ExpressRoute80

ISDN Router

USER'S MANUAL

Printing History

Version 1.0 (Original Release)   October 1997
Version 2.0 (2nd Release)   April 1998

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency, energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-   Reorient or relocate the receiving antenna.

-   Increase the separation between the equipment and receiver.

-   Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-   Consult the dealer or an experienced radio/TV technician for help.

Use only shielded cables to connect I/O devices to this equipment.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions. (1)This device may not cause harmful interference and (2)This device must accept any interference received, including interference that may cause undesired operation.

Manual Part No. M-E80-01

Contents

1 INTRODUCTION

The ExpressRoute 80 (E80) is a compact router/bridge designed for small office and home applications by providing a consolidated data and voice link to Internet, Intranet, and the telephone network over a single ISDN line.
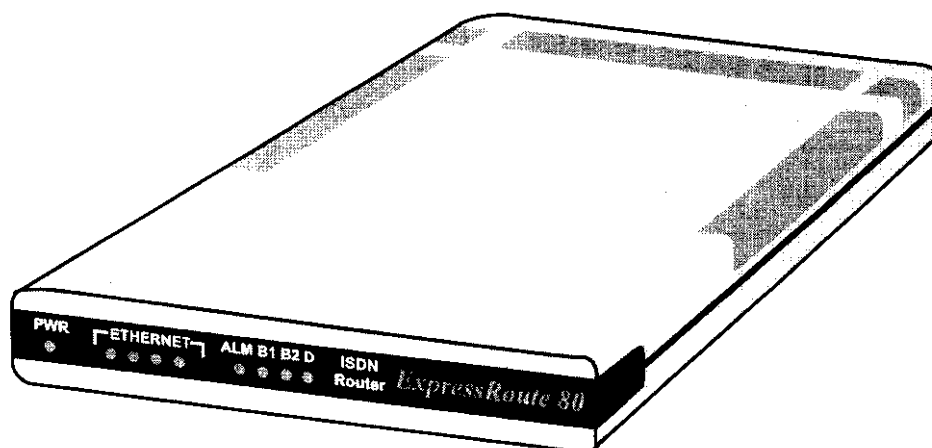

Figure 1-1 The ExpressRoute 80

The E80 ISDN Router provides an ideal means of connecting a local area network consisting of Ethernet stations to the Internet through a local Internet Service Provider (ISP) and using conventional voice and fax services over the same ISDN line.

Using the E80, users at the Ethernet workstations can communicate freely with each other over private intranet and can access Internet servers all via the same ISDN line. The E80 establishes the ISDN connection when required and automatically drops when it is not in use.

By using up to 128 KBPS bandwidth of an ISDN digital line, the E80 overcomes the slow response times, noise and data corruption which may be exhibited by modems using analog lines. The E80 includes all the hardware and software necessary for accessing the Internet and corporate LANs.

The E80 includes full management capabilities which permit easy configuration of the router and ISDN parameters. Management may be performed from a console, through SNMP network management software, or through a web browser.

A schematic of how the E80 is used is shown in Figure 1-2 An E80 ISDN Router Application.
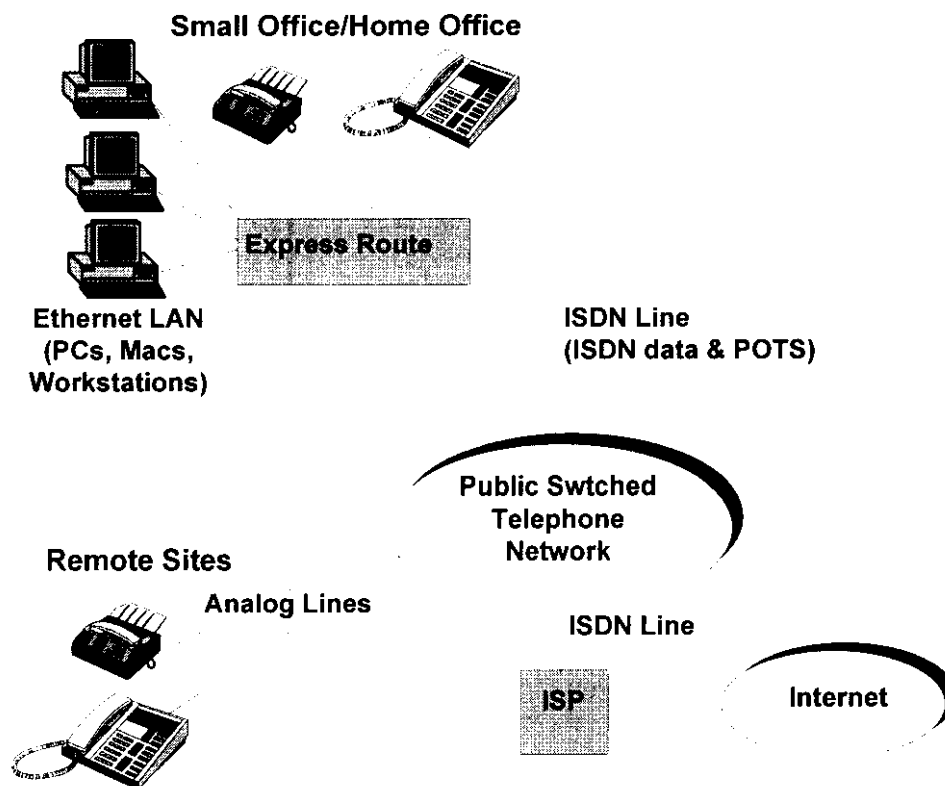
Small Office/Home Office

Figure 1-2 An E80 ISDN Router Application

The E80 supports the following features:

ISDN

- U or ST interfaces

- Switched ISDN service for various switches worldwide :

National ISDN, ATT 5ESS, DMS switches in North America
   EuroISDN(ETSI) switches in Europe
   NTT switches in Japan
   EuroISDN switches in Taiwan, Singapore
   ATT 5ESS switches in Korea

- Detailed accounting including dialed numbers, disconnect causes, frame statistics

- Auto Dial-out triggered by outgoing LAN traffic, auto disconnect due to inactive connection

- Bandwidth-On-Demand, 0<->1<->2 bandwidth management,1B to 2B if traffic increases beyond threshold,. 2B to 1B if traffic falls below threshold, 1B to 0B if traffic is idle for more than an pre-defined period

Ethernet

- 4 port Ethernet Repeater with unlimited LAN users

Internet/Intranet

- PPP, MultiLink PPP (MLPPP), LCP, IPCP, IPXCP, and BCP

- Internet and Intranet connection profiles. Allows one B channel for Internet connection and the other B channel for intranet connection

- STAC LZS data compression with 128 KPBS -> 512 KBPS, 4:1 compression ratio on normal text file

- Static or dynamic IP address assignment

- Static or dynamic IP Route

Security

- CLID (caller ID)

- Call-Back (hang-up and dial the caller)

- PAP/CHAP (PPP authentication protocol)

- Access List (filtering of packets bases upon IP address)

- NAT (network address translation). Hides internal IP addresses from outside world, no need to change existing IP address assignments, allows the subscription of single IP address account for the entire LAN.

Network Management

- From local console, NMS/SNMP or Web Browser/HTTP

- NMS runs on Windows 3.1, Windows95 and Windows NT platforms

- Alarm warning on ISDN usage

- Configuration file save and restore

Analog Services

- 2 RJ-11 ports for telephone, modem or fax analog devices

Router Software

- Software upgraded through TFTP and stored in FLASH memory

About this Manual

Chapter 2, Installation. This chapter provides details of how to install the E80 hardware and software. Guidance is provided about the ISDN line that is required from your telephone company and the personal computer requirements to use the Network Management System software.

Chapter 3, Concepts and Principles of Operation. This chapter covers the concepts and principles of operation of three major topics : ISDN, Data Services, and voice services. The E80 operation principles in the area of Internet/Intranet profiles, and bandwidth management are discussed in detail. This chapter also includes information about ISDN line provisioning.

Chapter 4, Set-up and Configuration. This chapter provides details of how to setup and configure your E80 for operation. This chapter provides brief details of how to perform this from a console or from a Browser. Full details are provided for the recommended method of setup and configuration from the NMS software provided with the E80 router.

Chapter 5, Troubleshooting. This chapter provides troubleshooting procedures in the unlikely event that E80 does not function properly.

An index is provided at the end of the manual.

2 INSTALLATION

General

The E80 is shipped in a box which contains the following items:

• The E80 router

• One Power Adapter with cable

• One ISDN cable, 6 foot long with an RJ45 connector at each end

• One data cable with a DB9 connector at each end

• One 3½" diskette containing the E80 NMS software

• One 3½" diskette containing the E80 EasyWeb software

• This E80 user manual

Check the contents of the box and ensure that everything is included. If there are any items that are missing or appear to be damaged, replace all the items back in the box and contact your sales representative.

Hardware Installation

Before installing the hardware, you will need:

A 100 to 230 VAC wall outlet within a few feet of where you intend to place the E80 router.

An ISDN BRI line RJ45 termination within a few feet of where you intend to place the E80 router.

If you intend to connect an analog modem, telephone or fax to your E80, you will need a standard RJ11 telephone cable for each of the connected devices.

Each Ethernet LAN connection to the E80 must use a normal straight through twisted pair cable with an RJ45 connector. If the LAN employs coaxial cable, an adapter converting the coaxial cable to a twisted pair RJ45 cable must be used.

All connections during the hardware installation are made at the E80 rear panel shown in Figure 2-1, E80 Rear Panel.
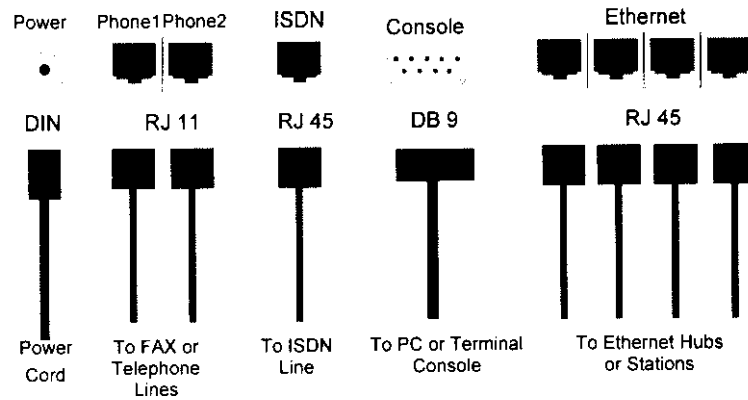

Figure 2-1, E80 Rear Panel

1. Determine the place where the E80 is to reside, it is designed to rest on a flat level surface such as a desktop or table. Make sure that an AC power source and the ISDN termination are nearby.

    Connect the Ethernet LAN to any or all of the four RJ 45 ports labeled Ethernet using cables with RJ45 connectors. You may daisy-chain the E80 embedded repeater to other external Ethernet hubs to accommodate more than 4 LAN users by using a cross-over RJ45 cable (see Figure 2-2, Using Ethernet Hubs).
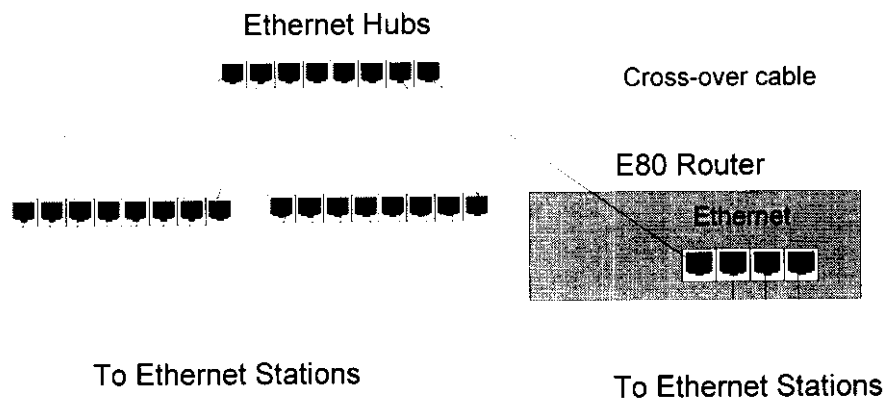

Figure 2-2, Using Ethernet Hubs, all Ethernet stations can access the Internet through the E80 Router

2. Connect the ISDN line to the E80 Router using the supplied RJ45 cable. Connect one end to the ISDN line termination and the other end to the RJ45 on the E80 rear panel labeled ISDN. If your E80 is equipped with ST interface, use the same RJ45 cable to connect the

E80 to the a NT1 device (normally provided by the telephone company).

3. If you intend to connect analog devices such as modems, telephones or faxes to the E80, use standard telephone RJ11 cable and connect them to the two RJ11 ports on the E80 rear panel labeled Phone1 and Phone2. These are general purpose ports and either can be used for any analog devices, phone, modem, fax machine.

4. If you intend to use an alphanumeric terminal as a console for managing the E80, connect its RS232 port to the DB9 port on the E80 rear panel labeled Console. Use the DB9 to DB9 straight through cable. You may need a DB9 to DB25 adapter at the terminal end if the terminal's RS232 uses a DB25 connector.

5. Apply power to E80 using the AC power adapter and cable supplied with the E80. Connect the end of the cable with the small round DIN connector to the DIN port on the rear panel of the E80 labeled Power. Plug the adapter into the AC wall outlet.
There is no ON/OFF switch on the E80, when the adapter is plugged into the wall outlet, the E80 is automatically ON and is operational.

Software Installation

The E80 software diskettes contain two software packages, namely, NMS and EasyWeb.

The E80 Network Management System (NMS) is used to manage the E80 from a Windows based PC equipped with TCP/IP protocol stack. NMS communicates with the E80 through Simple Network Management Protocol (SNMP)

NMS consists of two applications, One is the SNMP management which is used to configure the E80 router and the other is ClearMon which displays the E80 real-time status in a front panel like mini-window.

EasyWeb, which also runs on a Windows95/NT (not Windows 3.1) based PC on the attached Ethernet. EasyWeb is a proxy web server and acts as an adjunct to a PC web browser. EasyWeb translates HTTP requests into SNMP requests and forwards them to the E80. Likewise, SNMP responses from the E80 are translated into HTTP responses and delivered to the browser. EasyWeb makes it possible to manage the E80 from any PC with a web browser.

Installing the E80 NMS

1. Select a Windows-based PC on the Ethernet network that is attached to the E80 directly or indirectly through another repeater. Insert the supplied E80 NMS software diskette into the disk drive.

2. Under Windows 95/NT select Run in the Start Menu and type A:\Setup.exe in the Open field and click OK.

   Under Window 3.1 select Run in the File menu of the Program Manager window and type A:\Setup.exe in the Command Line, and click OK.

   Note: If the designation of the floppy disk drive is B: use this instead of A:.

3. The setup program will assign a default directory for the installed program. You will be asked to either accept the default directory or assign a different one.

4. When the setup program is finished, you will see:

   Wishcom NMS and ClearMon in the Start/Programs menu under Windows 95/NT.

   The NMS and ClearMon icons under Windows 3.1 (see Figure 2-3, E80 Software Icons) are :.

Figure 2-3, E80 Software Icons

5. When the setup is complete, the programs may be launched. Details of launching and operating the programs are described in Chapter 3.

Uninstalling NMS

Under Window95/NT you can uninstall Wishcom NMS by selecting Add/Remove Programs in the Start/Settings/Control Panel window. Select NMS from the list and click the Add/Remove button.

Installing EasyWeb

The procedure for installing EasyWeb depends upon whether your system has an installed HTTP server or not.

Installing EasyWeb if there is NO installed HTTP server.

1. Select a Windows95/NT-based PC on the Ethernet network that is attached to the E80 and there is no HTTP server running. Stop the active HTTP server if there's one. Insert the supplied E80 EasyWeb software diskette into the disk drive.

2. Select Run in the Start Menu and type A:\Setup.exe in the Open field and click OK.

   Note: If the designation of the floppy disk drive is B: use this instead of A:.

3. The setup program will assign a default directory for the installed program. You will be asked to either accept the default directory or assign a different one.

4. When the setup program is finished, you will see in the Start/Programs.

5. When the setup is complete, the programs may be launched. Details of launching and operating the programs are described in Chapter 3.

Installing EasyWeb if there is an installed HTTP server.

1. Select a Windows95/NT-based PC on the Ethernet network that is attached to the E80. Insert the supplied E80 EasyWeb software diskette into the disk drive.

2. Select Run in the Start Menu and type A:\Setup.exe in the Open field and click OK.

   Note: If the designation of the floppy disk drive is B: use this instead of A:.

3. The EasyWeb setup program will install all the HTML files and the cgi executable file that will be required to run EasyWeb. To make these files accessible to the browser you must administer your existing web server.

   Copy the cgi-bin file installed by Setup (found in the <install path>\EasyWeb directory) to the directory specified by your web server's cgi-bin. to the directory specified by your web server's cgi-bin. X

   Note: <install path> is the path that was used to install EasyWeb during the setup process

   You may have to consult your web server's vendor to find out how to configure aliases and directories.

   Example using the Microsoft Personal web server on Windows 95.

1. Run the Microsoft Personal web server on Windows 95

2. Double click the icon on the right end of the task bar. A tagged Personal Web Server Properties) dialog box pops up.

3. Select the Administration page.

4. Press the Administration button to launch the default web browser on your system.

5. The Internet Services Administration web page is shown on the browser. Select WWW Administration to bring up the Internet Services Administrator-WWW page.

6. Select directories. A list of directories and aliases is displayed.

7. Add an alias for the EasyWeb html alias.

   a) Click the hyperlink Add under Action

   b) Enter the path of the installed Wishcom web pages (<install path>\EasyWeb\).

   c) Enter the alias name, for example, EasyWeb.

   d) Set the access mode to READ

8. If cgi-bin is defined in the directory list, copy the cgi files into this directory. Otherwise add the cgi-bin alias.

   a) Click the hyperlink Add under Action.

   b) Enter the path of the installed cgi-bin file (<install path>\EasyWeb\cgi-bin)

   c) Enter the alias name as cgi-bin.

   d) Set the access mode to Execute and Read

Restart your web server. You can access by the URL: http//<your web server name>/EasyWeb/login.htm.

3. Concepts and Principles of Operation

ExpressRoute 80 provides two types of communication services, namely, data communication services and voice communication services.

The data communication service enables the LAN users to access the Internet resources by a ISDN dial-up to an ISP, and access the corporate resources by the ISDN dial-up to the office.

The voice communication service enables users to place or receive phone calls using the ordinary analog telephone, modem, or fax machine.

In this chapter, three major topics : ISDN, Data Service, and voice service are discussed in details. This chapter also includes information about ISDN line provisioning, and the E80 operation principles in the area of Internet/Intranet profiles, and bandwidth management.

ISDN Overview

ISDN stands for Integrated Service Digital Network. The service is designed to deliver data, voice, video traffic in digital format. ISDN Basic Rate Interface (BRI) consists of 2B+D channels. The D channel at 16 KBPS is mainly used for ISDN signaling to establish or tear down the 2 bearer (B) channels. Each B channel operating at 64 KBPS is capable of delivering data or voice service. Although standardized by international standard body ITU, many countries and regions implement their ISDN network slightly different from each other. ExpressRoute is designed to support different ISDN switches for different countries and regions.

