# Table of Contents


**0. Preface** ..... 0-1

0.1 About This Manual ..... 0-2

0.2 Copyright Declarations ..... 0-2

0.3 Trademarks ..... 0-2

0.4 How To Become A Registered Owner ..... 0-2

0.5 Safety Instructions ..... 0-3

0.6 Warranty ..... 0-3

0.7 European Community Declarations ..... 0-4

**1. Getting Started** ..... 1-1

1.1 Introduction ..... 1-2

1.2 Vigor2200 Series Router Comparisons ..... 1-3

1.3 Unpacking Your Vigor2200 Series Router .... 1-5

1.4 LED Indicators & Rear Panels ..... 1-6

1.5 Key Features ..... 1-16

**2. Installation & Setup** ..... 2-1

2.1 Before you Begin ..... 2-2

2.2 Hardware Installation ..... 2-4

2.3 Setting up a Management PC ..... 2-7

2.4 Using the Smart Start Wizard ..... 2-13

2.5 Using the Web Configurator ..... 2-18

3. Basic Setup & Internet Access ..... 3-1
3.1 Basic Setup ..... 3-2
3.2 Wireless LAN Access Setup .....3-7
3.3 Internet Access Setup ..... 3-10
3.4 ISDN Dial-up Internet Access ..... 3-12
3.5 DSL/Cable Modem Internet Access ..... 3-15

4. Remote Access ..... 4-1
4.1 Introduction to Remote Access ..... 4-3
4.2 Remote Dial-in Access ..... 4-3
4.3 LAN-to-LAN Access ..... 4-8

5. Advanced Setup ..... 5-1
5.1 Enabling the Remote Activation Function .... 5-3
5.2 Call Control Setup ..... 5-4
5.3 Configuring the BOD Parameters ..... 5-4
5.4 NAT Setup ..... 5-6
5.5 Static Route Setup ..... 5-9
5.6 IP Filter/Firewall Setup ..... 5-14

6. Virtual TA Application ..... 6-1
6.1 Virtual TA Concepts ..... 6-2
6.2 Installing a Virtual TA Client ..... 6-3
6.3 Configuring a Virtual TA Client/Server ..... 6-4

7. System Management ..... 7-1
7.1 Online Status ..... 7-2
7.2 Management Setup ..... 7-5
7.3 Diagnostic Tools ..... 7-6
7.4 Reboot System ..... 7-13
7.5 Firmware Upgrade ..... 7-13

8. Troubleshooting & FAQ ..... 8-1
8.1 Using the Telnet Terminal Commands ..... 8-2
8.2 Viewing Call Logs ..... 8-4
8.3 Viewing ISDN Logs ..... 8-5
8.4 Viewing PPP Logs ..... 8-6
8.5 Viewing WAN Logs ..... 8-7
8.6 Troubleshooting the DHCP Client on WAN .. 8-7
8.7 FAQs ..... 8-9
Appendix-Virtual TA on Mac OS9.x ..9-1
Appendix-Virtual Private Network (VPN)

# 0

# Preface


0.1 About This Manual

0.2 Copyright Declarations

0.3 Trademarks

0.4 How To Become A Registered Owner

0.5 Safety Instructions

0.6 Warranty

0.7 European Community Declarations

## 0.1 About This Manual

This manual is designed to assist users in using the DrayTek Vigor2200 series router, including the Vigor2200, Vigor2200X and Vigor2200E, Vigor2200W. 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

Copyright 2000 & 2001 DrayTek Corporation. All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

## 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, except for the Vigor2200E model.

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

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

• The 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 to dispose of the router, please follow local regulations on conservation of the environment.

## 0.6 Warranty

We warrant to the original end user (purchaser) that the Vigor2200 series 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 re-

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

The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

## 0.7 European Community Declarations

Hereby, DrayTek Corporation declares that these Vigor2200 series routers are in compliance with the essential requirements and other relevant provisions of Directive 99/5/EC. The ISDN interface of Vigor2200, Vigor2200X and Vigor2200W is designed for the ISDN network throughout the EC-region.

# 1 Getting Started

1.1 Introduction
1.2 Vigor2200 Series Router Comparisons of Vigor2200/Vigor2200X/Vigor2200W/Vigor2200E
1.3 Unpacking Your Vigor2200 Series Router
1.4 LED Indicators & Rear Panels
1.5 Key Features

## 1.1 Introduction

The Vigor2200 series of routers is composed of the Vigor2200, the Vigor2200X, Vigor2200E, and the Vigor2200W. The Vigor2200E has no ISDN BRI interface. Therefore, no ISDN functions are available for the Vigor2200E and parts of this manual referring to such functions will not apply to the Vigor2200E.

From a technical point of view, the Vigor2000, Vigor2200X and Vigor2200W are broadband DSL/Cable routers within another WAN interface ---ISDN BRI. The interface offers traditional ISDN functions, such as remote access, LAN-to-LAN access, Virtual TA applications, and ISDN dial-backup. The Vigor2200E is a pure Ethernet-to-Ethernet router.

The Vigor2200 series routers provide multiple users with efficient and reliable access over a single ISDN, DSL line, or Cable Modem service to the Internet and corporate LAN for using E-mail, sharing documents, Web surfing, file transfers, etc.

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

For traditional ISDN users, the Vigor2200, Vigor2200X and Vigor2200W feature a built-in Virtual TA (Remote CAPI) server which can operate 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 .

## 1.2 Vigor2200 Series Router Comparisons

| Items\Models | Vigor2200 | Vigor2200X | Vigor2200W | Vigor2200E |
|---|---|---|---|---|
| VPN/IPSec support | Yes | Yes | Yes | Yes |
| 10/100BaseTX Switch (LAN 1) | Yes | Yes | Yes | Yes |
| LAN Ethernet Speed | Yes | Yes | Yes | Yes |
| ISDN Interface | Yes | Yes | Yes | No |
| Broadband Interface (WAN port) | 10BaseT Ethernet port | 10BaseT Ethernet port | 10BaseT Ethernet port | 10BaseT Ethernet port |
| Broadband Access Capability | DSL/Cable Modem | DSL/Cable Modem | DSL/Cable Modem | DSL/Cable Modem |
| Wireless Access Point | - | - | Yes | - |

The above table shows a brief comparison of the Vigor2200 series routers: the Vigor2200, Vigor2200X, Vigor2200E and Vigor2200W. Note that the Vigor2200E does not have an ISDN BRI interface and that LAN-to-LAN, remote access, and ISDN dial-backup are not available. For the local Ethernet interface, LAN1 supports 10/100 Base-TX on all models, though the Vigor2200X, the Vigor2200E and the Vigor2200W have a built-in 4-port 10/100 Base-TX switch.

Only Vigor2200W has the IEEE802.11b wireless Access Point which has the WEP 64/128bits encryption for secured wireless LAN.

Broadband DSL/Cable Modem Connection Features:

1. Seamless migration from ISDN to a broadband connection for multiple SOHO users.

2. Easily use ISDN for dial-backup and/or remote access while concurrently using the DSL/Cable modem connection.

3. PPPoE allows users on the LAN2(WAN) 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 client software is required for the computers. Hassle free!

4. The Vigor2200 series DHCP client allows users on the LAN2(WAN) interface to access the Internet via an external cable modem.

## 1.3 Unpacking Your Vigor2200 Series Router

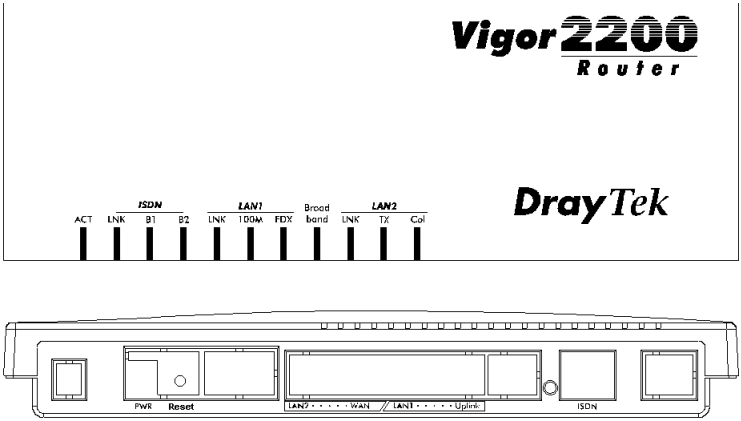
Your Vigor2200 series router package should contain the items listed below. If any item is missing or damaged, contact your dealer or DrayTek Customer Service Department immediately.

- One User manual with warranty/registration card
- One CD-ROM; includes User Manual in electronic form, latest released firmware, and utilities
- One RJ-45 ISDN telephone cable (black). Note that the Vigor2200E package does not contain this cable.
- One AC/AC power adapter (black), AC100-230V, input AC 15 to 17V/1A for Vigor2200,Vigor2200X and Vigor2200E be used in EU and China
- One AC/AC power adapter (black), AC100-230V, input AC 15 to 17V/1A for Vigor2200,Vigor2200X and Vigor2200E be used in Ireland and the UK
- One AC/AC power adapter (black), AC100-230V, input AC 15 to 17V/1A for Vigor2200,Vigor2200X and Vigor2200E be used in the America and Taiwan
- One AC/DC power adapter (black), AC100-240V, input DC5V/ 2.8A output for Vigor2200W be used in EU and China
- One AC/DC power adapter (black), AC100-240V, input DC5V/ 2.4A output for Vigor2200W be used in Ireland and the UK
- One AC/DC power adapter (black), AC100-240V, input DC5V/ 2.8A output for Vigor2200W be used in the America and Taiwan
- One Ethernet LAN cable (blue) for connection to a computer or hub

## 1.4 LED Indicators & Rear Panels

Each of the Vigor2200 series front and rear panel are different. The following sections describe the models individually.

### Vigor2200:




**LED Indicators**

There are eleven LEDs on the front panel; ACT, LNK, B1, B2, LNK, 100M, FDX, Broadband, LNK, TX, and Col.

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

**ISDN Group:**

**LNK** (Link)
ON when the ISDN network is correctly setup.

**Note:**
On some NT-1 boxes, the ISDN LNK LED will go OFF when the ISDN line has been idle for a while. When the router is dialling or answering a call, it should be ON again.

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

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

**LAN1 Group:**

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

**100M**
ON when the connected network card or hub support 100Mbps Fast Ethernet.

**FDX** (Full-Duplex)
ON when the connected network card or hub supports full-duplex transmission mode.

**LAN2 Group:**

**Broadband**
ON when broadband access is active.

**LNK** (Link)
ON when the connected network card or hub is connected.
Blinking when the LAN2(WAN) port receives packets.

**TX** (Transmit)
Blinks when the LAN2(WAN) port transmits data.

**Col** (Collision)
ON when there are collisions occurring on the LAN2(WAN) port.

**Rear Panel Description**

The Vigor2200 has a reset button, a power jack, and five RJ-45 ports on the rear panel:

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

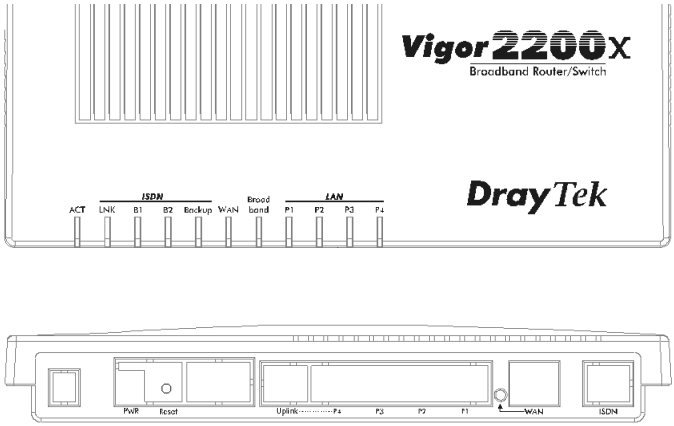
**Reset**
For firmware upgrades: Press and hold the button, then power ON. The ACT and LNK LEDs will blink simultaneously (see section 7.5).
To restore default settings: While the device is running, press the button and hold for more than five seconds. When the ACT LED begins to blink rapidly, release the Reset button. The router will restart with the default configuration.

**LAN2 ... WAN**
These ports are the same Ethernet port with a mutual crossover. Normally, the DSL/Cable modem should be connected to the WAN port.

**LAN1 ... Uplink**
These ports are the same Ethernet port with a mutual crossover. Normally, you should connect your PC to the LAN1 port and an Ethernet switch/hub to the Uplink port.

**ISDN**
Connects to a NT1 box provided by your ISDN service provider.

**Vigor2200X:**




**LED Indicators**

As shown above, there are 11 LEDs on the front panel. Reading from left to right, they are marked ACT, LNK, B1, B2, Backup, WAN, Broadband, P1, P2, P3 and P4. Their functions are as follows:

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

**ISDN Group:**

**LNK** (Link)
ON when the ISDN network is correctly setup.

> **Note:**
> For some NT-1 boxes, the ISDN LNK LED will go OFF when the ISDN line has been idle for a while. When the router is dialling or answering a call, it should be ON again.

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

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

**Backup**
ON when ISDN backup dial is active.

**WAN Group:**

**WAN**
ON when the WAN port is connected.

**Broadband**
ON when broadband access is active.

**P1, P2, P3, P4**
These indicators are dual-color LEDs: Yellow means the port is connected to a 10Mbps device, and Green indicates the connected device is 100Mbps.
ON when the connected network device has been linked up correctly.
Blinking when there are Ethernet packets passing through the switch port.

**Rear Panel Description**

The Vigor2200X has one reset button, one power jack and seven RJ-45 ports on the rear panel. Detailed descriptions are as follows:

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

**Reset**
For upgrading the firmware: Press the button and hold, then power ON. The ACT and LNK LEDs will blink simultaneously (see section 7.5).
To restore default settings: While the device is running, press the button and hold for more than five seconds. When the ACT LED begins to blink rapidly, release the Reset button. The router will restart with the default configuration.

**Uplink ... P4**
These ports are the same Ethernet port with a mutual crossover. Normally, the Uplink port should be connected to an external Ethernet switch/hub, the P4 port should be connected to your PC.

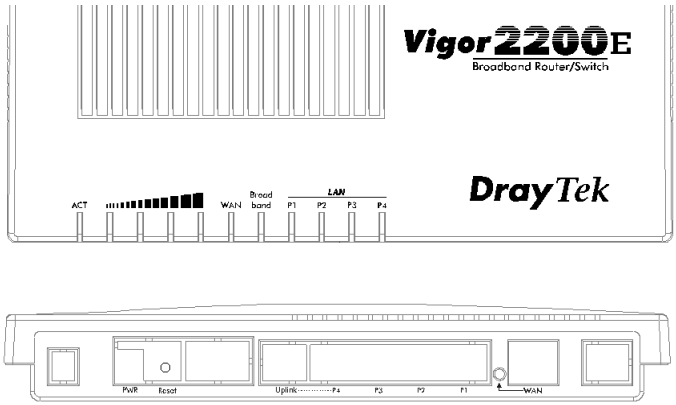
**P3, P2, P1**
These switch ports should be connected to your local PCs.

**WAN LED**
ON when the DSL/Cable modem is connected.
Blinking when data packets pass through the port.

**WAN**
This port should be connected to the Ethernet port of an external DSL/Cable modem.

**ISDN**
Connects to an NT1 box provided by your ISDN service provider.

## Vigor2200E:




### LED Indicators

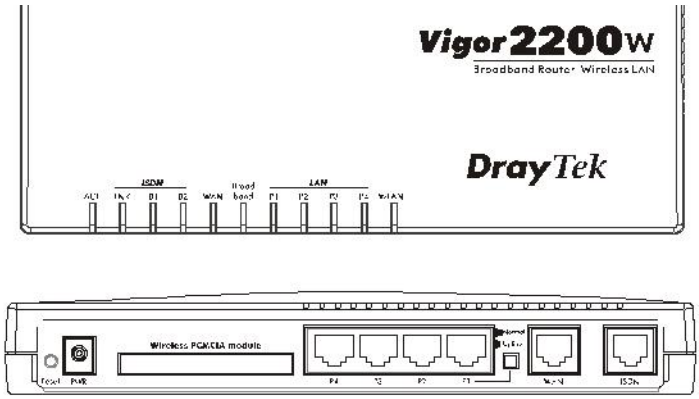
As shown above, there are 11 LEDs, reading from left to right, they are ACT, four bandwidth utilization bar LEDs for the WAN port, WAN, Broadband, P1, P2, P3 and P4. Most of the LEDs are the same as those of the Vigor2200X, except for the additional Bandwidth Utilization LEDs for the WAN port. The following describes only the difference.

There are four LEDs below the bandwidth utilization bar. From left to right they indicate bandwidth utilization, from low to high.

### Rear Panel Description

The Vigor2200E has no ISDN port, the rest of the rear panel is the same as that of the Vigor2200X.

**Vigor2200W:**




**LED Indicators**

As shown above, there are 11 LEDs on the front panel. Reading from left to right, they are marked ACT, LNK, B1, B2, WAN, Broadband, P1, P2, P3 and P4, WLAN. Their functions are as follows:

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

**ISDN Group:**

**LNK** (Link)
ON when the ISDN network is correctly setup.

> **Note:**
> For some NT-1 boxes, the ISDN LNK LED will go OFF when the ISDN line has been idle for a while. When the router is dialling or answering a call, it should be ON again.

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

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

**Backup**
ON when ISDN backup dial is active.

**WAN Group:**

**WAN LED**
ON when the DSL/Cable modem is connected.
Blinking when data packets pass through the port.

**Broadband**
ON when broadband access is active.

**P1, P2, P3, P4**
These indicators are dual-color LEDs: Yellow means the port is connected to a 10Mbps device, and Green indicates the connected device is 100Mbps.
ON when the connected network device has been linked up correctly.
Blinking when there are Ethernet packets passing through the switch port.

**WLAN**
On when there is wireless PCMCIA card on Vigor2200W. Blinking when there are data packets transmissing in and out the wireless access point.

**Rear Panel Description**
The Vigor2200W has one reset button, one power jack and seven RJ-45 ports on the rear panel. Detailed descriptions are as follows:

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

**Reset**
For upgrading the firmware: Press the button and hold, then power ON. The ACT and LNK LEDs will blink simultaneously (see section 7.5).
To restore default settings: While the device is running, press the button and hold for more than five seconds. When the ACT LED begins to blink rapidly, release the Reset button. The router will restart with the default configuration.

**Uplink ... P4**
These ports are the same Ethernet port with a mutual crossover. Normally, the Uplink port should be connected to an external Ethernet switch/hub, the P4 port should be connected to your PC.

**P3, P2, P1**
These switch ports should be connected to your local PCs.

**Wireless PCMCIA module**
The DrayTek Vigor wireless PCMCIA should be connected to the wireless PCMCIA module for wireless LAN access.

Please only insert the Vigor wireless PCMCIA into the wireless PCMCIA module of Vigor2200W. In principle, the IEEE802.11b wireless LAN adapter for wireless terminals can work with wireless LAN access point of Vigor2200W. For detailed interoperability concern and procurement of wireless LAN adapter for wireless terminal, please contact your dealers or DrayTek support @draytek.com.tw .

**ISDN**
Connects to an NT1 box provided by your ISDN service provider.

## 1.5 Key Features

The Vigor2200 Routers provide many built-in server and software features to provide a convenient comprehensive solution for your SOHO network.

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

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

3. **Web (HTTP) Server**: A Web browser is the most common tool used to surf the Internet. You may use Microsoft's **Internet Explorer** or **Netscape's** browser etc, to configure the Vigor2200 series routers as easily as surfing a website.

4. **Virtual TA Server (VTA)**: The terminology Virtual TA" means the Vigor2200 and Vigor2200X can operate as traditional ISDN TA' s 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. Vigor2200 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 of domain names and IP addresses. The proxy also remembers DNS query packets sent through the router and saves them into its own DNS cache. For enhanced speed, when a DNS query packet enters the 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 umatched 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) Client on WAN Port**: In most cable modem environments, the Vigor2200 series supports a DHCP client on the WAN port. They can automatically get IP network settings from a cable head-end access server.

10. **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.

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

12. **Point-to-Point Protocol 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-Point Tunnelling Protocol (PPTP) Client Support**:

Some DSL modems (e.g. Alcatel modems), only provide a PPTP local connection for an end user computer. The Vigor2200 series 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 client driver on your computers.

14. **Firewall**: In addition to the built-in NAT mechanism, the Vigor2200 series 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, or ISDN or DSL WAN interface.

17. **Wireless LAN Access Point**: enables high mobility of several simultaneous users accessing all LAN facilities just like on a wired LAN as well as Internet and WAN access.

18. **Wired Equivalent Privacy (WEP)**: The wireless terminals that obtains a proper security key can be allowed to access the network.

19. **VPN(Virtual Private Network) with IPSec encryption**: enables linking of remote Networks via the Internet through authenticated and secure tunnels.

