCP/IP) in Windows 95/98. For more detailed information on TCP/IP setup, refer to the Windows 95/98 help files. For other operating systems refer to the user manuals.

1. On the desktop, right click "**Network Neighborhood**". Click "**Properties**". The Network screen will open (see the next page).

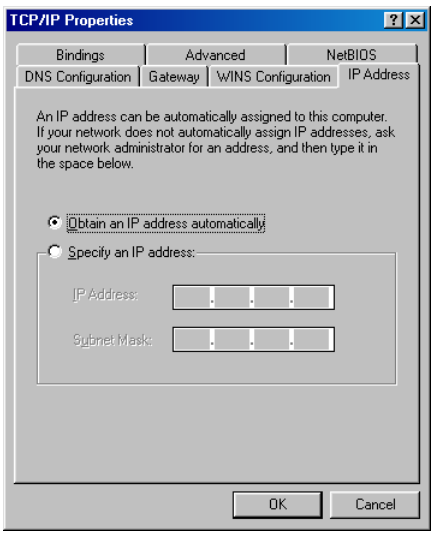


Your particular system will be different from the screen shown here. Check that you have an Ethernet network card installed. If not, refer to the card manufacturers documentation and install the card and drivers. If your card is installed,

1. Click the "**Add**" button. The Select Network Component Type dialog box will open. The box will show four options: *Client, Adapter, Protocol, Service.*
2. Select Protocol and click the "**Add**" button. The Select Network Protocol dialog box will open.
3. Select Microsoft in the left scrolling window, then select TCP/IP in the right, and click "**OK**". You will be returned to the Network dialog box.

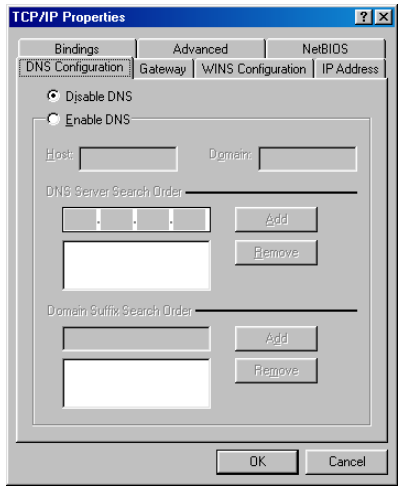
2.3.2 Configuring the TCP/IP Protocol

1. On the Network dialog box Configuration card, select TCP/IP and then click "**Properties**". The TCP/IP Properties dialog box will open.

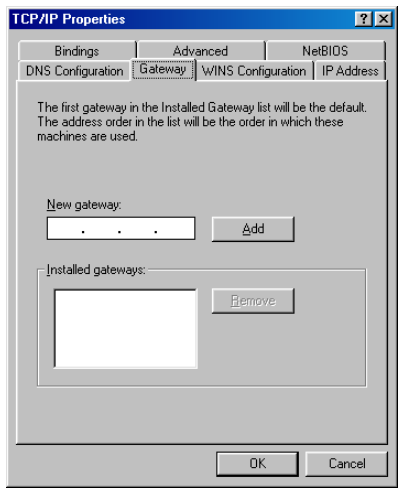


2. On the IP Address tab, click "**Obtain an IP address automatically**". As the DHCP (Dynamic Host Configuration Protocol) server built into the router is enabled by default, your computer will get an IP address, subnet mask, and other related IP network settings from the router.

3. On the DNS Configuration tab, click "**Disable DNS**".



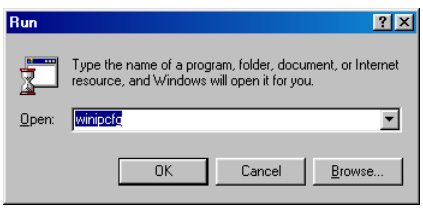
4. Click the "**Gateway**" tab.

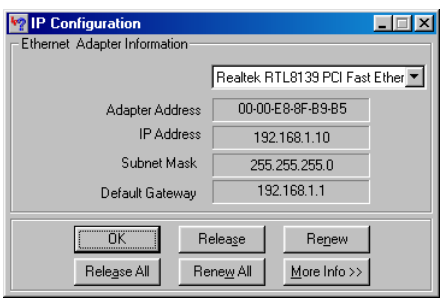


5. Make the **New gateway** and **Installed gateways** fields blank and click "**OK**". A dialog box will pop up asking you to restart the PC. Click "**Yes**"

2.3.3 Checking TCP/IP settings

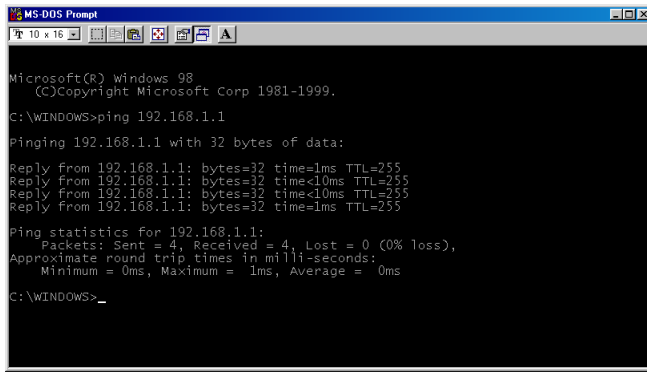
1. After completing the previous steps, click "**Start**" -> **Run**" and type "**winipcfg**". The **IP Configuration** window will open. If the PC does not show an IP address in the **192.168.1.2** to **192.168.1.254** range, click the "**Release**" button to release the current configuration. Wait a few seconds and click "**Renew**" to get a new IP configuration from the router.





2. If the IP configuration is correct, you will be able to use the PING diagnostic utility built into Microsoft Windows to ping the router. Click "**Start** -> **Programs** -> **MS-DOS Prompt**".

A a command mode window will open. Type "**ping 192.168.1.1**"(default IP of the router) to check the network connectivity. If both hardware and software are correct, your computer will receive a response from the router as shown on the next page. If not, verify that the Ethernet cable is connected to the router properly and the Ethernet port LED on the front panel is lit.



2.4 Using the Smart Start Wizard

The **Smart Start Wizard** will guide you through using the Web Configurator or Telnet Terminal (command-line based management). Also, if your currently installed network is not located in the 192.168.1.x IP range, the wizard will find the router and change the router's default IP address and IP mask to match the current network.

If you are familiar with using a web browser (Microsoft Internet Explorer, Netcape Communicator, etc.) or telnet client software, you may jump directly to the next section (page 2-18). We suggest you use the most up-to-date version of your web browser.

Installing the Router Tools

1. Insert the CD supplied with the router into the CD-ROM drive. The autorun CD will display the main menu.

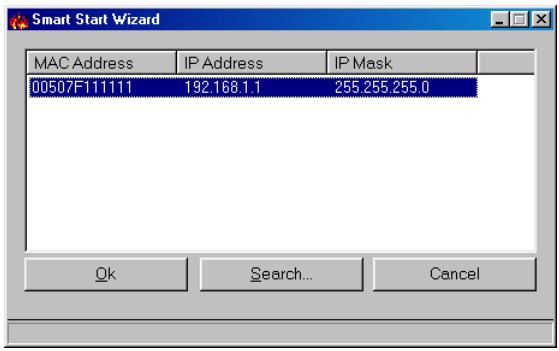
> **Note:**
>
> If autorun fails to start the installation program, click autostart.exe on the root directory of the CD to start the program.

2. Click "**Router Tools**" and select the OS platform you wish to install to. The Router Tools utilities include the **Firmware Upgrade Utility**, and the **Smart Start Wizard.**

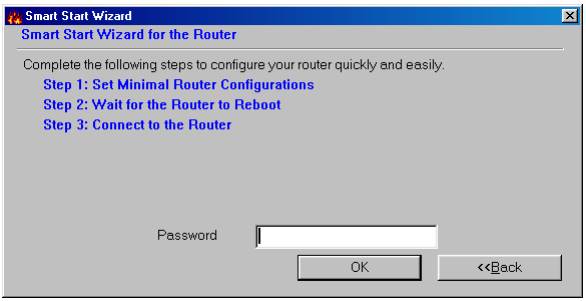
Using the Wizard

1. Click "**Start** > **Programs** > **Router Tools** > **Smart Start Wizard**".

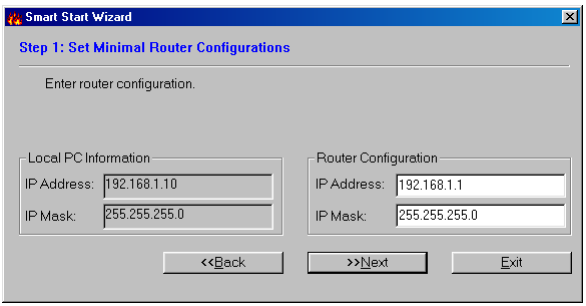
The following screen will open.



2. Click "**Search**" to find the router on your network.
3. Click "**OK**" to go to the login password screen.

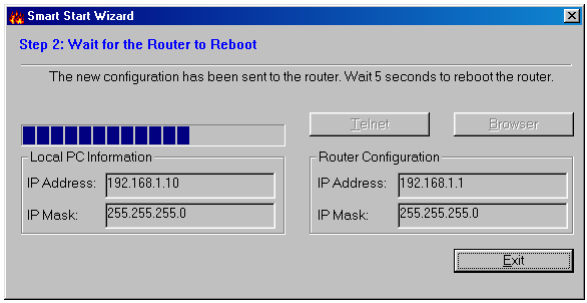


4. If this is a first time setup of the router, do not enter a password. Click "**OK**" to go to next screen.

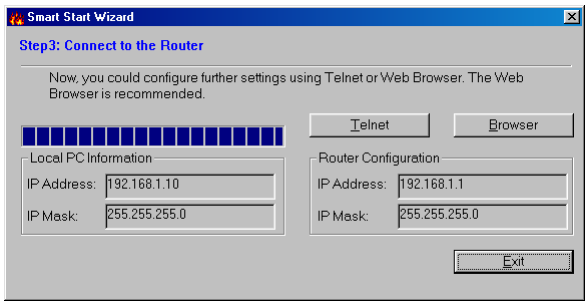


The screen shows read-only IP and IP mask settings for the PC you are using, and also the **IP Address** and **IP Mask** settings for the router. Here you may change the router settings to match your current network environment, or keep the default settings.

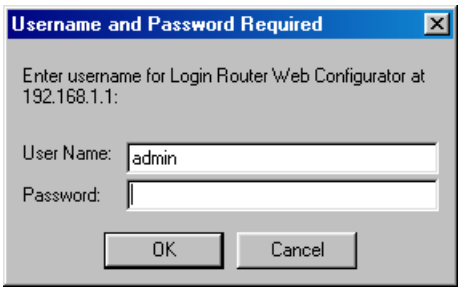
5. Click "**Next**" to update the settings to the router.



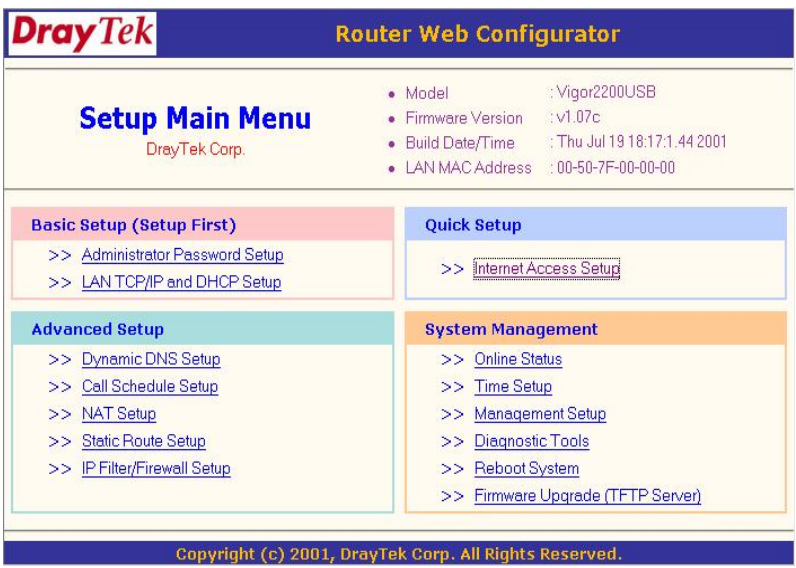
6. Wait for a few seconds. The **Telnet** and the **Browser** buttons will become active (see the next page).



7. If the IP address and IP Mask of your PC and of the router are not located on the same subnet, renew your PC's IP address, using *winipcfg.exe* on Windows95/98/Me,or *ipconfig.exe* on Windows NT/2000. When the browser is launched, the following pop-up window will ask for a User Name and Password.



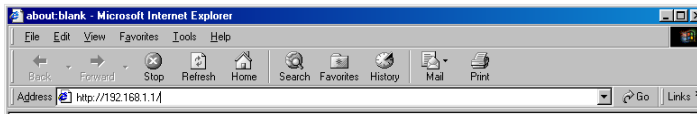
8. Enter "**admin**" as the User Name and leave the Password field blank. The Web Configurator will open. In the following examples we use the Netscape™ web browser (see the next page).



