# BIPAC-645

## DSL/Cable Router Plus ISDN Router

**With 4-Port 10/100M LAN Switch**

User's Manual

# Table of Contents

# Chapter 1
# Introduction

## 1.1 An overview of BIPAC-645

BIPAC-645 provides fast Ethernet port for connecting to ADSL modem or Cable modem. It allows all users in a local network to be quickly and easily connected to high-speed Internet (via DSL or Cable service) using PPPoE. The ISDN Router is built-in and acts as a backup when the DSL/Cable service fails or if the service is not available. In addition, BIPAC-645 supports remote ISDN dial-in and remote access.

BIPAC-645 is a small desktop router that sits between your local Ethernet network and a remote network (For example, the Internet or a remote office). It contains an ISDN S/T interface, a 10 Mbps WAN port, four 10/100 Base-T LAN ports, and an auxiliary port for a directly connected management console.

With BIPAC-645, users don't need to worry about a shortage of IP address resources. Dozens of network users can surf on the Internet simultaneously by using one ISP account and a single IP address.

Sitting between your computer and remote network, the device acts as a firewall and protects your computer from unwanted intruders.

BIPAC-645 supports Bandwidth-on-Demand and Dial-on-Demand. Depending on the data flow through an open B channel, the device will establish another B channel connection to allow greater data throughput. This extra line will then be dropped again, once the demand decreases, saving money on phone calls.

## 1.2 Package contents

1. BIPAC-645
2. AC Power Adapter (9V, 1Amp)
3. RS-232 cable (Null modem type)
4. RJ-45 ISDN cable
5. RJ-45 LAN cable
6. CD containing the on-line manual
7. Quick Start Guide

## 1.3 BIPAC-645 Features

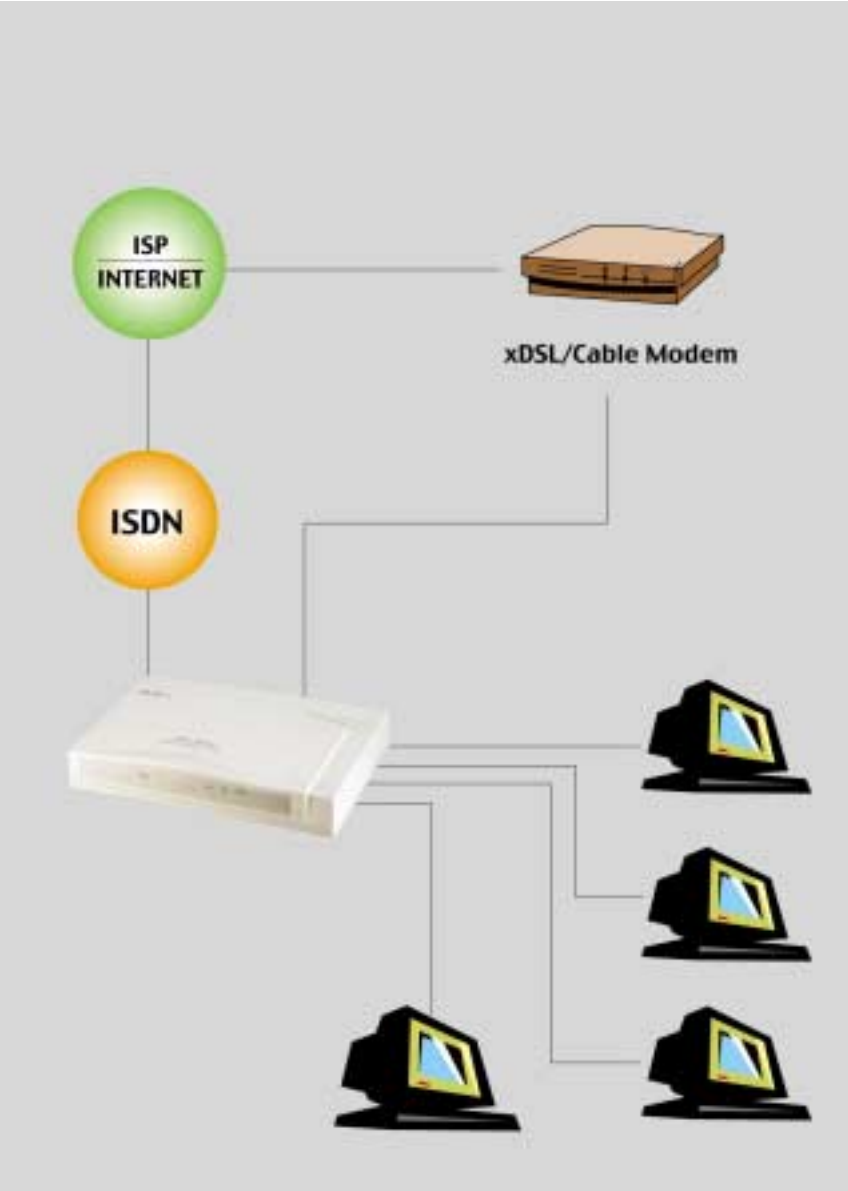
BIPAC-645 provides the following features

- The 10 Mbps broadband router, equipped with a single ISDN Basic Rate Interface (2B+D) that supports S/T interface specification, will also support European ISDN requirements.

- Supports remote access functions among branch offices and allows remote users to dial-in to your network.

- Supports IP sharing function, allowing multiple users share one internet account.
- Supports industry standard Point-to-Point Protocol (PPP), Multilink PPP, and PPPoE.
- Supports Dial-on-Demand and Bandwidth on Demand function.
- User-friendly management through web-based configurator, telnet management, console port management, and remote upgrades.
- PAP/CHAP/MS-CHAP, Call Back, IP Packet Filtering, and Caller ID Authentication for firewall security.
- Supports operating systems such as Windows 95/98/NT/2000/ME, Mac, Unix and Linux

## 1.4 This Router Device Application



# Chapter 2
# Using BIPAC-645

## 2.1 Cautions for using BIPAC-645

*Do not place BIPAC-645 under high humidity and high temperature.*

*Do not use the same power source for BIPAC-645 with other equipment.*

*Do not open or repair the case yourself. If BIPAC-645 is too hot, turn off the power immediately and have a qualified serviceman repair it.*

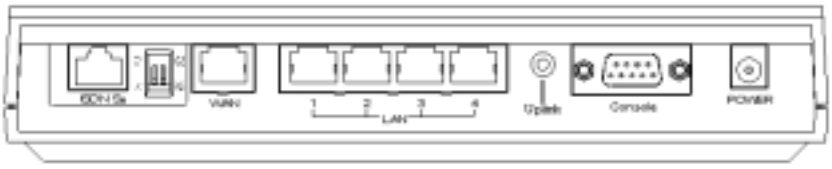
*Place BIPAC-645 on the stable surface.*

*Only use the power adapter that comes with the package.*

## 2.2 The front LEDs


| LED | | Meaning |
|---|---|---|
| 1 | **Power** | **Lit** when AC power is connected |
| 2 | **LAN 1-4 / ACT/COL** | **Lit** Green when connected to a LAN device<br>**Flashes** Green when sending/receiving data<br>**Flashes** Yellow when collisions happen |
| 3 | **WAN/ ACT / COL** | **Lit** Green when connected to a WAN device<br>**Flashes** Green when sending/receiving data<br>**Flashes** Yellow when collisions happen |
| 4 | **PPP** | **Lit** when PPPoE connection is activated |
| 5 | **ISDN / SYNC** | **Lit** when ISDN Layer 1 is activated |
| 6 | **ISDN / B1/B2** | **Lit** Green when B1 channel is activated<br>**Lit** Yellow when B2 channel is activated<br>**Lit** Green +Yellow when B1 and B2 channels are activated |

# 2.3 The rear ports



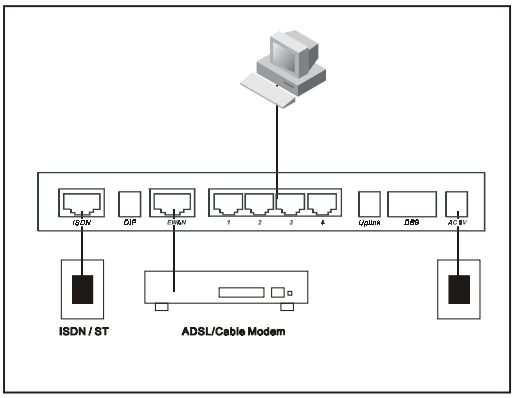
| | |
|---|---|
| **Power (jack)** | Connect the supplied power adapter to this jack |
| **Console (port)** | Connect the supplied RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port). |
| **ISDN So (RJ-45 connector)** | Connect an RJ-45 cable to this port when connecting to the ISDN. |
| **LAN 1-4 (RJ-45 connector)** | Connect an UTP Ethernet cable to this port when connecting to a LAN such as an office or home network. |
| **WAN (RJ-45 connector)** | Connect an UTP Ethernet cable to this port when connecting to the Internet or making other WAN connections |

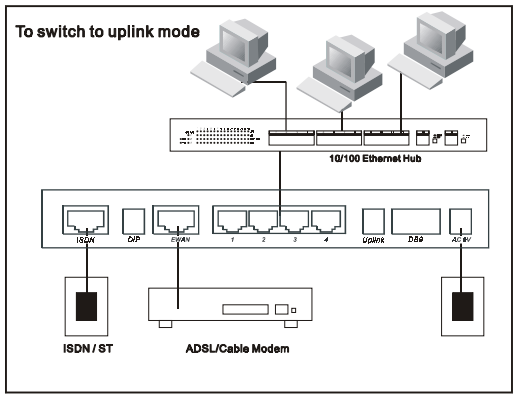
# 2.4 Cabling

Now you should be ready to connect your BIPAC-645 on your LAN and WAN or ISDN jacks. Follow these steps to install:

- Connect the router from EWAN port to an ADSL/cable modem, or attach the ISDN line to the ISDN connector (S/T interface).

- Connect the PC to the RJ-45 LAN connector. Two or more PCs can connect to a multi-port Hub first and then uplink (cascade) port on the hub must be connected to LAN port.



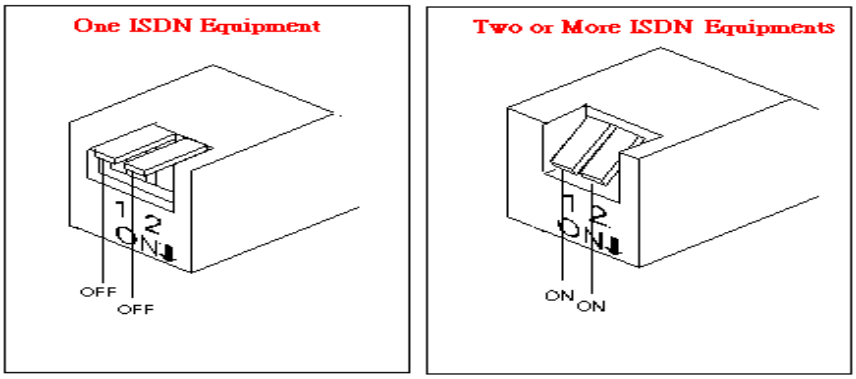




- Plug the power adapter into a wall outlet and into the AC connector on the back of BIPAC-645.

- The Auxiliary connector is only used to connect a terminal to run the Command Line Interface using the null modem cable. (This is an optional connection.)

- There is a DIPswitch located on the rear panel for setting the terminating resistor.

You only need to adjust this switch if there are two or more external ISDN equipments attached to the local telephone line.



# Chapter 3
# Configuration

## 3.1 Before Configuration

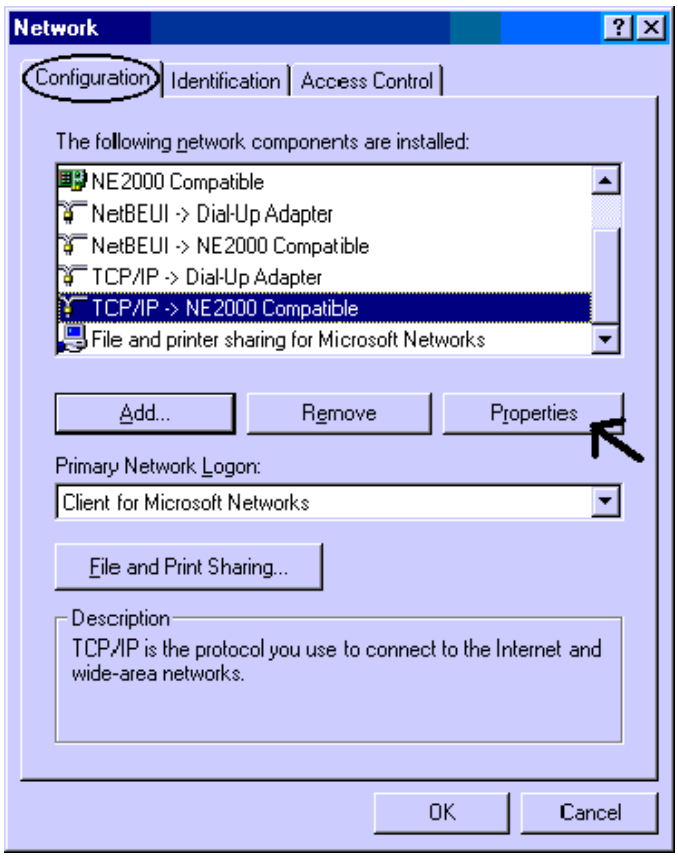
This section describes the configuration required by LAN-attached PCs that communicate with BIPAC-645, either to configure the BIPAC-645, or for network access. These PCs must have an Ethernet interface installed properly, be connected to the BIPAC-645 either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server.

Directly connect a Windows OS to the BIPAC-645. If TCP/IP is not already installed, follow the steps below for its installation.

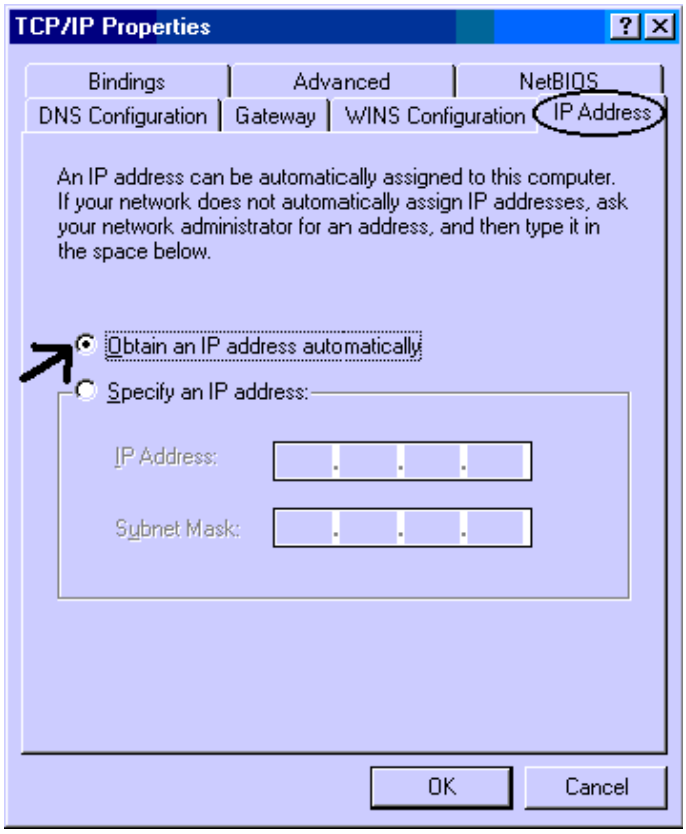

**Any TCP/IP capable workstation can be used to communicate with or through BIPAC-645. To configure other types of workstations, please consult the manufacturer's documentation**

## Configuring PC in Windows 95/98/ME

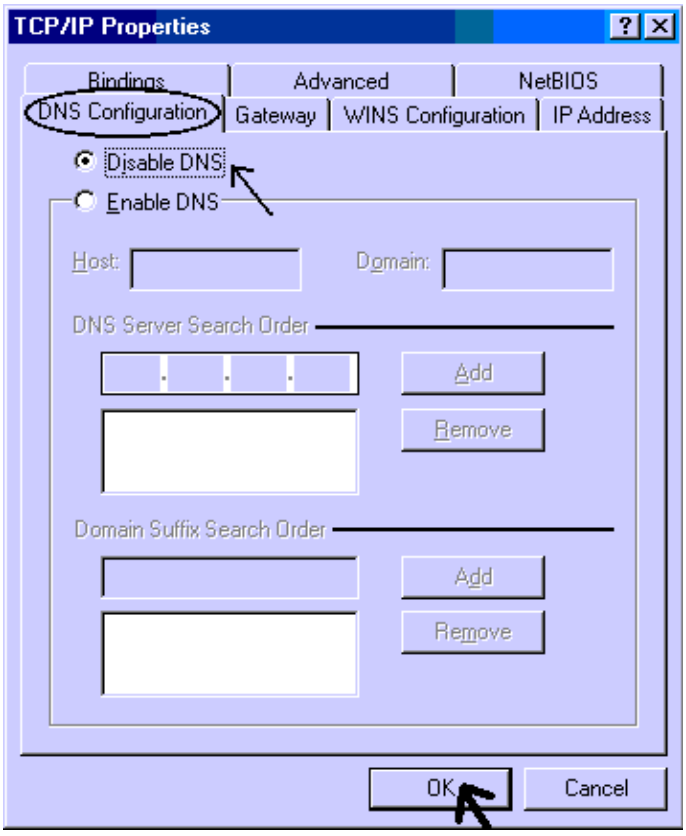
1. Go to **Start/Settings/Control** Panel. In the Control Panel double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP -> NE2000 Compatible**, or any Network Interface Card (NIC) in your PC.



3. Select the **Obtain an IP address automatically** radio button.

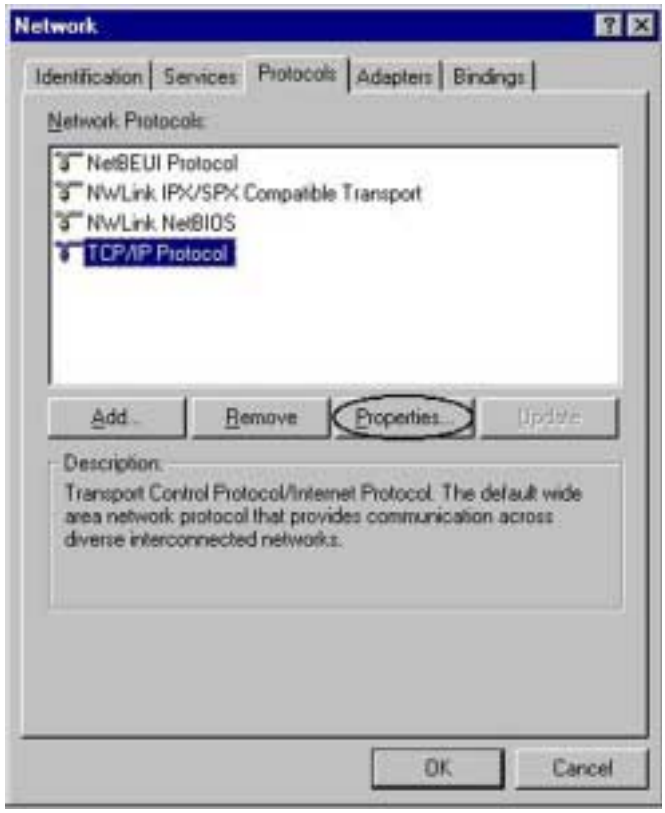



4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

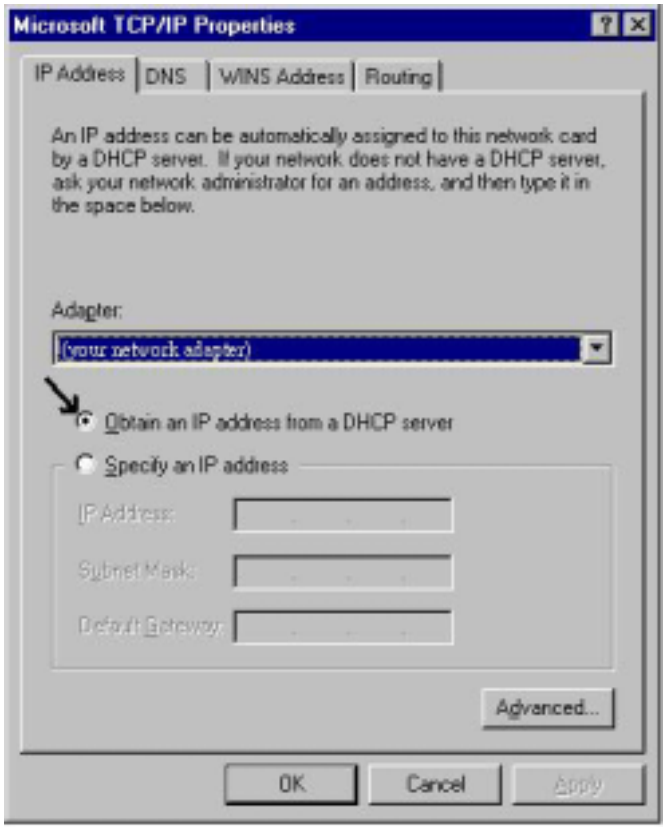


# Configuring PC in Windows NT4.0

1. Go to **Start/Settings/ Control Panel**. In the Control Panel double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.

