Table of Contents

0

Preface

0.1 About This Manual

This manual is designed to assist users in using the DrayTek Vigor2000 Router. 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 support@draytek.com.tw . For latest product info and features, visit our website at www.draytek.com.tw.

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. Please visit the following website: http://www.draytek.com.tw/registration.htm. 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

! Please read the installation guide thoroughly before you set up the router.

! The router can be used only with a BRI (Basic Rate Interface) ISDN line.

! The router is a complicated electronic unit that may be repaired only by authorized and qualified personnel. Do not try to open or repair the router yourself.

! Do not place the router in a damp or humid place, e.g. a bathroom.

! The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.

! Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

! Keep the packaging out of reach of children.

! When you want to dispose the router, please follow local regulations on conservation of the environment.

0.6 Warranty

We warrant to the original end user (purchaser) that the Vigor2000 Routers 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, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equiva-

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

The warranty does not cover the bundled or licensed software of other vendors. Defects that 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 hereby without obligation to notify any person of such revision or changes.

0.7 European Community Declarations

The Vigor2000 Routers have been approved for connection to the Public Switched Telecommunication Network using interfaces compatible with ITU-TSS recommendation I.430 (Basic Rate ISDN user access). The Vigor2000 Routers comply with the R&TTE Directive 99/5/EC.

1 Getting Started

1.1 Introduction

The Vigor2000 Router provides multiple users with efficient and reliable access over a single ISDN BRI, IDSL (U Interface), DSL line, or Cable Modem (not support Dynamic IP) service to the Internet and corporate LAN for using E-mail, sharing documents, Web surfing, file transfers, etc. Moreover, the provision of a built-in six-port 10BaseT Ethernet hub and one Uplink port may give cost-effective workgroup connectivity over Ethernet.

In addition to improving the productivity of employee, flexible telecommuting access, and affordable management cost, Vigor2000 Router accommodates room for business growth from 6-7 computers to more. The smart solution of DrayTek Vigor2000 Route provides SOHO users an `easy to setup and use`, `instant internet and intranet connection`, `high interoperablility`, and `good security` for network management.

The broadband access protocol supports PPPoE, PPTP, and Static IP. These protocols comply with worldwide Ethernet-based DSL/Cable Modem standards.

For traditional ISDN users, the Vigor2000 Router features a built-in Virtual TA (Remote CAPI) server which operates as a CAPI-based ISDN TA for LAN users. To run FAX transmission or data transfer services, users need to install a Virtual TA client driver on the PCs and use third-party CAPI-based software .

Vigor2000 Router provides seamless migration from ISDN to a broadband connection for multiple SOHO users and easy usage of ISDN for backup-dial and/or remote access while concurrently using the DSL/Cable modem connection.

PPPoE / PPTP allows users on the LAN interface to setup a dial-on-demand DSL connection sharing the same IP account, and paying for only ONE connection. The idle-timeout function prevents wasted connection charges by shutting down the connection when it is idle. No PPPoE / PPTP client software is required for the computers. Hassle free!

1.2 Unpacking Your Vigor2000 Router

Your Vigor2000 Router package should contain items listed below. If any item is missing or damaged, contact your dealer or DrayTek Customer Service Department immediately.

- One User manual with warranty/registration card
- One CD-ROM, including User Manual in electronic form, latest released firmware, and utilities
- One RJ-45 ISDN telephone cable (black)
- One AC/AC power adapter (black)
- One Console cable (gray)
- One RJ45 to RS232 (9 pin) converter for console cable
- One Ethernet LAN cable (blue) for connection to a computer or hub

Dimensions (cm) of Vigor2000 Router

21.8 (L) x 15.8 (W) x 3.6 (H)

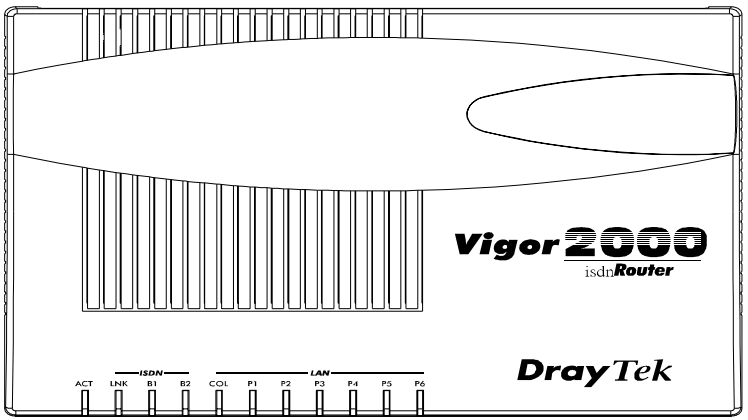
Weight: 399 grams

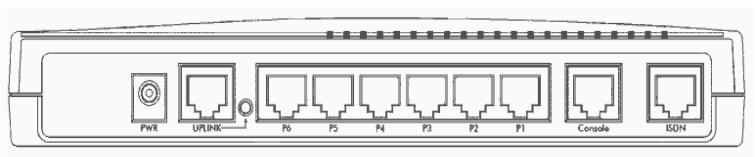
Maximum Power: 10W

Power Adapter: AC adapter; Class2 transformer; input is 230VAC 50Hz; minimum output is from 15 to 17V AC 600mA

1.3 Front Panel & Rear Panel Descriptions

Vigor2000 Router:





Front Panel Description -- LED Indicators
There are eleven LEDs on the front panel, including ACT, LNK,B1, B2, COL, and P1 ~ P6.

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

ISDN Group:

> **Note:**
>
> On some NT1 boxes, the LNK LED will go OFF when the ISDN line has been idle for a while. When the router is dialing or answering a call, it should be ON again.

LNK (Link)
ON when the connected network card or hub has linked up.
Blinking when the Ethernet packets pass through the interface.

B1
ON when there is successful remote connection on the ISDN BRI B1 channel.

B2
ON when there is successful remote connection on the ISDN BRI B2 channel.

LAN Group:

Col (Collision)
BLINK when there is collision of packets within the Ethernet.

P1 ~ P6

- ON when the computer is connected and has no packet transmission going.
- BLINK when packets are sending/receiving through hub or connected computer.

Rear Panel Description
The Vigor2000 has a power jack, an uplink port, six RJ-45 ports, a console port, and an ISDN port on the rear panel:

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

UPLINK (back panel)
Use attached 10BaseT LAN cable to connect to another hub. The light besides the port will be ON when the router is connected to another hub.

LAN - P1, P2, P3, P4, P5, P6
These switch ports should be connected to your local PCs.

CONSOLE
Connects to the computer you want to use to configure Vigor2000 Router.

ISDN (Varied by Router Model)

- For S/T Interface Router Model: Connects to a NT1 box provided by your ISDN service provider.

- For U Interface Router Model: If your ISDN service provider does not provide the NT1 box or your ISP provides IDSL connection, use this model for connection.

1.4 Key Features

The Vigor2000 Router 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 **Internet Explorer** or **Netscapes** browser etc, to configure the Vigor2000 Router as easily as surfing web sites.

4. **Virtual TA Server (VTA)**: The terminology Virtual TA means the Vigor2000 can operate as traditional ISDN TA to transmit and receive data, FAX, and voice transmissions via third-party software running on a desktop computer. In fact, a virtual TA server works as a network TA to exchange packets between an ISDN BRI and an Ethernet LAN. Therefore, desktop computers can use the ISDN line resource via an Ethernet LAN. In short, multiple users can share a network TA for backward compatibility with traditional applications, such as BBS, file transfer, sending/receiving FAXs etc.

5. **Remote Access Server (RAS)**: RAS provides remote dial-in access services for home workers, branch offices, or telecommuters. Vigor2000 Routers offer 10 dial-in user profiles, including an authentication mechanism through CHAP/PAP and Calling Line Identification (CLID), secure callback functions, and 16 Lan-to-Lan Dialer Profiles, etc.

6. **Routing Information Protocol (RIP) Support**: Used in most

LAN-to-LAN applications. The RIP protocol exchanges routing information between routers.

7. **Domain Name Server (DNS) Proxy**: The DNS proxy maintains a DNS cache, including a mapping table between 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 router, the proxy searches its local DNS cache. If matched, the router sends an answer to the host that sent the DNS query packet. Only unmatched DNS queries require querying a WAN Domain Name Server.

8. **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.

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

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

11. **ISDN Digital Subscriber Line (IDSL) Client Support**: If your ISP provides ISDL connection, you can use the router to connect at 64/128k bps (U Interface Leased Line Type only).

12. **Point-to-Point over Ethernet (PPPoE) Client Support**: If you are a DSL user, the router 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.

13. **Point-to-Ponit Tunnelling Protocol (PPTP) Client Support**: Some DSL modems (e.g. Alcatel modems) only provide a PPTP local connection for an end user computer. The Vigor2000 Routers have a

built-in PPTP client for establishing a DSL link transport protocol for your entire local network. There is no need to install a PPTP driver on your computers.

14. **Firewall**: In addition to the built-in NAT mechanism, the Vigor2000 Routers feature another powerful firewall to protect your local network, or to deny specified local users access to unauthorized network services.

15. **Bandwidth-on-Demand (BOD) for ISDN Interface**: As the ISDN BRI interface has two independent B channels, the BOD mechanism allows you to automatically add/drop a B channel according to data traffic throughput.

16. **Remote Management**: The system manager can remotely manage the routers through an ISDN remote dial-in, ISDN, or DSL WAN interface.

2 Installation & Setup

2.1 Before You Begin

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

2. Know the type of interface provided by your ISP or telecom. The standard model only supports the ISDN BRI S/T-interface. If you are an ISDN U-interface user, you need to order a U-interface model. If you are an ISDN S/T-interface user, you should have an NT-1 or NT-1 plus provided by your ISP or telecom. Also, make sure the ISDN line is available.

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

4. Locate the device in a clean location. Do not block the ventilating slots on the rear panel.

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

6. If you use S/T-interface, do not extend the ISDN line greater than 100 meters from the NT-1 (NT-1 plus) box and the router.

7. If you use DSL/Cable, check that your subscribed DSL/Cable modem supports the Ethernet interface for connecting to your PC. If not, you will be unable to connect it to the router.

8. Before you set up the router, you need to know the default settings of Vigor2000 Router as shown below:-

Factory Default Settings:

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

DNS Server IP Address

- Primary IP Address: empty
- Secondary IP Address: empty

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 allowed

Virtual TA Server: Enabled

Remote Dial-In Server: Disable

IP Address Assignment for Dial-In User: 192.168.1.200

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 PCs:

1. Attach the Ethernet cable (blue color cable) to any P1 ~ P6 port.

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

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

4. Attach the Console cable to Console port.

5. Connect the other end of the Console cable to the Management PC (p6~p23) you want to use to configure the Vigor2000 Router.

> **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:

1. Attach the Ethernet cable (blue color cable) to the **Uplink** port.

2. Connect the other end of the Ethernet cable to the external

Ethernet hub or switch.

3. The LED indicators on both the Uplink 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, or create a handmade cable.

2.2.3 Connecting to an ISDN BRI Line

A. S/T-Interface Model

1. Locate the ISDN cable (black color cable).

2. Plug one of the RJ-45 connectors on the cable into the ISDN port on the rear panel of the router.

3. Plug the other end of the cable into any of the NT-1 (or NT1 plus) S/T-interface ports.

B. U-Interface Model

1. Locate the ISDN cable (black color cable).

2. Plug one of the RJ-45 connectors on the cable into the ISDN port on the rear panel of the router.

3. Plug the other end of the cable into the ISDN wall outlet.

2.2.4 Connecting to a DSL/Cable Modem

The router supports connection of a DSL modem via an Ethernet interface only. Non-Ethernet interface DSL modems, such as USB and ATMF-25, will not be supported.

1. Attach the Ethernet cable to the Ethernet port of the DSL/Cable

modem.

2. Plug the other end of the cable into the **P1 ~ P6** port.

3. If the Pn (the port that be plugged) LED is not bright, please change the direct cable to cross cable.

The hardware installation is now complete. The following sections will guide you through setting up your management PC and connecting to the Web Configurator.

> Note:
>
> The Web Configurator is a management utility that handles all configuration and provides web-based management.

2.3 Setting Up a Management PC

The Vigor2000 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.

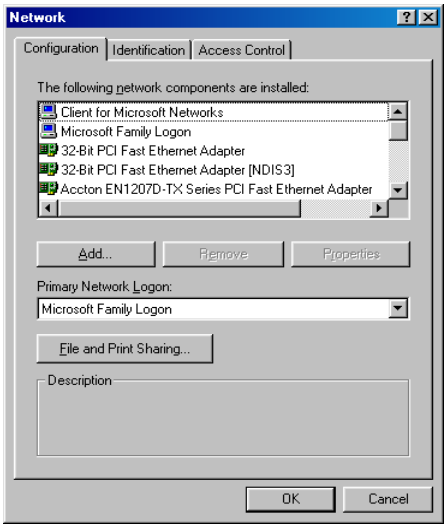
For the dynamic IP address, you need to set the PC as a DHCP client, and then restart or renew the network settings. The DHCP server implanted in the router is enabled by default so the PC will then be assigned an IP address and related settings by the router.

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 may differ from the screen shown here. Check if you have an Ethernet Network Interface card (NIC) installed. If not, refer to the installation documentation from the NIC card manufacturer and install the card and drivers.

If your have installed the NIC card,

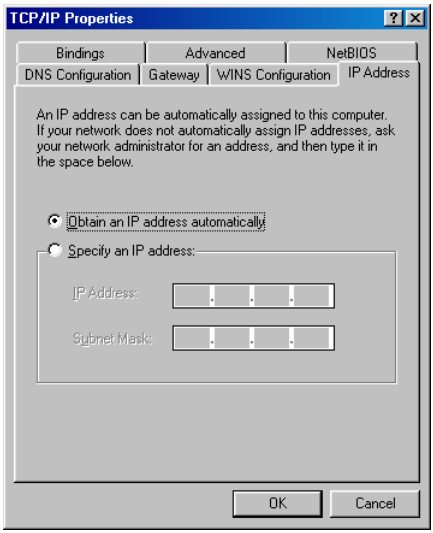
1. Click the **"Add"** button. The "**Select Network Component Type**" dialog box will open. This box has four options: *Client, Adapter, Protocol, Service.*

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 on the right, and click **"OK"**. It will return to the Network dialog box.

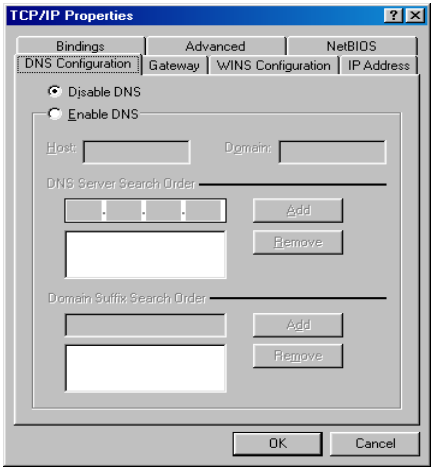
2.3.2 Configuring the TCP/IP Protocol

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

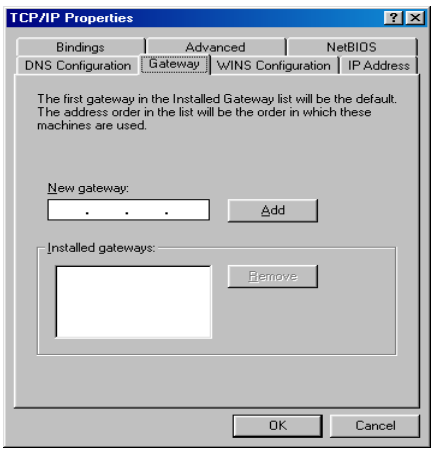


2. On the IP Address tab, click "**Obtain an IP address automatically**". As the DHCP (Dynamic Host Configuration Protocol) server built into the router is enabled by default, your computer will get an IP address, subnet mask, and other related IP network settings from the router.