# 2 Installation & Setup


2.1 Before you Begin

2.2 Hardware Installation

2.3 Setting up a Management PC

2.4 Using the Smart Start Wizard

2.5 Using the Web Configurator

## 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 telcom. 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 telcom. Also, make sure an ISDN line is available (only applies to the Vigor2200, Vigor2200X and Vigor2200W).

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

4. Locate the device in a clean location. Do not block the ventilation 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 are an S/T-interface user, don't extend the ISDN line greater than 100 meters from the NT-1 (NT-1 plus) box and the router (only for Vigor2200,Vigor2200X and Vigor2200W).

7. If you are a DSL/Cable user, check that your 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 setting of the router as shown on the next page:

**Factory Default Settings:**

**Default IP Network Settings of Router:**

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

**DHCP Server:** Enabled

Start IP Address: 192.168.1.10

IP Pool Counts: 50

**Web Configurator:**

Username: admin

Password: <blank>

Note: Blank means no password required.

**Telnet Console:**

Password: <blank>

Note: Blank means no password required.

**Management from the Internet:**

Not allow.

The following items apply only to the Vigor2200, Vigor2200X and Vigor2200W.

**Virtual TA Server**: Enabled

**Remote Dial-In Server:** Disabled

Assigned IP Address: 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 a PC:

1. Attach the Ethernet cable (blue color cable) to the LAN 1 port (Vigor2200) or to any P1 ~ P4 port (Vigor2200X, Vigor2200w, and Vigor2200E).

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

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

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

B. Connecting to an External Ethernet Hub or Switch:

1. Attach the Ethernet cable (blue color cable) to 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.

### 2.2.3 Connecting to an ISDN BRI Line (Vigor2200, Vigor2200X and Vigor2200W only)

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, ATMF-25 are not supported.

1. Locate your Ethernet cable (should be provided by your ISP or telcom).

2. Attach the Ethernet cable to the Ethernet port of the DSL/ Cable modem.

3. Plug the other end of the cable into the **WAN** port.

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

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

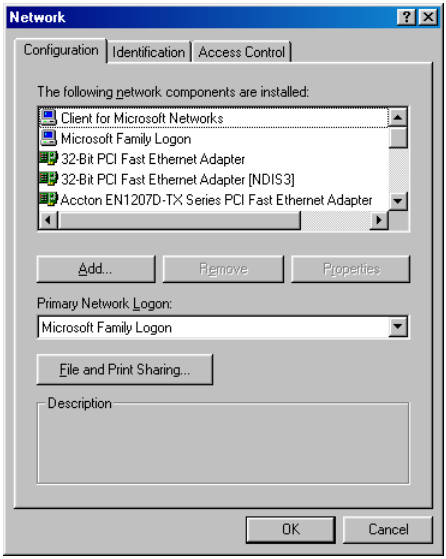
For a dynamic IP address, you need to set the PC as a DHCP client, and then restart or renew the network settings. The DHCP server of router is enabled by default so the PC will then be assigned an IP address and related settings by the router.

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

### 2.3.1 Checking the Network IP Configuration

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

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



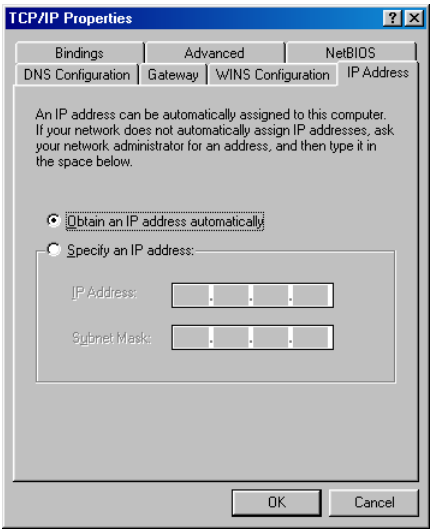

Your particular system will be different from the screen shown here. Check that you have an Ethernet network card installed. If not, refer to the card manufacturers documentation and install the card and drivers.

If your card is installed,

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

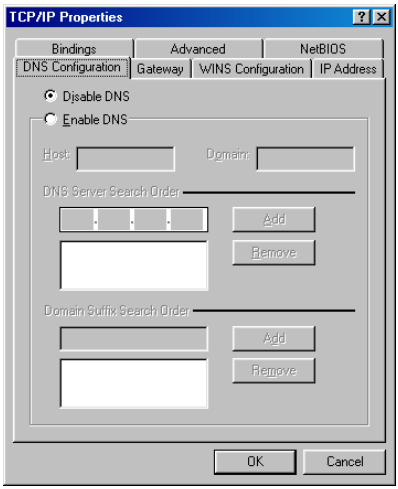
### 2.3.2 Configuring the TCP/IP Protocol

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

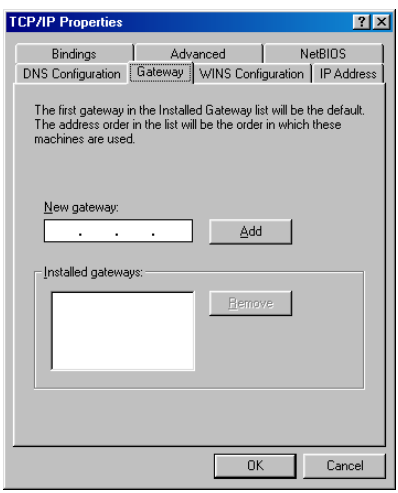



2. On the IP Address tab, click **Obtain an IP address automatically.** As the DHCP (Dynamic Host Configuration Protocol) server built into the router is enabled by default, your computer will get an IP address, subnet mask, and other related IP network settings from the router.

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



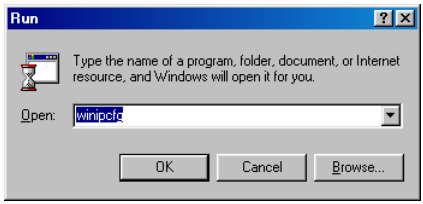

4. Click the **Gateway** tab.

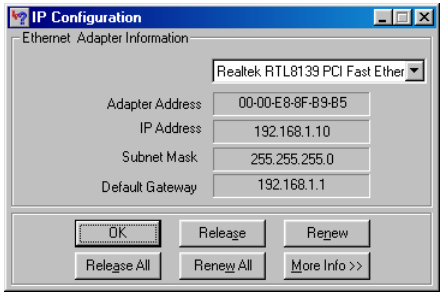


5. Make the **New gateway** and **Installed gateways** fields blank and click **OK.** A dialog box will pop up asking you to restart the PC. Click **Yes**".

### 2.3.3 Checking TCP/IP settings

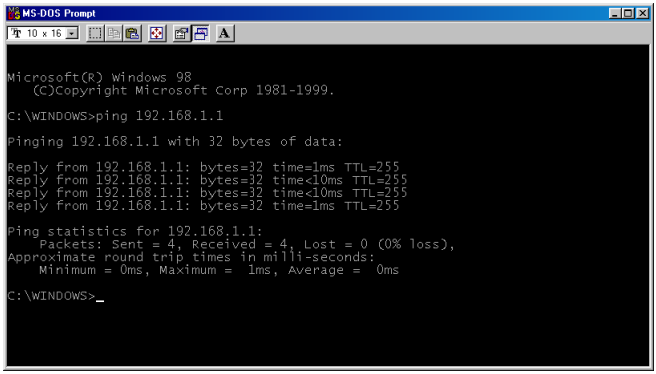
1. After completing the previous steps, click **Start** -> **Run** -> and type **winipcfg**. The **IP Configuration** window will open. If the PC does not show an IP address in the **192.168.1.2** to **192.168.1.254** range, click the **Release** button to release the current configuration. Wait a few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




2. If the IP configuration is correct, you will be able to use the PING diagnostic utility built into Microsoft Windows to ping the router. Click **Start** -> **Programs** -> **MS-DOS Prompt**. A a command mode window will open. Type "**ping 192.168.1.1**" (default IP of the router) to check the network connectivity. If both hardware and software are correct, your computer will receive a response from the router as shown on the next page. If

not, verify that the Ethernet cable is connected to the router properly and the Ethernet port LED on the front panel is lit.



## 2.4 Using the Smart Start Wizard

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

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

### Installing the Router Tools

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

**Note:**

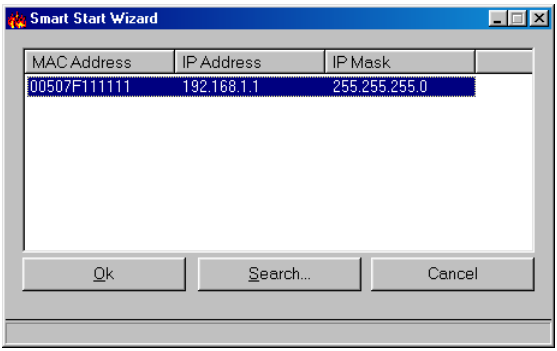
If auto-run fails to start the installation program. Click autostart.exe on the root directory of the CD to start the program.

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

### Using the Wizard

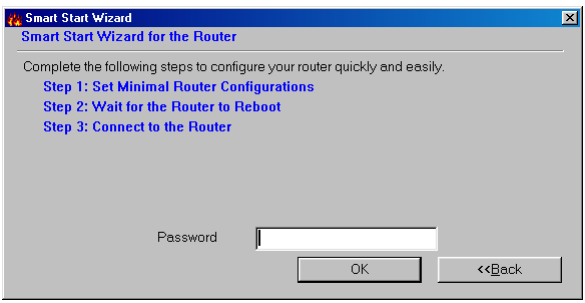
1. Click **Start** ->**Programs** -> **Router Tools**-> **Smart Start Wizard**" .

The following screen will open.

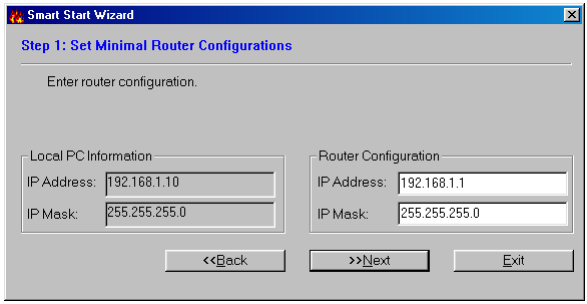



2. Click **Search** to find the router on your network.

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

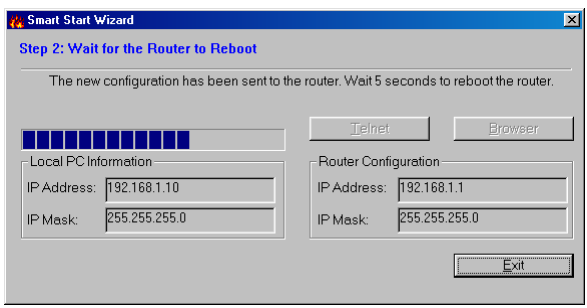



3. If this is a first time setup of the router, do not enter a password. Click **OK** to go to next screen.

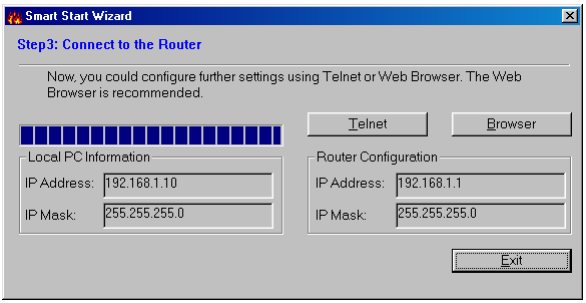



The screen shows read-only IP and IP mask settings for the PC you are using, and also the **IP Address** and **IP Mask** settings for the router. Here you may change the router settings to match your current network environment, or keep the default settings.

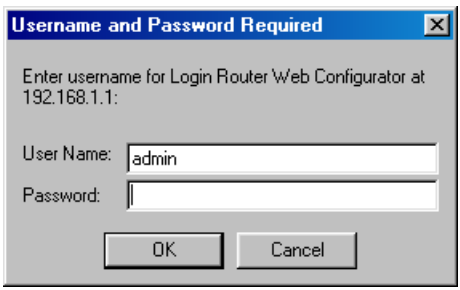
4. Click **Next** to update the settings to the router.



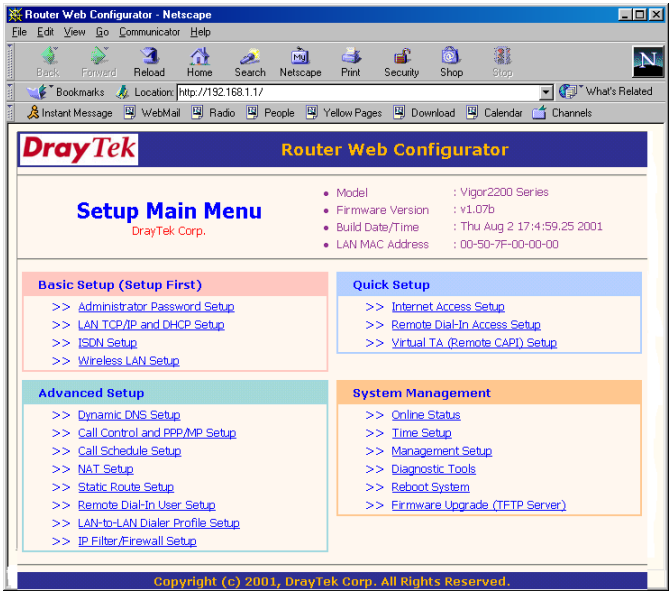

5. Wait for a few seconds. The **Telnet** and the **Browser** buttons will become active (see the next page).




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



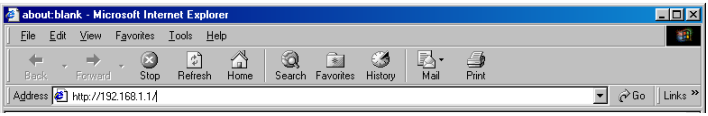

Enter **admin** as the User Name and leave the Password field blank. The Web Configurator will open. In the following examples we use the Netscape™ web browser (see the next page).


Router Web Configurator - 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 : Vigor2200 Series
Firmware Version : v1.07b
Build Date/Time : Thu Aug 2 17:4:59.25 2001
LAN MAC Address : 00-50-7F-00-00-00
Basic Setup (Setup First)
>> Administrator Password Setup
>> LAN TCP/IP and DHCP Setup
>> ISDN Setup
>> Wireless LAN Setup
Quick Setup
>> Internet Access Setup
>> Remote Dial-In Access Setup
>> Virtual TA (Remote CAPI) Setup
Advanced Setup
>> Dynamic DNS Setup
>> Call Control and PPP/MP Setup
>> Call Schedule 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
>> Time Setup
>> Management Setup
>> Diagnostic Tools
>> Reboot System
>> Firmware Upgrade (TFTP Server)
Copyright (c) 2001, DrayTek Corp. All Rights Reserved.

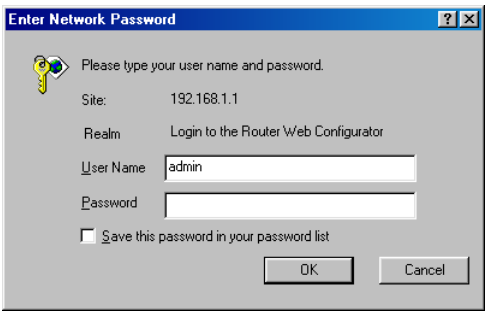
## 2.5 Using the Web Configurator

### 2.5.1 Connecting to the Web Configurator via a Web Browser

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

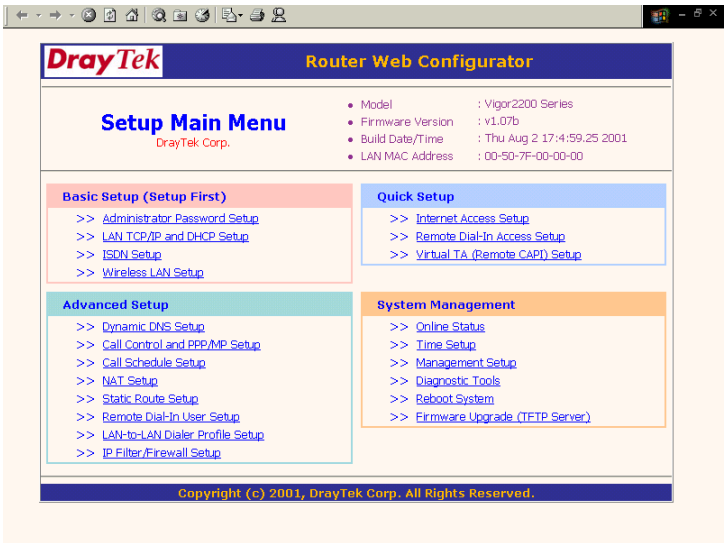



2. An authentication dialog box will open.




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

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




### 2.5.2 Overview of the Web Configurator

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

**Basic Setup (Setup First):**

1. Administrator Password Setup:

   Sets/changes the administrator password.

2. LAN1 TCP/IP and DHCP Setup:

   Modifies the IP address and DHCP server settings of the router.

3. ISDN Setup: (Vigor2200, Vigor2200X, and Vigor2200W)

   ISDN users need to select a country code. Sets 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: (Vigor2200,Vigor2200X, Vigor2200W)

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

3.Virtual TA (Remote CAPI) Setup:(Vigor2200, Vigor2200X,Vigor2200W)

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 (Vigor2200, Vigor2200X,Vigor2200W)

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, DMZ 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 (Vigor2200, Vigor2200X, Vigor2200W)

The Vigor2200 and Vigor2200X support 10 remote dial-in accounts for remote access applications. You can manage these dial-in accounts from this menu.

5. LAN-to-LAN Dialer Profile Setup (Vigor2200, Vigor2200X, Vigor2200W)

The LAN-to-LAN Dialer Profile differs from the 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 system's current online status and statistics.

2. Management Setup

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

3. Diagnostic Tools

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

4. Reboot System

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

5. Firmware Upgrade (TFTP Server)

Enables the TFTP server for firmware upgrades.

**Note:**
1. 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.
2. The Vigor2200E model does not have an ISDN BRI interface. Therefore, ISDN-related features and functions are not available and some setup menus will not appear.

# 3 Basic Setup & Internet Access


3.1 Basic Setup

3.2 Wireless LAN Setup

3.3 Internet Access Setup

3.4 ISDN Dial-up Internet Access

3.5 DSL/Cable Modem 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).

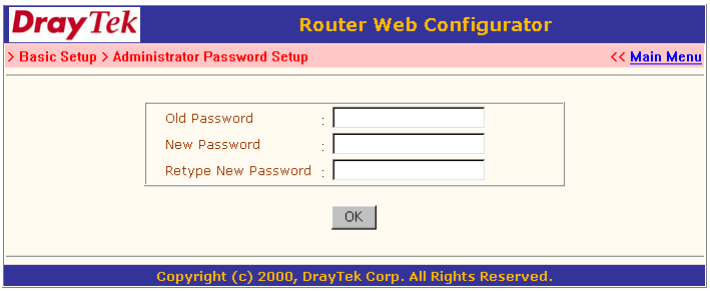
## 3.1 Basic Setup (Setup First)

This group includes **Administrator Password Setup**, **LAN 1 TCP/IP and DHCP Setup** and **ISDN Setup**. The Vigor2200E model does not offer an ISDN interface and therefore does not have the **ISDN Setup** menu.

### 3.1.1 Changing the Administrator Password

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

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



**Old Password:**

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

**New Password:**

Enter an administrator password.

**Retype New Password:**

Type the password again for confirmation.

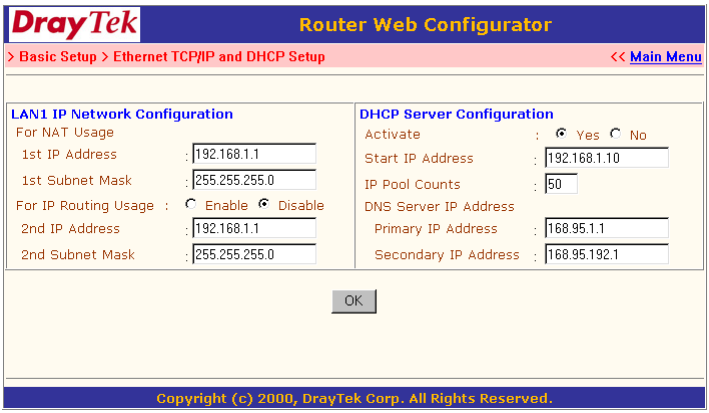
Click **OK**".

### 3.1.2 Configuring LAN 1 IP Address and DHCP Server

Each of the Vigor2200 series routers has two Ethernet interfaces, one is for connecting to local network users, the other is for connecting to an external broadband device (i.e. DSL modem/router or Cable modem). The LAN1 port is connected to the local Ethernet network. LAN 2 (WAN) is connected to the external broadband device.

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

For example, for some ISDN accounts, 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 IP addresses of the users will be translated to the 2nd IP address by the router and sent out via ISDN.




## LAN 1 IP Network Configuration

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

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

**For IP Routing Usage:** (Default: Disable).

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

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

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

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

## DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. It can automatically dispatch related IP settings to any local user configured as a DHCP client. The DHCP server supports up to 253 users (PCs) on

the local network.