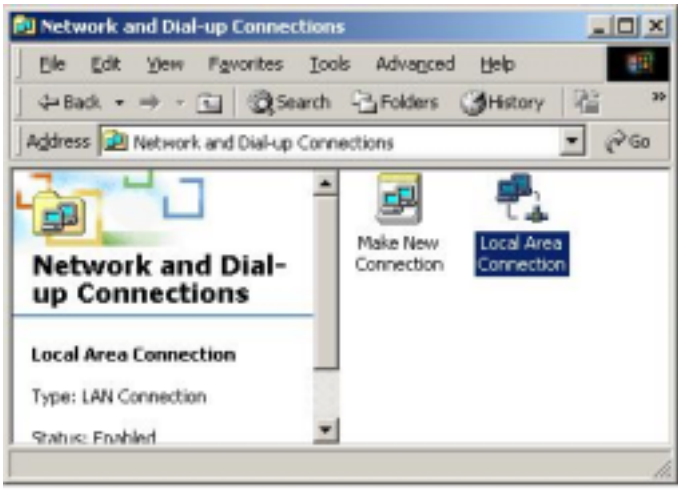



3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.

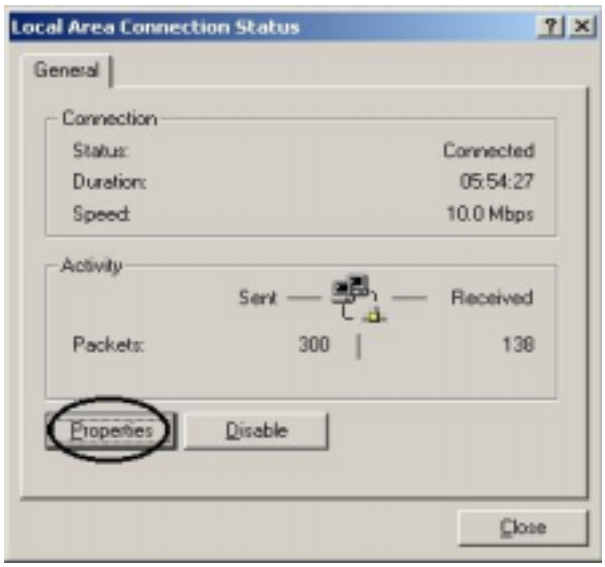


# Configuring PC in Windows 2000

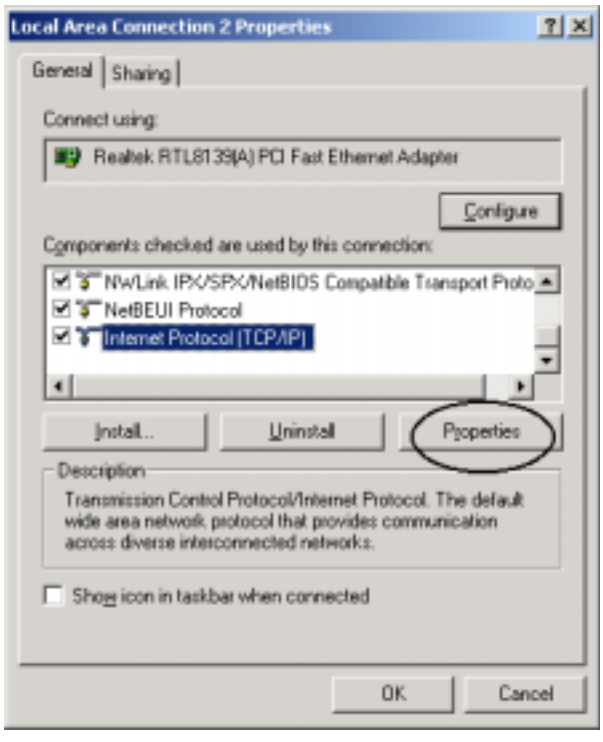
1. Go to **Start/Settings/Control Panel**. In the Control Panel double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.



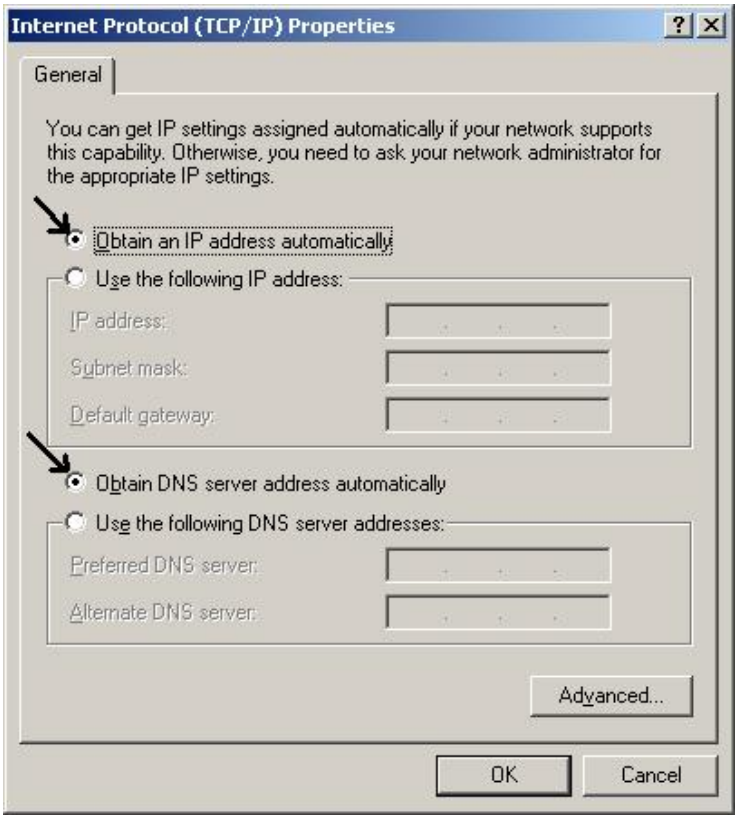

3. In the **Local Area Connection Status** window click **Properties**.




4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.




# 3.2 Configuring with GUI program

## 3.2.1 Using Different Browsers for BIPAC-645

To configure your BIPAC-645, you can use a popular browser, such as Netscape 4.x and Internet Explorer 5.x. The following describes how to use it to start "Local Router Manager" through IE or Navigator.

**Netscape Navigator 4.x:**

In the Location box (where you normally enter the URL address), enter the default private IP address of this BIPAC-645 followed by hitting the return key:

http://192.168.168.230

**Internet Explorer 5.x:**

In the Address box (where you normally enter the URL address), enter the default private IP address of this BIPAC-645 followed by hitting the return key:

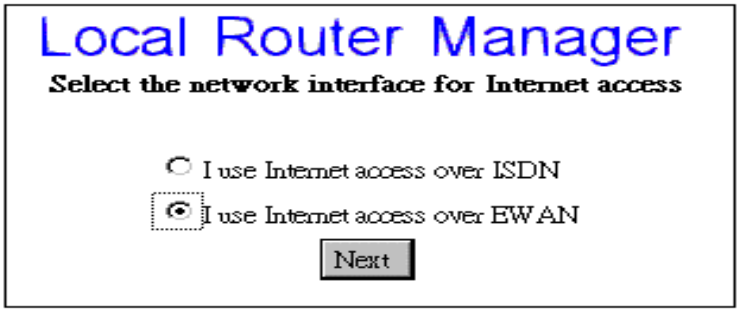
http://192.168.168.230

## 3.2.2 Password

A password screen will ask you to log on after you enter the default IP address described above. If you are logging on for the first time, you should accept the factory default password (which is "password"). The password is always displayed as a string of asterisks ("*"). Clicking the **Log On** button will begin the Configurations for BIPAC-645.


The next time you log in, even if you have modified the password, the default password ("password") will still be used as the default. You need to change it to the correct password before you will be let in. No matter what password you use, each character will always be displayed as a "*". If you forget the password, you need to follow the steps described in the later chapter to be able to log on.

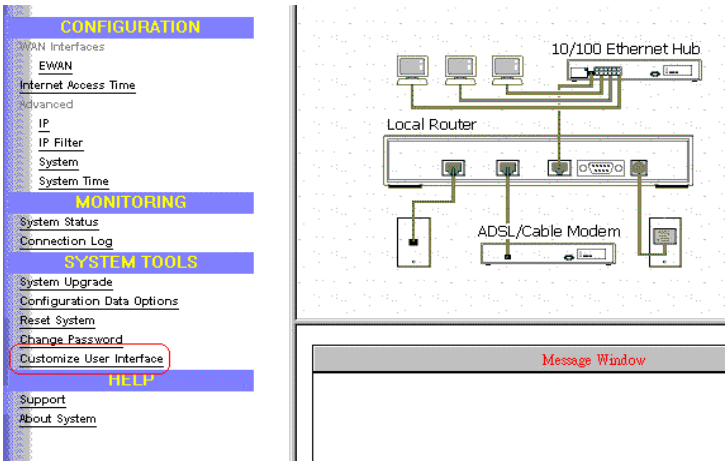
After you clicking **Log On**, the following screen will display, and you must select either ISDN or EWAN as interface for Internet Access. Click **Next** to proceed the configuration. Please see the following context for details.




### 3.2.3 Customize User Interface

When you enter into the main configuration window, click "**Customize User Interface**" in the **SYSTEM TOOLS** Menu on the left side of the screen, allowing you to customize **Local Router Manager** to suit your own specific needs: The selections you make determine what configuration menus and buttons will appear in the screen. For example, if you select **Basic Internet Access** only, the interface will only display buttons that you need for basic Internet access.

If you subsequently use Local Router Manager to configure BIPAC-645 for other applications, you can return to this screen to "re-customize" your interface by selecting **Customize User Interface** from the SYSTEM TOOLS Menu.



### Basic Internet Access

Select this option if you need basic Internet access. This will enable you to configure Internet Access for all of your LAN users. There are two Internet access interface selections provided by BIPAC-645: through ISDN or through EWAN.

### Internet Access with Advanced Configuration

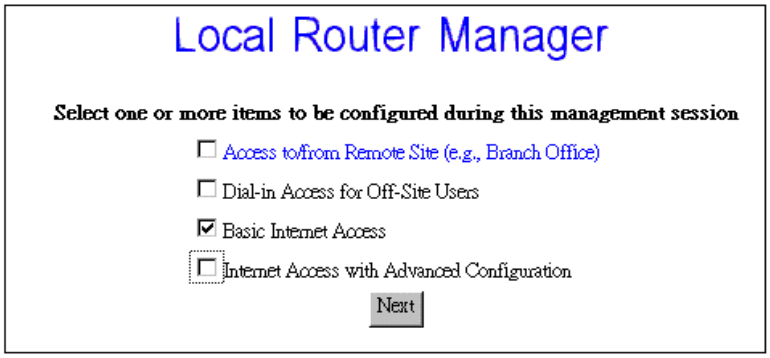
Select this option if you want to configure advanced options, such as changing the private IP address (for example, when you intend to create your own private WAN between multiple routers), or adding a public IP address (for example, when you want to install servers on the LAN which are accessible from the Internet).

### Access to/from Remote Site (e.g., Branch Office)

Select this option if you want to create connections to other LAN sites, that is, users at each site can share resources. If you use Windows PCs, for example, then from Network Neighborhood facility, you can access files from remote PCs directly. This feature is valid only when you select ISDN as interface for Internet access.

### Dial-in Access for Off-Site Users

Select this option if you want to allow users on a stand-alone computer to dial in and access resources on your network. This feature is valid only you select ISDN as interface for Internet access.




Click **Next** when you have selected the options you want. The quantity of selections is not limited but step-by-step configuration is recommend.

## 3.2.4 Basic Internet Access Configuration via EWAN


**EWAN is Ethernet WAN port that you can use xDSL/Cable modem via internet access.**

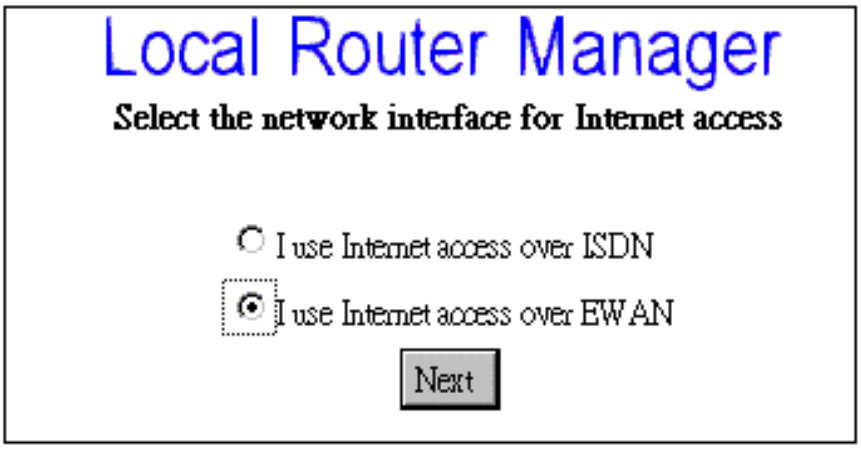
This section describes the steps to set configuration for **Basic Internet Access** via EWAN.

You will find that BIPAC-645 is optimized for **Basic Internet Access**. You don't need to understand, to apply for or to assign any IP addresses in your entire network. BIPAC-645 does these things for you automatically. You need to configure each device on your LAN in a uniform way described in Chapter 2.

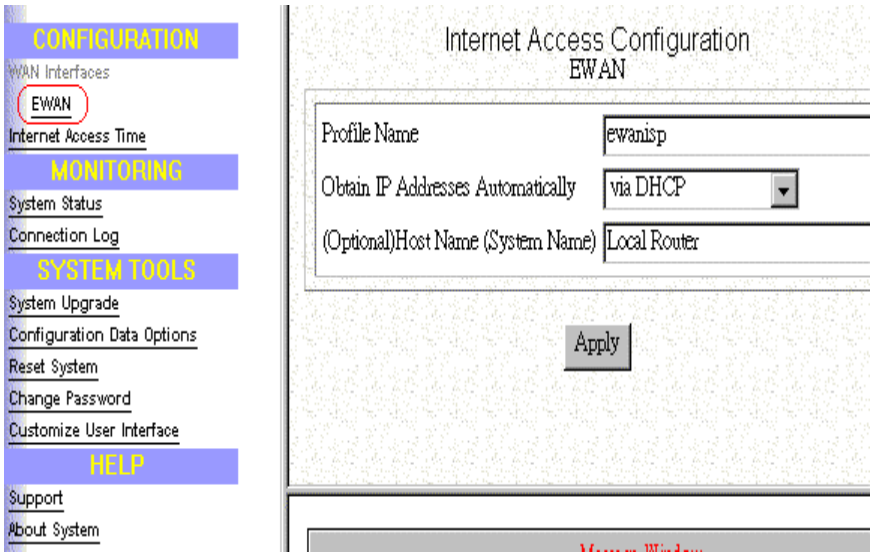
What is Basic Internet Access? It means accessing the Internet, surfing the web, accessing a remote FTP server (to send or receive files), and sending and receiving e-mail. These are the tasks that users perform most.

When you apply for an account with your Internet Service Provider (ISP), you will be given the username, password, and other necessary information. Follow the steps below.

**Step 1:** When you logon, select **Customize User Interface** in the SYSTEM TOOLS Menu. Accept the **Basic Internet Access** selection and click **Next**. The following window will be displayed , and select " **I use Internet access over EWAN** ". Click **Next**.

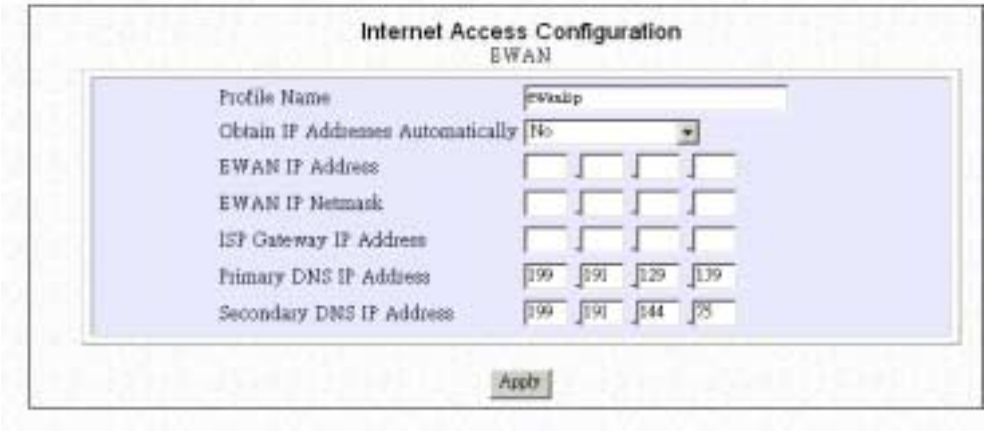



**Step 2:** Click **EWAN** in the CONFIGURATION Menu.




First you need to make a decision about **Obtain IP Address Automatically.** Available options are **via PPP over Ethernet**, **via DHCP**, or **No**. If you choose **No** go to step 3. If you choose **via DHCP** go to step 4, and if you choose **via PPP over Ethernet** go to step 5. If you choose **via PPTP**, go to step 6.

**Step 3**: If you choose **No** for the selection of **Obtain IP Address Automatically.** The following screen will be displayed. Enter the following information and then Click **Apply.**




**Profile Name:** the name that you will use to identify this Internet access profile.

**EWAN IP Address:** the IP address of your EWAN.

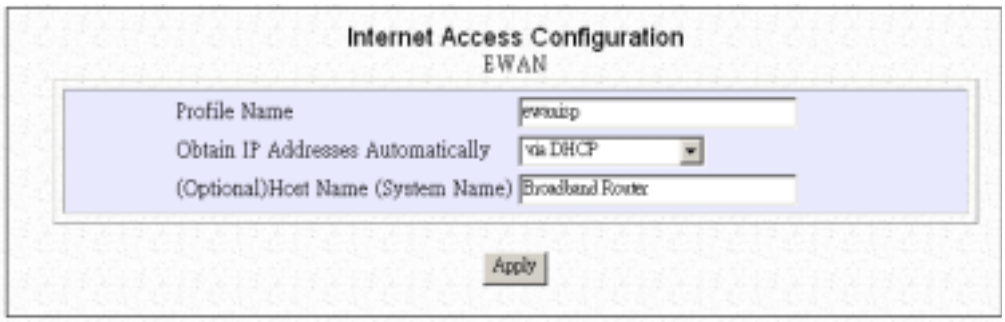
**EWAN IP Netmask:** the IP Netmask of your EWAN.

**ISP Gateway IP Address:** the IP Address of your ISP Gateway

**Primary DNS IP Address:** the IP Address of your Primary DNS.

**Secondary DNS IP Address:** the IP Address of your Secondary DNS

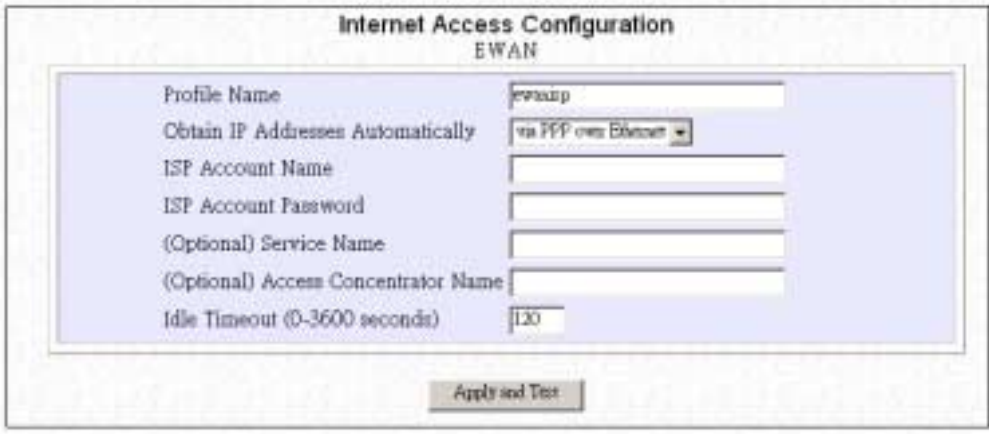
**Step 4:** If you choose **via DHCP** for the selection of **Obtain IP Address Automatically.** The following screen will be displayed. Enter the following information and then Click **Apply.**




**Profile Name:** the name that you will use to identify this Internet access profile.

**(Optional) Host Name (System Name):** the Host Name provided by your system.

**Step 5**: If you choose **via PPP over Ethernet** for the selection of **Obtain IP Address Automatically.** The following screen will be displayed. Enter the following information and then Click **Apply and Test.**



**Profile Name:** the name that you will use to identify this Internet access profile

**Obtain IP Addresses Automatically:** get the IP Address via PPP over Ethernet. Some DSL-based ISPs use PPPoE to establish communications with an end-user. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE

**ISP Account Name:** the username of your ISP account

**ISP Account Password:** the password of your ISP account

**(Optional) Service Name:** Enter the Service Name provided by your ISP if it is required.

**(Optional) Access Concentrator Name:** Enter the Access Concentrator Name provided by your ISP if it is required.

**Idle Timeout (0-3600 seconds):** The default value of the idle timeout is 120 seconds. It represents the number of seconds of inactivity over the connection: when this value is reached, BIPAC-645 will disconnect the connection. You can change the idle timeout value to anything between 0 to 3600 seconds. But if you select **0**, the connection never times out.