Physical Interface

The ISDN physical interface is a available in two types, U and S/T. The S/T interface relies on a external device called NT1 to connect the user equipment to the ISDN line. The S/T interface is used in most parts of the world. The U interface, widely used in North America, is designed for user equipment with built-in NT1. The NT1 (also called ISDN DSU) built-in ISDN device is also allowed In Japan. The Japanese U interface however works differently from the rest of the world.

ISDN Switch Variants

When your ExpressRoute is delivered, it is preset to use a default ISDN variant. The ISDN variant is the type of ISDN operation run by your Telephone company.

Interface Type	National ISDN Variants	Default Setting
U	North American	National ISDN
S/T	Japan	NTT
S/T	Rest of the World	EURO-ISDN

You must have the right ISDN variant (switch) configured as provided by your ISDN service provider or telephone company.

Directory numbers

A directory number is the address or telephone number for the ISDN line assigned by your ISDN service provider or telephone company. The number of directory numbers allocated depends on which Service Provider you are using. If you are using an NI-1 line, you will be assigned one directory number per B-channel. Otherwise, you will be assigned one directory number per device.

Service Profile Identifiers (SPIDs)

Note: Service Profile Identifiers are only allocated by Service Providers in North America.

When you order an ISDN service, your Service Provider needs to know which ISDN features you require, for example, Calling Line Identification (Caller ID). This is known as a service profile. Your service provider then allocates you a unique Service Profile Identifier (SPID) that allows you to use these particular features.

Depending on your ISDN variant, you will have none, one or two SPIDs assigned to your ISDN line as shown below.

ISDN Variant	Directory numbers	SPIDs
AT&T 5ESS P-P	1 (1 per device)	None
AT&T 5ESS M-P	2 (1 per B-channel)	2 (1 per B-channel)
NTI DMS	2 (1 per B-channel)	2 (1 per B-channel)
NI-1	2 (1 per B-channel)	2 (1 per B-channel)
NI-2	1 (1 per device)	1 (1 per device)
European	1 (1 per device)	None
1TR6	1 (1 per device)	None
NTT	1 (1 per device)	None
Austel (TS013)	1 (1 per device)	None

AT&T Point to Point ignores the Directory number from the user equipment, so you could be sending anything that will sync up, and it will place a call. One should leave the SPIDs blank while configure the E80 for AT&T Point to Point Switch. ATT Multi-point, NTI, and NI1 are very specific about DN directory Number and SPID numbers. If they are wrong, you cannot place a call.

56K/64K Rate Adaption

The Rate Adaptation of the line is the speed at which data can be transmitted over that line. This can be 64 KBPS or 56kbit/s. If you are connected to a European ISDN Service, always set the Rate Adaptation to 64 KBPS (the default value). If you are connected to a North American ISDN Service, always select 64 KBPS for local calls. You may need to select 56 KBPS for international or some inter-state calls. Some area in North America, dialing 1+10 digit is required in order to access the 64kbit/s. You should generally select 64 KBP in most part of the world.

ISDN Permanent (Nailed) Circuit

Most telephone companies offer only switched ISDN circuits. In. Germany leased line ISDN service is also offered as a option. German ISDN Permanent connection services (types 64S, S01 and S02) is available from Deutsche Telekom. This service provides a permanently open leased line with an ISDN interface at each end, which allows you to take advantage of Deutsche Telekom tariff rates.

Service type	Number of channels
64S	One B-channel
S01	One B- and one D-channel
S02	Two B- and one D-channel

Japan NTT also offers leased line ISDN service :

Service type	Number of channels
DA64	One B-channel
DA128	Two B channels

Data Communication Services

Two widely used inter-networking mechanisms are bridging and routing. Bridging offers a straightforward methods of interconnecting network segments. Bridges are simple to use. However, if you are bridging across a

WAN using ISDN, you can incur unnecessary costs from the ISDN bill. A more controllable way of moving data cross networks is by routing. For Internet access, TCP/IP is *the* routing protocol. For Intranet access, IPX, and bridging for other protocols (e.g. NETBIOS) may be needed occasionally.

Bridging

A bridge automatically learns addresses of all active stations on its Local Area Network (LAN). It examines all the packets on the LAN, reading their source and destination addresses, and does not forward those packets which are intended for a local destination, while forwarding all others across the WAN to the next LAN. This means that traffic which is intended only for the local segment does not cross the bridge. However, there are some packets which a bridge *must* forward across the WAN to all parts of the network, such as broadcasts, multicasts and packets with unknown destinations to the bridge. The broadcast and multicast transmission or transmission to an unknown destination may initiate an ISDN call. Every ISDN call costs money. Bridging is not recommended unless absolutely necessary.

Routing

Routing is moving user data traffic across the inter-network from source to destination based on the network layer address. Along the way, at least one intermediate router is typically encountered. Routing and bridging is designed to accomplish precisely the same purpose. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, while routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving user data from source to destination. There are several different kinds of routing in use, most widely used are IP, and IPX routing.

Internet and Intranet Connection Profiles

E80 maintains two connection profiles one for Internet and the other for Intranet. The Internet connection by definition is for users to reach Internet, the Intranet connection is made between two offices. The Internet profile contains the configuration parameters required by the Internet connection. The categories available under Internet profile are : ISDN, PPP, IP, and NAT. The Intranet profile contains the configuration parameters required by the Intranet connection. The categories available under the Intranet profile are ISDN, PPP, IP, IPX, and Bridge. NAT is intended for Internet only where security and ISP monthly charge is of concerned. The IPX and Bridging is only designed for Intranet where protocols other than IP may be required. Users should make sure not to configure conflicting information between these two profiles, such as setting the same remote IP address or ISDN dialing number to both profiles. These two types of connections are shown in Figure 3-1, Internet and Intranet Connections.
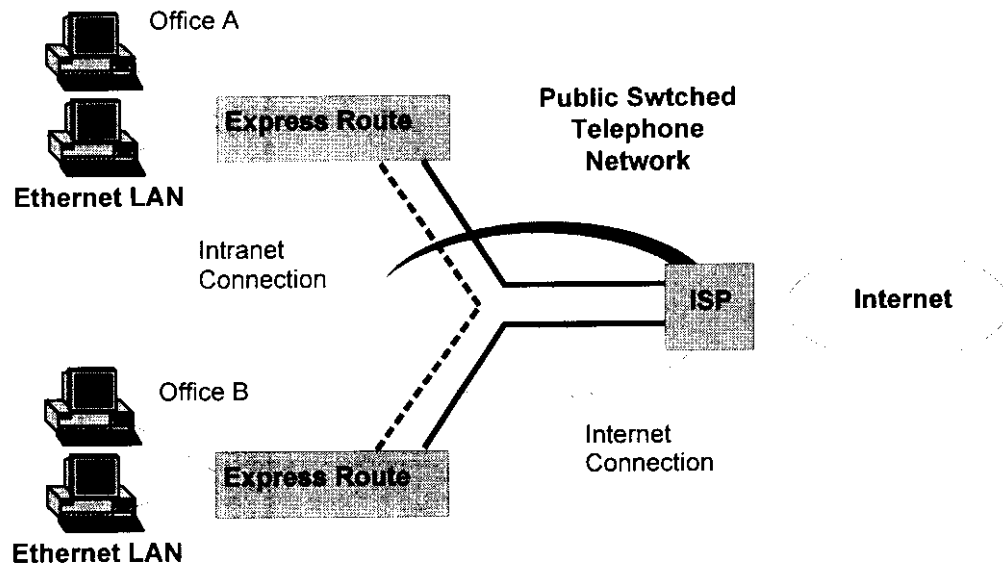
Figure 3-1, Internet and Intranet Connections

IP Address and Subnet Mask

The address which the IP routing bases on is the IP address. An IP Address is a 32-bit address which must be assigned to every host that wants to use IP to communicate across the Internet. If you are connecting to the Internet, in general the IP addresses of the computers and router are assigned from your Internet service provider unless Network Address Translation (NAT) is used which we will discuss later.

The IP address are specified in a.b.c.d where a,b,c,d are each decimal numbers between 0 and 255 with some restrictions applied. The ExpressRoute Ethernet IP address must be on the same network as your PCs on the LAN. A network can be subnetted into one or more physical networks which form a subset of the main network. The Subnet Mask is a number identifying a subnet within a network.

Routing Table

In order to move data from port to port, the router has to make routing decision based on the routing table. Each routing entry describes what network can be reached through which interface via a certain gateway.

Some routing entries are system creation based on the router interface configuration. Some routing entries may be created by users classified as static routes, and other may be created based on the information learned from the router protocol (eg. RIP). Static Routes is a cost-saving feature which avoids running RIP over WAN links. The active route is advertised by ExpressRoute via RIP (if enabled) on its LAN interface. For SOHO ISDN router, the default

route created by the system is automatically set toward Internet remote router. User need to enter static route entries only when there are multiple subnets at the Intranet remote end.

IP Address, Un-Numbered, or Numbered

You can set ExpressRoute IP addresses to be 'un-numbered' or 'numbered'. By setting it to "un-numbered", you can route IP over a link between two devices without assigning IP addresses to the ISDN interfaces. This allows you to save valuable IP address space. There are situation where traditional "numbered" IP address scheme is inevitable.

In Figure 3-2, Unnumbered ISDN Link, there is an unnumbered link between an ISDN router and a remote router at the ISP site. These two devices can still communicate with each other, although neither of the ISDN interfaces has been assigned an IP address. Instead, a route is assigned between a device and its destination network, using interfaces instead of IP addresses.

SOHO ISDN Router   unnumbered link   Remote Router at ISP

eth1   eth1
50.0.0.1   90.0.0.1
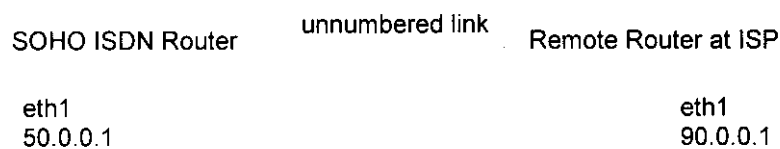
Figure 3-2, Unnumbered ISDN Link

InFigure 3-3, Numbered ISDN Link, there is an numbered link between an ISDN router and a remote router at the ISP site. An IP address is assigned at each end of the numbered link.
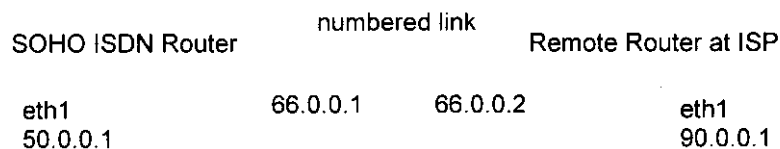
SOHO ISDN Router   numbered link   Remote Router at ISP

eth1   66.0.0.1   66.0.0.2   eth1
50.0.0.1   90.0.0.1

*Figure 3-3, Numbered ISDN Link*

Dynamic IP address Assignment

If you are subscrbing to a single user account, the ISP won't assign to you static (semi-permanent) IP address(es), instead, an IP address is dynamically assigned at the login time. E80 will accept the dynamically assigned IP address for its ISDN interface and update the routing table accordingly. The assigned IP address will be freed, and the associated routing table entry is

deleted when the session is closed. The NAT feature is required for multiple LAN users to access the Internet using the single IP account.

IPX

IPX is the protocol used by Novel Netware as the network layer protocol. Novel IPX also uses Routing Information Protocol (RIP) for routing protocol. The IPX address consists of two part: a 4-byte network number, and a 6- byte node number. Often time, the node number is assigned equivalently to the Ethernet MAC address. In a bridging environment, all Netware clients and servers share the same external network number. In a IPX routing environment, networks connected by IPX routers are assigned with unique IPX network numbers.

An IPX client wish to connect to a Netware server first sends a "find nearest server" request trying to locate a server. After servers response to the request, Netware client login process to the server may begin. If a Netware server is not locally connected to the client's network, the router connecting to the client's network is responsible for responding to the "find nearest server" request. A router such as E80 learns the existence of remote server by manual configuration, and through Service Advertising Protocol (SAP).

external network AA-AA-AA-AA   external network BB-BB-BB-BB
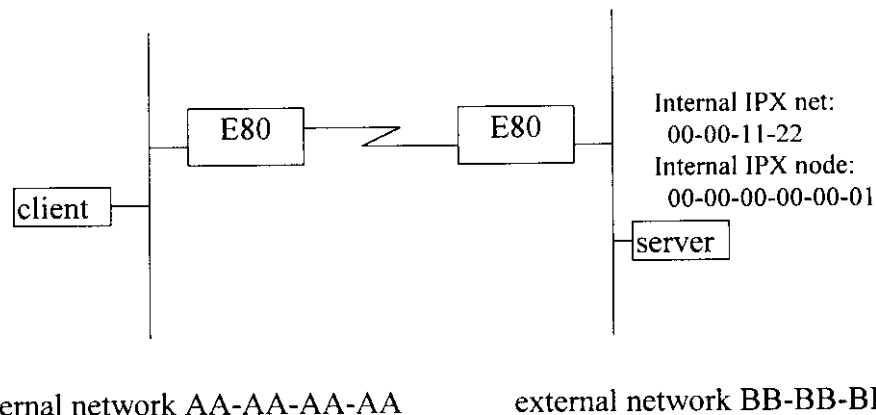
IPX Address

Netware 3.x and later use the notations of external IPX address and internal IPX IPX address. Any Netware device physically connected to a network have a external IPX address. A Netware server such as file server is also assigned with an internal IPX address. The internal address refers to the internal network within a server allowing internal processes to communicate. All external and internal addresses must be unique from one another.

IPX Frame Type

The IPX frames can be encoded in 4 frame types of the following formats:

Ethernet II (0x81,0x37,...),

802.3 (length, 0xFF, 0xFF,....),

802.2 (length, 0xE0, 0xE0, 0x03, 0xFF, 0xFF,......), and

SNAP (length, 0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37,...).

Among them, 802.3 and 802.2 are two most commonly used format. E80 routes only IPX traffic of certain frame type. Other frame type of IPX traffic may be bridged if so enabled.

RIP

Novel IPX also uses Routing Information Protocol (RIP) for routing protocol. Although it is similarly named to the IP equivalent, it uses a different protocol. IPX RIP broadcasts packets to the network every 60 second to inform other IPX routers or servers about the networkd it knows about. Upon receiving a IPX RIP packet, a router adds one to the hop count of each router advertised and broadcast a RIP packet to other networks it is connected to.

SAP

Netware Servers such as file servers use SAP protocol to advertize their service throughout the network. A router such as E80 listens to the SAP packets from servers to learn what services are available in the local network. Routers also exchange SAP packet so that the router learn what services are available at the remote networks. With that global knowledge, the router is able to respond the "find nearest server" request for the remote IPX networks.

IPX Spoofing

A Netware server regularly send a "keep alive" message to a once login client every 3-5 minutes for connectivity verification. If a client fails to respond within the allowed limit, the server closes the client's connection. The IPX "keep alive" packets tend to keep the dial-up connection on line. To minimize the un-necessary dial-up connection time, E80 equipped with IPX spoofing function will respond the "keep alive" on behalf of the remote Netware clients for a pre-configured period. A dial-up call may be triggered by the "keep alive" packets only after the spoofing timer expires.

PPP

The Point-to-Point Protocol (PPP) is the de-facto standard as the link encapsulation protocol for Internet Access. PPP consists of a suites of protocols including LCP, PAP, CHAP, IPCP and other related protocols. Link Control Protocol (LCP) is used to negotiate the link parameters, such as what authentication protocol to use. LCP is specified in RFC 1570. Password Authentication Protocol (PAP), and Challenge Authentication Protocol (CHAP) are used to inform the remote site (eg. ISP) about which router is connecting to it. CHAP and PAP are specified in RFC 1334. IPCP is used to negotiate IP specific parameters such IP address. IPCP is specified in RFC 1332.

PAP/CHAP

When an CHAP authentication connection to the ISP is attempted, the remote router or access server sends a CHAP packet to ExpressRoute. The CHAP packet "challenges" ExpressRoute to respond. The challenge packet consists of an ID, a random number, and the host name of the remote router. The required response consists of an encrypted version of the ID, a secret password, and the random number of the local name. When the remote router or access server receives the response, it verifies the secret password by performing the same encryption operation as indicated in the response and looking up the required host/user name. ExpressRoute and the remote router must agree on the identical secret passwords. By transmitting this response, the secret password is never transmitted in clear text, preventing other devices from stealing it and gaining illegal access to the system. Without the proper response, the remote will reject the PPP connection request.

If PAP authentication is enabled, attempting to connect to the ISP or remote router is required to send an authentication request including the user name and password. If the user name and password are accepted, the ISP or the remote router sends an authentication acknowledgment to conclude the authentication process.

you have choice of specifying two sets of authentication protocol and password. One set for Internet connection and one set for Intranet connections. Each set consists of two pairs of authentication configuration. The Dial-out authentication -password pair is applied to the PPP connection initiated by E80. The call-in authentication-password pair is applied to the PPP connection initiated from the remote end. The dial-out authentication protocol (none, PAP, CHAP) specifies the authentication protocol that E80 will insist on when initiating a PPP connection. The remote end is supposed to accept the specified authentication protocol for the PPP negotiation to proceed. The setting of "either" as the call-in authentication protocol allows E80 to negotiate for either PAP or CHAP authentication protocol whichever the remote end prefers.

Multilink PPP

The PPP Multilink Protocol (RFC 1717) is a standardized extension of the PPP (Point-to-Point Protocol) standard. It allows you to combine channels into a 'Multilink bundle' so that data can be sent at higher rates. Some Multilink PPP implementing a feature known as 'packet fragmentation' where larger individual packets are chopped into smaller fragments. These fragments are then distributed among two channels in use. The receiver at the other end of the links collects the fragments, reassembles them and delivers them in the original order.