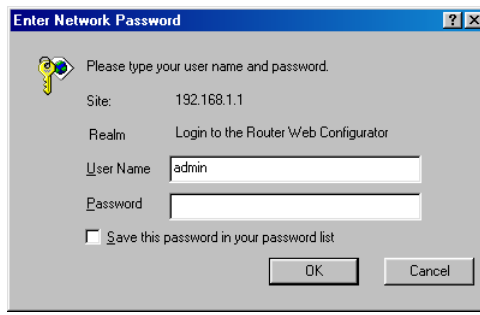
2.5 Using the Web Configurator

2.5.1 Connecting to the Web Configurator via a Web Browser

1. Launch the Web browser. Enter "**http://192.168.1.1**" into the browser **Address** window and press the Enter key.

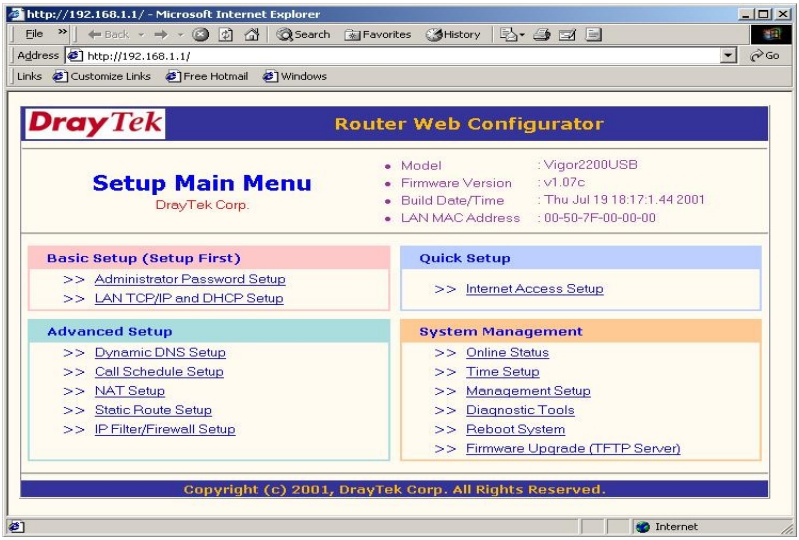


2. An authentication dialog box will open.



3. If this is a first time setup of the router, type "**admin**" as the User Name and leave the Password field blank. Click "**OK**".

4. The Web Configurator Setup Main Menu will open. On the main page, Model, Firmware Version, Build Date/Time and LAN MAC (Hardware) Address information will be displayed.



2.5.2 Overview of the Web Configurator

The *Setup Main Menu* (see above figure) consists of four groups: *Basic Setup (Setup First), Quick Setup, Advanced Setup, and System Management*. The following outlines each configuration menu.

Basic Setup (Setup First):

1. Administrator Password Setup:

   Sets/changes the administrator password.

2. LAN1 TCP/IP and DHCP Setup:

   Modifies the router' s IP address and DHCP server settings.

Quick Setup:

1. Internet Access Setup: (required for Internet access)

   Usually the router functions as a border router for SOHO or home networking so you must enter settings here to enable access to the Internet.

Advanced Setup:

The following settings are for advanced configurations only. These items do not need to be configured for standard Internet access.

1. NAT (Network Address Translation) Setup

   Sets NAT configurations, such as Port Redirection, DMZ etc.

2. Static Route Setup

   This menu has 10 routing rules for static routing usage. Here you may add/delete or activate/deactivate any static route.

3. IP Filter/Firewall Setup

   The router has a powerful built-in firewall. Up to 84 Call Filter and Data Filter rules may be set.

System Management:

1. Online Status

   Click this item to view current online status and statistics of the system.

2. Management Setup

The item allows you to set or limit access rights to manage the router. Also, you may set HTTP or Telnet ports to specific port numbers of your choice.

3. Diagnostic Tools

Diagnostic tools offers useful tools for diagnosing the router or your network, e.g. view ARP table, routing table, NAT port map, DHCP server status, last triggered packet, etc.

4. Reboot System

You can restart the router with the default configuration or with the current running configuration.

5. Firmware Upgrade (TFTP Server)

Enables the TFTP server for firmware upgrades.

Note:
You should now have some basic concepts on how to setup and configure the router. The following chapters will explain each setup menu and related settings in more detail.

3 Basic Quick Setup

The Web Configurator Setup Main Menu includes four groups: **Basic Setup (Setup First)**, **Quick Setup**, **Advanced Setup,** and **System Management**.

This chapter explains the Basic Setup group and Internet Access Setup (which is in the Quick Setup group).

3.1 Administrator Password Setup

For security reasons, we strongly recommend that you set an administrator password for the router. On first setup the router requires no password. If you don't set a password the router is open and can be logged into and settings changed by any user from the local network or the Internet.

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

Old Password:

If this is the first time to set a password, leave this field blank.

New Password:

Enter an administrator password.

Retype New Password:

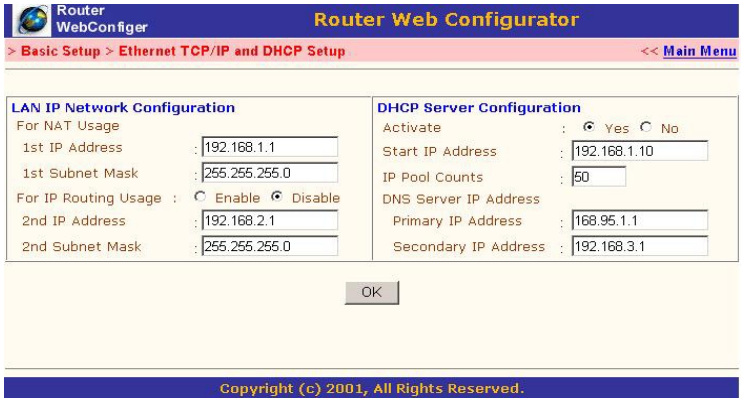
Type the password again for confirmation.

Click "**OK**".

3.2 LAN TCP/IP and DHCP Setup

The Vigor2200USB has one Ethernet LAN port for connecting to the local Ethernet network..

There are two sets of IP address settings for the LAN interface. The 1st IP address/netmask is for private users or NAT users, and the 2nd IP address/netmask is for public users. To allow public users requires you to have subscribed to a globally reachable subnet from your ISP.



LAN IP Network Configuration

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: Enables the 2nd IP address settings.

Disable: Disables the 2nd IP address settings.

2nd IP Address: Sets a public IP address.

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

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. The DHCP server supports up to 253 users (PCs) on the local network.

Activate: (Default: Yes).

Yes: Enables the DHCP server.

No: Disables the DHCP server.

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

IP Pool Counts: Sets the number of IPs in the IP address pool.

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 human friendly name into it's equivalent IP address.

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

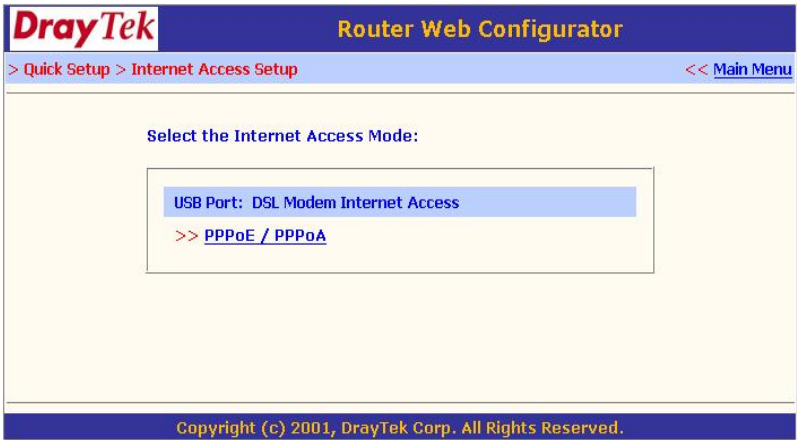
Secondary IP Address: Sets the IP address of the secondary DNS server.

Note:

If both the Primary IP and Secondary IP Address fields are left blank, 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) connection.

3.3 Internet Access Setup

For most users, Internet access is the primary application. When you click **Internet Access Setup** from within the **Quick Setup** group, the following setup page will be shown.



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

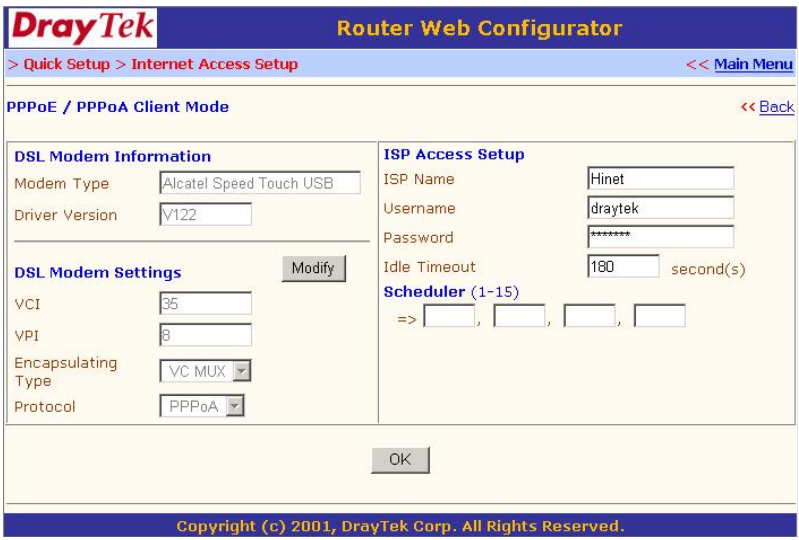
3.3.1 Getting USB Modem Settings

Before you connect a broadband access device, e.g. a DSL modem, to the router, you need to know what kind of Internet access is provided by your ISP.

When you install DSL USB modem firmware via installation tool, it will collect the following messages and configure router automatically.

Driver Type: PPPoA or PPPoE
Encapsulation Mode: VC MUX or LLC/SNAP
VCI: virtual channel identifier assigned by ISP.
VPI: virtual pipe identifier assigned by ISP.

You do not need to modify the settings. But if your ISP have changed the setting or you install the USB ADSL modem firmware from another environment, you can click Internet Access Setup to enter the PPPoE/PPPoA setting page to change it.



3.3.2 Using PPPoE/PPPoA with a DSL Modem

DSL Modem Information

Modem Type: display the usb dsl modem model name

Driver Version: display the firmware version of usb dsl modem

DSL Modem Settings

VCI: virtual channel identifier assigned by ISP.
VPI: virtual pipe identifier assigned by ISP.
Encapsulation Mode: VC MUX or LLC/SNAP
Driver Type: PPPoA or PPPoE

ISP Access Setup

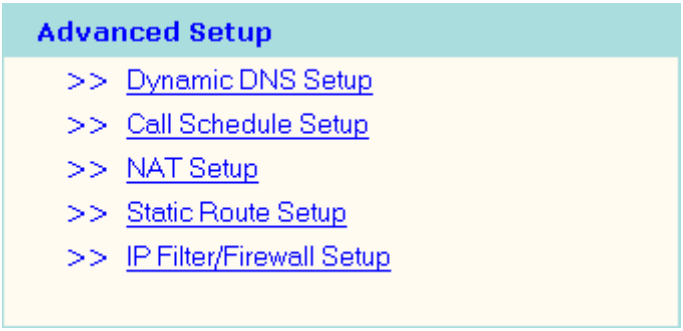
ISP Name: Enter the ISP name.

Username: Enter the ISP supplied username.

Password: Enter the ISP supplied password.

4 Advanced Setup

This chapter explains the options available in Advanced Setup:



4.1 Dynamic DNS Setup

1. Before You Set Up Dynamic DNS Function

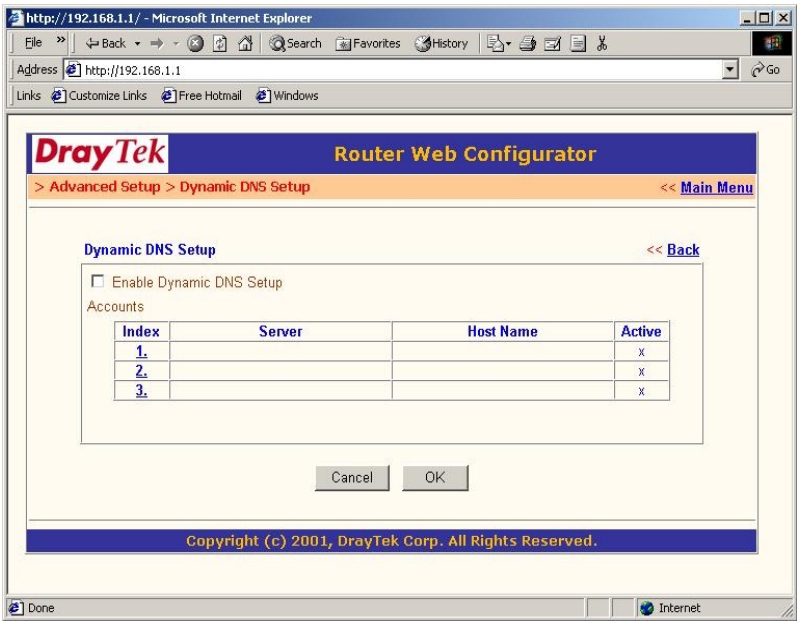
DDNS is short for Dynamic Domain Name System. This function could give a domain name to the router when it has been connecting to the Internet. Normally, most Internet access users have no their own domain name. If they want to set up Internet servers (ex. FTP, Web or Mail server) in the private local network using Port Redirection function, it's not easy way. Because the WAN IP address is always changing for every online. DDNS function makes the router can have one or many Domain Names. When the router has been connecting to the ISP, other Internet hosts or routers will be able to use the name(s) to reach or visit it whatever the WAN IP address is changing.

Before enabling the function, you should visit the web site www.dyndns.org to register an account and hostnames. Also, you will get more information in the web site. Now, the router just supports this DDNS service provider and 3 DDNS profiles. These profiles support the router can update its WAN IP address to three different domain names when it's online.