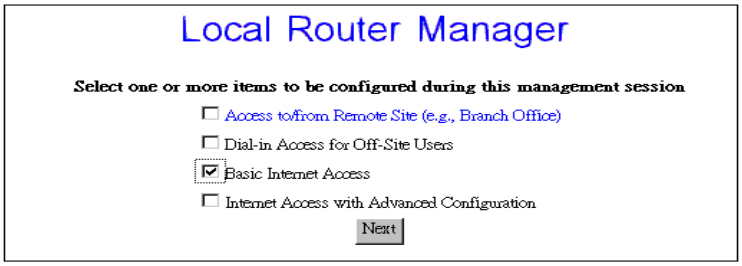
**Step 6**: If you choose **via PPTP** for the selection of **Obtain IP Address Automatically.** The following screen will be displayed. Enter the following information and then click **Apply and Test.**


***When you click Apply or Apply and Test, BIPAC-645 connects to your Internet Service Provider. Watch the Message Window for any messages. When the test is successful, your users will be ready to access the Internet.***

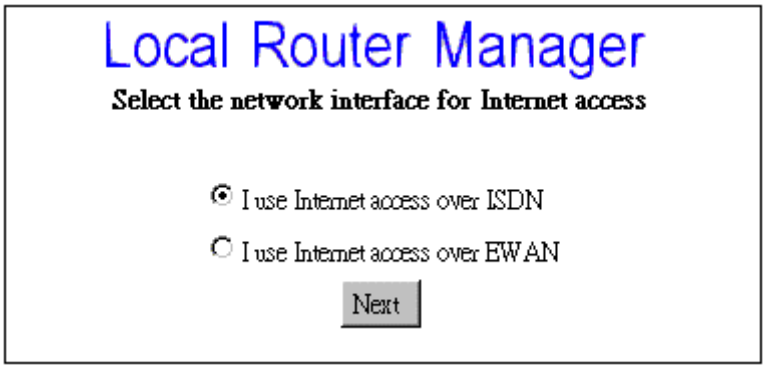
## 3.2.5 Basic Internet Access Configuration via ISDN

This section describes the steps to set configurations for **Basic Internet Access** via ISDN. When you apply for an account with your Internet Service Provider (ISP), you will be given the necessary information, including your account name, account password, and the ISP's local access ISDN telephone number. Have these available and then follow the steps below.

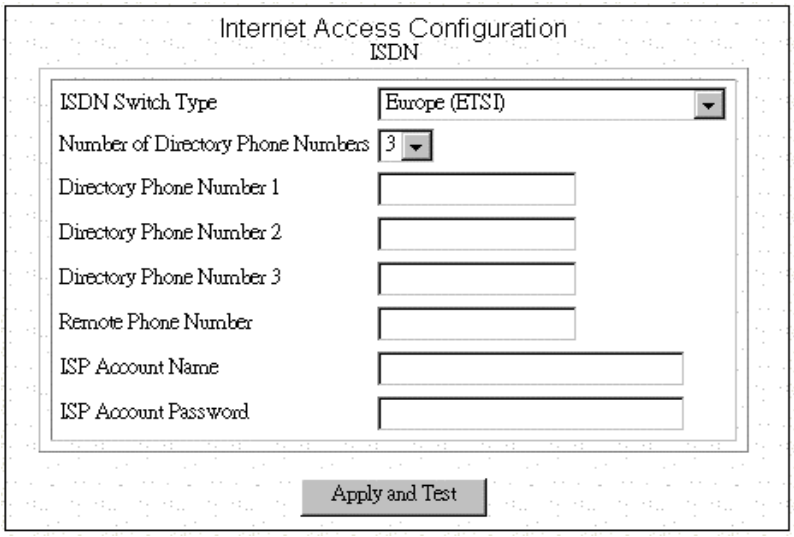
**Step 1:** When you logon, select **Customize User Interface** in the SYSTEM TOOLS Menu. Accept the **Basic Internet Access** selection and click **Next**. The configuration window will be displayed,



**Step 2:** Select **I use Internet Access over ISDN** and then click **Next**.




**Step 3:** Select **ISDN** in the Configuration Menu and the following screen will appear.




**Step 4:** Select the ISDN switch type that your ISP will tell you.

**Step 5:** Select the number of the directory phone numbers and enter the directory phone numbers in the corresponding blanks.

**Step 6:** Enter the following information:

**Remote Phone Number:** the ISDN telephone number of your ISP.

**ISP Account Name:** the username of your ISP account.

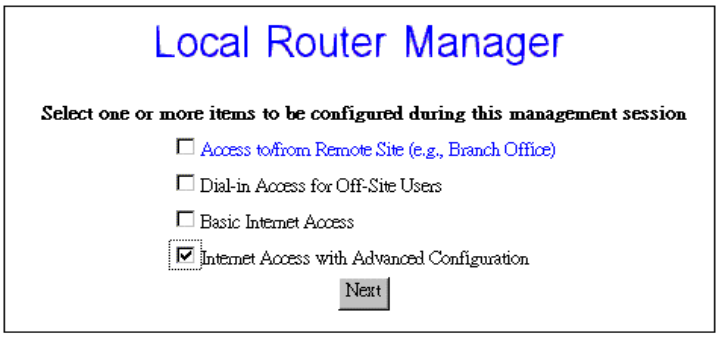
**ISP Account Password:** the password of your ISP account.

**Step 7:** Click **Apply and Test.**

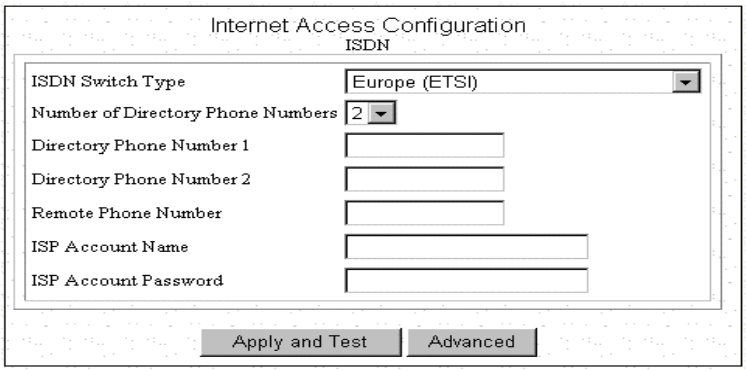
After the successful **Apply and Test,** any users in the LAN should restart their PC. Now you can surf in the Web, receive E-mails, or transmit files. For more advanced configurations, refer to the following context.

## 3.2.6 Internet Access with Advanced Configuration

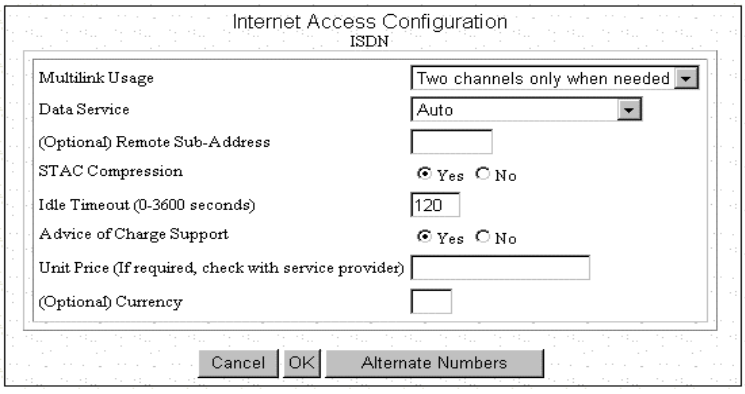
After completing basic Internet access configurations via ISDN, now you can set advanced ISDN Configuration if you back to the Local Router Manager screen and select Internet Access with Advanced Configuration.




**Step 1**: After entering the following parameters as the way described in the previous section. Click **Advanced.**




**Step 2:** The following configuration window will appear.




**Step 3:** Set **Multilink Usage** parameters. This determines how the device utilizes the two B channels for your Internet connection. Available options are:

**One B Channel Only:**

**Two B Channels Only When Needed:**

**Always two B Channels:**

**Step 4:** Select **Data Service**. Available options are **Data Over Voice Channel**, **64K** , **56K** , and **Auto**. Recommended selection is **Auto**.

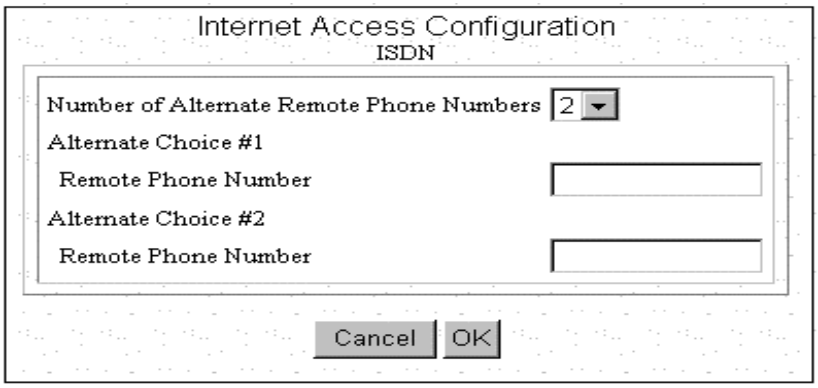
**Step 5:** Enter **Remote Sub Address Number** if necessary.

**Step 6:** Select **STAC compression** option.

**Step 7:** Set **Idle Timeout** number. The range is from 0 to 3600 seconds.

**Step 8:** Select **Advice of Charge Support** option and enter the **Unit Price** and **Currency** in the corresponding blanks if the selection is **Yes**.

**Step 9:** Click **OK** to return to the main configuration screen and skip to next step. Otherwise click **Alternative Number** if there is one or more alternative remote phone numbers. Enter the alternative remote phone number in the corresponding blanks. Then press **OK** to return to the previous screen. Again press **OK** to back to main configuration screen.




**Step 10:** Click **Apply and Test**

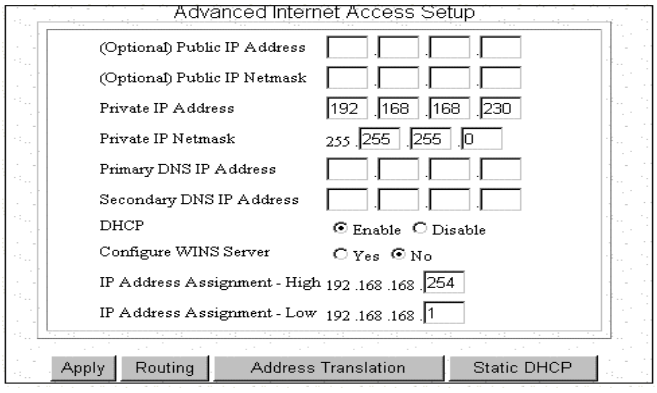
***After the test is successful, BIPAC-645 will disconnect from your ISP. If it is not successful, make any necessary changes based on progress messages that appear in the message window, and try again.***

## 3.2.7 IP Configuration for Internet Access

Using **IP** options in the Menu Window, you can assign a public IP address to the BIPAC-645, modify the private IP address, DNS addresses, and enable or disable DHCP.

**Step 1:** Select **Internet Access with Advanced Configuration** from Local Router Manager. Then click **IP** from the Menu Window.

**Step 2:** The **Advanced Internet Access Setup** screen appears:



***To install public servers on your network (For Example, Web or ftp servers), you need to apply for an IP address for each server plus one for the LAN port of this BIPAC-645. All these public IP addresses have to belong to the same IP network.***

**Set the following parameters:**

**Public IP Address:** the public IP address for the LAN interface on the BIPAC-645.

**Public IP Netmask:** the network mask for the public network address on LAN.

**Private IP Address:** the private IP address for the LAN interface on the BIPAC-645. The default private IP address is 192.168.168.230.

**Private IP Netmask:** the network mask for your private network. Its value is 255.255.255.0, and cannot be changed.

**Primary DNS IP Address:** the IP address of the primary Domain Name Server (DNS). If properly configured, when a device reboots and acquires the IP address from the BIPAC-645, the IP addresses of both the primary and the secondary DNS server will be provided for client workstations or PCs.

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

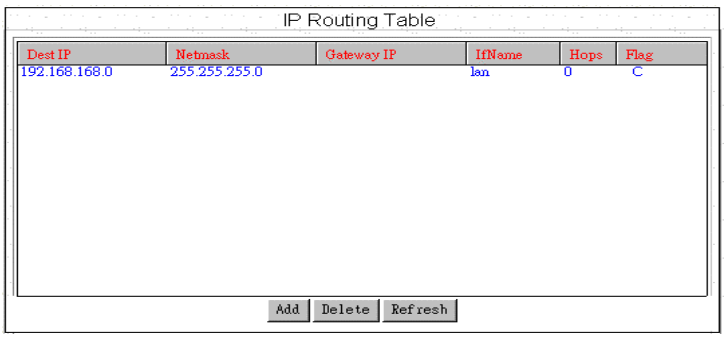
**DHCP:** If you want to act, as a DHCP server and assigns private IP addresses to any requesting DHCP client, make sure DHCP is enabled. When enabled, it will provide an IP address, network mask, gateway address (The BIPAC-645's private IP address), and DNS addresses to any workstations on the local area network that are configured as a DHCP client. Devices on your network that are configured with public IP addresses are not DHCP clients. Therefore, you need to assign their IP addresses, network mask, and default gateway's IP address, primary and secondary DNS IP addresses manually.

**IP Address Assignment-High & Low:** the setting about the maximum and minimum of private IP address for each client PC or workstation in the LAN. The range is from 1 to 254.

**Step 3:** Click **Routing**, **Address Translation** or **Static DHCP** if it is necessary to set these configurations. Otherwise click **Apply** to confirm the configuration and return to the main configuration screen.

## 3.2.8 The IP Routing Table

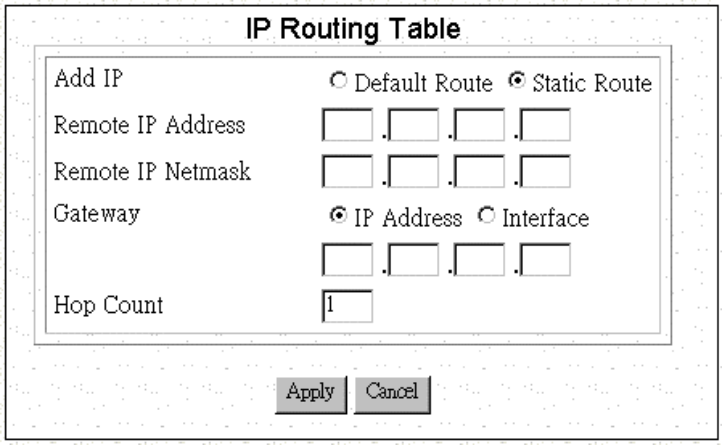
The IP Routing Table contains all the information that the BIPAC-645 needs to route an IP data packet. You can view the IP Routing Table by clicking on the **Routing** button at the bottom of the Advanced Internet Access Setup screen (described in the previous section). From this screen, you can also add new routing entries to the table. The following screen shows an example of the IP Routing Table.



An entry for a specific host or network may be added manually. An “S” in the Flags field indicates this “static route”. Other flag field entries are “**H**” for host, and “**G**” for gateway.

**Follow the steps to add or to change the default route or add a static route:**

**Step 1:** Click the **Add** button in the IP Routing Table screen to display the following screen:




**Step 2:** Enter the following information:

**Default Route:** select if you want to specify a new default route. Note that the Remote IP Address and Remote IP netmask fields do not appear if you select this option. **CAUTION**: Mis-configuring the default route may result in abnormal system behavior and/or unnecessary telephone charges.

**Static Route:** select if you want to add a static route.

**Remote IP Address:** the remote IP address of the new route.

**Remote IP Netmask:** the IP netmask of the new route.

**Gateway:** identifies if the gateway is an IP address or interface.

**Hop Count:** the maximum number of hops for this route.

**Step 3** Click **APPLY**.

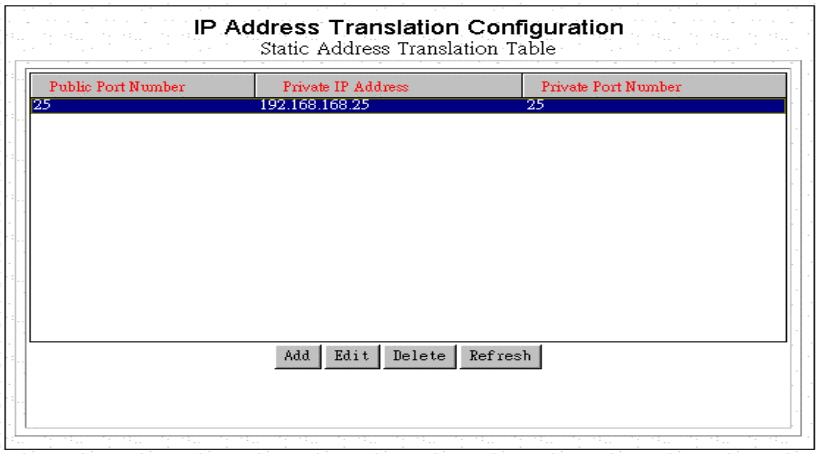
## 3.2.9 IP Address Translation Configuration

For security and economic purposes, BIPAC-645 supports Single User Account feature (SUA). Multiple users in the LAN can share a public IP address from ISP and Internet users will view the whole LAN as a big “device”. However, severs in the LAN are allowed to provide services to the Internet users if you properly configure the server’s private IP address “translated” to the corresponding service port number. For example, you can set the FTP server’s private IP address mapped to port 21. Follow the steps; it will automatically complete the mapping procedure.


**Remember to set a fixed private IP address for each server providing services to the Internet users, i.e., these servers can’t be DHCP clients.**

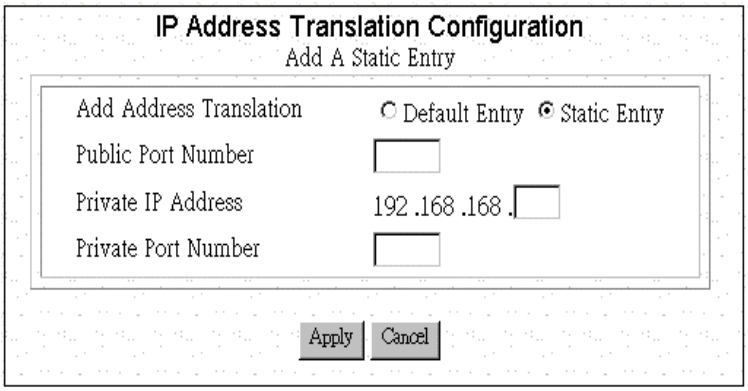
## 3.2.10 Add or Edit IP Address Translation

**Step 1**: Click **Address Translation** button in the Advanced Internet Access Setup screen. The following **IP Address Translation Configuration** screen will appear.




**Step 2:** Click **Add** for adding a set of IP address translation, or click **Edit** for editing an existing set of IP address translation after selecting the set of IP address translation that you want to edit. The Following screen will appear.

**Step 3:** Enter the following parameters.




**Add Address Translation:** Available options are Default Enter and Static Entry.

**Public Port Number:** The public port number corresponding to the service that the specific server provides.

**Private IP Address:** The private IP address that you want to assign to the server.

**Private Port Number:** The private port number corresponding to the service that the specific server provides. Public Port Number and Private Port Number should be the same.

**Step 4:** Click **Apply**.

**Delete a Set of IP Address Translation**

**Step 1:** Select the set of IP address translation that you want to delete from the IP Address Translation Configuration screen.

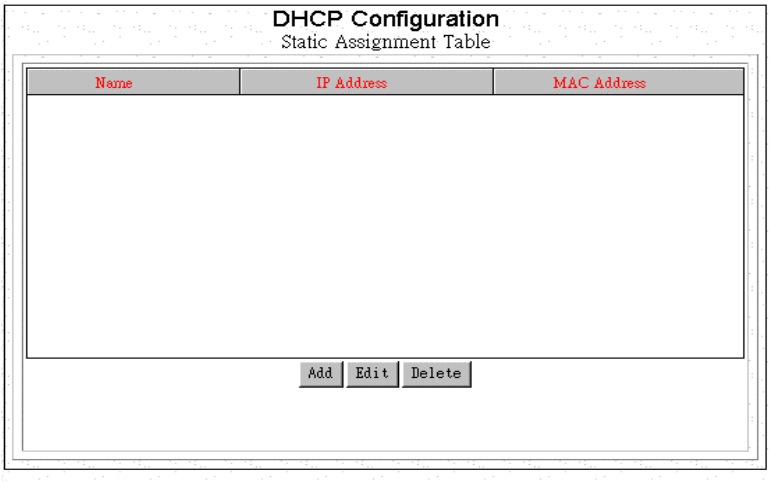
**Step 2:** Click **Edit**.