**Activate:** (Default: Yes).

**Yes:** Enables the DHCP server.

**No:** Disables the DHCP server.

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

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

**DNS Server IP Address:** (Default: None).

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

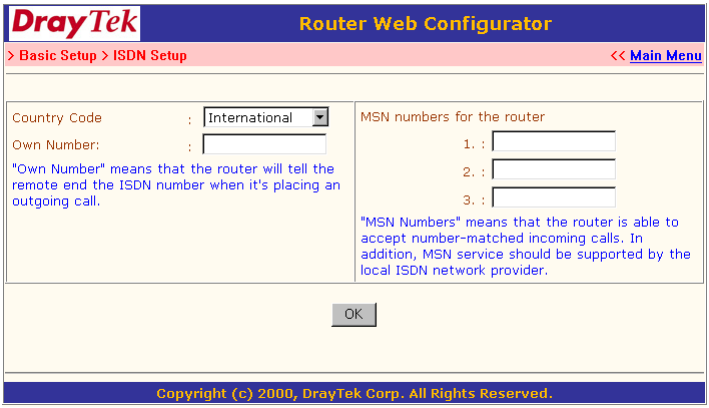
**Primary IP Address:** Sets the IP address of the primary DNS server.

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

**Note:**

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

### 3.1.3 Configuring the ISDN Interface




This setup page is present in the Vigor2200 and Vigor2200X, absent in the Vigro2200E.

**Country Code:**

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

**Own Number:**

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

**MSN Numbers for the Router:**

**MSN Numbers** means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by local ISDN network provider. The router provides three MSN number fields. Note that MSN services must be subscribed for from your local telecom.
By default, MSN function is disabled. Leave the MSN number fields blank, under which all incoming calls will be accepted

without number-matching.

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

## 3.2 Wireless LAN Setup

The Vigor Wireless Router is equipped with a wireless LAN interface compliant with the 11Mbps IEEE 802.11b protocol. The features of wireless LAN capability enable high mobility of several simultaneous users accessing all LAN facilities just like on a wired LAN as well as Internet and WAN access.

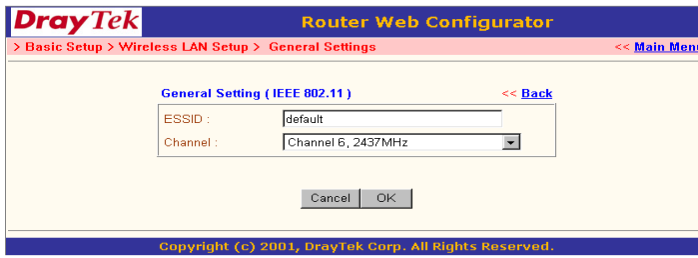
Caution:Before connnecting a wireless LAN access device, you need to install PCMCIA card(1 year warranty) in the Vigor2200W. The card for Vigor2200W is not hot plugable be sure to remove the power before installing the PCMCIA card. Only the DrayTek PCMCIA card is compatible with Vigor2200W, other types of PCMCIA card may cause permanent damage of Vigor2200W. The damage would not be covered by the 2 year warranty.

### 3.2.1 General Settings:

**ESSID:** You should set the ESSID same as your note book PC wireless card to allowed the client PC to access the network via this device. The default ESSID is "**default**".

**Channel:**To select a channel for Vigor2200W, The default channel is 6.

.



### 3.2.2 WEP Settings:

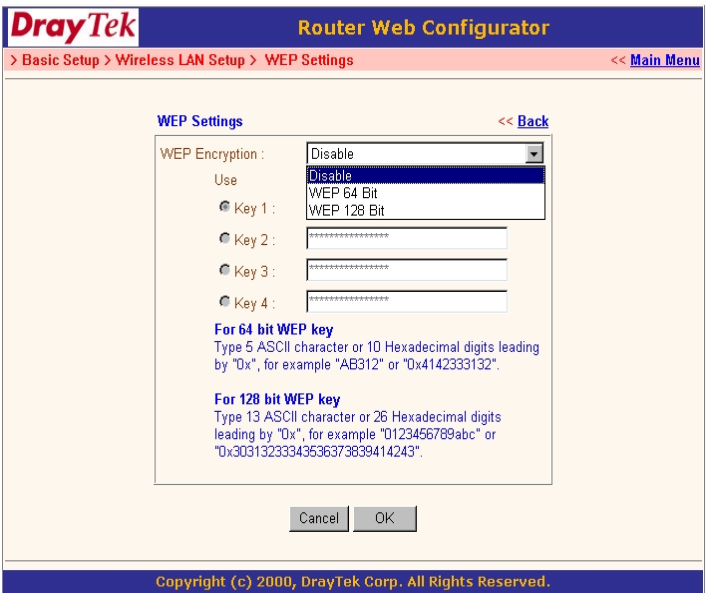
**WEP Encryption:** To improve the security and privacy of your wireless data packets the WEP encryption feature can be used. The WEP encrypts each frame transmited from the radio using one of the keys entered from this panel. WEP encryption can be enabled by selecting 64 bits or 128 bits from pull down menu.

There are 4 key sets can be entered and only one key can be selected. The key can be enterd by ASCII or Hexadecimal.For 64bits WEP key,either 5 Ascii character or 10 hexadecimal digitals leading by **0x** can be entered**.**

For example **ABCDE** or **0x4142434445.**

For 128bits 13 Ascii character or 26 hexadecimal digits leading by **0x** can be entered. For example,

**ABCDEFGHIJKLM** or **0x41424344454647484 94A4B4C4D.**



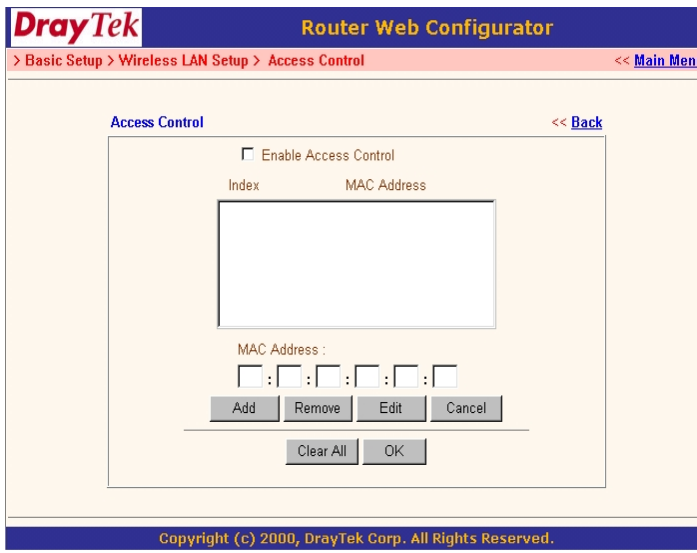
## 3.2.3 Access Control

For additional security of wireless access,Vigor2200W allows users to control the client MAC address. Only the valid MAC address which has been configured can then access the network.

**Enable Access Control:**pick up the **enable Access Control** to enable the MAC Address access control feature.
**MAC Address:** key in specific MAC Address to allow the client to access the network.
**ADD:** add a MAC Address
**Remove:** remove the selected MAC Address

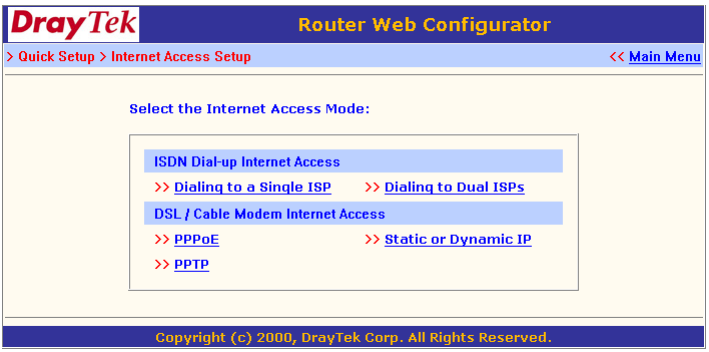
**Edit:** edit a MAC Address

**Cancel:** cancel a MAC Address setup
**Clean All:** clean all setups on MAC Address
**OK:** save all the MAC Address settings on Vigor2200W



### 3.3 Internet Access Setup

For most users, Internet access is the primary application. The Vigor2200, Vigor2200X and Vigor2200W support the ISDN WAN interface for Internet access and remote access. The following sections will explain more details of ISDN dial-up access and broadband access setup. When you click **Internet Access Setup**" from within the **Quick Setup** group, the following setup page will be shown.




Five methods are available for Internet Access.

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

**Dialing to Dual ISPs:** If you have more than one ISP, click here to set two ISP dialup profiles. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs that do not support Multiple-Link PPP (ML-PPP). In such cases

dialing to two ISPs can increase the bandwidth utilization of the ISDN line to 128kbps data speed.

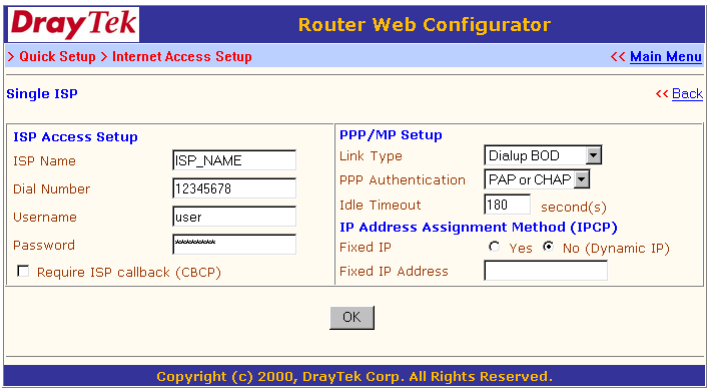
**PPPoE:** This is for most DSL modem users. All local users can share one PPPoE connection to access the Internet.

**PPTP:** Some DSL services 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 or Dynamic IP:** On this page you configure the LAN2/WAN interface to use a static (fixed) IP or dynamic (DHCP client) IP address. Most cable users will use the dynamic IP address mode to get a globally reachable IP address from the cable head-end system.

## 3.4 ISDN Dialup Internet Access

### 3.4.1 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

Disables the ISDN dial-out function.

Dialup 64Kbps

Uses one ISDN B channel for Internet access.

Dialup 128Kbps

Uses 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 dialled automatically. For more detailed BOD parameter settings, refer to the **Advanced Setup** group > **Call Control and PPP/MP Setup**.

**PPP Authentication:**

PAP Only

Sets 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.

**Idle Timeout:**

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

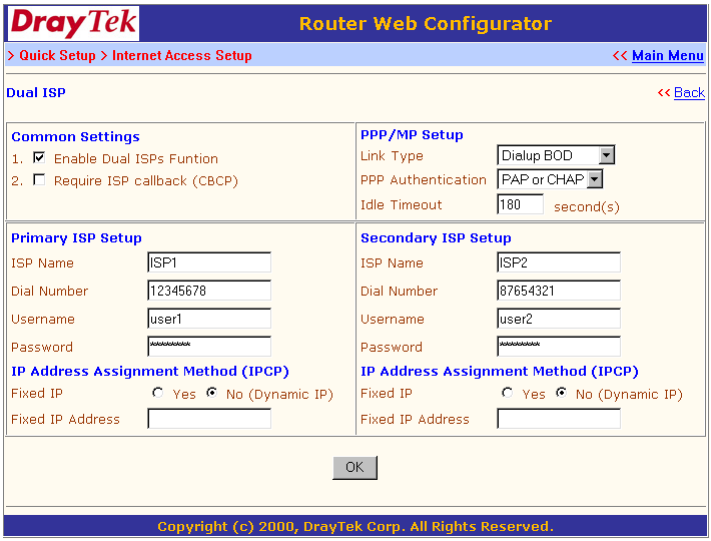
**IP Address Assignment Method (IPCP)**

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

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

Click “**OK**”.

### 3.4.2 Connecting to Dual ISPs




Most configuration parameters are the same as that in the 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.

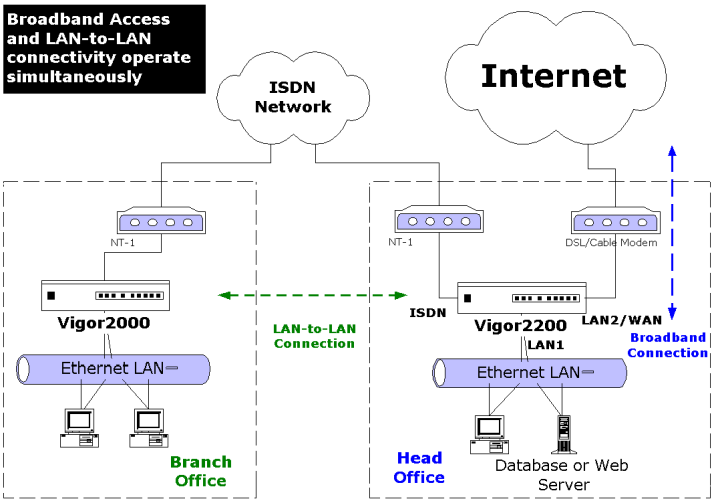
## 3.5 DSL/Cable Modem Internet Access

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.

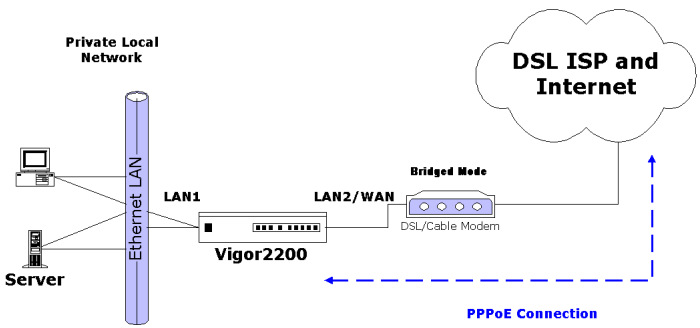
The following sections deal with four widely-used broadband access services. These are **PPPoE Client, PPTP Client** and **Static IP** for DSL, and **Dynamic IP (DHCP Client)** for Cable. In most cases, you will get a DSL or Cable modem from the broadband access service provider. The router is connected behind the broadband device (i.e. DSL/Cable modem) and works as a NAT or IP router for broadband 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 scenarios show that the head office is capable of getting on to the Internet through the Vigor2200 and a broadband device, and simultaneously connecting to the branch office via an ISDN network.

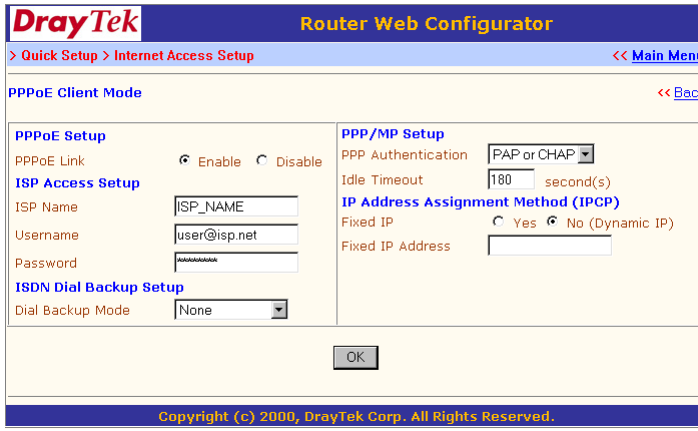
**Note:**
On the Vigor2200E the ISDN dial backup function, remote access, and LAN-to-LAN connectivity are not supported.




### 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 on the LAN2 interface.

### 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

This item will be described in more detail in section 3.4.5.

### 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.

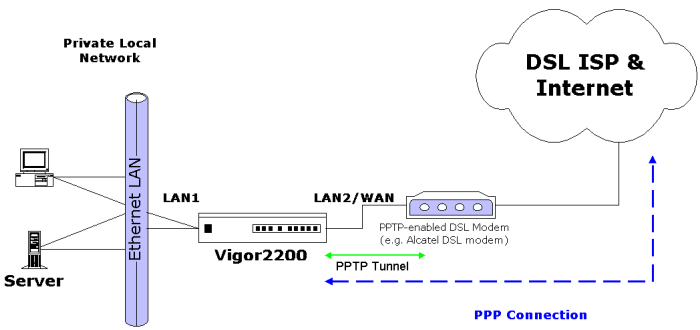
**IP Address Assignment Method (IPCP)**

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

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

Click **OK**.

### 3.5.2 Using PPTP with a DSL Modem

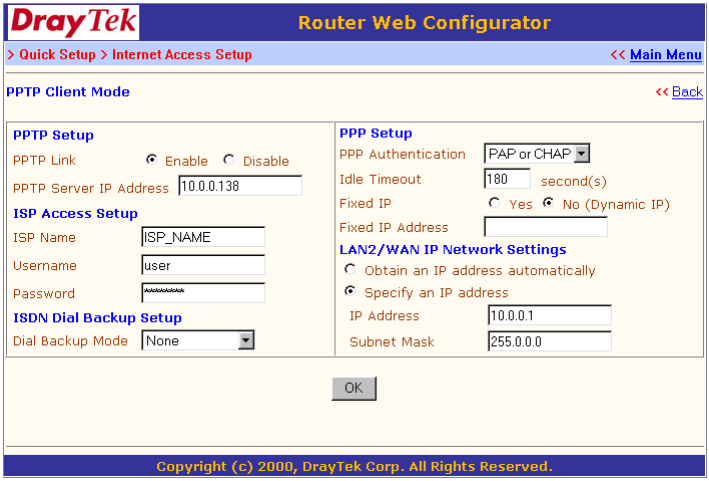



Click "**Internet Access Setup**" > "**PPTP**" to enter the setup page. The following setup page is just for example. The exact settings should be provided by your DSL service povider.

**PPTP Setup**

**PPTP Link:** Check **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the LAN2 interface.

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




### ISP Access Setup

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

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

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

### ISDN Dial Backup Setup

This item will be described in more detail in section 3.4.5.

### 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.

**IP Address Assignment Method (IPCP)**

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

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

**LAN2/WAN IP Network Settings**

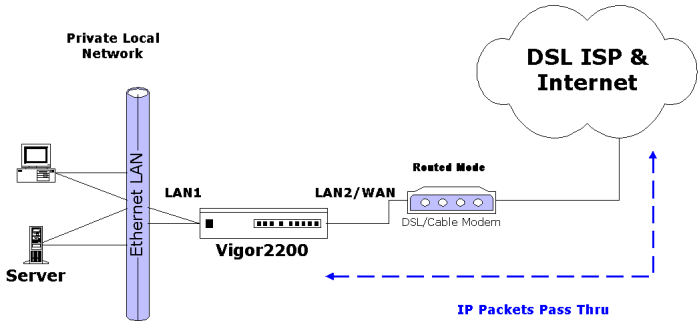
**Obtain an IP address automatically:** Sets the LAN2/WAN interface as a DHCP client that will ask for the IP network settings from the DHCP server or PPTP-enabled DSL modem.

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

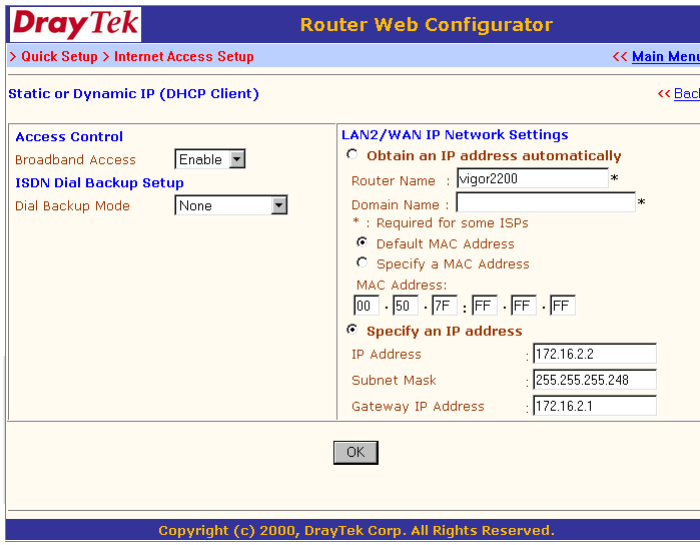
Click **OK**.

### 3.5.3 Using a Static IP with a DSL/Cable Modem

In this application, 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. If you have a public subnet, you should choose an IP address to assign to the LAN2/WAN interface.




Click **Internet Access Setup** > **Static or Dynamic IP** to enter the setup page.