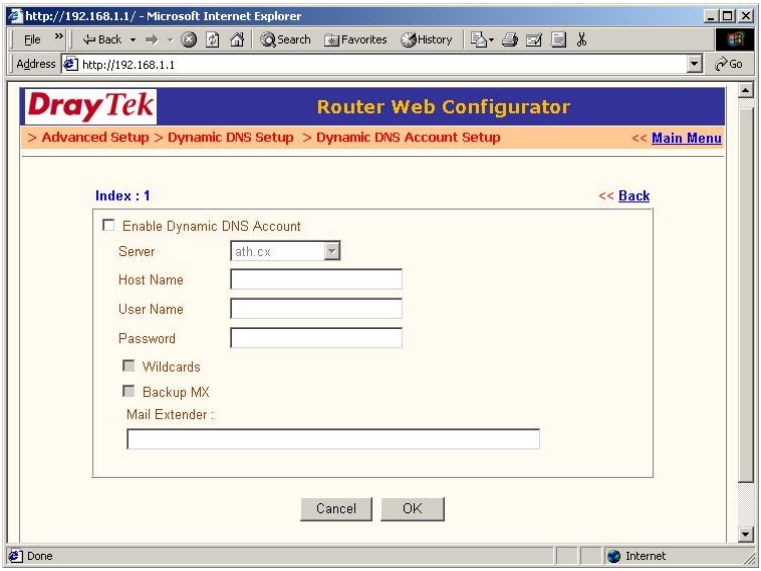
2. Configuring DDNS Function

(1) Register a DDNS account from the DDNS provider. You should visit the web site www.dyndns.org to register an account and hostnames first.

(2) Click "**Dynamic DNS Setup** " in the Advanced setup group. The following setup page will be shown.



(3) Click index "**1**" to set up a profile.

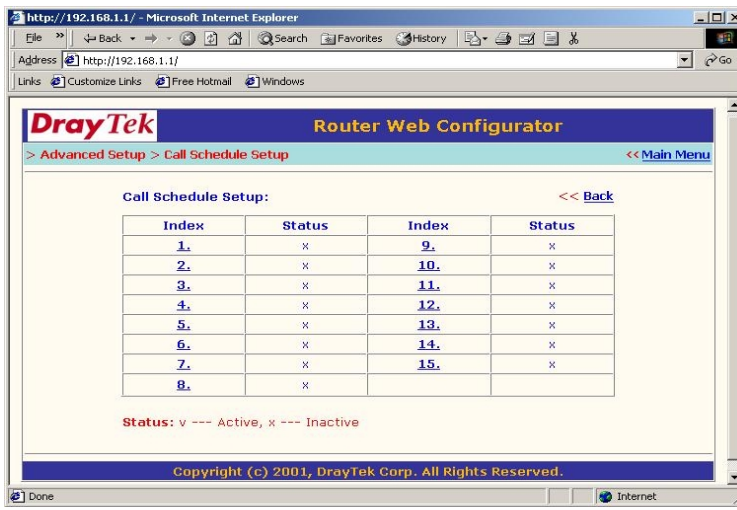


- Check "**Enable Dynamic DNS account**" to activate this account .
- Enter a name server for this account. This will depend on which name server you have registered on the www.dyndns.org web site.
- Put your own hostname in the "Host Name" field.
- Type your account in the "User Name" and "Password" fields.
- If the hostname is supported wildcard by the DDNS provider, you should check "Wildcard" to enable it. It also depends on whether the hostname has wildcard capability or not. For more detailed information, you also can get from the DDNS provider www.dyndns.org.
- Click "**OK**" to add an account.

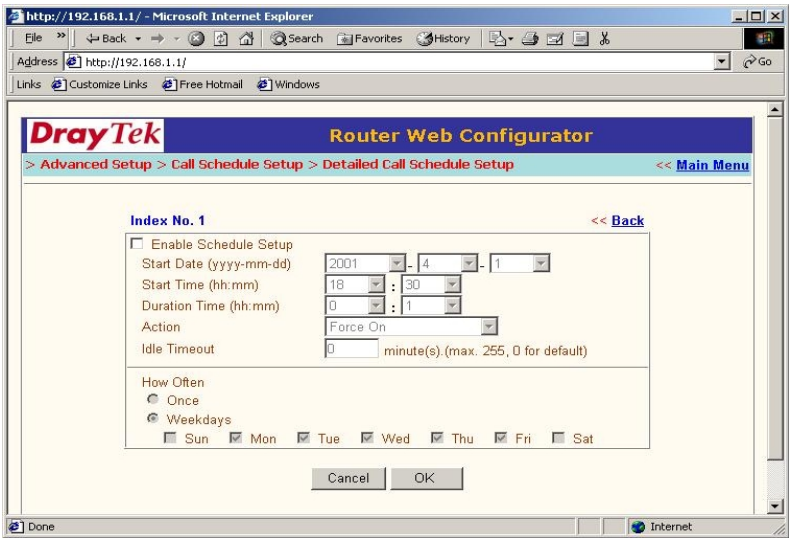
(4) Enable DDNS Function.
After configuring an account, the setup page will go back to upper level and "Dynamic DNS Setup" page will show again. The part of information regarding the account will show in the current page. Now check "Enable Dynamic DNS Setup" to enable the function and click "**OK**" to go back to "Setup Main Manual". The DDNS function has been finished.

4.2 Call Schedule Setup

Call Scheduler will control the router's dialer or connection manager what time should be up or down by these call schefule profiles. Before configuring the Call Scheduler function, you have to set uptime function properly, and arrange schedules for specified Internet access profile. Because it have to work with router's time.
The router supports total 15 profiles for call schedule usage. Click "**Call Shcedule Setup**" under Advanced Setup group, you will see these profiles as following.



Click any index the detailed settings of call schedule will be shown as below.



Enable Schedule Setup: Check it for enabling the schedule.
Start Date (yyyy-mm-dd): Specify the start date of the schedule.
Start Time (hh:mm): Specify the start time of the schedule.
Duration Time (hh:mm): Specify the duration (or period) ot the schedule.
Action: Specify which action should be applied by Call Scheduler during the time period of the schedule.

- Force On: Specify the connection up.
- Force Down: Specify the connection down.
- Enable Dial-On-Demand: Specify the connection is dial-on-demand and the value of idle timeout should be specified as following Idle Timeout field.

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

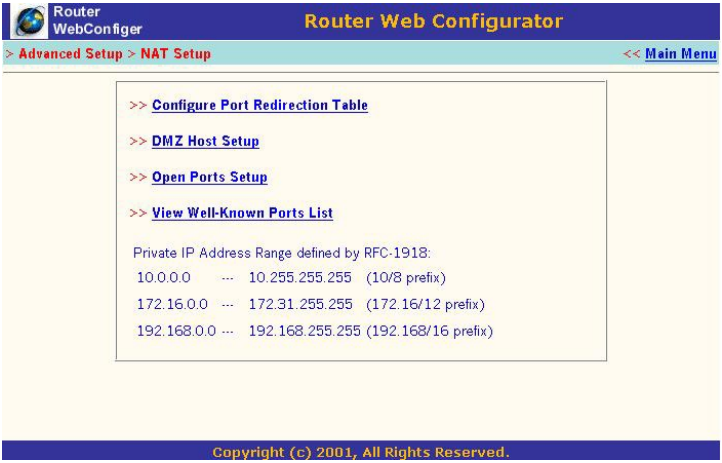
How Often: Specify how often the schedule will be applied.

- Once: Specify the schedule just once.
- Weekdays: Specify the schedule is according to weekdays.

4.3 NAT Setup

Usually you will use the router as a NAT-enabled router. NAT stands for Network Address Translation. It means the router gets one globally re-routeable IP address from the ISP. Local hosts will use private network IP address defined by RFC-1918 to communiate with the router. The router translates the private network addresses to a globally routeable IP address, which is then used to access the Internet. The following explains NAT features for specific applications.

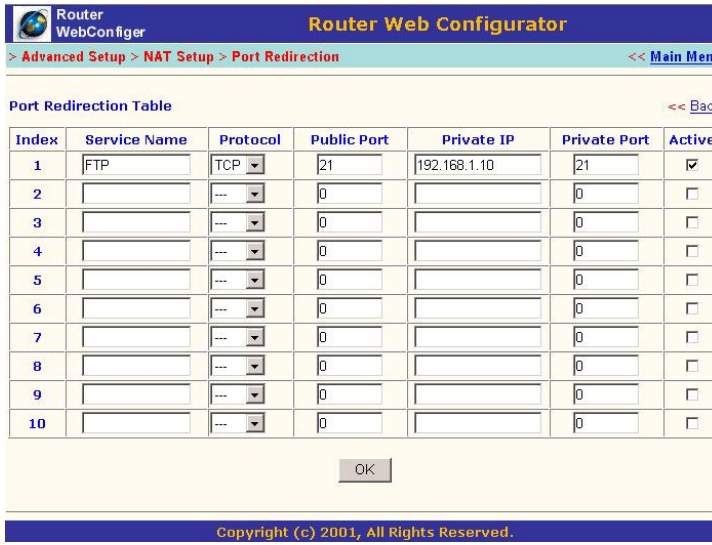
Click "**NAT Setup**" to open the setup page. On the page you will see the private IP address definitions defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the Vigor2200USB.



4.3.1 Exposing Internal Servers to the Public Domain

The Port Redirection Table may be used to expose internal servers to the public domain or open a specific port number to 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 an internal FTP server is exposed to the public domain. The internal FTP server is running on the local host addressed as 192.168.1.10.



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

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

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

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

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

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

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

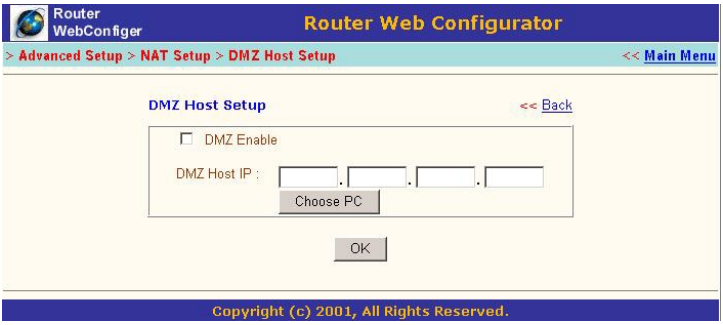
Click "**OK**".

4.3.2 DMZ Host Setup

Click "**DMZ Host Setup**". For outbound data packets, the DMZ host will not do TCP/UDP ports translation.On the other hand, for the inbound, the DMZ host will be forwarded to by default, even if no virtual server has been specified. The DMZ Host settings allow a defined internal user to be exposed to the Internet to use some special-purpose applications such as Netmeeting or Internet Games etc.

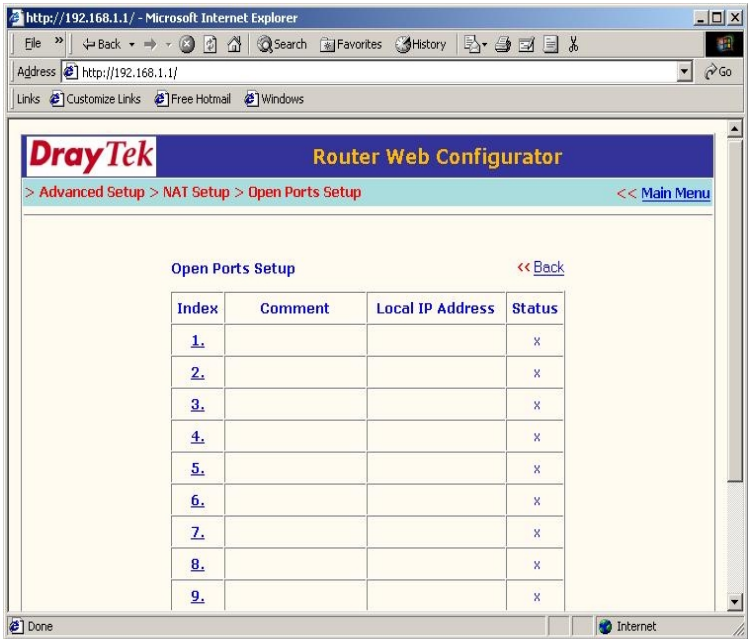
DMZ Enable: Check to enable the DMZ Host function.

DMZ Host IP: Enter the IP address of the DMZ host.

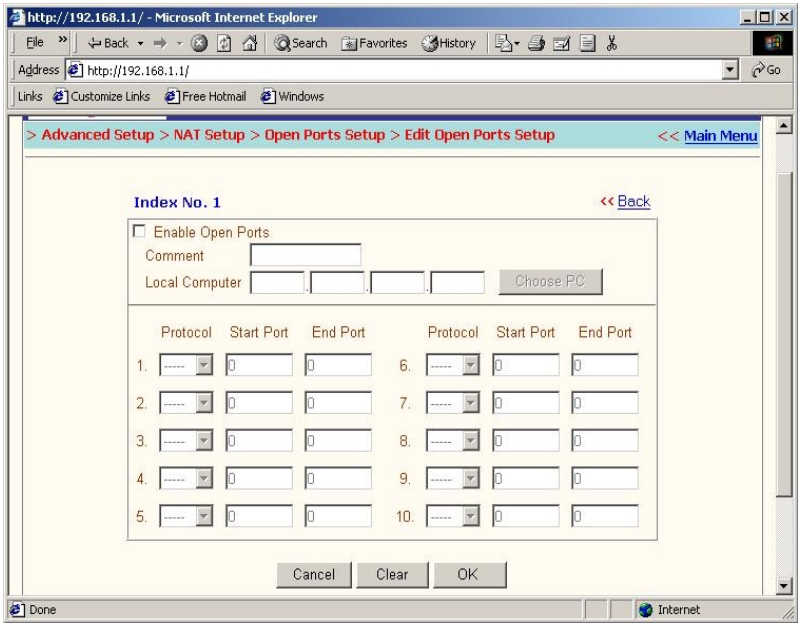


4.3.3 Open Ports Setup

Sometimes some of application software or Internet games have to pass many ports or range of ports through the router transparently. The Open Port Setup will help you to do that. Click "NAT Setup" under the Advanced Setup group, and "Open Ports Setup". The following setup page will be shown as below.



The router supports 10 profiles for Open Ports function. Each profile can allow you to open 10 different port ranges for a specified internet user (or host). Click index number, the following setup page will be shown as below.



Enable Open Ports: Check to enable this profile.

Note: The following settings will be allow changing after checking Enable Open Ports. Otherwise, these settings are no use.