Multilink PPP allows packet fragmentation over two B channels to reduce latency and speeds up transmission. The actual implementation of

fragmentation however demands significant CPU overhead. This overhead prevents most ISDN SOHO router vendors from doing the packet fragmentation, instead packets are distributed between two B channel in a round-robin fashion.
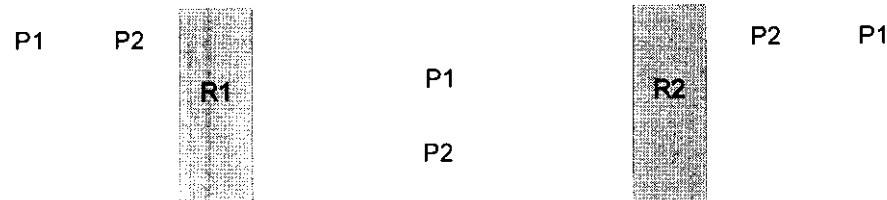

Figure 3-4, Packet transmission without fragmentation, round-robin

When packets are sent with fragmentation, the larger packets are chopped into two fragments of equal size and distributed from Router 1 to Router 2 over the two channels in use.
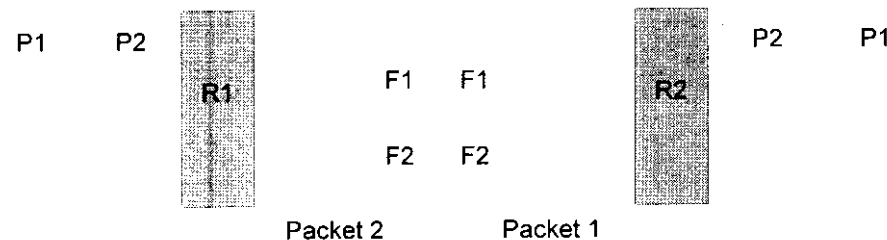

Figure 3-5, Packet transmission with fragmentation, chop-in-half

Not all ISDN router or access server accept packet fragmentation. To guarantee the compatibility, ExpressRoute sends packets in round-robin over the Multilink PPP. On the receiving direction. E80 accepts both round-robin, and fragmented packets. There is a possibility of packet out-of-sequence when sending and receiving packet in round-robin fashion, E80 will re-order the packets when compression is enabled. This will minimize the history reset request caused by the packet out-of-sequence. The diagram above illustrates how packet fragmentation changes the way packets are transmitted between two routes. When packets are send in round-robin , packets are sent whole across the B-channels.

Dial on Demand

When the ISDN router receives packets from Ethernet and decides to route packets to the WAN interface. An ISDN call is automatically made to the remote end, followed by the PPP negotiation. The PPP connection to remote router is triggered automatically by the LAN traffic without user intervention. On the other hand, when the traffic ride on the connection become idle for a

certain period, the ISDN router automatically release the ISDN/PPP connection.

Bandwidth on Demand

If Multilink PPP is enabled, the router will bring up the second B channel when the traffic ride on the first PPP channel pass beyond certain threshold for a certain period, as specified in "1->2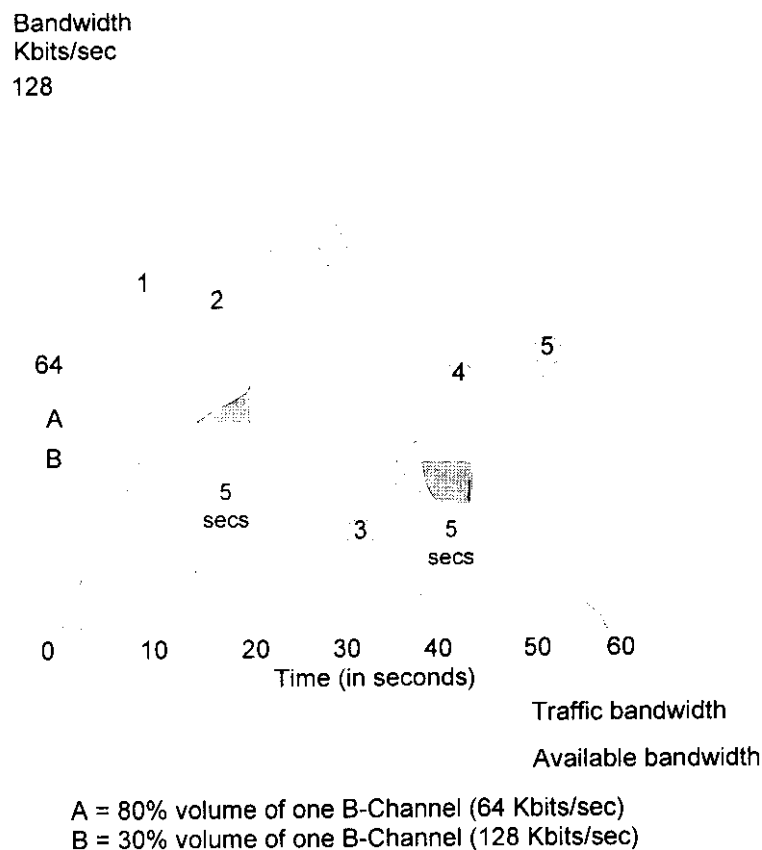 util" (increase from 1B to 2B), and "ave interval" (average) parameters. The router may also release the second B channel when the data traffic ride on the second channel has fallen below certain threshold for certain period, as specified in "2->1 util"(decrease from 2B to 1B), and "ave interval".

Bandwidth
Kbits/sec
128

1
2

5

64   4

A

B

5
secs   3   5
secs

0   10   20   30   40   50   60
Time (in seconds)

Traffic bandwidth

Available bandwidth

A = 80% volume of one B-Channel (64 Kbits/sec)
B = 30% volume of one B-Channel (128 Kbits/sec)

Figure 3-6, Bandwidth on Demand

Bandwidth on Demand occurs dynamically on an 'as needed' basis. Before you begin to set up Bandwidth on Demand parameters, you need to decide at what point you want the second B-channel to open. For example, you may want to open the second channel when the first is at 50% of its maximum throughput. You also need to work out how long you want traffic on the first B-channel to remain at this percentage level before the second channel opens up. The diagram above illustrates how Bandwidth on Demand works.

When an ISDN call is made, one B-channel is opened. Point 1 shows when data reaches the traffic load percentage value. This means that the volume of data has reached the percentage value that you have set on "1->2 util". You can configure ExpressRoute to wait for a set length of time before bringing the second B-channel into operation. In this case, data volume must exceed 80% volume for a certain length of time, as in "ave interval" before the second B-channel is opened. Point 2 marks the point at which data volume has exceeded the traffic load percentage value for five seconds. The second ISDN B-channel now opens automatically, and remains open until data volume drops below a configurable level as in parameter "2->1 util". Data is shared equally between the two B-channels. At point 3 in the diagram, traffic decreases temporarily before increasing again. Because bandwidth requirements can change suddenly like this, the second B-channel waits for a period of time before closing down. In the above diagram, this value has been set to 5 seconds. You can set this time to suit your own requirements.

At point 4, data drops below the lower traffic load percentage value. Because traffic volume must remain below this threshold for a certain length of time, the second B-channel does not close until point 5 (5 seconds later) has been reached.

Data Compression

Data compression allows the router to send and receive data more efficiently by compressing the data at sending and de-compress the data at receiving. When compression is enabled, ExpressRoute negotiates for STAC LZS compression scheme using the Compression Control Protocol (CCP). E80 supports both Ascend's pre-standard compression scheme, and the standard cimpression scheme as specified by ITEF. Depending on the actual data pattern, the STAC compression algorithm may accomplish the compression ratio of 4 against an ASCII file. No data compression can be gained against a file which has already been compressed. When working together with the Multilink PPP protocol, the compression algorithm does not function too well. The frequent packet out-of-sequence cause either end to requeset compression history reset.

Calling Line Identification (CLID)

Calling Line Identification (CLI) or Caller ID is a mechanism for identifying incoming calls. You may be able to order CLI from your telephone company as part of your ISDN Service. ExpressRoute allows one CLID for each Profile. In many circumstances, the incoming call indication signal does not include the Calling Line Identification (directory number) of the device which has just called you, or the Calling Line Identification (CLID) may not be passed to ExpressRoute. You may want to disable CLID authentication, instead, use the Challenge-Handshake Authentication Protocol (CHAP) for additional security if these circumstances apply.

Callback

Callback is available on ISDN circuits. It allows a router to request a return call from a remote router, meaning that when an incoming call is received on a circuit, the router drops that call and calls back the originating router. This feature allows you to take advantage of any differences in call charges and obtain centralized billing. Callback also provides additional security.

There are two scenarios of Callback operation:

1. Caller ID (CLID)
    When a call arrives ExpressRoute which is configured to accept Callback requests with the CLID enabled, ExpressRoute checks if the CLID matches as configured. If a match is found, ExpressRoute rejects the incoming SETUP message and calls back the originator using the number presented by Caller ID. This method means that there is either no charge or a minimal call setup charge (service provider dependent) to the originator. If the originator is not configured to request Callback but the receiving circuit is configured to call back the originator, then when a call arrives it will still be called back. If the originator is configured to request Callback but the receiving end is not configured to call back, the receiving end will accept the call and the originator will pay the cost of the call.

2. PPP
    If CLID is disabled as configured in ExpressRoute, a call is accepted by the Listener circuit then Callback is negotiated using PPP authentication. This method will mean a small cost is incurred at the originating end since the call has to be accepted before Callback is negotiated. If the PPP negotiation fails then the call is dropped as usual.

IP Packet Filtering, IP Access List

To provide an additional level of security once the connection is established, ExpressRoute allows users to configure access lists against the IP traffic. The access list specifies what kind of data packets are to be filtered or forwarded. Without access list being specified, all valid packets will be forwarded. You can specify in the IP access list the following criteria: source IP address, destination IP address, source port number, destination port number, and the protocol which when matched will be forwarded or filtered.

The IP packet filters specify IP packet-screening criteria used to filter IP traffic. You can create up to 8 IP packet filters through E80NMS. For every received IP packet, not destined for the router itself, E80 checks the packet content against the existing IP packet filters one by one. If any one of the filters *describes* (i.e. matches) the received packet, the action "accept" (i.e. forward) or "deny" (i.e. discard) associated with the filter is applied to the packet. Otherwise, the packet is forwarded by default.

A IP packet filter specifies and checks the following 4 attributes:
1. IP source address (IP address mask, IP address)
2. IP destination address (IP address mask, IP address)
3. Protocol
4. Port number

An IP packet filter *describes* an IP packet if **all** 4 attributes are evaluated match against the received IP packet. The associated action will be applied to the *described* packets.

IP source address, IP destination address

The following logic is evaluated against both IP source and destination address.
The packet's IP address is first AND-ed with the IP address mask specified in the filter. This attribute is considered match if the AND-operation result equals to the IP address specified in the filter.

For example,
An IP destination address attribute with
    Destination IP mask = 255.255.255.255, and
    Destination IP address = 192.31.7.130
Will match all IP packets with destination IP address = 192.31.7.130.

An IP source address attribute with
    Source IP mask = 255.255.255.0, and
    Source IP address = 192.168.16.0
Will match all IP packets with source IP address = 192.168.16.0 ~ 192.168.16.255.

Protocol

The protocol here means some of the well-known TCP/IP transport layer protocols such as ICMP used by "ping", TCP used by FTP, WWW, and UDP used by SNMP. This attribute is considered match if the protocol specified in the filter equals to the protocol field carried by the received IP packet. If the protocol=none, then attribute protocol is automatically match.

Port Number

Port Number here means the transport layers port number. This attribute is considered match if the port number specified in the filter equals to the source port number of destination port number carried in the received IP packet. If the port number = 0, then attribute port number is automatically match.

NAT

The ISP generally offers two type of accounts to SOHO users. The Single User account, and the LAN Access (Multiple Users) account. The Single User account is often referred as Terminal Adapter or Modem account where single user Internet access is assumed. The LAN Access account cost more than the Single User account because multiple IP addresses are assigned. Network Translation (NAT) is designed to allow multiple users on the LAN to access Internet simultaneously using the Single User account. In addition to cost saving, NAT also useful in areas in which security or convenience are a concern. It is convenient in the sense that, the users don't have to change the private legacy IP addressed already in use.

In order for the outside world to access the TCP/IP servers on the LAN, ExpressRoute allow a list of internal IP addresses to be associated with FTP, Telnet, HTTP, and Email servers. Traffic destined for the list servers are forwarded to the specified IP addresses. The inbound traffic distribution works only for static IP address arrangement where you can register an IP address against the domain names. You don't have a IP address to register or publish when access the Internet through the "single-user" account.

There are some limitation on the NAT application :

1. If the ISDN connection drops (e.g., because of an idle time-out), most likely that upon reconnection you will get a different IP address assigned. For example, if you are using a web browser and the connection drops because you go idle, if you then click on a link, you might get an error message because you now have a different IP address.

2. Certain applications, like some UDP-based Internet game and chat client programs, will work unreliably or not at all when using NAT because they report their private IP address to the server instead of the "correct" dynamically assigned address. The remote application while sending UDP packets toward the private IP address are not able deliverable.

NAT is available to Internet connection only. The Intranet connection is not affected by the Internet NAT setting.

DHCP

Managing IP addresses in an organization is often a headache for the MIS staffs. To ease the IP address management, the Dynamic Host Configuration Protocol (DHCP) is invented by IETF. DHCP protocol works in a client server configuration. One or more DHCP servers may be installed in the network. A workstation running DHCP client software (eg. Windows 95), when configured to request it IP address from the network, will send a DHCP request to the network asking for IP address assignment. In addition to assigning the IP address, the DHCP server can also provide other TCP/IP

configuration data such as IP sub-net mask, default gateway IP address, DNS server IP address(s). E80 with DHCP enabled functions as a DHCP server.

Voice Communication Service

Voice Preemption

If you pick up a phone while a 2-channel data call (Multilink PPP bundle) is active, ExpressRoute drops one of its data links to service the voice call unless the preemption is configured as disabled. An AT&T 5ESS switch limitation prevents users of AT&T Customer Multi-point or Point-to-Point service from receiving voice calls, when both data channels are in use. Outgoing calls are not affected by this switch limitation, because they are controlled locally at ExpressRoute. If you are using AT&T Multi-point or Point-to-Point service, and you want to make sure that voice calls are received, you should configure the link encapsulation protocol to PPP for both Internet and Intranet profile. However, this limits the ExpressRoute to 1-channel data calls, so each data call can handle a maximum of 64 kbps. The voice call will not be accepted if there is two 1-channel data calls in active.

Basic Rate ISDN Provisioning for United States and Canada

Introduction

This document outlines the steps required to successfully order the correct BRI ISDN service from your service provider for ExpressRoute.

Wishcom Line Provisioning Service

Wishcom line provisioning service can supply the ISDN provisioning information you require. This information is available at the following number (US and Canada only):

1-408-867-2045

Ordering the ISDN Line

You can order many different variants of ISDN. To ensure that you get the correct variant for ExpressRoute, you need to give your service provider certain information. In return, they will tell you the correct parameters to use when configuring ExpressRoute.

You must tell your service provider how you need the line provisioned for data, voice and other optional services.

Your service provider needs to tell you:

- the ISDN service and switch type

- the ISDN directory (or phone) numbers

- associated Service Profile Identifiers (SPIDs) (if required).

ISDN Switches and Services Supported

Wishcom ExpressRoute supports the most common switch types used in Northern America:

- AT&T 5ESS

- Northern Telecom DMS-100

ExpressRoute is also compatible with the National ISDN service offered through ,AT&T, Northern Telecom switches.

There are different ISDN services available on these switches. ExpressRoute supports the following services:Switch type	ISDN Service
AT&T 5ESS	Custom Point-to-Point
AT&T 5ESS	Custom Point-to-Multipoint
NT DMS-100	Custome Point-to-Multipoint
AT&T 5ESS	National ISDN 1 (NI-1)
AT&T 5ESS	National ISDN 2 (NI-2)
NT DMS-100	National ISDN 1 (NI-1)
NT DMS-100	National ISDN 2 (NI-2)

Provisioning the ISDN Line

To make sure that you get the correct ISDN service for ExpressRoute, you must tell your service provider how you need the ISDN line provisioned. This means whether you want data, voice or a combination of the two, what extra services you need and, possibly what terminal type you require.

Different service providers require this information in different ways; increasingly they are using ISDN Order Codes for simplicity, but some still require specific switch type details.

Using ISDN Order Codes

Placing an order for ISDN has been greatly simplified recently for National ISDN (NI-1 and NI-2) services by the use of ISDN Order Codes (IOC). This allows you

to order a specific service by simply quoting an order code rather than having to use a lot of complex subscription parameters.

There are three ways of ordering ISDN using these ISDN Order Codes:

- Capability Packages

  Note: ExpressRoute complies with Capability S.

- Solution Sets

- EZ-ISDN

Note: ExpressRoute complies with and is registered against EZ ISDN-1.

There are a number of other IOCs that can be used when ordering ISDN for ExpressRoute. They may not all be available in your area and you may need to check this with your service provider.

Capability Packages

The following list shows the Capability Packages that are appropriate for ExpressRoute.

Note: The Order Code used will depend on the data and voice services required; ExpressRoute will not necessarily exploit all the features of a given service.

Capability Package	ISDN Service
B	Only provides data on one B channel. Includes CLI (Calling Line Identification or Caller ID).
C	Provides alternate voice/data on one B channel. Includes CLI.
G	Includes voice on one B channel and data on the other B channel. Includes CLI and Additional Call Offering (ACO).
I	Includes data on two B channels. No voice capability provided.
J	Includes alternate voice/data on one B channel and data on the other B channel. CLI is included.
K	This is the same as J but also includes ACO for the voice.
M*	Includes alternate voice/data on two B channels. Includes CLI.
R	Almost the same as I except that two directory numbers are assigned. With package I, one or two directory numbers may be assigned depending on the central site switch.
S*	Almost the same as M but always with two directory numbers. Includes CLI. (This service complies with and is registered against EZ-ISDN 1.)
U*	Includes alternate voice/data on two B channels. Includes CLI and ACO.
V*	Includes alternate voice/data on two B channels. Includes CLI and ACO.

Those Capability Packages marked with a * are the recommended codes to use, if available. You will get the most functionality from your ExpressRoute through these services.

Solution Sets

Solution Sets have been created to correspond to a particular customer application. The Solution Sets appropriate to ExpressRoute are:

Solution Set	ISDN Service
Work at Home 3a	Provides voice on one B channel and data on the other B channel. Includes ACO and CLI (Caller ID).
Work at Home 4a	Provides voice/data on one B channel and data on the other B channel. ACO and CLI are included.
Desktop Collaboration 2a	Includes voice/data on one B channel and data on the other B channel. ACO and CLI are included

EZ-ISDN

EZ-ISDN codes mirror some of the Capability Packages described previously. They are another method of ordering the correct ISDN service.

In addition, to simplify the process of provisioning an ISDN line, ExpressRoute complies with and is registered against EZ ISDN-1. You should ask your ISDN service provider for EZ ISDN-1 provisioning. ExpressRoute conforms to Bellcore requirements for connection to National ISDN-1 services. If EZ-ISDN is not selectable, ExpressRoute also works fine with Intel-Blue provisioning.

Using Specific Switch Parameters

Your service provider may require specific details about the parameters for the switch you are connected to. The parameters will depend on the service you are selecting. The following information provides the switch settings that are appropriate for ExpressRoute connectivity.

AT&T 5ESS Custom

Switch Feature	Value
Term Type	A
Call Appearances	1
CSV	1 per Directory Number
CSV Limit	2
CSD	1 per Directory Number
CSD Limit	2

National ISDN 1 & National ISDN 2

For National ISDN 1, you receive two Directory numbers and, as a result, some of the switch features are per Directory Number. For National ISDN 2 you get one Directory Number.

Switch Feature	Value
Term Type	A
CSV	1
CSV Limit	2
CSD	2
CSD Limit	2
CSV Notification Busy Limit	1
CSD Notification Busy Limit	1
EKTS	No
ACO	Yes

Supplementary Services

There are some common supplementary data services that are applicable to ExpressRoute, namely:

- Calling Line Identification or Caller ID
- Multiple Subscriber Numbering (MSN)

Calling Line Identification (CLI) or Caller ID

CLI provides the caller's telephone number when you receive a call. This information is provided by the network and not the caller and so can be used as a security measure to identify calls to be accepted and rejected.