**Access Control**

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

**ISDN DIAL Backup Setup**

This item will be described in more detail in section 3.4.5

**LAN2/WAN IP Network Settings**

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

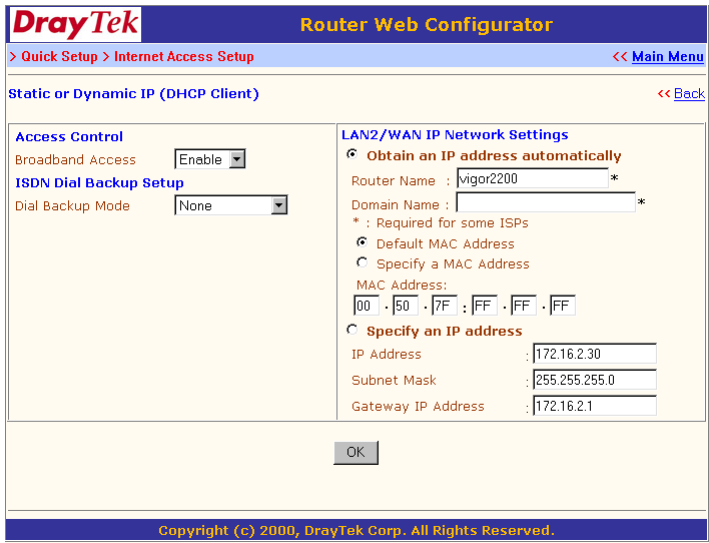
Click **OK**.

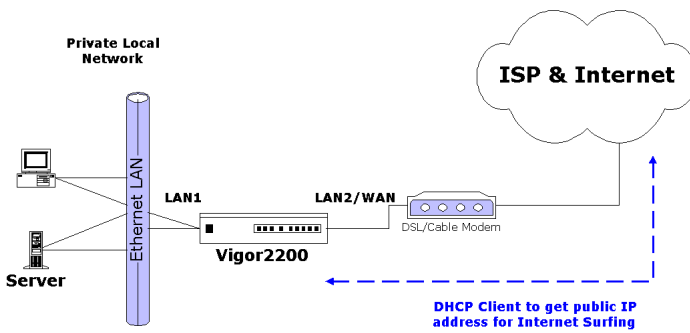
**Note:**

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

### 3.5.4 Using a Dynamic IP (DHCP Client) with a Cable Modem

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


DrayTek
Router Web Configurator
> Quick Setup > Internet Access Setup
<< Main Menu
Static or Dynamic IP (DHCP Client)
<< Back
Access Control
Broadband Access
Enable
ISDN Dial Backup Setup
Dial Backup Mode
None
LAN2/WAN IP Network Settings
Obtain an IP address automatically
Router Name : vigor2200 *
Domain Name : *
* : Required for some ISPs
Default MAC Address
Specify a MAC Address
MAC Address:
00 . 50 . 7F : FF . FF . FF
Specify an IP address
IP Address : 172.16.2.30
Subnet Mask : 255.255.255.0
Gateway IP Address : 172.16.2.1
OK
Copyright (c) 2000, DrayTek Corp. All Rights Reserved.


Private Local Network
ISP & Internet
Ethernet LAN
LAN1
LAN2/WAN
DSL/Cable Modem
Vigor2200
Server
DHCP Client to get public IP address for Internet Surfing

**Access Control**

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

**ISDN Dial Backup Setup**

This item is described in more detail in section 3.4.5

**LAN2/WAN IP Network Settings**

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

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

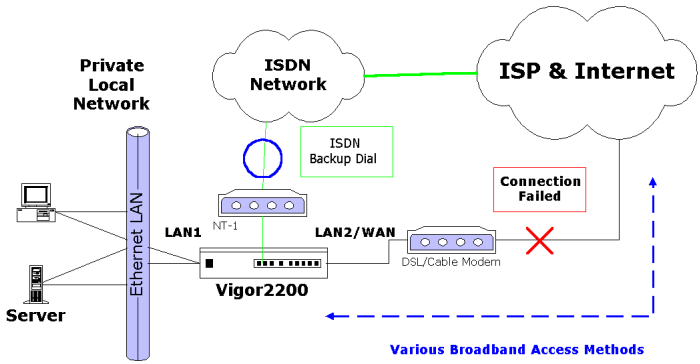
**Domain Name:** Depending on your Cable ISP this field may or may not be left blank.

**Default MAC Address & Specify a MAC Address:** These two options are mutually exclusive. Some Cable ISPs use a specific MAC address for access authentication. In such cases you need to check the **Specify a MAC Address** box and enter the MAC address in the MAC Address fields. The Default MAC Address of the router is the MAC address assigned by DrayTek.

Click **OK** and restart the router to allow the settings to take affect.

**Note:**
In the most cases, the only setting you need make is to check **Obtain an IP address automatically**".

### 3.5.5 Configuring ISDN Dial Backup




As the Vigor2200E has no ISDN interface, it does not support the ISDN dial backup function. Therefore, the following setup options will not be available for this model.

**ISDN Dial Backup Setup**

**Dial Backup Mode:**

None:

Disables the backup function.

Packet Trigger:

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

Always On:

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

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

# 4 Remote Access

4.1 Introduction to Remote Access
4.2 Remote Dial-in Access
4.3 LAN-to-LAN Access

This chapter explains the capabilities of remote access on the Vigor2200 series routers. Use the following setup links on the Setup Main Menu to setup remote access functions.

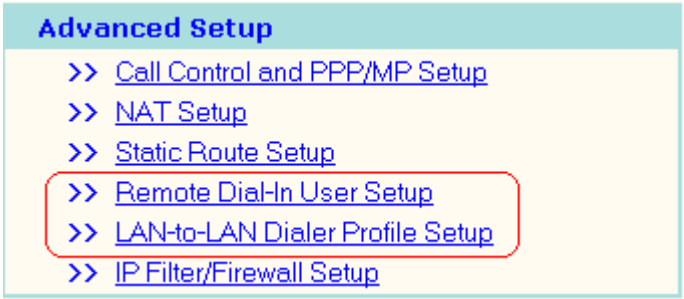
**Quick Setup**

**> Remote Dial-In Access Setup**

**Advanced Setup**

**> Remote Dial-In User Setup**

**> LAN-to-LAN Dialer Profile Setup**



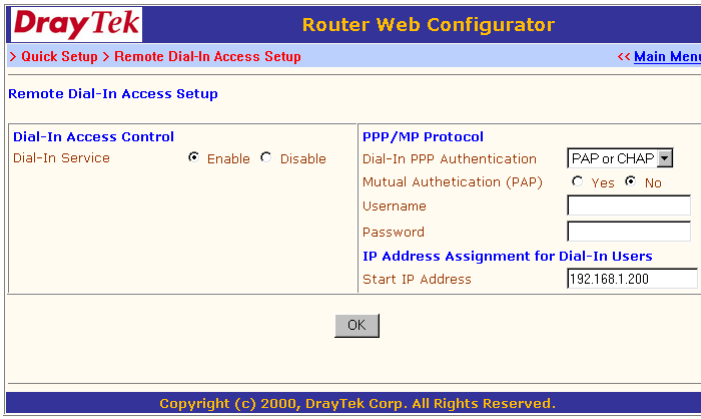
## 4.1 Introduction to Remote Access

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 to share the network resources of the local network, or to surf the Internet via a broadband device connected to the LAN2/WAN port. 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**

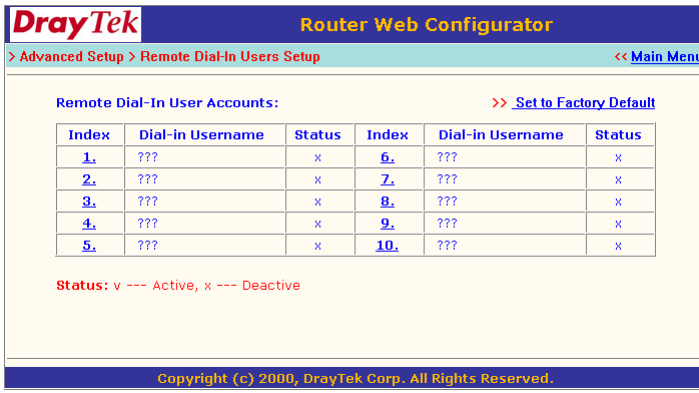
**Start IP Address:** Enter a start IP address to be assigned to the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 to be the Start IP Address.

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, 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 account 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.



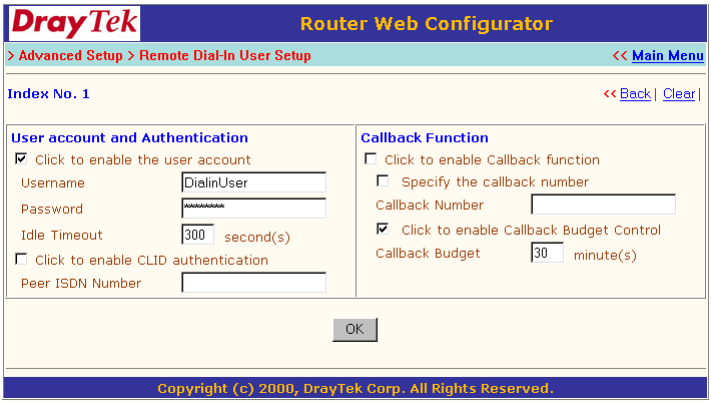

**Set to Factory Default:** Clicking here will clear all dial-in user accounts.

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

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

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

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




## User Account and Authentication

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

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

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

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

**Check 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.

**Check to enable the Callback function:** Enables the callback function.

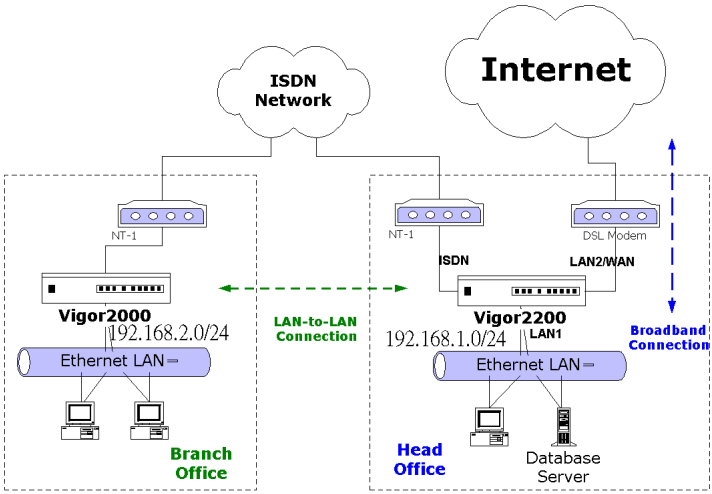
**Specify the callback number:** The option is for extra security. Once enabled, the router will only call back to the specified ISDN number defined in the next parameter, Callback Number.

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

**Check to enable Callback Budget Control:** By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.

**Callback Budget (Unit: minutes):** Specifies the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

## 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 192.168.1.0/24 is located at head office, the off-site branch office's network is 192.168.2.0/24.

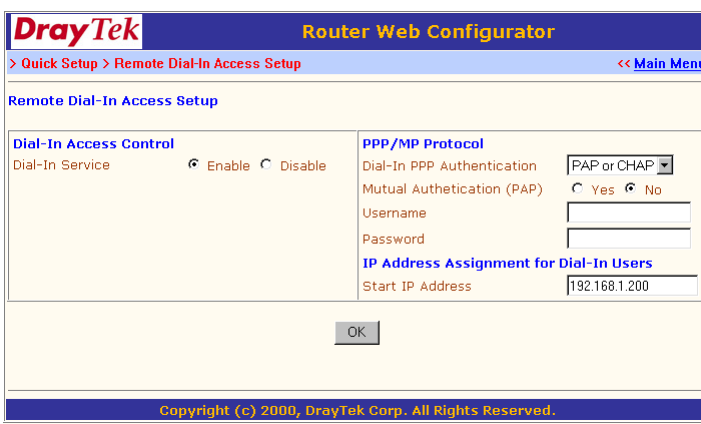
Before you begin to setup a LAN-to-LAN profile for each network, you should gather the information shown in the following table.

| | 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<br>PW: head | UN: branch<br>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:**

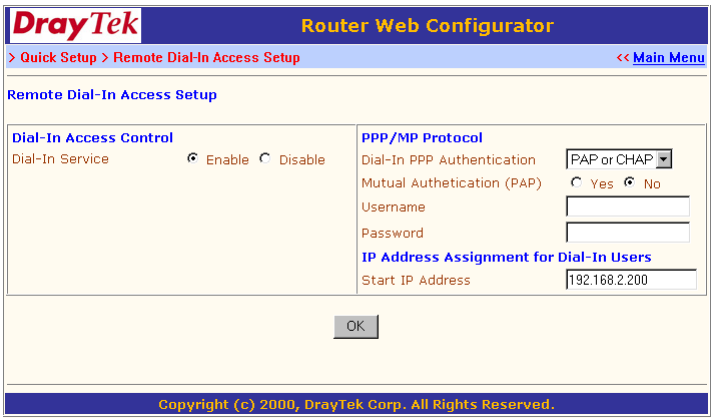


Because the network of the Head Office is 192.168.1.0/24, the settings should be as below:

**Dial-In Service:** Enable

**Start IP Address:** 192.168.1.200

**Branch Office:**



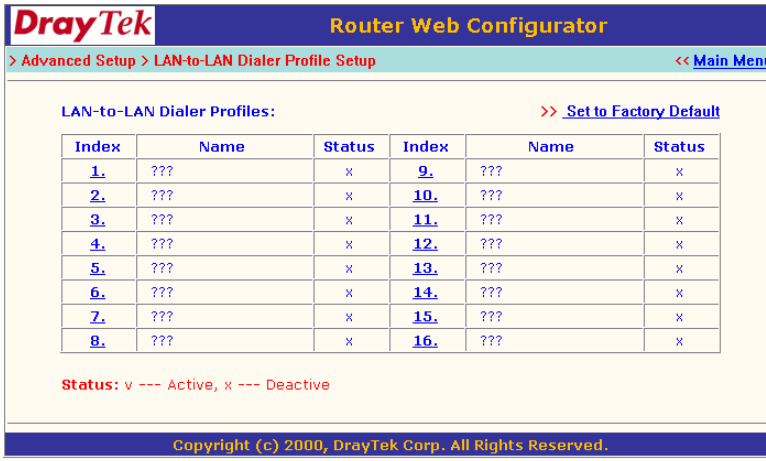

Because the Branch Office's network is 192.168.2.0/24, the settings should be as below:

**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. Click **LAN-to-LAN Dialer Profile** on the Setup Main Menu to enter the setup page.




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

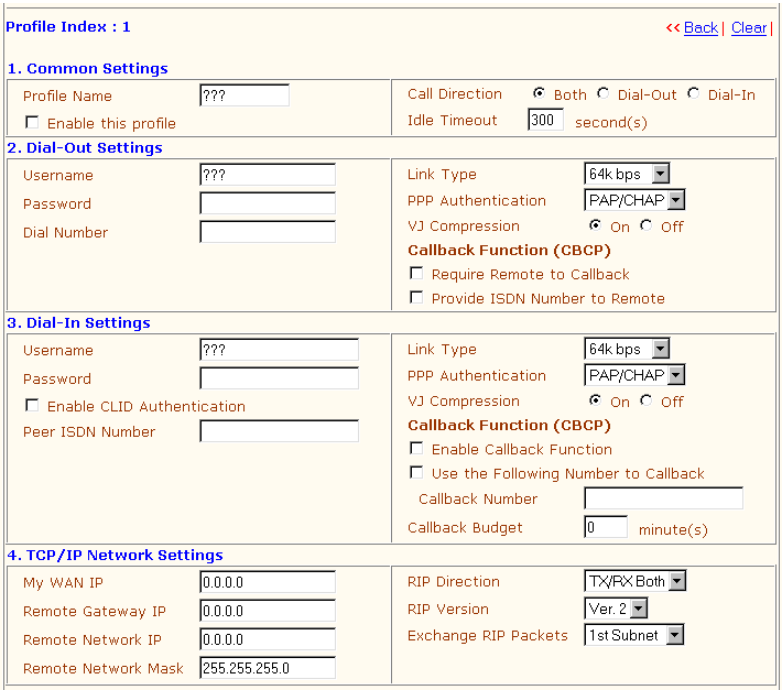
**Set to Factory Default:** Clicking here will clear all the LAN-to-LAN profiles.

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

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

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

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




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

**Common Settings**

**Profile Name:** Specifies a name for the remote network.

**Enable this profile:** Check here to activate this profile.

**Call Direction:** Specifies the call direction for this profile. **Both**

means it can be used for outgoing and incoming access. **Dial-Out** means it can only be used for outgoing access. **Dial-In** allows only incoming access.

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

**Dial-Out Settings**

**Username:** Specifies a username for authentication by the remote router.

**Password:** Specifies a password for authentication by the remote router.

**Dial Number:** Specifies the destination ISDN number for dialup.

**Link Type:** Indicates the dial-out link type.

Disable: Deactivates the dial-out action.

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

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

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

**PPP Authentication:** Specifies 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 which is part 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.

**Dial-In Settings**

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

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

**Enable CLID Authentication:** Limits the dial-in router to calling from a specific ISDN number.

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

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

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

**Callback Function (CBCP)**

**Enable Callback Function:** Checking here allows this router to accept requests from a remote router for call back.

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

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

**TCP/IP Network Settings**

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.

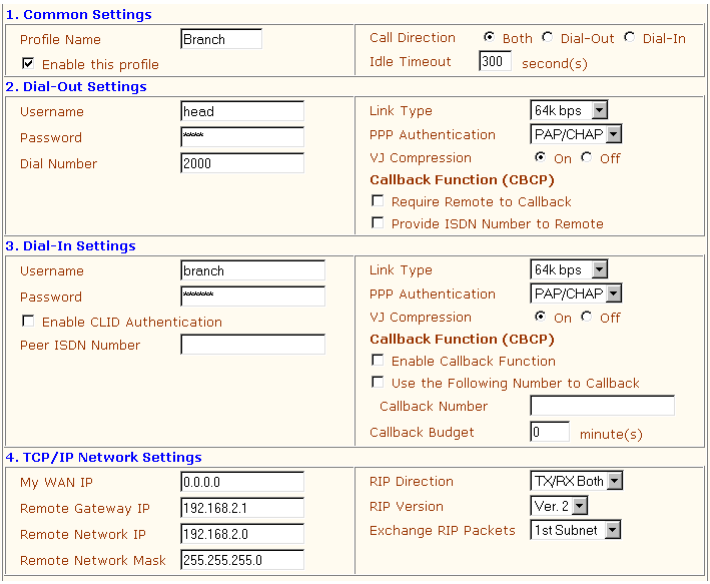
**RIP Direction:** The option specifies the direction of RIP (Routing Information Protocol) packets through the ISDN WAN connection.

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

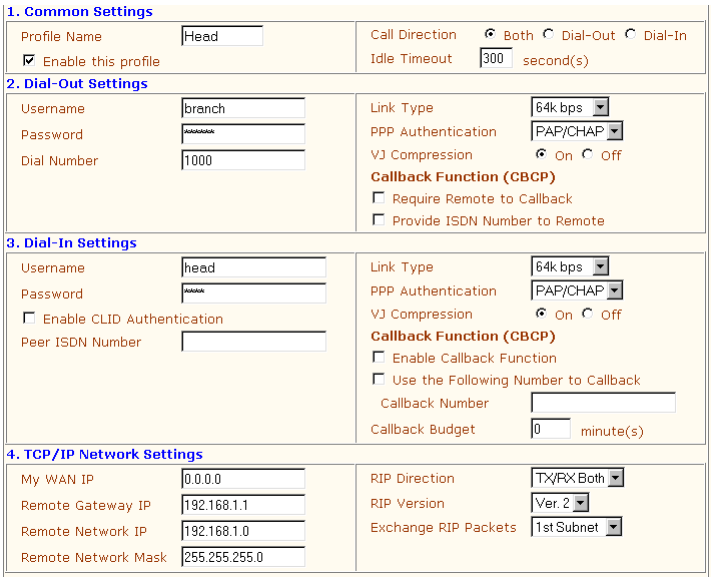
**Exchange RIP Packets:** The router has two local IP networks: the1st subnet and 2nd subnet. Here you set which subnet will exchange RIP packets with the remote network. Usually set to **1st subnet** for routing between the 1st subnet and the remote network.

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

**Head Office:**



## Branch Office:



# 5 Advanced Setup


5.1 Enabling the Remote Activation Function

5.2 Call Control Setup

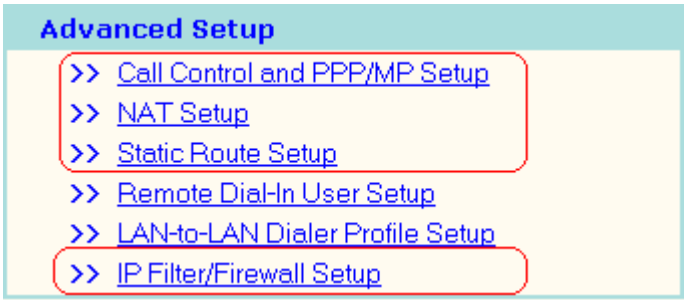
5.3 Configuring the BOD Parameters

5.4 NAT Setup

5.5 Static Route Setup

5.6 IP Filter/Firewall Setup

This chapter explains the options available in Advanced Setup:




**Advanced Setup**

**> Call Control and PPP/MP Setup**

**> NAT Setup**

**> Static Route Setup**

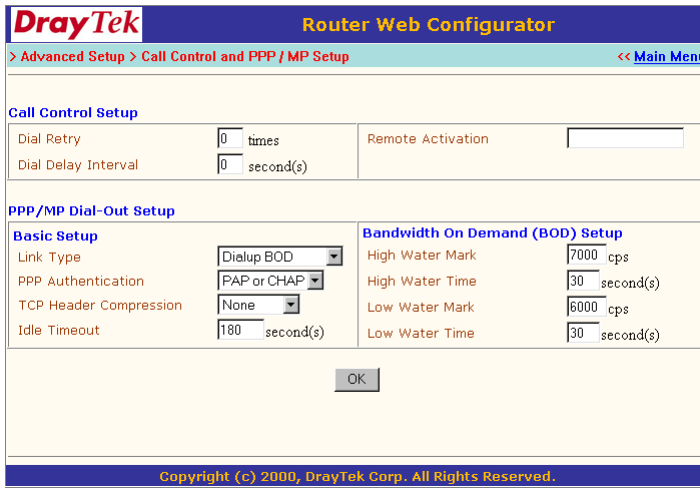
**> IP Filter/Firewall Setup**

Note:
As the Vigor2200E model does not feature an ISDN interface, Call Control and PPP/MP Setup will not be available.