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



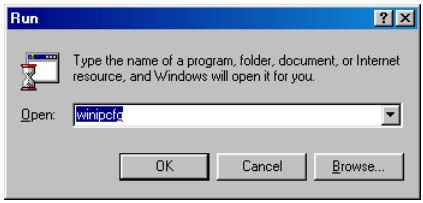
4. Click the "**Gateway**" tab.

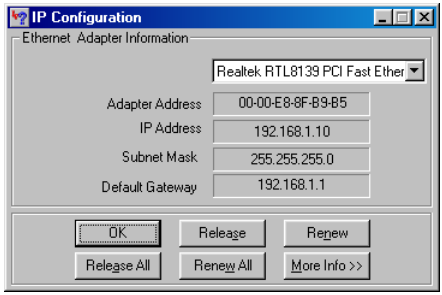


5. Make the "**New gateway**" and "**Installed gateways**" fields blank and click "**OK**". A dialog box will pop up asking you to restart the PC. Click "**Yes**".

2.3.3 Checking TCP/IP Settings

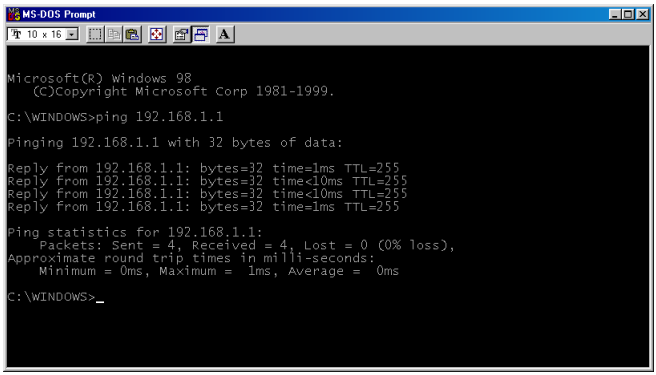
1. After completing the previous steps, click "**Start**" -> "**Run**". Click the "**Gateway**" tab and type **winipcfg**. The **IP Configuration** window will open. If the PC does not show an IP address in the **192.168.1.2** to **192.168.1.254** range, click the "**Release**" button to release the 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 in Microsoft Windows to ping the router. Click "**Start**" -> "**Programs**" -> "**MS-DOS Prompt**". A command mode window will open. Type **ping 192.168.1.1** (default IP of the router) to diagnose 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 to the Web Configurator or Telnet Terminal (command-line based management). Also, if the network you currently installed 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, Netscape Communicator, etc.) or telnet client software, you may jump directly to the next section. 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 auto-run CD will display the main menu.

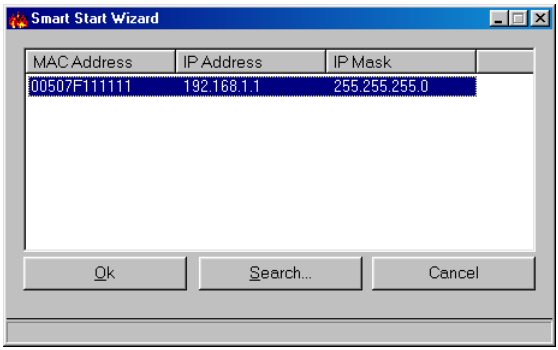
> **Note:**
>
> If auto-run fails to start the installation program, click autostart.exe on the root directory of the CD to start the program.

2. Click "**Router Tools**" for install. The Router Tools utilities include **Firmware Upgrade Utility**, **Smart Start Wizard,** and **Uninstall Router Tools.**

Using the Wizard

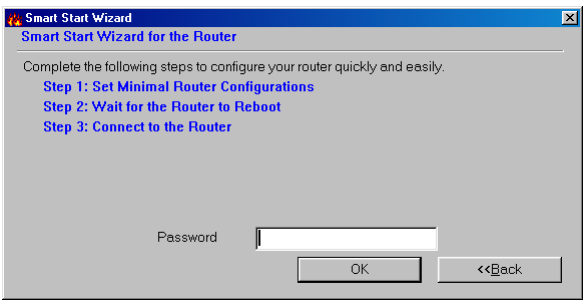
1. Click "**Start**" > "**Programs**" > "**Router Tools**" > "**Smart Start Wizard**". (see below)

The following screen will open.

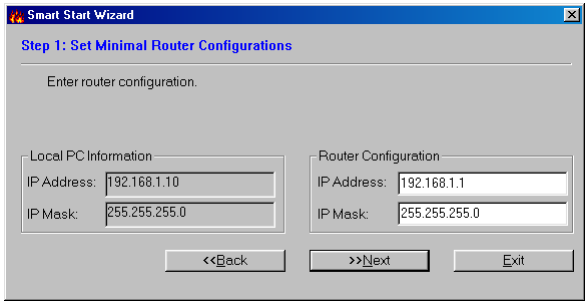


2. Click "**Search**" to find the router on your network.

3. Click "**OK**" to go to the login password screen.

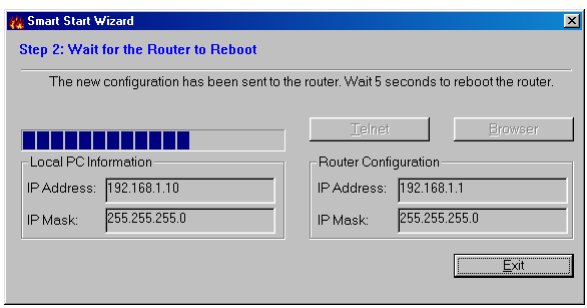


4. If this is the first time you setup the router, do not enter any password. Click **"OK"** to go to the next screen.

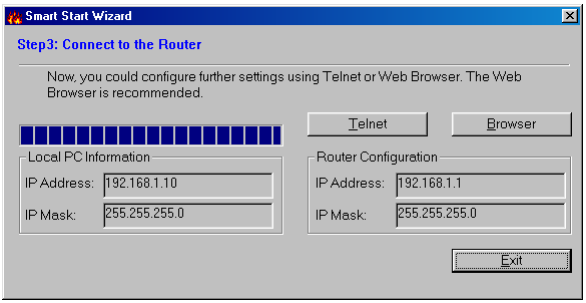


The screen shows read-only IP and IP mask settings for the PC you are using, and also the **IP Address** and **IP Mask** settings for the router. Here you may change the settings of the router to match your current network environment, or keep the default settings.

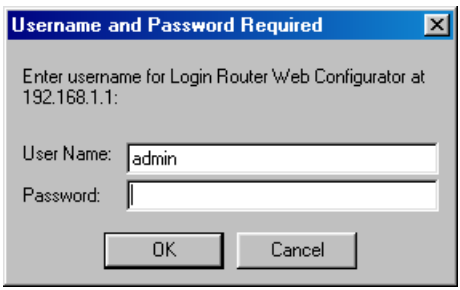
5. Click "**Next**" to update the settings of the router.



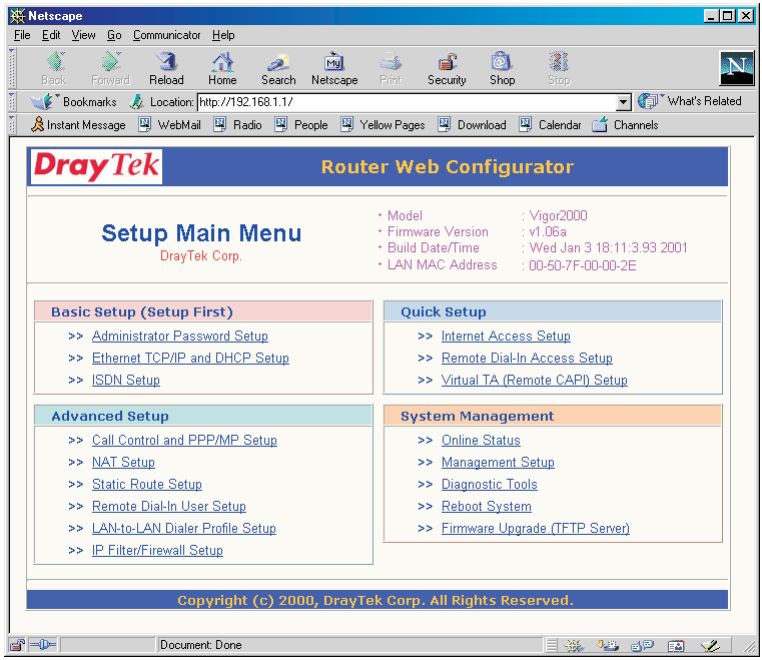
6. Wait for a few seconds. The "**Telnet**" and the "**Browser**" will be clear (see below).



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



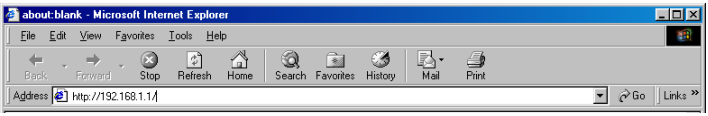
Enter **admin** as the User Name and leave the Password field blank. The Web Configurator will open. In the following examples we use the Netscape™ web browser.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.1.1/ What's Related
Instant Message WebMail Radio People Yellow Pages Download Calendar Channels
DrayTek
Router Web Configurator
Setup Main Menu
DrayTek Corp.
• Model : Vigor2000
• Firmware Version : v1.06a
• Build Date/Time : Wed Jan 3 18:11:3.93 2001
• LAN MAC Address : 00-50-7F-00-00-2E
Basic Setup (Setup First)
>> Administrator Password Setup
>> Ethernet TCP/IP and DHCP Setup
>> ISDN Setup
Quick Setup
>> Internet Access Setup
>> Remote Dial-In Access Setup
>> Virtual TA (Remote CAPI) Setup
Advanced Setup
>> Call Control and PPP/MP Setup
>> NAT Setup
>> Static Route Setup
>> Remote Dial-In User Setup
>> LAN-to-LAN Dialer Profile Setup
>> IP Filter/Firewall Setup
System Management
>> Online Status
>> Management Setup
>> Diagnostic Tools
>> Reboot System
>> Firmware Upgrade (TFTP Server)
Copyright (c) 2000, DrayTek Corp. All Rights Reserved.
Document: Done

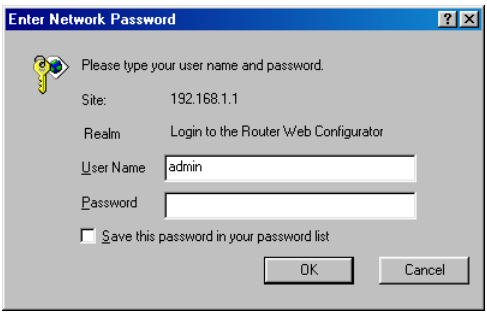
2.5 Using the Web Configurator

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.

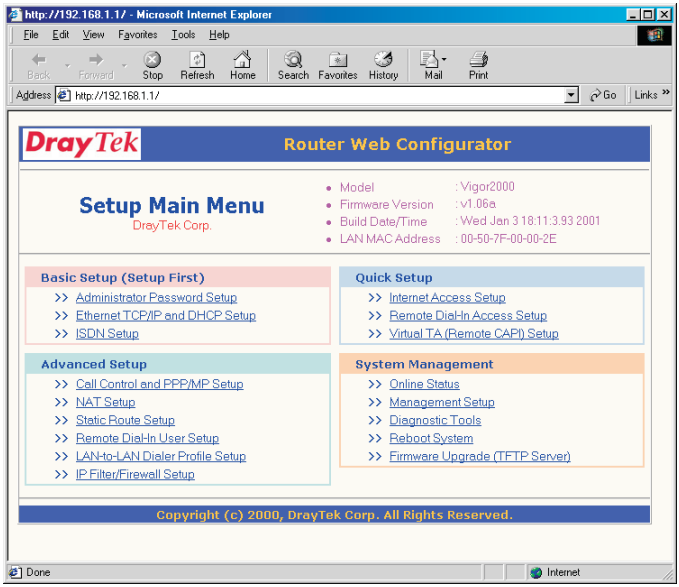


2. An authentication dialog box will open.



3. If this is the first time you setup 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 will describe the outline for each configuration menu.

Basic Setup (Setup First):

1. Administrator Password Setup:

   Sets/changes the administrator password.

2. Ethernet TCP/IP and DHCP Setup:

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

3. ISDN Setup:

ISDN users need to select a country code. Sets some ISDN numbering settings, e.g. MSN numbers and Own (Calling) numbers.

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.

2. Remote Dial-In Access Setup:

Remote access or LAN-to-LAN remote access settings are made here.

3. Virtual TA (Remote CAPI) Setup:

Use this menu to create a Virtual TA user account and enable/disable the built-in Virtual TA server.

Advanced Setup:

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

1. Call Control and PPP/MP Setup

Sets bandwidth-on-demand (BOD) parameters for the MP (Multiple link PPP) protocol. Also, some call control parameters may be set here.

2. NAT (Network Address Translation) Setup

Sets NAT configurations, such as Port Redirection, etc.

3. Static Route Setup

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

4. Remote Dial-in User Setup

This menu supports 10 remote dial-in account for remote access applications. You can manage these dial-in accounts under the setup menu.

5. LAN-to-LAN Dialer Profile Setup

The LAN-to-LAN Dialer Profiles are different from last setup menu. Here up to 16 LAN to LAN profiles can be set for access to up to 16 remote networks via an ISDN line. These profiles have dial-out/dial-in/static route functions.

6. 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 the current online status and statistics of the system.

2. Management Setup

Here allow you to grand 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 to diagnose 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 Setup & Internet Access

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).

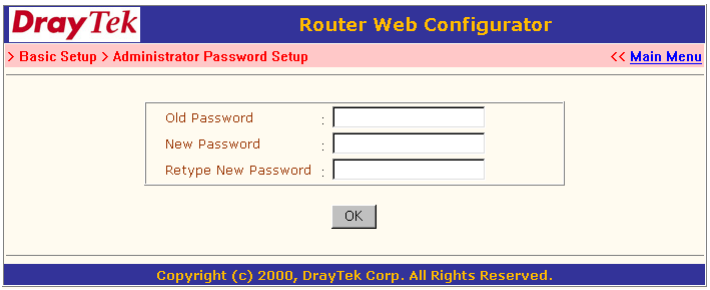
3.1 Basic Setup (Setup First)

This group includes **Administrator Password Setup**, **Ethernet TCP/IP and DHCP Setup,** and **ISDN Setup**.

3.1.1 Changing the Administrator Password

On first setup the router requires no password. However, for security reasons, we strongly recommend that you set an administrator password for the router. If you do not set a password for the router, any user can access the setting of the router and make changes randomly from local network or the Internet.

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



Old Password:

If this is the first time you enter this menu, leave this field blank.

New Password:

Enter an administrator password.