You should order CLI if available.

Multiple Subscriber Numbering (MSN)

MSN allows multiple telephone numbers to be assigned to a single BRI connection. This allows you to assign specific numbers to specific devices.

For ExpressRoute, there will be one LAN connected and one or two analog devices (e.g. telephone, fax). It is possible to give each device a separate number through multiple subscriber numbering, allowing calls to be routed to the correct analog device. This will also depend on the service you are connected to.

When connecting to AT&T 5ESS Custom, you are provided with one telephone number (directory number). If you only need to connect one analog device (say a telephone) then one number is all that is required, but if you have two analog devices then you will need to subscribe to MSN. This will allow you to differentiate between the two analog devices and direct calls to the correct device.

When connecting to National ISDN 1, you are provided with two telephone numbers (directory numbers). ExpressRoute can differentiate between voice and data calls. This means one telephone number can be assigned to, say, the telephone (and the call will be directed to the correct device automatically) and the other directory number assigned to, say, the fax machine. There is no requirement for extra MSN service in this case.

Terminal Types

When connecting to an AT&T switch, you may need to specify a terminal type to the service provider as part of the ISDN provisioning. This is a letter that defines the type of device you are connecting to. For ExpressRoute the correct Terminal Type is **A.**

Information from your Service Provider - Directory numbers and SPIDs

In return for providing the ordering information, your service provider will provide you with Directory Number(s) and SPID(s). SPIDs are not provided for the AT&T Custom service.

A **Directory Number** is simply the address or ISDN telephone number for the ISDN line assigned by the service provider. Each ISDN line receives (at least) one telephone number, called the **Primary Directory Number**. Depending on the service offered by your service provider, you may also have a second directory number.

Your service provider will provide you with the **Service Profile Identifiers (SPIDs)**. These are associated with the service you have ordered and you must use these as part of the configuration for ExpressRoute before any ISDN connections can be made (except for AT&T Custom). The SPID is similar to the ISDN telephone number and its format is unimportant so long as the information is entered correctly when configuring ExpressRoute.

If you subscribe to NI-1 you will get two directory numbers and two SPIDs. If you subscribe to NI-2 you will get one directory number and one SPID.

More Information

You can get more information on ISDN provisioning from the following Web sites:

* http://www.bellcore.com/ISDN/index.html (Bellcore's ISDN home page)

* http://alumni.caltech.edu/~dank/isdn (Dan Kegel's home page)

For more information on ISDN (including ISDN provisioning), consult the following book:

* ISDN for Dummies by David Angell, published by IDG Books. ISBN 1-56884-331-3.

4. Configuration and Management

Introduction

The E80 ISDN router can be managed via three means :

1. NMS Windows Program

2. Web Browser

3. ASCII Console

NMS is a Windows application program running on Windows 3.1, Windows 95, and Windows NT platforms. Among the above management tools, NMS delivers the richest set of functionality in managing the E80 ISDN router. NMS consists of two applications : the SNMP management, and the SNMP monitor (ClearMon). The SNMP management is used to configure the ISDN router, and SNMP monitor is used to monitor the LAN, ISDN channel activities, and events.

Most PCs nowadays have the web browser installed. Their popularity makes E80 ISDN router virtually manageable from any PC workstation. When managed by a web browser, the HTTP requests from a web browser are delivered to a software module called EasyWeb, which translates the HTTP requests into SNMP requests and forwards them to the E80 ISDN router. The ISDN router returns the SNMP responses to the EasyWeb which in turn translates them back into HTTP responses and forwards them back to the browser.

Console offers the most fundamental user interface for the router management. The E80 displays the ASCII based menu on a console, or on PC running console emulation program. The console management focuses on the most basic management information such as "Quick Conf" for Internet access, and Ethernet/ISDN statistical data.

Because it is the most feature rich and the easiest to use, the NMS alternative is clearly the recommended choice for configuring and managing the E80 ISDN Router. For this reason, this chapter is mostly devoted to this alternative. Descriptions of the other two alternative, however are also included.

NMS

General NMS Menu Structure

Once logged in, the main menu shows up with a title bar "Wishcom SNMP Manager" at the top, system utilities (File, Diagnostic, Product info, View, Help) below it, and rest is the main body of the main menu. The main body is organized into two levels. The top level menu contains six items:Quick Config, Local, Internet, Intranet, SNMP, and Statistics. Each top level menu contains one or more bottom level items. The rest of the main body shows the contents of the active sub-menu which is determined by the top level menu item, and the bottom level menu item.

The NMS menus are organized into a hierarchical structure shown in Figure 4-1, NMS Menu Structure:

Login

Quick Config	Local	Internet	Intranet	SNMP	Statistics
Internet	Ethernet	ISDN	ISDN	SNMP	ISDN
	ISDN	PPP	PPP		Ethernet
	IP	IP	IP		Trace
		NAT	IPX		
			Bridge		
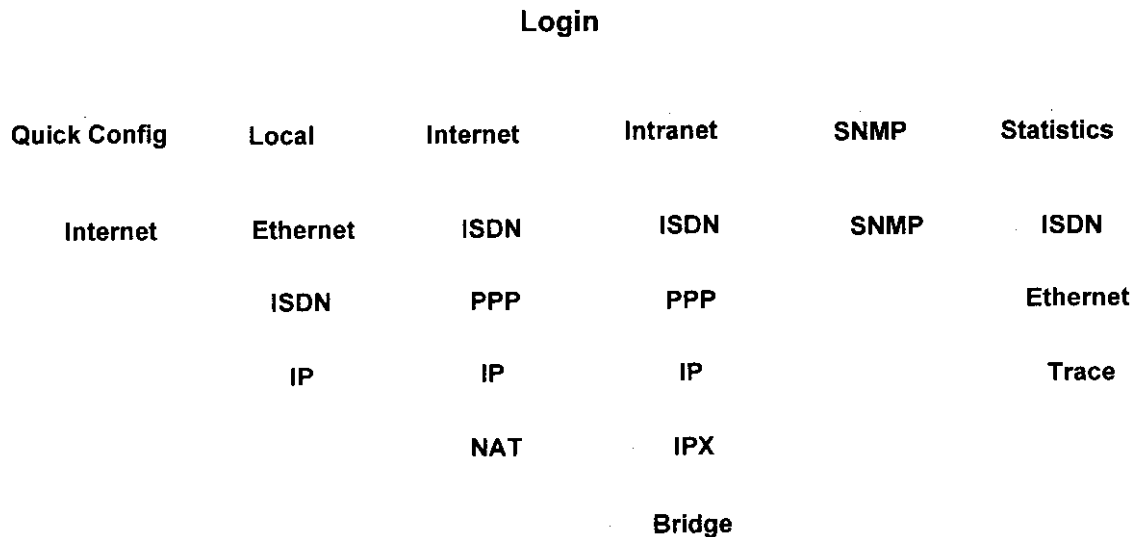
Figure 4-1, NMS Menu Structure

The "Quick Config" menu provides a quick and easy way for users to configure the ISDN router for Internet Access. For straightforward Internet access, this menu is probably the only menu that is required. For more advanced configuration, the "Local", "Internet", and "Intranet" menu can be handy. The "Local" menu is for configuration of the router itself. The "Internet" menu is for configuring specifics of the Internet connection, and the "Intranet" menu is for configuring specifics of the Intranet connection. The "SNMP" is used to set a basic MIB II system, MIB parameters and destination to where the traps will be delivered when enabled. The "Statistics" menu provides a very useful tool for monitoring the router operation and for troubling shooting.

In addition to the menus described above, there are a number of system utilities providing services such as up/down loading of router configuration file, updating

router firmware, resetting the device, disconnecting Internet/Intranet, and help information.

NMS Windows

NMS displays use the Windows 3.1, Windows95/NT conventions for windows management such as positioning, sizing, and closing windows.

A tab for each top menu is displayed across the top of all windows. Clicking one of these tabs displays the window for that top-menu. In each top menu window, tabs for each of the top menu's sub-menus are displayed. Clicking a sub-menu tab, displays the window for that sub-menu.

Each sub-menu windows displays the parameters that can be selected or entered in the form of fields displayed within the window.

Figure 4-2, Example Sub-menu Window shows the window for the Internet sub-menu under the Quick Config main window. This is indicated by the bold lettering of the Quick Config main menu tab and the Internet sub-menu tab.
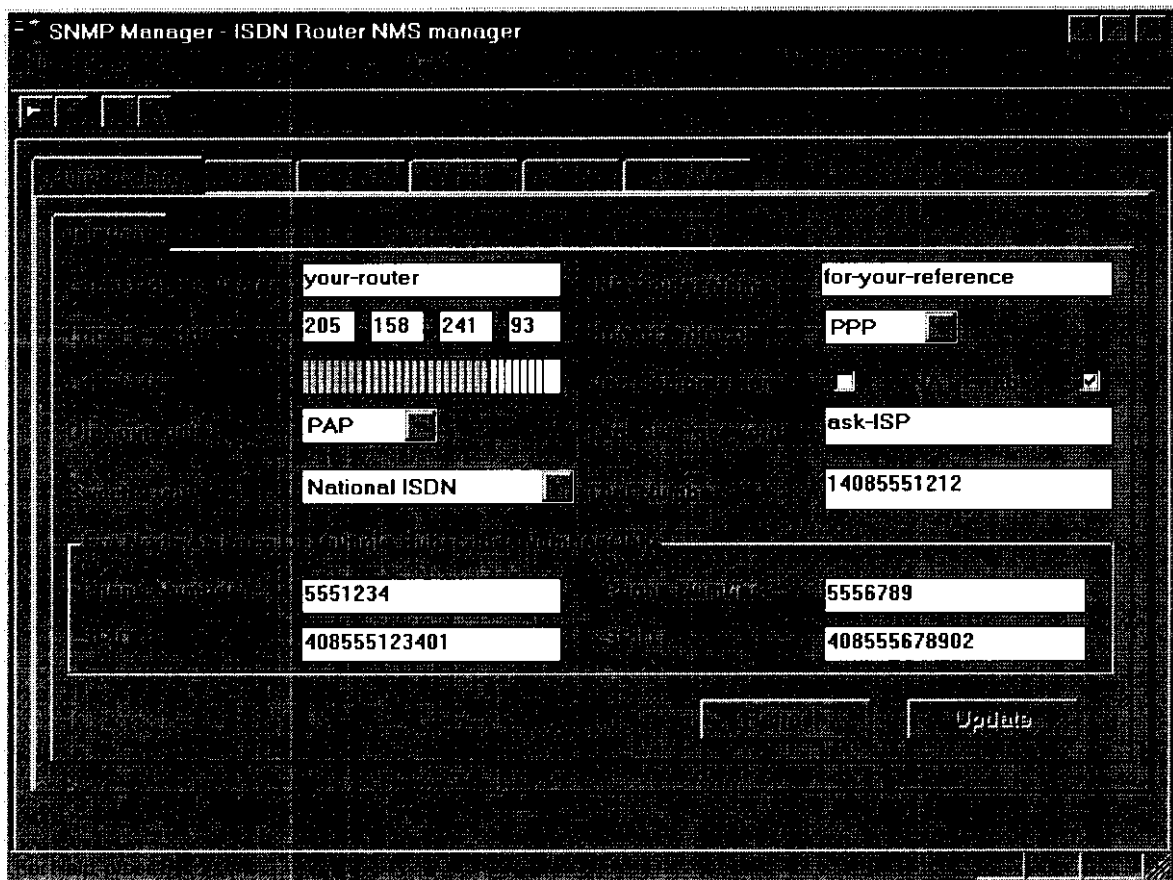
Figure 4-2, Example Sub-menu Window

Clicking in a field selects the field for entering a value. The selected field is indicated by a blinking insertion point (vertical bar). The Tab key can be used to tab to the next field and the Shift-Tab keys can be used to tab to the previous field.

When entering a value, the normal word processing functions of delete, backspace, etc. apply. Pressing the Enter key signifies that the entry is complete. In many instances, entering an invalid entry (for example, an invalid IP address) will cause the entry to be rejected with an error message.

Some fields require the selection of an item from a menu. These fields are indicated by a down pointing triangle to the right of the field. In the example, the Encap Protocol is such a field. Clicking on these fields causes a drop down menu to appear. The user must select an item from the menu by clicking it with the mouse.

Some field are indicated by small round buttons (called radio buttons). In these fields, the user makes a selection by clicking on a radio button. In the example, Data Service has two radio buttons, namely, 56K and 64K. Only one radio button can be selected at a time.

Each screen includes a Refresh button and an Update button. The Refresh button is used to restore all the values in the fields to those when the window was opened. The Update button is used when the displayed field values are correct and the values are to be stored in the E80.

NMS System Menus

In addition to the NMS menus, which are indicated by the tabs along the top of the displays, there are five System Menus which are listed along the very top of the window. These menus are File, Diagnostic, Product Info., View and Help.

The **File** menu consists of:
> Save Config
> Load Config
> Download Config to Device
> Reset Config
> Load Code
> Recent Files
> Exit.

The "Save Config" is used to save the router configuration to a file, which may be restored to at the later time. The "Load Config" is used to restore the saved configuration file to the NMS and optionally to the router. If you choose not to restore the configuration directly to the router, you can do it with "Download Configuration to Device". The "Reset Config" is used to reset the router configuration to its manufacturer default values. Finally in this category, the "Load Code" is used to perform the TFTP firmware update. Please use "Reset Config" and "Load Code" with care. The NMS will pop you a warning dialog box for confirmation.

The **Diagnostic** menu consists of:
> Ping
> Reset Device

Disconnect Internet
Disconnect Intranet

The "Ping" utility is use to send ICMP messages to a destination station for connectivity check. The "Reset Device" is used to reset the ISDN router. The "Disconnect Internet" is used to manually terminate the Internet connection. And the "Disconnect Intranet" is used to manually terminate the Intranet connection.

The Product Info. menu displays a window showing the version and release of the NMS product.

The View menu includes items for turning the Toolbar and Statusbar on and off.

The Help menu includes:

Index for accessing specific help topics

Using Help for information about the help system

About NMS for version and release information about NMS.

NMS Toolbar

NMS also includes a toolbar of four items which are displayed as four icons at the top right of the display.

Figure 4-3, NMS Toolbar

From left to right, these tools are:

• Open a file

• Save as

• About NMS

• Context sensitive help. Clicking this tool causes the mouse arrow to appear as a question mark. The user can position the question mark over a field and click the mouse to get help information about that field.

Required Information

Before configuring the E80, certain information must be available. Some of these information will be provided by the telephone company supplying the ISDN line (the ISDN provider), some will be provided by the Internet Service Provider (ISP) and some by the local system administrator. The following table shows the information that must be available.

Description	Source	Required or Optional
Local Router Name	ISP/MIS	Required
Local IP Address	ISP/MIS	Required
Remote Router Name	ISP/MIS	Optional
Remote IP Address	ISP/MIS	Optional
Local IP Mask	ISP/MIS	Required
Remote IP Mask	ISP/MIS	Optional
Remote ISDN Number	ISP	Required
ISDN Switch Type	Telephone Company	Required
Phone Number 1	Telephone Company	switch dependent
Phone Number 2	Telephone Company	switch dependent
SPID 1	Telephone Company	switch dependent
SPID 2	Telephone Company	switch dependent
Dial-out Password	ISP/MIS	Required
Call-in Password	ISP/MIS	Optional

Starting NMS

In Windows 95/NT, NMS is started by clicking Start/Programs/Wishcom NMS.

In Windows 3.1, NMS is started by clicking the NMS icon in the NMS window.

Logging Into NMS

The login dialog box (shown in Figure 4-4 Login Dialog Box) pops up when you start the NMS program. The login dialog box serves two purposes : It lets you enter the IP address to select a specific E80 ISDN router to manage, it also lets you assign the IP address to an E80 ISDN router by clicking the associated check box. This convenient way of assigning an IP address to the router does not require you to enter the IP address through the console. If you assign an IP address to the E80 ISDN router through the login dialog box, the E80 will reset itself after receiving the IP address assignment request. The assigned IP address will be stored in the non-volatile RAM. The login dialog box will wait about 10 seconds giving the router ample time to reset itself before polling the configuration data from E80 and show you the main menu shown in next page.

There should be only one active ExpressRoute E80 router on the Ethernet when performing the IP address assignment through the Login dialog box. If there is more than one E80 on the LAN, power-down or detach from the LAN temporarily all the E80 routers except the one that is having its IP address assigned. Restore the other E80s when the IP address has been assigned.

Once you have successfully assigned the IP address to the router, you should not click the "assign IP address" check box again next time you run the NMS program unless you want to change the router's IP address.
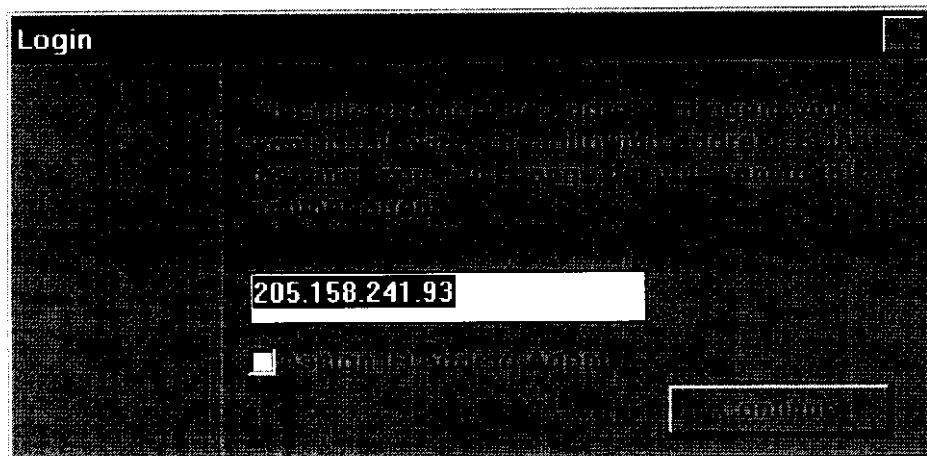
Figure 4-4 Login Dialog Box

Quick Configuration Menu

The Quick Config (see Figure 4-5, Quick Config Menu) is the first menu you will see after completing the login dialog box.

There is only one sub-menu, Internet, for Quick Configuration menu.

If you have successfully logged into the router, you should see most fields in this page containing data; if this is not the case, it indicates communication problems between NMS and the E80. See diagnostics hints in Chapter 5 if you run into such a problem.

For most users, the "Quick Config" menu is the only menu required to be entered for normal Internet Access. The other menus such as "Local", and "Statistics" are useful for diagnostics and advanced management purposes.

Local Router Name

The local router name is the name assigned to this ISDN router. Any text character is acceptable up to 32 characters. The local router name is required by ISP whenever you dial into your ISP's point of presence as part of the authentication procedure. It is assigned to you by your ISP. Upper case or lower case characters are significant for this field.