## 3.2.11 Static DHCP Configuration

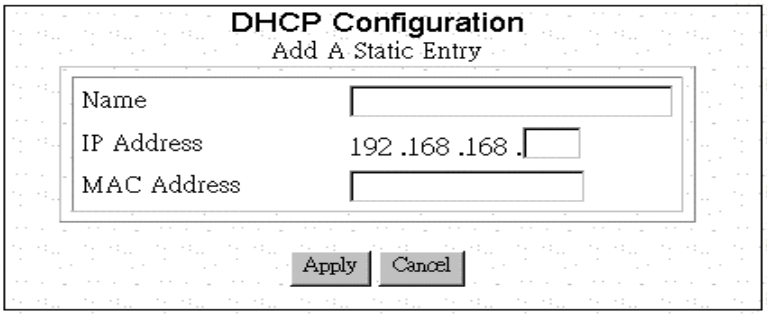
By built-in DHCP feature, the device can automatically assign a private IP address to each PC or workstation in the LAN. But under some situations, you need to set a static private IP address for certain PCs or workstations. Follow the steps to assign a static private IP address to a PC or a workstation.

### Add or Edit a Set of static private IP address

**Step 1:** Click **Static DHCP** from Advanced Internet Access Setup Screen. The following screen will appear.




**Step 2:** Click **Add** for adding a set of static private IP address, or click **Edit** for editing a existing set of static private IP address after selecting the set of static private IP address. The following screen will appear.




**Name:** A name is assigned for router manager identification purpose.

**IP Address:** The static private IP address that you want to assign.

**MAC Address:** The MAC address of the physical interface between the device and the PC or workstation.

**Step 3**: Click **Apply**.

### Delete a Set of static private IP address

**Step 1:** Select the Set of static private IP address that you want to delete form the DHCP Configuration window.

**Step 2:** Click **Delete**.

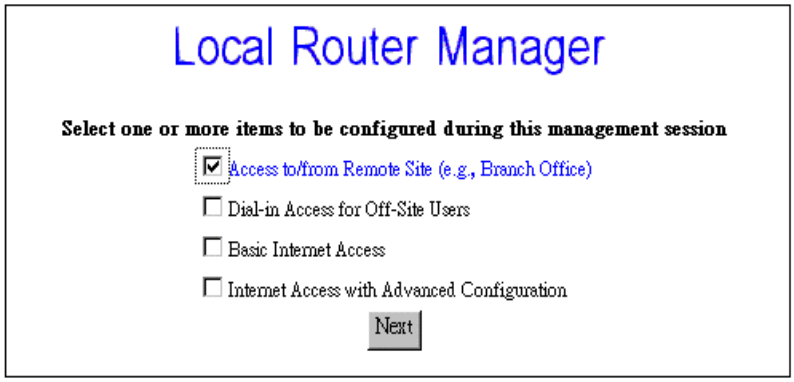
# Chapter 4
# Remote Configuration

**The remote site does not have to have a router, and may not be configurable by the local administrator. Make sure the configuration matches the requirements of the remote site.**

## 4.1 Remote Office Access by ISDN

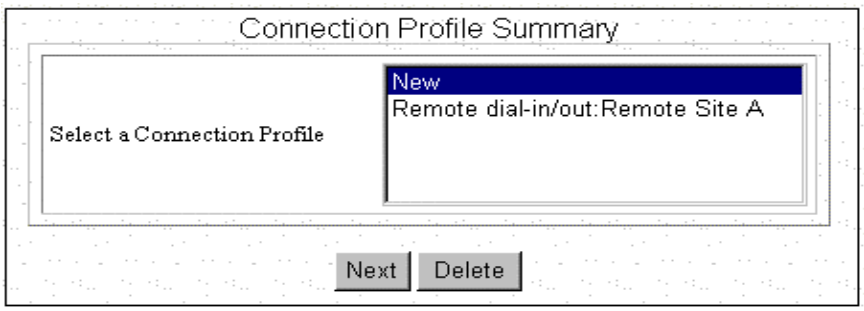
To configuring the ISDN interface for Remote Office connectivity, follow these steps:

**Step 1:** Select **Access to/from Remote Site** in the **Local Router Manager** screen and click **Next**:

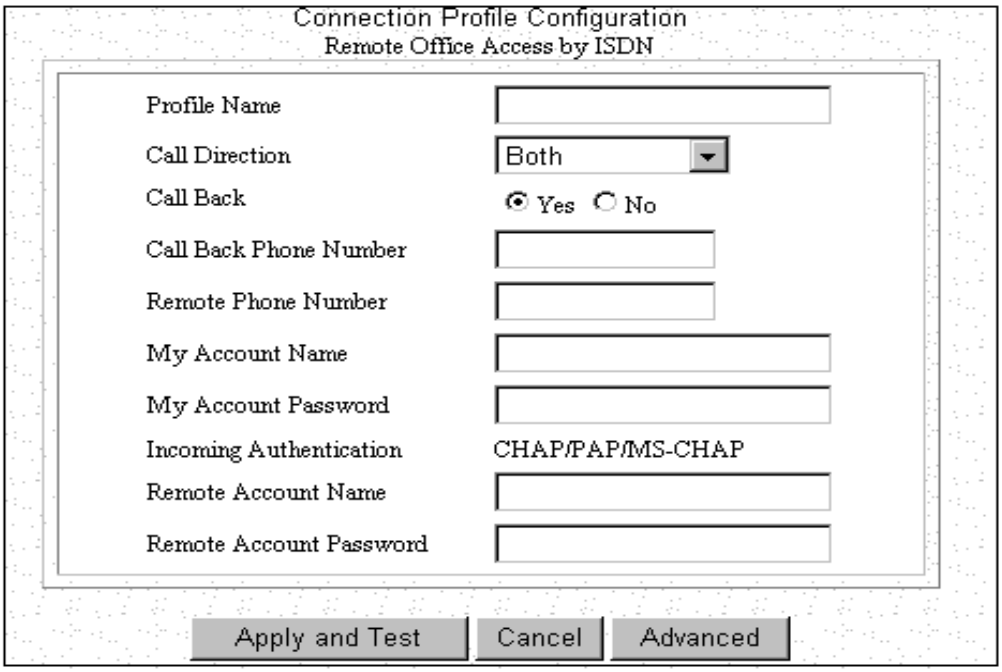



**Step 2:** If you have already configured your ISDN interface, skip to Step 3. Otherwise, configure your ISDN interface in the way described in the chapter 3.

**Step 3:** Click **Connection Profiles** in the Menu Window. The **Connection Profile Summary** window will appear if there is already any connection profile configured previously.




**Step 4:** Select **New** and Click **Next**, the **Connection Profile Configuration** window should appear as follows,




**Step 5:** Enter the following information**:**

**Profile Name:** a name associated with this profile.

**Call Direction:** if the remote site will be dialing in, select **Incoming**. If the BIPAC-645 will dial out to the remote site, select **Outgoing**. Select **Both** if either side can initiate the connection. The default setting is **Both**.

**Call Back:** if Call Back is enabled (**Yes** is selected), it checks the Remote System Name and Remote Password. If a call is received and authentication succeeds, it disconnects the incoming call, and calls the number in the Call Back field. If Call Back is not enabled (No), the Call Back Number field will not display. If the Call Direction is Outgoing only, Call Back options will not display.

**Remote Phone Number:**

**My Account Name:**

**My Account Password:**


**Make sure the remote site is configured with the same values you specify in My Account Name and My Account Password.**

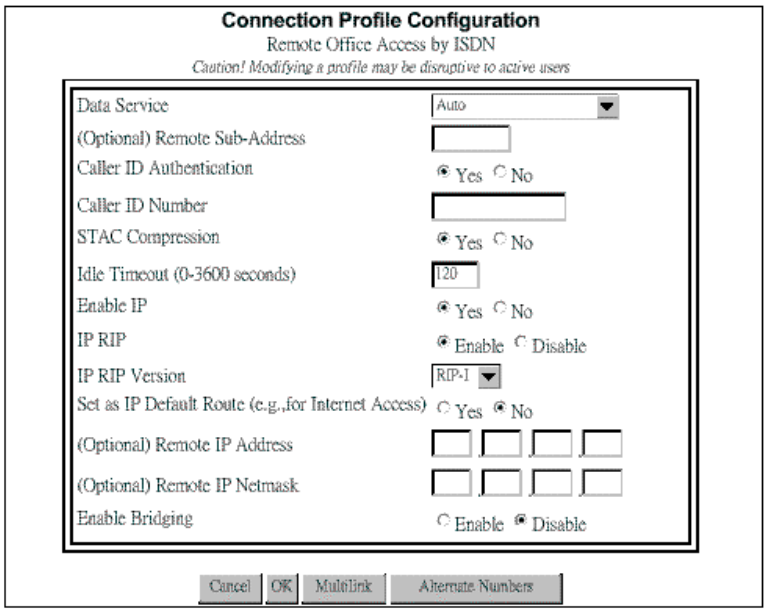
**Remote Account Name:**

**Remote Account Password:**

**Step 6:** If you selected **Outgoing** or **Both** as your **Call Direction**, click **APPLY and TEST**, or select **ADVANCED** for more options. You must still click **Apply and Test** even if the other end of the connection has not been configured. In this case the test will fail, but that can be considered normal.

# 4.2 Advanced Options for Remote Office Access Profiles

If you press the **Advanced** button from the above **Connection Profile Configuration,** the following screen appears.




**Step 1:** Set any of the following parameters:

**Data Service:** choose **64K**, **56K**, or **Auto**. Select **Auto** unless you know the speed required by the other end of the connection requiring either 64K or 56K.

**Remote Sub-Address:**

**Caller ID Authentication:** select **Yes** if you want to check the caller ID before accepting the call. This service may require a special agreement with your ISDN service provider.

**Caller ID Number:**

**STAC Compression:** allows outgoing data to be compressed to achieve higher throughput, and compressed incoming data to be recognized. The ability to use compression depends on the capabilities of the ISP.

**Idle Timeout:** the number of seconds of inactivity over the connection. When this value is reached, it will disconnect the call. You can set the idle timeout from 0 to 3600 seconds. The default setting is **120** seconds. If you select 0, the connection never times out.

**Enable IP:**

**IP RIP:**

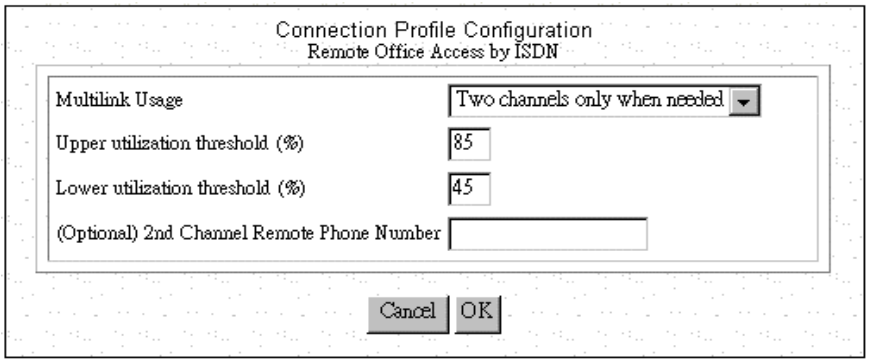
**Remote IP Address:**

**Remote IP Netmask:**

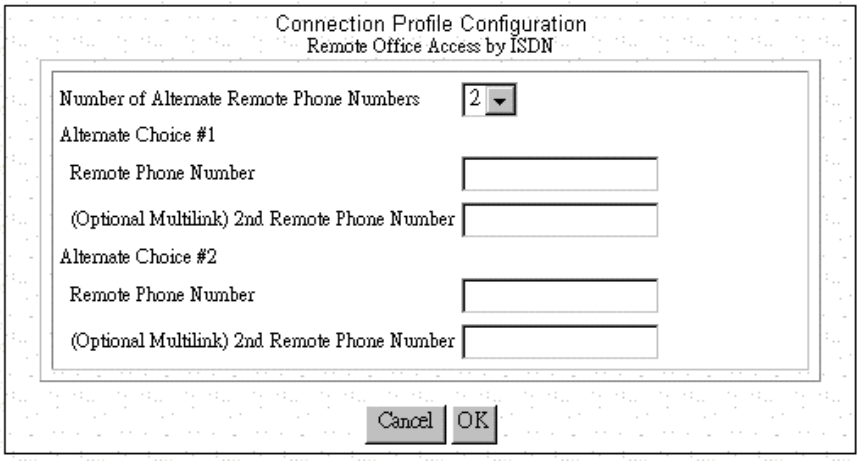
**Enable Bridging:**

**Step 2:** If advanced configuration is required for the operation on the ISDN, and its load sharing capabilities, then click **Multilink**. Alternatively skip to step 4.

**Step 3:** Click **OK** after completing the parameters in the following windows.




**Step 4:** Skip to step 6 or click **Alternative Numbers** if it is required to set more than one choice of remote phone numbers. The screen will appears as follows,




**Step 5:** Select the Number of **Alternative Remote Phone Numbers** and then enter the remote phone numbers in the corresponding blanks. Click **OK** to back to the previous screen.

**Step 6:** Click **OK** to back to main configuration screen and click **Apply and Test**.

# 4.3 Deleting Remote Office Access Profile

Follow the steps to delete a Connection Profile:

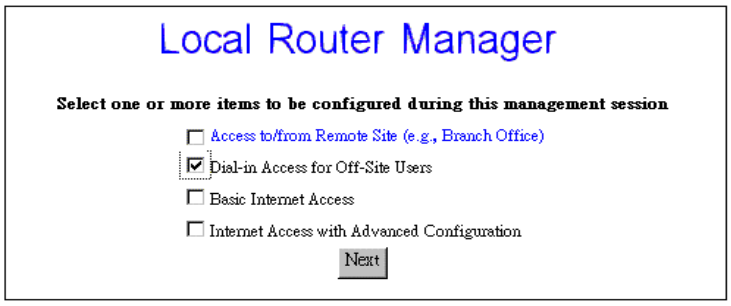
**Step 1:** Select **Connection Profiles** in the Menu Window.

**Step 2:** Highlight the entry in the list you want to delete, and click **Delete**.

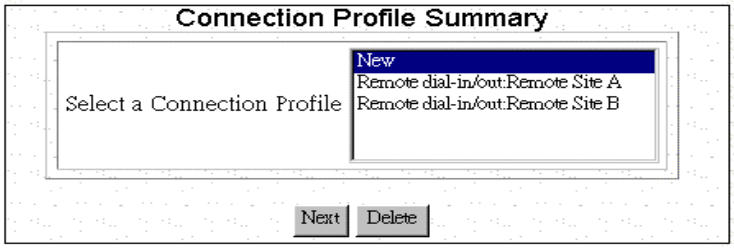
# Chapter 5
# Dial-in User Access Configuration

## 5.1 Configuring a Dial-in User Profile

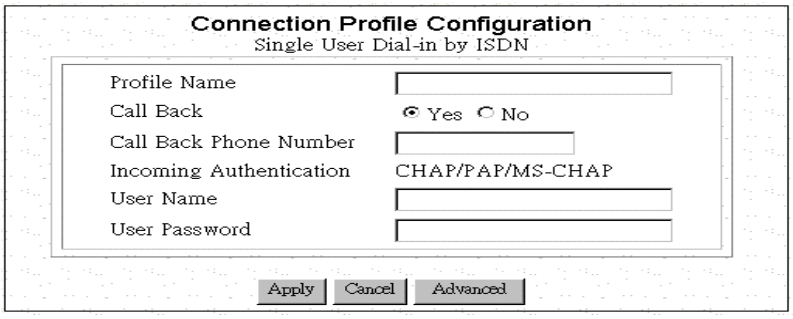
**Step 1:** Select **Dial-in Access for Off-Site Users** in the **Local Router Manager** screen.




**Step 2:** Select **Connection Profiles** from the Menu Window**.** Information about each dial-in user who is allowed to access is stored in a "connection profile." When you select **Connection Profiles**, the **Connection Profile Summary** screen appears only if there is any existing Connection Profile. Select **New** from the pull-down menu.

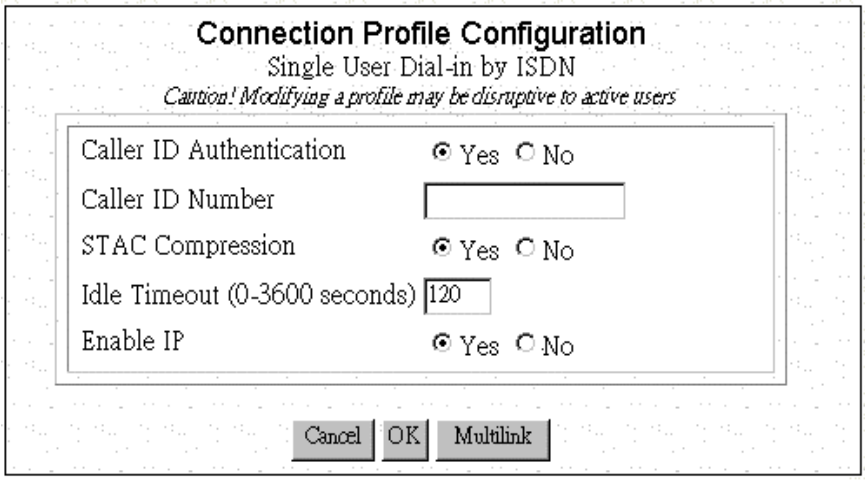



**Step 3:** Click **Next** to continue and display the **Connection Profile Configuration** screen. The following screen will appear.



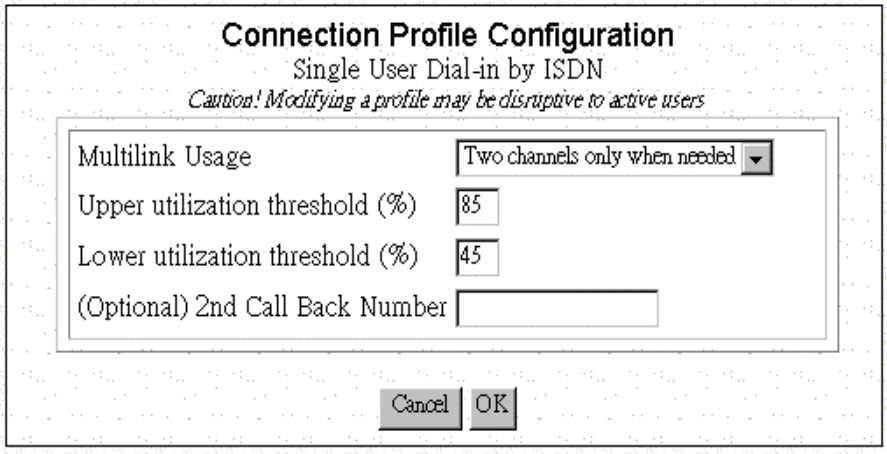

**Step 4:** Enter the information of screen:

**Step 5:** Select **APPLY** to add the connection profile to it's database, or select **ADVANCED** for more options and proceed to following steps.




**Step 6:** Enter the information:

**Step 7:** Click **OK** to return to the previous screen and click **APPLY** to add the connection profile to its database. Otherwise click **Multilink** if advanced configuration is required for the operation on the ISDN, and its load sharing capabilities. Then enter the following parameters.




**Step 8:** Click **OK** to back to the previous screen and click **OK** again to back to Connection Profile Configuration screen.

# 5.2 Deleting Dial-in User Profiles

Follow the steps to delete a Dial-in User Connection Profile.

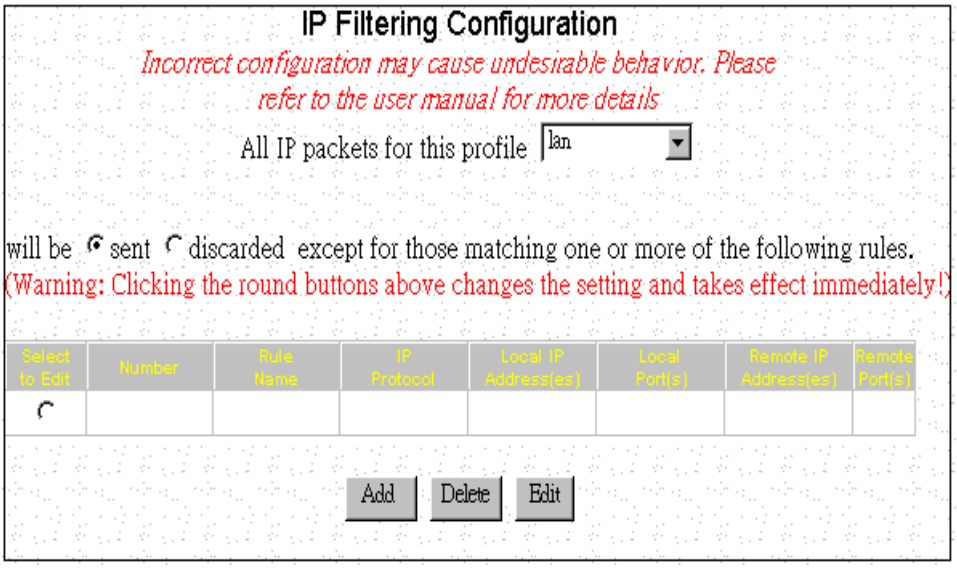
**Step 1:** Select **Connection Profiles** from the Menu Window.