Retype New Password:

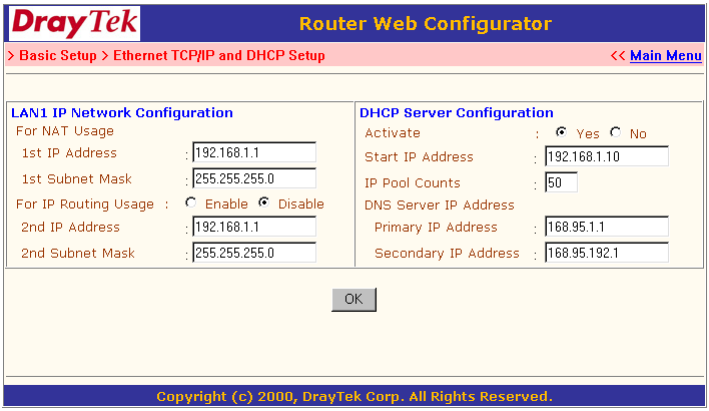
Type the password again to confirm.

3.1.2 Configuring Ethernet TCP/IP Address and DHCP Server

Vigor2000 Router has six Ethernet ports for connecting to the local Ethernet network and external broadband device (i.e. DSL modem/ router or Cable modem).

There are two sets of IP address settings for the Ethernet. The 1st IP address/netmask is for private users or NAT users, and the 2nd IP address/netmask is for public users or pure router (not NAT) user. To allow access of public users you need to subscribe a globally reachable subnet from your ISP.

For example, for some ISDN dial-up access, the ISP will assign a few public IP addresses for your local network usage. You could use one IP address for your router; the 2nd IP address/netmask should be configured using the public IP address. Other local PCs should set the router IP address as the default gateway. When the ISDN connection to the ISP has been established, each local PC will directly route to the Internet. Also, you could use the 1st IP address/netmask to connect to other private users (PCs). These user's IP addresses will be translated to the 2nd IP address by the router and sent out via ISDN.



Router 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: Enable the 2nd IP address settings.

Disable: Disable the 2nd IP address settings.

2nd IP Address: Set a public IP address.

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

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: Enable the DHCP server.

No: Disable the DHCP server.

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

IP Pool Counts: Set 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. They may also have a human-friendly and easy-to-remember name such as www.yahoo.com. The DNS server converts this name into its equivalent IP address.

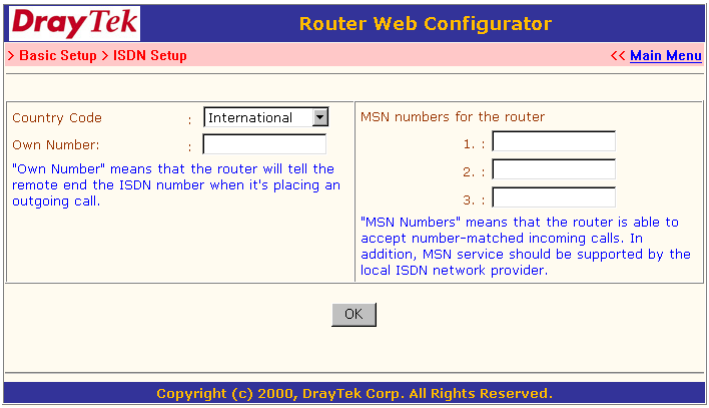
Primary IP Address: Set the IP address of the primary DNS server.

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

Note:

If you leave both Primary IP and Secondary IP Address fields 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. ISDN or DSL/Cable) connection.

3.1.3 Configuring the ISDN Interface



Country Code:

Set the correct country code for proper function on your local ISDN network.

Own Number:

Set your ISDN number. The number you entered in this field will be carried with every outgoing call to the users you called.

MSN Numbers for the Router:

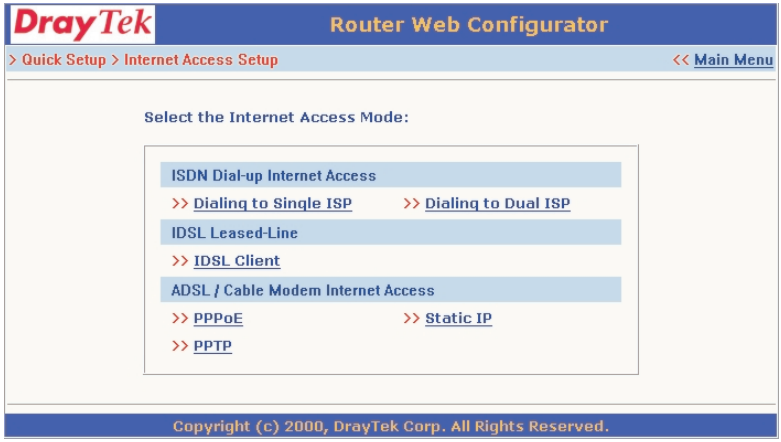
"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, local ISDN network provider shoud support MSN service. The router provides three MSN number fields. Note that MSN services must be subscribed from your local telecom.

By default, MSN function is disabled (i.e. leave the MSN number fields blank) under which all incoming calls will be accepted without number matching.

Click **OK** to return to the **Main Setup Menu**.

3.2 Internet Access Setup

For most users, Internet access is the primary application. The following sections will explain more details of ISDN dial-up access and broadband access setup. When you click "**Internet Access Setup**" within the **Quick Setup** group, the following setup page will be shown.



Six methods are available for Internet Access.

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

Dialing to Dual ISP: If you have more than one ISP, click here to set up two ISP dialup profiles. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs who do not support Multiple link PPP (ML-PPP). In such cases dialing to two ISPs can increase the bandwidth utilization of the ISDN line to 128kbps data speed.

IDSL Client (For U Interface Model Only): If you are an IDSL subscriber, you must use U Interface Vigor2000 Router for direct connection. If the model you have is S/T Interface, you will not be able to use IDSL for Internet access.

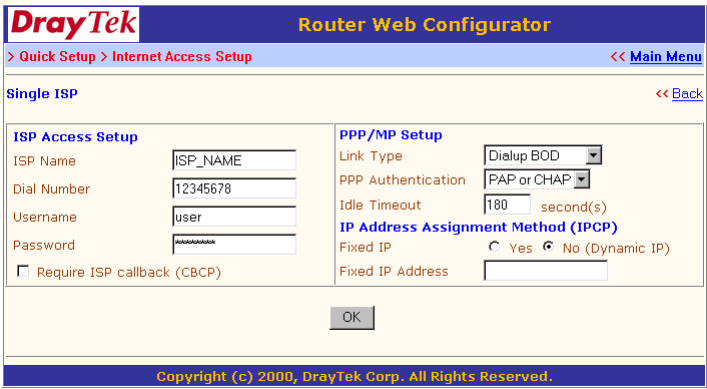
PPPoE: This is for most DSL modem users. All local users can share one PPPoE connection to access the Internet.

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

Static IP: If you have obtained public IP address from DSL, Leased-Line or Cable (static IP only) service provider, select Static IP to setup your Internet Access mode.

3.3 ISDN Dial-up Internet Access

3.3.1 Connecting to a Single ISP



ISP Access Setup

ISP Name: Enter your ISP name.

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

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Require ISP Callback (CBCP): If your ISP supports the callback function, check **"Require ISP Callback (CBCP)"** to enable the Callback Control Protocol during PPP negotiations.

PPP/MP Setup

Link type: There are four link types

- Link Disable

  Disable the ISDN dial-out function.

- Dialup 64Kbps

  Use one ISDN B channel for Internet access.

- Dialup 128Kbps

  Use both ISDN B channels for Internet access.

- Dialup BOD

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

PPP Authentication: two types of authentication

- PAP Only

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

- PAP or CHAP

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

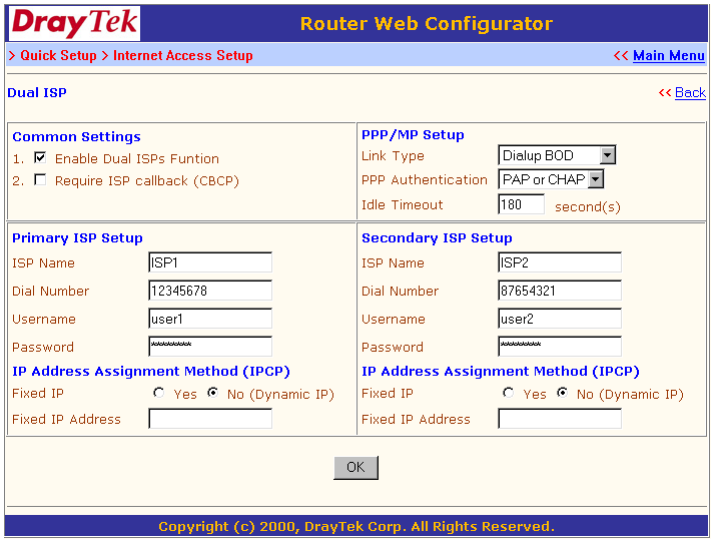
Idle Timeout: Idle timeout means the router will disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection will remain always connected to the ISP.

IP Address Assignment Method (IPCP)

Fixed IP and Fixed IP Address:

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

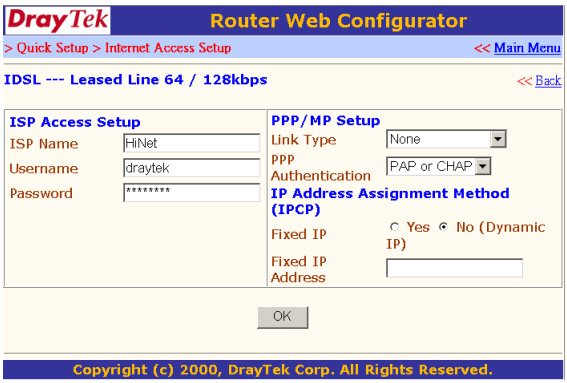
3.3.2 Connecting to Dual ISPs



Most configuration parameters are the same as last section. This page provides an "**Enable Dual ISPs Function**" check box and adds a secondary ISP Setup section. Check the box and enter the second ISP information.

3.4 IDSL Leased - Line

IDSL Client



ISP Access Setup

ISP Name: Enter the Internet Service Provider Name.

Username: Enter the username obtained from your ISP provider.

Password: Enter the password obtained from your ISP provider.

PPP/MP Setup

Link Type: you have three selections

- Link Disable

  Disable the IDSL link.

- Leased 64Kbps

  Use one B channel for Internet access.

- Leased 128Kbps

Use both B channels for Internet access.

PPP Authentication: two types of authentication

- PAP Only

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

- PAP or CHAP

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

IP Address Assignment Method (ICPC)

Fixed IP and Fixed IP Address:

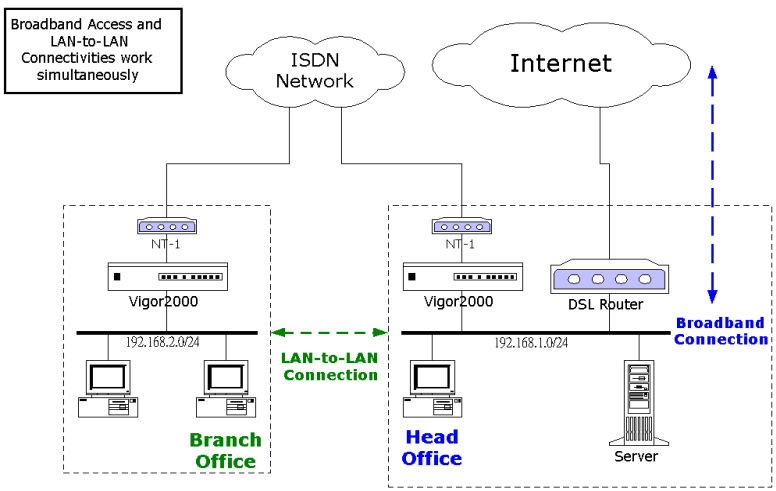
In most environments you should not change the default settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **"Yes"** and enter the assigned IP address in the Fixed IP Address field.

3.5 DSL/Cable Modem Internet Access

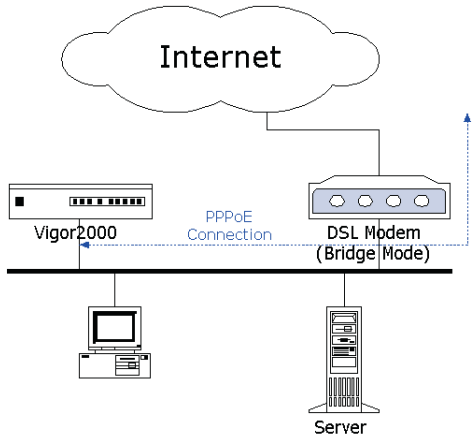
Before you connect a broadband access device, e.g. a DSL/Cable modem, to the router, you need to know what kind of Internet access is provided by your ISP.

The following paragraphs deal with three widely used broadband access services. These are **PPPoE Client, PPTP Client,** and **Static IP** for DSL/Cable Modem. In most cases, you will get a DSL/Cable modem from the broadband access service provider. The router is connected behind the broadband device and works as a NAT or IP router for broadband and ISDN connections.

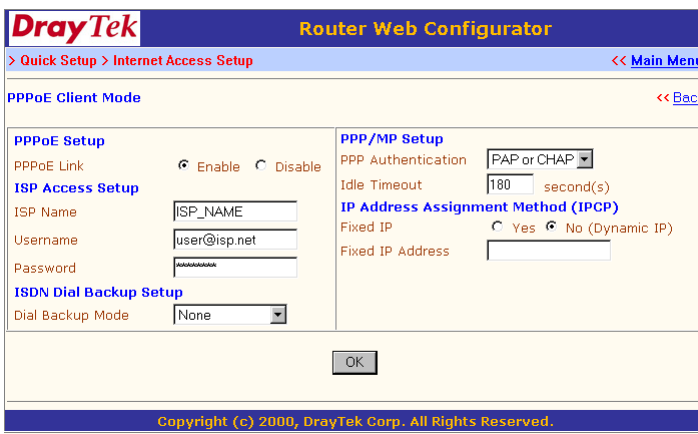
In addition to broadband access capabilities, the **ISDN** port can do dial backup, or provide remote access and remote management functions to support more flexible network connectivity. The following application scenario shows that the head office is capable of getting on to the Internet through the Vigor2000 and a broadband device and connecting to the branch office via an ISDN network simultaneously.



3.5.1 Using PPPoE with a DSL Modem



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



PPPoE Setup

PPPoE Link: Check "**Enable**" to enable the PPPoE client protocol.

ISP Access Setup

ISP Name: Enter the ISP name.

Username: Enter the ISP supplied username.

Password: Enter the ISP supplied password.

ISDN Dial Backup Setup

Dial Backup Mode: Select "**None**" to disable this feature or select "**Packet Trigger**" to activate this feature (refer to 3.5.4).

PPP/MP Setup

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

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

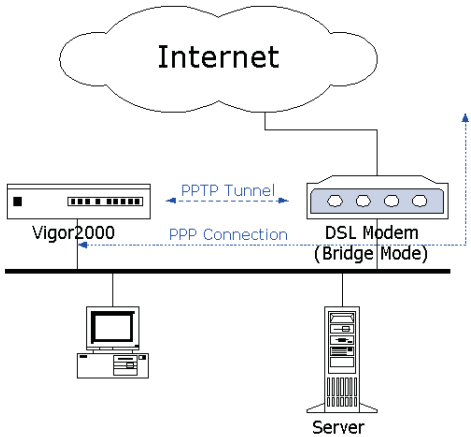
Fixed IP: Check "**No (Dynamic IP)**" unless your ISP has provided you with a static IP address.