ISP Router Name

The remote router name is the name assigned to the remote router located at your ISP site. Any text character is acceptable for up to 20 characters. The remote router name is used during the call-in authentication process, and is not required

when you want to dial into your ISP's point of presence. In general, your ISP assigns to you a remote router name for administration and reference purpose.

Figure 4-5, Quick Config Menu

Local IP Address

The local IP address is the IP address assigned to this router. The IP address is entered in the standard IP address format of a.b.c.d. The local IP address is required during the PPP negotiation. Please ask your ISP if you don't possess one.

You would need to reset the router if this field get changed.

Local IP Mask

The local IP mask is used to describe the local IP sub-netting. The IP mask is entered by clicking the IP address bit map. The number of bit assigned for the IP subnet is shown next to the IP address bit map as a decimal number for your reference. You would need to reset the router if this field get changed.

Dial (ISDN) number

The remote ISDN number is the ISP's ISDN number you want to dial to gain access to the Internet. Your ISP will provide you a list of ISDN numbers for you to choose from. In North America, the dialing of a '1' followed by 10 digits is required in order to access the clean 64K BPS ISDN B channel(s). There should be only digits in this field, no space or other terminators are acceptable.

Encapsulation Protocol

The encapsulation protocol specifies the protocol you want to run over the data channel. Select PPP, if you want to run single channel PPP. Select MLPPP, if you want two channel PPP.

Compression

The compression field specifies if the Stac compression protocol will be turned on for the Internet connection.

Network Address Translation Enable

This field enables or disables the NAT function. This configuration becomes effective immediately after setting.

Dial-out Authentication

The dial-out authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when you initiate an ISDN call to your ISP. Most ISPs support PAP and CHAP protocols.

Dial-out Password

The dial-out password specifies the password to use during the dial-out authentication process. This field is case sensitive, and is given to you by your ISP.

ISDN Switch Type

The ISDN switch type specifies the switch type of the ISDN switch to which your ISDN line is connected. Please pull down the switch-type box, and select the one right for your ISDN line. The ISDN switch type has to be correctly selected in order for your ISDN router to synchronize with the telephone company's ISDN switch. Please check your local phone company for the exact switch type. In Northern America, the dominated switch type is National ISDN-1 (NI-1). For the rest of the world, the dominated switch type is EuroISDN (ETSI). You would need to reset the router if this field get changed.

Phone Number 1

In Northern America, the local phone company assigns two phone numbers for each ISDN line. This field specifies the first assigned phone number. This field is ignored outside Northern America. You would need to reset the router if this field get changed.

Phone Number 2

In Northern America, the local phone company assigns two phone numbers for each ISDN line. This field specifies the second assigned phone number. This field is ignored outside Northern America. You would need to reset the router if this field get changed.

SPID 1

In Northern America, the local phone company assigns two SPIDs for each ISDN line. This field specifies the first assigned SPID. This field is ignored for users outside Northern America.

The SPIDs, when given, come in different form usually in the format of prefix + phone number + suffix. Please ask your local company for the exact assignment. You would need to reset the router if this field get changed.

SPID 2

In Northern America, the local phone company assigns two SPIDs for each ISDN line. This field specifies the second assigned SPID. This field is ignored for users outside Northern America.

The SPIDs when given come in different form usually in the format of prefix + phone number + suffix. Please ask your local company for the exact assignment.

You would need to reset the router if this field get changed.

Dial-out Authentication

The dial-out authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when you initiate an ISDN call to your ISP. Most ISPs support PAP and CHAP protocols.

Dial-out Password

The dial-out password specifies the password to use during the dial-out authentication process. This field is case sensitive, and is given to you by your ISP.

Call-in Authentication

The call-in authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when the ISP initiates an ISDN call to you. In real operation, your ISP will not initiate a call to you.

Call-in Password

The call-in password specifies the password to use during the call-in authentication process. This field is case sensitive.

Local Menu

The local configuration contains the detailed local configuration information of this router. Under the local configuration, there are three sub-menus : Ethernet, ISDN, IP, and DHCP (server).

Local Ethernet Sub-menu

This Ethernet menu describes the Ethernet aspects of the local configuration. Some of the fields are linked to the menu "Quick Config".
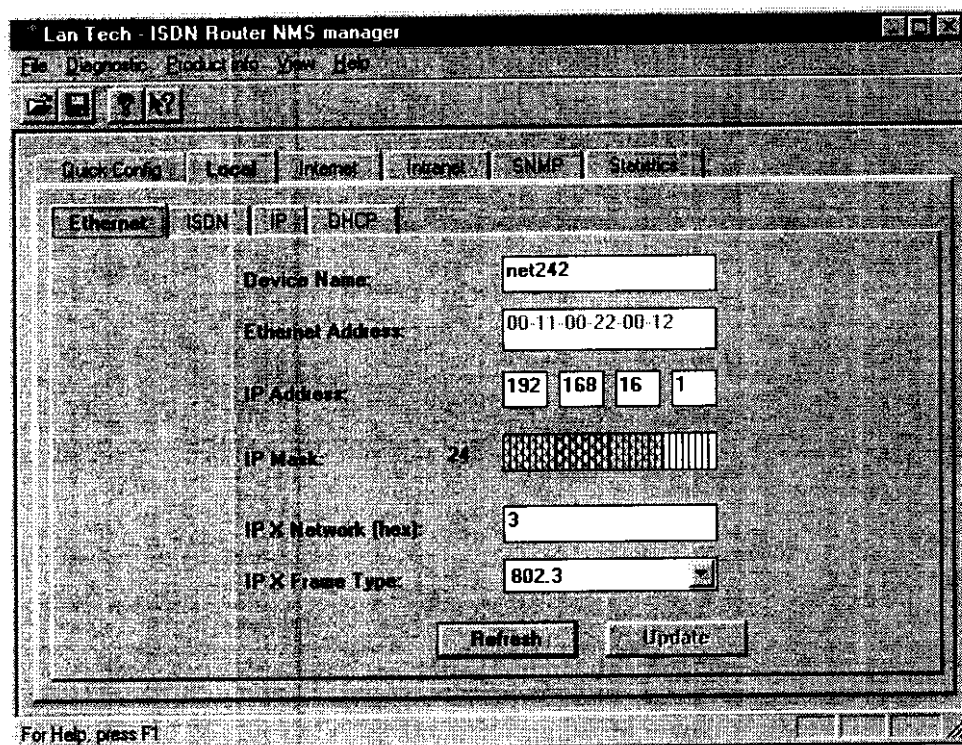
Figure 4-6, Local Ethernet Window

Device Name

The device name specifies the name of this ISDN router. This field is linked to Local Router Name in the menu "Quick Configuration". Any text character is acceptable for up to 32 characters.

IP Address

The IP address describes the IP address assigned to this router by your ISP. This field is linked to Local IP Address in menu "Quick Configuration".

IP Mask

The IP mask describes the local IP sub-netting. This field is linked to Local IP Mask in menu "Quick Configuration".

IPX Network

The IPX network specifies the IPX network number of the Ethernet this router is directly connected to. This 4-byte field is entered in 8 hex characters. With the given IPX network number, E80 creates a route entry in the IPX route table automatically. The IPX network has to be configured correctly for E80 to route IPX traffic.

IPX Frame Type

The IPX frame type specifies the frame encapsultion scheme this router will recognize as the IPX frames from the local Ethernet. The IPX frame type is selected from the pull-down menu including Ethernet II, 802.3, 802.2, and SNAP. E80 will route IPX packets of the specified IPX frame type. Other frame type of IPX may be bridged if enabled.

Local ISDN Sub-menu

This Local ISDN menu (see Figure 4-7, Local ISDN Window) describes the ISDN aspects of the local configuration. Certain parameters have to be set correctly as given by your local telephone company for the ISDN router to function properly. The switch type is a parameter that has to be entered precisely. For North-America, the SPIDs are also required. Some of the fields are linked to the menu "Quick Config".

Switch Type

The switch type specifies the switch type of the ISDN switch to which your ISDN line is connected. The switch type is selected by pulling down the switch-type box, and pick the one right for your ISDN line. This selection has to be perfectly matched for your ISDN to function. Please check your local phone company for the exact switch type. In Northern America, the dominated switch type is National ISDN-1 (NI-1). For the rest of the world, the dominated switch type is EuroISDN

(ETSI) or NET3. For Germany and France, same EuroISDN switch type is supported.

B Channel Alarm Threshold

This field is used to set the alarm threshold. When the B channel usage level passes beyond this threshold, the alarm LED will be flashed at high speed to catch your attention. Since there are two B channels in an ISDN line, threshold set to 50% means either one of the B channel is in use 100% of the time, or both channels are in use 50% of the time, or other equilibrium combination of usage.

Figure 4-7, Local ISDN Window

SPID 1

In Northern America, the local phone company assigns two SPIDs for each ISDN line. This field should be ignored for users outside Northern America. Please refer to explanation under "Quick Config".

SPID 2

In Northern America, the local phone company assigns two SPIDs for each ISDN line. This field should be ignored for users outside Northern America. Please refer to explanation under "Quick Config".

Phone Number 1

In Northern America, the local phone company assigns two phone numbers for each ISDN line. This field specifies the first phone number. This field is ignored by users outside Northern America. Please refer to explanation under "Quick Config".

Phone Number 2

In Northern America, the local phone company assigns two phone numbers for each ISDN line. This field specifies the first phone number. This field is ignored by users outside Northern America. Please refer to explanation under "Quick Config".

Phone 1 Usage

The phone 1 usage specifies the which SPID the phone 1 is associated with. This field is ignored by users outside Northern America.

Phone 2 Usage

The phone 2 usage specifies which SPID the phone 1 is associated with. This field is ignored by users outside Northern America.

Data Usage

The data usage specifies which SPID(s) the data connection will be associated. This field is ignored by users outside Northern America.

Local IP Sub-menu

The Local IP menu (see Figure 4-8, Local IP Window) describes the IP protocol related parameters at the local end of the ISDN router.

Route Table

For simple Internet Access where you want to connect an IP network to the Internet, the route table is created automatically. You need to manipulate the IP route table only if you have more complicated network topology. If your local Ethernet network is divided into multiple IP subnets, you need to add a static route entry with interface (IF) marked as "ether" for each local subnet. If you plan to connect to a remote office through the Intranet, and there are multiple IP subnets at remote site, you need to add a static route entry with interface (IF) masked as "intra" for each remote IP subnets. You may choose to turn on the RIP protocol to update the route table automatically instead of manipulating the route table. Turning on the RIP protocol is not recommended. The periodical exchange of RIP protocol packets will keep your ISDN line up all the time, and results in expensive telephone bill.

Route Table


```
 SNMP Manager - ISDN Router NMS manager

  0.0.0.0/0              205.158.241.93    0    rmt1    direct/local
  205.158.241.0/24      205.158.241.93    0    ether   direct/local
```
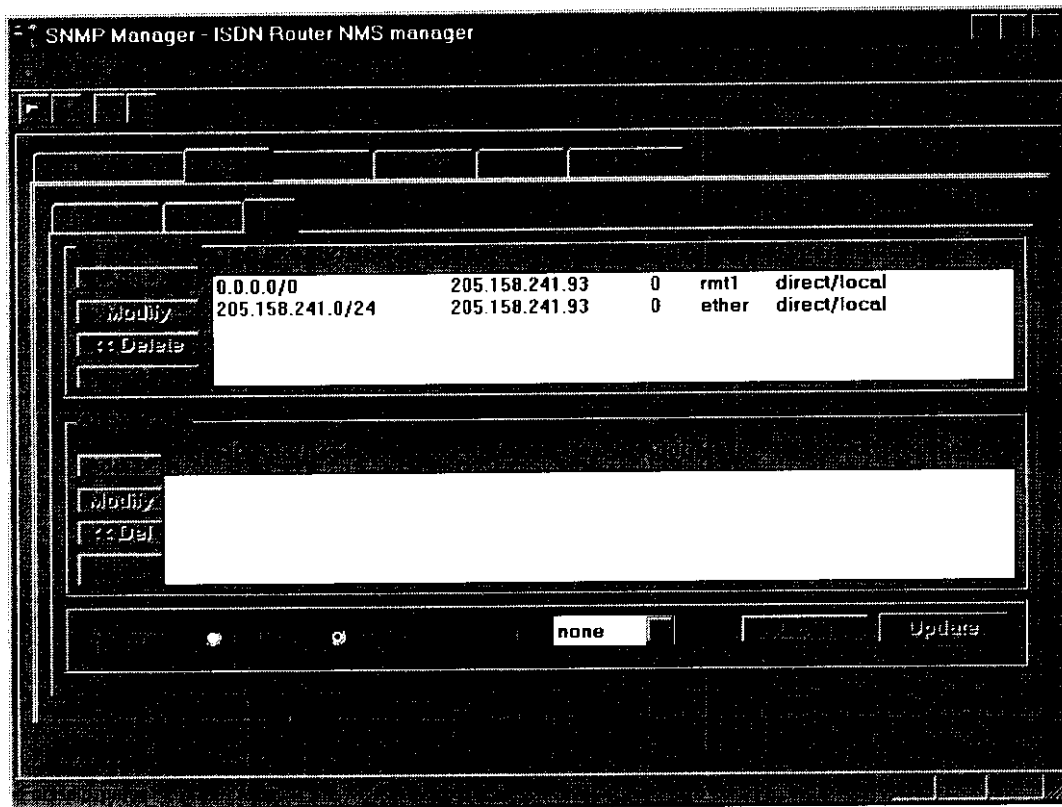
Figure 4-8, Local IP Window

Access List

The access list is a filtering table for security application. You may selectively filter or forward certain packet according to its source IP address, protocol, destination IP protocol, and destination port number. For example, if you intend to block web page being retrieved from a certain web server, you may create an entry of that particular IP address in the access list table to deny its traffic.

ARP Proxy

The ARP Proxy when enabled causes the ISDN router to send ARP responses to the LAN on behalf of those remote IP addresses. ARP proxy enables the the LAN users to communicate with the remote dial-up users without configure a static IP address for them.

RIP Protocol

The RIP protocol when enabled will cause the ISDN router to exchange RIP information with other RIP-enabled routers in the system. Enabling the RIP protocol will create the complete IP route table. The IP RIP packets are exchanged only when connection is up. IP RIP will not trigger ISDN connection.

Local DHCP Sub-menu

The DHCP sub-menu contains the DHCP parameters which describe how E80 as a DHCP server operates, and what TCP/IP configuration information to release.

IP Address Pool (Start Address, End Address)

The IP address pool as indicated by the Start Address and End Address is used by the DHCP server to release the IP addresses to the DHCP clients. E80 supports 16 IP addresses even if user specifies a IP address pool larger than 16 IP addresses. The start address and end address are set by default having the same IP subnet as the router's Ethernet address.

Subnet Mask

While leasing an IP address to a client, the IP Subnet Mask is among other configuration information available from DHCP server.

Gateway Address

While leasing an IP address to a client, the gateway IP address is among other configuration information available from DHCP server.

Primary DNS

While leasing an IP address to a client, the primary DNS IP address is among other configuration information available from DHCP server.

Secondary DNS

While leasing an IP address to a client, the secondary DNS IP address is among other configuration information available from DHCP server.

Domain Name

While leasing an IP address to a client, the domain name is among other configuration information available from DHCP server.

Lease Duration

The lease duration describes the maximum time length the IP address is leased to a client. A client usually renews the IP address half way before the lease duration expired.

The maximum lease duration is 100 days. The minimum lease duration is 1 day even if a duration of less than one day is entered. Note that when NMS modify the DHCP lease duration, the lease duration associated with a leased IP address remains unchanged until expired.

Active Lease(s)

This number indicates how many IP addresses have been leased to clients.

Lease Table Entry

Each table entry describes to whom the IP address was leased and for how long.

DCHP Enable

The check box let the user dynamically enable or disable the DHCP function. Note that if all stations including the NMS depend on E80 for assigning IP addresses, and NMS disable the E80 DHCP function. Under that circumstance, NMS may not be able to communicate with E80 if DHCP service is not re-enabled before the lease duration expired.

Internet Menu

The Internet configuration contains ISDN, PPP, IP, NAT sub-menus.

Internet ISDN Sub-menu

The Internet ISDN menu (see igure 4-9, Internet ISDN Window) is used to configure the ISDN connection to the Internet access.
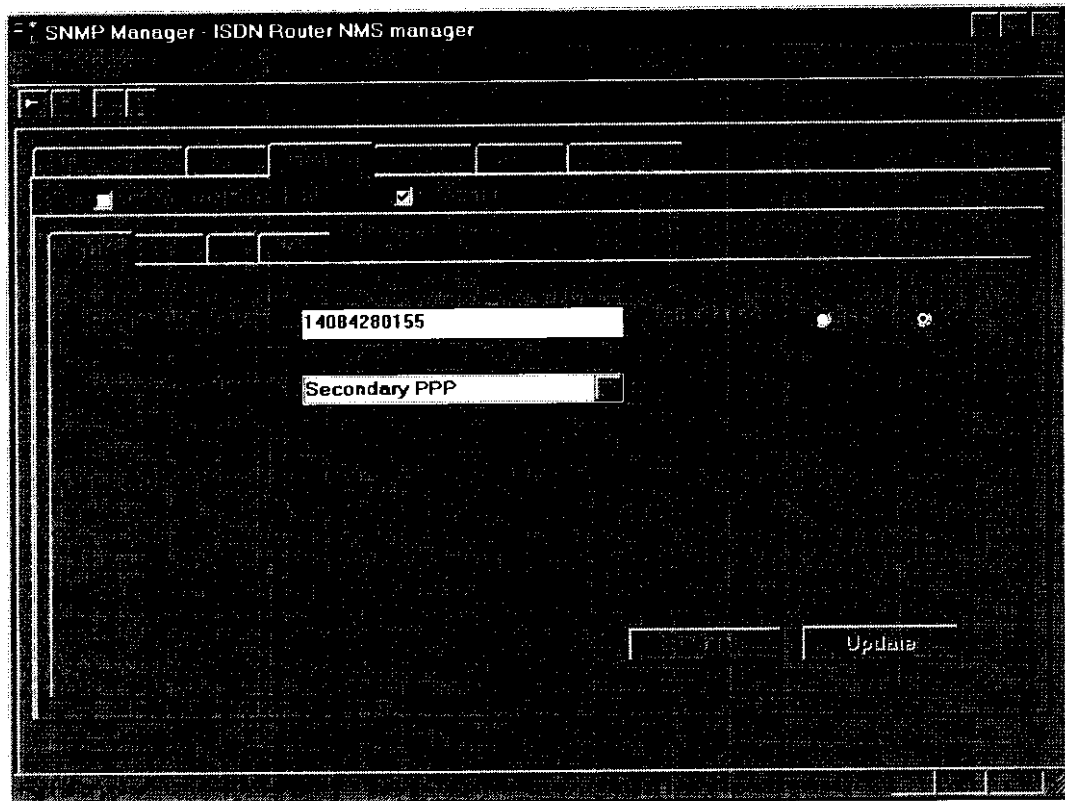
igure 4-9, Internet ISDN Window

Remote ISDN number

The remote ISDN number field specifies the ISP's ISDN number you would like to dial to. Your ISP will provide this number to you.