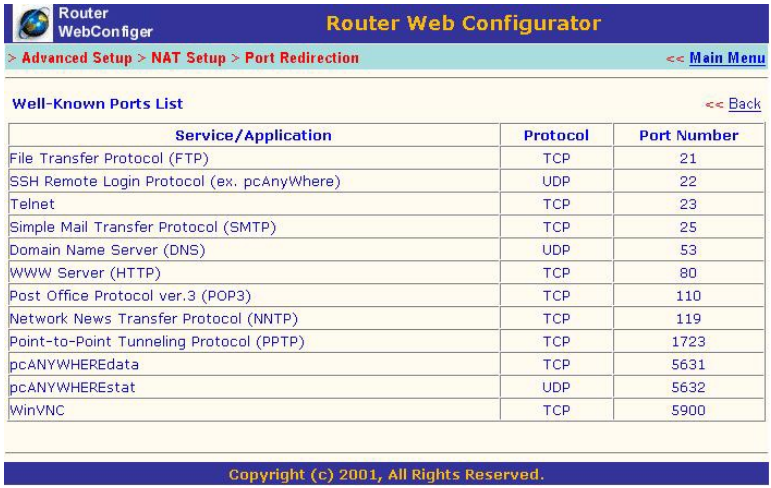
Comment: Type up to 12 characters for this profile.

Local Computer: Specify the IP address for a specified user. Also you can press "Choose PC" button to select the user.

For each profile, the router supports 10 port ranges could be configured.
Protocol: Specify the protocol.
Start Port: Specify the start port of a range.
End Port: Specify the end port of a range.

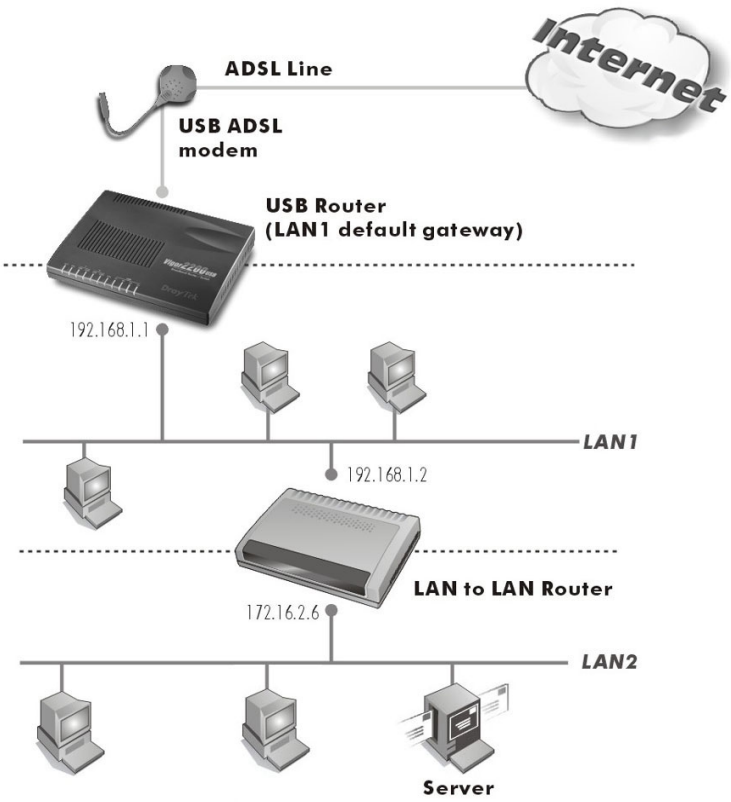
4.3.4 Well-known Port Number List

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

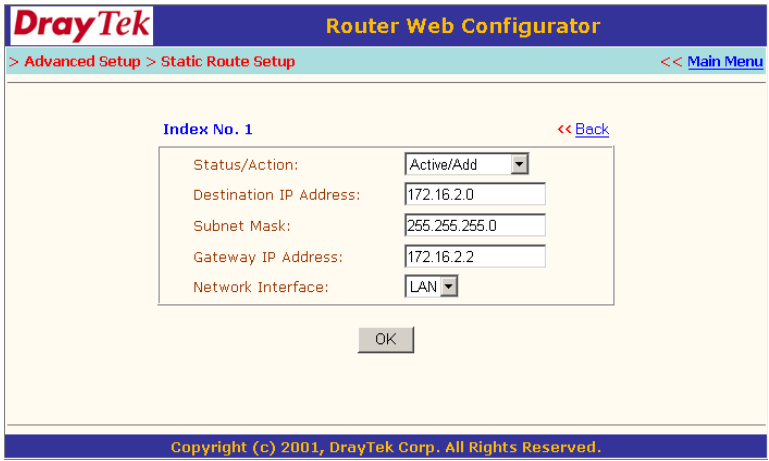


4.4 Static Route

You may need to access the other machines which behind other routers in the same network. You can use static route function to indicate the routing path for this kind of accessing.



For this example, when you in LAN1 and if you want to access the mail server behind 203.69.175.x, the IP packets will pass through internet to reach the mail server. If you use static route function, the IP packets can be forwarded to the mail server through the LAN-to-LAN router directly.



Status/Action : Set to Active/Add.

Destination IP Address : Specifies the target network IP or host IP. In this example, we use netwrk IP 203.69.175.0 as routed target.

Subnet Mask : Specific the target network mask. In this example, we hope to forward all 203.69.175.0/32 IP packets to the gateway.

Gateway IP Address : Specifies the IP address of the next hop router.

Network Interface : LAN

4.5 IP Filter/Firewall Setup

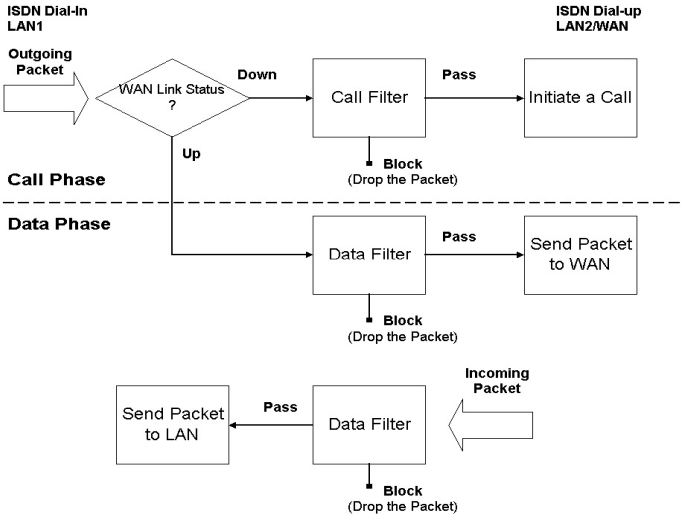
The IP Filter/Firewall function helps pretect your local network against attack from outside. It also provides a method of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

4.5.1 An Overview of the Firewall

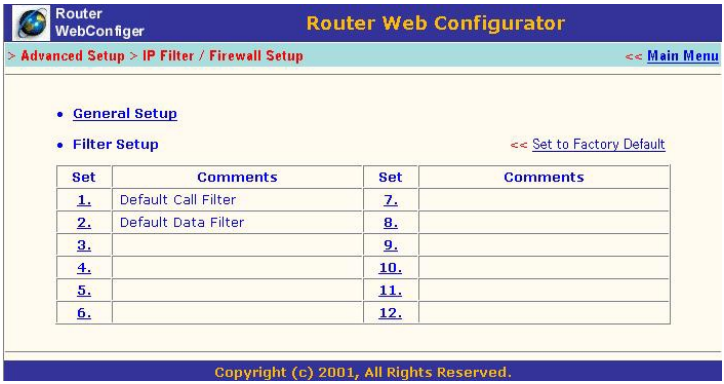
The IP Filter/Firewall includes two types of filter: Call Filter and Data Filter. The former is designed to block or allow IP packets that will trigger the router to establish an outgoing connection. The latter is designed to block or allow which kind of IP packets are allowed to pass through the router when the WAN connection has been established.

In concept, 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 dialling, 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 as below.



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



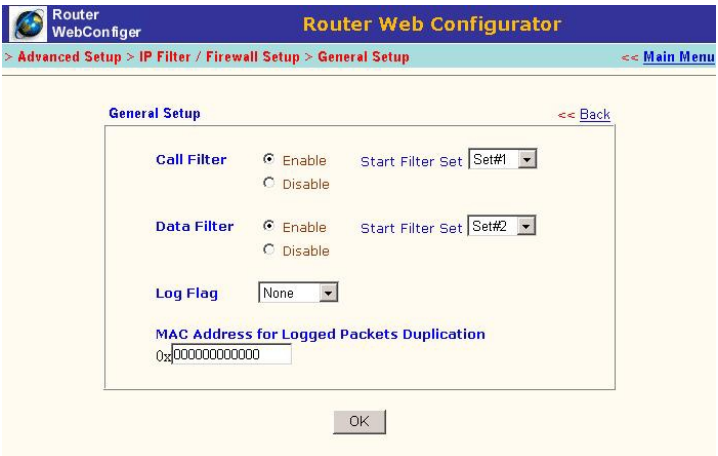
General Setup: Some general settings are available from this link.

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

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

4.5.2 General Setup

On 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.



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.

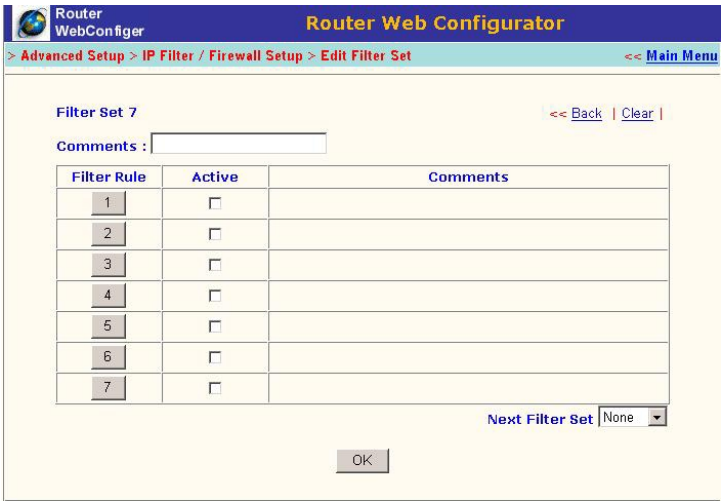
Pass: All passed packets will be logged.

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

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 MAC Address (HEX Format) of the other devices. Type 0 to disable the feature (also see Duplicate to LAN). The feature will be helpful under Ethernet environments.

4.5.3Editing the Filter Sets



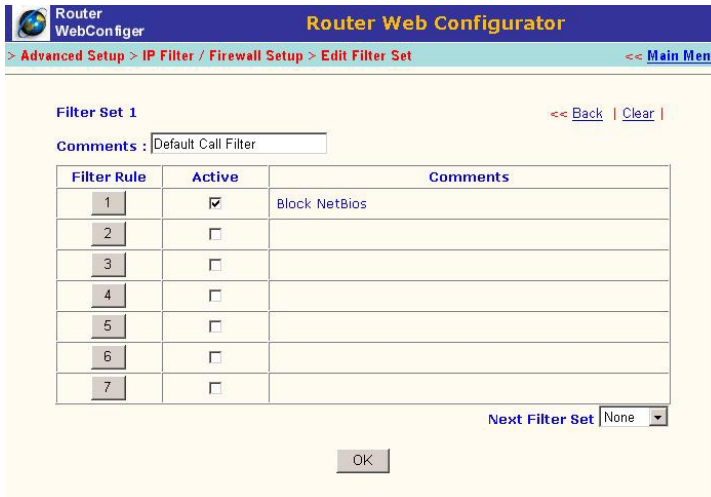
Comments: Enter filter set comments/description. Maximum length is 22 characters.

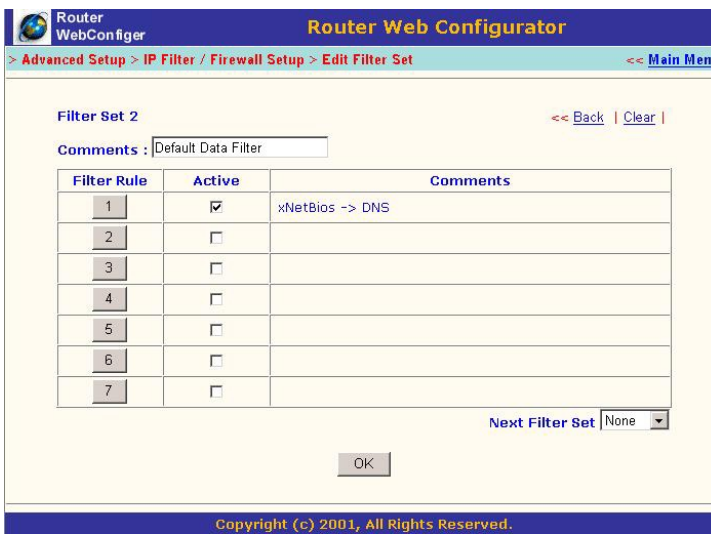
Filter Rule: Click a button numbered **1** ~ **7** to edit the filter rule.

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.


Router WebConfiger
Router Web Configurator
> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set
<< Main Menu
Filter Set 1
<< Back | Clear |
Comments : Default Call Filter
Filter Rule
Active
Comments
1
Block NetBios
2
3
4
5
6
7
Next Filter Set None
OK


Router WebConfiger
Router Web Configurator
> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set
<< Main Menu
Filter Set 2
<< Back | Clear |
Comments : Default Data Filter
Filter Rule
Active
Comments
1
xNetBios -> DNS
2
3
4
5
6
7
Next Filter Set None
OK
Copyright (c) 2001, All Rights Reserved.

4.5.4 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.