## 5.1 Enabling the Remote Activation Function

Some applications require that the router 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. It may be that while working in the office, you want to get some files from home. This function allows you to make a phone call to the router and ask it to dial up to the ISP. Then you 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**. The following screen will open.

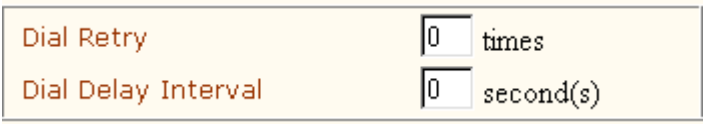


Specify a phone number in the Remote Activation field.

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

## 5.2 Call Control Setup

On the **Call Control and PPP/MP Setup** setup page, you will see **Dial Retry** and **Dial Delay Interval**.



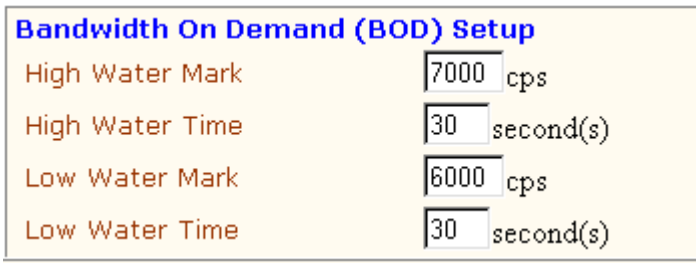

These two parameters set global settings for ISDN dialup access.

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

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

## 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 two B channel's utilization 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).

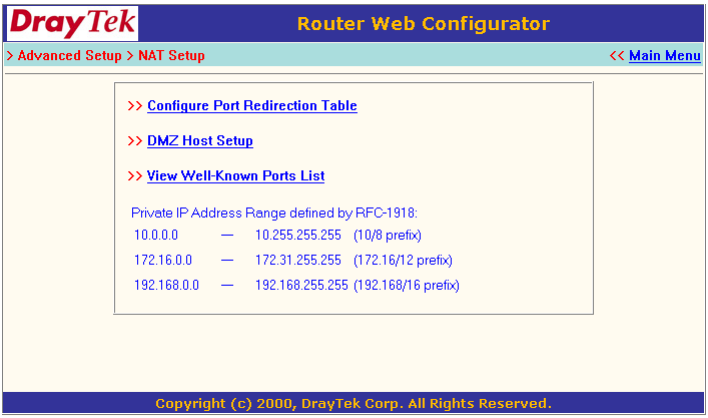
**Note:**
If you are not familiar with ISDN and ML-PPP's operation, be wary of changing the default values.

Click **OK**.

## 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 ISP mode) globally re-routeable IP addresses from the ISP. Local hosts will use private network IP addresses defined by RFC-1918 to communiate with the router. The router translates the private network addresses to a globally routeable IP address, which is then used to access the Internet. The following explains NAT features for specific applications.

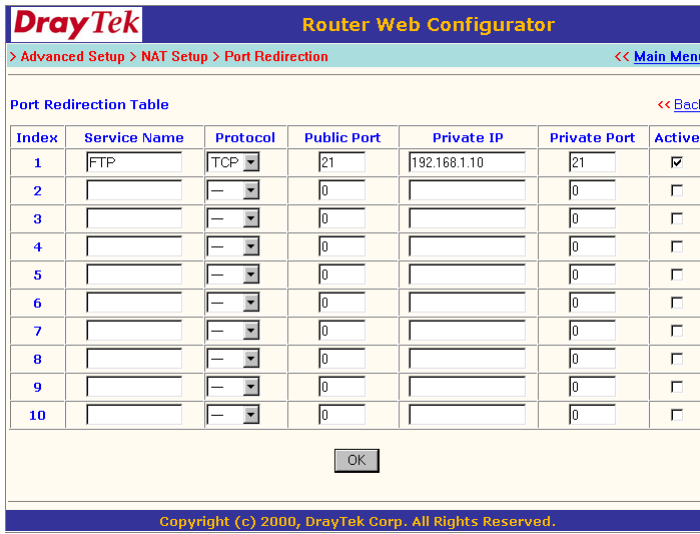
Click **NAT Setup**" to open the setup page. On the page you will see the private IP address definitions defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router.




### 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 open a specific port number to internal hosts. Internet hosts can use the WAN IP address to access internal network services, such as FTP, WWW, etc.

The following example shows how an internal FTP server is exposed to the public domain. The internal FTP server is running on the local host addressed as 192.168.1.10.




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

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

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

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

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

**Private Port:** Specifies the private port number of the service

offered by the internal host.

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

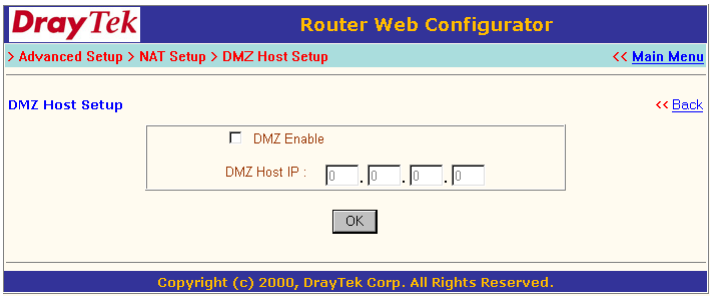
Click **OK**" .

### 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.

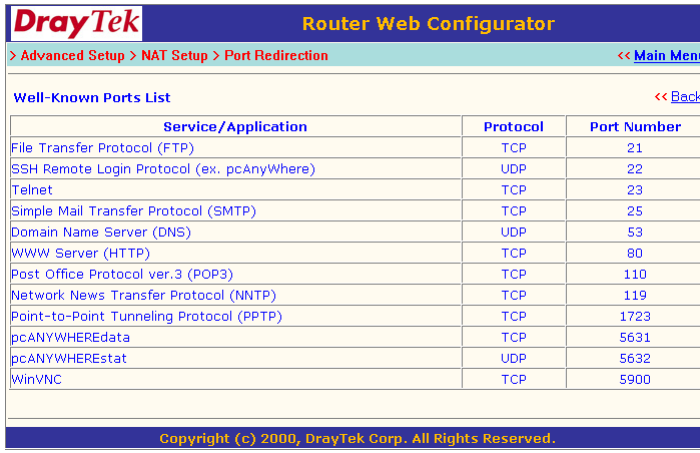
**DMZ Enable**: Check to enable the DMZ Host function.

**DMZ Host IP**: Enter the IP address of the 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 |

Copyright (c) 2000, DrayTek Corp. All Rights Reserved.

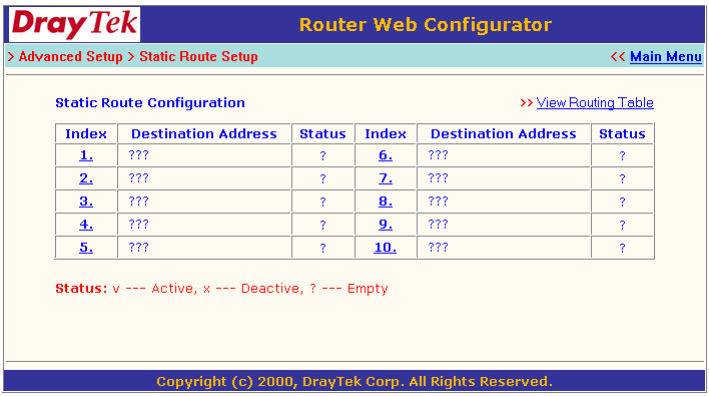
## 5.5 Static Route Setup

Vigor2200 series routers can also be set to operate as pure IP routers. You should specify the IP network configuration for the LAN1 interface using the 2nd IP address and 2nd subnet mask fields on the **LAN1 TCP/IP and DHCP Setup** page, and for the LAN2 interface using **Internet Access Setup** > **Static or Dynamic IP** (See Chapter 3.2 Internet Access Setup).

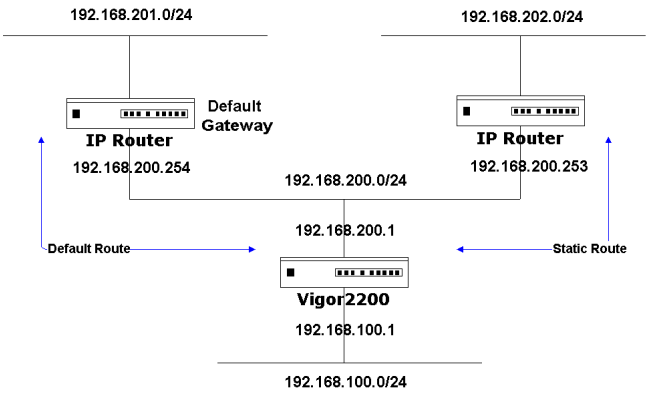
> **Note**:
> The Vigor2200 series routers have RIP (Routing Information Protocol) built-in by default. If the remote routers have the same protocol, the RIP will be used for exchanging routing information. Here, the **Static Route Setup** just provides a way to guide specified IP packets through specified routers statically.

In this application, you may want to assign static routing rules for LAN1 or LAN2. **Static Route Setup** provides this function. The

router supports 10 static route rules for your configurations. Click the numbers in the index to enter the setup page for each rule.

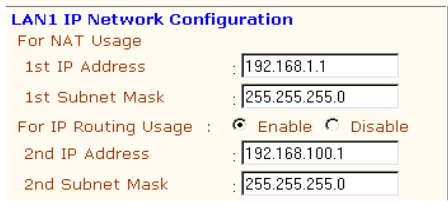



The following gives a network example with more detailed descriptions. For example, you have a network 192.168.100.0/24 connected on the LAN1 interface, and 192.168.200.0/24 connected on the LAN2(WAN) interface. Example settings are as follows.



**For LAN1:**

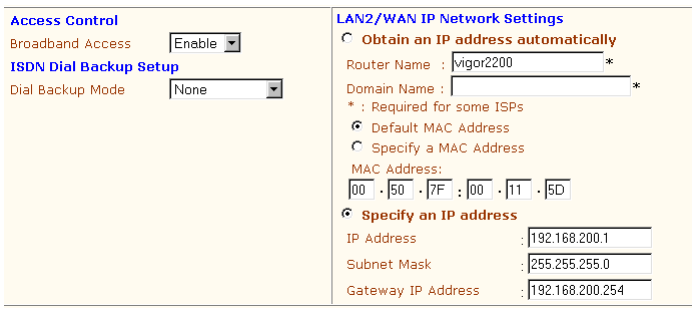
Click **LAN1 TCP/IP and DHCP Setup** to configure your LAN1 interface for IP routing.




Check **Enable** and assign **192.168.100.1** in the **2nd IP Address** field, **255.255.255.0** in the **2nd Subnet Mask** field. You now have a routeable network 192.168.100.0/24 connected on the LAN1 interface.

**For LAN2(WAN):**

To configure the LAN2(WAN), on the Main Setup Menu click **Internet Access Setup**" > **Static or Dynamic IP** to enter the setup page.

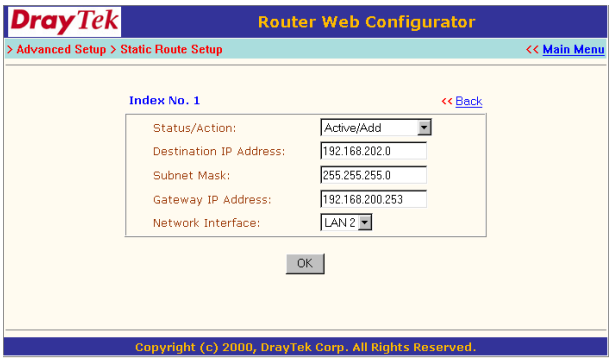



Note that **Broadband Access** is enabled and we assigned LAN2(WAN) a static IP, **192.168.200.1,** with a subnet mask of **255.255.255.0,** and a default gateway of **192.168.200.254**. The default gateway is a next hop router connected to another IP network, 192.168.201.0/24. In addition, we assume another router, 192.168.200.253/24, is also con-

nected to the same Ethernet segment as LAN2(WAN). Behind the router is another IP network, 192.168.202.0/24. The following subsections based on this example give more detailed explanations.

### 5.5.1 Add a Static Route

In the above example, if you want the 192.168.202.0/24 and 192.168.100.0/24 network to have access to each other, you should add a static route in the Vigor2200 router and also in the 192.168.200.253 IP Router. The following setting show the Vigor2200's static route configurations.




**Status/Action:** Set to **Active/Add**.

**Destination IP Address:** Specifies the target network IP or host IP. In this example we use network IP 192.168.202.0 as the routed target.

**Subnet Mask:** Specifies the target network mask. In the example, we use the subnet mask of network 192.168.202.0.

**Gateway IP Address:** Specifies the IP address of the next hop router. In the example, we set this to 192.168.200.253 as the 192.168.202.0 network is behind the router.

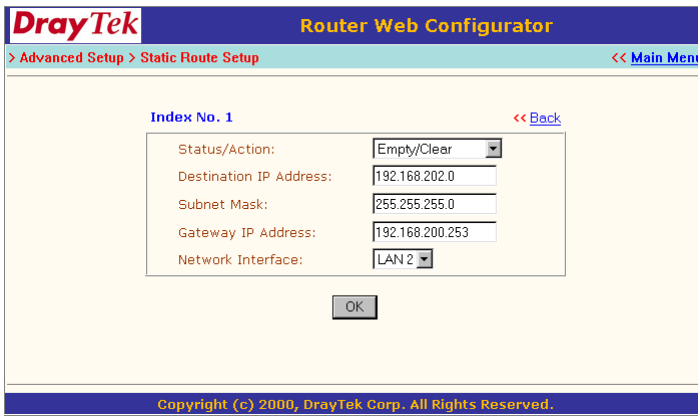
**Network Interface:** Specifies the network interface. In the example, we use LAN2 to connect to the next hop router 192.168.200.253.

Click **OK**" .

**Note:**
For the static route to work, the next hop router must also have added a static route to forward all 192.168.100.0/24 IP packets to the Vigor2200 router. After clicking the "**OK**" button, you will see the added route is shown in the current running routing table. Click " **View Routing table**" to verify.

### 5.5.2 Clear a Static Route

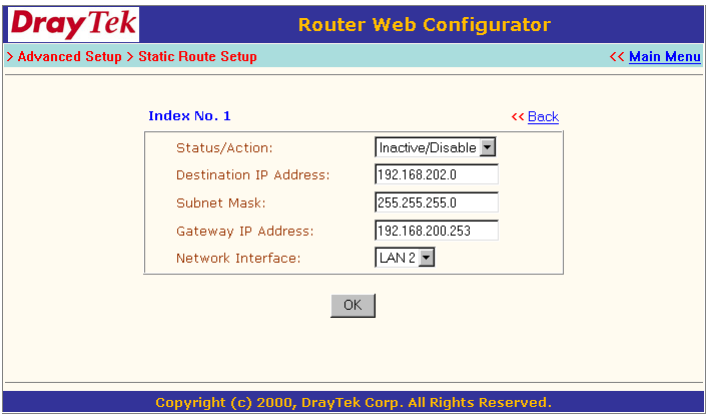
To clear a static route, set the **Status/Action** field to **Empty/Clear,** as shown below.



Click **OK.** All items on the above setup page will be cleared and be removed from the routing table.

### 5.5.3 Deactivate a Preset Static Route

Sometimes you may want to deactivate but not clear the preset static route. Set the **Status/Action** field to **Inactive/Disable** as shown below.




Click **OK.** to disable/make the preset static route inactive.

## 5.6 IP Filter/Firewall Setup

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

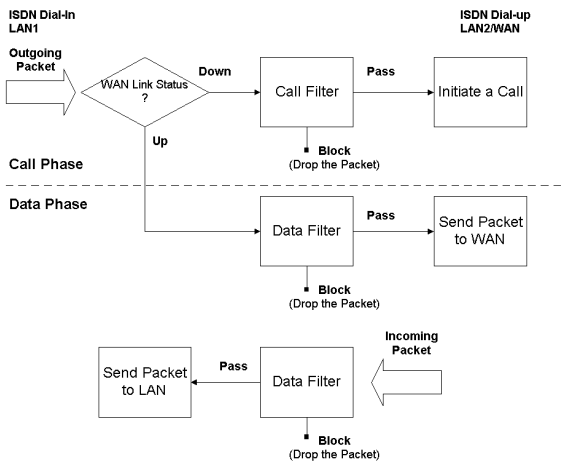
### 5.6.1 An Overview of the Firewall

The IP Filter/Firewall includes two types of filter: Call Filter and Data

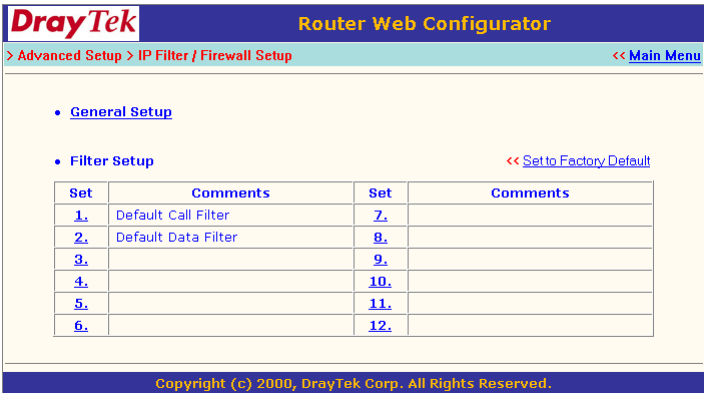
Filter. The former is designed to block or allow IP packets that will trigger the router to establish an outgoing connection. The latter is designed to block or allow which kind of IP packets are allowed to pass through the router when the WAN connection has been established.

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

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



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



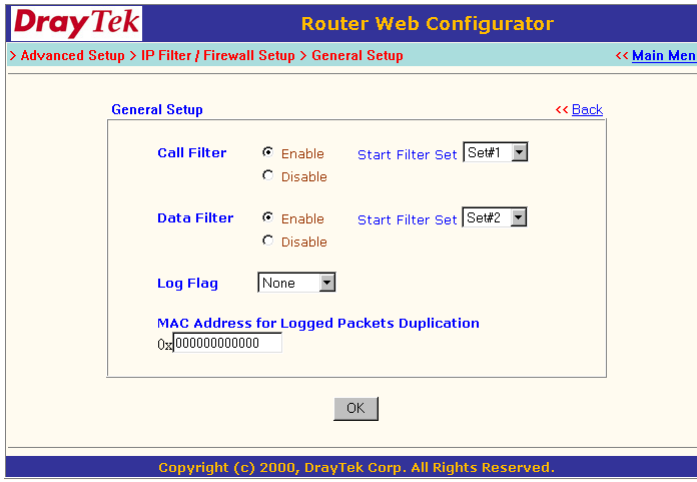

**General Setup:** Some general settings are available from this link.

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

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

### 5.6.2 General Setup

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




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

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

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

**None:** The log function is inactive.

**Block:** All blocked packets will be logged.

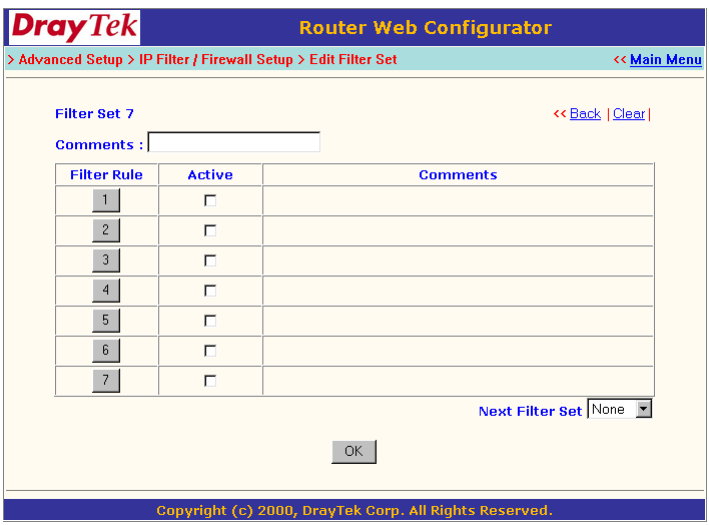
**Pass:** All passed packets will be logged.