Data Service

The data service field is to select 56 Kbps or 64 Kbps for the ISDN call bandwidth. 64Kbps is the most common one. In rare situation such as international call where 56Kbps may be the only choice.

Preemption Allowed

This field specifies if the Internet connection is allowed to be preempted by phone call or not, and in what way. The Internet connection can be blocked from preemption at all, or be allowed on the 2nd PPP only, or 1st PPP as well.

Internet PPP Sub-menu

The Internet PPP menu (see

Figure 4-10, Internet PPP Window) is used to configure the PPP parameters for

the Internet connection.

Figure 4-10, Internet PPP Window

Remote Router Name

The remote router name is the name assigned to the remote router located at the ISP end. Any visible ASCII characters are acceptable. The remote router name is not required when you want to dial into your ISP's point of presence. In general, your ISP assigns to you a remote IP address for administration purpose.

Compression

The compression field specifies if the Stac compression protocol will be turned on for the Internet connection.

Encapsulation Protocol

The encapsulation protocol field specifies the protocol you want to run as the link protocol. Select PPP if you want to run single channel PPP. Select MLPPP if you intend to run two channel PPP when traffic becomes heavy.

Dial-out Authentication

The dial-out authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when you initiate an ISDN call to your ISP. Most ISPs support PAP and CHAP protocols.

Dial-out Password

The dial-out password specifies the password to use during the dial-out authentication process. This field is case sensitive, and is given to you by your ISP.

Call-in Authentication

The call-in authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when the ISP initiates an ISDN call to you. In real operation, your ISP will not initiate a call to you.

Call-in Password

The call-in password specifies the password to use during the call-in authentication process. This field is case sensitive, and is given to you by your ISP.

Ave Interval

The Average Interval(Ave Interval) specifies the period in seconds used for traffic measurement by the bandwidth manager. The longer period (e.g. greater than 30 seconds) causes the ISDN channel to be added or deleted in a slower but smoother pace. If this parameter is set too short, the ISDN channel may be added due to a short burst of Internet traffic or be deleted due to short idle period. Therefore, internally, the Ave Interval is set to minimum at 10 seconds. This parameter is available only if the MP protocol is selected as the Internet encapsulation protocol.

1->2 Util

The 1->2 Utilization specifies the Internet connection traffic level; beyond that, the second ISDN channel will be requested to enlarge the PPP bundle. The value ranges from 0% to 100%. This parameter is available only if the MP protocol is selected as the data encapsulation protocol.

2->1 Util

The 2->1 Utilization specifies the Internet connection traffic level; below that, the second PPP channel will be released from the PPP bundle. The value ranges from 0% to 100%. This parameter is available only if the MP protocol is selected as the Internet encapsulation protocol.

1->0 Idle

The bandwidth management function will remove the (primary) Internet connection when it is being detected idle for a specific period. The 1->0 Idle parameter specifies the that idle period in seconds. Assigning 0 second to this parameter has special meaning. It disables the 1->0 bandwidth management. The user has to manually disconnect the Internet Connection.

Internet IP Sub-menu

The Internet IP sub-menu (see Figure 4-11, Internet IP Window) is used to configure the IP related parameters of the Internet connection. For most Internet application, the un-numbered interface based configuration is appropriate. You need only to specify a remote IP address, instead of a pair of IP addresses for local end and remote end of the IP connection.

Remote SNMP Enable

This check box is to enable or disable SNMP management from remote. If disabled, the ISDN router will only response to the SNMP requests from the local Ethernet.

IP Enable

This parameter is to enable or disable the IP routing function. If IP routing is disabled, bridging must be enabled for IP packet to be forwarded through the router. Bridging is rarely used as the protocol for Internet access.

IP Address of Remote Ethernet

The remote IP address is the IP address of the remote router located at your ISP site. The IP address is entered in the standard IP address format of a.b.c.d. The remote IP address is required during PPP negotiation. Please ask from your ISP if you don't possess one.

Figure 4-11, Internet IP Window

IP Mask of Remote Ethernet

The remote IP mask is used to describe the remote IP sub-netting. The IP mask is entered by clicking the IP address bit map. The number of bit assigned for IP subnet is shown next to the IP address bit map as a decimal number for your reference.

Local End IP Address of ISDN Line

This field specifies the local end of the IP address of an IP connection. This field is applicable to the "numbered interface" IP address setting.

Remote End IP Address of ISDN Line

This field specifies the remote end of the IP address of an IP connection. This field is applicable to the "numbered interface" IP address setting.

IP Mask of ISDN Line

This field specifies the IP mask of the ISDN line when the "numbered interface" IP address scheme is used. Both local end and remote end should use the same IP mask.

Internet NAT Sub-menu

The Internet NAT sub-menu (see Figure 4-12, Internet NAT Window) is used to configure the NAT feature. NAT is a feature designed for security protection and cost saving for Internet access. NAT hides internal IP addresses from the outside world therefore decreases the possibility of hacker attack. NAT translates the internal IP addresses into a single IP address for Internet access. If the number of IP address assigned by the ISP is a factor for billing, NAT can save the monthly bill.
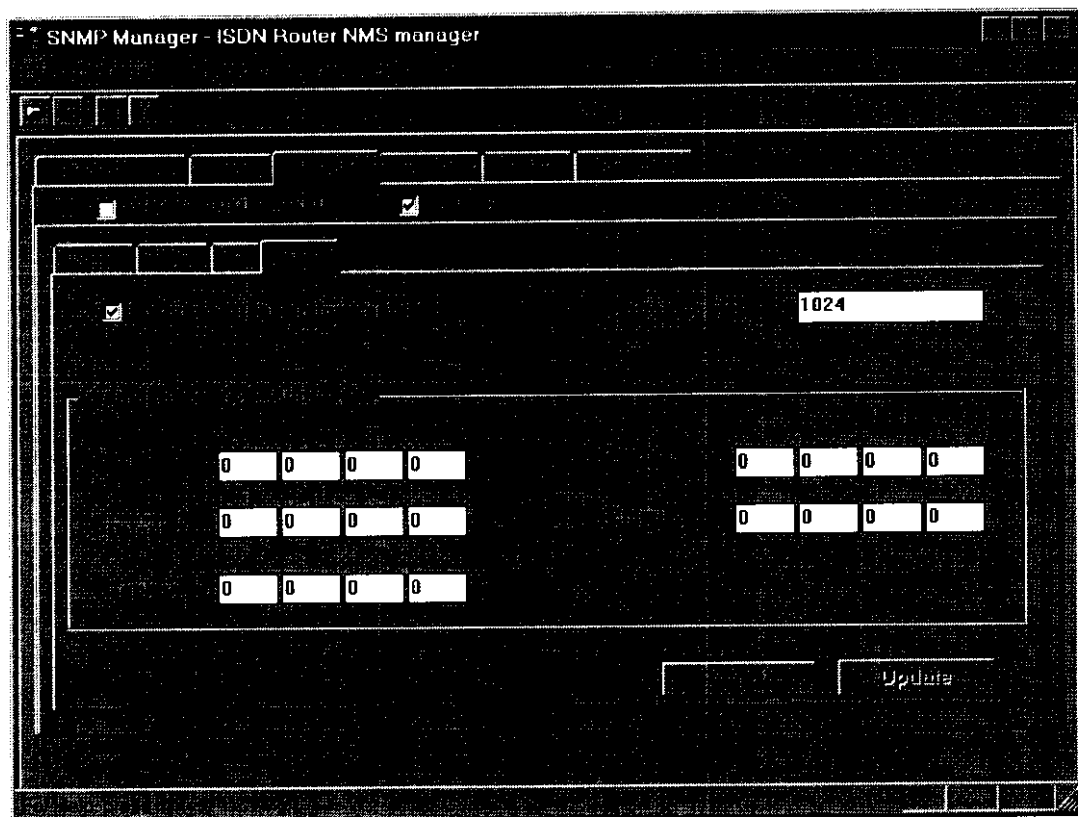
Figure 4-12, Internet NAT Window

Network Address Translation Enable

This field enables or disables the NAT function. Please note that, with NAT enabled your FTP or Telnet session may become invalid, if the ISDN connection

to the ISP is disconnected during the sessions. The ISDN disconnection may be due to no Internet traffic for too long that causes 1->0 bandwidth transition.

Starting Port

This field specifies the starting port number NAT would use to support the NAT function. 1024 is the default port number.

FTP Server

The internal IP address of the FTP server that provides FTP service to outside world. All incoming FTP service requests are routed to the specified FTP server.

HTTP Server

The internal IP address of the HTTP server that provides HTTP service to outside world. All incoming HTTP service requests are routed to the specified HTTP server.

Telnet Server

The internal IP address of the Telnet server that provides Telnet service to outside world. All incoming Telnet service requests are routed to the specified Telnet server.

Email Server

The internal IP address of the Email server that provides Email service to outside world. All incoming Email service requests are routed to the specified Email server.

Gopher Server

The internal IP address of the Gopher server that provides Gopher service to outside world. All incoming Gopher service requests are routed to the specified Gopher server.

Intranet Menu

The Intranet configuration contains ISDN, PPP, IP, and IPX, sub-menus.

Intranet ISDN Sub-menu

The Intranet ISDN sub-menu is shown in Figure 4-13, Intranet ISDN Window. This window is used to configure the ISDN connection to an Intranet access.

Remote ISDN number

The remote ISDN number field specifies the ISP's ISDN number you would like to dial to. Your ISP will provide this number to you.

Data Service

The data service field is to select 56 Kbps or 64 Kbps for the ISDN call bandwidth. 64Kbps is the most common one. In rare situation such as international call where 56Kbps may be the only choice.

Preemption Allowed

This field is specified if the Internet connection is allowed to be preempted by phone call or not, and in what way. The Internet connection can be blocked from preemption at all, or be allowed on the 2nd PPP only, or 1st PPP as well.
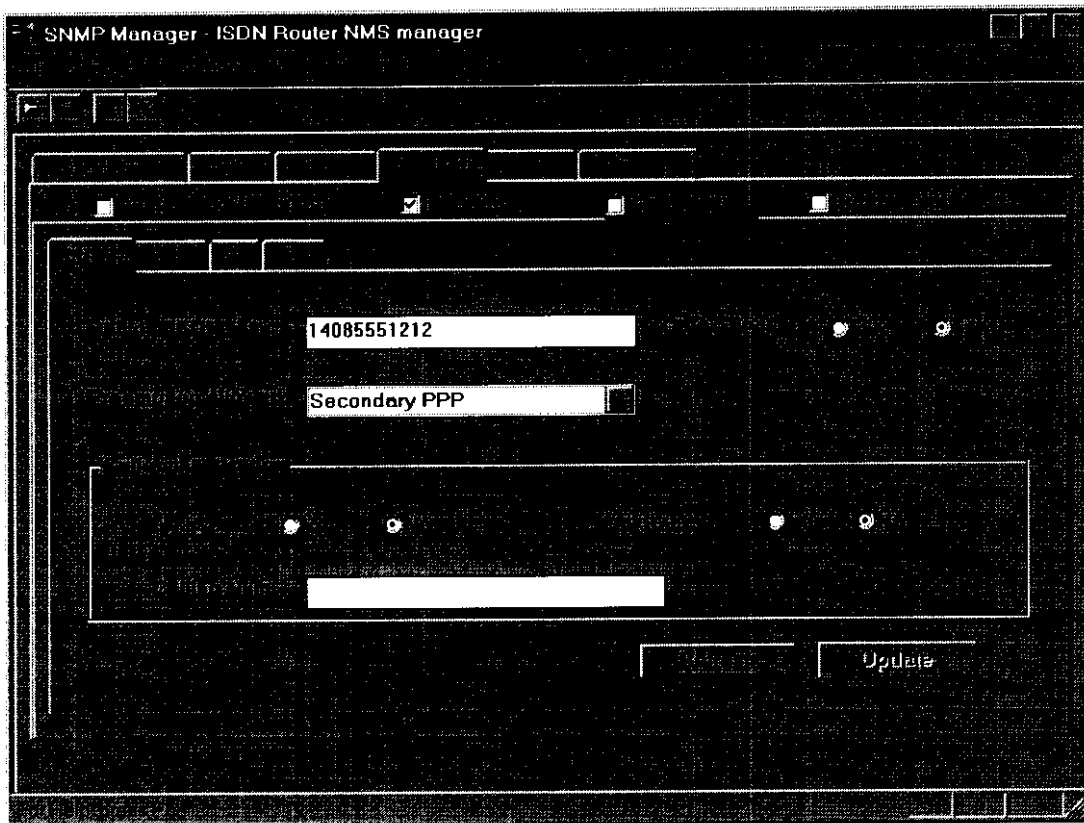
Figure 4-13, Intranet ISDN Window

CLID

Caller ID is used to qualify the incoming call. Only the incoming call whose calling number matches the CLID will be accepted. This is an Intranet feature. The data call will not be answered if the local telephone company is not supplying the calling party number to the ISDN router. Please use with care.

Callback

Call back function is a security feature which enables the router to disconnect the incoming call upon verification the CLID and call back to the CLID. This is an

Intranet feature. And again the local telephone company has to supply the calling party number to the ISDN router in order for this feature to work.

Calling Num

The number the router will call when the Callback function is enabled. This is an Intranet feature.

Intranet PPP Sub-menu

The Intranet PPP sub-menu is shown in Figure 4-14, Intranet PPP Window. This
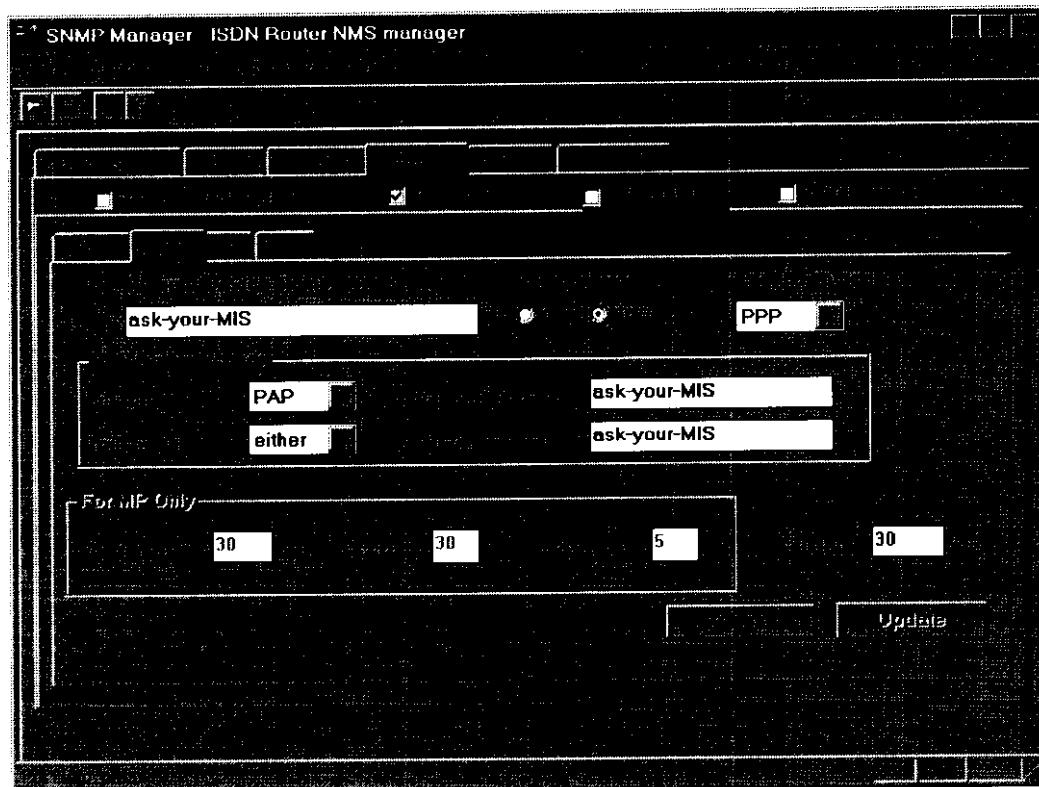
menu is used to configure the PPP parameters for an Intranet connection.

Figure 4-14, Intranet PPP Window

Remote Router Name

The remote router name is the name assigned to the remote router located at the ISP end. Any visible ASCII characters are acceptable. The remote router name is not required when you want to dial into your ISP's point of presence. In general, your ISP assign to you a remote IP address for administration purpose.

Compression

The compression field specifies if the Stac compression protocol will be turned on for the Internet connection.

Encapsulation Protocol

The encapsulation protocol field specifies the protocol you want to run as the link protocol. Select PPP if you want to run single channel PPP. Select MLPPP if you intend to run two channel PPP when traffic becomes heavy.

Dial-out Authentication

The dial-out authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when you initiate an ISDN call to your ISP. Most ISPs support PAP and CHAP protocols.

Dial-out Password

The dial-out password specifies the password to use during the dial-out authentication process. This field is case sensitive, and is given to you by your ISP.

Call-in Authentication

The call-in authentication field specifies which protocol you want to run as the PPP/MLPPP authentication protocol when the ISP initiates an ISDN call to you. In real operation, your ISP will not initiate a call to you.

Call-in Password

The call-in password specifies the password to use during the dial-in authentication process. This field is case sensitive, and is given to you by your ISP.

Ave Interval

The Average Interval specifies the period in seconds used for traffic measurement. The longer period (e.g. greater than 30 seconds) causes the ISDN channel to be added or deleted in a slower but smoother pace. If this parameter is set too short, the ISDN channel may be added due to a short burst of Intranet traffic or be deleted due to short idle period. Therefore, internally, the Ave Interval is set to minimum at 10 seconds. This parameter is available only if the MP protocol is selected as the Internet encapsulation protocol.

1->2 Util

The 1->2 Utilization specifies the Intranet connection traffic level beyond that the second ISDN channel will be requested to enlarge the PPP bundle. The value

range from 0% to 100%. This parameter is available only if the MP protocol is selected as the data encapsulation protocol.

2->1 Util

The 2->1 Utilization specifies the Intranet connection traffic level; below that the second PPP channel will be released from the PPP bundle. The value ranges from 0% to 100%. This parameter is available only if the MP protocol is selected as the Internet encapsulation protocol.

1->0 Idle

The bandwidth management function will remove the (primary) Intranet connection when it is being detected idle for a specific period. The 1->0 Idle parameter specifies the idle period in seconds. Assigning 0 second to this parameter has special meaning. It disables the 1->0 bandwidth management. The user has to manually disconnect the Intranet Connection.