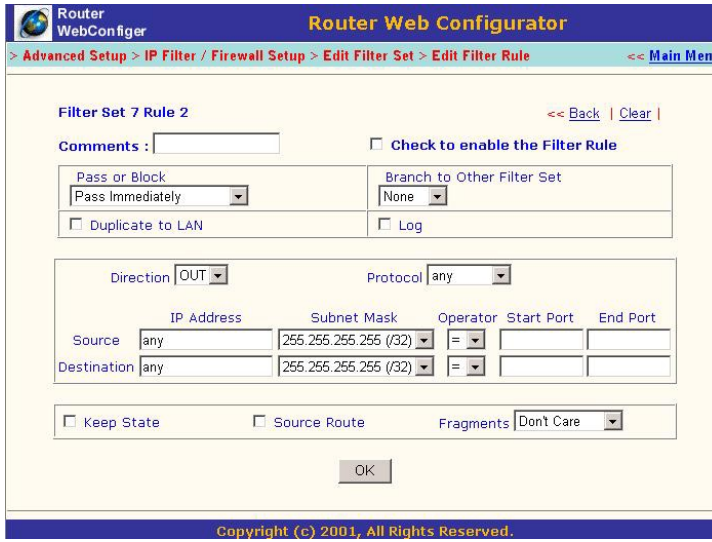
Pass or Block: Specifies the action to be taken when packets match the rule.

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.



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

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

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

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

For the Data Filter:

IN: Specifies the rule for filtering incoming packets.

OUT: Specifies the rule for filtering outgoing packets.

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

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

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

Operator: The operator column specifies the port number. If the **End Port** is empty, the port number is not equal to the value of the **Start Port.** Otherwise, this port number is not between the **Start Port** and the **End Port** (including the **Start Port** and **End Port**).

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

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

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

Fragments: Specifies a fragmented packets action.

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

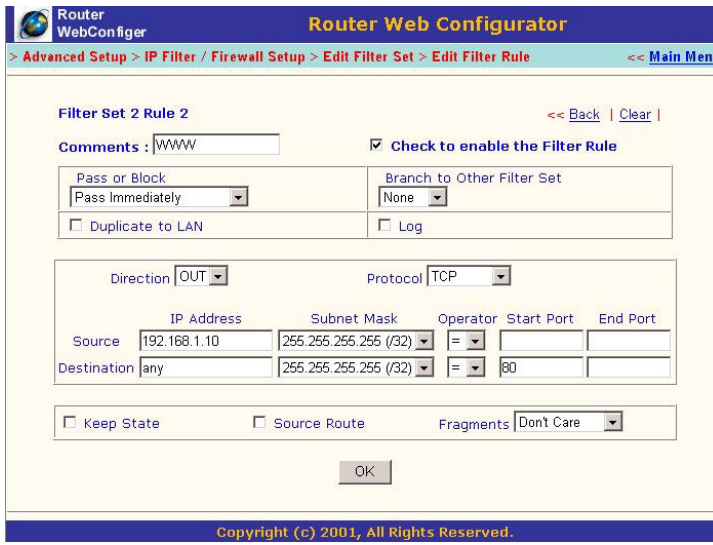
Unfragmented: Applies the rule to unfragmented packets.

Fragmented : Appliesthe rule to fragmented packets.

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

4.4.5 Restricting Unauthorized Internet Services

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

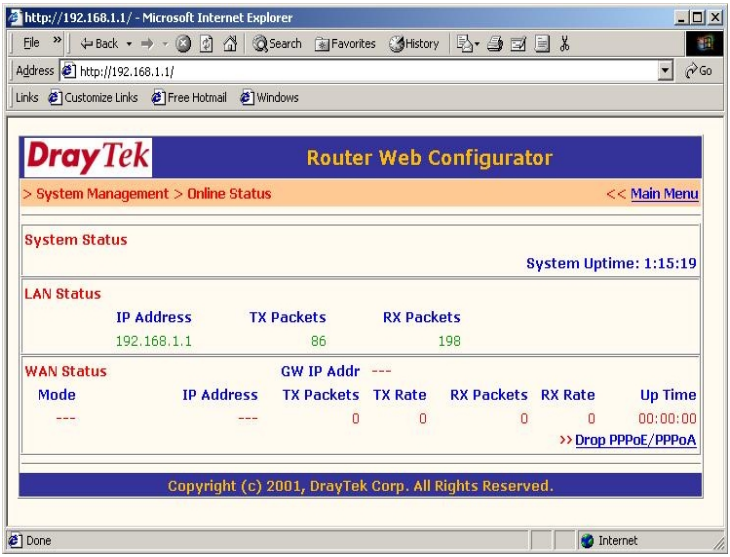


5 System Management

This chapter will show you how to manage your router using the **System Management** tools shown below.

5.1 Online Status

Click "**Online Status**" to open the *Online Status* page. The *Online Status* page contains three subgroups: *System Status, LAN Status, WAN Status.*



System Status:

System Uptime: Display the time the router was powered on.

LAN Status:

IP Address: IP address of the LAN interface.

TX Packets: Total number of transmitted IP packets sent since the router was powered on.

RX Packets: Total number of received IP packets received since the router was powered on.

WAN Status:

Mode: USB DSL modem model.

GW IP Addr : Gateway IP Address

IP Address: IP address of the WAN interface.

TX Packets: Total number of transmitted IP packets sent since the Vigor2200USB was powered on.

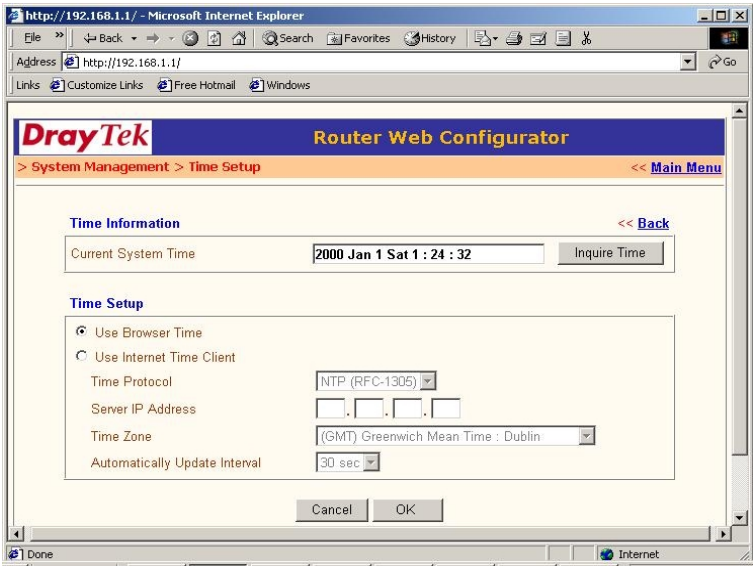
RX Packets: Total number of received IP packets received since the Vigor2200USB was powered on.

UP Time : Link up time

5.2 Time Setup

The router has been implemented a time client which can get time information from the Internet or local time server. If you want to use any time-based function (ex. Call Scheduler), the time client should be worked properly in advance.

Click "**Time Setup**" under System Management group to enter the setup page as below.



The page has two blocks, one is Time Information, the other is Time Setup. In the Time Inforamtion block, the Current System Time is showing the current time of the router. And press the Inquire Time button could get more updated time. In the Time Setup block supports few necessary settings. The details will be described as following.

Use Browser Time: Check to specify the time base from the web bowser which you are configuring. Note that if your computer time is not correct, the Vigor2200USB will get the wrong time.

Use Internet Time Client: Click to specify the time base from the Internet time protocol (ex. NTP).

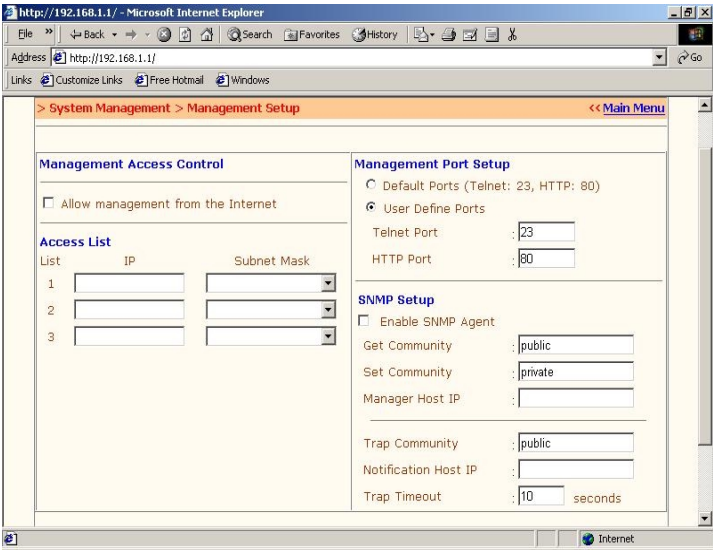
- Time Protocol: Specify time protocol.
- Server IP Address: Specify the IP address of time server.
- Time Zone: Specify the time zone.
- Automatioc Update Interval: Specify the interval to update time information from the time server.

Press "**OK**" to enable the time function.

5.3 Management Setup

By default, the Vigor2200USB may be configured and managed with 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 lists to protect the router, or reject system administrator login from the Internet.

Click "**Management Setup**". The following setup page will be displayed.



Management Access Control

Allow management from the Internet: Check to allow system administrators to login from the Internet. The default is not allowed.

Access List

You may 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 may be entered.

IP: Specifies an IP address allowed to login to the router.

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

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.

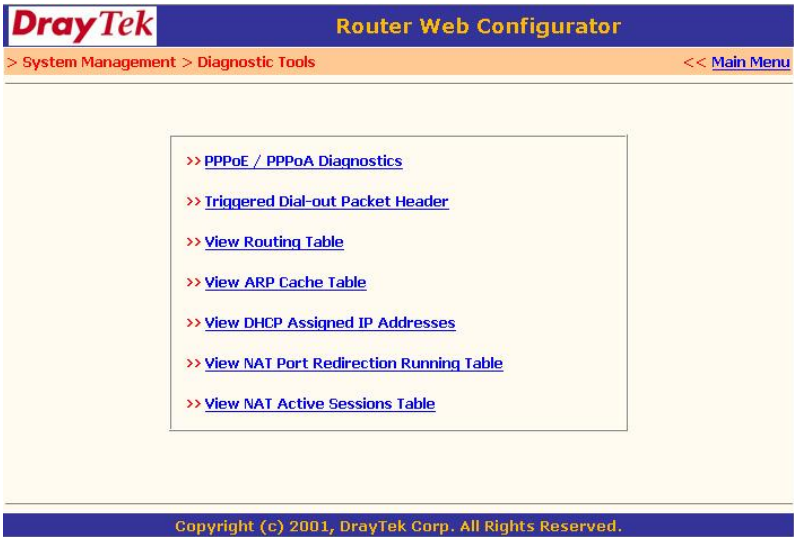
SNMP Setup

The Simple Network Management Protocol (SNMP) is an application layer protocol that communicates message between manager and agent. You can use third-party manager (SNMP utility) to manage the router. The Management Information Base (MIB) is an information store that contains network information. The SNMP agent contains the MIBs that the SNMP manager can get or set. The agent can send trap messages to the manager if the Vigor2200USB has a problem. The SNMP uses the community name for authentication.

Enable SNMP Agent : Check here to enable SNMP Agent
Get Community : Specify the **Get** and **Get-Next** community name. Default value is public.
Set Community : Specify the **Set** community name. Default value is private.
Manger Host IP : Specify the manager. If this field is empty, every host can use SNMP manager to man age.
Trap Community : Specify the **Trap** community name. Default value is public.
Notification Host IP : Specify the recipient of the trap message. If this field is empty, router disable the trap function.
Trap Timeout : Define how often to resend the trap message. If this field is 0, router does not resend trap message.

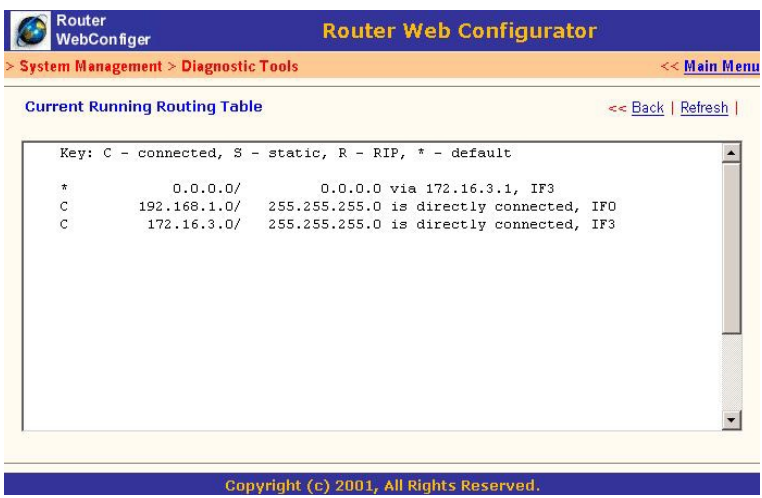
5.4 Diagnostic Tools

Diagnostic Tools provide useful tools for viewing or diagnosing the router. Click "**Diagnostic Tools**" to enter the following page.



View Routing Table:

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



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

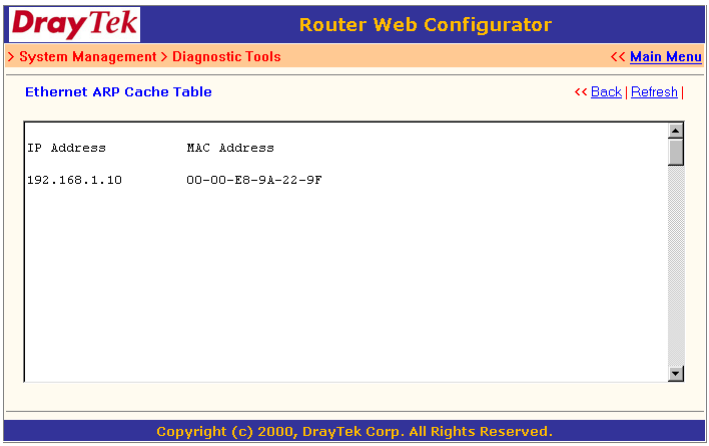
C --- Directly connected.
S --- Static route.
R --- RIP.
***** --- Default route.

To the right of each routing rule you will see an interface identifier:

IF0 --- Local LAN interface.
IF1 --- ISDN B1 channel.
IF2 --- ISDN B2 channel.
IF3 --- WAN(LAN2) interface.