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

ISDN Dial Backup Setup

Dial Backup Mode: Select "**None**" to disable this feature or select "**Packet Trigger**" to activate this feature (refer to 3.5.4).

3.5.2 Using PPTP with a DSL Modem



PPTP Setup

PPTP Link: Check "**Enable**" to enable a PPTP client to establish a tunnel to a DSL/Cable modem.

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

Click "**Internet Access Setup**" -> **"PPTP"** to enter the setup page. The following setup page is just for example. Your DSL/Cable service provide should provide the exact settings.

ISP Access Setup

ISP Name: Enter the ISP name.

Username: Enter the ISP supplied username.

Password: Enter the ISP supplied password.

ISDN Dial Backup Setup

Dial Backup Mode: Select "**None**" to disable this feature or select "**Packet Trigger**" to activate this feature (refer to 3.5.4).

PPP Setup

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

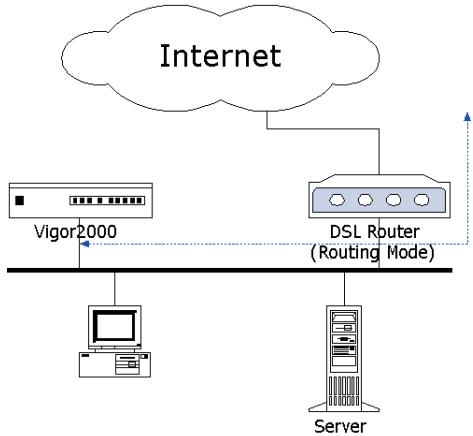
Idle Timeout: Idle timeout means the router will disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the PPP session will not terminate itself.

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

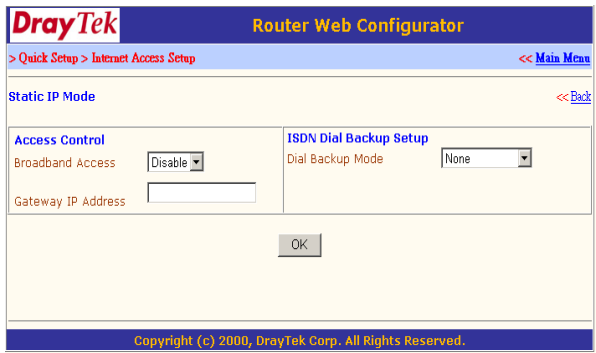
Fixed IP Address: If your ISP has provided you with a static IP address enter it here.

3.5.3 Using a Static IP with a DSL/Cable Modem

Select this access mode if you receive a fixed public IP address or a public subnet from your DSL or Cable ISP. In most cases, a Cable ISP will provide a fixed public IP, while a DSL ISP will provide a public subnet. You must enable IP Routing Usage, and enter the fixed public IP or choose one public IP from the public subnet for Ethernet TCP/IP Setup (refer to 3.1.2).



Click "**Internet Access Setup**" -> "**Static IP**" to enter the setup page.



Access Control

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

Gateway IP Address: Enter the IP address from DSL service provider as Router IP address or the fixed IP gateway IP address.

ISDN Dial Backup Setup

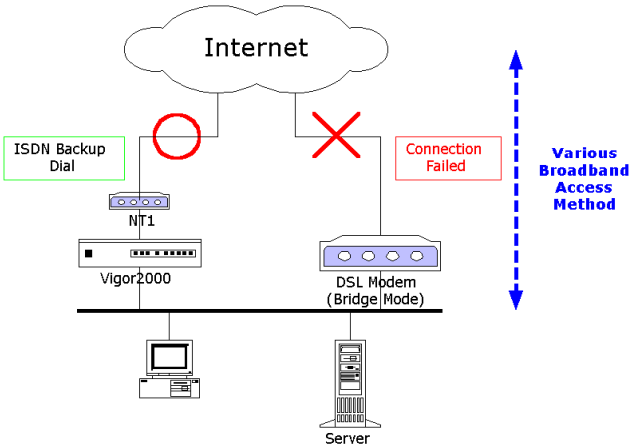
Dial Backup Mode: Select "**None**" to disable this feature or select "**Packet Trigger**" to activate this feature (refer to 3.5.4).

Note:

The router should be restarted to allow the settings to take effect.

3.5.4 Configuring ISDN Dial Backup

ISDN Dial Backup Setup



Dial Backup Mode:

None: Disable the backup function.

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

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

To start ISDN Dial Backup function, you must create a dial backup profile. Click "**Internet Access Setup**" -> "**Dialing to a Single ISP**" to setup the backup profile. Refer to section 3.3.1 for details.

4 Remote Access

This chapter explains the capabilities of remote access of the Vigor2000 Router. Use the following setup links on the Setup Main Menu to setup remote access functions.

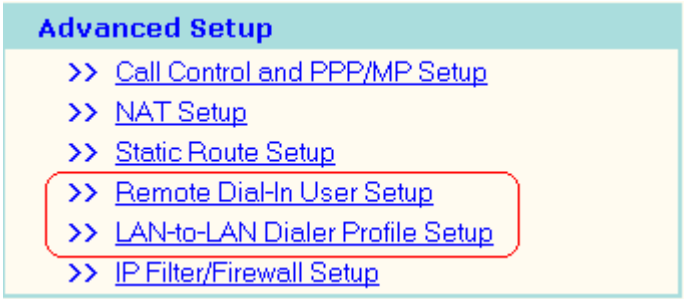
Quick Setup

> Remote Dial-In Access Setup

Advanced Setup

> Remote Dial-In User Setup

> LAN-to-LAN Dialer Profile Setup



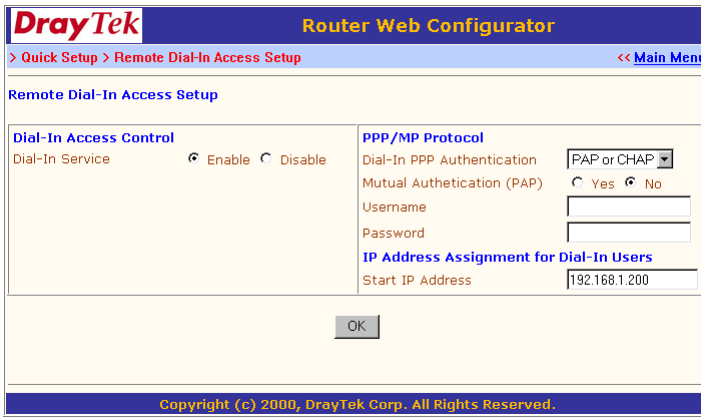
4.1 Introduction to Remote Access

Here the term "Remote Access" covers two types of remote access. The first, "Remote Dial-In Access" means the router allows normal ISDN TA users or NAT routers (IP sharing routers) to dial into the router for sharing the network resources of the local network, or to surf the Internet via a broadband device. The other remote access function, "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.

4.2 Remote Dial-In Access

4.2.1 Activating Remote Dial-In

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



Dial-In Access Control

Dial-In Service: Check "**Enable**" to allow dial-in service. Note that if you check "**Disable**", the router will not accept any incoming ISDN calls.

PPP/MP Setup

Dial-In PPP Authentication:

PAP: Selecting this option will force the router to authenticate dial-in users with the PAP protocol.

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

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 can choose 192.168.1.200 to be the Start IP Address.

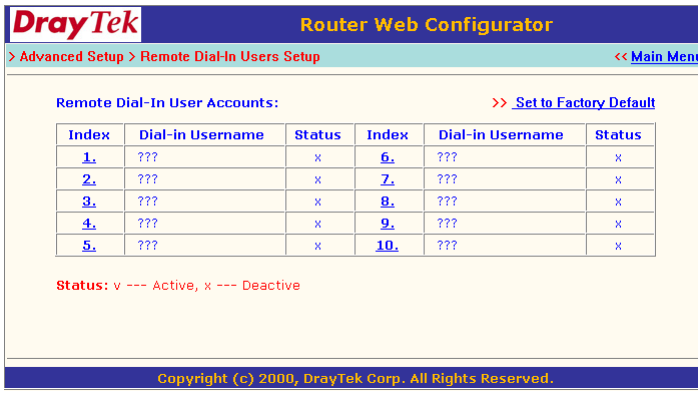
Because one ISDN BRI has two independent data channels (B-channels), it is possible to allow two dial-in users at the same time. The first dial-in user would be assigned the start IP address and the second would be assigned the start IP address plus 1.

Click "**OK**"

4.2.2 Creating an Access Account for a Dial-in User

After activating the dial-in capability, you must create an access ac-

count for each dial-in user. From the Advanced Setup menu, click "**Remote Dial-In User Setup**" to open the page shown below. The router provides 10 access accounts for dial-in users.



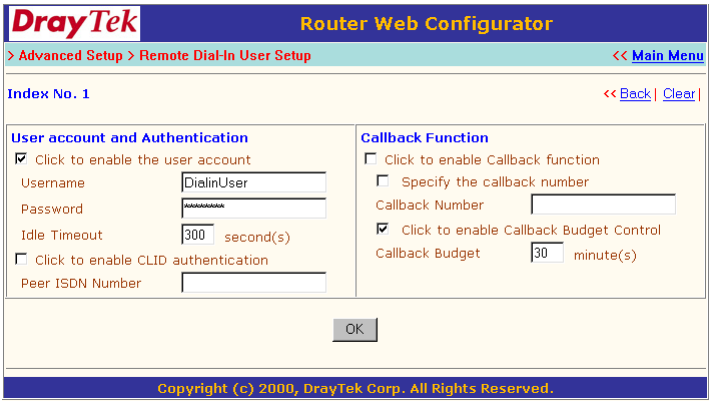
Set to Factory Default: Clicking here will clear all dial-in user accounts.

Index: Click one of the index numbers to open an individual setup page and enter the detail setting for each account.

Dial-In Username: The **"???"** means the access account has not set up yet. 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 detail setting.



User Account and Authentication

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

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

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

Idle Timeout: Default setting is 300 seconds. When a dial-in connection has been idled longer than the time limit, the router will drop the connection.

Click to enable CLID authentication: For extra security, enables the option to allow the dial-in user to call only from a specific number. CLID stands for Calling Line Identification.

Peer ISDN Number: If CLID authentication has been enabled, enter the dial-in user's ISDN number.

Callback Function

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

Click to enable the Callback function: Enable the callback function.

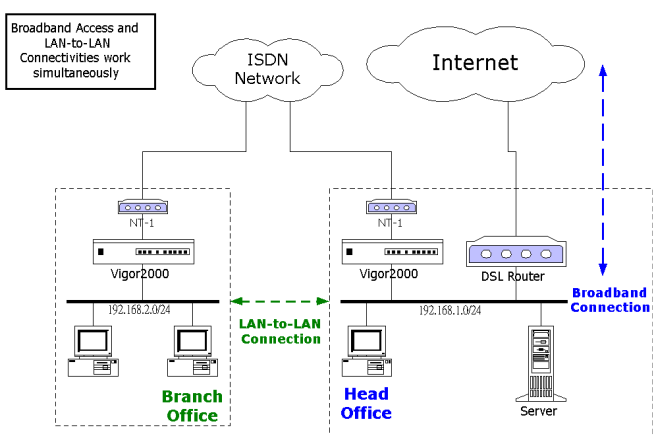
Specify the callback number: The option is for extra security. Once enabled, the router will only call back to the specified ISDN number defined in the next parameter, Callback Number.

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

Click to enable Callback Budget Control: Enable the callback budget control.

Callback Budget (Unit: minutes): By default, the callback function has a 30-minutes time restriction. The budget will be decreased automatically per callback connection. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.

4.3 LAN-to-LAN Access



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. In the above network layout, the private network of the head office is 192.168.1.0/24 and the off-site branch office network is 192.168.2.0/24.

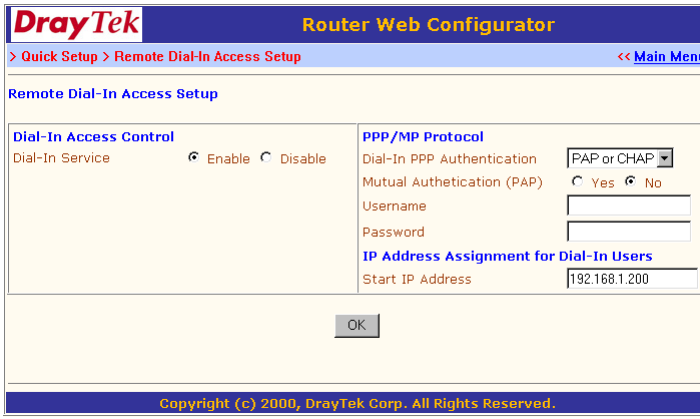
Before you begin to setup a LAN-to-LAN profile for each network, you should gather the information shown in the following table.

	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
Assigned IP for dial-in connection	192.168.1.200	192.168.2.200
Access Account	UN: head PW: head	UN: branch PW: branch
ISDN line number	1000	2000
Callback Function	Disable	Disable

4.3.1 Activating the Remote Dial-In Capability

In the Quick Setup group of the Setup Main Menu, click "Remote Dial-In Access Setup" to enter the setup page. See 4.2 Remote Dial-In Access for a full explanation of the fields on this page.

Head Office:

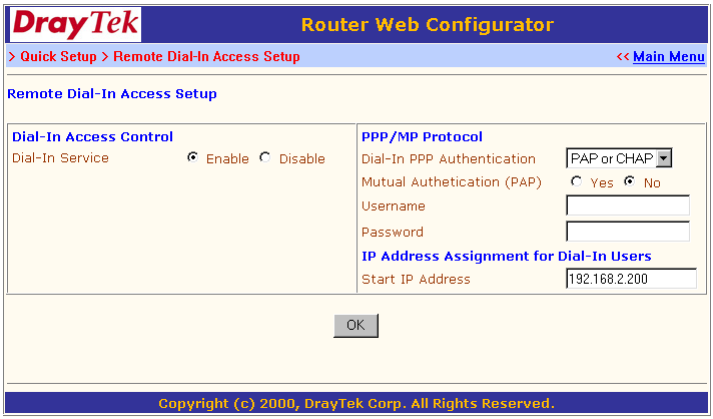


The IP range of the Head Office network is 192.168.1.0/24, the settings should be as below:

Dial-In Service: Enable

Start IP Address: 192.168.1.200

Branch Office:



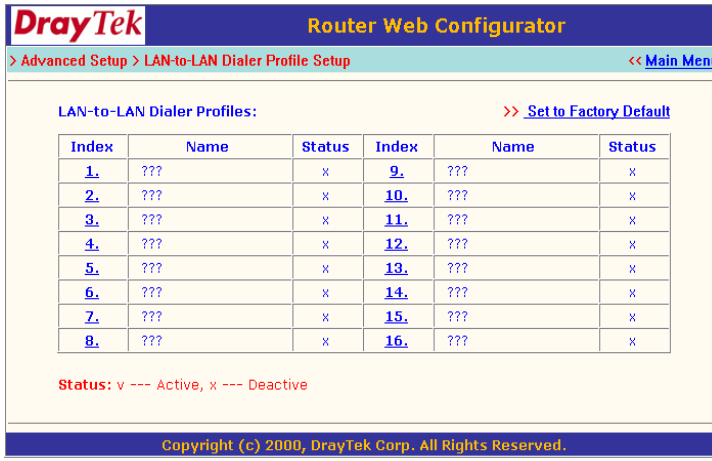
The IP range of the Branch Office network is 192.168.2.0/24, the settings should be as below:

Dial-In Service: Enable

Start IP Address: 192.168.2.200

4.3.2 Creating a LAN-to-LAN Dialer Profile

After enabling the Dial-in service, you must create a LAN-to-LAN profile for each network. From the Advance Setup menu, click "**LAN-to-LAN Dialer Profile**" to enter the setup page as below.