Intranet IP Menu

The Intranet *IP* sub-menu is shown in Figure 4-15, Intranet IP Window. This menu is used to configure the IP related parameters of the Intranet connection.
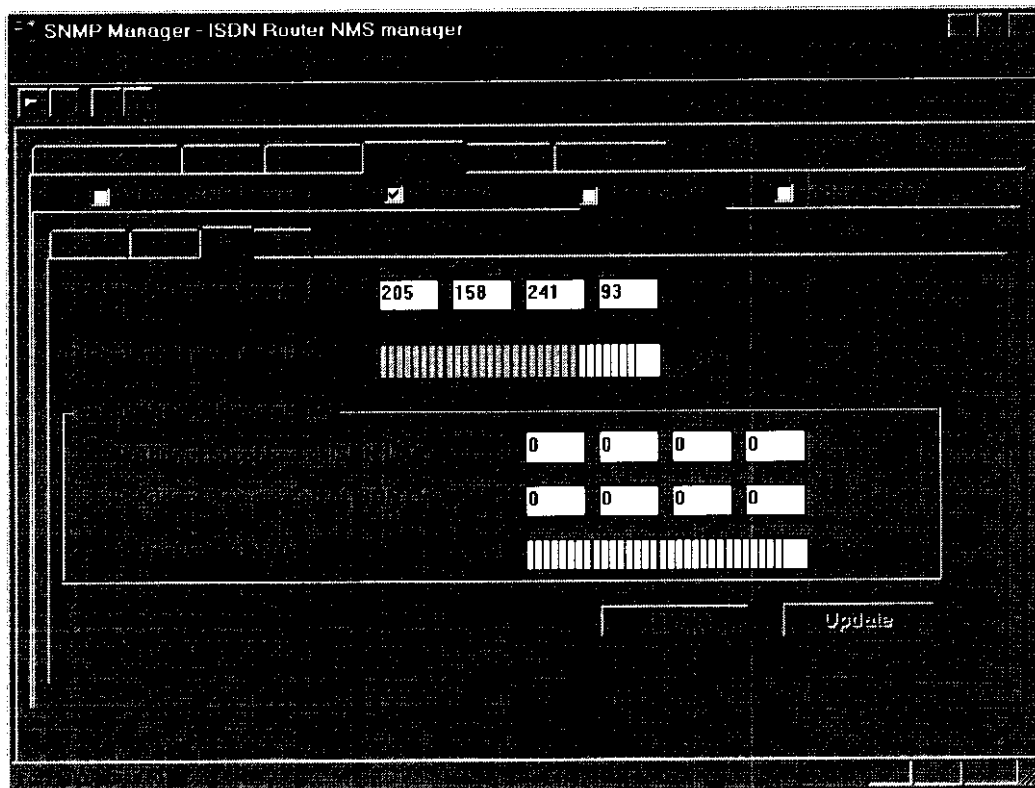
Figure 4-15, Intranet IP Window

Remote SNMP Enable

This check box is to enable or disable SNMP management from remote. If disabled, the ISDN router will only response to the SNMP requests from the local Ethernet.

IP Enable

This parameter is to enable or disable the IP routing function. If IP routing is disabled, bridging must be enabled for IP packet to be forwarded through the router. Bridging is rarely used as the protocol for Internet access.

IP Address of Remote Ethernet

The remote IP address is the IP address of the remote router located at your ISP site. The IP address is entered in the standard IP address format of a.b.c.d. The remote IP address is required during PPP negotiation. Please ask from your ISP if you don't possess one.

IP Mask of Remote Ethernet

The remote IP mask is used to describe the remote IP sub-netting. The IP mask is entered by clicking the IP address bit map. The number of bit assigned for IP subnet is shown next to the IP address bit map as a decimal number for your reference.

Local End IP Address of ISDN Line

This field specifies the local end of the IP address of an IP connection. This field is applicable to the "numbered interface" IP address setting.

Remote End IP Address of ISDN Line

This field specifies the remote end of the IP address of an IP connection. This field is applicable to the "numbered interface" IP address setting.

IP Mask of ISDN Line

This field specifies the IP mask of the ISDN line when the "numbered interface" IP address scheme is used. Both local end and remote end should use the same IP mask.

Intranet IPX Menu

The Intranet IPX sub-menu is shown in Figure 4-16, Intranet IPX Window. This menu is used to configure an IPX connection on an Intranet. Two key points to remember for IPX configuration:

1) Set IPX network number and frame type at both local and remote router.

2) Assuming Netware server exists only at remote site, add an SAP entry at local router that describe all necessay Netware server information (name, Internal Network Number, internal Node Number….)
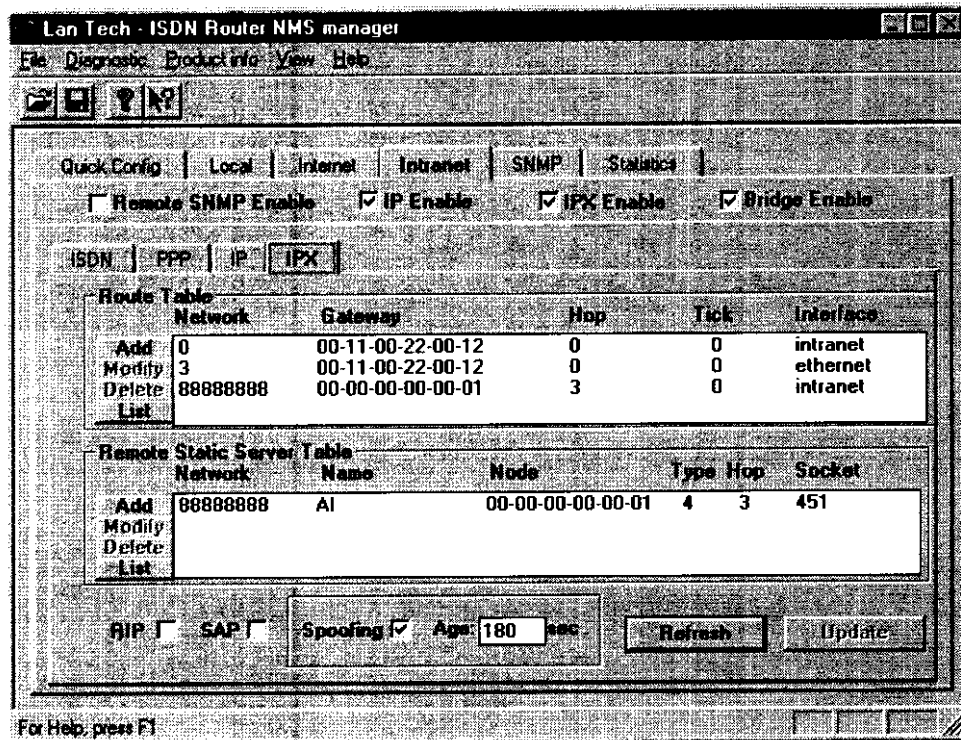
Figure 4-16, Intranet IPX Window

RIP

The IPX RIP packets will always be exchanged over the WAN when the ISDN connection is up. The RIP box when checked is to allow Netware RIP traffic to initiate the ISDN connection.

SAP

The IPX SAP packets will always be exchanged over the WAN when the ISDN connection is up. The SAP box when checked is to allow Netware SAP traffic to initiate the ISDN connection.

Spoofing

The check box is to enable or disable the IPX spoofing function. The spoofing function minimizes the dial-up connection time by responding to the "keep alive" request on behalf of the remote IPX clients. The spoofing function try to minimize the ISDN dial-up against the IPX "keep alive" messages but not the regular IPX or SPX messages.
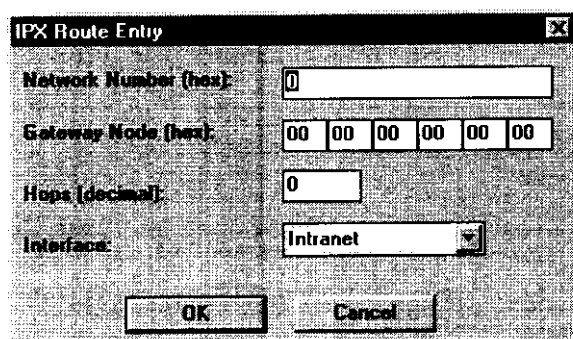
Age

The IPX spoofing age configures how long E80 will perform spoofing function before the ISDN dial-up is allowed by the "keep alive" message. Once the dial-up connection is up, the age timer is reset.

IPX Route Table

An IPX route table entry contains IPX routing information for a known IPX network. The network number identifies the unique IPX network. The gateway node is the node address for the gateway to that network. The hop count indicate how far away is that network. The interface is either local Ethernet or Intranet through the ISDN connection.
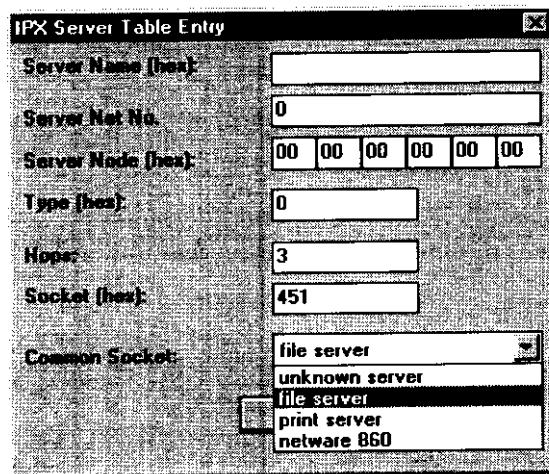
For most applications, user is not required to create or modify IPX table.

IPX SAP Table

An IPX SAP table entry contains information about a remote server. The server name is the name of the server. The network is the internal network number of the server. The node number is the internal node address of the server. The type is the service type of the server. The socket is the socket number of the server. The hop count indicates the distance to the server. The NMS user is required to add a SAP entry for every remote server the local clients intend to connect. For a given SAP entry, E80 automatically add a route entry in the IPX route table.
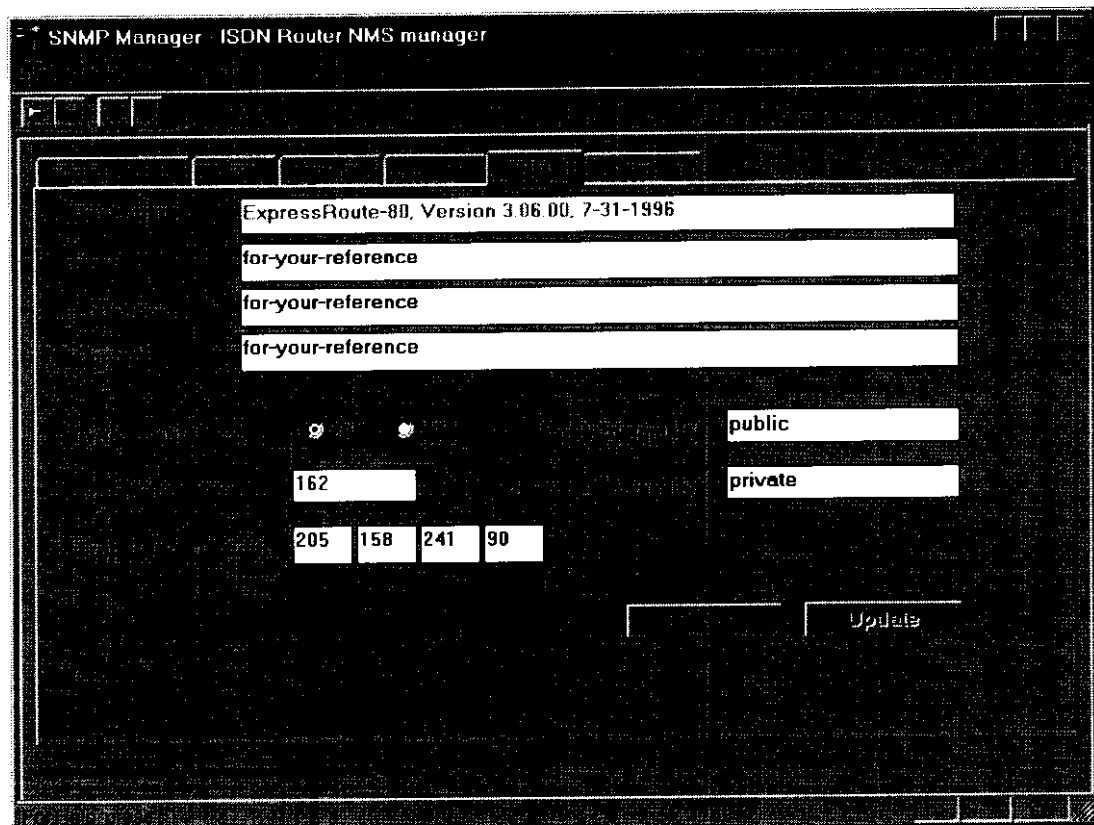
SNMP Menu

The SNMP menu (see Figure 4-17, SNMP Window) is used to configure the SNMP specific parameters. Some of the parameters are corresponding to the objects defined in system MIB. The rest are for managing the SNMP access, and

trap delivery.

Figure 4-17, SNMP Window

Description

The field gives a brief description of the product, as provided by the manufacturer.

Name

This field is used by user to assign a name to this ISDN router.

Location

This field is used by user to describe the location of this ISDN router.

Contact

This field is used by user to describe the contact person of this ISDN router.

Read Community

This field is used to assign a "password" for SNMP read operation.

Read-Write Community

This field is used to assign a "password" for SNMP read-write operation.

Trap Enable

This parameter is used to enable or disable the trap delivery.

Trap Server Port

This parameter specifies which UDP port the traps are sent to.

Trap Server IP Address

This parameter specifies IP address where the traps are sent to.

Statistics Menu

Statistics Ethernet Sub-menu

The Statistics Ethernet sub-menu (see Figure 4-18, Statistics Ethernet Window) contains the statistics data collected on the Ethernet interface. Both directions of the traffic, receive and transmit, are monitored. . The "refresh" button is used to collect a new page of statistics data. The "periodic on" button is used to refresh this menu every second.

System Up Time

This is the time elapsed since the time the ISDN router has been powered-up, or reset.

Bytes

This counter displays the number of byte the Ethernet has received or transmitted.

Frames

This counter displays the number of frames the Ethernet has received or transmitted.

Broadcasts

This counter displays the number of broadcast frames the Ethernet has received or transmitted.
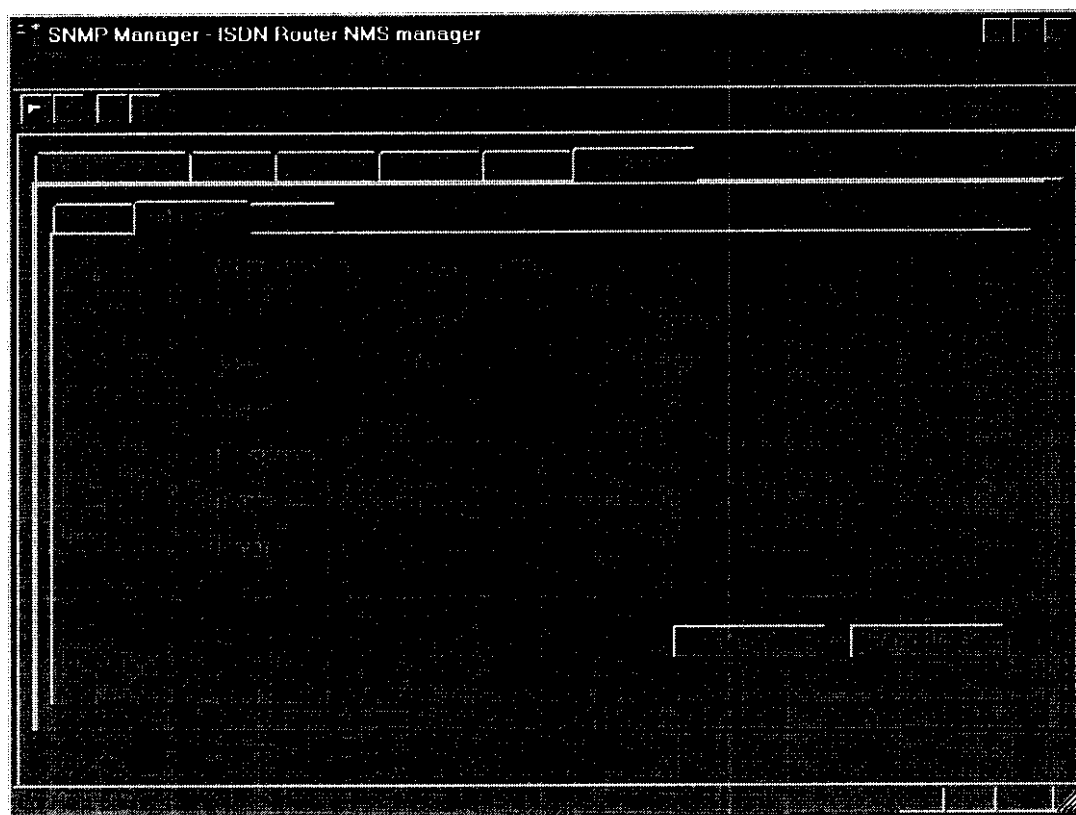
Figure 4-18, Statistics Ethernet Window

Errors

This counter displays the number of error frames the Ethernet has received or transmitted. The error conditions are : too short, mis-alignment, excess collision.

Discards

This counter displays the number of frames the Ethernet has discarded due to lack of buffer resource or error detection..

Statistics ISDN Sub-menu

The Statistics ISDN menu (see Figure 4-19, Statistics ISDN Window) contains the statistics and status data collected on the ISDN interface. The "refresh" button is used to collect a new page of statistics data. The "periodic on" button is used to refresh this menu every second.
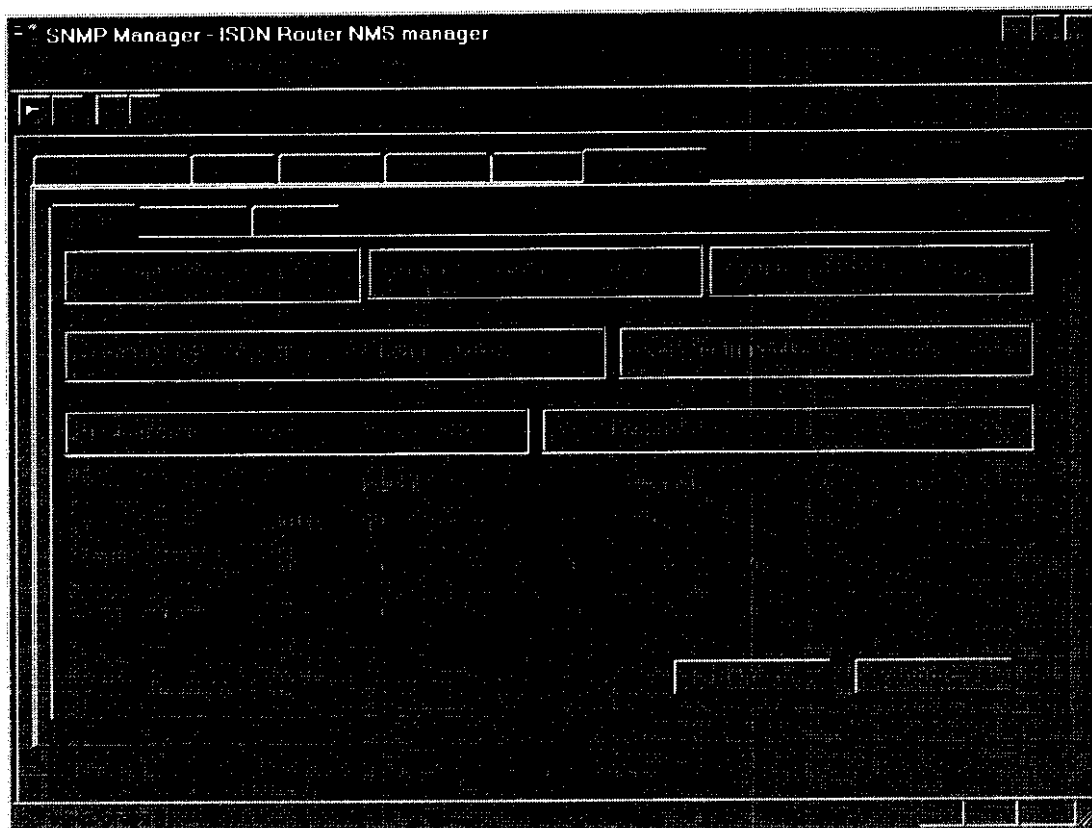
Figure 4-19, Statistics ISDN Window

D Channel Status

This field indicates the current D channel status. The D channel is either Up or Down.