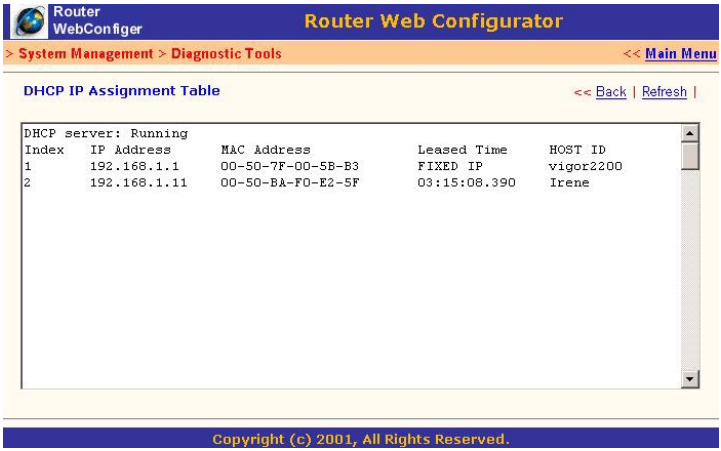
View ARP Cache Table:

Click "**View ARP Cache Table** " to view 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.



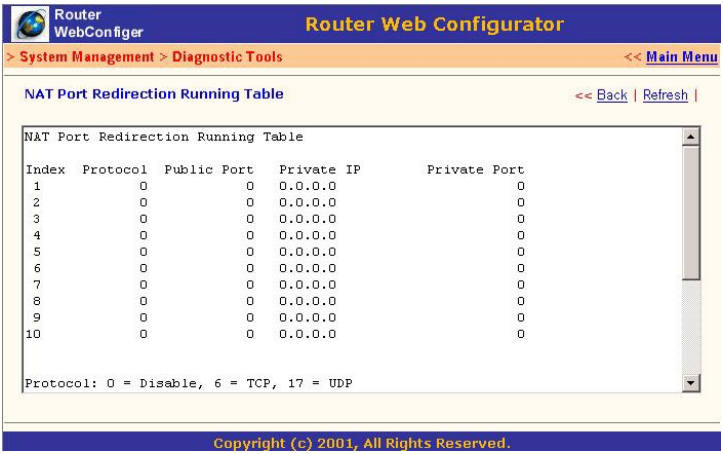
View DHCP Assigned IP Addresses:

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.



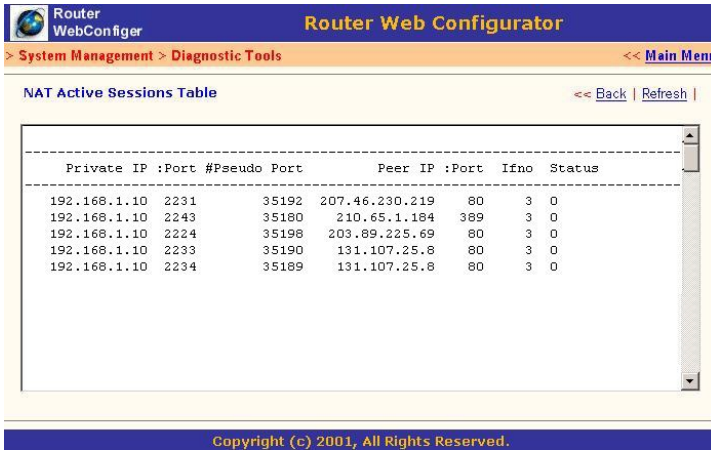
View NAT Port Redirection Running Table:

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



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.



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

Private IP: Port >>

The IP address and port number of internal users (PCs).

#Pseudo Port >>

The public port number.

Peer IP: Port >>

The IP address and port number of peer users (PCs).

Ifno >>

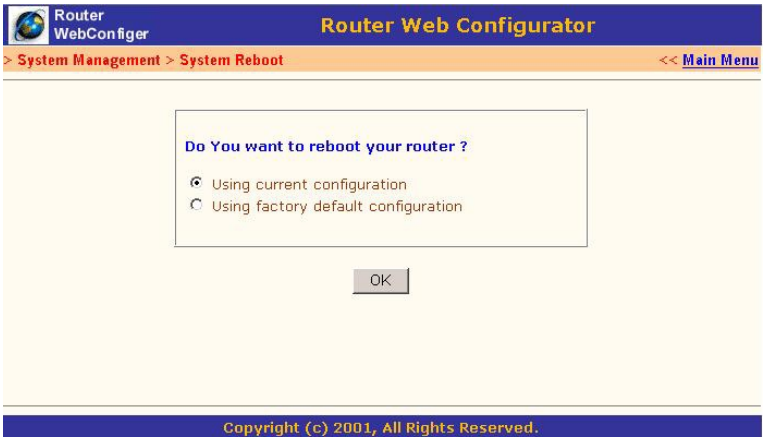
Stands for interface number. The definition is listed below:

0 --- LAN interface.

1 --- WAN(LAN2) interface.

5.5 Reboot System

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



There are two reboot options: **Using current configuration** and **Using factory default configuration**. If you want to reboot the router using current running configurations, 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.

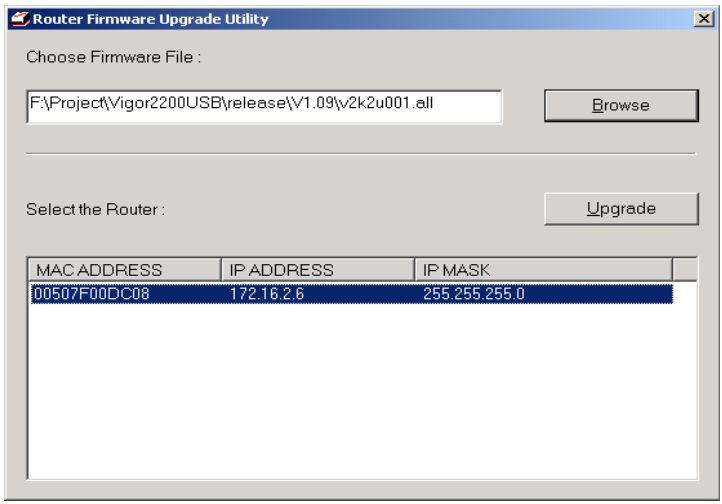
5.6 Firmware Upgrade

Before upgrading your router firmware, you need to install the **Router Tools**. The **Firmware Upgrade Utility** is included in the tools. The following steps will guide you through an upgrade. Note that the examples below use a Windows OS.

1. Download the latest firmware from DrayTek's web site or FTP site.

DrayTek web site : www.draytek.com.tw
(or local DrayTek's web site)
FTP site : ftp.draytek.com

2. Click **"Start > Programs > Router Tools > Router Firmware Upgrade Utility** " to launch the **Firmware Upgrade Utility**.



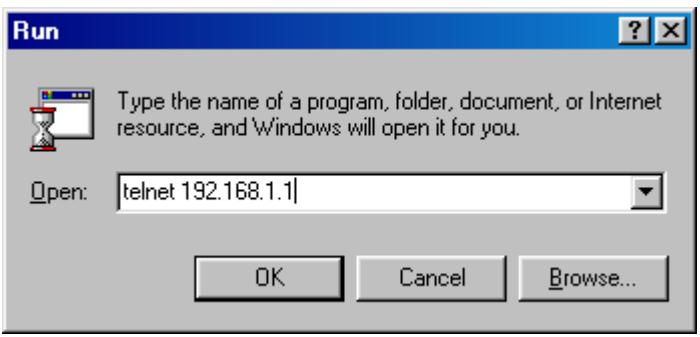
Click the '**Browse'** button to local the new firmware file. The program will search for any Vigor routers on your LAN and display them by IP. Select the 'IP address' of the router to upgrade, then press '**Upgrade**'. Enter the router's password when asked (or press '**OK**' if there is no password).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

6 Troubleshooting & FAQ

The following section explains how to use Telnet terminal commands to diagnose your network problems via the built-in debug tool. Our examples use Windows' Telnet client software. If you are a Mac user, you should install third-party Telnet client software on your computer. By default, Linux has a built-in Telnet client.

6.1 Using the Telnet Terminal Commands

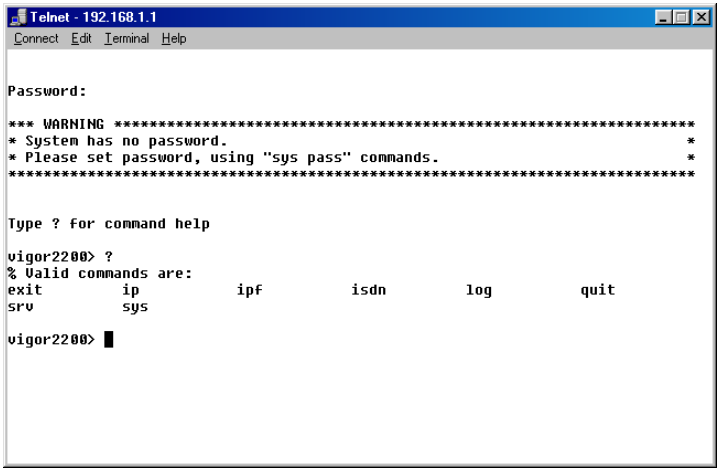
Click "**Start** > **Run** " and type "**Telnet 192.168.1.1**" in the **Open** box as below. Note that the IP address in the example is the router's default address. If you have changed the default, enter the routers current IP address.



Click "**OK** ". The Telnet terminal will open. If an administrator password has not already been assigned, follow the on-screen instructions to assign one.

```
*** WARNING ************************************************************
* System has no password.                                               *
* Please set password, using "sys pass" commands.                       *
************************************************************************
```

After assigning a password, type ?. You will see a list of valid commands.



Command Help:

If you are not familiar with these commands, type the command followed by a question mark ?. For example, the **ip** command is a first level command. Type "ip ?" to get next level commands as shown below.

```
vigor2200> ip ?
% Valid subcommands are:
addr         arp          dhcpc        ping         route        wanaddr

vigor2200>
```

Recall Commands:

The Telnet terminal also provides a method to recall the command history. Use the **Up** and **Down** arrow keys on your keyboard to recall previous commands.

Quitting the Telnet Terminal:

Type "**quit**" or "**exit**" to quit the Telnet terminal.

6.2 Viewing Call Logs

The Call log provides a simple method for troubleshooting call setup or WAN connection problems. By default, the router records WAN connection messages. This information can be helpful in diagnosing WAN connection problems. If you do not understand the content, you can easily save the log and send it to a support technician.

The steps are:

1. Login to the Telnet terminal.
2. Type "**log -F c**" to clear all call logs.
3. Ping to any outside host to trigger the router to dial from your PC.
4. Type "**log -c**" to display the latest call log.

```
vigor2200> log -c
15:04:10.320 >>> Dial-up triggered by user : 192.168.1.18
             proto=icmp, to 168.95.1.1
15:04:10.760 PPP Start (PPPoE)
15:04:13.310 PAP Login OK (PPPoE)
15:04:13.450 IPCP Opening (PPPoE)
             Own IP Address : 168.95.186.16  Peer IP Address : 168.95.186.254
             Primary DNS : 168.95.192.1  Secondary DNS : 168.95.1.1
vigor2200>
```

6.3 Viewing PPP Logs

To view PPP logs, type "**log -p**".

The steps are:

1. Login to the Telnet terminal.
2. Type "**log -F w**" to clear all PPP logs.
3. Ping to any outside host to trigger the router to dial from your PC.
4. Type "**log -p**" to display the latest PPP log. To display all PPP logs, use the "**log -p -t**" command.

```
vigor2200> log -p
16:07:00.000 >>>>B1 Len=27
    Protocol:LCP(c021)
        ConfReq Identifier:0x00
            Protocol Field Compression
            Address/Control Field Compression
            MRRU: 1500
            Short Sequence Number Header Format
            Endpoint Discriminator
                Locally Assigned Address: 00 0f 77 24 00 0f ##

16:07:00.970 >>>>B1 Len=27
    Protocol:LCP(c021)
        ConfReq Identifier:0x01
            Protocol Field Compression
            Address/Control Field Compression
            MRRU: 1500
            Short Sequence Number Header Format
            Endpoint Discriminator
                Locally Assigned Address: 00 0f 77 24 00 0f ##
```

The PPP log is useful in solving communication problems for normal ISDN dialup, or PPPoE and PPTP dialup via a DSL modem.

6.4 FAQs

The following frequently asked questions cover common questions. For more FAQs, visit DrayTek's website (www.draytek.com) or contact your local technical support.

Installing

1. Download Utility shows *Cant Analyze USB modem*:

A: The version of your USB ADSL modem driver is not supported by the download utility. Please contact support@draytek.com.tw for this issue and further support

2. Download Utility shows Version not Supported:

A : Make sure that the drivers for your USB ADSL modem are installed on your PC correctly.

3. USB LED does not light up after connecting the modem:

A: Check that the modem firmware is correctly installed into the Vigor2200USB; from the Vigor2200USB's ISP setup screen, it will show the modem firmware version.

4. DSL LED does not light :

A: Check if the phone line is connected properly and confirm that the line is in working condition by connecting the modem to your PC and testing it.

5. LINK LED does not light when trying to access the Internet:

A: Make sure you have correctly configured your ISPs Username and Password as described in the previous section.

Router

1. What is the default administrator password to login to the router?

A: By default, you don't need a password to login to the router. For security, you should assign a password to pro tect your router against hacker attacks.

2. I forgot the administrator password. What should should I do?

A: Press the **Reset** button on the rear panel for over 5 seconds to reset all settings to default values.

3. What is the default IP address of the router?

A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0.

4. Why does the router dial out very often?

A: Examine the packets that trigger the router to dial out. Login to the Web Configurator and click "**Diagnostic Tools**" > "**Trig gered Dial-out Packet Header**". You will see the triggered packet contents. Report the results to technical support by e-mail or telephone.