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

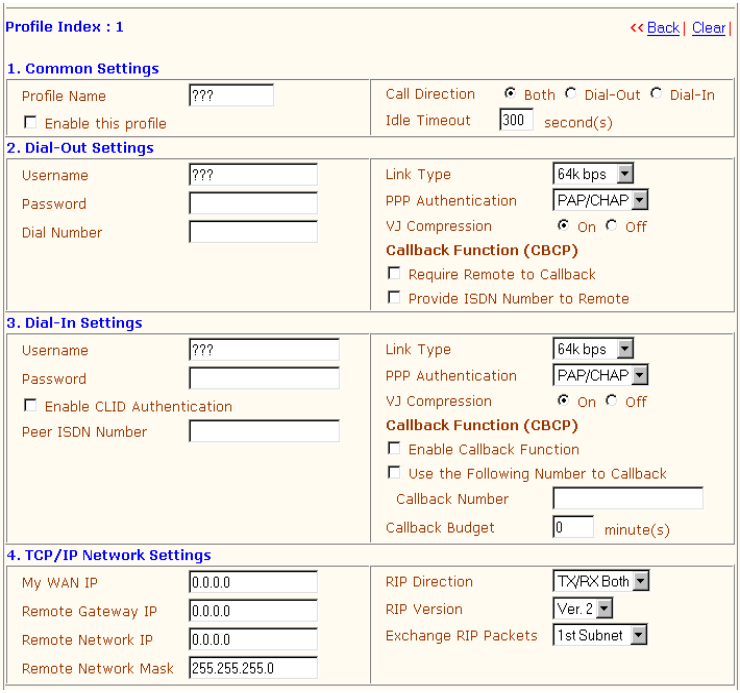
Set to Factory Default: Clicking here will clear all the LAN-to-LAN profiles.

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

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

Status: Indicate the status of the individual profiles. The symbol "v" means the profile is active and "x" means it is inactive.

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



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 every subgroup in detail.

Common Settings

Profile Name: Specify a name for the remote network.

Enable this profile: Check here to activate this profile.

Call Direction: Specify the allowed call direction for this profile.

Both: allow access of both outgoing and incoming calls.

Dial-Out**:** allow access of outgoing calls only.

Dial-In**:** allow access of incoming calls only.

Idle Timeout: Default setting is 300 seconds. When a connection of a profile has been idled longer than the time limit , the router will drop the connection.

Dial-Out Settings

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

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

Dial Number: Specify the destination ISDN number for dialup.

Link Type: Indicate the dial-out link type.

Disable: Deactivate the dial-out action.

64kbps: Specify the outgoing connection speed is restricted to 64kbps (one B-channel).

128k bps: Specify the outgoing connection speed is 128kbps (two B-channels).

BOD: Specify the link type to be dynamic bandwidth control (Bandwidth-on-Demand).

PPP Authentication: Specify the authentication method. 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.

Callback Function (CBCP): The callback function is implemented by the CBCP protocol that is one of the PPP protocol suite.

- Require Remote to Callback: Inactive by default. When active, the router exchanges connection information with the remote router and requires the remote router to call back to make a connection.

- Provide ISDN Number to Remote: In some cases, the remote router requires the ISDN number for calling back. Check here to allow the local router to send the ISDN number to the remote router. The remote router owner will be charged the connection fee by the telecom.

Dial-In Settings

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

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

Enable CLID Authentication: Limit the dial-in router to be called from a specific ISDN number.

Peer ISDN Number: If CLID Authentication is enabled, enter the remote router's ISDN number in this field

Link Type: Refer to **Dial-Out Settings**.

PPP Authentication: Refer to **Dial-Out Settings**.

CVJ Compression: Refer to **Dial-Out Settings**

Callback Function (CBCP): Checking here allows this router to accept requests from a remote router for call back.

Enable Callback Function: Checking here to enable this function. The router owner will be charged the connection fee by the telecom.

Use the Following Number to Callback

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

- Callback Budget: Specify a time budget for the callback function. By default the budget is set to zero, which means no call back attempt will work.

TCP/IP Network Settings

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

My WAN IP: 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: Specify the IP address of the remote router.

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

Remote Network Mask: Specify the netmask of the remote network.

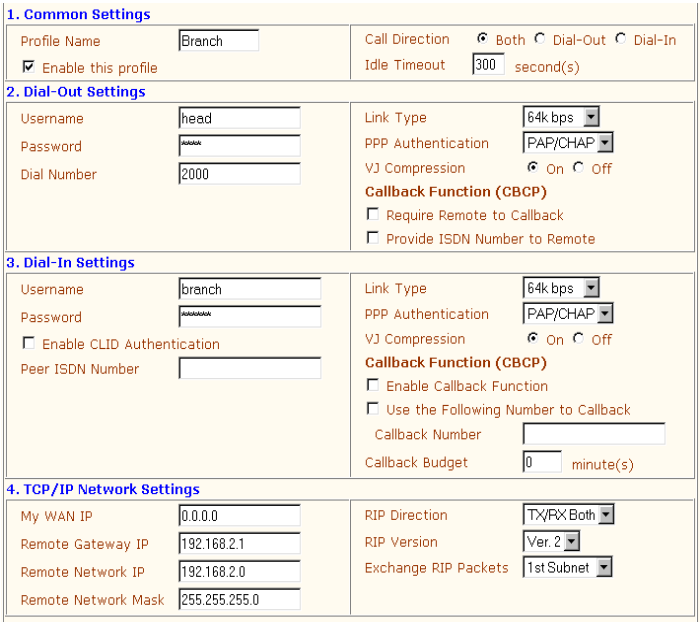
RIP Direction: The option specify the direction of RIP (Routing Information Protocol) packets through the ISDN WAN connection.

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

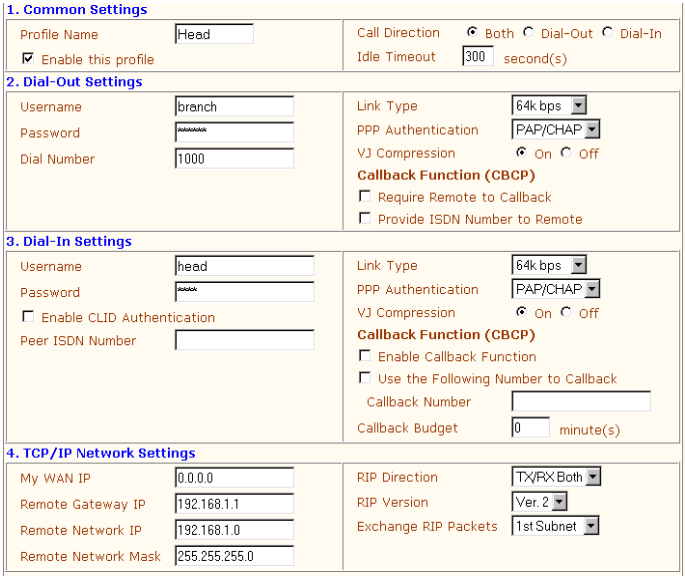
Exchange RIP Packets: The router has two local IP networks: the 1st subnet and 2nd subnet. Here you set which subnet will exchange RIP packets with the remote network. Usually set to 1st subnet for routing between the 1st subnet and the remote network.

Recall the LAN-to-LAN example described in section 4.3. The LAN-to-LAN Dialer Profile could be configured as below.

Head Office:

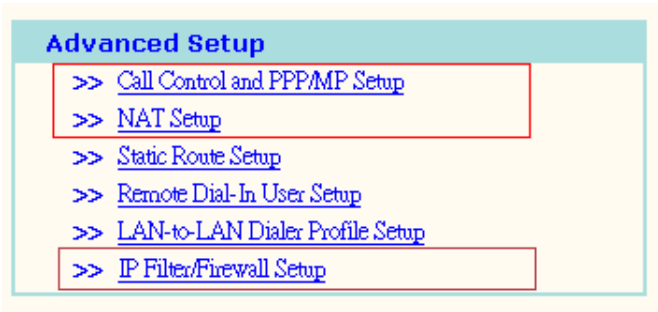

1. Common Settings
Profile Name
Branch
Enable this profile
Call Direction
Both
Dial-Out
Dial-In
Idle Timeout
300
second(s)
2. Dial-Out Settings
Username
head
Password
Dial Number
2000
Link Type
64k bps
PPP Authentication
PAP/CHAP
VJ Compression
On
Off
Callback Function (CBCP)
Require Remote to Callback
Provide ISDN Number to Remote
3. Dial-In Settings
Username
branch
Password
Enable CLID Authentication
Peer ISDN Number
Link Type
64k bps
PPP Authentication
PAP/CHAP
VJ Compression
On
Off
Callback Function (CBCP)
Enable Callback Function
Use the Following Number to Callback
Callback Number
Callback Budget
0
minute(s)
4. TCP/IP Network Settings
My WAN IP
0.0.0.0
Remote Gateway IP
192.168.2.1
Remote Network IP
192.168.2.0
Remote Network Mask
255.255.255.0
RIP Direction
TX/RX Both
RIP Version
Ver. 2
Exchange RIP Packets
1st Subnet

Branch Office:



5 Advanced Setup

This chapter explains the remaining options available in Advanced Setup:



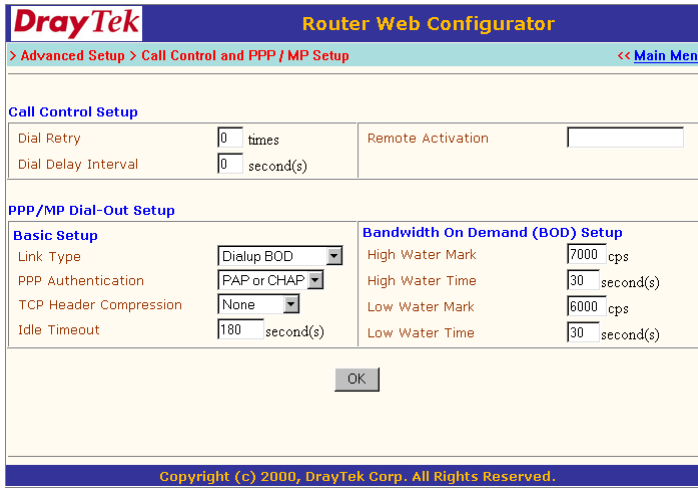
Advanced Setup

> Call Control and PPP/MP Setup

> NAT Setup

> IP Filter/Firewall Setup

As you click "**Call Control and PPP/MP Setup**" will open the setup page as below. The page will describe in the following three sections for specific application.



5.1 Enabling the Remote Activation Function

Some applications require the router to be remotely activated, or dial up to the ISP using the ISDN interface. For instance, if you are a user who accesses the Internet via ISDN from home, usually the dialup connection is idle when you are not at home. You may want to get some files from home while you are working in the office. This function allows you to make a phone call to the router and ask it to dial up to the ISP. Then you can access your home network to retrieve the files. Of course, you have to have a fixed IP address and expose some internal network resources, such as FTP, WWW etc.

Click "**Call Control and PPP/MP Setup**" and specify a phone number in the Remote Activation field.

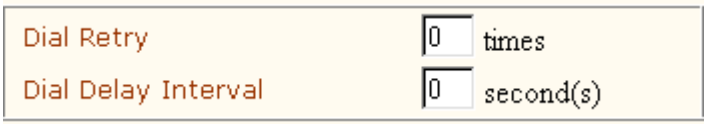
5.2 Call Control Setup

Remote Activation

If the router accepts a call from the number 12345678, it will disconnect immediately and dial to the ISP. Note that "**Internet Access Setup**" -> "**Dialing to a Single ISP**" should be preset properly.

Dial Retry and Dial Delay Interval

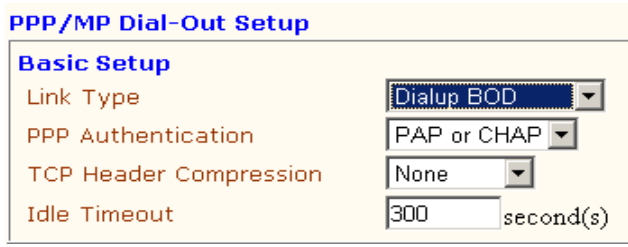
These two parameters set global settings for ISDN dialup access.



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

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

PPP/MP Dial-Out Setup

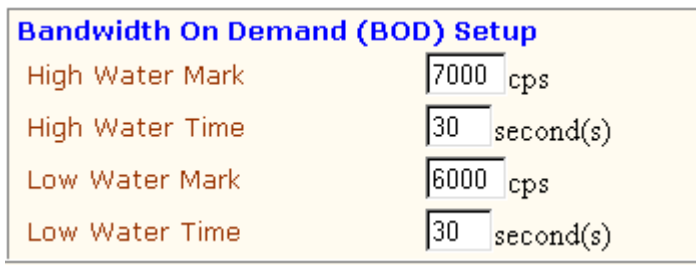


Basic Setup

Select according to the ISP service type you subscribed and enter parameters according to the setup you entered for Remote Access Setup (Chap 4).

5.3 Configuring the BOD Parameters

BOD stands for bandwidth-on-demand for Multiple Link PPP (ML-PPP or MP). Click "**Call Control and PPP/MP Setup**" to see the following settings.



These parameters are activated when you set the **Link Type** to **Dialup**

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

High Water Mark and High Water Time: These parameters specify the conditions under which the second channel will be activated. When the utilization of the first connected channel goes over the High Water Mark and past the High Water Time, the additional channel will be activated. The link speed will then be 128kbps (two B channels).

Low Water Mark and Low Water Time: These parameters specify the conditions under which the second channel will be dropped. When the utilization of two B channels is under the Low Water Mark and past the High Water Time, the additional channel will be dropped. The link speed will be 64kbps (one B channel).

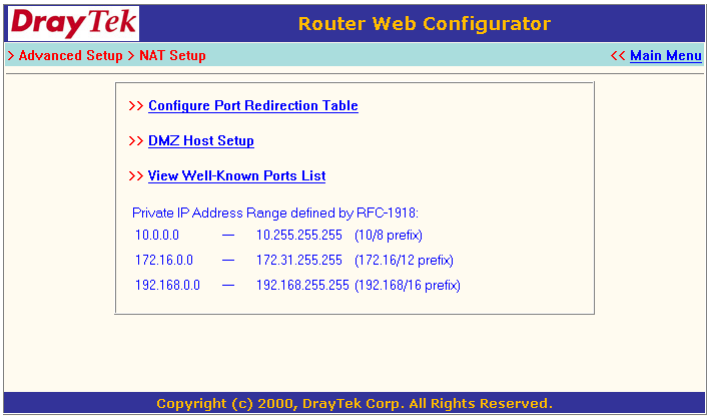
Note:

If you are not familiar with the operation of ISDN and ML-PPP, be wary of changing the default values.

5.4 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 (in Single ISP, PPPoE, PPTP) or two (in Dual ISPs mode) globally re-routable IP addresses from the ISP. Local hosts will use private network IP addresses defined by RFC-1918 to communicate with the router. The router translates the private network addresses to a globally routable IP address that 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 router.

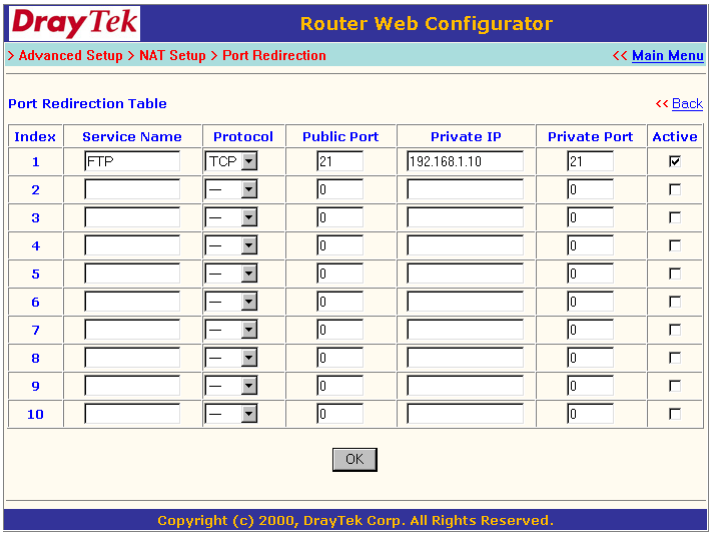


5.4.1 Exposing Internal Servers to the Public Domain

The Port Redirection Table may be used to expose internal servers to the public domain or to directly assign a specific port number to internal hosts. External hosts or domain can specify port numbers 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** provides 10 port-mapping entries for internal hosts.

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

Protocol: Specify the transport layer protocol that supports TCP and UDP options.

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

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

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

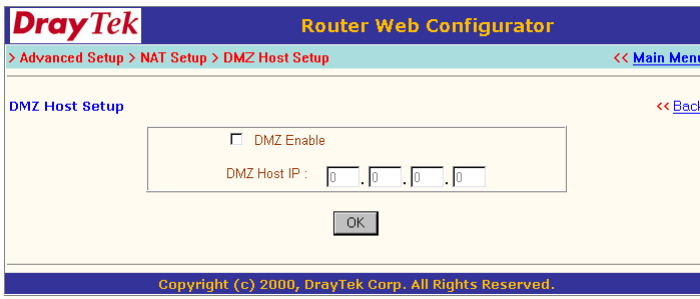
Active: Check here to activate the port-mapping entry.

5.4.2 DMZ Host Setup

Click "**DMZ Host Setup**" to open the setup page. 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.

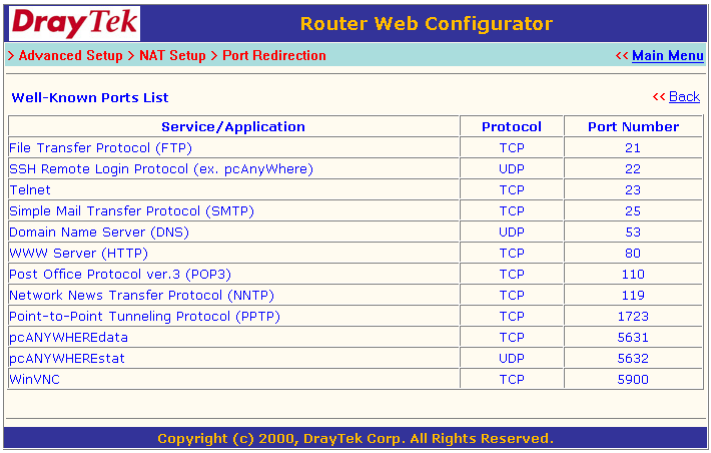
DMZ Enable: Check to enable the DMZ Host function.

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



5.4.3 Well-known Port Number List

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



DrayTek Router Web Configurator

> Advanced Setup > NAT Setup > Port Redirection << Main Menu

Well-Known Ports List << Back

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

5.5 IP Filter/Firewall Setup

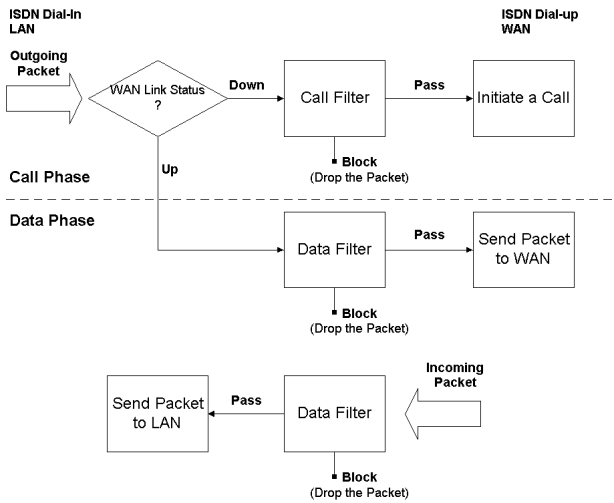
The IP Filter/Firewall function helps to prevent your local network against attack from outside. It also provides a method of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

5.5.1 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 later 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.

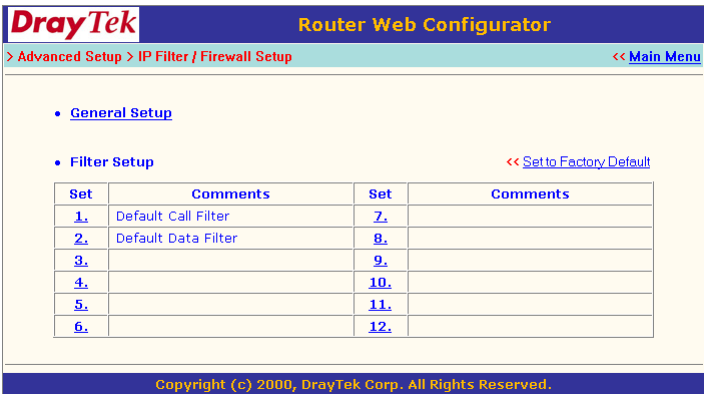
In concept, when an outgoing packet is routed to the WAN, the IP Filter will decide if the packet should be forwarded to the Call Filter or Data Filter. If the WAN connection has not been established, the packet will enter the Call Filter. If the packet is not allowed to trigger router dialing, it will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

If the WAN connection of the router has been established, the packet will pass through the Data Filter. Packets match the block rule will be dropped and the contrary 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 packets match the block rule, 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 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.



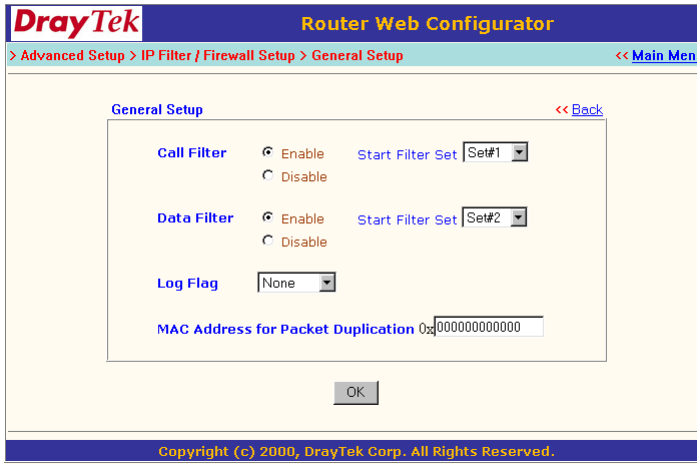
General Setup: Some general settings are in the setup link.

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.

5.5.2 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 the MAC address for duplicate packets.



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

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

Log Flag: For troubleshooting purpose, you need to 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.

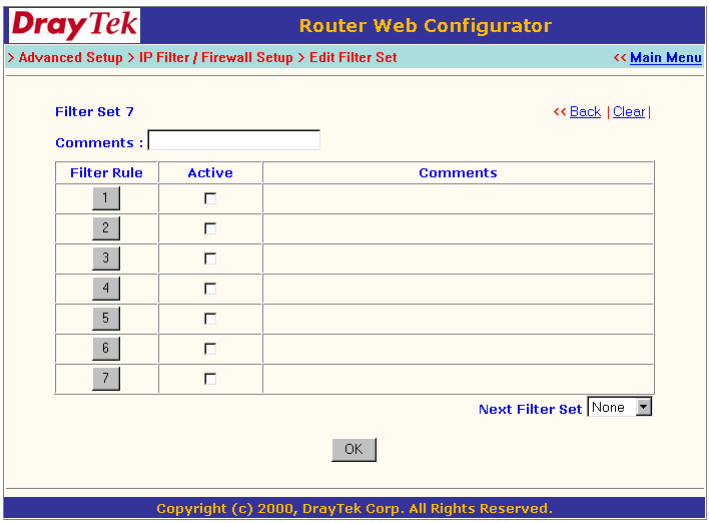
No Match**:** The log function will record all packets that are unmatched.

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. Enter "0" to disable the feature (also see "**Duplicate to LAN**" on page 5-22). The feature will be helpful under Ethernet switch environment.

5.5.3 Editing the Filter Sets



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

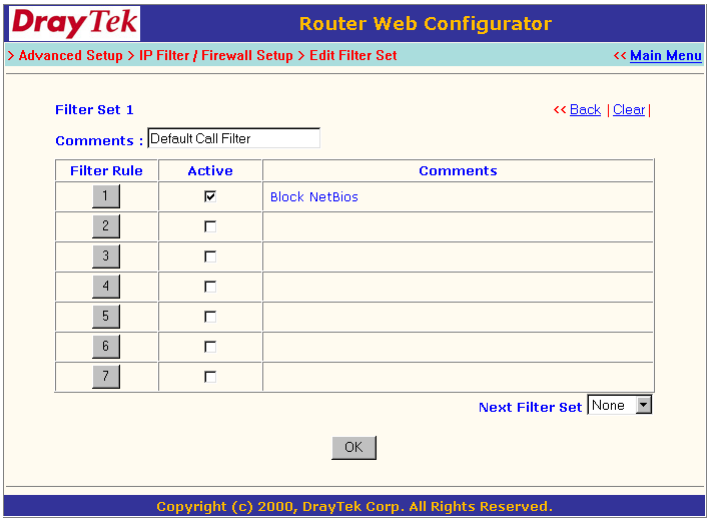
Filter Rule: Click a button numbered "**1**" ~ "**7**" to edit the filter rule.

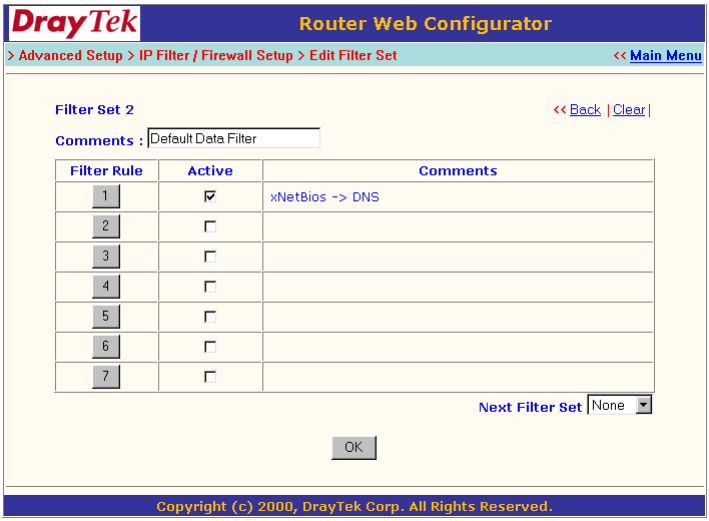
Active: Enable or disable the filter rule.

Next Filter Set: Specify the next filter set to link to after the current filter set. Be aware of the sequence of the link and avoid

any possible loop among the filter sets.

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





5.5.4 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 comment/description. Its maximum length is 14 characters.

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

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

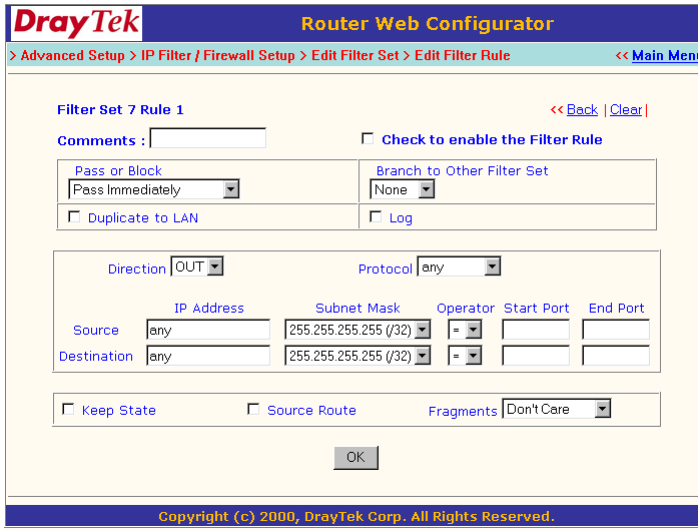
Block Immediately: Packets matching the rule will be dropped immediately.

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 pass 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 Packet Duplication**".

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

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

For the Data Filter:

IN: Specify the rule for filtering incoming packets.

OUT: Specify the rule for filtering outgoing packets.

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

IP Address: Specify a source and destination IP address for this filter rule to apply to. 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: Specify the Subnet Mask for the IP Address column for this filter rule to apply to.

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

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

!= : If the **End Port** is empty, the port number is not equal to the value of the **Start Port.** Otherwise, this port number is not between the **Start Port** and the **End Port** (including the **Start Port** and **End Port**).

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

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

Keep State: When checked, protocol information about the TCP/UDP/ICMP communication sessions will be kept by the IP Filter/Firewall (the Firewall **Protocol** option (see fig. 5.x on page 5-17) requires that TCP or UDP or TCP/UDP or ICMP be selected for this to operate correctly).

Fragments: Specify a fragmented packets action.

Don't Care: Specify no fragment options in the filter rule.

Unfragmented: Apply the rule to unfragmented packets.

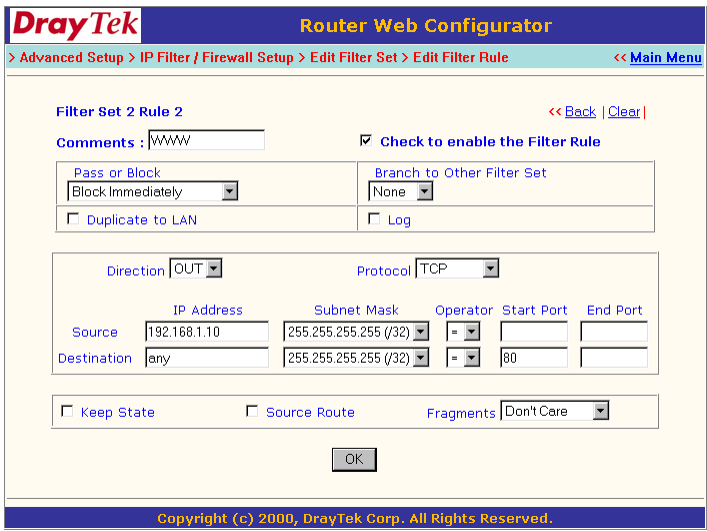
Fragmented: Apply the rule to fragmented packets.

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

5.5.5 Restricting Unauthorized Internet Services

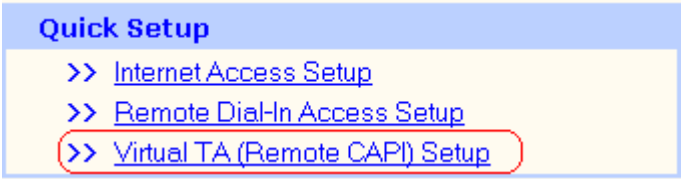
This section will show a simple example to restrict access of WWW from certain locations. In this example, we assume the IP address of the access-restricted user is 192.168.1.10. The filter rule is created in the Data Filter set and is shown as below.

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



6 Virtual TA Application

This chapter covers Virtual TA concepts and explains how to setup a Virtual TA.



Quick Setup

> Virtual TA (Remote CAPI) Setup

6.1 Virtual TA Concepts

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

Note:

1. The Virtual TA client is only supported on Microsoft™ Windows 95 OSR2.1/98/98SE/Me/2000 platforms.

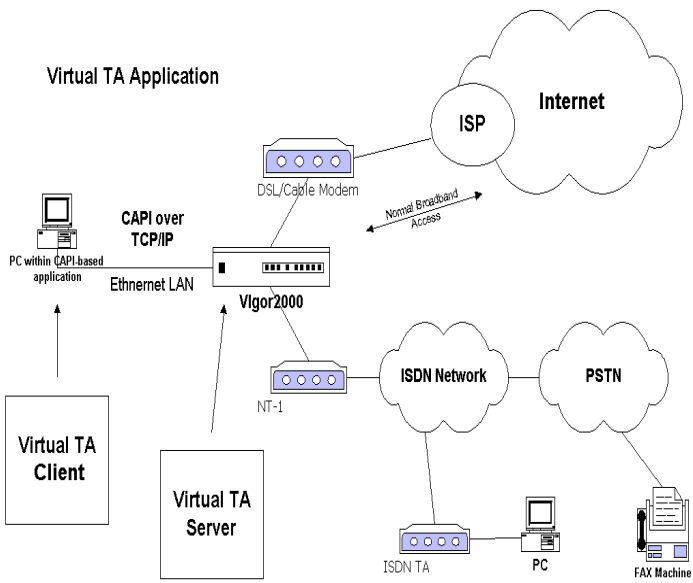
2. The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.

3. One ISDN BRI interface only has two B channels. The

maximum number of active clients is also 2.

4. Before you set up the Virtual TA, you must set the correct country code. Click "**ISDN Setup**" in the **Basic Setup** group.

As the following application chart shows, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA etc.



6.2 Installing a Virtual TA Client

1. Insert the CD-ROM supplied with your Vigor2000, or directly double-click the installer file. Vsetup95.exe is for Windows 95 OSR2.1 or higher. Vsetup98.exe is for Windows 98, 98SE and Me. Vsetup2k.exe is for Windows 2000.

2. Follow the on screen instruction of the installer. The last step requires you to restart your computer. Click "**OK"** to restart.

3. After the computer restarted, you will see a VT icon on the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.

When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Read your software user guide for detailed configuration.

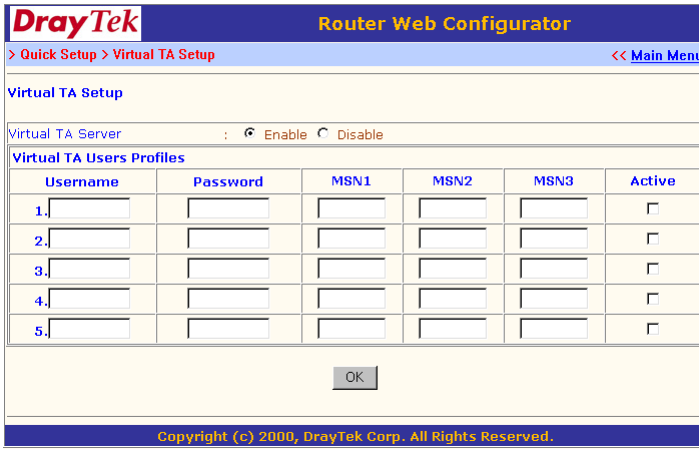
If the icon text is RED, it means the client lost the connection with the server. Check the physical Ethernet connection

6.3 Configuring a Virtual TA Client/Server

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

By default, the Virtual TA server is enabled and the username and password fields are blank. Any Virtual TA client may login to the server. Once a single Username and Password field has been filled,

the Virtual TA server will only allow clients with a valid username and password to login.



Virtual TA Server:

Enable: Check to activate the server.

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

Virtual TA User Profiles:

Username: Specify the username for a specific client.

Password: Specify the password for a specific client.

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

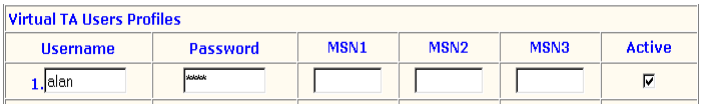
Active: Check to enable the client to access the server.

Creating a User Profile

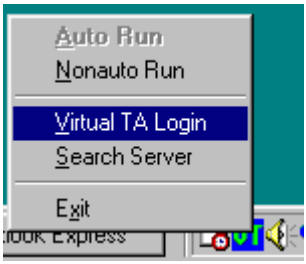
Note that creating a single user access account limits access to the Virtual TA server to only the specified account holders.

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

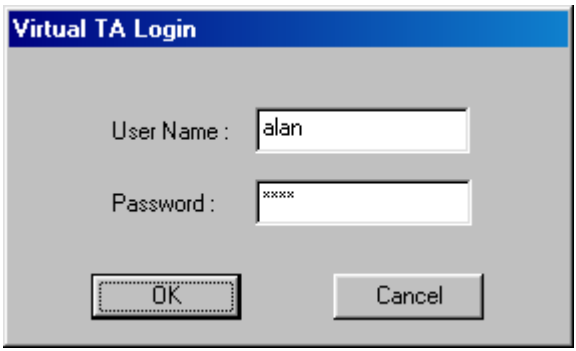
1. On the server: Click "**Virtual TA (Remote CAPI) Setup**", and fill in the **Username** and **Password** fields. Check the "**Active**" checkbox to enable the account.



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



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

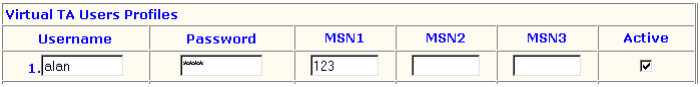


4. Enter the **Username** and **Password** and click "**OK**". After a short period of time the VT icon text will turn green.

Configuring the MSN Number

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

1. As an example, you could assign the MSN number "123" to the client.



Virtual TA Users Profiles					
Username	Password	MSN1	MSN2	MSN3	Active
1. alan	•••••	123			☑

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

7 System Management

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

System Management

> Online Status

> Management Setup

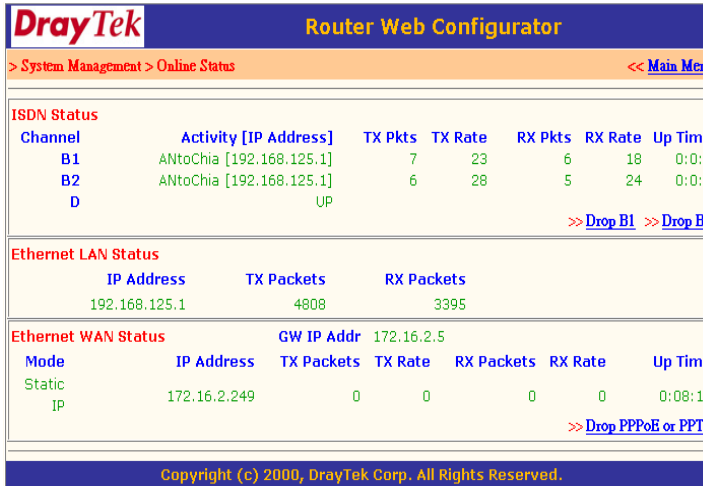
> Diagnostic Tools

> Reboot System

> Firmware Upgrade (TFTP Server)

7.1 Online Status

Click "**Online Status**" to open the Online Status page. The example shown in the next page has both ISDN B1 and B2 channel active and also a Static IP connection.



The Online Status page contains three subgroups: ISDN Status, Ethernet LAN Status, and Ethernet WAN Status.

ISDN Status:

Shows the connection status of B1, B2, and D channel, including ISP dialup, active remote dial-in user, or LAN-to-LAN connection.

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

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

TX Rate: Transmission rate for outgoing data. The unit is characters per second (cps).

RX Pkts: Total number of received IP packets received during this connection session.

RX Rate: Reception rate for ingoing data. The unit is characters per second (cps).

Up Time: Connection time. The format is HH:MM:SS where HH means hours, MM means minutes, and SS means seconds.

Drop B1: Click to disconnect the B1 channel.

Drop B2: Click to disconnect the B2 channel.

Ethernet LAN Status:

IP Address: IP address of the LAN interface.

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

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

Ethernet WAN Status:

Mode: Indicates which broadband access mode is active. Depending upon the broadband access mode, you may see Static IP, PPTP, or PPPoE.

GW IP Address: Indicates the gateway IP address.

IP Address: The 2nd IP Address of Ethernet or the IP address of WAN interface that is from PPTP/PPPoE connection.

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

TX Rate: Transmission rate for outgoing data. The unit is characters per second (cps).

RX Packets: Total number of transmitted IP packets received during this connection session.

RX Rate: Reception rate for ingoing data. The unit is characters per second (cps).

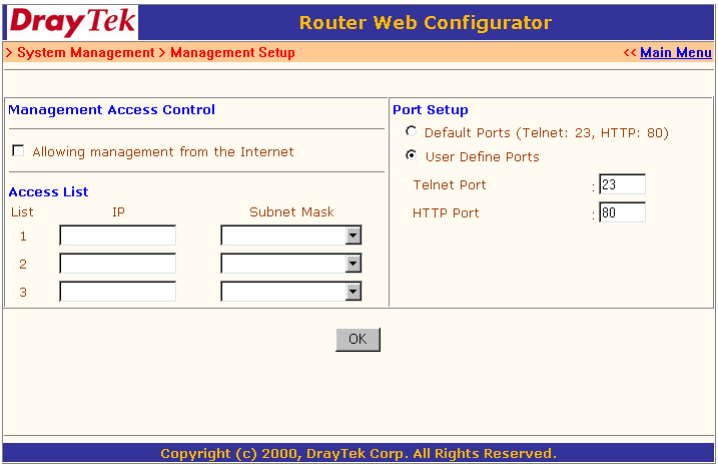
Up Time: Connection time. The format is HH:MM:SS where HH means hour, MM means minute, and SS means second.

Drop PPPoE or PPTP: Click to disconnect the PPPoE or PPTP connection.

7.2 Management Setup

By default, the router 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 display.



Management Access Control

Allow management from the Internet: Check to allow system administrators to login from the Internet. The default setting 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.

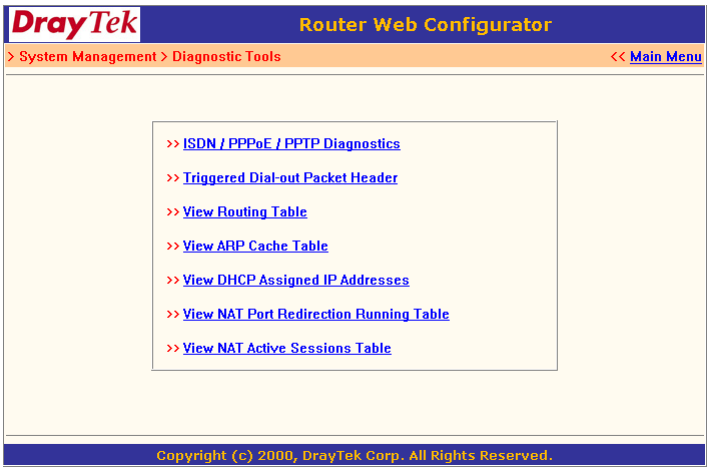
Port Setup

Default Ports: Check to use standard port numbers for the Telnet and HTTP servers.

User Defined Ports: Check and enter user-defined port numbers for the Telnet and HTTP servers.

7.3 Diagnostic Tools

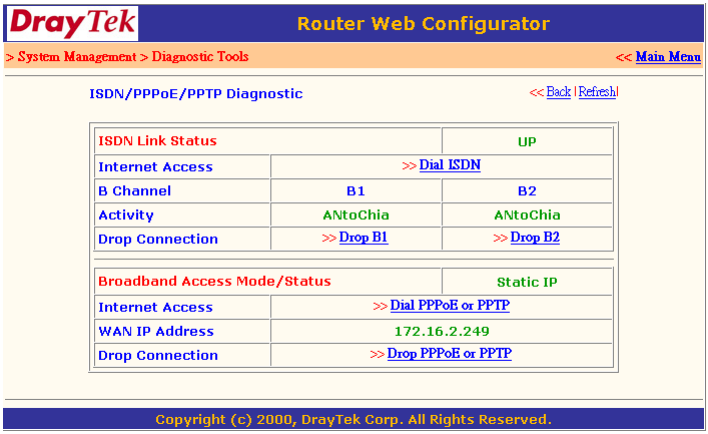
Diagnostic Tools provide useful tools for viewing or diagnosing the router. Click Diagnostic Tools to enter the following page.



ISDN / PPPoE / PPTP Diagnostics

Click to open the following page. The page shown here is for reference only; different networks will show different results.

This page has been grouped into two subgroups; the upper one is for ISDN link status and the lower one is for broadband access status.



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

ISDN:

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

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

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

Drop B1: Click to disconnect the B1 channel.

Drop B2: Click to disconnect the B2 channel.

Broadband Access:

Broadband Access Mode/Status: Displays the broadband access mode and status. If the broadband connection is active,

it will show **PPPoE**, **PPTP**, **or Static IP** depending on which access mode is enabled. If the connection is idle, it will show "**- - -**".

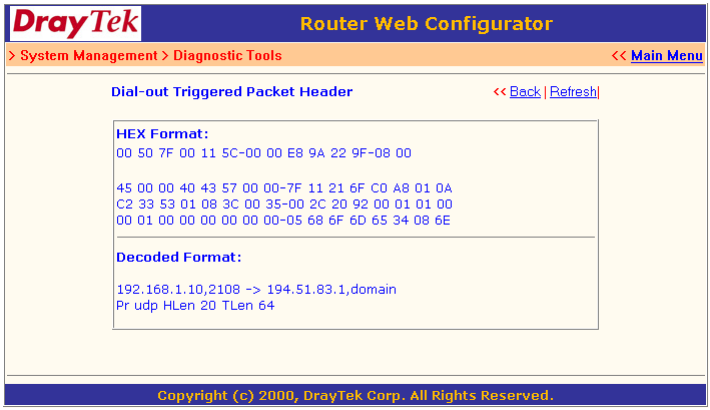
WAN IP Address: The WAN IP address for the active connection.

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

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

Triggered Dial-out Packet Header:

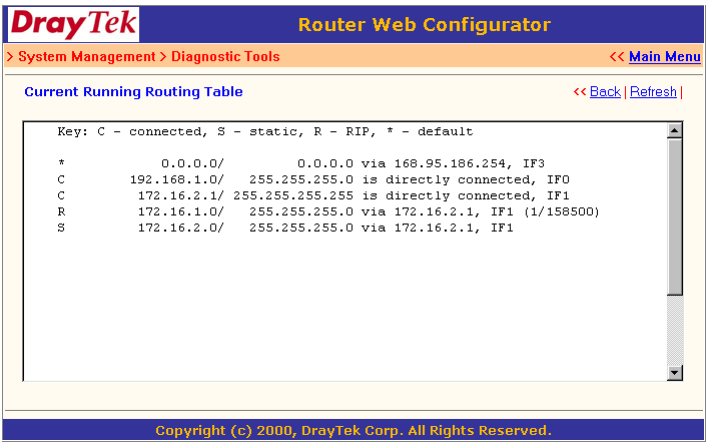
Triggered Dial-out Packet Header shows the last IP packet header that triggers the router to dial out.



Refresh: Click to reload the 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:

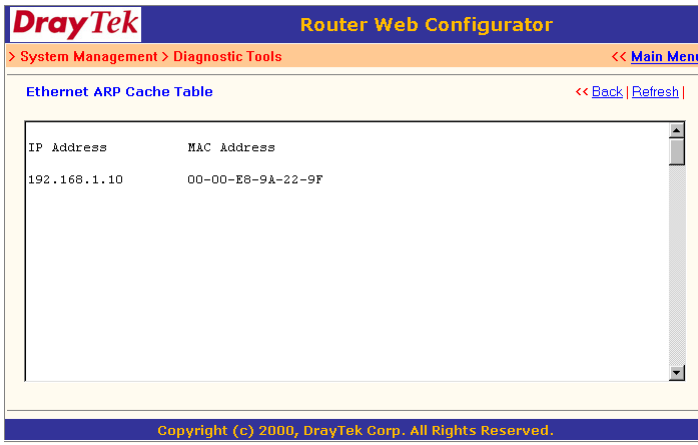
IF0 --- Local LAN interface.

IF1 --- ISDN B1 channel.

IF2 --- ISDN B2 channel.

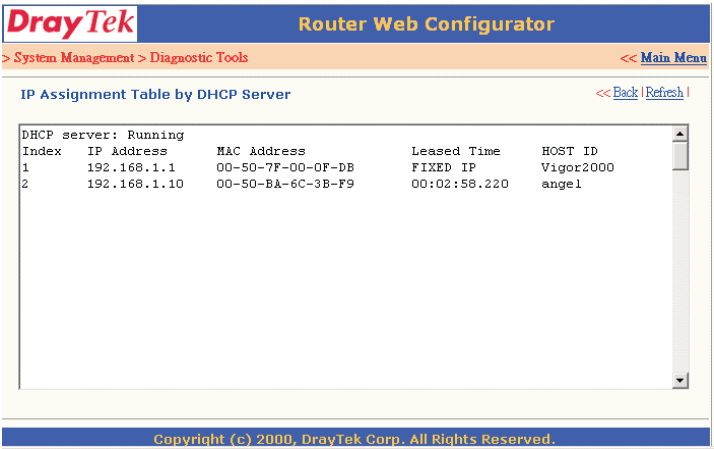
View ARP Cache Table:

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.

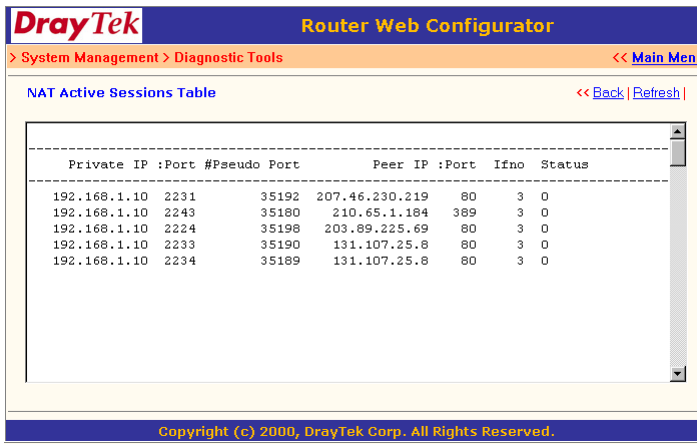


View NAT Port Redirection Running Table:

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 is getting on 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 internal user's (PC's) IP address and port number.

#Pseudo Port: The public port number.

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

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

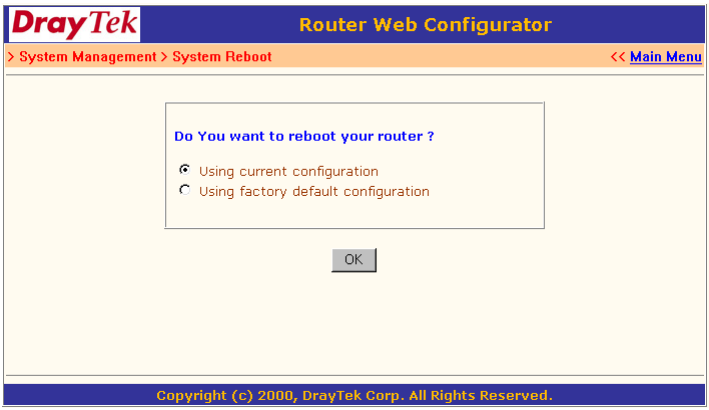
0 --- LAN interface.

1 --- B1 interface

2 --- B2 interface.

7.4 Reboot System

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



There is 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's settings to default values, check **Using factory default configuration** and click "**OK**".

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

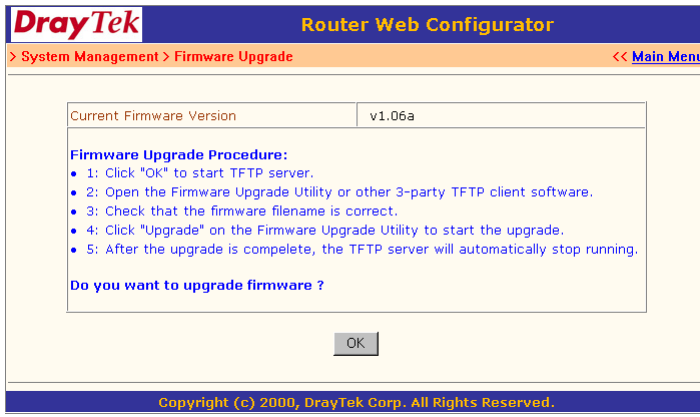
7.5 Firmware Upgrade

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

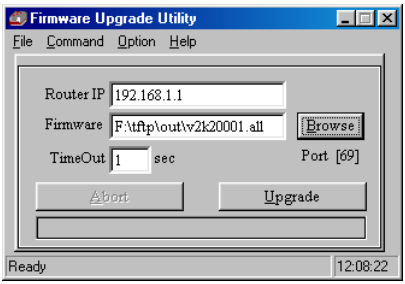
1. Download the latest firmware from DrayTek's website or FTP site (ftp://ftp.draytek.com/vigor2000/).

2. Use Web Configurator to enable the Firmware Upgrade function.

Click **Firmware Upgrade (TFTP Server)** to open the following screen. Click "**OK**" to enable the function.



3. Click **Start -> Programs -> Router Tools -> Firmware Upgrade Utility** to launch the **Firmware Upgrade Utility**.



The **Router IP** field will show the IP address of your router. Click "**Browse**" to select the new firmware file. The file shown here (v2k00106.bin) is for example purpose only and the latest firmware will have a different file name. Click "**Upgrade**". The upgrade status will be shown on the progress bar.

Note:

The definition of firmware filename:
v2kxxxxx.bin: Binary code file of the firmware.
v2kxxxxx.web: WebPages file of the firmware.
v2kxxxxx.cfg: Default settings file of the firmware.
v2kxxxxx.all: v2kxxxxx.bin + v2kxxxxx.web.
v2kxxxxx.rst: v2kxxxxx.cfg + v2kxxxxx.bin + v2kxxxxx.web.

Note:

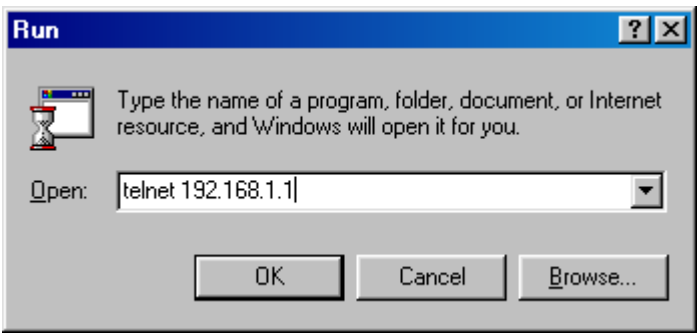
When you upgrade firmware, the *.bin file should be the first file you upload and then the *.web. After 30 seconds, reboot your router. If you do not follow these steps, you may have problems upgrade the firmware.

8 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, the Linux has a built-in Telnet client.

8.1 Using the Telnet Terminal Commands

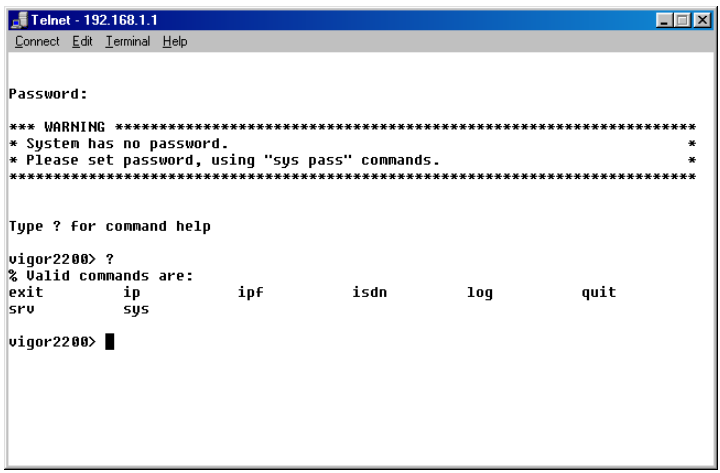
Click **Start** -> **Run** and type "**Telnet 192.168.1.1**" in the **Open** box as below. Note that the IP address in the example is the default address of the Vigor2000 router. If you have changed the default, enter the current IP address of the router.



Click "**OK**". The Telnet terminal will open. If an administrator password has not 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 all possible Telnet 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.

```
vigor2000> ip ?
% Valid subcommands are:
addr          arp           route

vigor2000>
```

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:

Enter **quit** or **exit** to quit the Telnet terminal.

8.2 Viewing Call Logs

The Call log provides a simple method for troubleshooting the 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.

ISDN example:

```
vigor2000> log -c
18:25:59.470 >>> Dial-up triggered by user : 0.6.234.255
             proto=0, to 255.255.226.77
18:25:59.470 Dialing ISP (HiNet) : 04125678
18:25:59.990 PPP Start (B1)
18:26:03.250 PAP Login OK (B1)
18:26:03.300 IPCP Opening (B1)
             Own IP Address : 163.31.241.230  Peer IP Address : 168.95.67.195
             Primary DNS : 168.95.192.1  Secondary DNS : 168.95.1.1
vigor2000>
```

PPPoE example:

```
vigor2000> log -c
00:13:28.130 >>> Dial-up triggered by user : 0.6.234.255
             proto=0, to 255.255.226.77
00:13:28.820 PPP Start (PPPoE)
00:13:31.210 PAP Login OK (PPPoE)
00:13:31.360 IPCP Opening (PPPoE)
             Own IP Address : 211.23.53.10  Peer IP Address : 211.23.53.254
             Primary DNS : 168.95.192.1  Secondary DNS : 168.95.1.1
vigor2000>
```

8.3 Viewing ISDN Logs

To capture messages exchanged on the ISDN interface, clear all ISDN logs before you start capturing the new log.

The steps are:

1. Login to the Telnet terminal.
2. Type "**log -F w**" to clear all ISDN logs.
3. Ping to any outside host to trigger the router to dial from your PC.
4. Type "**log -i**" to display the latest ISDN log. To display all ISDN logs saved in the log buffer, type "**log -i -t**".

Detailed ISDN log example:

```
15:15:59.550 ---->D Len=27 LAPD TE C  SAPI=0  TEI=75  INFO P=0 NR=4    NS=4
        23   bytes  ETSI  102
    Orig    CR=0x3E      PD=Q.931 SETUP
 1  00000100 INFORMATION  ELEMENT : Bear Capability
 2  00000010 IE length : 2   octets
 3  1------- Extension bit : not continued
    -00----- Coding standard : CCITT standard coding as described below
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
    ---01000 Info. transfer capability : unrestricted digital information
 4  1------- Extension bit : not continued
    -00----- Transfer mode : circuit mode
    ---10000 Information transfer rate : 64 kbit/s
 1  00011000 INFORMATION  ELEMENT : Channel Identification
 2  00000001 IE length : 1   octets
 3  1------- Extension bit : not continued
    -0------ Interface ident. : implicit identified
    --0----- Interface type : basic interface
    ---0---- Spare
    ----0--- Preferred/exclusive : indicate channel is preferred
    -----0-- D-channel indicator : the channel identified is not the D-channel
    ------11 Information channel selection : any channel
 1  01110000 INFORMATION  ELEMENT : Called Party Number
 2  00001001 IE length : 9   octets
 3  1------- Extension bit : not continued
    -000---- Type of number : unknown
    ----0000 Numbering plan : unknown
 4  ******** Number digits : [04125678]
 19 10100001 INFORMATION  ELEMENT : 0xA1
```

The above example shows detailed D-channel **SETUP** messages only. Note that all ISDN D-channel messages will be displayed when you type the **log -i -t** command. To use the command, you will get to know whether the ISDN connection could be established or not. Note that if you cannot read the details, please save these messages in file and attach to support technician.

8.4 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.

```
vigor2000> log -p
16:18:59.990 >>>>B1 Len=12
    Protocol:LCP(c021)
        ConfReq Identifier:0x00
            Protocol Field Compression
            Address/Control Field Compression ##

16:19:00.790 <<<<B1 Len=46
    Protocol:LCP(c021)
        ConfReq Identifier:0x00
            Authentication Type:
                CHAP 80
            Magic Number: 0x69f7
            MRRU: 1614
            Endpoint Discriminator
                Locally Assigned Address: c5 1f 0c f0 d1 7c 11 d4 87 d4 00 10 b5
4b 1f fb 00 00 00 00 ##
```

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

8.5 Viewing WAN Logs

To view all WAN logs including ISDN D-channel and PPP/PPPoE/ PPTP messages, the simplest way is to type "**log -w -t**".

The steps are:

1. Login to the Telnet terminal.

2. Type "**log -F w**" to clear all PPP/PPPoE/PPTP and ISDN logs.

3. Ping to any outside host to trigger the router to dial from your PC.

4. Type "**log -w**" to display the latest WAN log. If you want to

display all WAN logs, use the "**log -w -t**" command.

8.6 FAQs

The following session cover answers for some frequently asked questions. For more FAQs, please visit DrayTek website (www.draytek.com) or contact your local technical support.

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

A: By default, you do not need a password to login to the router. However, for security reason, you should assign a password to protect your router against misusage and hacker attack.

2. 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.

3. 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**" > "**Triggered Dial-out Packet Header**". You will see the triggered packet contents. Report the results to technical support by e-mail or telephone.

4. Why can't I connect to the Web Configurator?

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

5. Why can I ping to outside hosts but can not access Internet websites?

A: Check if the Primary and the Secondary DNS server have been correctly setup on your PC. Your should have received the DNS server settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address settings. Because the router will assign the DNS settings to the DHCP-client-enabled PC.

6. How many IP addresses the DHCP server of the router can assign to local PCs?

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