B1 Channel Status

This field indicates the current B1 channel status. The B channel states are Up, Down, or Calling (in the process of call establishment).

B2 Channel Status

This field indicates the current B2 channel status. The B channel states are in Up, Down, or Calling (in the process of call establishment)..

B Channel(s) Up Time

This field display the time the ISDN channel, B1 or B2, has stayed up since last reset. Both channels up for 1 minute is counted as 2 minutes.

B Channel(s) In Use

This field displays the percentage of time the B channel, B1 or B2, has stayed up since last reset. 50% in use may mean one B channel is up all the time, and the other B is down all the time or both channels are up for 50% of the time. 100% in use means both B channels are up all the time.

B1 Utilization

This field displays the current B1 channel utilization, ranging for 0 to 100%. Utilization 0% means the channel is currently idle. Utilization 100% means full 64 Kbps of the B channel bandwidth is busy in data traffic delivery.

B2 Utilization

This field displays the current B1 channel utilization, ranging for 0 to 100%. 0% means the channel is currently idle. 100% means full 64 Kbps of the B channel bandwidth is busy in data traffic delivery.

Good Frames

This field displays the number of good frames are received or transmitted on the corresponding channel.

Error Frames

This field displays the number of error frames are received or transmitted on the corresponding channel. The error conditions are : mis-alignment, or CRC error.

Statistics Trace Sub-menu

The Statistics Trace (see Figure 4-20, Statistics Trace Window) menu provides the trace information of the ISDN router. This menu is the most useful menu for diagnostic purpose.

Trouble Shooting

Also under the name of Detail Log, the trouble shooting enable the ISDN router to send a lot of more detail IP, PPP, and ISDN activity trap to NMS for trouble shooting. It should only be enabled during the trouble shooting stage. Keep it on all time will increase the Ethernet traffic, and work load to the ISDN router and therefore is not beneficial to the performance.

Clear Trap List

This click button is used to clear the traps previously stored in the trap history.

Detail Log Enable

This click button ask ISDN router to send all detaled trace. It is good source for trouble shooting. At the system reset time, the detail log is always disabled.

Trap History

Each trap is described in date, time, type, and a brief information about the cause of the traps. Within the trap history area, up to 100 traps are stored for review with the most recent trap on top of the list.
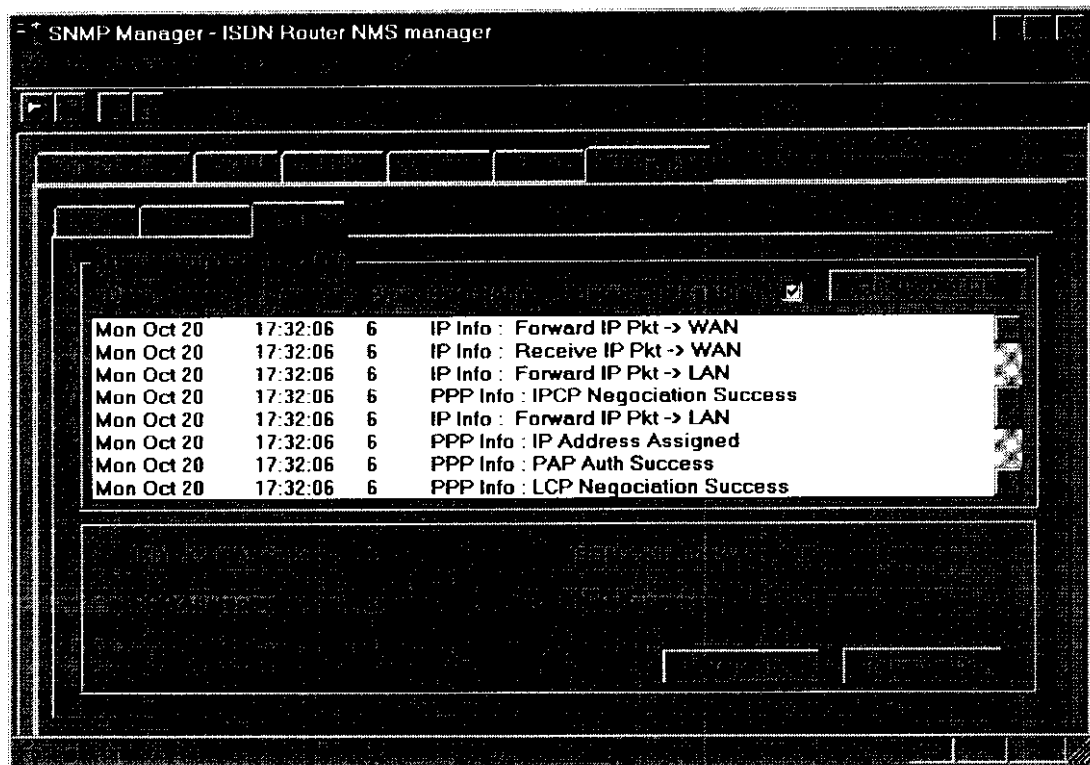
Figure 4-20, Statistics Trace Window

ISDN Data Call Attempts

This field displays how many times the ISDN router has tried to make ISDN data call since last reset. Note that the incoming ISDN data call is not contributed to this counter.

ISDN Data Call Success

This field displays how many times the ISDN router has succeeded in making ISDN data call since last reset. Note that the incoming ISDN data call is not contributed to this counter.

PPP Attempts

This field displays how many times the ISDN router has tried to negotiate PPP data connection since last reset.

PPP Success

This field displays how many times the ISDN router has succeeded in negotiating PPP data connection since last reset.

Monitoring Status with ClearMon.

ClearMon is a utility program which, while running, displays the E80 front panel including real-time display of the LED status and activity lights. A typical ClearMon display is shown in Figure 4-21, ClearMon Display
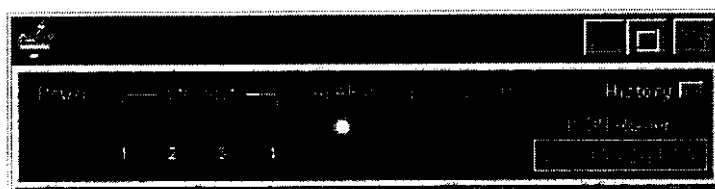
Figure 4-21, ClearMon Display

The top space will show the most recently trap received. You may click "History" to review old traps maintained by ClearMon.

The virtual LED basically reflect what you will see from the E80 front panel. Under B1 and B2 virtual LEDs, the "phone", "Internet"(one networked PC), and "Intranet" (2 networked PC) icons help to indicate if the B channel is used for voice, and data connection.

Managing the E80 from a Console

The E80 can be configured through an alphanumeric terminal (or a PC with a terminal emulation program) which is used as a console by connecting it to the DB-9 connector on the E80 rear panel. See Chapter 2, Installation for more details.

The terminal should be set to emulate a DEC VT100 terminal at 9600 bps with 8 character bits, no parity bit and one stop bit.

The session can be started by pressing the Enter key a few times to display the login screen. A typical login screen is shown in Figure 4-22, Console Login Screen. This example is one in which a PC operating the Hyperterminal program is emulating a VT100.

Figure 4-22, Console Login Screen

The login screen allows the user to enter a password. The first time this window is used the user can enter any password up to 16 alphanumeric characters. Users are urged to set up a new password using "F2 Change User Password".

When the password has been successfully entered, press the Enter key to display the console quick config screen as shown in Figure 4-23, Console Quick Config Screen.

```
dircom1 - HyperTerminal                                                    

                          Quick Configuration


Local Router Name    [abc                  ] Remote Router Name  [aimnet            ]

Local IP Address     [205.158.241.93       ] Remote IP Address   [0.0.0.0           ]
Local IP Mask        [255.255.255.0        ] Remote IP Mask      [0.0.0.0           ]
Ethernet Address     [000011223344         ]

Remote ISDN Number   [14084280155          ] B Channel Speed     [2] (1:56K,2:64K)
Phone Number 1       [5551212              ] Phone Number 2      [5551234           ]
SPID 1               [408555121201         ] SPID 2              [408555123402      ]

Switch Type          [1]                      Link Protocol      [1]
(1:NI-1,2:ATT,3:ATTPP,4:NT1,5:ETSI)           (1:PPP,2:MP)
(6:NTT,7:1TR6,8:VN,9:Taiwan)
Send Authentication [2]                       Send Password      [riverdale         ]
Recv Authentication [4]                       Recv Password      [NA                ]
(1:none,2:PAP,3:CHAP,4:either)


Trap    :
Status  :
                                                                  F4:  Exit
```

Figure 4-23, Console Quick Config Screen

The Console Quick Config screen permits the user to enter configuration data. Use the Tab key to move to the next field and the Shift-Tab key to move to the previous field.

Route Table data can be seen by pressing the F2 key and Statistics date by pressing the F3 key.

The F4 key can be used to exit a screen.

Managing the E80 from a Browser

The E80 can be configured and managed from an attached Ethernet station using virtually any standard Web Browser. The station must have the EasyWeb program installed as described in Chapter 2.

Start the browser and enter the URL: http://<your web server name>/EasyWeb/login.htm. This will cause the screen shown in Figure 4-24, EasyWeb SNMP Manager to be displayed.

Enter the IP Address and click on the Submit button.

Follow the instructions on the subsequent screens to configure and manage the
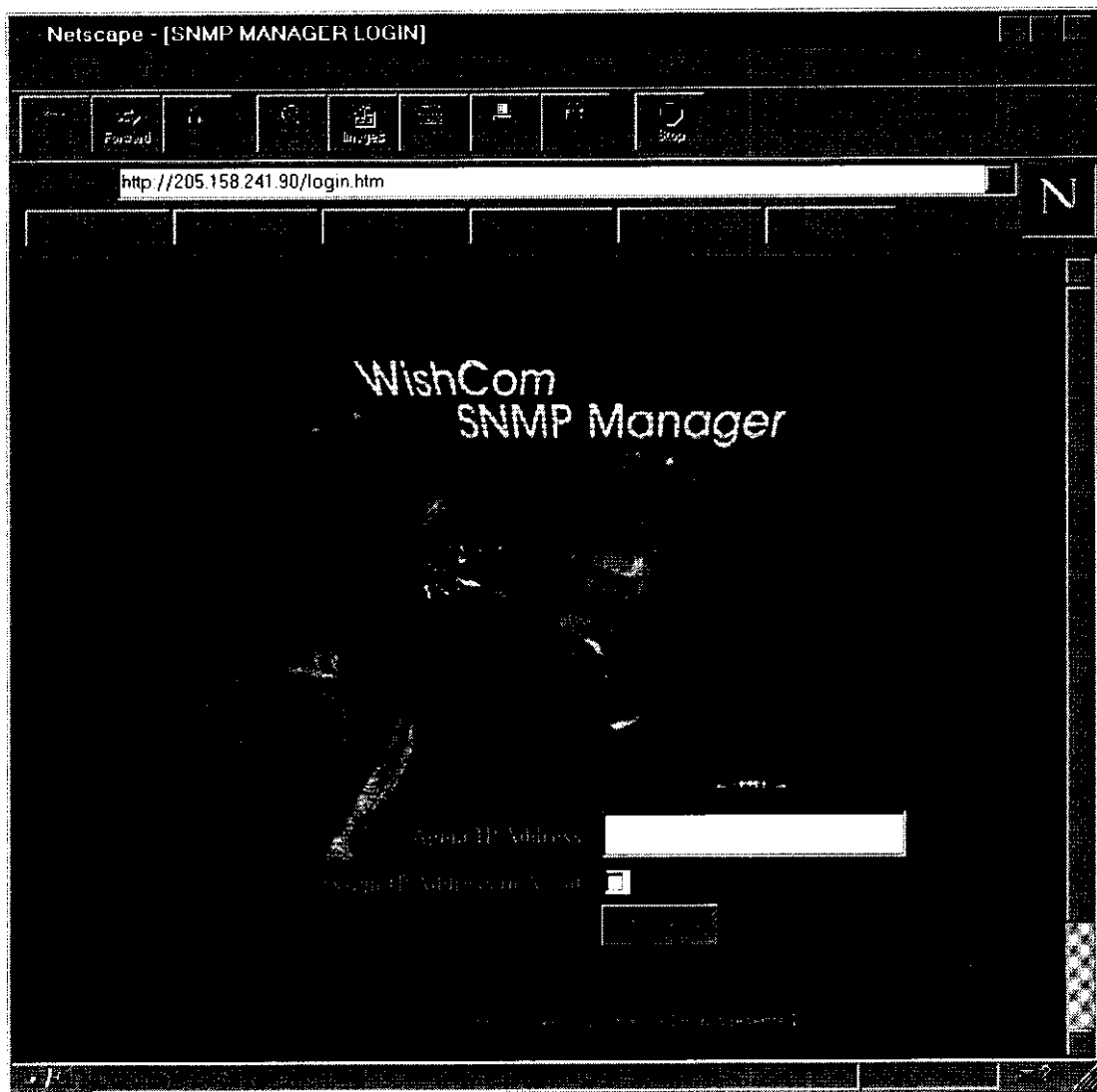
E80 router.

Figure 4-24, EasyWeb SNMP Manager

5. Troubleshooting

This chapter explains how to isolate and resolve simple problems encountered with the Express Route 80 ISDN router. Problem may stem from incorrect configuration setting or improper installation. Follow the following steps should help you resolve most of the symptoms. If problem persists, please contact your technical support with a list of symptoms, LED display status.
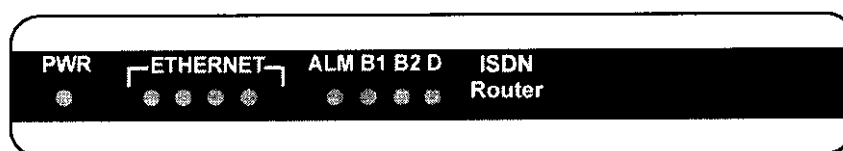
Figure 5-1, Front Panel LEDs

Troubleshooting Tips

Before you call technical support organization for assistance, check the following :

1. **The power supply is connected and the power LED is on.**

2. **Turn the power off and on again, observe the alarm (ALM) LED During power-up self-test, the ALM LED flashes.**

    If the ALM LED flashes and remains on for more than 10 seconds, there is an internal hardware failure. Notify your reseller that the ISDN router has failed the self-test, and order a replacement.

    If the LED goes off after the test has been completed, the power-up self-test has been successful.

3. **Verify that the ISDN cable (RJ45, 8 pin position) is connected to the ISDN router and make sure that it is an ISDN connection, not a plain old telephone connection.**

    The ISDN router will not operate if connected to an analog telephone wall jack. If your ISDN router is equipped with U interface, make sure that the ISDN router is connected directly into the ISDN wall outlet. If your ISDN router is equipped with a S/T interface, make sure that the ISDN router is connected to an intermediate telephone device called NT-1.

4. **Monitor the status of the D channel LED**

When you are connected to a live ISDN line, the D channel LED will be lighted or flashed

If the D channel LED remains off, it indicates that either no ISDN signal is presents or E80 is not able to sync-up at physical level with the central office. It is likely that there is a poor connection to the local Telephone Company. Make sure that the ISDN cable is in good condition, and securely plugged-in. If the LED remains off, call your local telephone company for trouble shooting assistance. The problem may be the ISDN wire, or telephone company equipment. In this situation, D channel will brink-on every 10 seconds or so to indicate that E80 is running (healthy in code execution).

If the D channel LED remains on, it indicates D channel physical level has been in-sync. Occasionally the D channel LED will brink-off that indicates ISDN messages are exchanged between E80 and phone company ISDN switch.

5. **Monitor the status of the B channel LEDs**

There are two B channel LEDs : B1 LED and B2 LED B1 indicate your ISDN channel activities.

If the B channel LED is off, it indicates that the B channel is in idle state. If the B channel LED is lighted on, the associated B channel is in use. It can be used for data connection or voice/fax/modem connection.

6. **Monitor the status of the Ethernet LEDs.**

There are four Ethernet LEDs, each designated for a Ethernet Port.

If an Ethernet LED is lighted on, it indicates that there is a Ethernet device connected to the associated Ethernet port transmitting valid Ethernet signal. If the Ethernet LED is off, either no Ethernet device is connected at the remote end, or there is a problem with the Ethernet UTP cable (RJ45) or with the Ethernet Network Interface Card (NIC).

A Ethernet LED will brink when there is Ethernet frames transmitted to or received from that Ethernet device. The Ethernet indicates the occurrence of the Ethernet traffic but not the intensity of the Ethernet traffic.

7. **If your are unable to communicate with the router through console port**

The ISDN router is designed to communicate with a VT100 terminal all time. If you are unable to communicate with the router, make sure the RS232 cable is a 9-pin male to female straight-through cable, and the baud rate is set to 9,600 baud per second.

8. **If your are unable to communicate with the router through NMS.**

   The Network Management System (NMS) communicates with the router through Ethernet using the SNMP protocol. If your NMS is unable to get SNMP response from the router, check the following :

   Ping a known active station in the local Ethernet. If you are unable to receive the ICMP response, you may have problem with your TCP/IP installation. Check the NMS Ethernet cable, NIC, and TCP/IP configuration.

   If you are able to ping other TCP/IP stations but not the ISDN router. Make sure that the ISDN router is active, and it is assigned with the correct IP address.

9. **If your are unable to make voice call**

   If you are unable to make a voice call when there is no B channel or only one B channel is in used as indicated by the B channel LEDs. Check the RJ11 telephone cable and the analog device itself.

10. **If your are unable to make data call**

   This is a more complicated problem than any of the previous list. It is suggested that you use NMS statistics, and trace utilities to help you perform the diagnosis. The NMS trace utility show you the network activities in detailed. The NMS statistics give you detailed LAN and WAN frame count.

   If you are sending traffic towards Internet or Intranet, but the B channel LED or trace window show no ISDN activities. You should check your IP network configuration.

If the ISDN router fails at ISDN dialing attempt, check the telephone number you configure. The number has to be a correct one associates with a ISDN data device at the remote end. The trace windows should provide you with precise error message.

If the ISDN call is connected briefly for a few seconds, and then disconnected. Mostly likely your PPP configuration mismatches with the

remote end's. Check your PPP configuration including PPP authentication protocol, and password.

Index

1

2

A

B

C

D

E

F

G

H

I