5. Why can I connect to the Web Configurator?

A: Remove the proxy server settings in your web browser.

6. Why is it that I can ping to outside hosts, but not access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address set ting. As the router will as sign the DNS settings to the DHCP-client-enabled PC.

7. What is the maximum number of IP addresses that the router DHCP server can assign to local PCs?

A: The built-in DHCP server can support 253 IP addresses for local network usage.

8. What is a DSL Router?

A: The Vigor2200USB router have no built-in DSL mo dem. They must be connected to an external DSL modem for broadband access.

VPN Virtual Private Network and Remote Access

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

Quick Setup

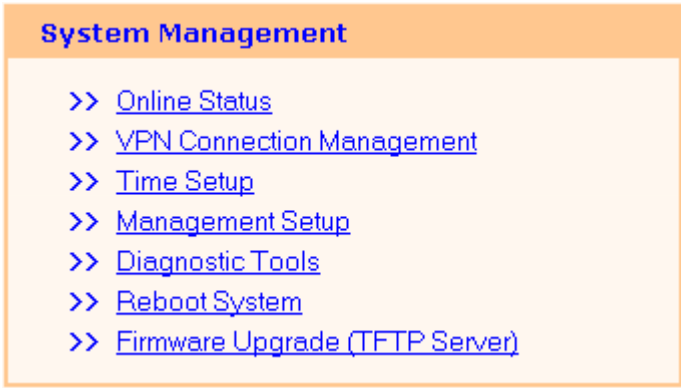
> VPN Remote Dial-In Access Setup

Advanced Setup

> VPN IKE / IPSec Setup
> VPN Remote Dial-In User Setup
> VPN LAN-to-LAN Dialer Profile Setup

System Management

> VPN Commection Management



1. Introduction to VPNs and Remote Access

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 internetwork 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 first, " Remote Dial-In Access " means the router 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 second, "LAN-to-LAN Access " 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.

Virtual private networking (VPN) supports Internet-industry standards technology to provide customers with open interoperable VPN solutions such as Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) as well as Point-to-Point Tunneling Protocol (PPTP).

2. VPN IKE/IPSec Setup

Dial-in Setup

IKE Authentication Method: Currently only supports Pre-Shared Key authentication.

Pre-Shared Key: Specifices a key for IKE authentication.

Re-type Pre-Shared-Key: Confirms pre-shared-key. (Maximum 64 characters)

IPSec Security Method: Selects allowed IPSec security method.

Medium (AH): Data will be authentic, but not be encrypted.

High (ESP): Data will be encrypted and authentic.

Note: If you leave Pre-Shared Key to blank or both Medium and High IPSec Security Method to uncheck. The dial-in IPSec function will be disable. That means router will not respond any incoming IKE negeotiation packet.

Dial-out Setup

IKE Authentication Method: Currently only supports Pre-Shared Key authentication.

Pre-Shared Key: Specifices a key for IKE authentication.

Re-type Pre-Shared-Key: Confirms pre-shared-key.

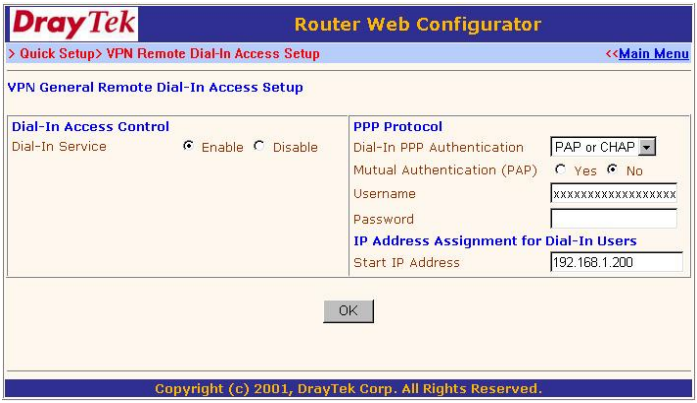
Note: If you leave Pre-Shared Key to blank. The dial-out IPSec function will be disable. Any IPSec related dial-out function(L2TP with IPSec and IPSec Tunnel) will be disable.
(Maximum 64 characters)

3. VPN Remote Dial-In Access

There are 2 types of VPN connection for remote dial-in access. One is PPTP, and the other is L2TP.

3.1 Activating Remote Dial-In

In the Quick Setup group of Setup Main Menu, click "VPN Remote Dial In Access Setup" to enter the setup page.



Dial-In Access Control

Dial-In Service: Check **Enable** to allow VPN dial-in service

PPP Setup

Dial-In PPP Authentication:

PAP: Selecting this option will force the router to authenti cate 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.

Mutual Authentication (PAP): Enable this only if the connecting router requires mutual authentication. By default, the option is set to **No**.

IP Address Assignment for Dial-In Users

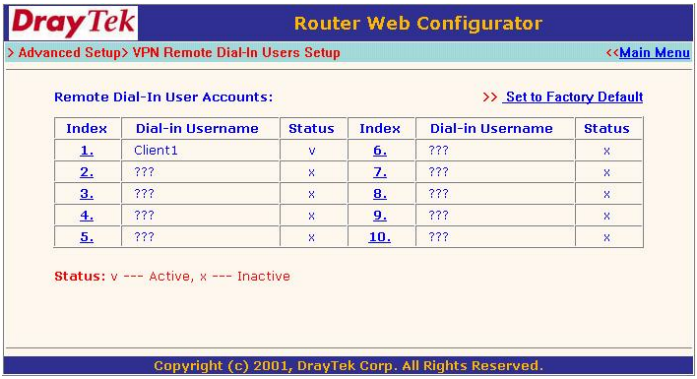
Start IP Address: Enter a start IP address to be assigned to the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 to be the Start IP Address.

Click "OK"

3.2 Creating an Access Account for a Dial-in User

After activating the dial-in capability, you must create an access account for each dial-in user. The router provides 10 access accounts for dial-in users.

> Advanced Setup > VPN Remote Dial-In User Setup



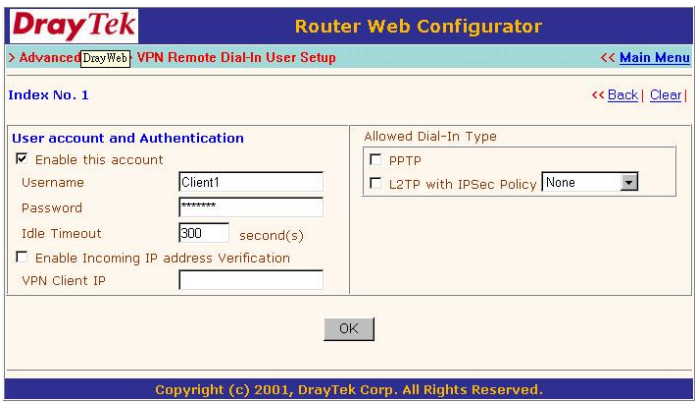
Set to Factory Default: Clicking here will clear all dial-in user accounts.

Index: Click the index number to open an individual setup page for detailed setting of each account.

Dial-In Username: The ??? means the access account is free. If an access account has been configured, the username will be shown.

Status: The symbol v means the account is active, x means inactive.

Click the index number of an account to open an individual setup page for detailed setting.



User Account and Authentication

Check to enable the user account: Check this item to activate the individual user account.

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

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

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

Enable Incoming IP address verification: For extra security, enables the option to allow the dial-in user to call only from a specific IP address.

Allowed Dial-In Type : Select allowed dial-in types.

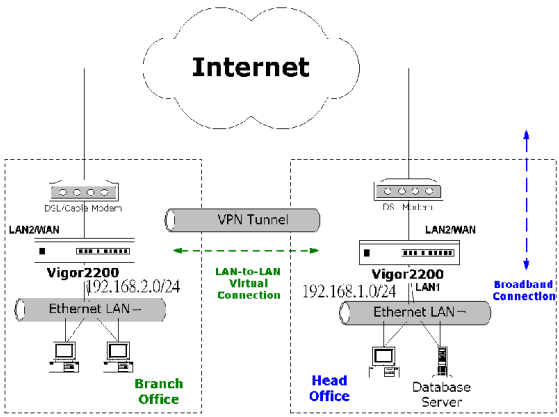
PPTP: Allowed remote dial-in user to make a PPTP VPN connection through the Internet.

L2TP: Allowed remote dial-in user to make a L2TP VPN connection through the Internet. Specifies the IPSec policy to “None”, “Nice to Have”, or “Must”.

4. VPN LAN-to-LAN Access

This section illustrates the following LAN-to-LAN application design.

LAN-to-LAN through the Internet (VPN)



4.1 LAN-to-LAN through the Internet (VPN)

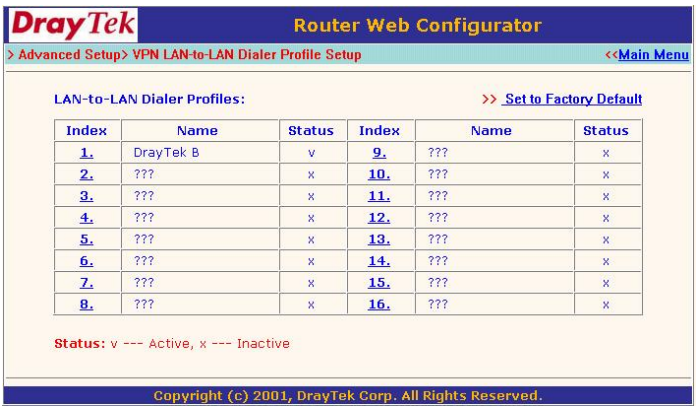
The following sections are based on the network layout above to describe how to set up a LAN-to-LAN profile to connect two private networks through Internet. In the above network layout, the private network 192.168.1.0/24 is located at head office, the network of off-site branch office is 192.168.2.0/24.

Before you begin to setup a LAN-to-LAN profile for each network, you need to gather the information shown in the follow table.

	Head Office	Branch Office
Network ID	192.168.1.0/24	192.168.2.0/24
Router IP address/netmask	192.168.1.1/24	192.168.2.1/24
Access Account	UN : head PW : head	UN : branch PW : branch
VPN Server IP Address	87.65.43.21	123.45.67.89
Type of VPN connection	L2TP over IPSec	L2TP over IPSec
IKE Pre-shared Key	ABC123	ABC 213
IPSec Security Method	AH	AH

4.2 Creating a LAN-to-LAN Dialer Profile

First, you must create a LAN-to-LAN profile for each network. Click **LAN-to-LAN Dialer Profile** on the Setup Main Menu to enter the setup page.



The router provides 16 LAN-to-LAN profiles for connecting to up to 16 different remote networks.

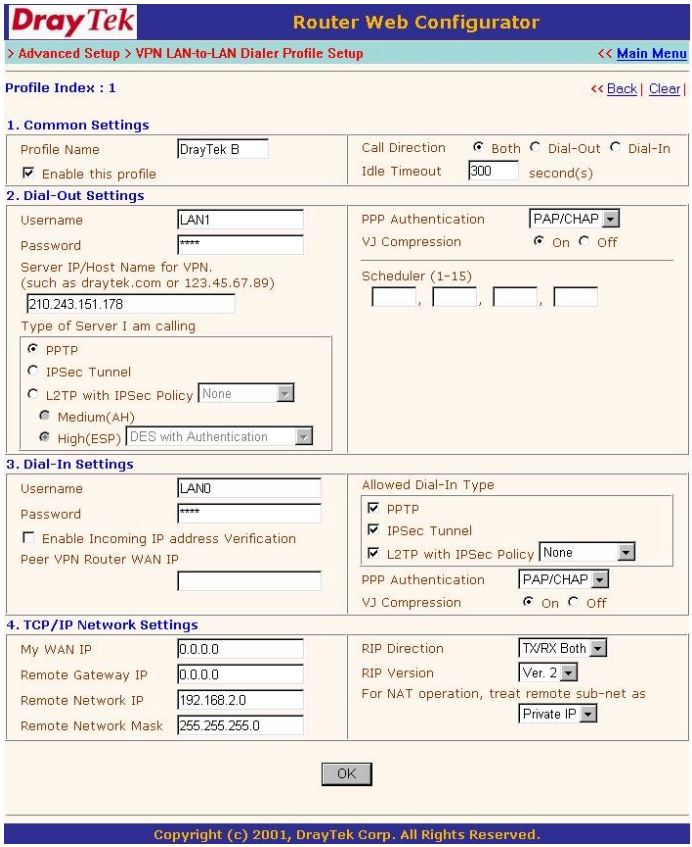
Set to Factory Default: Clicking here will clear all the LAN-to-LAN profiles.

Index: Click a number in the Index to open a detailed settings page for each profile.

Name: Indicates the name of the LAN-to-LAN profile. The symbol ??? means the profile is available.

Status: Indicates the status of the individual profiles. The symbol v means the profile is active, x that it is inactive.

Click an index number to open an individual LAN-to-LAN profile settings page.


DrayTek
Router Web Configurator
> Advanced Setup > VPN LAN-to-LAN Dialer Profile Setup
<< Main Menu
Profile Index : 1
<< Back | Clear |
1. Common Settings
Profile Name
DrayTek B
Enable this profile
Call Direction
Both
Dial-Out
Dial-In
Idle Timeout
300
second(s)
2. Dial-Out Settings
Username
LAN1
Password
****
Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
210.243.151.178
Type of Server I am calling
PPTP
IPSec Tunnel
L2TP with IPSec Policy
None
Medium(AH)
High(ESP)
DES with Authentication
PPP Authentication
PAP/CHAP
VJ Compression
On
Off
Scheduler (1-15)
3. Dial-In Settings
Username
LAN0
Password
****
Enable Incoming IP address Verification
Peer VPN Router WAN IP
Allowed Dial-In Type
PPTP
IPSec Tunnel
L2TP with IPSec Policy
None
PPP Authentication
PAP/CHAP
VJ Compression
On
Off
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
RIP Direction
TX/RX Both
RIP Version
Ver. 2
For NAT operation, treat remote sub-net as
Private IP
OK
Copyright (c) 2001, DrayTek Corp. All Rights Reserved.