**Step 2:** Highlight the entry in the list you want to delete, and click **Delete**.

# 5.3 Packet Filtering

To add a new packet rule or to edit an existing one, select **IP Filter** from the Configuration Menu. Then **IP Filtering Configuration** window will appear.

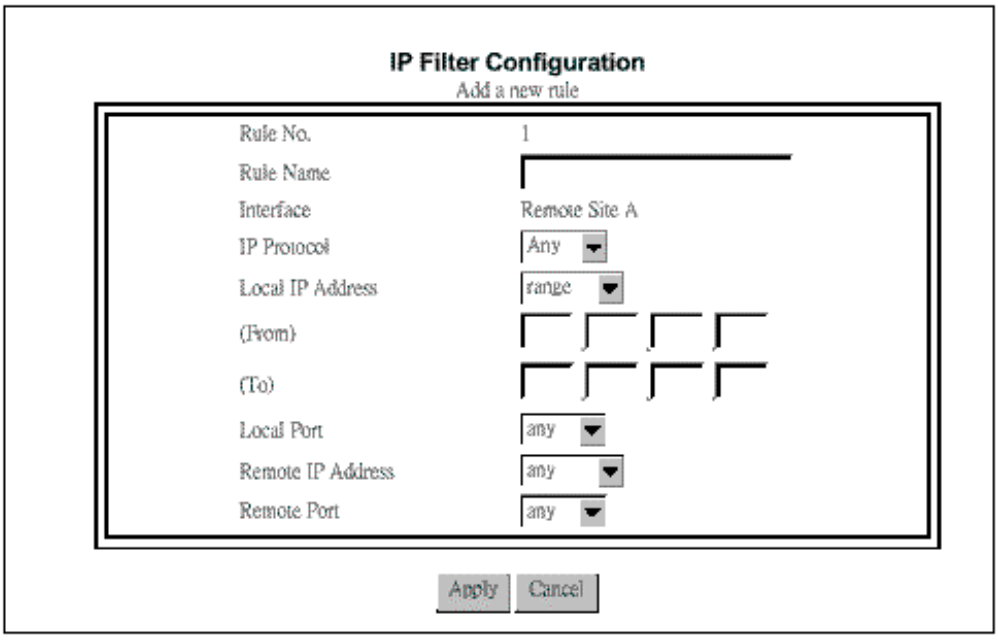
**Step 1:** From the **IP Filtering Configuration** screen, select the WAN profile of interest from the pull down menu. For example, if your only need is to access the Internet, you should only select the Internet access profile.




**Step 2:** Select **send** or **discarded** as desired, which is equivalent to allow and disallow, respectively.

**Step 3:** If you are just starting, click **Add** to add a new selection rule. If you have previously defined rules, you will see those rules shown as entries in the rule table, and you can edit the rule by first highlighting the desired entry in the rule table followed by clicking the **Edit** button.

**Step 4:** In case of adding a new selection rule, the following screen shows.



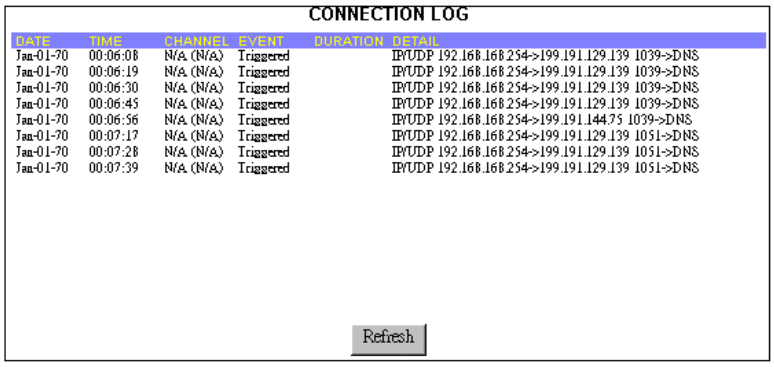

If you highlighted an existing entry in the **IP Filtering Configuration** window and clicked **Edit** instead, a similar screen will display, with all fields already filled out previously. Then you can make changes if necessary. If you highlighted an existing entry and clicked **Delete** instead, the corresponding entry in the rule table will be removed.

# Chapter 6
# Management

## 6.1 How to View the Connection Log

BIPAC-645 provides a connection log that you can use to track the telephone connections in and out of your BIPAC-645. Connect and disconnect messages can be useful in determining your telephone costs, and trigger messages are useful in determining which applications and tasks trigger a connection. These messages contain the IP address of the PC, which caused the connection to be established, as well as the port number or application name.

To view the Connection Log, select **Connection Log** from the **Monitoring** Menu. The Connection Log Window will appear.



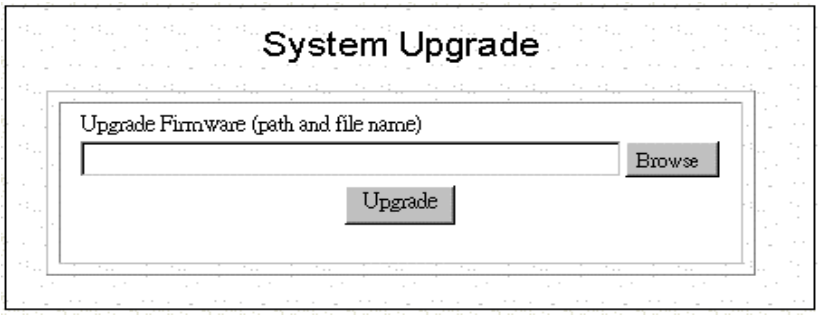

There are three types of messages that appear in the Connection Log:

**Connect** and **Disconnect** messages: Shows the date, time, and port (channel) when a connection is completed or disconnected.

**Trigger** messages: Shows the date, time, channel, duration, and details of an event that triggers a connection.

## 6.2 How to Upgrade the Firmware

**Step 1:** Select **System Upgrade** from the Menu Window. The following screen is displayed:

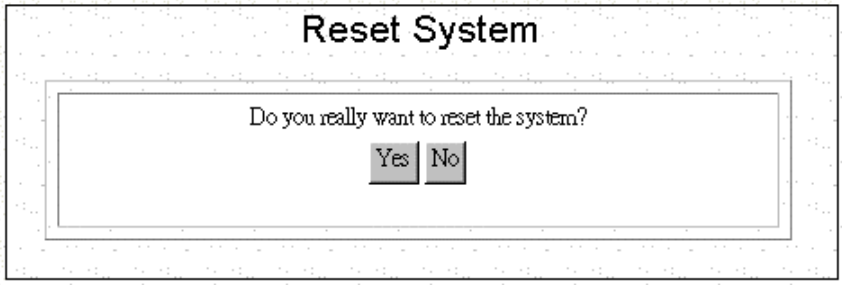


**Step 2:** To update BIPAC-645 firmware, download the firmware from Billion's web site and install the firmware in your local environment first, then from the above screen enter a path or filename, or click **Browse** to select a path to the firmware. Next, Click the **Upgrade** button below the file name and follow the onscreen instructions. The new firmware will begin loading across the network. After the operation is complete, be sure to reset the system to have the new firmware take effect.

# 6.3 How to Reset

You can reset the system from the System Tools Menu or by unplugging and plugging back in the power connector to the BIPAC-645. Follow the steps to reset the system:

**Step 1:** Select **Reset System** from the System Tools Menu. The following screen displays.

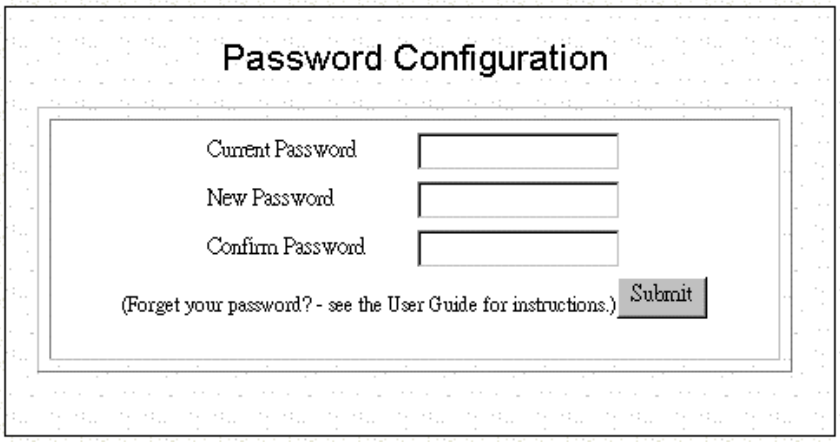



**Step 2:** Click **YES** to reset BIPAC-645.

# 6.4 How to Change the BIPAC-645 Manager Password

After you start using the BIPAC-645, you should change the factory default password. Follow the steps to change the password.

**Step 1:** Select **Change Password** from the System Tools Menu: The following screen displays:




**Step 2:** Enter the following information:

**Current Password:**

**New Password:**

**Confirm Password:**

**Step 3** Click **Submit**.

# 6.5 What if I Forget the Password?

If you forget the BIPAC-645 Manager password, the only way to recover is clear the entire configuration and return the unit to its original state as shipped from the factory. Unfortunately, this means that you have to re-enter all of your configuration data.

To clear the configuration and restore the password to the default, follow these steps:

**Step 1:** Using the supplied Null Modem Cable, connect a console (or a PC running a terminal emulation program such as HyperTerminal) to Router Console port. The default port settings are 19200, N, 8, 1, no flow control.

**Step 2:** Turn off the BIPAC-645, and then turn it on again. In the console window, you'll see the message "Loading firmware...".

**Step 3:** When you see the message "Ready", **immediately** (within one second) press Ctrl+C.

**Step 4:** When this is complete, BIPAC-645 will return all settings to the factory default. The password will once again be "password".

# Chapter 7
# Troubleshooting

- **What is NAT?**

**Answer.** NAT is Network Address Translation. It is proposed and described in RFC-1631 and is originally for solving the IP address depletion problem. Basically, "each NAT box has a table consisting of pairs of locally private IP addresses and globally unique public IP addresses," by which the box can "translate" the private IP addresses to public IP address and vice versa. BIPAC-645 supports the feature of NAT. With proper configuration, multiple users can access the Internet using a single account via the NAT device.

- **How many rules can be used in IP Filtering function?**

**Answer.** There are totally 8 filtering rules can be applied in the LAN and WAN ports.

- **How do I change the CLI mode form Advanced Prompt Mode into Express Prompt Mode? And vice versa?**

**Answer.** Press Ctrl +E key under CLI mode, it will show Advanced Prompt Mode, then press Ctrl +E key again, it will back to Express Prompt Mode.

- **Why should I need to assign static private IP Address to certain workstations or PCs?**

**Answer.** With built-in DHCP feature, each workstation or PC will be assigned by BIPAC-645 a different private IP address whenever power is on. For specific-purpose workstations, such as Mail server, FTP server, or Mail Server, we need to set up the static private IP address to prevent from losing connection.

- **How do I set up the Idle Time?**

**Answer.** The default setting for Idle Time is 120 seconds; meaning that BIPAC-645 will shut down ISDN connection automatically once it have no traffic on the connection over 120 seconds. To keep ISDN on without interruption, reset the Idle Time to 0.

- **Is there any effect if I add another DHCP server into the local network in which connected with an existing DHCP server?**

**Answer.** When it hooks up with power and network, it will detect whether there is any DHCP Server existed automatically. If it does, BIPAC-645 will shut down DHCP feature automatically, and will close this detective function as well.

Meanwhile, it will also detect the DHCP once Private IP changed.

- **Do I be able to pick up more than one configuration-selection at once while I set up Customize User Interface function?**

**Answer.** Yes, you do, but we would like to recommend that users should configure BIPAC-645 step by manual.

- **Why does the configuration lost from previous usage?**

**Answer.** Please keep in mind to save all configurations while you complete setting process.

Please choice Configuration Data Options\Save Button.

- **Why do I spend longer time to update firmware in GUI screen?**

**Answer.** Because the GUI of BIPAC-645 was written by JAVA program, we would like to suggest user to use Netscape Navigator, and please enable JAVA function under Internet Explorer environment. Please also keep in mind to close other application programs while updating firmware.

- **What's Data over Voice Channel?**

**Answer.** In Europe, there is some Tele-company have higher charging in data calls than voice calls. Using the Data over Voice Channel can save you more money.

- **Why can't I use ICQ software under the device?**

**Answer.** With built- in NAT (network address translation), it can't transfer ICQ packets via default TCP port to ICQ server. It means ICQ can't work well under such circumstances.

**Solution.** In order to solve this problem, we can use ISQ software with the function of automatically searching TCP port, or we can set up the TCP port to port 21(FTP port). For other games over the Internet, we must add a set of static network address translation to ensure TCP ports are used by the game.

- **If I have several legal IP addresses, how do I use it on WAN to LAN communication?**

**Answer.** The public IP address is used in PC connected with BIPAC-645 as a FTP/Mail/Web server, the others PC connected with BIPAC-645 will get the private IP address from the DHCP server of Router automatically.

**Solution.** First of all, to ensure it's under off-line condition, and complete the profile set up process, then add another Routing Table entry.

(1) Under GUI Mode:

Key in correct Public IP address for Gateway / Netmask

(2) Under CLI Mode:

Add a PAT Entry

Set IP LAN "Public Gateway Address" "Netmask",

For example, set IP LAN to 202.39.52.190 255.255.255.0

- **What can I do if PCs or workstations in the LAN can't be connected to Internet after setting public IP address?**

**Solution.** First, Please make sure that the public IP address you set is a legal public IP address, and then check that the public IP address has not occupied by other users. Second, make sure the IP address of each server is static and the IP Address/ Netmask/ Gateway information is completed.

And to make sure all PC is connects router with correct ISP.

- **Why can't I set up IP Filter function in GUI?**

**Answer.** Due to the consideration of security, you only can set up Profile in GUI Mode, and for the LAN; it only can be revised under the CLI Mode.

**Solution.** Connect the PC to BIPAC-645 with a null modem type cable and enter CLI mode to start IP Filtering by Telnet or Hyper-terminal.

- **What should I do if the Firmware upgraded fail in the device, and it affects me have trouble to get into CLI & GUI screen?**

**Answer.** It will go through the process of Vector->Boot Code->App Code once its power on, the CLI can be used to update Firmware as long as the Boot Code doesn't expired.

**Solution.**

1. Open Hyper terminal

2. Make sure baud rate is 19200,n, 8,1,none

3. Connect the cable with both Com Port and Console Port

4. Turn on BIPAC-645

5. Choice the connection speed, then you can update the Firmware by delivery the chosen Firmware file.

- **How can I get into Router what if I forgot the password?**

**Answer.** If you forget the password, you can clean the password first, but all configuration will be disappeared once the password cleaned.

**Solution.**

1. To get into Hyper Terminal first.

2. Make sure baud rate is 19200,n, 8,1,none

3. Turn off BIPAC-645, and connect the Console Port Cable.

4. Turn on BIPAC-645.

5. Press Ctrl +C while the message “Loading Firmware” shows up.

6. Then it will show “Clearing System Configuration” once the system is ready.

7. Therefore, it will recover the default password while the router reboot automatically.

- **Why does BIPAC-645 connect with ISP sometimes automatically?**

**Answer.** BIPAC-645 will build up connected function once LAN’s PC has any packet need to send. This function calls Dial on Demand.

- **Why didn’t BIPAC-645 offline automatically even my Idle Time exceeded?**

**Answer.** There are several reasons for in-completed offline:

1. The setting Idle time is greater than the confirmed connection packet from ISP.

2. If there is any packet flow into the LAN, Idle Time will always recalculated.

3. LAN’s PC is running Program for the Network, And Program send the packet to the Internet.

You could use the window in Show Profile Status to monitor the packet quantity in Network.

- **Why can’t I connect successfully while I use Remote Dial-in?**

**Answer.** Please be sure both Remote User’s Username and password are correct, and keep the setting information identically at two sides of Router. The best way is setting the BIPAC-645 in MultiPPP.

# Appendix A
# Console Commands

## General Guidelines

When the router is powered up, the user can connect a terminal (or the PC running terminal emulation software) to the auxiliary (console) port to perform configuration and management functions. Alternatively, the Command Line Interface may be accessed via a standard telnet application. When properly connected, setting the console speed to a baud rate of 19200 bits per second, eight data bits, no parity, one stop bit, and pressing a carriage return key, the user will see a system sign-on message followed by a password prompt as follows.

*Local Router Manager Console Version*[1]*:* **rev_no**

*Please enter your password: *********

A default password "*password*" has been pre-configured with the system. The user should use it to log into the system until the password is explicitly changed using the ***change password*** command. Note that the entered password is case-sensitive. This password may also be changed using the browser-based GUI configuration utility.

The password entered will be echoed as asterisks (*). After the Carriage Return is entered, if the password string is validated, the command prompt ***Router>*** will be displayed, and the user can then issue other commands. Otherwise, the password prompt will be redisplayed.

Many commands are single-line commands, and commands are not context sensitive: each command is independent of other commands before or after it. Exceptions to the single line mode are indicated in this manual by the prefix "⊕". These commands invoke an interactive user dialog.

The command syntax is straightforward.

The following briefly summarizes the guideline for the interface.

- At any time, the user can type a " **?**" (preceded by a space) to request context-sensitive help on what the user can enter next.
- At any time, the user can type control-p (^p, by pressing both the Ctrl key and the p key at the same time) to repeat the previous command, or control n to return to the following (next) command. At startup, typing ^p or ^n will not cause anything to happen - since previous commands do not yet exist. In normal operation typing ^p will cause the previous command to show, and the cursor will sit at the end of the command. At this point, the user can either type a carriage return to accept the command, or type backspaces to edit the command from the end, or ^p to get to its previous command, or ^n to get to its following command (if applicable). Up to 15 previously entered commands can be invoked through ^p's and ^n's.

- If a keyword is expected when the user types " ?", all valid keywords will be displayed, then the command typed so far will be re-displayed, with the cursor sitting at the end (waiting for the user to continue).
- If the user had previously typed part of the keyword but did not finish it, and if the characters typed so far uniquely identify the keyword, if the user types a tab (or a space) character, and the system will complete the keyword automatically. If the characters typed so far do not uniquely identify a keyword, nothing will happen.

If the user is not sure what to type next, he can type " ?", which will cause those keywords that match the characters typed so far to be displayed.

If an interactive mode is entered, the system will prompt for each parameter required, such as:

**…**

***enter Link management protocol (none, none/Annex-D):***

***enter polling interval in seconds (10, 5 - 30):***

**…**

The first prompt means there are two choices (**none** and **Annex-D**), with **none** being the default. The second prompt means a number between 5 and 30 is expected, with 10 being the default.

If it is the first time a particular parameter is configured, typing a carriage return will cause the default value to be selected. Otherwise, typing a carriage return means no change to the existing value.

Some interactive commands will query the user for the type of parameter to be entered. For example,

**…**

***enter Day-of-the-week (all, (a)ll/(d)ay-range): d***

***enter dd1-dd2 (Unspecified): mon-sat***

**…**

# "Express Mode" vs. "Advanced Mode"

The Command Line Interface operates in one of two modes: *Express Mode* or *Advanced Mode*. In Express Mode, not all parameters may be displayed. Default values are set for parameters not displayed in multi-line commands. In Advanced Mode, users have the option to modify all possible values appropriate to each operation.

The user can toggle between Express Mode and Advanced Mode by typing ^E (Control-E) at any time. Normally, the system prompt will be changed by appending ">>" to the configured prompt when in Advanced Mode.

# Conventions

Note that the meaning of "port n" may differ depending upon the model being managed. Examples using the terminology are model-specific.

The following notations will be used:

1. lan means the LAN port;
2. <> specifies the arguments of the command, <1-4> means a number between 1 to 4;
3. [ ] indicates a required or optional parameter, or choice of parameters;

- Interface Name or ifName represents a profile interface, which can be the LAN port (lan), a PPP profile, a PPPoE profile, an ISDN connection profile, or a modem profile.

4. Profile Name means a WAN profile, such as a PPP profile, LAN-to-LAN profile, Internet profile, or Single User Dial-in profile, not the LAN port.
5. xxx/yyy means xxx, or yyy;
6. num means any integer number (such as 19200, 9600, ...);
7. MacAddr, or nn-nn-nn-nn-nn-nn means any MAC address in hexadecimal format, where each nn can be 00, 01, ... 09, 0A, 0B, 0C, 0D, 0E, 0F, 10, 11,… FF;
8. ipAddr, netMask, or xxx.xxx.xxx.xxx means any ip address or network mask, where xxx is a decimal integer between 0 and 255
9. the term *string* means a string of characters up to the specified length, which may be enclosed in double quotes (“) (required if the string contains embedded blanks

# Command Categories

From a functional point of view, commands can be grouped into the following functional categories:

| | | |
|---|---|---|
| *(1) Bridging* | *(2) Compression* | *(3) Diagnostics* |
| *(4) Filtering* | *(5) IP* | *(6) Port* |
| *(7) Profile* | *(8) Security* | *(9) SNMP* |
| *(10) Statistics* | *(11) System* | |

This list may vary depending upon the router model and the installed features.