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

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

**MAC Adddress for Packet Duplication:** Logged packets may also be logged to another location via Ethernet. If you want to duplicate logged packets from the router to another network device, you must enter the other devices' MAC Address (HEX Format). Type "0" to disable the feature (also see "Duplicate to LAN" on page 5-21). The feature will be helpful under Ethernet environments.

## 5.6.3 Editing the Filter Sets



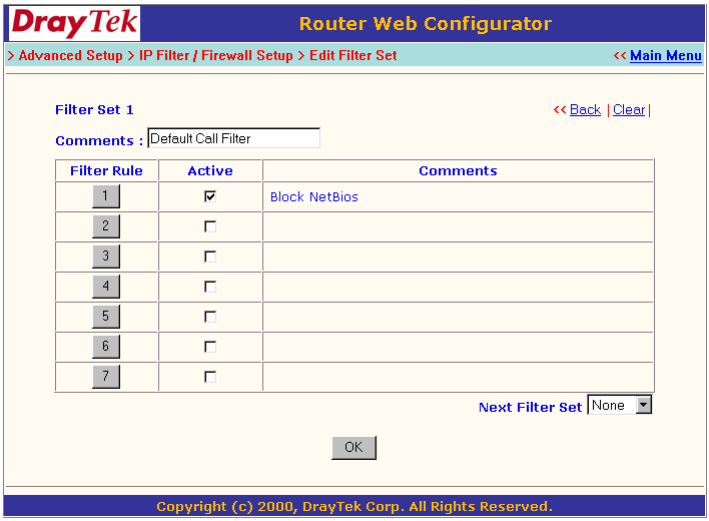

**Comments**: Enter filter set comments/description. Maximum length is 22 characters.

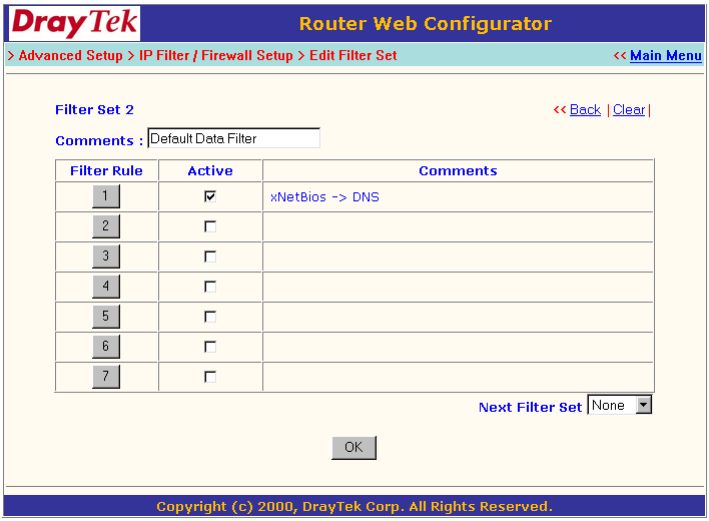
**Filter Rule**: Click a button numbered **1 ~ 7** to edit the filter rule.

**Active**: Enable or disable the filter rule.

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

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






## 5.6.4 Editing the Filter Rules

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

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

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

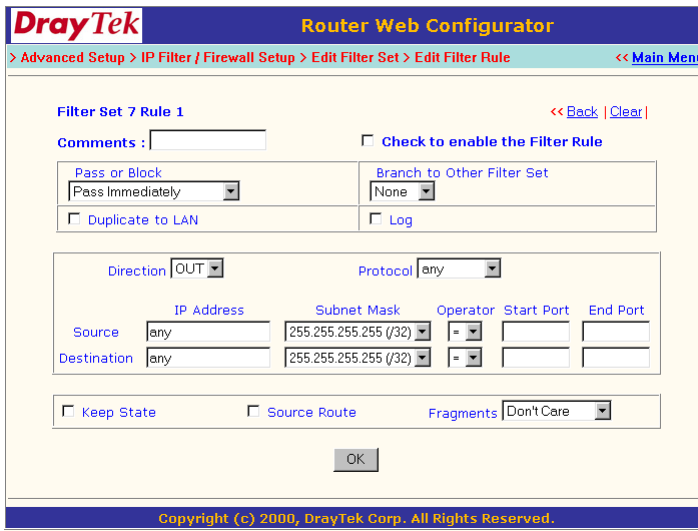
**Pass or Block:** Specifies the action to be taken when packets match the rule.

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

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

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

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




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

**Duplicate to LAN:** If you want to log the matched packets to another network device, check this box to enable it. The MAC Address is defined in **General Setup** > **MAC Address for Logged Packets Duplication** (see page 5-17).

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

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

For the Data Filter:

**IN:** Specifies the rule for filtering incoming packets.

**OUT:** Specifies the rule for filtering outgoing packets.

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

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

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

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

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

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

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

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

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

**Fragments:** Specifies a fragmented packets action.

Don't Care **(Do not Care):** Specifies no fragment options in the filter rule.

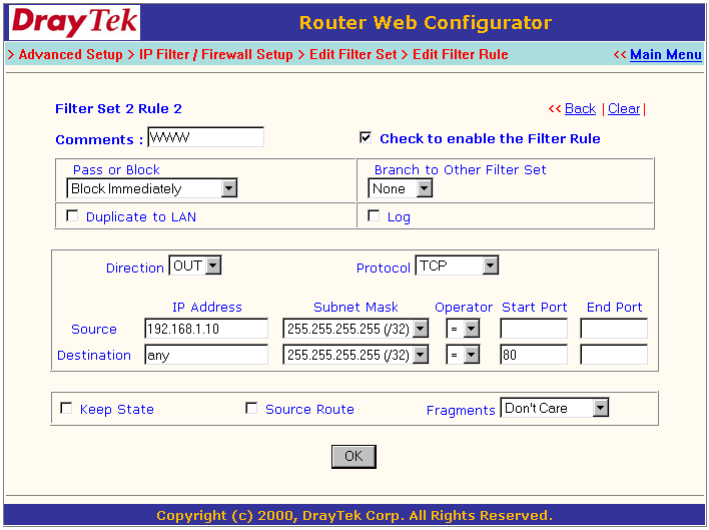
**Unfragmented:** Applies the rule to unfragmented packets.

**Fragmented:** Applies the rule to fragmented packets.

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

### 5.6.5 Restricting Unauthorized Internet Services

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

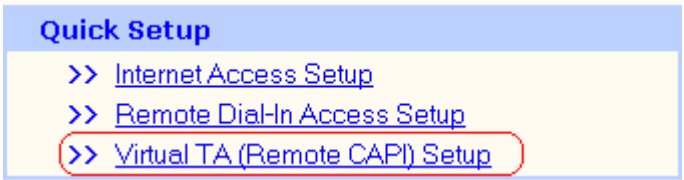


# 6 Virtual TA Application

6.1 Virtual TA Concepts
6.2 Installing a Virtual TA Client
6.3 Configuring a Virtual TA Client/Server

## Note: Not supported on the Vigor2200E model.

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.

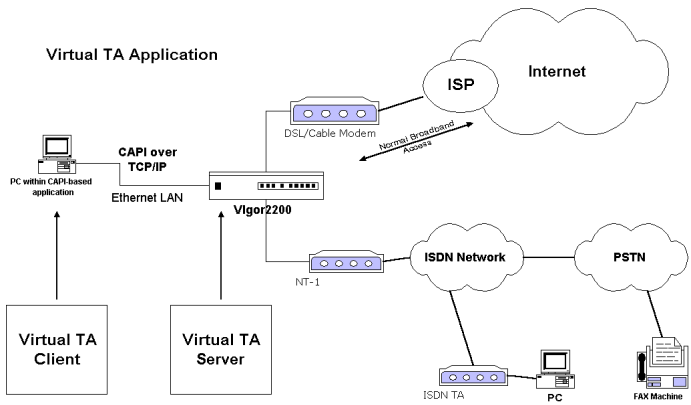
2. The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.

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 Vigor2200, or directly double-click the installer file. Vsetup95.exe is for Windows 95 OSR2.1 or higher, Vsetup98.exe is for Windows 98, 98SE and Me, and Vsetup2k.exe is for Windows 2000.

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

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

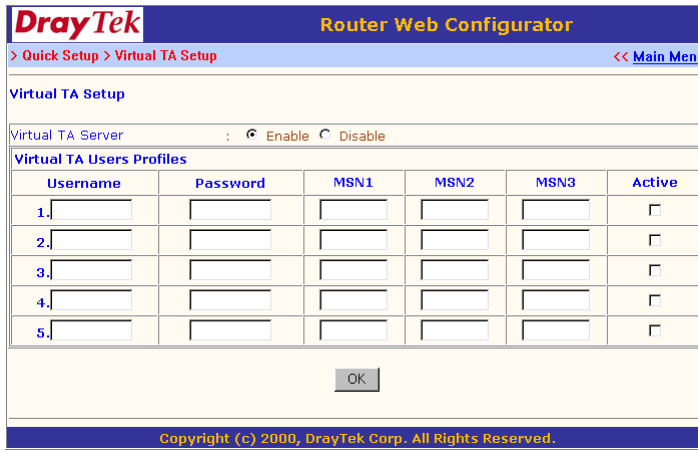
When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Read your software user guide for detailed configuration.

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

### 6.3 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:** Specifies the username for a specific client.

**Password:** Specifies the password for a specific client.

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

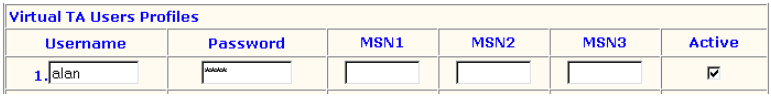
**Active:** Check to enable the client to access the server.

### Creating a User Profile

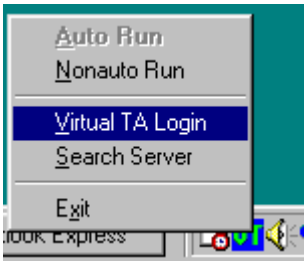
Note that creating a single user access account limits access to the Virtual TA server to only the specified account holders.

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

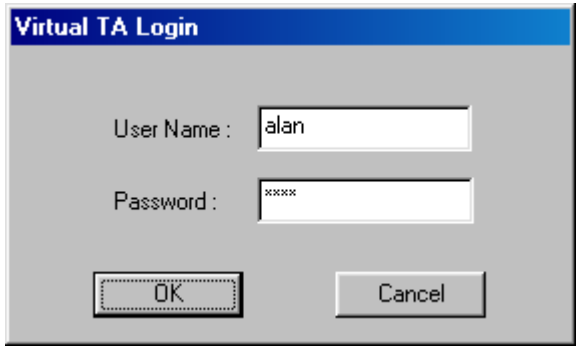
1. On the server: Click **Virtual TA (Remote CAPI) Setup**, and fill in the Username and Password fields. Check the **Active** checkbox to enable the account.




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 time the VT icon text will become 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 "alan" client.

Virtual TA Users Profiles

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

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

# 7 System Management

7.1 Online Status
7.2 Management Setup
7.3 Diagnostic Tools
7.4 Reboot System
7.5 Firmware Upgrade

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

**System Management**

**> Online Status**

**> Management Setup**

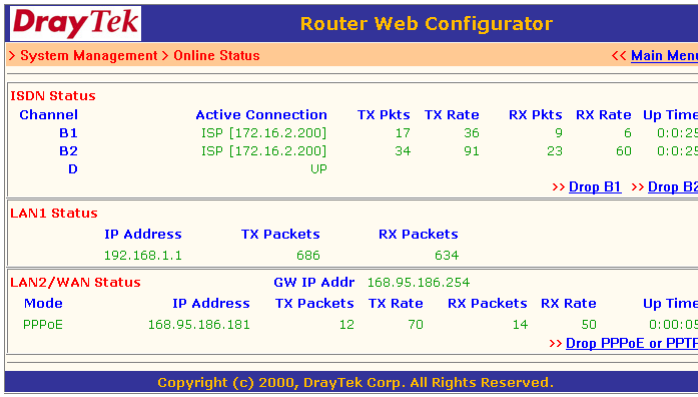
**> Diagnostic Tools**

**> Reboot System**

**> Firmware Upgrade (TFTP Server)**

## 7.1 Online Status

Click **Online Status** to open the Online Status page. In the example, on the following page, both the ISDN B1 and B2 channel are active and also a PPPoE connection is up on the LAN2/WAN interface.




The Online Status page contains three subgroups: ISDN Status, LAN1 Status and LAN2/WAN Status.

**ISDN Status: (Vigor2200, Vigor2200X and Vigor2200W Only)**

**Active Connection:** 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 number of transmitted IP packets sent during this connection session.

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

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

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

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

**Drop B1:** Click to disconnect the B1 channel.

**Drop B2:** Click to disconnect the B2 channel.

**LAN1 Status:**

**IP Address:** IP address of the LAN1 interface.

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

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

**LAN2/WAN Status:**

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

**GW IP Addr:** Indicates the gateway IP address.

**IP Address:** IP address of the LAN2/WAN interface.

**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 received IP packets received during this connection session.

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

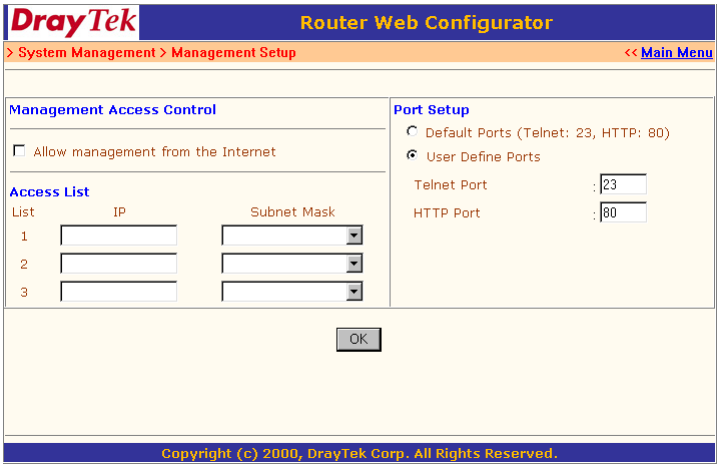
**Up Time:** Connection time. The format is HH:MM:SS where HH means hours, MM means minutes, and SS means seconds.

**Drop PPPoE or PPTP:** Click the link 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 be displayed.




### Management Access Control

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

### Access List

You may specify that the system administrator can only login from a

specific host or network defined in the list. A maximum of three IPs/ subnet masks may be entered.

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

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

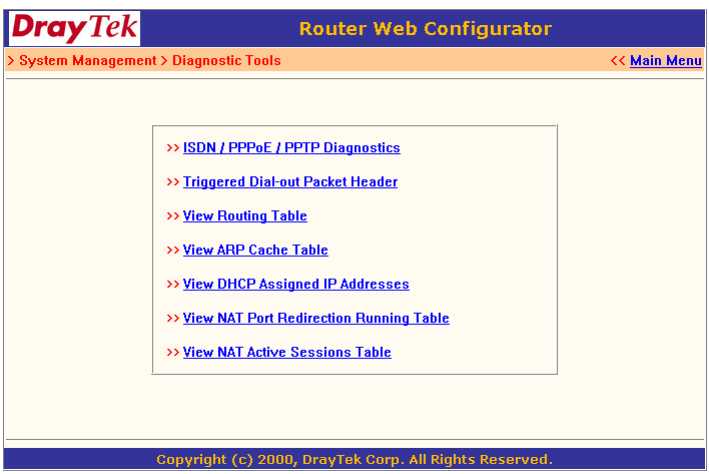
**Port Setup**

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

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

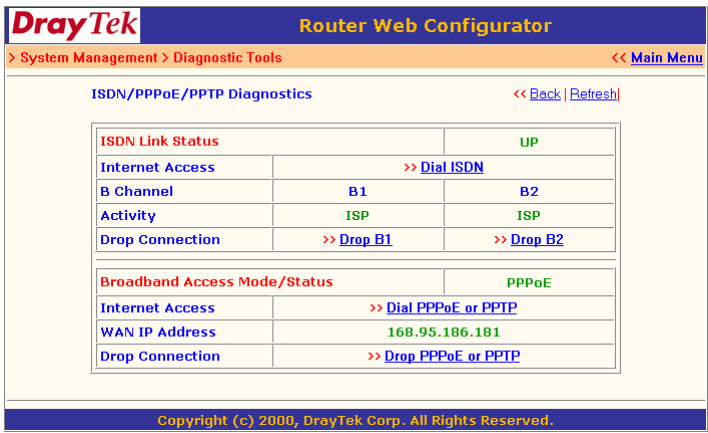
## 7.3 Diagnostic Tools

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



**ISDN / PPPoE / PPTP Diagnostics:** Click here to open the following page. The page shown here is for reference only; individual networks will show different results.

The page has been grouped into two subgroups, the upper is for ISDN link status, the lower 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**, **Static IP,** or **DHCP Client** depending on which access mode is enabled. If the connection is idle, it will show "**---**" .

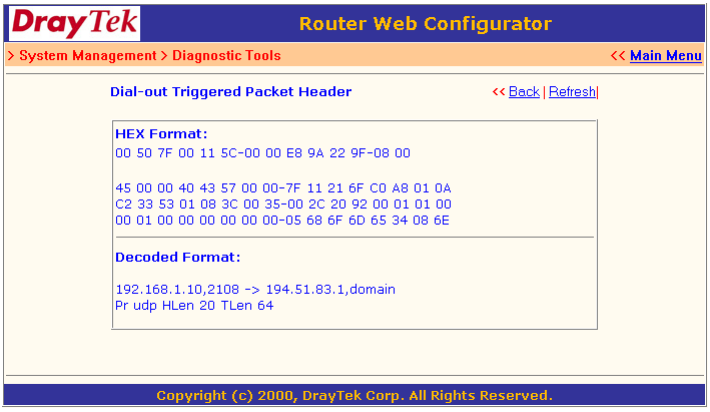
**WAN IP Address:** The WAN IP address for the active connection.

**Dial PPPoE or PPTP:** Click 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:**

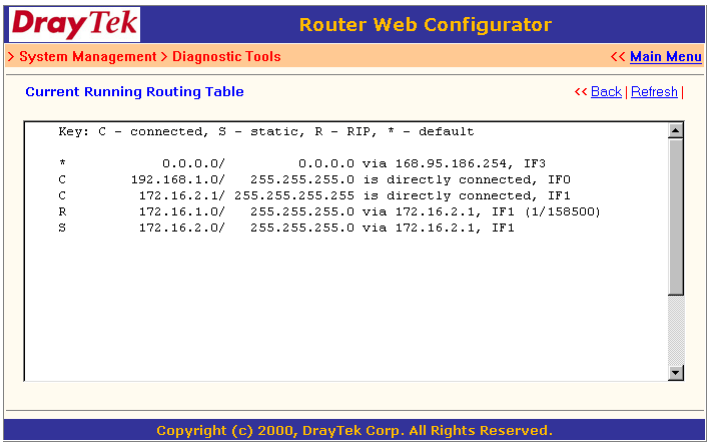
Triggered Dial-out Packet Header shows the last IP packet header that triggered the router to dial out.



**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:

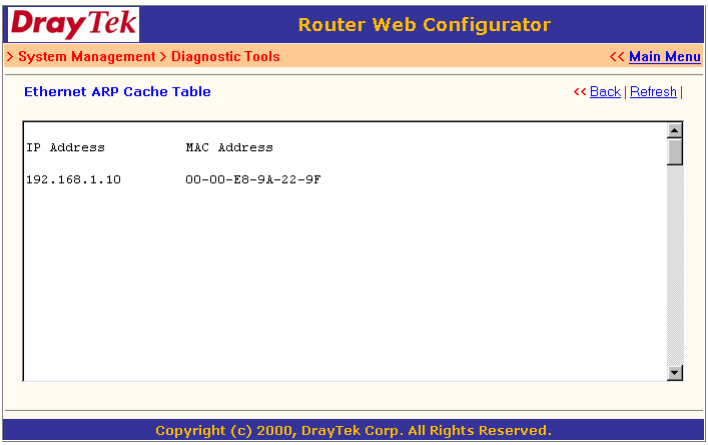
**C** --- Directly connected.
**S** --- Static route.
**R** --- RIP.
***** --- Default route.

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.
**IF3** --- WAN(LAN2) interface.