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

Common Settings

Profile Name: Specifies a name for the remote network.
Enable this profile: Check here to activate this profile.
Call Direction: Specifies 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.
Idle Timeout: By default, set to 300 seconds. If the profiles connection is idle for over the limit set by the timer, the router will drop the connection.

Dial-Out Settings

Username: Specifies a username for authentication by the remote router.
Password: Specifies a password for authentication by the remote router.
Server IP/Host Name for VPN: Specifies the destination VPN server IP or Host Name for dialup.
Type of Server I am calling: Indicates the dial-out VPN type.
PPTP: Specifies the dial-out VPN connection is PPTP.
IPSec Tunnel: Specifies the dial-out VPN connection is IPSec Tunnel.
L2TP: Specifies the dial-out VPN connection is L2TP.

L2TP with IPSec Policy: Specifies IPSec policy for L2TP.

None: Does not apply IPSec.
Nice to Have: Applies IPSec first. If fails, tries without IPSec again.
Must: Species L2TP over IPSec.

If IPSec Tunnel or L2TP with IPSec Policy set to Nice to Have or Must, select security methods as described in followings. Please refers to section 4.2 to set up IKE pre-shared key.

Medium(AH): Specifies the IPSec protocol is the Authentication Header protocol. The data will be authentic, but will not be encrypted.

High(ESP): Specifies the IPSec protocol is the Encapsulating Security Payload protocol. The data will be encrypted.

DES without Authentication: Uses DES encryption algorithm and does not applies any authentication.

DES with Authentication: Uses DES encryption algorithm and applies MD5 or SHA-1 authentication algorithm.

3DES without Authentication: Uses triple DES encryption algorithm and does not applies any authentication.

3DES with Authentication: Uses triple DES encryption algorithm and applies MD5 or SHA-1 authentication algorithm.

PPP Authentication: Specifies the PPP authentication method for PPTP and L2TP. Normally set to PAP/CHAP for the widest compatibility.

VJ Compression: VJ Compression means TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.

Dial-In Settings

Username: Specifies a username to authenticate the dial-in router.
Password: Specifies a password to authenticate the dial-in router.
Enable Incoming IP address verification: Limits the dial-in VPN router to calling from a specific IP address.
Peer VPN Router WAN IP: If it is enabled, enter the remote VPN server IP address in this field.
Allowed Dial-In Type: indicates the allowed dia-in connection type.
PPTP: Check to allow PPTP dial-in connection.
IPSec Tunnel: Check to allow IPSec tunnel dial-in connection.
L2TP: Check to allow L2TP dial-in connection.
L2TP with IPSec Policy: Specifies IPSec policy for L2TP.
None: Does not apply IPSec.
Nice to Have: Applies IPSec first. If fails, tries without IPSec again.

Must: Species L2TP over IPSec.

If IPSec Tunnel or L2TP with IPSec Policy set to Nice to Have or Must, select security methods as described in followings. Please refers to section 4.2 to set up IKE pre-shared key and IPSec security method.

PPP Authentication: Refer to Dial-Out Settings.

TCP/IP Network Settings

The following settings are required for proper LAN-to-LAN operation.
My WAN IP: (can use default) In most cases you may accept the default value 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, specify the fixed IP address here.

Remote Gateway IP: (can use default) Specify the IP address of the remote router.
In most cases you may accept the default value 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, specify the fixed IP address here.

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

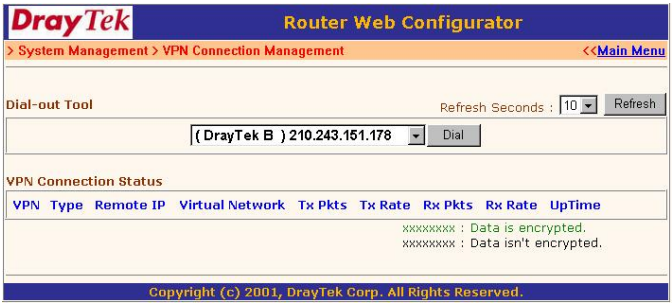
Remote Network Mask: (Must specify) Specify the netmask of the remote network.

RIP Direction: The option specifies the direction of RIP (Routing Information Protocol) packets through the ISDN WAN connection.

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

For NAT operation, treat remote sub-net as: The router has two local IP networks: the1st subnet and 2nd subnet. Here you set which subnet will be used as local network for VPN connection and exchange RIP packets with the remote network. Usually set to "1st subnet " for routing between the 1st subnet and the remote network.

5. VPN Connection Management



You can use "VPN Connection Management " to make VPN connection and monitor the VPN connection status.

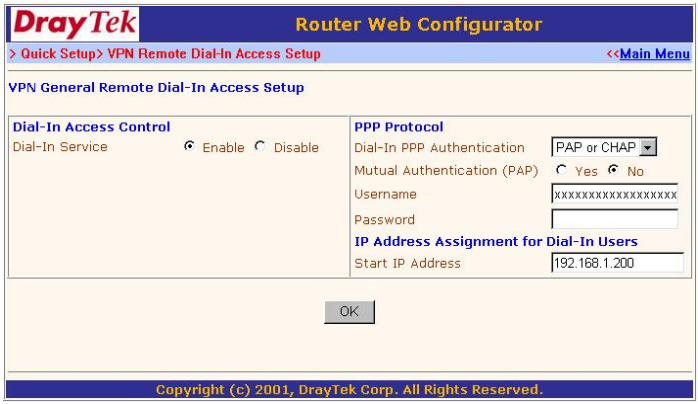
6. Example

A. Accept VPN Dial-Iin

Step 1. > Quick Setup > VPN Remote Dial-In Access Setup

Enable Dial-In Service

If peer side needs mutual authentication, specify the username/password, otherwise, keep it blank.

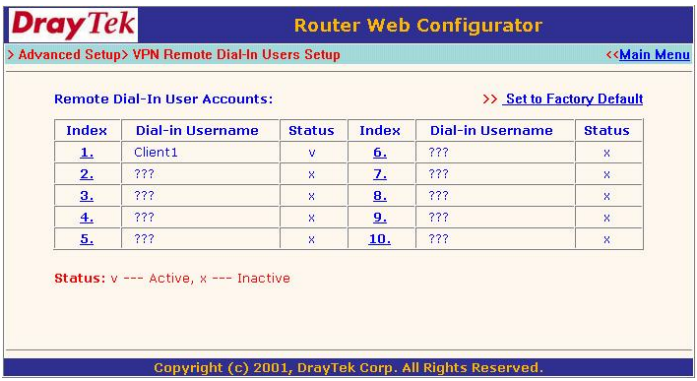


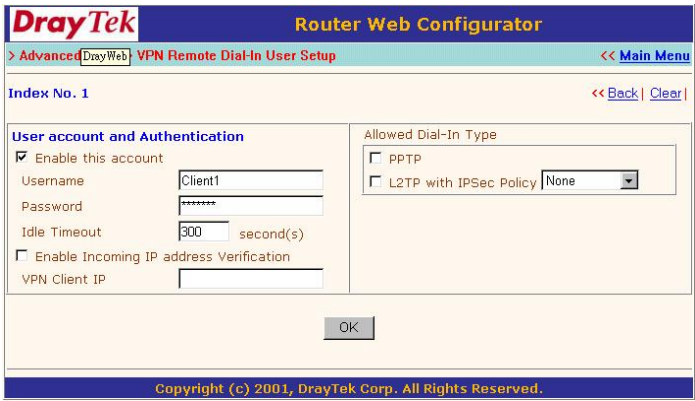
Step 2. > Advanced Setup > VPN IKE/IPSec Setup

Set Pre-Shared key, this key is same as peer side used.

For Client access-

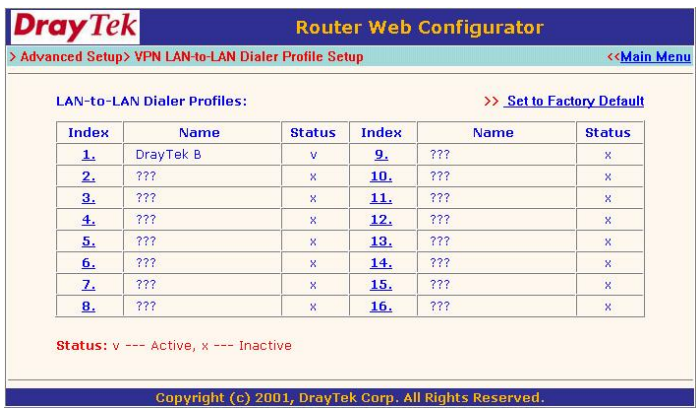
Step 3a. > Advanced Setup > VPN Remote Dial-In Users Setup
Establish a remote dial-in user account





For LAN-to-LAN access-

Step 3b. > Advanced Setup > VPN LAN-to-LAN
Dialer profile Setup
Establish a LAN-to-LAN Dialer Profiles



"Common Settings "
- Enable this profile and give a profile name
- Select "call Direction "' to "Both "' or "Dial-In "

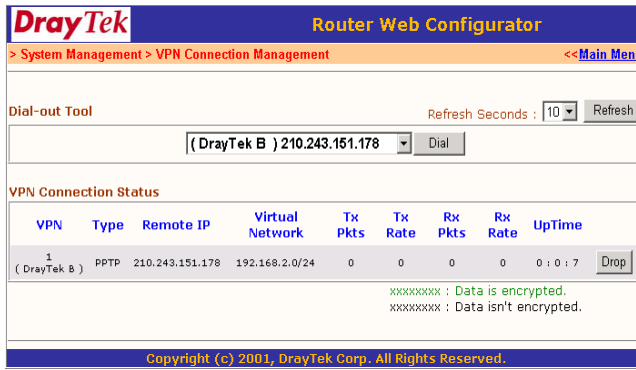
"Dial-In Settings "
- Specify username / password
- Select "Dial-In Type "

"TCP/IP Network Settings "
- You can leave "My WAN IP "' & "Remote Gateway IP " as default
- Set "Remote Network IP"' & "Remote Network Mask"

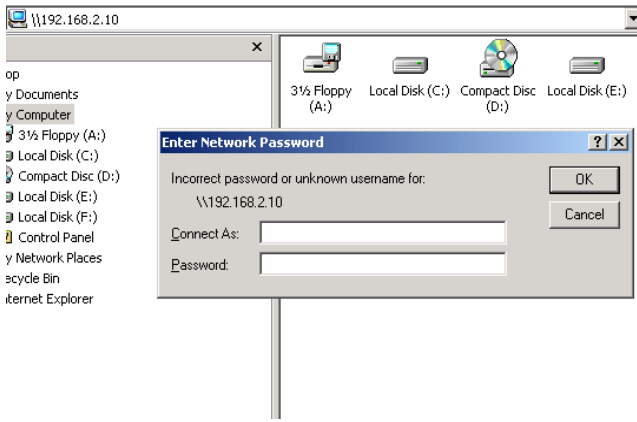
Now you can accept VPN dial in.

Note: If you have used any personal firewall on PC, for example,"Zone Alarm", you need to disable it while using VPN.

After connecing, you can monitor the VPN connection in formate via "> System Management > VPN connection Mangement ".



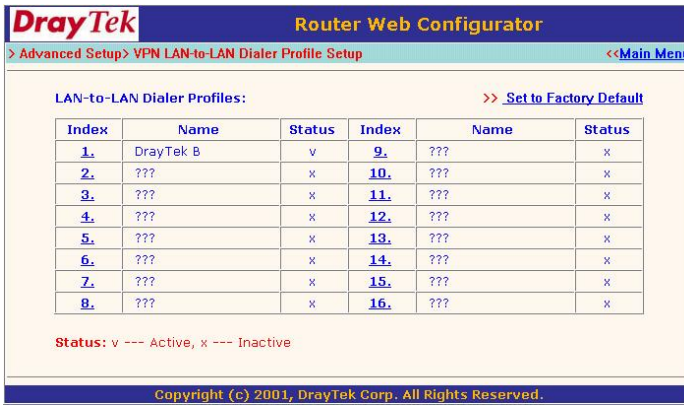
Via Explore, you can access files of 'remote' LAN PC.



B. Make VPN Connection

Step 1. > Advanced Setup > VPN IKE/IPSec Setup
Set Pre-Shared key, this key is same as peer side used.

Step 2. > Advanced Setup > VPN LAN-to-LAN Dialer profile Setup
Establish a LAN-to-LAN Dialer Profiles



"Common Setting "

- Enable this profile and give a profile name
- Select "Call Direction " to "Both" or "Dial-Out "

"Dial-Out Settings "

- Specify username / password and server IP address
- Select the protocol type : PPTP, IPSec or L2TP

"TCP/IP Network Settings "

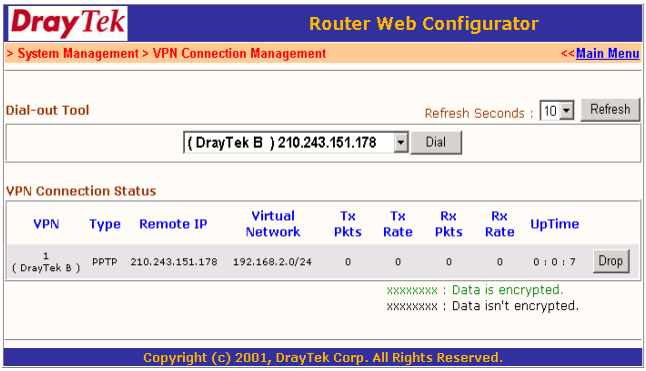
- You can leave "My WAN IP " & "Remote Gateway IP " as default
- Set "Remote Network IP "' & "Remote Network Mask "

Step 3. > System Management > VPN Connection Management

Select profile and press dial

Note: If you have used any personal firewall on PC, for example,"Zone Alarm", you need to disable it while using VPN.

After connecing, you can monitor the VPN connection in formate via ">> System Management > VPN connection Mangement ".



Via Explore, you can access files of "remote" LAN PC.