For convenience, the section *Command List* summarizes all commands using the following categories:

- Bridging
- Compression
- Diagnostics
- DHCP
- Dial-In Users
- IP
- Port Commands
- Profile Commands
- Security Command
- SNMP
- Statistics
- System

This summary is followed by examples in subsequent sections. Examples will be given in the following format:

***Command Syntax***

**Description**: the description of the command is given here.

**Example:**

*Router>* ***command (with parameters)***

*Output …*

# Command List

Note that commands may apply either to a specific router model or with a particular Feature Key enabled. Each command below which is affected, is identified by a symbol which is associated with either a router model or a Feature Key as follows:

In addition, those commands which involve an interactive user dialog are prefixed with the symbol, "⊕".

## Bridging Commands

Disable bridging <Interface Name>

Disable learning

Enable bridging <Interface Name>

Enable learning

Show bridging

Show learning

Show learning <Interface Name>

## Compression Commands

clear compression statistics <Profile Name>

disable compression <Profile Name>

enable compression <Profile Name>

show compression statistics <Profile Name>

## DHCP Commands

⊕add dhcp entry <entry name>

add dns <primary/secondary> <IP_addr>

delete dhcp entry <entry name>

delete dns <primary/secondary>

disable dhcp

enable dhcp

⊕set dhcp

⊕set range

show dhcp

show dhcp table

show range

## Diagnostic Commands

connect profile <Profile Name>

disable trace

disconnect profile <Profile Name>

enable trace

ping <ip_addr> [integer greater than 0][packet length, greater than or equal to 56]

set log level <1-10>

test isdn <dial name> <64k/56k>

## Dial-in User Commands

⊕add user <profile name>

delete user <profile name>

show user [profile name]

## Filtering Commands

⊕add filter <1-8>

delete filter <1-8>

⊕set filter default

show filter

show filter <1-8>

## IP Commands

add ip route <ip_addr> <Network Mask> <ip_addr> <hop count, 1-15>

add ip route <ip_addr> <Network Mask> <Profile Name> <hop count, 1-15>

⊕add pat entry <public port #>

⊕add pat entry default

delete ip default route

delete ip route <ip_addr> <network mask>

delete ip <Interface Name>

delete pat entry <public port #>

delete pat entry default

disable spoofing <Interface Name> <iprip>

enable spoofing <Interface Name> <iprip>

ping <ip_addr> [integer >=1] [packet length, >=56]

set ip default route <ip_addr>

set ip default route <Profile Name>

set ip lan <ip_addr> <network mask>

set ip private <ip_addr> <network mask>

set ip rip <disabled / passive / active> <rip1/rip2>

set ip rip [Interface Name] <disabled / passive / active> <RIP1/RIP2>

set ip <Profile Name>

set ip <Profile Name> <ip_addr> <network mask> <ip_addr>

show arp table

show icmp statistics

show ip

show ip <interface name>

show ip routing table

show ip statistics

show pat

show tcp statistics

show udp statistics

## Port Commands

clear port statistics [port name]

disable port <port name>

enable port <port name>

⊕set port <port name>

show port

show port <port name>

show port statistics <port name>

## Profile Commands

⊕add profile <Profile Name>

clear profile statistics [Profile Name]

connect profile <Profile Name>

delete profile <Profile Name>

disable profile <Profile Name>

disconnect profile <Profile Name>

enable profile <Profile Name>

show profile

show profile <Profile Name>

show profile statistics

show profile statistics <Profile Name>

## Security Command

set ip private <ip_Addr><netMask>

## SNMP Commands

clear trap manager <1-5>

disable trap

enable trap

set community string read <string up to 30 characters, inclusive>

set trap manager <1-5> <ip_addr>

show snmp statistics

show trap manager [1-5]

## Statistics Commands

clear compression statistics [Interface Name]

clear port statistics [port name]

clear profile statistics [Profile Name]

show compression statistics <Profile Name>

show icmp statistics

show ip statistics

show port statistics <port name>

show profile statistics [Profile Name]

show snmp statistics

show tcp statistics

show udp statistics

show <Interface Name> statistics

## System Commands

change password

clear config

disable remote-mgt

enable remote-mgt

disconnect telnet session <1-5>

download config <file_name> from <ip_addr>

download firmware

help

logout

reset system

save config

set console baud <baudrate>

set console timeout <timeout value, 1- 60>

set date <mm-dd-yy>

set daylight time <on/off>

⊕set internet access time

set log level <1-10>

set prompt <string up to 15 characters, inclusive>

set system contact <string up to 60 characters, inclusive>

set system location <string up to 60 characters, inclusive>

set system name <string up to 30 characters, inclusive>

set time <hh:mm:ss>

set timezone <-12:00 - +12:00>

show config

show connection log

show interface list

show internet access time

show system

show system log

show telnet session

show time

upload config <string up to 60 characters, inclusive> to <ip_addr>

# Command Detail

# Bridging Commands

Although routing is preferred over bridging for transmitting data across wide area connections, occasionally bridging is required. For example, when the data packets to be transmitted are neither IP nor IPX (such as NetBEUI, SNA or AppleTalk), or when the other end of the WAN connection only supports bridging.

Bridging uses an intelligent learning algorithm to build up a MAC-address-to-interface mapping, which it then uses to make forwarding or filtering decisions for each packet it receives, whether the packet is from the LAN side or from one of the WAN connections.

## disable bridging <Interface Name>

**Description:** This command disables bridging over the specified interface. If the interface already has IP/IPX routing enabled, then routing will take precedence. For example, if both bridging and IP routing are enabled over interface profile1, IP data will be routed, and all non-IP data will be bridged.

**Example:**

*Router> disable bridging profile1*

## disable learning

**Description:** This command enables or disables address learning for all bridging ports. The default mode is **enabled**.

When learning is enabled, MAC addresses will be learned and maintained in the address table. However, an entry will be “aged out” (removed) if the same address is not re-learned within a fixed time period, When learning is disabled, all addresses learned so far will no longer be aged out.

## enable bridging <Interface Name>

**Description:** This command enables bridging over the specified interface.

## enable learning

**Description:** This command enables or disables address learning for all bridging ports.

## show bridging

**Description:** This command displays the bridging configuration over all interfaces.

**Example:**

| *IfName* | *IP* | *Other* |
|---|---|---|
| *ppp2* | *disabled* | *enabled* |
| *isp1* | *enabled* | *disabled* |
| *lan* | *enabled* | *enabled* |

## show learning

**Description:** This command displays MAC addresses learned from all bridging-enabled interfaces.

**Example:**

*Router> show learning*

*lan: MAC Address*

*---*

*12-22-33-3D-D5-00*

*00-60-54-16-67-01*

*00-96-33-58-BD-DE*

*Total MAC addresses: 3*

*newyork: MAC Address*

*---*

*00-40-33-3D-D5-DB*

*00-60-20-16-00-01*

*00-40-33-58-07-DE*

*Total MAC addresses: 3*

## show learning <Interface Name>

**Description:** This command displays MAC addresses learned from a specified interface.

**Example:**

*Router> show learning lan*

*MAC Address*

*---*

*00-40-33-3D-D5-DB*

*00-60-20-16-00-01*

*00-40-33-58-07-DE*

*Total MAC addresses: 3*

# Compression Commands

Compression can be enabled over serial interfaces running the PPP protocol in order to allow more efficient use of the WAN bandwidth. Currently, STAC based compression is supported. In units containing hardware-assisted compression, these commands will automatically utilize this resource.

Note that these commands cannot manage the operation of modem-based compression (MNP5/V.42). Modem initialization strings manage this type of compression.

## clear compression statistics <Profile Name>

**Description:** The statistics counters associated with compression over the specified interface are reset.

### disable compression <Profile Name>

**Description:** This command disables compression over the specified interface.

### enable compression <Profile Name>

**Description:** This command enables compression over the specified interface.

### show compression statistics <Profile Name>

**Description:** This command displays compression related statistics for the specified interface.

## DHCP Commands

The Dynamic Host Control Protocol (DHCP) is a client/server protocol[2] that defines an efficient and convenient means of dynamically assigning IP addresses and other networking parameters for a period of time upon request. In a router environment, this means either the dynamic assignment of "private" IP addresses to PCs co-residing on the LAN segment with the router or a static assignment of these addresses according to the station identification (the MAC address) of the requesting client.

Since the routers are, by default, configured with a private IP address for its LAN connection, the DHCP server is automatically enabled. (The DHCP function is disabled if the router discovers another DHCP server at initialization time, or if the user has explicitly disabled this function.) DHCP clients residing in LAN-resident machines, such as those running Windows 95/98, may then request a lease on an IP address from a DHCP server. As the term implies, the assignment of the address is temporary. The default lease period in a router's DHCP server is ten hours. The DHCP client is responsible for the renewal of the lease.

Both static and dynamic DHCP assignments are supported. The range of IP addresses in the dynamic pool from which the server selects an address to satisfy a request depends upon the currently configured private address and network mask of the router. The router's defaultIP private address is 192.168.168.230 with a network mask of 255.255.255.0. This private address may be changed to any private address and network mask as specified in the following table:

| Class | Network Address | Network Prefix | Default Network Mask | Maximum Number of Host Addresses | Lowest/Highest Address |
|---|---|---|---|---|---|
| A | 10.0.0.0 | 8 bits | 255.0.0.0 | 16,777,214 | 10.0.0.1/10.255.255.254 |
| B | 172.xx.0.0<br>31 ≥ xx ≥ 16 | 12 bits | 255.255.0.0 | 65534 | 172.xx.0.1/172.xx.255.254<br>31 ≥ xx ≥ 16 |
| C | 192.168.xx.0<br>255 ≥ xx ≥ 0 | 16 bits | 255.255.255.0 | 254 | 192.168.xx.1/192.168.xx.254<br>255 ≥ xx ≥ 0 |

[2]The Internet Engineering Task Force (IETF) defines DHCP in RFC-2131 and RFC-2132.

Once configured, the DHCP server will assign private addresses from within the defined private address range with the highest available address being assigned first. This address range may be modified using the "set range" command. Statically assigned addresses must be within this range as well. Up to 20 static DHCP assignments may be configured and saved.

If the Default Network Mask is modified, the DHCP address range is likewise modified, with the highest configurable address being assigned first, by default (also modifiable via the "set range" command).

## ⊕add dhcp entry <entry name>

**Description**: This command adds or edits a static DHCP assignment entry. An entry added to the Static DHCP Assignment Table causes a DHCP client to be assigned the same IP address whenever a DHCP client request is received from a machine with the specified MAC address.

**Example**:

*Router> add dhcp entry daniel*

*enter IP address (Unspecified): 192.168.168.134*

*enter MAC address (Unspecified): 00-40-05-35-db-4f*

***Note that the format of the MAC address uses embedded dashes***

## add dns <primary/secondary> <IP_addr>

**Description:** This command allows the specific assignment of Domain Name Server (DNS) IP addresses that will be subsequently assigned to requesting DHCP clients. Note that these addresses also can be automatically obtained via protocol negotiation when connecting to a remote IP network, e.g., a connection to an ISP. Both a **primary** DNS server address and a **secondary** DNS server address may be assigned using separate commands.

## delete dhcp entry <entry name>

**Description**: This command deletes the specified entry from the Static DHCP Assignment Table.

## delete dns <primary/secondary>

**Description:** The specified Domain Name Server IP address will no longer be assigned by the DHCP server to requesting clients. Note that a subsequent connection to an ISP may once again cause these values to be assigned to requesting clients.

## disable dhcp

**Description:** This command disables the Dynamic Host Control Protocol server functions within the router. The router will no longer respond to lease requests. Existing leaseholders will not be able to renew their leases after the lease term expires, unless another DHCP server resides within the network.

## enable dhcp

**Description:** This command enables the Dynamic Host Control Protocol server functionality within the router. When enabled, the router will service a client request for IP address and net mask assignment, as well as assignments of default gateway, DNS server addresses, WINS server addresses and NetBIOS Node Type. The pool of addresses from which the router selects is defined in the table above.. The default

is 192.168.168.230, unless re-configured with the “set ip private…” command (or its HTTP equivalent). The term of the lease is 10 hours. The factory default is enabled.

## ⊕set dhcp

**Description**: This command configures the global parameters to be supplied to all requesting DHCP clients. Note that the DHCP service can also be enabled or disabled from this command.

**Example**:

*Router> set dhcp*
*enable DHCP (Yes, Yes/No): yes*
*configure WINS server (No, Yes/No): yes*
*enter primary WINS server address (Unspecified): 63.221.98.5*
*enter secondary WINS server address (Unspecified): 63.221.98.7*
*enter NetBIOS node type (none, none/b/p/m/h): h*
*Router>*

## ⊕set range

**Description**: This command sets the bounds for dynamic assignment of IP addresses to both DHCP clients and dial in users. A dialog ensues wherein the user is asked first to enter the upper bound address, and then the lower bound address. The default upper bound is the highest address in the configured private IP subnet. For example, if the configured private IP subnet is 192.168.168.0/255.255.255.0, then the default upper bound for dynamic assignment is 192.168.168.254. The default lower bound is the high address less 253, which, in our example, is 192.168.168.1. Any address lower than the lower bound is not assigned automatically by the router to requesting DHCP clients or dial-in users and may be used for manual configuration of a LAN device (unless used by another router elsewhere on the LAN).

The administrator may alter these addresses to any address that is valid within the configured private IP subnet. The upper bound address must be greater than the lower bound address.

Note that dial in users will be assigned addresses in pairs.

The router will check before assignment of any dynamic address to ensure that it is not in use elsewhere in the network.

If the router’s private IP network is modified, the range values that are in conflict with the new IP network settings will revert to the above mentioned defaults until manually altered by the administrator.

**Example**:

*Router> set range*
*enter upper bound address (192.168.168.254):*
*enter lower bound address (192.168.168.1):*

## show dhcp

**Description:** This command displays the current status of the Dynamic Host Control Protocol server.

**Example**:

```
Router> show dhcp
  Admin Status:      Enable                  Default Lease:10 hours
  Network address: 192.168.168.0     Netmask:              255.255.255.0
  Default gateway: 192.168.168.230
  Primary DNS:    199.191.129.139   Secondary DNS:      199.191.144.75
  Primary WINS:          63.221.98.5        Secondary WINS:63.221.98.7
  Node Type              h-node

  IP-Address          Mac-Addr            Lease-Expires        Entry Type
  ------------------------------------------------------------------------
  192.168.168.134     00400535db4f06-15-99 14:24:5     Static
  192.168.168.254     222222222222        06-15-99 16:43:7     Dynamic
```

### show dhcp table

**Description**: This command displays the entries currently configured in the Static DHCP Assignment Table

**Example**:

```
Router> show dhcp table
    Static DHCP Assignments
    Name              IP-Address                Mac-Address
  ------------------------------------------------------------------------
    daniel            192.168.168.134           00-40-05-35-DB-4F
```

### show range

**Description:** This command displays the upper and lower bound addresses currently being used for the dynamic assignment of private IP addresses to DHCP clients and dial in users. (See "***set range***", above)

**Example**:

```
Router> show range
 IP address assignment range: 192.168.168.1 – 192.168.168.254
```

## Diagnostic Commands

### connect profile <Profile Name>

**Description:** For switched profiles, this command activates the profile as if a trigger occurred. This command has no effect on leased line profiles.

### disable trace

**Description:** This command disables the debug trace messages.

### disconnect profile <Profile Name>

**Description:** For active switched profiles, this command terminates the connection as if an idle timeout occurred. This command has no effect on leased line profiles.

### enable trace

**Description:** This command enables the debug trace messages. When enabled, all log messages entered into the system log will appear in the console session from which this command is issued.

### ping ipAddr [<n_times> < n_size>]

**Description:** This command allows the user to ping an IP device (send a diagnostic message to be echoed by the receiving device). If *n_times* and *n_size* are optionally specified, the ping will be performed *n_times* times, and each time with size equal to *n_size*. Otherwise, ping will only be executed once with the packet size equal to 56 bytes. The maximum value of *n_times* is 100: any value larger than this will be set to 100. The maximum value of *n_size* is 1932: any value larger than this will be set to 1932.

**Example:**

*Router> ping 10.0.0.2 100 1000*

*repeating times = 100, data length = 1000*

*Ping packets -- total: 100 sent: 100 received: 100*

*Router> ping 10.0.0.2*

*repeating times = 1, data length = 56*

*Ping packets -- total: 1 sent: 1 received: 1*

### set log level <1-10>

**Description:** For a description of this command, see "set log level <1-10>" under System Commands.

### test isdn <dial name> <64k/56k>

**Description:** This command causes a modem call to the specified telephone number. The call is cleared immediately after a connection is established. This command is only valid when the ISDN port has been configured and enabled. Please refer to "Set Port" and "Enable Port" commands for details.

## Dial-in User Commands

Dial-in user profiles are used by stand-alone remote workstations connecting via a switched connection through an ISDN line. A user workstation effectively becomes a LAN node for the duration of its connection. Its ARP information is proxied by the router.

When a switched call is answered, the local profile database is searched for a match with the received name. If an appropriate profile is not found, the call is rejected. If a profile is found, the information in the entry is used to authenticate and configure the connection.

### ⊕add user <profile name> *(where "profile name" is a string <= 30 chars)*

**Description:** This command configures an entry in the local profile database. The users added with this command might be single workstations dialing in through the ISDN line. The following examples illustrate the dialog that ensues and the items of information that the router needs for these profiles:

**Example 1**:

Add the following Single Workstation dialing into a router using the CLI Express Mode (you can toggle between Express Mode and Advanced Mode by using the Ctrl-E key combination)

*Router> add user u1*
*Add new user profile "u1" ...*
*user name (Unspecified): user1*
*user password (Unspecified): ***
*password confirm (***): ***

The Express method of configuring a dial-in user will use the following defaults:

10. PPP Authentication: Either CHAP or PAP
11. Multilink: No
12. Callback: No
13. Caller ID Authentication: No
14. IP Enabled
15. IP RIP Disabled
16. No Compression
17. Default Idle Timeout (model-dependent)

**Example 2**:

Add the following Single Workstation dialing into the router using the CLI Advanced Mode

*Router>>> add user u2*
*Add new user profile "u2" ...*
*user name (Unspecified): user2*
*user password (Unspecified): ***
*password confirm (***): ***
*enable call back (No, yes/no): y*
*call back number (Unspecified): 5554444*
*enable caller ID authenticatication (N0, yes/no): yes*
*caller ID (Unspecified): 5556666*
*multilink option (No, no/loadsharing/overflow): over*
*second caller ID (Unspecified): 5557777*
*second call back number (Unspecified): 5557777*
*compression (No, no/stac):*
*idle timeout (120, 0[none]-3600):*
*enable IP (Yes, yes/no):*
*use dynamic IP address assignment? (Yes, yes/no): yes*
*bridging (No, yes/no):*

## delete user <profile name>

**Description:** Deletes a dial-in user entry from the local user database.

### show user [profile name]

**Description:** Displays the current local profile database.

**Example 1:** Without the user name parameter the output appears as follows.

```
Router> show user

  profile name:   u2
  user name:      user2       dial in from:   Workstation
  enable IP:      Yes         IP RIP:         Disable

  profile name:   u1
  user name:      user1       dial in from:   Workstation
  enable IP:      Yes         IP RIP:         Disable
```

**Example 2:** When a specific user is named, the output appears as follows:

```
Router> show user u1
  Profile name:   u1
  User Name:      user1       Dial In From:     Workstation
  Port Type:      ISDN        Multilink:        No
  Caller ID:      None        Callback #:       None
  Auth Method:    Either      Compression:      No
  Encryption:     No          Idle Timeout:     300
  Enable IP:      Yes         IP RIP:           Disable
  IP Address:     Dynamic
  Bridging:       No
```

## Filtering Commands

### ⊕add filter <1-8>

**Description:** This command adds or modifies the nth IP filter rule in the system

Packet Filtering allows each IP packet exiting a router interface to be examined for a match with a configured set of rules. If all of the conditions in any rule do not match the contents of the packet, then the packet is either forwarded or discarded, depending upon the filter default for that interface. Otherwise, the exception action is taken, i.e., the packet is discarded or forwarded, the opposite of the default action. The default action for an interface is set by the set *filter default* command described below.

The total number of rules system-wide in this version of the firmware is limited to eight. Each of these rules may be assigned to one specific interface.

The conditions that may be specified are:

| Conditions | Values |
|---|---|
| IP Protocol | 1. Any Protocol<br>2. TCP<br>3. UDP<br>4. ICMP<br>5. IGMP |

| | |
|---|---|
| Source IP Address | 1. Any value (wildcard)<br>2. Individual IP Address (xxx.xxx.xxx.xxx)<br>3. Range of consecutive IP Addresses (xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy)<br>4. A Network of IP Addresses (and its associated subnet mask). (xxx.xxx.xxx.xxx/mmm.mmm.mmm.mmm) |
| Destination IP Address | 1. Any value (wildcard)<br>2. Individual IP Address (xxx.xxx.xxx.xxx)<br>3. Range of consecutive IP Addresses (xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy)<br>4. A Network of IP Addresses (and its associated subnet mask). (xxx.xxx.xxx.xxx/mmm.mmm.mmm.mmm) |
| Source TCP/UDP Port | 1. Any value (wildcard)<br>2. A TCP or UDP Port Number<br>3. A consecutive range of TCP/UDP Port Numbers |
| Destination TCP/UDP Port | 1. Any value (wildcard)<br>2. A TCP or UDP Port Number<br>3. A consecutive range of TCP/UDP Port Numbers |

Filter is specified by a number.

**Note: Incorrect or mistyped filtering entries may cause undesired or unpredictable behavior. It is strongly recommended that this feature be used with the utmost care and planning. For a more detailed description of Filtering, please refer to the User Guide for your particular model.**

**Example**:

*Router> add filter 1*

*enter filter name (Unspecified):*

*enter interface (Unspecified):*

*enter IP protocol (any, (a)ny/TCP/UDP/ICMP/IGMP):*

*enter Source IP Address (any, (a)ny/(s)ingle/(r)ange/(n)etwork):*

/* if "s" or "single" specified */

*enter single ip_addr (Unspecified):*

/* endif "single" */

/*if "r" or "range" specified */

*enter ip_addr1-ip_addr2 (Unspecified):*

/* endif "range" */

/* if "n" or "network" specified */

*enter ip_net_addr/netmask (Unspecified):*

/* endif "network" */

*enter Destination IP Address (any, a)ny/(s)ingle/(r)ange/(n)etwork):*

*enter Source TCP/UDP Port(any, (a)ny/(s)ingle/(r)ange):*

*enter Destination TCP/UDP Port(any, (a)ny/(s)ingle/(r)ange):*

## delete filter <1-8>

**Description:** This command deletes the specified rule.

**Example**:

*Router> delete filter 1*

## ⊕set filter default

**Description:** This command sets the default action to be taken when an IP packet does not match any rule on the specified interface. See the description for the *add filter* command above.

**Example**:

```
Router> set filter default
 enter interface (Unspecified): isp
 enter default action (forward, forward/discard) : forward
```

## show filter

**Description:** This command displays the entire configured rule set.

**Example:**

```
Router> show filter
 Interface Name : abc
  Default action is forward, and current exception rules are :
    Filter 1:
    Filter Name:      Rule1
    Interface Name:   ppp2                IP Protocol:   any
    Src. IP:          212.54.104.1        Src. Port:     136
    Dest. IP:         any                 Dest. Port:    any
```

## show filter <1-8 >

**Description:** This command displays the definition of the nth rule.

**Example:**

```
Router> show filter 1
      Filter 1:
      Filter Name:        Rule1
      Interface Name:   ppp2                IP Protocol:   any
      Src. IP:          212.54.104.1        Src. Port:     136
      Dest. IP:         any                 Dest. Port:    any
```

# IP Commands

## add ip route <dest-ipAddr><netMask><gateway-ipAddr ><hop count, 1-15>

## add ip route <dest-ipAddr><netMask><Profile Name>< hop count, 1-15>

**Description:** This command adds a static route to the IP routing table. The first example means that to send a packet to the destination IP address ***204.71.220.153***, the packet should be forwarded to ***204.23.0.1*** first, and the target is ***4*** hops away. The second example means that to send a packet to the destination IP address ***204.71.220.153***, the packet should be sent out over the frame relay profile *isp2* first, and the target is ***4*** hops away.

**Example:**

```
Router> add ip route 204.71.220.153 255.255.255.0 204.23.0.1    4
Router> add ip route 204.71.220.153 255.255.255.0 isp2 4
```

## ⊕add pat entry <public port #>

## ⊕add pat entry default

**Description:** Each IP packet received from the Internet interface is examined. If the destination address is the public address of the interface, the Network Address Translation Table is searched for a match. If the address is found, the destination address is replaced with the associated private address and port number. The packet is then forwarded to the IP routing process. If no match is found and a Default Private Receiver is defined, the packet is forwarded to this machine. If no match is found and a Default Private Receiver is not defined, the packet is discarded.

Static entries may be created in this table by these commands.

Note that static entries are mapped according to port number and therefore multiple protocols using the same port number will be routed to the mapped entry.

**Example 1:**

IP packets received with the public IP address of the router and a destination port number of 123 will be translated to port 234 with a destination private IP address of 10.0.1.120. Here, it is assumed that the private IP network is 10.0.1.0 with a subnet mask of 255.255.255.0.

*Router> add pat entry 123*

*Enter Private IP Address (unspecified): 10.0.1.120*

*Enter Private Port Number (unspecified): 234*

**Example 2:**

IP packets received with a destination port number not found in the Address Translation Table will be translated to a destination private IP address of 192.168.168.121. Here, it is assumed that the private IP network is 192.168.168.0 with a subnet mask of 255.255.255.0.

*Router> add pat entry default*

*Enter Private IP Address (unspecified): 192.168.168.121*

## delete ip default route

**Description:** This command deletes the default route from the IP routing table. Packets normally sent to the default router will then be discarded.

## delete ip route <ipAddr> <net_mask>

**Description:** This command deletes the static route for ***204.71.220.153*** from the IP routing table.

**Example:**

*Router> delete ip route 204.71.220.153 255.255.255.0*

## delete ip <Interface Name>

**Description:** This command deletes the IP protocol configuration from the specified interface. The corresponding IP routing table entry for this IP address is also deleted.

## delete pat entry <public port #>

**Description:** This command deletes the specified port mapping from the Network Address Translation Table.

## delete pat entry default

**Description:** This command deletes the default port mapping from the Network Address Translation Table.

## disable spoofing <Interface Name> <iprip>

## enable spoofing <Interface Name> <iprip>

**Description:** These commands enable/disable spoofing over switched connection profiles.

Since dial-up connection (e.g. ISDN calls) charges are based on the connection time, a technique called IP spoofing is often used to limit or prevent unnecessary connection time. This is done by (1) allowing control packets to be sent only when the connection is already up transmitting user data, or (2) allowing control packets to be spoofed (faked) so that they don't add load to the WAN traffic. IP RIP broadcasts are sent only when the connection is up.

**Example:**

*Router> enable spoofing isdn1 iprip*

*Router> disable spoofing isp2 iprip*

## ping <ipAddr> [n_times] [n_size]

**Description:** See description under Diagnostics.

## set ip default route <gateway-ipAddr>

## set ip default route <Profile Name>

**Description:** This command is used to set the IP default route. The default route will be used when an IP packet's destination IP address cannot be found in the IP routing table. If the default route is not defined, such a packet is discarded.

**Example:**

*Router> set ip default route 204.71.220.153*

*Router> set ip default route isp1*

## set ip lan <ip_addr> <netMask>

**Description:** This command assigns a "public" IP address to the LAN port of the router. As a consequence, the LAN port maps to two IP addresses (one public and one private), and is therefore on two networks.

**Example:**

*Router> set ip lan 204.71.220.153 255.255.255.0*

## set ip private <ip_addr> <netMask>

**Description:** This command is used to modify the "private" IP address on the router's LAN interface.

The IP network corresponding to the "set ip private" command becomes the private network. Private addresses are not legal for use on the Internet and therefore, devices in this network are no longer accessible from public devices on the Internet side. All devices within this "private" network are represented by one single IP address: the IP address received from an Internet Service Provider at connect time. Note that ***192.168.168.230*** is the default private address used for routers, and the private network address is ***192.168.168.0***, and therefore all private devices (by default) should have IP addresses within the range of ***192.168.168.1*** to ***192.168.168.254***. Private IP addresses may be any Class A, B or C address as described in the "DHCP" section of this manual.

Note that the router may also communicate with devices in a "public" IP network, as defined in the command "set ip lan <ip_addr> <netMask>~~set ip lan <ip_addr> <netMask>~~".

When you modify the private IP network, related routes in the IP Routing Table and all entries in the Static DHCP table and the Network Address Translation table which conflict with the new address space will be deleted. You will receive a warning message asking if you would like this to be done.

**Example:**

*Router> set ip private 10.0.1.168 255.255.255.0*

## set ip rip [Interface Name] <disabled/passive/active> <rip1/rip2>

**Description:** This command sets the IP RIP state to the **disabled** mode, **passive** mode or **active** mode. When in the **passive** mode, the router will receive RIP broadcast data from other routers (but not transmit); when in **active** mode, it will receive RIP broadcast data from other routers, and also broadcast the routing table and routing table updates as necessary. When "***Interface Name***" is omitted, the command applies to the entire system. The default mode is **Active**.

One common way of configuring routers for a central site and a remote (relatively small) site network is as follows: assume the local site is a small branch network, which is connected to a central site, through which many other networks can be reached. Instead of allowing both routers to turn on RIP, a better way is to turn on RIP for the branch, but set the central site to be in the **passive** mode only. Thus, the central site will not send its routing table to the branch router, but the branch site will send the routing table and updates to the central site. Additionally, on the branch router, the user should set the default route to the WAN connection that leads to the central site.

Now, from the central site's point of view, since it still sees all networks at the branch site, it has no problem routing any packet to the remote site. On the other hand, from the remote site's perspective, whenever a packet is to be routed, the remote site router will apply the standard routing algorithm to the packet and, if no route can be found, the packet will just be passed on to the central site for resolution. The idea is that the central site has the complete routing table, and thus "should" know how to route the packet. With that assumption, the branch router is relieved of the burden of having to receive routing table updates from the central site (which, in case of a large network, could be a huge routing table containing hundreds or thousands of routing entries).

RIP, version 1 (or RIP1) transmits its routing table without subnet or next hop information, while RIP, version 2 (or RIP2) includes this information. These two versions are not compatible and RIP2 should only be specified when communicating to other RIP2 routers.

## set ip <Profile Name>

## set ip <Profile Name> < local-ipAddr> <netMask> <remote-ipAddr>

**Description:** This command enables IP routing over the connection specified by *Profile Name*. Additionally, a WAN connection that supports IP routing, may, either be assigned zero or two IP addresses. If none are assigned, the connection is termed **unnumbered**, a popular feature available in newer routers (since the connection does not consume IP addresses). **Numbered** connections are assigned two addresses, one at each end of the connection (complete with the network mask).

**Example 1:**

This example assigns IP addresses to the two sides of the PPP connection *ppp2* ***204.71.220.153*** is for the local side of *ppp2*, while ***204.71.220.151*** is for the remote side; both use the same network mask, ***255.255.255.0***.

*Router> set ip ppp2 204.71.220.153 255.255.255.0 204.71.220.151*

**Example 2:**

This command activates IP routing over the ISDN connection profile isdnprofile1. When a connection is set up using profile isdnprofile1, unnumbered IP routing will be turned on. (Refer to the section "Profile Commands~~Profile Commands~~")

*Router> set ip isdnprofile1*

## show arp table

**Description:** This command displays the ARP (Address Resolution Protocol) cache table, which contains up to 16 most recent MAC-to-IP-address mappings that have not been aged out.

**Example:**

*Router> show arp table*

*110.0.0.1 at 00:60:20:00:00:15 permanent*

*110.0.0.2 at 00:40:33:3D:D5:DB*

## show icmp statistics

**Description:** This command displays statistical information associated with the Internet Control Message Protocol (ICMP).

**Example:**

*Router> show icmp statistics*

| | *Received* | *Transmitted* |
|---|---|---|
| *Dest Unreachable:* | *0* | *0* |
| *Time Exceeded:* | *0* | *0* |
| *IP Header Error:* | *0* | *0* |

```
Source Quench:          0                       0
Redirect:               0                       0
Echo Request:           0                       0
Echo Reply:                     0                       0
Timestamp Request:      0                       0
Timestamp Reply:        0                       0
Address Mask Request:   0                       0
Address Mask Reply:     0                       0
Calls to icmp error:                            0
Messages Reflected:                             0
```

## show ip

**Description:** This command displays all interfaces on which IP routing has been enabled.

**Example:**

```
Router> show ip
            Admin. Oper.                                Destination/
IfName      State   State   IP Address    Netmask Broadcast Addr
-------------------------------------------------------------------
ppp2        Enabled     Up      20.0.0.1        255.0.0.0 20.0.0.2
lan Enabled     Up      110.0.0.1    255.0.0.0     110.255.255.255
dlci16      Enabled     Up      10.0.0.1        255.0.0.0 10.0.0.2
dlci17      Enabled     Up      (Unnumbered)
```

## show ip <interface name>

**Description:** This command displays the IP configuration over the specified interface.

**Example:**

```
Router> show ip lan
    Interface: lan
    ------------------------------------------------------------------
    IP Address:         192.168.168.230
    Netmask:                255.255.255.0
    Dest. IP Address:   192.168.168.255
    Opr./Admin. State:  Up
    RIP State:          Active Ver.1
    IP Multicast:       Disabled
```

## show ip routing table

**Description:** This command displays the IP routing table. Each entry in the routing table corresponds to a network or a host, and contains necessary information that is required for routing data packets to that network or host. For example, entry 8 means that to send a packet to 110.0.0.1, the packet should be sent to the next hop router (gateway), whose IP address is 40.0.0.5. The destination is, according to the table, 5 hops away (where a “hop” is a traversal of a link from one router to another).

Any entry whose Interface Name is ***lo*** means the corresponding destination network is locally attached to one of the serial interfaces. Also, if the Gateway field is empty, it means either the destination IP network

is directly attached to the router (i.e., the destination is on the same LAN the router is connected to), or the destination is reachable through an unnumbered serial interface.

The meanings of the flags are:

| | |
|---|---|
| | Host |
| S | Static Route |
| G | Gateway |
| C | Cloned Entry |

**Example:**

*Router> show ip routing table*

| *Destination* | *Netmask* | *Gateway* | | *Hop* | *IfName* | *Flags* | |
|---|---|---|---|---|---|---|---|
| *40.0.0.0* | | | *0* | *lan* | | | |
| *192.168.168.0* | *255.255.255.0* | *0* | *lan* | | *C* | | |
| *10.0.0.1* | | | *0* | *lo* | | *H* | |
| *20.0.0.1* | | | *0* | *lo* | | *H* | |
| *20.0.0.2* | | | *0* | *ppp2* | | *H* | |
| *110.0.0.0* | *255.0.0.0* | *40.0.0.5* | *5* | *lan* | | *G* | *S* |
| *120.0.0.0* | *255.0.0.0* | *40.0.0.5* | *1* | *lan* | | *G* | *S* |

## show ip statistics

**Description:** This csommand displays IP routing related statistics.

**Example:**

*Router> show ip statistics*

| | *Received* | *Transmitted* |
|---|---|---|
| *Packets received* | *17418* | |
| *Datagrams generated Locally* | *123* | |
| *Packets Forwarded* | | *15768* |
| *Datagrams Delivered to Upper Layer* | *3241* | |
| *Raw Packets Sent* | | *1650* |
| *Redirects Sent:* | | *0* |
| | | |
| *Packet drops:* | | |
| *IP Header Errors* | *0* | |
| *Unknown Protocols* | *0* | |
| *Not Forwardable:* | *0* | |
| *DONT-FRAGMENT Bit ON:* | *0* | |
| *No Buffers:* | *0* | |
| *No Route:* | *0* | |
| | | |
| *fragmentation:* | | |
| *Total Fragments* | *0* | *0* |
| *Datagrams Reassembled* | *0* | |
| *Datagrams Fragmented for Output* | | *0* |

*Fragments Dropped after Timeout* *0*

*Fragments Dropped (Duplicates/No Space* *0*

## show pat

**Description:** This command displays the static configuration entries in the Network Address Translation Table.

**Example:**

*Router> show pat*

| *Public Port Number* | *Private IP Address* | *Private Port Number* |
|---|---|---|
| *Default* | *192.168.168.121* | |
| *123* | *192.168.168.120* | *234* |
| *26* | *192.168.168.120* | *26* |

*Router>*

## show tcp statistics

**Example:**

*Router> show tcp statistics*

| | *Received* | *Sent* |
|---|---|---|
| *Total Packets* | *0* | *0* |

## show udp statistics

**Example:**

*Router> show udp statistics*

| | *Received* | *Delivered* |
|---|---|---|
| *Total datagrams* | *19368* | *5424* |
| *Datagrams with checksum error* | *0* | |
| *Datagrams with incorrect length* | *0* | |
| *Datagrams dropped due to buffer full* | *1133* | |
| *Datagrams with dest. port unreachable* | *0* | |

# Port Commands

Port related commands allow configuration of a port, the protocol running on the port, and the corresponding protocol parameters. In addition, commands are available for clearing statistical counters, enabling/disabling ports, and displaying port configuration and statistics.

There are two modes of operation when setting a port: (1) the advanced mode, which causes detailed prompts to be displayed, allowing the user to configure all parameters, (2) the express mode, which assumes default values for most parameters, and therefore causes a minimal number of prompts to show. The system will come up in the express mode. Typing a Ctrl-E (^E, i.e., pressing both the E and control key together) will cause the mode to be toggled.

## clear port statistics [port name]

**Description:** This command clears port statistics. If a port is not specified, the statistics counters on all ports are cleared.

## disable port <port name>

## enable port <port name>

**Description:** These two commands is used to disable or enable a port.

## ⊕set port <port name>

The *set port* command is used to initialize or modify the characteristics of a hardware port on your router. Hardware ports are identified by port name and are model-specific. The name "ISDN" means the ISDN BRI interface. The name "ewan" stands for Ethernet-based WAN port which is connected to broadband modem.

**PORT TYPE: ISDN**

**Description:** This command configures the ISDN port. For European users, select Switch Type as "Europe (ETSI)" and configure the related parameters.

**Example:**

```
Router> set port isdn
 enter switch : 1> Japan (INS Net) 2> Europe (ETSI) 3> NT DMS-100
                4> NI-1            5> ATT5ESS (MP)   6> ATT5ESS (P2P)
                7> Taiwan          8> OCN            9> Permanent 64K
               10> IDSL/Perm 128K 0> AutoDetect, [0]: 2
 How many directory numbers [DN] are assigned (1, 0-3): 2
 enter Directory Number 1 [DN1] [Unspecified]: 5551111
 enter Directory Number 2 [DN2] [Unspecified]: 5552222
 Port isdn is configured successfully.
Router>
```

**PORT TYPE: EWAN**

**Description:** This command is used to enable the ewan port.

**Example:**

```
Router> set port ewan
 Port ewan is configured successfully.
Router>
```

## show port

**Description:** This command displays the configuration information for all ports.

**Example:**

```
Router> show port
    Port Name :   isdn              Port Type :        ISDN
    Admin Status: Enabled           Op State:              Down
    Directory#1:  5551111           Directory#2:       5552222
    Sub-addr Req:No
    Switch Type:  Europe (ETSI)
    Advice of Charge
    Unit price:   Unspecified   Currency:              Unspecified

    Port Name :   ewan              Port Type :        EWAN
    Admin State : Enabled           Data Link Type:    Ethernet
```

## show port <port name>

**Description:** This command displays the configuration of a WAN interface port.

**Example 1:**

```
Router> show port isdn
    Port Name :   isdn              Port Type :        ISDN
    Admin Status: Enabled           Op State:              Down
    Directory#1:  5551111           Directory#2:       5552222
    Sub-addr Req:No
    Switch Type:  Europe (ETSI)
    Advice of Charge
    Unit price:   Unspecified   Currency:              Unspecified
Router>
```

**Example 2:**

```
Router> show port ewan
    Port Name:    ewan              Port Type:         EWAN
    Admin State:  Enabled
    Data Link Type:Ethernet         Speed:                 10 Mb
     MAC Address:       90-00-12-34-56-79

     Profile type:  EWAN            Admin. State:  Enabled
     Encapsulation:     Ethernet        MAC Address:90-00-12-34-56-79
     Oper. State:   Down            Max Receive Unit:  1500
     System Name:Local Router
```

## show port statistics <port name>

**Example 1:**

```
Router> show port statistics isdn
                                    Received:          Transmitted:
    ------------------------------------------------------------
D-Channel
    Total Octets:           230                 347
    Total Packets:          14                  8
```

*Total Error:* *0* *0*

*B1-Channel*

*Total Octets:* *2316* *375*

*Total Packets:* *46* *10*

*Total Error:* *0* *0*

*B2-Channel*

*Total Octets:* *0* *0*

*Total Packets:* *0* *0*

*Total Error:* *0* *0*

**Example 2:**

```
Router> show port statistics ewan
    interface: e1
    ------------------------------------------------------------------
                                                  Received        Transmitted
    ------------------------------------------------------------------
    Total packets                          0              368
    Total octets                           0              217120
    Multicast packets                      0              0
    Error on interface                     0              0
    CSMA collisions                        0
    Packets dropped                        0
    Packets with unsupported protocol      0
    Last update time (sec)                 4841
Router>
```

# Profile Commands

This section details the commands used to create and manipulate static profiles. Static profiles are created for connections communicating with a remote router. Examples of this type are Internet connections and Remote LAN connections. Unlike user profiles (see "Dial-in User Commands~~Dial-in User Commands~~"), which are created dynamically, static profiles are maintained permanently and created at system initialization time from configuration information stored in Flash ROM. The creation of a static profile may cause a static routing entry to be added to one or more of the routing tables, if routing is defined over that profile.

Up to three alternate phone numbers are configurable within a switched connection profile so that if the primary telephone number cannot be connected, each alternate phone number is tried, in turn. An alternate number may be used if the previously tried number failed to connect for any reason. After a disconnection, subsequent connect attempts use the original phone number list.

All other parameters of the Connection Profile will be used for any connected number. A static route is associated with the profile, not any particular telephone number.

The System Log messages will identify any alternate numbers being used. The Connection Log will include the phone number used for a successful connection.

For each alternate phone number, there may be an alternate secondary phone number for multilink connection.

Existing profiles are edited also using the “add profile” command. In this case, the defaults shown are the existing configured values.

This router only support one profile over EWAN interface. When an ewan profile is configured, the following new added profile(s) will select ISDN automatically. User can modify the ewan profile by using “add profile” command or “delete profile”, then “add profile” again.

## ⊕add profile <Profile Name>

**Example 1 – Set up an Internet Access Profile over ISDN**

*Router> add profile daniel*
*The system is currently in Advanced Mode, press Ctrl-E to switch to*
*Express Mode.*
*Add new connection profile “daniel” ...*
*Interface type: ISDN*[3]
*enter access type: 1> internet access only*
*2> remote office dial in/out (1): 1*
*enter remote directory number (Unspecified): 5553333*
*enter ISP account name (Unspecified): user-name*
*enter ISP account password (Unspecified): ****
*enable compression (No, yes/no):*
*Profile daniel is configured successfully. Configuring Network*
*Protocol over daniel ...*
*enable IP routing (Yes, yes/no):*
*Set this profile as IP default route (Yes, yes/no):*
*Router>*

**Example 2 – Set up a Remote Office Profile over ISDN**

*Router> add profile julia*
*The system is currently in Advanced Mode, press Ctrl-E to switch to*
*Express Mode.*
*Add new connection profile “julia” ...*
*Interface type: ISDN*
*enter access type: 1> internet access only*
*2> remote office dial in/out (1): 2*
*enter action mode (Dial only, dial only/answer only/both): d*
*enter remote directory number (Unspecified): 5556666*
*enter my account name (Unspecified): user1*
*enter my account password (Unspecified): ****
*enable compression (No, yes/no):*
*Profile julia is configured successfully. Configuring Network*
*Protocol over julia ...*
*enable IP routing (Yes, yes/no):*
*Set this profile as IP default route (No, yes/no):*

[3] Assume one ewan profile is already configured.

*enter remote network IP address (Unspecified): 192.168.167.0*

*enter remote network IP netmask (Unspecified): 255.255.255.0*

*Router>*

**Example 3 – Internet Access through EWAN port:**

*Router> add profile wilson*

*The system is currently in Advanced Mode, press Ctrl-E to switch to*

*Express Mode.*

*Add new connection profile "wilson" ...*

*enter interface type (ISDN, ISDN/EWAN): ewan*

*enter access type: 1> internet access only*

*2> remote office dial in/out (1): 1*

*enter encapsulation type (Ethernet, Ethernet/PPPoE):*

*Profile wilson is configured successfully. Configuring Network*

*Protocol over wilson ..*

*enable IP routing (Yes, yes/no):*

*obtain IP addresses automatically (Yes, Yes/No):*

*enter host name [system name] (Local Router):*

## clear profile statistics [Profile Name]

The statistics fields in the specified static profile are reset to initial values when the *Profile Name* parameter is provided in command line. If no *Profile Name* is specified, all profile statistics are cleared.

## connect profile <Profile Name>

For switched profiles, this command activates the profile as if a trigger occurred. This command has no effect on leased line profiles.

## delete profile <Profile Name>

The specified profile is removed from the system.

## disable profile <Profile Name>

The administrative state of the specified profile is set to "disabled". A profile cannot be used unless it is enabled.

## disconnect profile < Profile Name>

For active switched profiles, this command terminates the connection as if an idle timeout occurred. This command has no effect on leased line profiles.

## enable profile <Profile Name>

The state of the specified profile is set to "enabled". Only enabled profiles are available for use. A profile's state is set by default to *enabled* when it is created.

## show profile

This command displays a summary of all configured static profiles.

**Example:**

```
Router> show profile
Profile                          Admin          Remote         Call
Name          Type               State          Number         Originator
----------------------------------------------------------------------
wilson        EWAN               Enabled
daniel        ISDN               Enabled        5553333        Local only
julia         ISDN               Enabled        5556666        Local only
```

## show profile <Profile Name>

**Description:** The details of a configured static profile are displayed.

**Example 1:**

```
Router> show profile wilson
  Profile type:              ISDN          Admin. State:          Enabled
  Call Originator:           Local only    Remote DN:             5553333
  Data Service:              Autodetect    Clid Auth:             No
  Call Back:                 No            Call Back #:
  PPP Oper. State:           Down
  Max Receive Unit :         1524
  My Account Name :          user-name
  Remote Account Name:
  Send Auth. Type:           Either  Recv Auth. Type:       None
  TCP/IP VJ Compression:     Disabled      Inactivity Timeout:    120
  Multilink Type:            Overflow      Second Dial Number:
  Second Caller ID:                        Second Callback Number:
  Upper Threshold:           85            Lower Threshold:       45
```

**Example 2:**

```
Router> show profile wilson
  Profile type:   EWAN              Admin. State:       Enabled
  Encapsulation:        Ethernet            MAC Address:       90-00-12-34-56-79
  Oper. State:    Down              Max Receive Unit: 1500
  System Name: Local Router
```

## show profile statistics

**Example:**

```
Router> show profile statistics
  Prof       Oper.       Packets       Packets       Errors Errors Q-full
  Name       StateSent             Rcv'ed Sent             Rcv'ed Discard
 ----------------------------------------------------------------------
```

*wilson Down 0 0 0 0 0*

### show profile statistics <Profile Name>

**Example:**

*Router> show profile statistics wilson*

| *wilson* | *Received* | *Transmitted* |
|---|---|---|
| *Total octets:* | *0* | *0* |
| *Total packets:* | *0* | *0* |
| *Total errors:* | *0* | *0* |

## Security Command

### set ip private <ip_addr> <netMask>

**Description:** This command is used to modify the "private" IP address on the router's LAN interface. Please refer to IP command category for details.

## SNMP Commands

Remote SNMP management consoles can access the set of MIBs implemented in the router. MIB information is transferred from the router's SNMP Agent to the SNMP Management console via SNMP *Gets* and *Traps* (*Set* commands are not supported).. *Traps* are unsolicited status messages sent from the router to report management events asynchronously. Trap Managers must be configured in order to receive these messages.

### clear trap manager <1-5>

**Description:** This command clears the IP address for the specified trap manager. When an SNMP trap condition is met, and if trap generation has been enabled, a trap message will automatically be sent out to each trap manager whose IP address has been defined. A total of five trap managers can be defined in the system.

### disable trap

### enable trap

**Description:** This command is used to enable or disable trap message generation. When trap generation is disabled, no SNMP trap messages will be generated. When it is enabled, any SNMP traps will be sent to each of the trap managers that have been defined.

### set community string read <"password">

**Description:** This command sets the community string used for authenticating SNMP get and getnext requests.

The default for the read community string is "public". The community string is case sensitive.

## set trap manager <1-5> <ipAddr>

**Description:** This command sets the IP address of the nth trap manager (n=1-5).

**Example:**

*Router> set trap manager 1 203.23.12.71*

## show snmp statistics

**Example:**

*Router> show snmp statistics*

| | *Received* | *Transmitted* |
|---|---|---|
| *Total Packets* | *0* | *0* |
| *Request Variables* | *0* | |
| *SET Variables* | *0* | |
| *GET Requests* | *0* | |
| *GETNEXT Requests* | *0* | |
| *GET-RESPONSEs* | *0* | *0* |

*Errors:*

| | | |
|---|---|---|
| *Bad Versions* | *0* | |
| *Bad Community Uses:* | *0* | |
| *ASN1 Parse Errors* | *0* | |
| *Packet Too Long* | *0* | |
| *NO-SUCH-NAME Errors* | *0* | |
| *BAD-VALUE Errors* | *0* | |
| *READ-ONLY Errors* | *0* | |
| *GENERAL-ERR Errors* | *0* | |

## show trap manager [1-5]

**Description:** This command displays the trap managers that are currently defined. If a trap number is used, only that trap manager is displayed.

**Example:**

*Router> show trap manager*

| *No* | *Trap Manager IP-Address* |
|---|---|
| *1* | *11.22.33.44* |
| *2* | *55.66.77.88* |

# Statistics Commands

## clear compression statistics <Profile Name>

**Description:** Refer to this command under Compression Commands.

### clear port statistics [port name]

**Description:** Refer to this command under Port Commands.

### clear profile statistics [Profile Name]

**Description:** Refer to this command under Profile Commands.

### show compression statistics <Profile Name>

**Description:** Refer to this command under Compression Commands.

### show icmp statistics

**Description:** Refer to this command under IP Commands.

### show ip statistics

**Description:** Refer to this command under IP Commands.

### show port statistics <port name>

**Description:** Refer to this command under Port Commands.

### show profile statistics [Profile Name]

**Description:** Refer to this command under Profile Commands.

### show snmp statistics

**Description:** Refer to this command under SNMP Commands.

### show tcp statistics

**Description:** Refer to this command under IP Commands.

### show udp statistics

**Description:** Refer to this command under IP Commands.

### show <Interface Name> statistics

**Description:** This command displays statistical information associated with the specified profile or the LAN.

## System Commands

### change password

**Description**: This command allows the user to change the password used to log on to the Command Line

Interface or the HTTP. A password is a character string that starts with a letter and contains at least 6 and up to a total of 15 alphanumeric characters. The password is case sensitive. The default factory setting is “password”.

If you forget the password, the only way to recover is clear the entire configuration and return the unit to its original state as shipped from the factory. Unfortunately, this means that you have to re-enter all of your configuration data.

To clear the configuration and restore the password to the default, follow these steps:

Connect a console to the Console port.

Turn off the router, then turn it on again. In the console window, you’ll see the message “Loading firmware...”

When you see the message "Ready", **immediately** (within one second) press Control-C.

The router will now reset. When this is complete, the router will return all settings to the factory default. The password will once again be “password”.

**Example:**

*Router> change password*

*Please enter the old password:*

*Please enter the new password:*

*Please re-enter the new password:*

## clear config

**Description:** This command is used to clear the configuration data in the flash memory. After clearing, the system will reboot. All user-configured data are lost. The configuration will return to the factory default settings.

## disable remote-mgt

## enable remote-mgt

**Description:** This command allows the administrator to lock out or enable both HTTP and telnet management connections. Only a direct console connection is supported if remote management is disabled.

## disconnect telnet session <1-5>

**Description:** This command disconnects an existing telnet session. This command is only valid in Console port.

**Example:**

*Router> disconnect telnet session 1*

## download config <fileName> from <ipAddr>

**Description:** This command causes configuration file **router.cfg** to be downloaded to the system from a tftp server with the specified IP address.

**Example:**

*Router> download config router.cfg from 205.51.23.12*

## download firmware

**Description**: This command causes the product firmware to be downloaded to the system from a directly attached PC running the terminal emulation software (one with file download capability). Note that this command cannot be used from a telnet session. This is an alternative to downloading the software using the HTTP browser.

Since the router will reset after this operation is complete, the system will first prompt for the confirmation. The system will ask the user to select the download speed. The user may then change the terminal baud rate for a faster download and press enter to continue (some terminal emulators require a "disconnect" followed by a "connect" in order for the changed parameters to take effect). Select the Z-modem protocol for use in downloading the firmware. The user then selects (opens) the firmware file for actual downloading.

## help

(This list may differ depending upon the router model):

*Router> help*

*Commands are categorized as follows:*

| | | |
|---|---|---|
| *(1) Bridging* | *(2) Compression* | *(3) Diagnostics* |
| *(4) Filtering* | *(5) IP* | *(6) Port* |
| *(7) Profile* | *(8) Security* | *(9) SNMP* |
| *(10) Statistics* | *(11) System* | |

*Please enter a selection number [1..11] for more detail information: 1*

*disable bridging <ifName>*
*disable learning*
*enable bridging <ifName>*
*enable learning*
*show bridging*
*show learning*
*show learning <ifName>*

*Please enter a selection number [1..11] for more detail information:*

## logout

**Description:** This command logs the user out of the system.

## reset system

**Description:** This command allows the user to reset the system. A confirmation will be displayed.

## save config

**Description:** This command saves any configuration changes to the flash memory.

In the background, the system is already periodically checking to see if any configuration changes have been made.

If so, the entire configuration will be automatically saved to the flash memory. However, this command can also be used to execute the save operation immediately after some configuration changes, e.g., when the user intends to power down the system.

## set console baud <baudrate>

**Description:** This command is used to set the baud rate for the auxiliary (console) port. The default baud rate is 19200 bits per second. After the baud rate is changed, the console will no longer work properly until the terminal baud rate is changed accordingly. Other allowed speeds include 115.2K, 57.6K, 38.4K, 28.8K, 19.2K, 14.4K, 9.6K, 4.8K, 2.4K, and 1.2K.

**Example:**

*Router> set console baud 19200*

## set console timeout <1-60>

**Description:** This command is used to set the console time-out value (in minutes). The default value is 10 minutes. That means if the user does not type anything on the console for 10 minutes, the console session will automatically be terminated.

This timeout value also applies to telnet sessions.

**Example:**

*Router> set console timeout 20*

## set date <mm-dd-yy>

**Description:** This command sets the current date in the router.

**Example:**

*Router> set date 4-12-01*

## set daylight time <on/off>

**Description**: This command sets the setting for Daylight Savings Time. This is only used for display purposes and has no effect on the System Time. Normally this parameter would be learned from a managing browser session.

## ⊕set internet access time

**Description:** This is the time during which access to the Internet (an ISP switched profile) will be enabled and triggered. Outside of this time range, this connection profile will not be enabled. For this purpose the connection to the Internet is defined as the default IP route. The router time is set either manually through the *set time* command, or automatically via a connection to an HTTP browser. Of course, this restriction only makes sense for switched connections. Leased line connections are not affected.

Note that the router may lose its time setting in the event of a reset or a power cycle. If this is the case, until the system time is once again set, then Internet Access is either enabled or disabled until depending upon the response to the last question.

**Example:**

*Router> set internet access time*

*enter Day-of-the-week (all, (a)ll/(d)ay-range): d*

*enter dd1-dd2 (Unspecified): mon-sat*

*enter Time-of-day (all, (a)ll/(t)ime-range): t*

*enter hh1:mm1-hh2:mm2 (Unspecified): 07:00-18:00*

*If the system loses its time setting, allow Internet Access ? (Yes, Yes/No):*

## set log level <1-10>

**Description:** This command changes the system log level, causing different events to be logged into the system log table. It is often used for debugging purposes. The default log level is 2, which means all events belonging to log level 2 or below will be logged into the system log.

## set prompt <"prompt">

**Description:** This command defines a new command prompt. A prompt of up to 15 characters may be entered. The default prompt is "Router>".

**Example:**

*Router> set prompt "Yes, Master"*

*Yes, Master>*

## set system contact <"name">

**Description:** This command sets the system contact information. The maximum number of characters allowed is 60. This information is displayed in the "show system" command, as well as in the "System Information" screen in the HTTP browser screen.

**Example:**

*Router> set system contact "John Doe, pager: (408) 731-4567"*

## set system location <"location information">

**Description:** This command sets the system location. The maximum number of characters allowed is 60. This information is displayed in the "show system" command, as well as in the "System Information" screen in the HTTP browser screen.

**Example:**

*Router> set system location "480 Mercury Drive, Sunnyvale, CA 94086"*

## set system name <"system name">

**Description:** This command sets the system name. The maximum number of characters allowed is 30. This information is displayed in the "show system" command, as well as in the "System Information" screen in the HTTP browser screen.

**Example:**

*Router> set system name "Home Gateway1"*

## set time <hh:mm:ss>

**Description:** This command sets the time of the day (24-hour clock). Note that the time will normally be set automatically when an HTTP browser first connects to the router.

**Example:**

*Router> set time 20:33:00*

## set timezone <-12 - +12>

**Description:** This command specifies the time zone for the location as an offset from Greenwich Mean Time (GMT). The time zone is normally set automatically when an HTTP browser first connects to the router.

**Example:**

*Router> set timezone -8*

*Time Zone is set to GMT-8 hours.*

## show config

**Description:** A concise summary of the router configuration is displayed.

**Example:**

*Router> show config*

*IP Addr: 192.168.168.230 NetMask: 255.255.255.0 IP RIP: D*

*Port 1: ISDN PPP ENABLED Europe (ETSI)*

*Ewan : EWAN ENABLED Speed = 10 Mb*

## show connection log

**Description:** The connection log is displayed by the system. Up to 128 entries are maintained by the router in wraparound fashion. For a complete description of these entries, refer the *User Guide* for your system.

**Example:**

*Router> show connection log*

*1 9/14/99 22:15:38 N/A(N/A): Triggered Detail: IP/TCP 192.168.168.240->63.192.*

*151.44 1905->139*

*2 9/14/99 22:16:28 Modem 3(Office): Connected Detail: Outgoing Call to 14085553456*

## show interface list

**Description:** This command displays the status of all interfaces in the system, including their encryption status.

```
Router> show interface list
                                        Oper.       IP          BRG         Comp.
IfName          Type                    State   MTU Status  Status  Status
------------------------------------------------------------------------
lo              LOOPBACK                Up      1536 Enable Disable n/a
lan     ETHERNET        Up      1500 Enable Enable n/a
```

## show internet access time

**Description:** The current setting of the Internet time restriction is displayed. See *set internet access time* for details.

**Example:**

```
Router> show internet access time
    Day-of-the-week     : Mon-Sat
    Time-of-day         : 13:30- 5:00
```

## show system

**Description:** This command displays system and SNMP related configuration. All of them can be changed through individual commands, except for the S/W and H/W version numbers that are constant for each version of the product.

**Example:**

```
Router> show system

    System Name: Router             Up Time:    0 months    1 days 21:21:05
    ------------------------------------------------------------------------
    system description:         IP Brouter Over ISDN Line
    system contact:             Unknown
    system location:            Unknown
    community string (read):    public
    Trap generation:            Disabled

    Total Serial Ports: 1  S/W Version:  1.03    H/W Version:  1.0

    MAC Address:        00-60-20-10-00-70
    Console Baud Rate :  19200
    Console Timeout:    10(min)             Learning State:     Enabled

    Remote Management State:   Enabled
    DHCP State:         Enabled
    IP RIP Mode:        Active    Ver.1
    IP address:         0.0.0.0             network mask:0.0.0.0
    Private IP address:  192.168.168.230    network mask:255.255.255.0
    Enabled features:   HTTP Compression SNMP Filter NAS CLI L2L Bridging
```

## *show system log*

**Description:** The system log contains logs of various events of interest, depending on the log level set at the time. Common events include login, a PPP connection goes up or down (log level 2), a frame relay DLCI connection goes up or down (log level 2), … as well as certain protocol progress messages for

debugging purposes.

This command shows the next 22 entries of the system log. For example, if there are 60 entries in the log, the first "show system log" command will show log entries 1 through 23, the next command will show entries 24 through 46, and the next command will show entries 47 through 60, followed by 1 through 9. When the system powers up, the log is re-initialized and contains no entries. As time passes, when the 128-entry log table becomes full, new entries will simply replace the oldest entries, thus a first-in, first-out scheme is used.

**Example:**

```
1   Sep-03-99   16:52:48   PPP Network Protocol Event: mdm3.2 IPCP Inactivity
2   Sep-03-99   17:21:59   ISDN: ACTV REQ
3   Sep-03-99   17:22:11   ISDN: T3 Expire State = F4
4   Sep-03-99   17:22:11   ISDN: Line De-activated
5   Sep-03-99   17:27:40   ISDN: ACTV REQ
6   Sep-03-99   17:27:50   ISDN: ACTV REQ
7   Sep-03-99   17:27:52   ISDN: T3 Expire State = F4
8   Sep-03-99   17:27:52   ISDN: Line De-activated
```

## show telnet session

**Description:** This command is used to display all existing telnet sessions.

**Example:**

```
Session Id      Remote IP           Remote Port
-------------------------------------------------------
1                           204.71.212.38 2052
2                           204.71.212.39 2564
```

## show time

**Description:** This command shows the time zone, daylight savings time setting, date and time of the day. For router systems, the time is only correct after an HTTP session has accessed this system or the time has been manually set using the "set time" command.

**Example:**

```
Time (GMT-8) (Daylight Saving Time) : Thu Apr 22 11:20:24 1999
```

## upload config <fileName> to <ipAddr>

**Description:** This command causes the system configuration to be uploaded to the specified tftp server (whose IP address is 205.51.23.12) as a file called **router.cfg**.

**Example:**

```
Router> upload config router.cfg    to 205.51.23.12
```