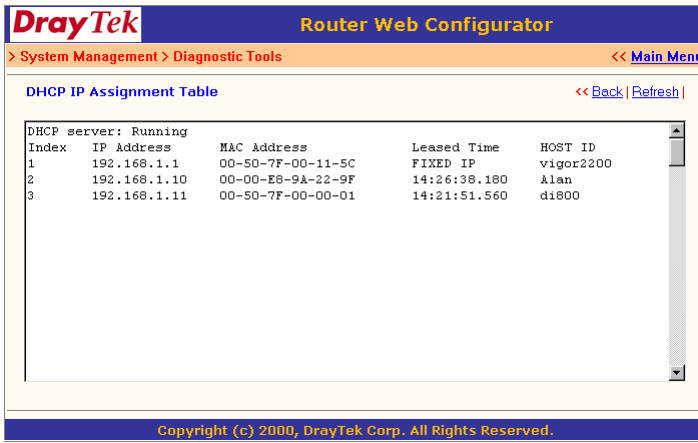
### View ARP Cache Table:

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



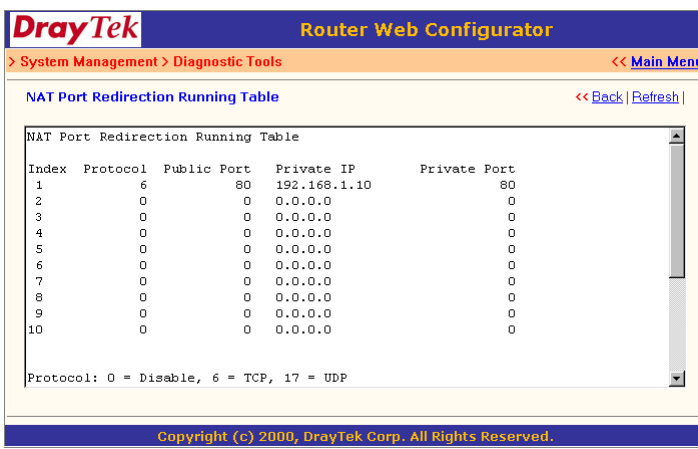

### View DHCP Assigned IP Addresses:

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



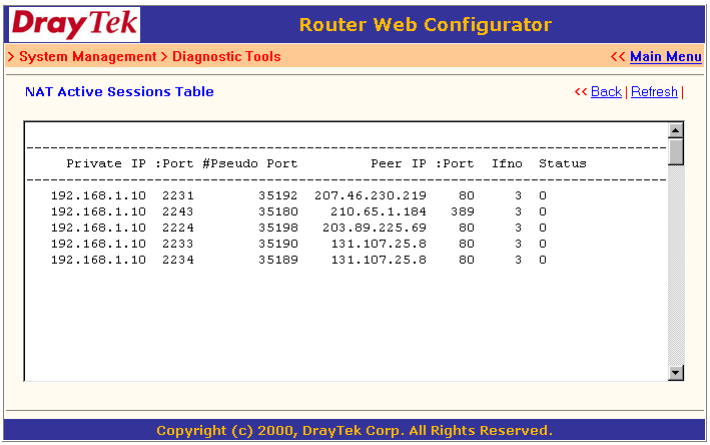

## View NAT Port Redirection Running Table:

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



### View NAT Active Sessions Table:

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

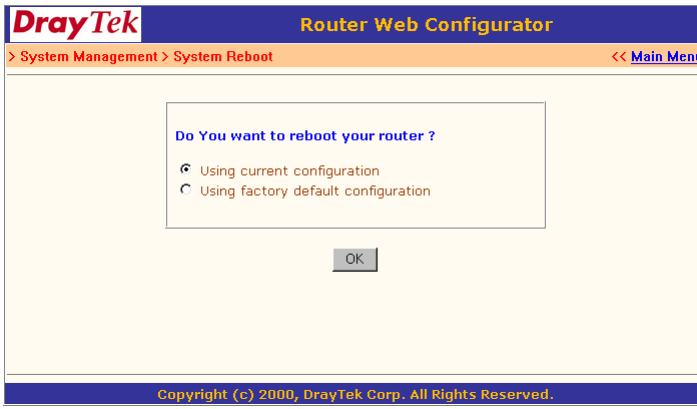



Each line across the screen indicates an active session. The following information is displayed:

**Private IP, Port:** The internal user's (PC's) IP address and port number.
**#Pseudo Port:** The public port number.
**Peer IP, Port:** The peer user's (PC's) IP address and port number.
**Ifno:** Stands for interface number. The definition is listed below:
0 --- LAN interface.
1 --- B1 interface
2 --- B2 interface.
3 --- WAN(LAN2) interface.

## 7.4 Reboot System

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



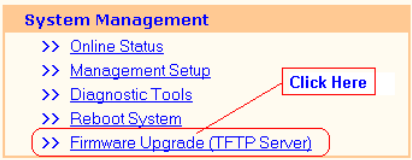

There are two reboot options: **Using current configuration** and **Using factory default configuration**. If you want to reboot the router using current running configurations, check **Using current configuration** and click "**OK**". To reset the router' s settings to default values, check **Using factory default configuration** and click "**OK**".
The router will take 3 to 5 seconds to reboot the system.

## 7.5 Firmware Upgrade

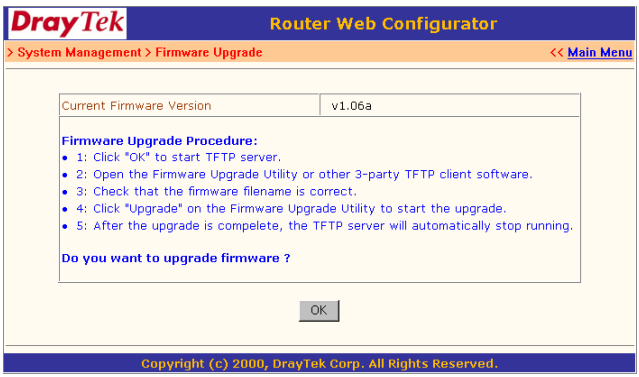
Before upgrading your router firmware, you must install the **Router Tools**. The **Firmware Upgrade Utility** is included in the tools. The following steps will guide you through an upgrade. Note that the examples below use a Windows OS.

1. Download the latest firmware from the web site or FTP site of DrayTek (ftp://ftp.draytek.com/vigor2200/).

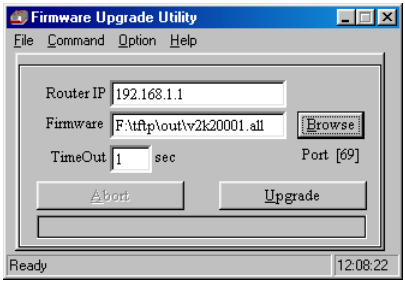
2. Use the Web Configurator to enable the Firmware Upgrade function.




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 (v2k200001.all) is for example purposes only and the latest firmware will have a different file name. Click **Upgrade**. The upgrade status will be shown on the progress bar.

# 8 Troubleshooting & FAQ


8.1 Using the Telnet Terminal Commands

8.2 Viewing Call Logs

8.3 Viewing ISDN Logs

8.4 Viewing PPP Logs

8.5 Viewing WAN Logs

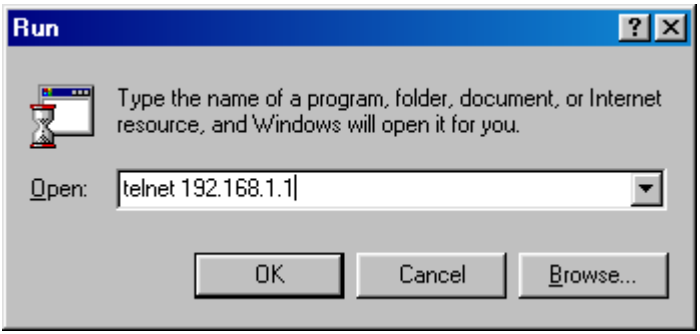
8.6 Troubleshooting the DHCP Client on WAN

8.7 FAQs

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

## 8.1 Using the Telnet Terminal Commands

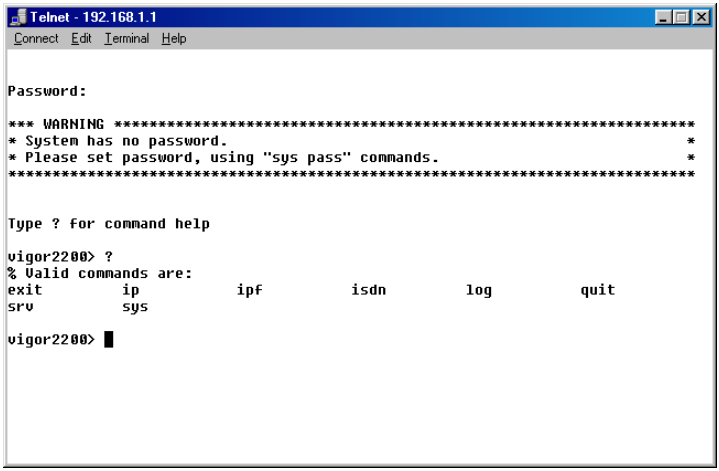
Click **Start** > **Run** and type **Telnet 192.168.1.1**" in the **Open** box as below. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.




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

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

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




**Command Help:**

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

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

vigor2200>
```

**Recall Commands:**

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

**Quitting the Telnet Terminal:**

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

## 8.2 Viewing Call Logs

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

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

ISDN example:

```
vigor2200> log -c
14:48:59.480 >>> Dial-up triggered by user : 192.168.1.18
             proto=icmp, to 168.95.1.1
14:48:59.480 Dialing ISP (Hinet) : 04125678
14:49:00.000 PPP Start (B1)
14:49:03.230 PAP Login OK (B1)
14:49:03.280 IPCP Opening (B1)
             Own IP Address : 163.31.241.167  Peer IP Address : 168.95.67.195
             Primary DNS : 168.95.192.1  Secondary DNS : 168.95.1.1
vigor2200>
```

PPPoE example:

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

## 8.3 Viewing ISDN Logs

To capture messages exchanged on the ISDN interface, use the **log -i** command to dump all exchanged messages on the ISDN interface.

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. This command allows you to see whether the ISDN connection could be established or not. Note that if you cannot understand the details, save these messages in a file and send it to a 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.

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

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

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

## 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 Troubleshooting the DHCP Client on WAN

In a Cable access environment, the DHCP client (dynamic IP) is a popular way to access the Internet. The router provides "**ip dhcpc ...**" commands to help you to diagnose DHCP client problems. These commands are similar in function to the **ipconfig.exe** or **winipcfg.exe** tools on MS Windows OS platforms.

Type the "ip dhcpc ?" command. You will get the subcommands shown below:

```
vigor2200> ip dhcpc ?
% Valid subcommands are:
release      renew        status

vigor2200>
```

### Releasing the IP Address

The command to release the WAN IP address is **ip dhcpc release**. After typing the command, the router will release all IP settings on the WAN interface.

```
vigor2200> ip dhcpc release
vigor2200> ip dhcpc status

DHCP Client Status:

DHCP Server IP : 0.0.0.0
WAN IP         : 0.0.0.0
WAN Netmask    : 0.0.0.0
WAN Gateway    :
Primary DNS    :
Secondary DNS  :
Leased Time    : 0
Leased Time T1 : 0
Leased Time T2 : 0

vigor2200>
```

## Renewing the IP Address

Type **ip dhcpc renew** to get a new IP address from the cable service provider.

```
vigor2200> ip dhcpc renew
vigor2200> ip dhcpc statu

DHCP Client Status:

DHCP Server IP : 192.168.3.1
WAN IP         : 192.168.3.83
WAN Netmask    : 255.255.255.0
WAN Gateway    : 192.168.3.1
Primary DNS    : 168.95.1.1
Secondary DNS  : 192.168.3.1
Leased Time    : 259200
Leased Time T1 : 129600
Leased Time T2 : 226800

vigor2200>
```

## Viewing the WAN Status

Type **ip dhcpc status** to show the status of the DHCP client for the WAN interface.

## Viewing DHCP Logs

In some special cases, you may want to capture the detailed DHCP messages sent between the WAN interface and the cable head-end access server. Type “log -i” to dump these DHCP exchanged messages. Note that the DHCP client messages will be shown using the **log -i** command when the LAN2/WAN interface has been configured

as **Obtain an IP address automatically**.

```
vigor2200> log -i
00:00:00.020 ---->DHCP Len=300 (Request)
          01 01 06 00 76 56 9A A4 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 50 7F 00 11 5D 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 63 82 53 63
          35 01 01 3D 07 01 00 50 7F 00 11 5D 0C 09 76 69 67 6F 72 32
          32 30 30 37 08 01 03 06 0F 2C 2E 2F 39 FF 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

## 8.7 FAQs

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

**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. For security, you should assign a password to protect your router against hacker attacks.

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

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

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

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

**4. Why does the router dial out very often?**

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

**5. Why can not I connect to the Web Configurator?**

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

**6. What are the differences between the Vigor2200, Vigor2200X, Vigor2200W, and Vigor2200E?**

**A:** Please refer to section 1.2. **Vigor2200 Series Router Comparisons** for more details.

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

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

**8. What is the maximum number of IP addresses that 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.

**9. What is a DSL/Cable Router?**

**A:** The Vigor2200 router series have no built-in Cable or DSL modem. They must be connected to an external Cable or DSL modem for broadband access.

## Installing a Virtual TA Client

1. Insert the CD-ROM supplied with your router, or directly double-click the VTA Client Installer file.

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

3. After the computer restarts, you will see a VT icon on the Control Strip(usually in the bottom-left of the screen) 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 communication oftware 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.

## Configuring a Virtual TA Client

1. On the client: Click the mouse on the VT icon. The following pop-up menu will be shown.

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

3. Enter the Username and Password and click "**OK**". After a short time the VT icon text will become green.

# VPN

# Vitual Private Network and Remote Access

**VPN.1 Introduction to VPNs and Remote Access**

**VPN.2 IKE/IPSec Setup**

**VPN.3 Remote Dial-in Access**

**VPN.4 LAN-to-LAN Access**

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

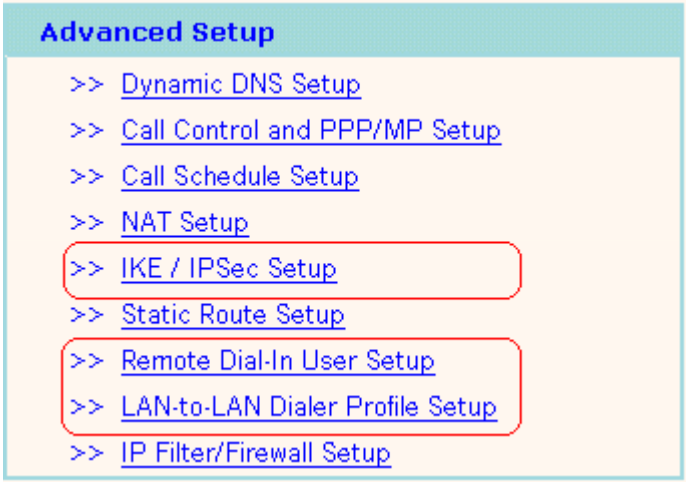
**Quick Setup**

**> Remote Dial-In Access Setup**

**Advanced Setup**

**> Remote Dial-In User Setup**

**> LAN-to-LAN Dialer Profile Setup**



## 1 Introduction to VPNs and Remote Access

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

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

Draytek Vigor 2200 series router’s virtual private networking (VPN) supports Internet-industry standards technology to provide customers with open interoperable VPN solutions such as Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) as well as Point-to-Point Tunneling Protocol (PPTP).

For Vigor 2200, Vigor 2200X and Vigor 2200W models which have ISDN port, not only VPN connection is provided but also physically private network connection is provided for remote access through ISDN connection.

## 2 IKE/IPSec Setup

### Dial-in Setup

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

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

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

**IPSec Security Method:** Selects allowed IPSec security method.

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

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

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

**Dial-out Setup**

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

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

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

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

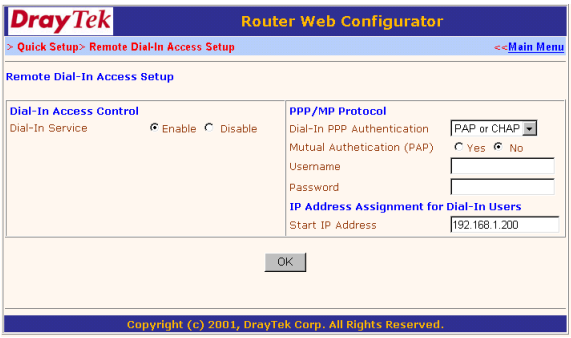
## 3 Remote Dial-In Access

There are 2 types of VPN connection for remote dial-in access. One is PPTP, and the other is L2TP. And also you can have an additional choice through ISDN physically remote dial-in for 2200, 2200X, and Vigor2200W models.

### 3.1 Activating Remote Dial-In

In the Quick Setup group of 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

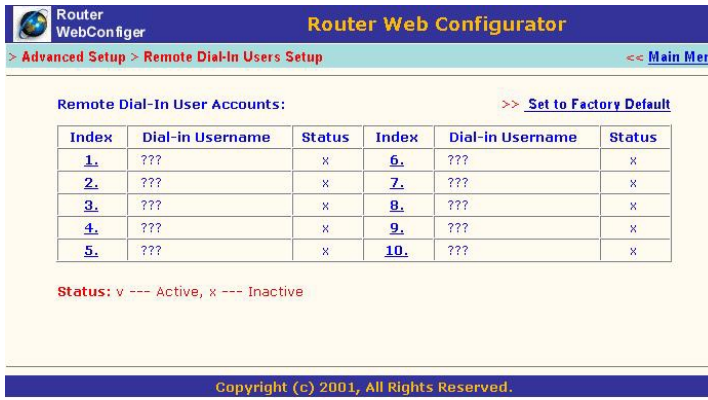
**Start IP Address:** Enter a start IP address to be assigned to the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 to be the Start IP Address.

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

Click "**OK**"

### 3.2 Creating an Access Account for a Dial-in User

After activating the dial-in capability, you must create an access account for each dial-in user. 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.

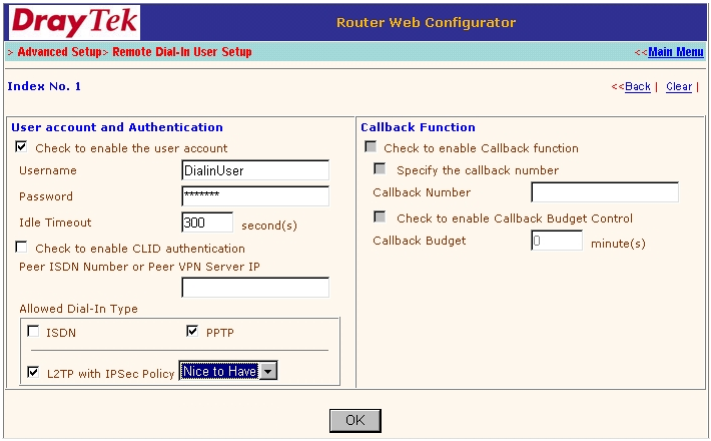
**Index:** Click the index number to open an individual setup page for

detailed setting of each account.

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

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

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




### User Account and Authentication

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

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

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

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

the connection.

**Check 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 OR Remote Dial-in User IP:** If CLID authentication has been enabled, enter the dial-in user's ISDN number or IP address if .

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

ISDN: Allowed remote dial-in user to make a physically private network connection through ISDN. Only applies to Vigor 2200 series router with ISDN port model.

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

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

**Callback Function**

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

**Check to enable the Callback function:** Enables the callback function.

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

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

**Check to enable Callback Budget Control:** By default, the

callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.

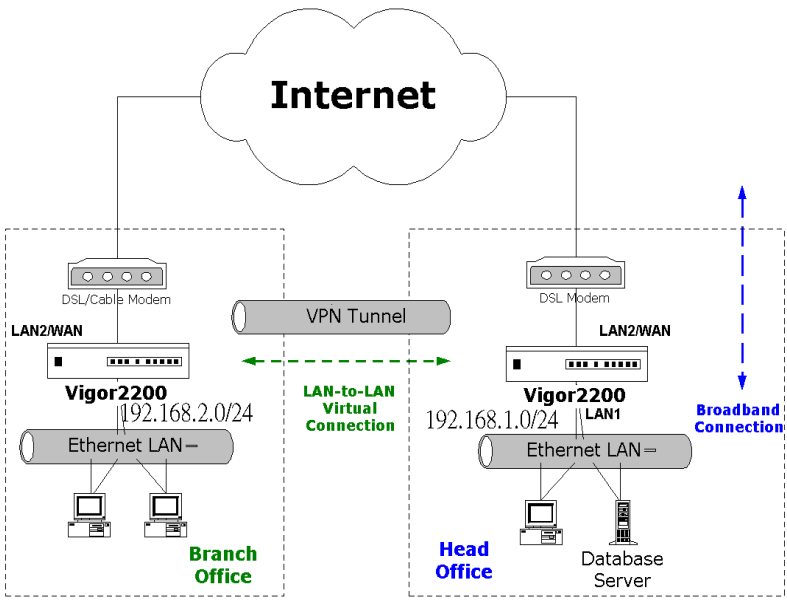
**Callback Budget (Unit: minutes):** Specifies the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

## 4 LAN-to-LAN Access

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

LAN-to-LAN through the Internet (VPN)

LAN-to-LAN through ISDN connection




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

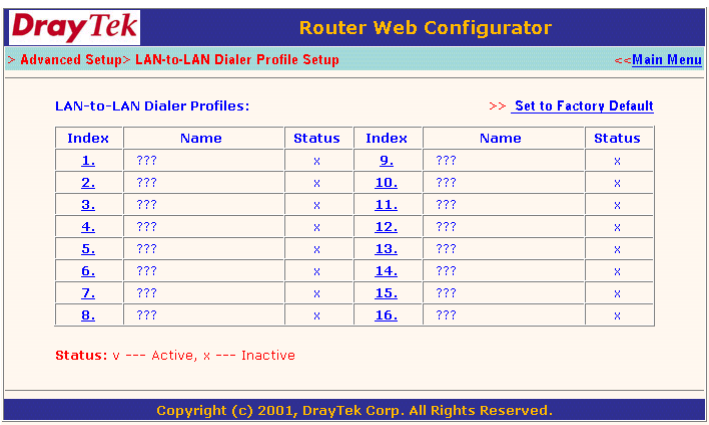
The following sections are based on the network layout above to describe how to set up a LAN-to-LAN profile to connect two private networks through Internet. In the above network layout, the private network 192.168.1.0/24 is located at head office, the network of off-site branch office is 192.168.2.0/24.

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

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

## 4.2 Creating a LAN-to-LAN Dialer Profile

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



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

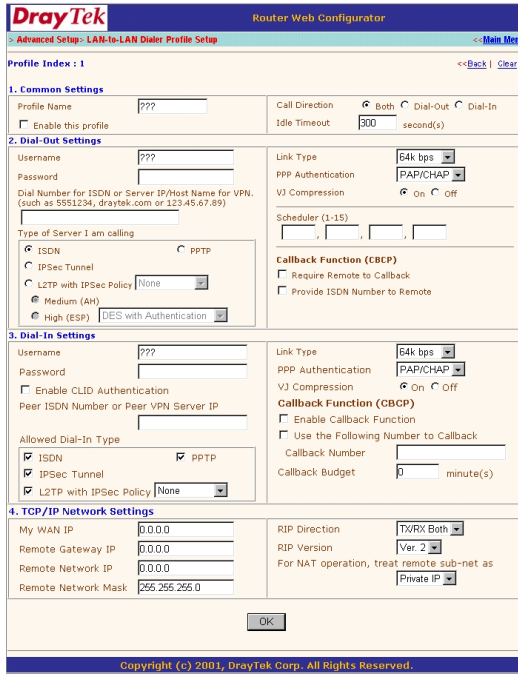
**Set to Factory Default:** Clicking here will clear all the LAN-to-LAN profiles.

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

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

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

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



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

**Common Settings**

**Profile Name:** Specifies a name for the remote network.

**Enable this profile:** Check here to activate this profile.

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

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

**Dial-Out Settings**

**Username:** Specifies a username for authentication by the remote router.

**Password:** Specifies a password for authentication by the remote router.

**Dial Number for ISDN or Server IP/Host Name for VPN:** Specifies the destination VPN server IP or Host Name for dialup.

**Type of Server I am calling:** Indicates the dial-out VPN type.

PPTP: Specifies the dial-out VPN connection is PPTP.

IPSec Tunnel: Specifies the dial-out VPN connection is IPSec Tunnel.

L2TP: Specifies the dial-out VPN connection is L2TP.

L2TP with IPSec Policy: Specifies IPSec policy for L2TP.

None: Does not apply IPSec.

Nice to Have: Applies IPSec first. If fails, tries without IPSec again.

Must: Species L2TP over IPSec.

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

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

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

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

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

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

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

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

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

**Dial-In Settings**

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

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

**Enable CLID Authentication:** Limits the dial-in VPN router to calling from a specific IP address.

**Peer ISDN Number or Peer VPN Server IP:** If CLID Authentication is enabled, enter the remote VPN server IP address in this field.

**Allowed Dial-In Type: indicates the allowed dia-in connection type.**

PPTP: Check to allow PPTP dial-in connection.

IPSec Tunnel: Check to allow IPSec tunnel dial-in connection.

L2TP: Check to allow L2TP dial-in connection.

L2TP with IPSec Policy: Specifies IPSec policy for L2TP.

None: Does not apply IPSec.

Nice to Have: Applies IPSec first. If fails, tries without IPSec again.

Must: Species L2TP over IPSec.

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

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

**TCP/IP Network Settings**

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

**My WAN IP:** 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.

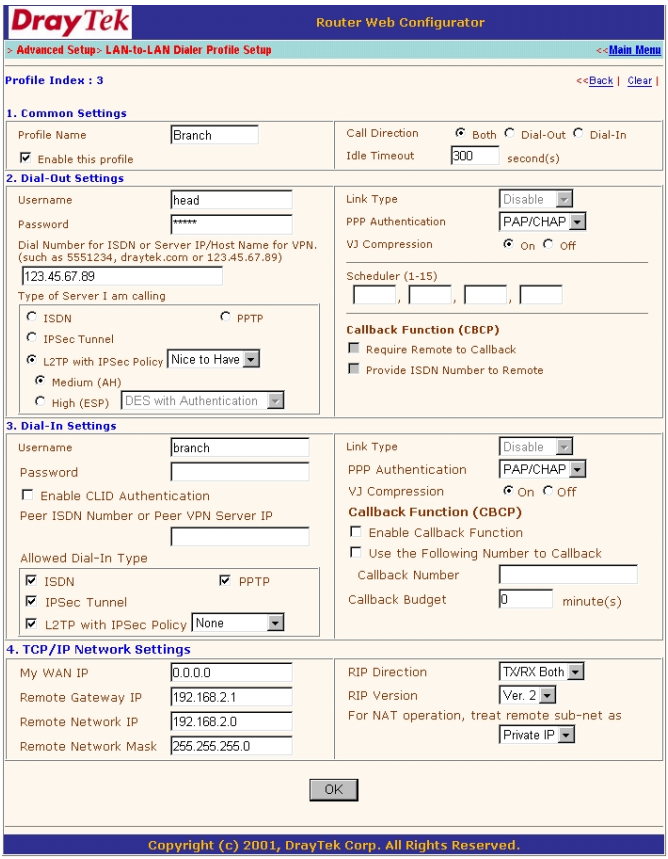
**RIP Direction:** The option specifies the direction of RIP (Routing Information Protocol) packets through the ISDN WAN connection.

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

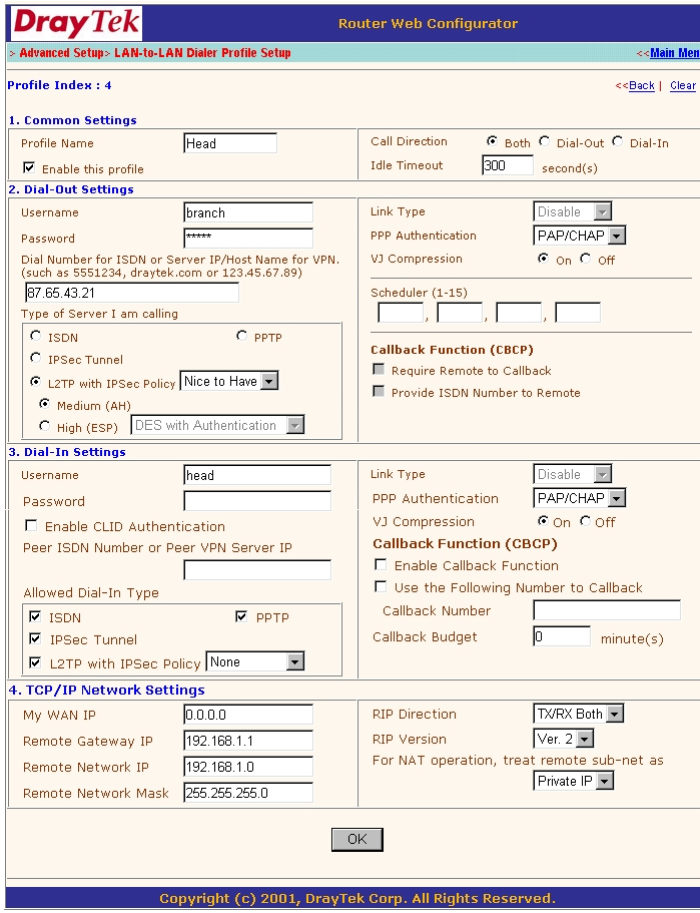
**For NAT operation, treat remote sub-net as:** The router has two local IP networks: the1st subnet and 2nd subnet. Here you set which subnet will be used as local network for VPN connection and exchange RIP packets with the remote network. Usually set to **1st subnet**" for routing between the 1st subnet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

Recall the LAN-to-LAN example described in section 4.1. The LAN-to-LAN Dialer Profile could be configured as below.

**Head Office:**

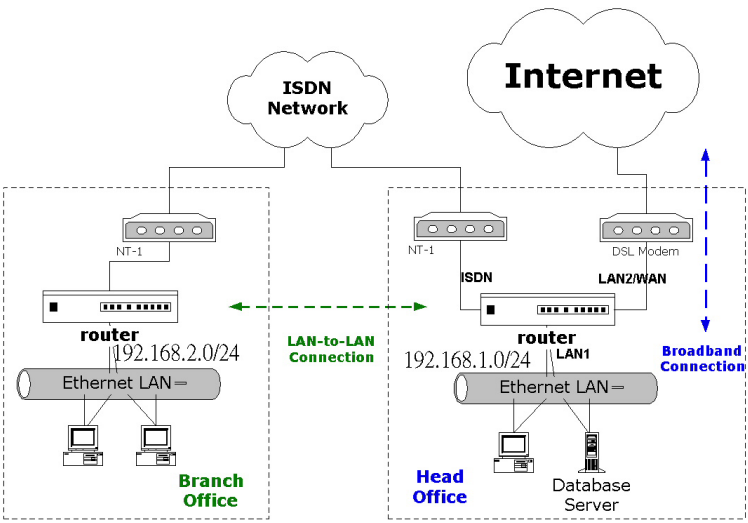


## Branch Office:



4.3 LAN-to-LAN through ISDN connection

The following sections are based on the following network layout to describe how to set up a LAN-to-LAN profile to connect two private networks. In the above network layout, the private network 192.168.1. 0/24 is located at head office, the network of off-sitebranch office is 192.168.2.0/24.



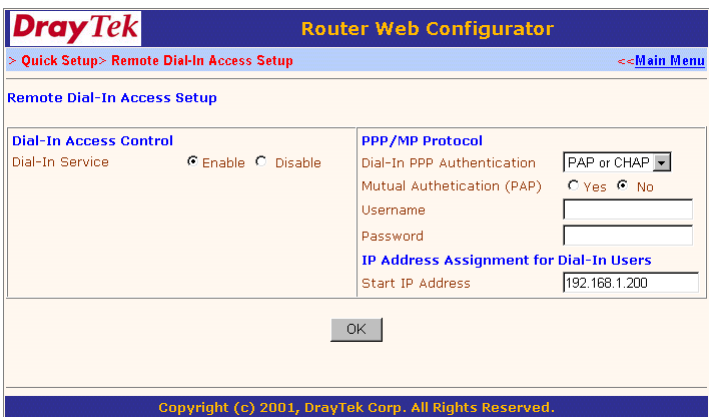

Before you begin to setup a LAN-to-LAN profile for each network, you should gather the information shown in the following table.

| | 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<br>PW: head | UN: branch<br>PW: branch |
| ISDN line number | 1000 | 2000 |
| Callback Function | Disable | Disable |

## 4.4 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 **section 3 Remote Dial-In Access** for a full explanation of the fields on this page.

**Head Office:**

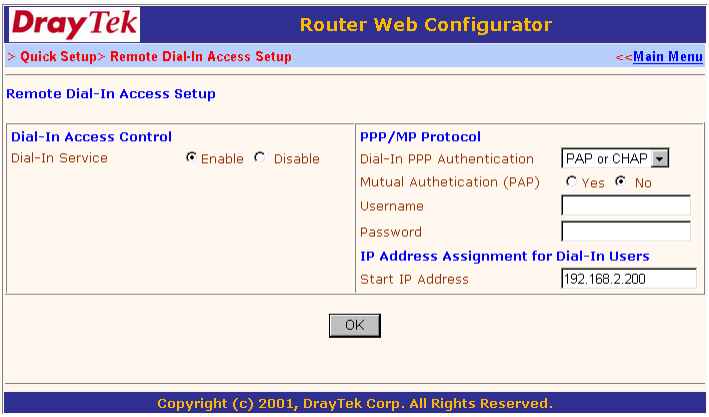


Because the Head Office's network is 192.168.1.0/24, the settings should be as below:

**Dial-In Service:** Enable

**Start IP Address:** 192.168.1.200

**Branch Office:**



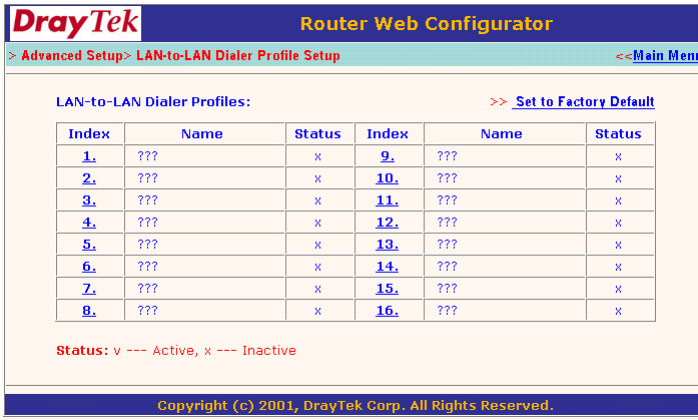

Because the Branch Office's network is 192.168.2.0/24, the settings should be as below:

**Dial-In Service:** Enable

**Start IP Address:** 192.168.2.200

### 4.5 Creating a LAN-to-LAN Dialer Profile

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




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

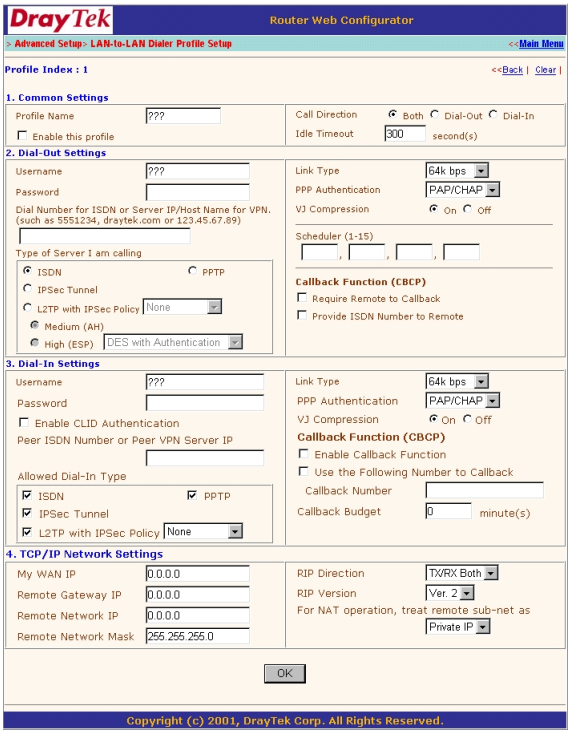
**Set to Factory Default:** Clicking here will clear all the LAN-to-LAN profiles.

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

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

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

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




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

### Common Settings

**Profile Name:** Specifies a name for the remote network.

**Enable this profile:** Check here to activate this profile.

**Call Direction:** Specifies the call direction for this profile. **Both** means it can be used for outgoing and incoming access. **Dial-**

**Out** means it can only be used for outgoing access. **Dial-In** allows only incoming access.

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

**Dial-Out Settings**

**Username:** Specifies a username for authentication by the remote router.

**Password:** Specifies a password for authentication by the remote router.

**Dial Number for ISDN or Server IP/Host Name for VPN:** Specifies the destination ISDN number for dialup.

**Type of Server I am calling:** Checks **ISDN** to indicate the dial-out type.

**Link Type:** Indicates the dial-out link type.

Disable: Deactivates the dial-out action.

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

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

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

**PPP Authentication:** Specifies 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.

The callback function is implemented by the CBCP protocol which is part 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.

**Dial-In Settings**

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

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

**Enable CLID Authentication:** Limits the dial-in router to calling from a specific ISDN number.

**Peer ISDN Number or Peer VPN Server IP:** If CLID Authentication is enabled, enter the remote VPN server IP address in this field.

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

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

**Callback Function (CBCP)**

**Enable Callback Function:** Checking here allows this router to accept requests from a remote router for call back.

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

### 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.

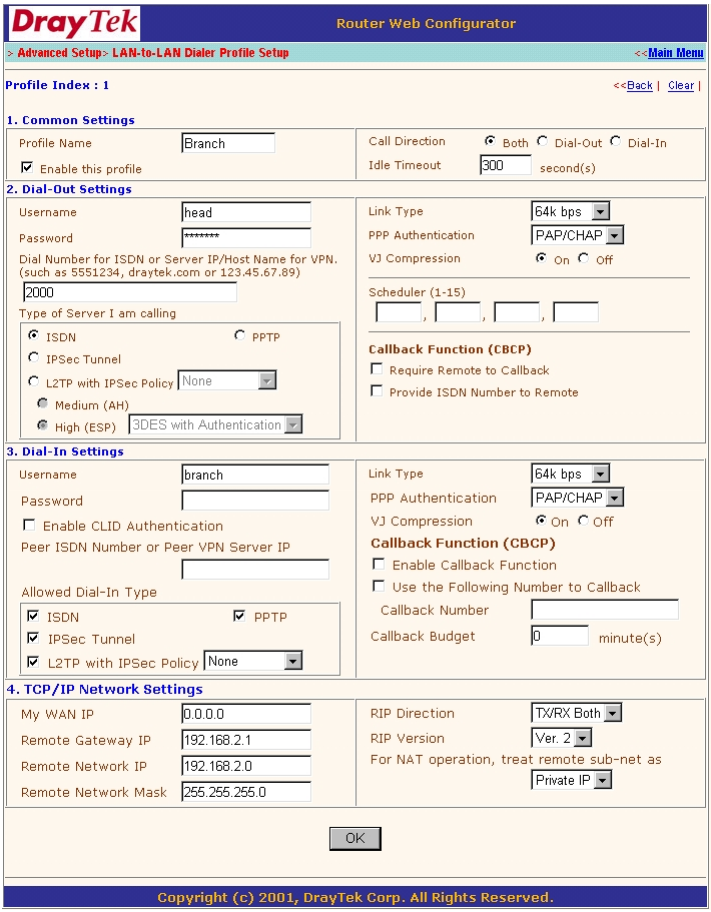
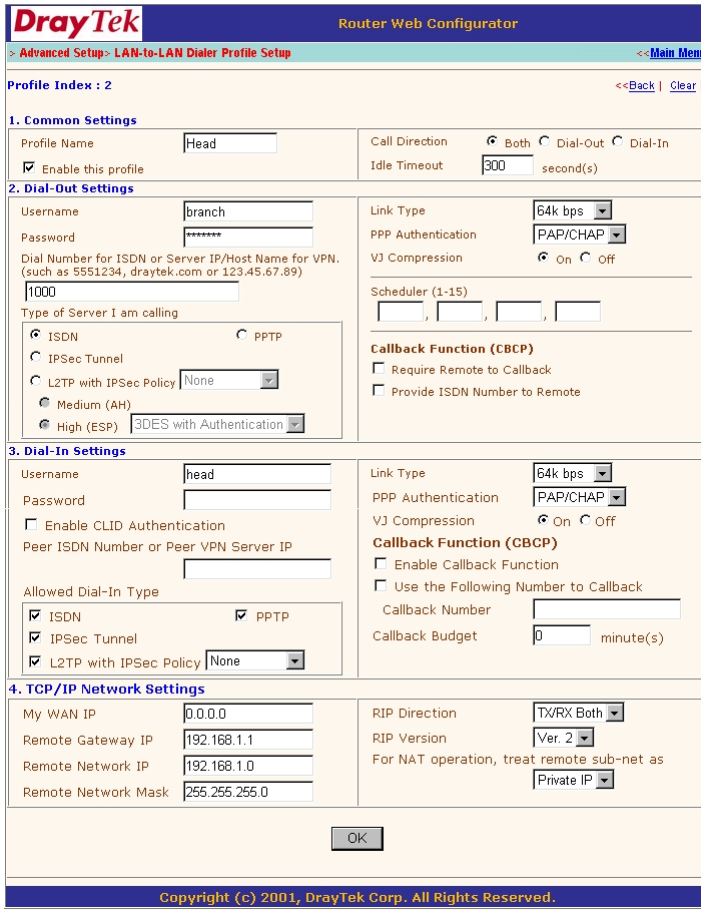
**RIP Direction:** The option specifies the direction of RIP (Routing Information Protocol) packets through the ISDN WAN connection.

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

**For NAT operation, treat remote sub-net as:** The router has two local IP networks: the1st subnet and 2nd subnet. Here you set which subnet will be used as local network for ISDN connection and 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 4.4.2. The LAN-to-LAN Dialer Profile could be configured as below.

**Head Office:**



## Branch Office: