ITK NetBlazer Products

ITK NetBlazer 4400

March 98

ITK Telekommunikation AG
Joseph-von-Fraunhofer-Straße 23
D-44227 Dortmund

Contents

Preface

Congratulations on purchasing the **ITK NetBlazer 4400**. This product is a powerful tool used to interconnect Local Area Networks (LANs) via ISDN, and provide remote access over analog Modem or GSM connections.

Merging LANs into regional and company-wide networks has become a cost-effective way, even for small and mid-size companies, to exchange large amounts of data. **Internet** and **Intranet** are the contemporary slogans used in global communication**.**

Interconnecting LANs over long distances is technically complicated. The **ITK NetBlazer 4400** makes it easy for you to interconnect your LANs.

If you are currently working with a PC connected to a remote LAN via a modem line or X.25 line, you may be experiencing slow data transmission. Working in such an environment with transfer rates of 2.4 to 9.6 kbit/s is simply not efficient.

When working with only one B channel, the response time using ISDN transfer technology is much faster. B channels are the digital transfer paths of an ISDN connection which carry *payload data* such as voice, data or video information at 64 kbit/s.

ITK's second-generation active ITK boards have automatic data compression capability. As a result, they can achieve a throughput performance that is 2 to 4 times faster per B channel.

Thus, with the **ITK NetBlazer 4400** and only one B channel, a wide range of applications may be operated at speeds that are acceptable for PC users accustomed to a LAN environment.

You can also use **ITK NetBlazer 4400** to transmit large quantities of data in a short time. By using *both* B channels of your ISDN base connection for the LAN interconnection (which is possible without additional hardware), you can achieve a physical transfer bandwidth totaling 128 kbit/s (without data compression).

You can also upgrade the *ITK Basic* board (requirement: 4 MB) to *ITK Octo* by adding an expansion board. This provides 8 B channels, and therefore a 512 kbit/s transfer bandwidth at your disposal. With *ITK Primary*, you can use 30 B channels in the ISDN at the same time and support up to 30 simultaneous physical connections to remote LANs.

This manual is intended for a network administrator who is responsible for one or more LANs and their external communications. The administrator should have extensive experience with virtually all LAN-related subjects.

How this Manual is Organized

- **Chapter 1** provides an **overview** of the scope of the product, the installation requirements, and several possible application scenarios for a LAN-LAN interconnection. Performance and Routing features are also explained in this chapter.
- **Chapter 2** describes the **installation** of ITK NetBlazer 4400.
- **Chapter 3** explains the **configuration** of the router. It shows you how to install, configure and test the WANODI and Virtual Ethernet ISDN drivers, as well as the call destinations for both interfaces.
- **Chapter 4** describes the **operation** of the router. It shows you how to handle and monitor connections, display journals and statistics, and evaluate them.
- **Chapter 5** provides a detailed **reference** about all settings and parameters of the various router menus.
- **Appendix A** shows you how to use WAN connections with NetWare 4.1 effectively, taking the NDS design and time synchronization into account.
- **Appendix B** explains how to use the different **ITK boards** from ITK Telekommunikation AG, and what you can expect in terms of performance.
- **Appendix C** provides a detailed explanation of **messages** and tells you how to correct errors that occur.
- The exhaustive **index** allows you to find your way around quickly in the manual so you can answer questions that occur during installation or operation, quickly and efficiently.

For more detailed information concerning the *ITK boards* themselves, specifically installing and operating them, as well as fundamental aspects of the ISDN technology and ISDN interfaces, please see the *Installation and Interfaces* manual for your *ITK board*.

After installing **ITK NetBlazer 4400**, you are ready for business. *Good luck*!

Sincerely, ITK Telekommunikation AG

By purchasing **ITK NetBlazer 4400**, you have acquired the right to use the software for **only one** installation! You may make a backup copy of the software you purchased, but if you wish to make several installations, you must **purchase a separate license** for each one. Violation of the rules governing the use of ITK software is subject to criminal prosecution.

1 Before you start

1 Before you start

This chapter provides you with an **overview** of the products, describes how the manual is organized, and helps you find your way around the manual efficiently.

In this section you will find

- a description of the **manual elements** and how they facilitate using the manual
- the PC **requirements** which must be met before the router is installed
- the **performance** and **routing features** of the products
  - ➪ ITK NetBlazer 4400
- an introduction to the ways in which the ISDN-LAN connection can be used
- a summary of the **background knowledge** needed for setting up, using and administering the router
- a brief description of the **ISDN network products**
  - ➪ ITK Columbus Client (formerly known as ITK connect/WS for Windows 95/NT 4.0)
  - ➪ ITK FaxWare
  - ➪ NetWare CAPI Manager

Please read this chapter carefully to take optimal advantage of the extended functionality provided by the ITK NetBlazer 4400.

1.1 How to use this Manual

Various features are employed consistently throughout the manual to facilitate its use.

Header

In addition to the page numbers ("1-2" means Chapter 1, page 2), the header also contains the current chapter and section number on left-hand (even-numbered) pages. On the right-hand (odd-numbered) pages of text you will find the *title of the current chapter* to guide you when you want to leaf through the manual.

On the even-numbered pages you will see the *version number of the ITK NetBlazer Products* on the right side of the header.

Note

Important information is shown with a gray background as follows:

> The gray background indicates an important point that you should not skip over.

Special note

Information that, if ignored, could easily lead to problems, is indicated by an exclamation mark symbol:

> This item is especially important. Ignoring this information may very quickly lead to problems or cause the product to malfunction!

Bold or *italic type*

Bold and italic type are used to **highlight** or *emphasize* information.

Expressions in angle brackets <>

Expressions in angle brackets refer to keys on your computer keyboard, for example: <Enter>.

They can also be used for the contents of variables, for example: <name of the primary server>.

General operating steps

Operating steps are presented as follows:

(1) Turn on your PC.

(2) [next operating step]

(3) [... additional operating steps]

(4) ...

Operating steps with text entry

Operating steps in which text is entered on the screen and keys that are pressed are presented as follows:

```
c:\>copy *.*
```

Enter the characters shown in **bold** type and press the <Enter> key.

1.2 ITK NetBlazer: Product Information

This manual describes the functionality of the ISDN routers.

- **ITK NetBlazer 4400**

The **ITK NetBlazer 4400** offers a highly-flexible solution for LAN Connectivity and Internet Access. Optimized for ISDN connectivity, remote peers may also access the system with a modem or GSM (European Mobile Phone) connection. A unique flexibility assures an optimal operation in small, medium, and large companies.
Both products are based on the Novell *NetWare MultiProtocol Router 3.1* and on the second generation of high-performance ITK ISDN boards. By optimally matching the two platforms, ITK offers a cost-effective, flexible and reliable solution for LAN-LAN interconnections and for connecting to remote workstations.

Introduction

In the age of Internet and global communication there are no longer limits in a LAN. The companies communicate via public networks (ISDN, Frame-Relay, X.25 and analog) and therefore have access to current information at any time. It doesn't matter whether the communication partner is located at home, with the client or in a subsidiary on another continent. Basically, there are two different options for global communication: to set up and use a private network, or to use existing public networks.
The largest existing public network is the worldwide accessible Internet. A connection to the Internet is established via an ISP (**I**nternet **S**ervice **P**rovider). ISPs usually provide POPs (**P**oint **O**f **P**resence) in the local area, offering economical connections and communication. The advantage of the Internet is the widespread distribution which makes it possible to communicate with clients, business partners, and suppliers all over the world.
A private network, an Intranet, has greater security and reliability over a WAN (**W**ide **A**rea **N**etwork). The transmission quality does not depend on the Internet Service Provider but on the infrastructure.
For most companies, it is useful to implement a mixture of the previously mentioned options for communication. In this way the internal communication will be executed via the Intranet and the external communication via the Internet. The result is a perfect unification of both methods. As the **ITK NetBlazer 4400** provides two different interfaces, the Intranet structure can be highly optimized for the companies purposes in LAN-LAN connectivity and Remote Client Access.

1.3 Application Scenarios

With **ITK NetBlazer 4400,** you open the world of data communication to your local network by using the WAN medium ISDN.

Remote Access via an analog modem and/or GSM connection is also possible if the ITK NetBlazer 4400 is equipped with an optional ITK MultiModem board, or an ITK DigitalModem board together with the ISDN boards ITK Octo or ITK Primary (see table on page B-2).

Three typical scenarios are described in this section:

- Setup of a corporate Intranet
- Remote access connections
- Internet Access options

These scenarios may be combined in accordance with individual needs.

1.3.1 Setting up Intranet

The following scenario describes recommendations for setting up a WAN infrastructure: Two distant LANs are connected via the ISDN to form a corporate Intranet.

Objectives

The “Jones Construction Equipment Manufacturing Company” in *Oldville* wants to allow its subsidiary in *Newville* access to current data. This makes it easier for the sales staff to conduct their daily business such as writing offers, confirming dates of delivery, or investigating unfulfilled offers.

ISDN was the solution made for the WAN because the connection will be established for less than 4 hours a day. Therefore it is not reasonable to set up a leased line. Using a modem is not acceptable because its highest speed does not fulfill the requirements.

The network in Oldville is an Novell network with 50 users. In Newville a Novell Server with 10 users is installed.

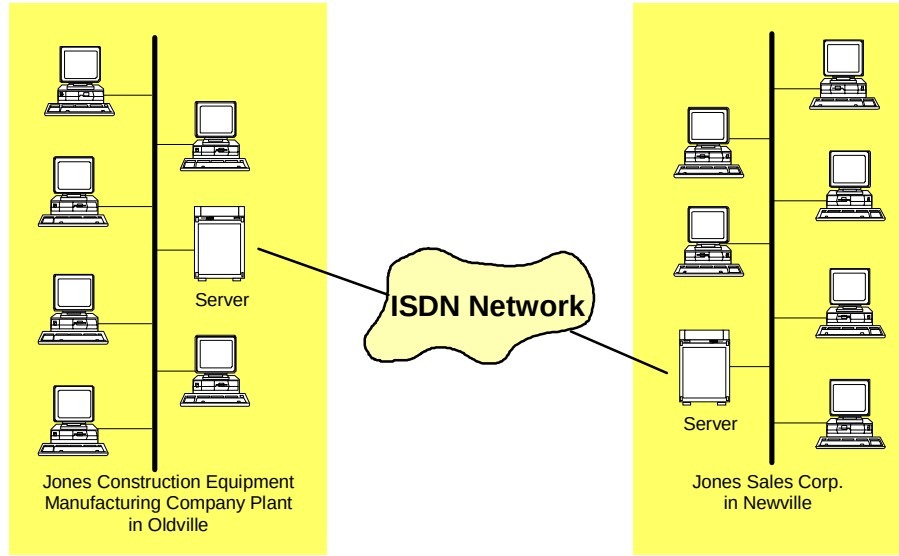


Fig. 1-1 Typical application scenario for an Intranet via ISDN

Solution

ITK NetBlazer 4400 is the right solution because it is cost-effective as well as simple to install. A LAN interconnection connects networks transparently. This means that the user doesn’t need to be trained. The user in Newville will not notice any difference whether he is accessing the server in Newville or Oldville. Differences in access time can be noticed only while accessing large files.

In Oldville, an **ITK NetBlazer 4400** and an ITK Basic board are installed. This system has future expansion capabilities. In case a connection to the Internet is planned, programs such as Novell GroupWise or Novell Web Server can also be installed. In case a network-wide fax solution should be used, ITK FaxWare can be installed on this server as well. ITK FaxWare also accesses the ISDN hardware installed in the server.

In Newville, the file and print server is also used as a router because the 10 users rarely access the server PC. With the **ITK NetBlazer 4400,** this parallel operation doesn't produce a noticeable server load.

1.3.2 Remote Access: Connecting Individual PCs to the Corporate Network

The **ITK NetBlazer 4400** permits PCs to be connected transparently to the corporate network. Telecommuters or local employees can directly dial into the LAN from remote locations and do the following:

- Send and receive E-Mail
- Access shared databases
- Perform file transfers
- Hosts connection
- Network management
- Groupware applications

In this way, all employees have the same access to the LAN as any other user.

Objectives

Some employees need to do some of their work at home, and they need to be able to access the corporate LAN from home. The programs which they will be using are installed locally on the employees' home computers. The ISDN network is used solely for the purpose of exchanging data.

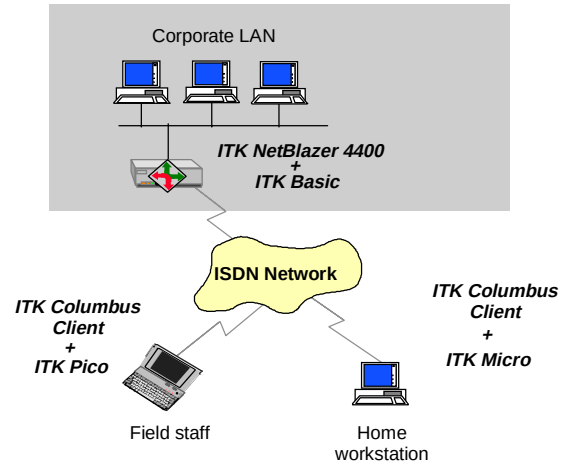


Fig. 1-2 Remote access with ITK Columbus Client (formerly known as ITK connect/WS for Windows 95/NT 4.0)

Solution

An **ITK NetBlazer 4400** is installed with an ITK Basic board at the corporate headquarters. Of course, if there are to be more than two remote sites, ITK Octo (4 x BRI) or ITK Primary (1 x PRI) active ISDN boards can also be used. Passive boards, either the ITK Micro or the ITK Pico, are used at the remote sites. The ITK Columbus Client (formerly known as ITK connect/WS for Windows 95/NT 4.0) software, which is available for DOS / Windows 3.1x / Windows 95 and Windows NT 4.0, is used for this purpose. This approach permits users to access the corporate network just as if they were actually working directly on the LAN.

If an ITK MultiModem board (together with ITK Octo or ITK Primary) is installed, users can also gain access with a modem and/or GSM connection (see table on page B-2). Independent from the access media, only one dial number is necessary.

If the level of traffic is expected to be high or if security requirements are high, employees who access the LAN remotely should use active ISDN boards.

Advantages of this solution

- Completely integrated in the Novell technology, so that access is totally transparent to the user
- Optimized for ISDN by eliminating the physical connection if no user data is transferred
- Extensive security mechanisms such as calling line identification, password protection, Ethernet address check, callback and optional authentication and encryption
- Based on the CAPI 2.0 standard thus allowing the ISDN board to be used by additional applications
- Interoperable with other third-party products (Cisco, 3Com, Windows NT) utilizing the PPP (Point-to-Point Protocol)

1.3.3 Internet Access: Your Entrance Ramp to the Information Superhighway

With its support of the TCP/IP network protocol, **ITK NetBlazer 4400** is ideally suited for connecting your company to the worldwide computer network Internet. You can explore the numerous options once you are connected to the Internet:

- Install a mail server. With a mail server you are accessible to all your customers and companies throughout the world via E-Mail.
- Use the countless options offered by the WWW (World Wide Web) to get a jump on the competition in the information game.
- Install your own WWW server to make your products and services available around the clock to the 30 million Internet users.

Objectives

The existing Novell network can be connected to any Internet Service Provider (for example, EUnet) via ISDN. Any employee should be able to access the various Internet services, such as the WWW, E-Mail, FTP (**F**ile **T**ransfer **P**rogram) or Telnet (remote access to host systems) from their own workstation.

Solution

An ITK Basic board will be installed in an existing Novell server and an **ITK NetBlazer 4400** is also installed. In addition, a standard TCP/IP application is required at every workstation that permits access to the Internet. An example of such an application is the Netscape browser included in IntranetWare.

Advantages of this solution

- The full ISDN 64 kbit/s bandwidth is used.
- The extensive PPP support makes it possible to connect to any desired Internet Service Provider.
- Internet access is administered from a central location.
- Security functions, such as firewalls (packet filter and proxy server), apply to the entire network, thus preventing unauthorized access to your LAN.
- Only *one* Internet access is required for the entire company.

- Costs are only incurred at one site, which makes them much easier to monitor.

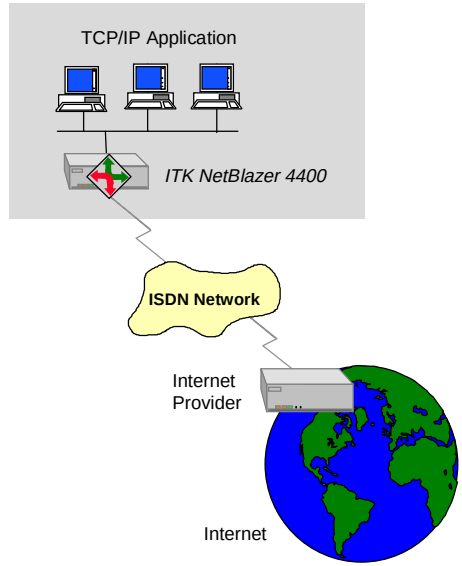


Fig. 1-3 Internet access with ITK NetBlazer 4400

1.4 Requirements for the Router PC

Even though the ITK NetBlazer 4400 is designed for Novell networks, it also supports various network protocols used by other systems, which makes it suitable for more demanding network configurations and heterogeneous corporate networks.

Therefore the ITK NetBlazer 4400 can be installed in various environments.

You can install the ITK NetBlazer 4400

- on a dedicated PC running under NetWare together with the Novell MultiProtocol Router respectively running under Novell IntranetWare.
- on an existing NetWare server together with the Novell MPR respectively on an existing IntranetWare server.

The minimum requirements for a NetWare server are

- a PC with 80486 processor and a CD ROM drive, at least 24 MB RAM, 120 MB NetWare partition, and 50 MB of additional free hard disk space.
- at least one active ITK board (ITK Basic, ITK Octo, ITK Primary) or a passive ITK board (ITK Micro 2.x)
- the NetWare 4.x or 3.12 operating system and the Novell NetWare MPR 3.1, **or** the Novell IntranetWare operating system

1.5 Performance Features of ITK NetBlazer 4400

1.5.1 Security

Security precautions are very important when setting up Intranets and connections of local networks to the Internet. By connecting field staff or clients to a local network or an Web server opened to the public, the usual firewall and security aspects of the local network are compromised. New dangers and risks may be encountered, for example viruses or potential intruders. The following information explains the security features of the ITK NetBlazer products, which prevents these dangers and risks, and works as securely in a WAN as in a LAN.

- **Calling line identification on incoming calls**

  The calling subscriber number is transmitted in ISDN. This number is compared to an accepted number list even before a connection has been established. If the calling subscriber number is present in the list, the connection will be established. If not, the connection request is rejected.

- **Callback**

  The callback may be performed if, for example, the remote location initiates a connection request. The router of the head office recognizes the incoming call according to the dial number transmitted in the D channel. It will then compare this information with the corresponding partner configuration. If the partner has activated the Callback option, the incoming call will be rejected and the remote partner is called back. In this way, no charges occur for the subsidiary and all charges are captured centrally.

- **Checking of the MAC address or the LAN segment**

  Each node in an IPX network has its MAC address (also node or layer2 address) and is located in a LAN segment, which has also a defined network number. The IntranetWare security features can require that individual users login only with a specified MAC address or from a defined LAN segment.

- **Firewall functionality**

  Within a network, a firewall is used to prevent unauthorized access to a network. This problem usually appears when a secure network is connected to an insecure one (for example, Internet or public WAN). A common solution for setting up these firewalls is the installation of a packet filter (screening router). Such a packet filter checks, according to defined rules, the incoming and outgoing packets, and decides if the packet corresponds to the rules and will therefore be forwarded to the remote partner.

  In this way, for example, E-Mail packets will be passed only for communication between Internet and E-Mail server. The E-Mail packet will not be forwarded if this E-Mail is destined for a different address.

- **Authentication mechanisms: PAP and CHAP**

  PAP is a simple standardized authentication protocol. During the establishment of each connection, the user ID and a password are exchanged and checked by the router of the remote partner. PAP does not encrypt the user ID and the password. CHAP is a standardized authentication protocol as well. The difference PAP and CHAP is the encryption of the user ID and password.

1.5.2 Cost efficiency

One of the most important features in using ISDN dial up lines in a WAN is cost efficiency. If the implemented solution offers many advantages in this application field, an investment that might be more expensive in the beginning pays for itself in a short time. With several years of experience and a deep integration in IntranetWare, the ITK solution offers many features in this application field and will therefore pay for itself within a short time.

- **Data compression**

  The higher the speed of a data transmission via the ISDN network, the lower the transmission costs. Also the response time is improved and therefore the satisfaction of the user as well. ITK products use a proprietary algorithm for their data compression. This algorithm is similar to the V.42bis algorithm known in the “modem world”: The data is compressed directly on the ISDN board. This procedure offers compression rates up to 1:5 (depending on the type of data). As a result, the ITK solution is superior to all available ISDN solutions. By executing the data compression on the ISDN board, the server or router PC is therefore available for other tasks.

Additionally, the ITK NetBlazer 4400 offers compression for PPP connections.

- **Channel bundling**

  To raise the transmission rate further, the B channels of an ISDN connection can be bundled logically. ITK has implemented, apart from a static channel bundling, a dynamic channel bundling: Depending on the data load or protocol to be transmitted, the B channels are added or removed.

- **Charge and time dependent Inactivity Timeout (Short Hold)**

  The charge and time-dependent inactivity timeout assures that while the ISDN connection is established, charges are only incurred when user data is actually transferred. This is very important for ISDN because the charges incurred depend on the call duration.

  Two different inactivity timeouts are possible:

  1. time dependent inactivity timeout

     The connection is released after a defined duration if no data has been transferred.

  2. charge dependent inactivity timeout

     The router checks the charge signal transferred in the D channel (available only in Germany) and will terminate the connection if no data has been transferred for a defined duration just before the next charge signal is due.

Even if the physical line is released between the peers, the connection on both sides is logically treated as if it was already established. In the case of a new data transmission request, the physical connection will be re-established automatically and transparently for the application.

- **Filtering and Spoofing**

  At the beginning of the NetWare development, it was assumed that all nodes of a network would be connected to a LAN. The available bandwidth was less important. Some small recurrent data packets (all 30 to 60 sec) were not important in local networks. Examples for these data packets are IPX Keep Alive Packets, SPX Keep Alive Packets or Novell Serialization Packets. If these packets are transmitted over an ISDN connection, higher charges are incurred: The ISDN connection is established every 30 to 60 sec (depending on the Short Hold) or remains established all the time.

  Filtering: To prevent such an cost intensive procedure, all outgoing data packets are examined. Some packets such as Novell Serialization Packets are dropped.

Spoofing: Other types of packets, for example IPX or SPX Keep Alive Packets cannot be filtered without problems. After transmitting those kind of packets, the sender expects an appropriate answer from the remote partner. The router now creates the expected answer by itself without establishing the connection. Such a reaction is called spoofing.

In every case packets are only filtered or spoofed if the line is not established physically. During an established connection, all packets are transmitted regardless of their function.

- **Time restrictions for each remote partner**

  To prevent unexpected high charges to a remote partner, time restrictions can be defined for those partners. In this way, the connection establishment to a remote partner can be locked for a pre-defined period (for example on weekends or overnight). If a connection establishment is requested, it will be ignored and a warning message is displayed in the Journal Window of the ISDN Communication Manager.

  The user may select between three different restriction values, for example to suppress NDS synchronization caused calls.

- **Charge accounts for each remote partner**

  Similar to time restrictions, it is possible to define a maximum value for the duration of the connection or for recurring charges (one-time, per day, per week or per month). If a defined value is exceeded, subsequent connection requests are ignored and a warning message is displayed in the Journal Window of the ISDN Communication Manager.

1.5.3 Interoperability

The ITK NetBlazer 4400 and previous ITK products offer two different protocols to communicate with different types of remote partners.

1. With a different ITK networking product such as ITK NetBlazer 4400 via the specific **Virtual Ethernet protocol (ITK X.75 protocol)**.
2. With most third-party router products such as Ascend, Cisco, Windows 95/NT, Bay Networks, and 3COM, if these products support the standard **PPP** (Point-to-Point Protocol).

- **Virtual Ethernet protocol**

The Virtual Ethernet protocol has been specially developed by ITK to maximize the full performance of the ITK ISDN boards and the ITK remote access products. The Virtual Ethernet protocol supports high-performance data compression and enhanced security mechanisms.

You should always use the Virtual Ethernet protocol between two ITK NetBlazer products, since this will allow you to use the high-performance data compression implemented on ITK ISDN boards. This data compression increases transfer rates and reduces connection costs.

- **Point to Point Protocol PPP**

In recent years, PPP has developed into a quasi standard for analog and digital WAN traffic communication. All leading hardware and software manufacturers, as well as Internet Service Providers, support this standard. The PPP specification was developed through Internet standardization committees. It is documented in documents called RFCs (**R**equest **f**or **C**omment).

The ITK NetBlazer 4400 supports the following RFCs:

Protocol	Specification Number
Point-to-Point Protocol	RFC 1661
PPP Internet Control Protocol (IPCP)	RFC 1332
PPP Internetwork Packet Exchange Protocol (IPXCP)	RFC 1552
PPP in HDLC Framing	RFC 1662
PPP Multilink	RFC 1717
PPP Authentication Protocol (CHAP and PAP)	RFC 1334

The following listing provides a precise summary of the range of PPP features offered on ITK NetBlazers:

- IP Address Negotiation
- Channel Bundling using the Multi Link Protocol MLP
- Authentication protocols CHAP and PAP
- Data compression
- Callback functionality

These extended PPP integration facilitates problem-free operation with most third party router products supporting the standards.

1.5.4 Expandability

Most users start with a small solution and expand as they go. For this procedure, it is important that the products chosen are expandable and scalable. Due to their modularity, ITK NetBlazer products offer this possibility.

- **Hardware Expandability**

  ITK NetBlazer 4400 supports all active ITK ISDN boards, the ITK Modem boards, and one passive ITK ISDN board:

  - ITK Basic
  - ITK Octo
  - ITK Primary EISA
  - ITK Primary PCI
  - ITK MultiModem
  - ITK DigitalModem
  - ITK Micro 2.x

  Up to four of these ISDN boards can be combined. This means that the ITK NetBlazer 4400 is scalable from 2 B channels (1 ITK Basic) up to 120 B channels (4 ITK Primary). Simply determine your requirements.

- **Software Expandability**

  One of the big advantages of ITK NetBlazer 4400 is the expandability by other applications running in parallel. These are other ISDN applications such as ITK FaxWare, which also access the ISDN hardware installed in your router. Furthermore, all applications available under IntranetWare can be operated in parallel with your ISDN router software. Examples are the Novell Webserver, Novell GroupWise, and NetWare for SAA. In this way, a PC used only for routing can be expanded to an IntranetWare communication server.

  A special feature of the ITK NetBlazer 4400 is the NDS integrated user authentication support of NetWare Connect. An incoming dial-in client will be authenticated independent of its destination by its system ID and remote password.

1.5.5 Management and Monitoring

The ISDN Communication Manager offers the following:

- **Overview about Status and Charges**

A detailed overview displays the current connection status for all connections. At a glance, you can check the charges accumulated for all connections as well as the charges for one connection.

- **Journal and Accounting File**

All operations with regard to connections and disconnections, errors, and messages are displayed in a Journal Window. Furthermore, all entries in this window are written to an Accounting File and are available for manual or automatic editing.

- **Detailed Statistics**

  The network administrator can refer to the ISDN Communication Manager for optimizing charges, and performance and accessibility of a WAN based on ISDN. Detailed information on each configured remote partner is displayed: transferred bytes and/or packets, duration of the connection, duration of the Short Hold, average logical connection time, number of B channels used, data transfer rate, and the total charges.

- **Analyzing Tools**

  Even in a stable configuration, it is sometimes possible that a packet sent during a connection causes charges that are hard to understand. This can happen within large networks or if a print server, modem server, or a similar device offers its service to the network. ITK NetBlazer 4400 has a feature that interprets and, at the same time, displays detailed information on a packet in the Journal Window.

  Another analysis opportunity is the partner-dependent storage of transferred data packets in a file. This file has been created according to the LANalyzer for Windows format and can therefore be analyzed with LANalyzer for Windows.

- **CAPI (COMMON-ISDN API)**

  Another important feature is the support of the CAPI standard. Since the beginning, ITK has always supported this important ISDN standard. ITK supports not only the standard CAPI 1.1, introduced some time ago, but also the new CAPI 2.0. With the support of CAPI 2.0, ITK offers, at the same time, support of the Novell CAPI Manager. This enables simultaneous operation of all programs developed for CAPI 2.0 and Novell IntranetWare with the ITK NetBlazer on one Novell file server.

1.6 Routing Functionality Features of ITK NetBlazer 4400

The ITK NetBlazer 4400 offers different connection types, transfer protocols, and interface-specific features which guarantee a highly flexible use of the system based on individual needs.

This section gives you a brief overview of the functionality and the handling of the ITK NetBlazer 4400.

Virtual Ethernet and WANODI connections

The ITK NetBlazer 4400 provides two ISDN interfaces: **WANODI** and **Virtual Ethernet**. The main difference between these two drivers lies in the characterization of an ISDN connection. While the Virtual Ethernet driver regards ISDN as a dedicated network; in a WANODI environment, the ISDN only represents one single line, similar to a cable connection.

1.6.1 Virtual Ethernet Concepts

In a LAN-LAN connection, each of the two routers sees the ISDN as an *independent network,* which can be accessed by a multitude of systems and can be used to access additional networks that are themselves connected to the ISDN. In this approach, the ISDN is addressed through its own *network address.*

The Virtual Ethernet also connects Remote Access Clients to a LAN by allowing a virtual For a user, the ISDN network is completely transparent such that there is no difference between a local and a remote access.

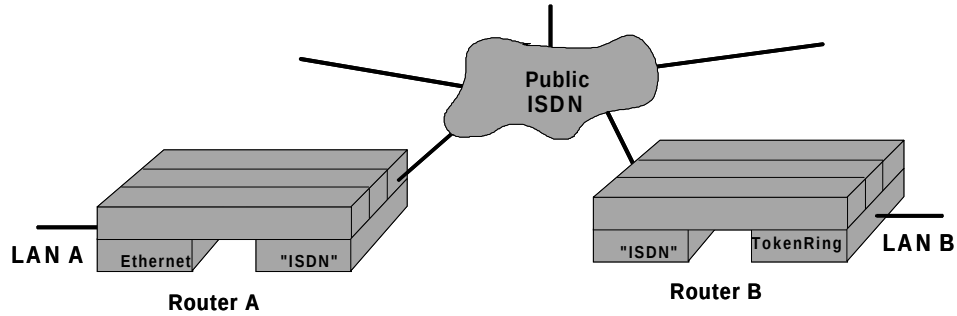


Fig. 1-4 The interconnection of two LANs by means of the ISDN using two routers to form a “virtual network”

Fig. 1-5 shows a specific example of three Novell LANs which are interconnected via the ISDN using three routers. This example shows the importance of having an unambiguous network address for the ISDN.

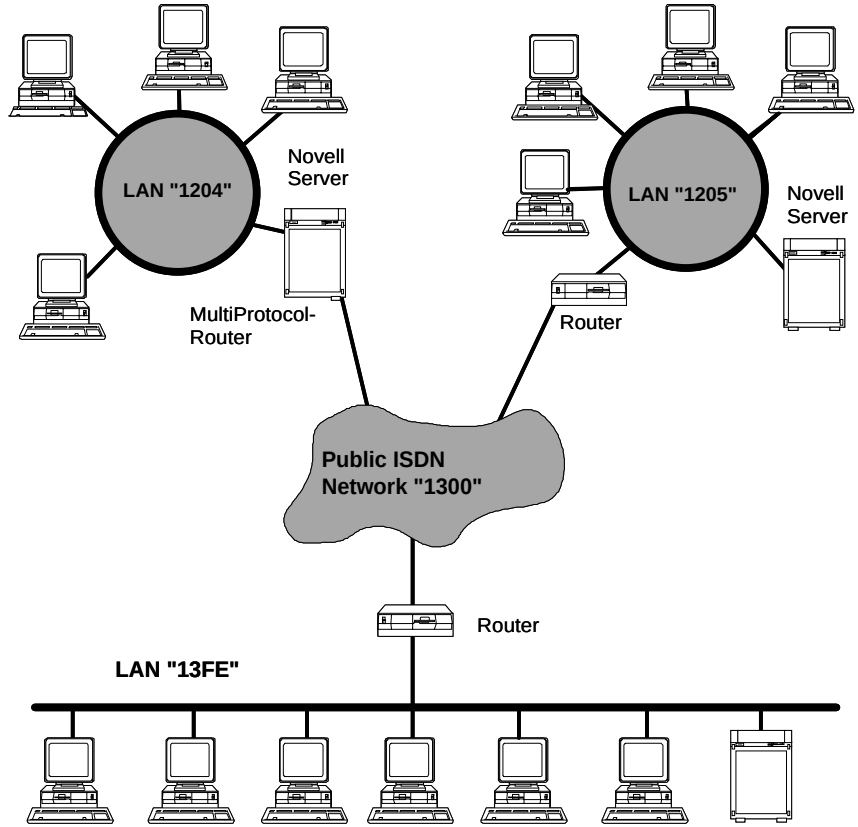


Fig. 1-5 Example of network addresses of three Novell LANs interconnected via the ISDN

In this example, the network addresses (for the Novell LAN IPX protocol) have been arbitrarily named “1204”, “1205” and “13FE” (hexadecimal display), and the ISDN network address has been named “1300”. In this case, the “1300” network has only three nodes: namely, the three ISDN routers. Thus, when setting up the integrated network, the IPX network address “1300” must be declared for the “ISDN links” of their network (see Fig. 1-5). Of course, each of the three ISDN boards which comprise these ISDN legs are assigned their own IPX *node address*, as explained in Chapter 3, *Configuring ITK NetBlazer 4400*.

If the networks in the above example were TCP/IP networks rather than IPX networks, the network addressing would be analog: An IP network address would then be assigned to the ISDN.

Virtual Ethernet Interface features

- **Remote Access**

The Virtual Ethernet interface allows remote workstation connectivity as well as Internet access and LAN-LAN interconnection. An individual PC connecting to its corporate LAN may access the system via ISDN, analog Modem, or a GSM-conforming mobile phone connection.

- **IP Address Negotiation**

Remote Clients using TCP/IP applications such as Netscape do not have to configure static IP addresses on their client stations. If they connect via the Point to Point Protocol PPP, an IP address will be assigned automatically during the call setup process and remain valid for the entire call duration. The number of available IP addresses and the address range is based on network needs.

- **Shared use of B channels**

In a typical network access situation, a client only needs periodic access to a LAN, but most of the time that line would still be unavailable even when not in use.

The inactivity timeout feature of the Remote Access Router 4000 enables the sharing of B channels so that an unused B channel may be accessed by other clients. This feature increases the accessibility of the system and allows better utilization of hardware resources.

- **Virtual LANs**

The Remote Access Router 4000 allows the ISDN “Network” to be divided into up to ten Virtual LANs. The Virtual Ethernet driver will be configured for each of these virtual LANs using a separate IPX Network address. This enables a routing function between ISDN partners.

Summary

You should use Virtual Ethernet ISDN connections if

- you want to interconnect Remote Workstations via ISDN
- you want to share B channels between multiple destinations

1.6.2 WANODI Concepts

In the WANODI concept, the ISDN is a *single* connection between two routers, which are used to exchange data packets with the remote LAN. The fact that this connection is established via the ISDN is irrelevant with regard to the two routers.

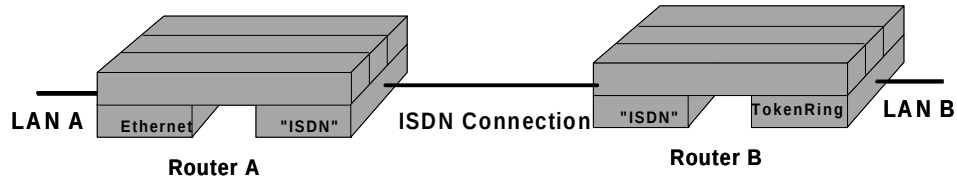


Fig. 1-6 The interconnection of two LANs using two routers via the ISDN with a WANODI connection

WANODI Interface features

- **Reserved B channels**

An ISDN B channel is reserved for the duration of a LAN-LAN connection between two routers(i.e., for every connection, a B channel must be available). Connections with continuous traffic or high priority connections should be connected via the WANODI interface. The inactivity timeout feature to minimize connection costs remains active.

- **Extended Routing functionality**

With regard to IPX and TCP/IP, WANODI connections support other network protocols such as Appletalk Routing or Source Route Bridging, and the NLSP or OSPF protocol.

- **Novell MPR integration**

The WANODI interface is deeply integrated into the MultiProtocol Router from Novell and supports all its features, such as an extended firewall functionality or static IPX routing. The line establishment handling of WANODI connections is performed by the Novell Call Manager Utility.

- **Flexible IP WAN connections**

When using IP for transferring data, for example to establish an Internet connection, two different access procedures are available:

- An unnumbered point-to-point-connection
- A numbered single point-to-point-connection

This gives you the maximum compatibility for most Internet Service Providers and various router systems.

With unnumbered point-to-point-connections, a unique IP address is not assigned for the ISDN connection. This means that your router is connected “directly” to the desired **remote partner**. The ISDN “cable connection” does not, like within a LAN, have its own address.

With numbered single point-to-point-connections, a unique IP address will be assigned for the ISDN “cable connection”. In this way network A will reach network B (for example, Internet) with a second, independent IP address via ISDN.

You can choose one of these connection options: Depending on whether or not your Internet Service Provider assigns an IP transit address or an IP gateway assigns an address to you.

Summary

You should use WANODI connections if

- you want to interconnect networks via ISDN
- you want to reserve B channels for a corresponding connection
- you want to route other protocols than IPX and/or TCP/IP
- you want to use unnumbered TCP/IP connections
- you want to use the full range of Novell MPR 3.1 functions

1.7 Static Routes and Routing Protocols

The standard delivery scope of ITK NetBlazer 4400 includes the Novell MultiProtocol Router 3.1, which offers two options for generating the required routing information for all routable protocols such as IPX, TCP/IP and AppleTalk:

- You can configure static routes and utilities manually.
- You can use a routing protocol.

The advantages and disadvantages of both approaches are summarized below.

The following recommendations apply to normal dial-up connections which result in charges depending on the connection time. The idea is to minimize costs for such connections.

If you use a leased line or a router connection in a PBX system, so that charges are not calculated based on connect times, you can safely use the dynamic version.

1.7.1 Static Routes

The advantage of using static routes instead of a routing protocol is that no routing and service information is exchanged via ISDN: This will always result in a lower telephone bill. However, the problem is that changes in networks – for example, the installation of new servers and new network segments – will not be immediately apparent on the remote end of the ISDN connection. Thus, using static routes will result in higher administration costs compared to the dynamic approach.

1.7.2 Routing Protocols

When routing protocols are used on the ISDN line, the disadvantages of the static routes become advantages, and vice versa. If your networks are changing dynamically, use ISDN routing protocols to reduce your administration costs. If you do this, however, you will have to accept the fact that the communication of routing information will sometimes cause physical connections to be established, which will result in additional communications charges.

Recommendation

- Use static routes if your networks are of a static nature.
- Configure only necessary routes and services to the remote side.
- Use the program FILTCFG to filter all unnecessary packets from IPX nodes, IP hosts, or network boards that will not require any access to the remote side.

1.8 Masquerading

Masquerading is the ability to connect LANs to the Internet with only one officially assigned IP address enabled by a function called “port mapping“.

The advantage: You reduce the costs of the official IP addresses, and the amount of users that will be able to connect to the Internet is unlimited.

1.8.1 Functionality

The masquerading module evaluates the IP addresses and ports in the TCP/IP headers and replaces them with the official IP address.

Example:

The Router is connected to the Internet, the “Provider“, and with a local network (for example, Ethernet) in the following example. The PCs in the local network have to configure the Router as a “Default Router“.

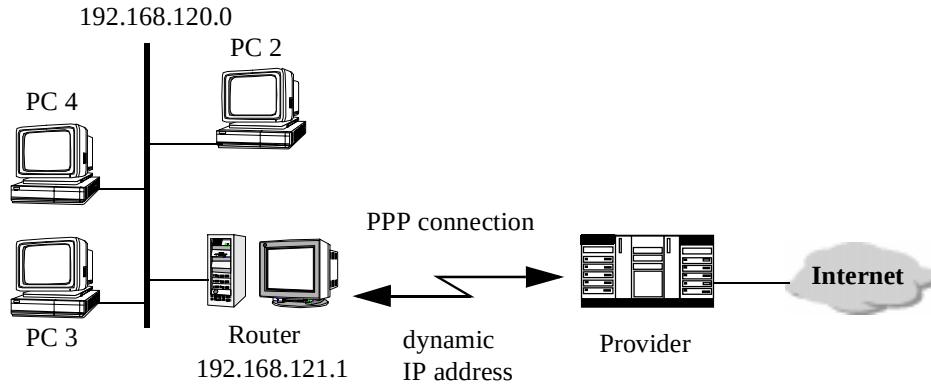


Fig. 1-7 Example for a network with IP masquerading

If PC 2 wants to access a Server anywhere in the Internet, it sends TCP/IP packets to the router. The router manipulates the IP source address and source port by replacing it with the masquerading IP address and a dynamical port, and then forwards the packet to the provider.

The answer from the host is returned to the router, which can determine the destination using the dynamical port.

IP Acception

One of the key features of the ITK NetBlazer 4400 is the use of an IP address that was dynamically assigned by remote router.

This feature together with masquerading allows you to connect a small LAN to the Internet using a personal connection.

1.9 Other ISDN Network Products

1.9.1 ITK Columbus Client

The ITK Columbus Client software package allows remote workstations to connect to your corporate LAN via ISDN. Telecommuters or field staff can use PCs or notebooks to dial in to the LAN directly. This allows them to send and receive E-Mail messages or to access shared data. The ITK Columbus Client software allows transparent connections to a remote LAN so that you can implement additional approaches utilizing groupware applications such as Lotus Notes or Novell GroupWise. Since the ISDN board supports Novell ODI technology, it functions like a normal network board and supports the most important protocols such as IPX and TCP/IP. This means that the user can work on the road in the same way as they would work in the office.

One application scenario for connecting a remote workstation to the corporate network is described in Chapter 1.3.2, *Remote Access: Connecting Individual PCs to the Corporate Network* (page 1-10).

ITK Columbus Client based on standards

The ITK Columbus Client software package is based on the widely used CAPI 2.0 (Common ISDN API) and PPP (Point-to-Point Protocol) standards.

CAPI 2.0 support permits ISDN applications to be used in parallel. This permits multifunctional workstations to be set up for telecommuters. The following additional functions are possible: FAX G3 and G4, Euro File transfer, voice mailboxes, telephone support, and access to online services such as America Online.

By providing extensive PPP support, ITK offers interoperability with third-party products. All the leading manufacturers such as Novell, Cisco, Microsoft, 3COM, and Bay Networks support this standard. PPP also permits interconnection to the Internet.

Security mechanisms provided by ITK Columbus Client

Security is crucial when you set up a remote access server. The ITK Columbus Client software provides various security levels to protect the local area network from unauthorized access. Security begins with a simple ISDN-specific calling line check. The common NetWare security mechanisms such as prompts for passwords, time restrictions, and the Ethernet address check are also used.

In addition, a callback option can be used. A firewall can be set up using the extended filters of the ITK NetBlazer products. With a firewall, all transferred data packets are tested according to predetermined rules, and all illegal data packets are rejected.

If further security features are required, ITK offers Extended Security Services (ESS) on its ITK Basic boards.

1.9.2 ITK FaxWare

ITK FaxWare is a NetWare based fax solution that fits easily into the Novell network operating environment. Network users can send and receive a fax directly from their workstations, store a fax in the network server, and print them out on the network printer. A mail box (ISDN dialing number) is assigned to each user. The ISDN hardware in the fax server can be used jointly by all network users. The users work from an easy-to-use operating interface. This makes sending a fax as easy as printing a document.

Flexibility

Based on the second-generation ISDN boards, it is possible to operate both B channels on an ISDN line using a single ITK Basic board. This means, for example, that a fax can be sent on one B channel at the same time as another fax is being received on the other B channel. As your needs increase, all you have to do is install additional ITK Basic boards or the ITK Octo expansion board in your computer to permit you to access additional B channels.

Faxing from DOS and Windows applications

Because of the software's high degree of integration in the operating systems (DOS, Windows 3.x, Windows 95), sending a fax is quite simple. To send a fax you simply press the ITK FaxWare "printer" button. All you have to do then is enter the number of the fax machine to which you are sending your message. Before you know it, your fax is on its way. Sending a fax to multiple addresses is also easy with ITK FaxWare. You can use the integrated fax multiple-address and broadcasting function to send your fax to addresses on various distribution lists.

Client-server architecture

Thanks to ITK FaxWare's powerful client-server architecture, the network administrator can take over the entire administration of fax communications (see Fig. 1-8). It is easy for the administrator to access functions such as configuring users, and evaluating send and receive logs.

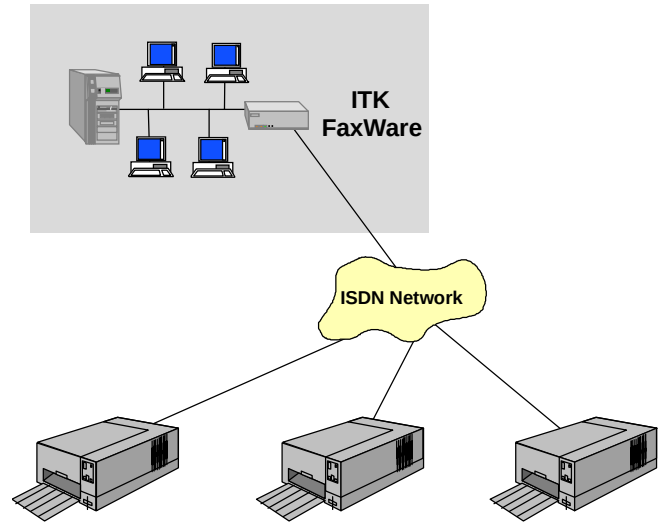


Fig. 1-8 Client-server architecture used in ITK FaxWare

1.9.3 NetWare CAPI Manager

CAPI standard

Applications that use ISDN technology have been available for a number of years. When development work began at the end of the 1980s, these applications were dependent on specific ISDN boards. This meant that application programers had to configure their applications to each individual ISDN board. Faced with these problems, a group of hardware and software manufacturers realized the importance of having uniform standards for accessing ISDN boards. This led to the development of an ISDN programing interface: “Common ISDN API” or CAPI for short. Applications that support this standard do not need to be configured for specific hardware. Moreover, manufacturers of ISDN boards merely need to supply a driver with their product to make it compatible with countless ISDN applications. At first, CAPI was written only for DOS. Today, there are versions for DOS, Windows 3.x, Windows 95, Windows NT, Unix and, of course, NetWare. CAPI, which was created in Germany, is now well on its way to becoming a European and world standard. Major software and hardware manufacturers such as Novell, Microsoft, Cisco, 3COM, Attachmate, Delrina, and Cheyenne are now offering CAPI support for their products.

ISDN under NetWare

The CAPI standard is implemented under NetWare 3.12 and 4.1 under the title CAPI Manager. The NetWare CAPI Manager provides functions for operating client-based ISDN CAPI applications. Thus, applications can request ISDN channels that have specific bandwidths or other properties such as fax-capability.

The NetWare CAPI Manager offers the following advantages:

- Support of standards
- Hardware independence
- Network users and applications on the LAN share ISDN boards (resource sharing)
- Security and administration from a single location
- A high-performance communication server with applications for LAN interconnection, remote access, faxing, Euro Filetransfer, access to online services, etc., can be set up

The NetWare CAPI Manager is an economical, high-performance, hardware-independent communication platform similar to the well-known ODI standard for network boards.

Fig. 1-9 provides a brief overview of the architecture of the NetWare CAPI Manager.

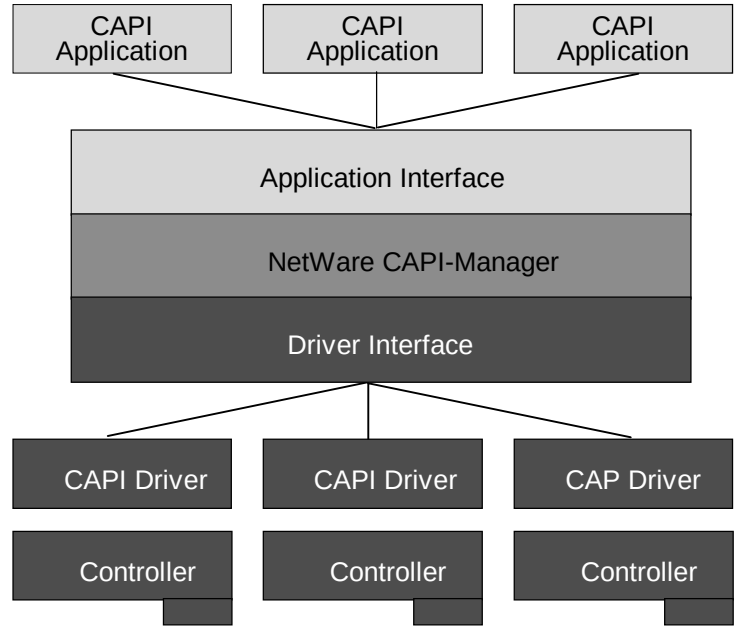


Fig. 1-9 Architecture of the NetWare CAPI Manager

2 Installing ITK NetBlazer Products

2 Installing ITK NetBlazer Products

This chapter covers the installation of

- ITK NetBlazer 4400

You have three options for installing the ITK NetBlazer 4400 on your router PC:

Option 1: Install the ITK NetBlazer 4400 on a router PC running under Novell IntranetWare / NetWare 4.11. This is the recommended installation scenario.

Refer to Chapter 2.2, *Installation on an IntranetWare Server* (page 2-5).

Option 2: Install ITK NetBlazer 4400 on a router PC running under NetWare 3.12.

Refer to Chapter 2.3, *Installation on a NetWare 3.12 Server* (page 2-9).

Option 3: Install ITK NetBlazer 4400 on a router PC running on an existing NetWare 4.10 operating system.

Refer to Chapter 2.4, *Installation on a NetWare 4.1x Server* (page 2-12).

We recommend you install the ITK NetBlazer 4400 on a Novell IntranetWare / NetWare 4.11 server.

2.1 Preliminary Tasks

You must install the ITK NetBlazer 4400 on your router PC.

Router PC means one of the following:

- a dedicated PC
- your NetWare server

Also refer to Chapter 1.4, *Requirements for the Router PC* (page 1-15).

Installation steps

The following installation steps need to be completed before transferring data via ISDN connections:

1. Install the Operating System for your router PC.
2. Install the ITK board(s) in your PC.
3. Install ITK NetBlazer 4400.

This chapter describes the installation of the ITK board and the installation of ITK NetBlazer 4400.

Installing the ITK board

First you install your ITK board(s) in the router PC.

- The necessary steps for installing the active ITK ISDN board are described in Chapter 1 of the *ix1 Installation and Interfaces* manual of your ITK board.
- The necessary steps for installing the passive ITK ISDN board are described in Chapter 1 of the *ITK Micro 2.x* manual.
- The necessary steps for installing the ITK modem board are described in Chapter 1 of the appropriate manual of your ITK modem board.

An installation example of an ITK Basic:

To install the ITK Basic board in a PC, perform the following steps:

(1) Turn off your router PC and remove the power cable connector from the connector socket.

(2) Remove the case from your router PC.

(3) Install the ITK board in an unused slot.

(4) Replace the case on your router PC.

After you have installed the ITK board(s), power up your router PC and switch on the PC.

2.2 Installation on an IntranetWare Server

The following requirements must be met if you wish to install ITK NetBlazer 4400 on an IntranetWare server:

- Your PC must be equipped with a CD-ROM drive.
- The DOS drivers or NetWare drivers for the CD-ROM drive must be installed.
- If you have already completed one or more tasks described in this chapter, you can skip the corresponding sections. A re-installation of the products is not necessary.

Please have the following CDs and diskettes available:

- The NetWare 4.11 Operating System CD
- The ITK NetBlazer 4400 CD
- The NetWare 4.11 / IntranetWare License Disk
- The IntranetWare Communication Engine Disk

We strongly recommend that you install the ITK NetBlazer 4400 on an English language version of NetWare. Several messages and help topics are only supported in this language. Using another language may cause severe problems.

Install the NetWare 4.11 Operating System

Complete the following steps to install NetWare 4.11:

(1) Insert the NetWare 4.11 Operating System CD in the CD-ROM drive of the computer on which you wish to install NetWare.

(2) Change to the CD-ROM drive.

(3) Run the installation program

```
install
```

(4) Complete the remaining steps as described in the Novell installation manual.

Install the ITK NetBlazer 4400

During the installation process the program automatically detects the presence of the necessary Novell MultiProtocol Router 3.1. If you have already installed the Novell Internet Access Server NIAS, the system will bypass the installation of the Novell MPR and will only install the additional ISDN-related files.

To install the ITK NetBlazer 4400 perform the following steps:

(1) Insert the ITK NetBlazer 4400 CD into your CD-ROM drive.

(2) Switch to the *System Console* under NetWare and run the Novell installation program:

```
load install
```

The following screen will appear:

```
+-------------------------------------------------------------+
|                   Installation Options                      |
|-------------------------------------------------------------+
| Driver options    (load/unload disk and network drivers)    |
| Disk options      (configure/mirror/test disk partitions)   |
| Volume options    (configure/mount/dismount volumes)        |
| License option    (install the server license)              |
| Copy files option (install NetWare system files)            |
| Directory options (install NetWare Directory Services)      |
| NCF files options (create/edit server startup files)        |
| Product options   (other optional installation items)       |
| Server options    (install/upgrade this server)             |
| Exit                                                        |
+-------------------------------------------------------------+
```

(3) Switch to *Product options,* and then select *Install a Product not listed*.

A pop-up menu will appear where you can define the desired installation drive.

(4) Press <F3> and enter your CD-ROM drive letter (d: designates your CD-ROM drive letter).

```
d:\
```

The installation starts from the root of the CD.

If you have mounted your CD under NetWare, enter the following path and confirm by pressing <Enter>.

```
NETBLAZER4400:\
```

(5) From the displayed screen, select *Install Product* and press <Enter>.

The *Install to Servers* window will appear. This window lists the servers on which you can install the product. The RSPAWN.NLM must be loaded for a server to appear on this list.

(6) Select the desired server(s) and press <Enter>.

If you want to install the product on a number of servers, you will need a separate license for each installation.

You cannot install the product on remote servers unless you have supervisor access rights to those systems.

(7) Answer `Yes` to the *Start installation?* prompt to begin the installation.

(8) Press <Enter>.

The *Install configuration files to <Server Name>?* window will appear.

(9) Select *No* as your entry and press <Enter>.

(10) Insert the *IntranetWare Communication Engine* Disk in the diskette drive, and press <Enter> twice when prompted.

The ITK NetBlazer 4400 files will now be installed on your system.

After the completion of the installation process, you are notified that the ITK NetBlazer 4400 has been installed successfully.

(11) Press <Enter> to confirm and leave the installation program by pressing <Esc>.

(12) Edit the STARTUP.NCF file as needed to match your setup. This information is presented in Chapter 2.5, *Modifying the STARTUP.NCF File* (page 2-15).

(13) Set the appropriate ISDN board parameters. This information is presented in Chapter 2.6, *Setting the ISDN Board Parameters* (page 2-16).

Optional: Install Recommended Novell Patches

Novell recommends that you install the latest file updates and patches for their systems. The ITK NetBlazer 4400 CD contains a collection of current file update kits for IntranetWare (Release Date 6/97). Please refer to the file README.TXT at the root of the CD for the corresponding installation paths.

2.3 Installation on a NetWare 3.12 Server

If you want to use a NetWare 3.12 server as the basis for ITK NetBlazer 4400, install NetWare 3.12 as described in the Novell documentation.

The NetWare 3.12 server files are located on the ITK NetBlazer 4400 CD in the directory \NW312\NETWARE.312\INSTALL.

Perform the following steps to install ITK NetBlazer 4400 on a NetWare 3.12 server:

(1) Enter the ITK NetBlazer 4400 CD into your CD-ROM drive.

(2) Switch to *System Console* under NetWare, and run the Novell INSTALL installation program.

```
load install
```

The following screen will appear:

```
+----------------------+
| Installation Options |
|----------------------|
| |Disk Options        |
| |Volume Options      |
| |System Options      |
| |Product Options     |
| |Exit                |
+----------------------+
```

(3) Select *Product Options* and press <Enter>.

The *Currently Installed Products* list will appear.

(4) Press the <Ins> key.

You will be asked to enter the installation path.

Option 1

If the *Novell MultiProtocol Router 3.1* is **not** installed on your system, the installation starts from the root of the CD.

(5a) Type the letter for your CD-ROM drive (d: designates your CD-ROM drive letter):

```
d:\
```

If you have mounted your CD under NetWare, enter the following path and confirm by pressing <Enter>:

```
NETBLAZER4400:\
```

The *MultiProtocol Router Installation Options submenu* will appear.

Option 2

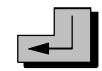
If the *Novell MultiProtocol Router 3.1* has **already** been installed on your system, perform the following steps:

(5b) Enter the following installation path (d: designates your CD-ROM drive letter):

```
d:\NB4400
```

If you have mounted your CD under NetWare, enter the following path and confirm by pressing <Enter>:

```
NETBLAZER4400:\NB4400
```



The *Installation Options* submenu will appear.

Install Product

(6) Select *Install Product,* and press <Enter>.

The *Install to Servers* window will appear. This window lists the servers on which you can install the ITK NetBlazer 4400. The RSPAWN.NLM must be loaded for a server to appear on this list.

(7) Use the <Ins> key to select the desired server(s), and press <Enter>.

> If you want to install the product on a number of servers, you will need a separate license for each installation.
>
> You cannot install on remote servers unless you have supervisor access rights to these systems.

(8) Answer `Yes` to the *Start installation?* prompt to begin the installation, and press <Enter>.

The *Install configuration files to <Server Name>?* window will appear.

(9) Select *No* as your entry, and press <Enter>.

(10) Insert the *IntranetWare Communication Engine* Disk in the diskette drive, and press <Enter> twice when prompted.

The Novell MPR and ITK NetBlazer 4400 files will now be installed on your system.

(11) After the copy process has been completed, choose *Exit,* and then press <Enter> and <Esc> to leave the installation program.

(12) Edit the *STARTUP.NCF* file as needed to match your setup. This information is presented in Chapter 2.5, *Modifying the STARTUP.NCF File* (page 2-15).

(13) Set the appropriate ISDN board parameters. This information is presented in Chapter 2.6, *Setting the ISDN Board Parameters* (page 2-16).

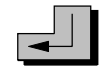
2.4 Installation on a NetWare 4.1x Server

To install the ITK NetBlazer 4400 on an existing NetWare 4.10 server, perform the following steps:

(1) Insert the ITK NetBlazer 4400 CD into your CD-ROM drive.

(2) From the *System Console* of your server, run the Novell installation program.

```
load install
```

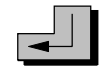


(3) Switch to *Product options,* and in this menu select *Install a Product not listed*.

A pop-up menu will appear where you can define the desired installation drive.

(4) Press <F3> and enter your CD-ROM drive letter (d: designates your CD-ROM drive letter).

```
d:\
```



The installation starts from the root of the CD.

If you have mounted your CD under NetWare, enter the following path and confirm by pressing <Enter>.

```
NETBLAZER4400:\
```

On the next menu you are asked to indicate which file groups you want to install.

(5) Press <F10> to install all of the groups marked.

The *Installation Options* submenu will appear to install the Novell NIAS files.

Install Product NIAS

(6) Select *Install Product,* and press <Enter>.

The *Install to Servers* window will appear. This window lists the servers on which you can install the Novell NIAS. The RSPAWN.NLM must be loaded for a server to appear on this list.

(7) Use the <Ins> key to select the desired server(s), and press <Enter>.

> If you want to install the product on a number of servers, you will need a separate license for each installation.
>
> You cannot install on remote servers unless you have supervisor access rights to these systems.

(8) Answer `Yes` to the *Start installation?* prompt to begin the installation, and press <Enter>.

The *Install configuration files to <Server Name>?* window will appear.

(9) Select *No* as your entry, and press <Enter>.

(10) Insert the *IntranetWare / NetWare 4.11 License* Disk in the diskette drive, and press <Enter> when prompted.

The Novell NIAS files will now be installed on your system.

(11) After the copy process has been completed, choose *Exit,* and then press <Enter> and <Esc> to leave the NIAS installation program.

The *Installation Options* submenu will appear again to install the ITK NetBlazer 4400 files.

Install Product ITK NetBlazer 4400

(12) Select *Install Product,* and press <Enter>.

The *Install to Servers* window will appear. This window lists the servers on which you can install the ITK NetBlazer 4400. The RSPAWN.NLM must be loaded for a server to appear on this list.

(13) Use the <Ins> key to select the desired server(s), and press <Enter>.

> If you want to install the product on a number of servers, you will need a separate license for each installation.
>
> You cannot install on remote servers unless you have supervisor access rights to these systems.

(14) Answer `Yes` to the *Start installation?* prompt to begin the installation, and press <Enter>.

The *Install configuration files to <Server Name>?* window will appear.

The ITK NetBlazer 4400 files will now be installed on your system.

(15) After the copy process has been completed, choose *Exit,* and then press <Enter> and <Esc> to leave the ITK NetBlazer 4400 installation program.

(16) Follow the indicated recommendations and press <Enter> to complete the installation.

After the completion of the installation process, you are informed that the ITK NetBlazer 4400 has been installed successfully.

(17) Press <Enter> to confirm, and leave the installation program by pressing <Esc>.

(18) Edit the STARTUP.NCF file as needed to match your setup. This information is presented in Chapter 2.5, *Modifying the STARTUP.NCF File* (page 2-15).

(19) Set the appropriate ISDN board parameters. This information is presented in Chapter 2.6, *Setting the ISDN Board Parameters* (page 2-16).

2.5 Modifying the STARTUP.NCF File

The special ASCII file STARTUP.NCF is included on the NetWare DOS partition (in the directory from which SERVER.EXE program is called). This file contains a series of important start-up data and environmental variables.

Edit the STARTUP.NCF file as needed to match your setup.

(1) Start the NetWare installation program by running.

```
load install
```

The installation program screen will be loaded, and an options menu will appear.

(2) Under NetWare 4.1x, select in the *NCF Files Options* menu the submenu ***Edit*** *STARTUP.NCF*, and press <Enter>.

Under NetWare 3.12, select in the *System Options* menu the submenu ***Edit*** *STARTUP.NCF*, and press <Enter>.

Do not select ***Create*** STARTUP.NCF, since this option will create a new file and will delete the entries that have already been made.

(3) Add the following lines to the entries in this file:

```
SET MINIMUM PACKET RECEIVE BUFFERS=300
```

If this entry is already present, increase the value to 300. If the existing value is higher, leave the existing value like it is.

(4) Save your changes by pressing <F10>.

(5) Leave the editor by pressing the <Esc> key twice.

(6) Reboot the server, so that the changes take effect.

(7) Set the appropriate ISDN board parameters. This information is presented in Chapter 2.6, *Setting the ISDN Board Parameters* (page 2-16).

2.6 Setting the ISDN Board Parameters

The ITK boards are shipped with the D channel protocol set to DSS-1 (the “Euro-ISDN” protocol) as the default. If you have a basic ISDN line which uses this protocol, then you will not need to change the D channel setting. You can also use your ITK board with a basic ISDN line which uses other protocols on a public telephone system, in a PBX system, or with some other protocol.

- If you want to use settings other than the default settings, edit the appropriate parameter in the IX1.INI configuration file for the active ISDN boards.
- If you want to use settings other than the default settings for the passive ISDN board and the modem boards, enter the appropriate parameters in a command line. The parameters are defined in the manual for your ITK board.

2.6.1 The active ITK ISDN boards

Details on the various ISDN interfaces and protocols are provided in the *ix1 Installation and Interfaces* manual that accompanies your active ITK board.

If you use an ITK Basic you have to use different bin files (see *ix1 Installation and Interfaces*). The appropriate bin files you find on the ITK NetBlazer 4400 CD in the following path:

```
NETBLAZER4400:\ITK_HW\basic.4MB (for an ITK Basic 4MB)
NETBLAZER4400:\ITK_HW\basic.fax (for an ITK Basic 1MB with
                                 fax extension)
NETBLAZER4400:\ITK_HW\basic.mod (for an ITK Basic 1MB with
                                 modem extension)
```

You can use the IXRDCONF.NLM program to display the current board settings from your configuration memory whenever you wish.

Please proceed as follows to change the ISDN settings for the active ITK ISDN boards:

(1) Enter the following command in order to create a configuration file ix1.ini.

```
:load ixinstall -n
```

If you are using DSS-1 as D channel protocol, this default configuration will be acceptable and you can proceed at Chapter 3, *Configuring ITK NetBlazer 4400*.

If you need any special configuration:

(2) Open the IX1.INI configuration file in an editor.

> The Novell system editor (*edit*) from NetWare 3.12 cannot handle large files. Please edit the ix1.ini configuration file with a different editor on your workstation.

(3) Edit the IX1.INI configuration file. You will find the description of all parameters in the manual *ix1 Installation and Interfaces* in the appendix, *ix1.ini Configuration File*.

(4) Save the edited IX1.INI configuration file.

> In order to finally activate the modified settings, you have to download the protocol software onto the ITK board.

(5) To do this, unload the module IXCAPI.NLM, and restart it:

```
:unload ixcapi
```

```
:load ixcapi
```

If you do not know exactly which D channel protocol is used on your ISDN line, call your telephone company or your PBX system provider.

If you change the ISDN settings, the CAPI board driver must be reloaded, for example by using the `connect` batch.

2.6.2 The passive ITK ISDN board

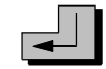
Details on the various ISDN interfaces and protocols are provided in the manual for the ITK Micro board.

You set the ISDN settings for the ITK Micro boards with the following parameters if you start the ITK Micro driver:

The driver can be loaded using the following parameters:

(1) At the *System Console* of the Novell FS/MPR enter the following command:

```
:load ixmicro.nlm <parameter>
```



```
Parameter:
[-d] [-a <IO-Address>][-t <TEI>] [-p <Protocol>]
[-s <SPID-type>,<SPID>]
[-m <phone number> (PN) mapping>]
[-n <phone number 1>,<phone number 2>,...]
```

The parameters are defined in the manual for your ITK Micro.

If you do not know exactly which D channel protocol is used on your ISDN line, call your telephone company or your PBX system provider.

If you change the ISDN settings, the CAPI board driver must be reloaded, for example by using the `connect` batch.

2.6.3 The ITK modem boards

Details on the various settings are provided in the manual of the ITK modem board.

ITK DigitalModem

The driver can be loaded using the following parameters:

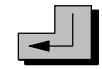
(1) At the *System Console* of the Novell FS/MPR enter the following command:

```
:load itkdm.nlm <parameter>
```

```
Parameter:
[port]  = <I/O address>
[mem]   = <memory address>
[cc]    = <country code>
[xl]    = <transmit level>
```

For example:

```
:load itkdm.nlm port=340 mem=D0000 cc=217
```



You load your ITK DigitalModem board using:

- I/O port 340,
- shared memory D0000 and
- the local settings for Germany.

The parameters are defined in the manual for your ITK DigitalModem.

If you change the ISDN settings, the CAPI board driver must be reloaded, for example by using the `connect` batch.

ITK MultiModem

Please proceed as follows to change the ISDN settings for the active ITK ISDN boards:

(1) Enter the following command in order to create a configuration file ix1.ini.

```
:load ixinstall -n
```

(2) Open the IX1.INI configuration file in an editor.

> The Novell system editor (*edit*) from NetWare 3.12 cannot handle large files. Please edit the ix1.ini configuration file with a different editor on your workstation.

(3) Edit the IX1.INI configuration file. You will find the description of all parameters in the *ITK MultiModem* manual.

(4) Save the edited IX1.INI configuration file.

> In order to finally activate the modified settings, you have to download the protocol software onto the ITK board.

(5) To do this, unload the module IXCAPI.NLM, and restart it:

```
:unload ixcapi
```

```
:load ixcapi
```

If you change the ISDN settings, the CAPI board driver must be reloaded, for example by using the `connect` batch.

3 Configuring ITK NetBlazer 4400

3 Configuring ITK NetBlazer 4400

The ITK NetBlazer 4400 requires several installation, configuration and administrative tasks which depend on individual customers needs.

This chapter describes the most common installation and configuration steps.

For a detailed description of the functionality and the meaning of every parameter see Chapter 5, *Reference for ITK NetBlazer 4400* (page 5-3).

Note that both ISDN drivers of the ITK NetBlazer 4400 can be used in parallel, even if you have only installed one ISDN board. If you have more than one controller, all tasks concerning the WANODI interface will be configured in the INETCFG program while those of the Virtual Ethernet Interface are made in the Main Screen of the ITK NetBlazer 4400.

If you want to configure the WANODI interface, read chapter 3.2, *Setup the WANODI Interface* (page 3-6)

If you want to configure the Virtual Ethernet interface, read chapter 3.3, *Setup the Virtual Ethernet Interface* (page 3-10)

3.1 About ISDN boards, Controllers and Interfaces

The definition of the terms **board**, **controller** and **interface** are treated in different meanings and the definitions may confuse.

An ISDN **board** defines a physical ISDN card, for example an ITK Basic ISDN board.

This ISDN board with its two B channels may be used in parallel for WANODI and Virtual Ethernet connections. In this case two different ISDN **drivers** have to be installed. These **drivers** are treated as **boards** in the Internetworking configuration program INTETCFG, so you define the two ISDN drivers WANODI and Virtual Ethernet in its BOARDS section, even if you have only one physical ISDN Board installed.

A **controller** represents one ISDN line, that means two B channels. An ITK Basic board acts as one controller. An ITK Octo with four lines and eight B channels is handled as four controllers, that means one controller per line.

Compared with that, an ITK Primary is again one controller with one line connection and 30 B channels.

For every controller used for WANODI connections you have to setup and configure one separate WANODI driver. The Virtual Ethernet driver is only installed once. The configuration of an additional Virtual Ethernet driver is only necessary for multiple Virtual LAN groups.

If you have installed one ITK Octo board you have four lines / controllers at your disposal. In case you want two controllers to be used for WANODI and two for Virtual Ethernet connections, you have to install a WANODI driver for each of the two controllers. For Virtual Ethernet connections the driver has to be installed only once.

3.2 Setup the WANODI Interface

The following describes how to configure the WANODI interface of the ITK NetBlazer 4400.

You should use WANODI connections if:

- you want to interconnect networks via ISDN
- you want to reserve B channels for a corresponding connection
- you want to route other protocols than IPX and/or TCP/IP
- you want to use unnumbered TCP/IP connections
- you want to exploit the full range of Novell MPR 3.1 functions

To configure the WANODI Driver, perform the following steps:

(1) Under NetWare, switch to the *System Console* and start the INETCFG program:

```
load inetcfg
```

The following main menu will appear:

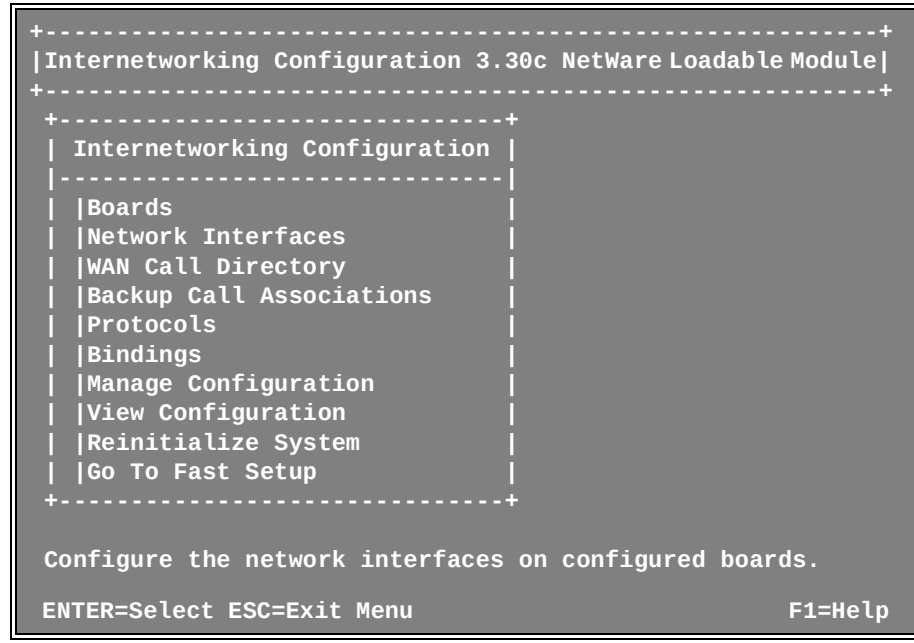


Fig. 3-1 The main menu of the INETCFG Program

To configure an ISDN board, perform the following steps:

(1) Select the *Boards* menu item in the main menu and press <Enter>.

A dialog box will appear that may look like this:

Board Name	Driver	Int	IOAddr.	MemAddr	Slot	Status	Comment
3c5x9_1	3c5x9 Transfe…	3	300	-	-	Enabled	

If you have not configured a board yet, an empty window will appear.

(2) Press <Ins> to display a list of all network drivers known to the system.

(3) Select the ITK ISDN WANODI Driver *ix1* from this list using the cursor keys and confirm your selection using <Enter>.

The *Board Configuration* dialog box will appear.

(4) Give the ISDN WANODI board a name. You may enter comments about the selected board in the *Comment* field. Leave the *Board Status* parameter set to `enabled`.

> Select a name containing the type of the driver and – if necessary – the controller number, for example, IX1_WAN_C0.

If you are using more than one ITK boards in your router, you have to manually enter the controller number specified by CAPI. To verify the order, you may enter the command LOAD IXRDCONF on the server console. The first board in the list receives the controller number “0”, the next board receives “1”, and so forth. If you are only using *one* ITK board, the value “0” always has to be present here.

You can find further information about controller numbering in the *ix1 Installation and Interfaces* manual of your ITK board.

(5) Press the <Esc> key to confirm the entry.

The newly defined board will appear in the configuration window.

If you want to configure an additional WANODI board, repeat steps **(2)** to **(5)**.

(6) Press the <Esc> key to return to the main menu.

Now you have to configure the previously installed WANODI Board in the section Network Interfaces.

Perform the following steps:

(1) Select the *Network Interfaces* menu item in the main menu of the INETCFG and press <Enter> to configure the installed ISDN board.

A list of the boards already installed will appear. Network boards (LAN Drivers) need no further entries at this point.

(2) Select the WANODI board to be configured (for example IX1_WAN_C0) from this list and press <Enter>.

(3) Enter your *Own ISDN Number*.

Use the following dial number scheme:

Country code - Area Code - Subscriber number - PBX extension

for example 49-123-8888-765

Separate each of the parts with a hyphen.

> For detailed information on possible dial number schemes, see *Chapter* , section *Supported Dial Number Formats* (page 5-5).

The other entries can remain in their default settings. For a detailed description about these parameters and the expert configuration see Chapter 3.12, *Fine Tuning the WANODI Interface* (page 3-28) and Chapter 5, *Reference for ITK NetBlazer 4400* (page 5-3).

Once you have configured all available WANODI boards, return to the main menu by pressing the <Esc> key.

Continue in the following way:

- Setup the Virtual Ethernet Interface - See the next chapter.
- Configure IPX Protocol Settings - See Chapter 3.4, *Configure IPX Protocol Settings* (page 3-11).
- Configure IP Protocol Settings - See Chapter 3.5, *Configure IP Protocol Settings* (page 3-12).

3.3 Setup the Virtual Ethernet Interface

The following describes how to configure the Virtual Ethernet interface of the ITK NetBlazer 4400. You should use Virtual Ethernet ISDN connections if

- you want to interconnect Remote Workstations via ISDN
- you want to share B channels between multiple destinations
- you want to enable Modem and/or GSM access
- you want to use the IP address negotiation functionality
- you want to use Masquerading for IP addresses

The activation of a Virtual Ethernet Driver using the INETCFG program is similar to the setup process of the WANODI driver described in the previous section of this chapter.

Perform the following steps:

(1) Start the INETCFG program:

```
load inetcfg
```

(2) Switch to the *Boards* menu item and press <Enter>.

The *Configured Boards* menu will appear.

(3) Press the <Ins> key to display a list of the drivers known to the system.

(4) From this list of drivers, select the Virtual Ethernet Driver *IX1VETH* using the cursor keys and confirm your selection with <Enter>.

The *Board Configuration* menu will appear.

(5) Give the Virtual Ethernet Driver a name and press <Enter>.

(6) In the *Virtual LAN Number* entry, enter the number of the virtual LAN this driver shall belong to and press <Enter>. Normally you leave the default setting “0” and change this parameter only if you require the routing between ISDN subscribers.

(7) Press the <Esc> key twice and confirm the *Save Changes message*.

In the *Configured Boards* menu, the Virtual Ethernet Driver will appear as a defined board.

Continue in the following way

- Configure IPX Protocol Settings - See the next chapter.
- Configure IP Protocol Settings - See Chapter 3.5, *Configure IP Protocol Settings* (page 3-12).

3.4 Configure IPX Protocol Settings

The following parameters are global parameters and are consequently only configured once for any LAN and WANODI driver.

You will only find references to parameter settings required for working with the ITK boards. Normally, the defaults of the other parameters can remain unchanged.

You will find further information in the *NetWare MPR Supervisor's Guide*.

Normally you do not need to change the default settings when configuring the IPX protocol. Nevertheless you have to confirm these settings.

Perform the following steps:

(1) In the *Protocols* menu item, select the *IPX* transfer protocol and press <Enter>.

The *IPX Protocol Configuration* dialog box will appear.

(2) Make sure that the Packet forwarding is "enabled" and the routing protocol is set to "NLSP with RIP/SAP compatibility" and exit the menus by pressing <Esc> twice.

Continue in the following way:

- Configure IP Protocol Settings - See the next chapter.
- Configure Bindings for the WANODI Interface - See Chapter 3.6, *Configure Bindings for the WANODI Interface* (page 3-13).
- Configure Bindings for the Virtual Ethernet Interface - See Chapter 3.7, *Configure Bindings for the Virtual Ethernet Interface* (page 3-16).

3.5 Configure IP Protocol Settings

To configure the TCP/IP protocol, perform the following steps:

(1) In the INETCFG program, select the *Protocols* menu item and the *TCP/IP* submenu there.

(2) Check the entries *TCP/IP status* and *IP Packet Forwarding* and make sure that they are `enabled` and `enabled("Router")`.

Leave all other parameters at their default settings.

You will find information about changing the various parameters in your Novell documentation.

Continue in the following way:

- Configure Bindings for the WANODI Interface - See the next chapter.
- Configure Bindings for the Virtual Ethernet Interface - See Chapter 3.7, *Configure Bindings for the Virtual Ethernet Interface* (page 3-16).

3.6 Configure Bindings for the WANODI Interface

Configuring the Bindings for the IPX Network Protocol

The settings described in steps **(6)** through **(13)** of this chapter are absolutely necessary for a trouble-free operation of the WANODI interface.

To bind a protocol to a network interface, perform the following steps:

(1) From the INETCFG main menu select Bindings and press the <Ins> key to select the network protocol that you want to bind to the WANODI board.

(2) Select `IPX` and confirm your selection using <Enter>.

(3) Select whether you wish to bind the protocol to a single interface or an interface group, choose *A Network Interface* and confirm with <Enter>.

(4) Select your WANODI interface using the cursor keys and press <Enter>.

The *Binding IPX to a WAN Interface* submenu will appear.

In the *WAN Call Destinations* submenu, you can define additional parameters for partners who are using this interface or interface group. In this submenu, you specify when a connection is to be established and whether static routing entries to this partner are to be defined.

Changes are not necessary at this point; they are described in Chapter 3.12, *Fine Tuning the WANODI Interface* (page 3-28).

(5) Change to the *Expert Bind Options* menu entry and confirm with <Enter>.

The *Expert WAN Bind Options* submenu will appear.

(6) Change the *Header Compression* entry from `enabled` to `disabled`.

Header Compression of the Novell MPR has to be switched off to activate the filter mechanisms of the ITK NetBlazer 4400. Performance does not suffer because the ITK boards use their own automatic data compression scheme to increase the throughput rate.

(7) Select the *RIP Bind Options* entry and press <Enter>.

The *RIP Bind Options* submenu will appear.

(8) Change the *Periodic Update Interval* entry from 2 to the maximum value of `10000`.

(9) Return to the *Expert WAN Bind Options* dialog window again by pressing the <Esc> key.

The exchange of routing information within a corporate network is either performed when a change occurs in this information or periodically once per minute.

If you are using the maximum value of 10 000 here, RIP information is exchanged once every 3.5 days in case of no changes.

(10) Select the *SAP Bind Options* entry and press <Enter>.

(11) Change the *Periodic Update Interval* entry from 2 to the maximum value of `10000.`

With the SAP protocol, servers offer, for example, their services over the entire network. The exchange interval is also increased to 3.5 days if no changes occur.

(12) Select the *NLSP Bind Options* entry and press <Enter>.

(13) Change the *NLSP State* entry to `Off` to switch off NLSP here for ISDN.

(14) Exit this menu by pressing the <Esc> key twice.

(15) Save the changes made by pressing the <Enter> key.

Now you have successfully completed binding the IPX protocol to the WANODI interface.

Continue in the following way:

- Configure IP-Bindings for the WANODI Interface - See the next section.
- Configure Bindings for the Virtual Ethernet Interface - See Chapter 3.7, *Configure Bindings for the Virtual Ethernet Interface* (page 3-16).
- Define WANODI Call Destinations - See Chapter 3.9, *Configure a WANODI Call Destination (X.75)* (page 3-21).

Configuring the Bindings for the IP Network Protocol

To bind the TCP/IP network protocol to a board, perform the following steps:

(1) In the *INETCFG Main* menu, select the *Bindings* menu item and press <Enter>

(2) Press the <Ins> key to select the network protocol that you want to bind to the ITK board and choose `TCP/IP`.

(3) Select whether you wish to bind the protocol to a single interface or an interface group. Choose *A Network Interface* and confirm with <Enter>.

(4) Select your WANODI interface using the cursor keys and press <Enter>.

A menu will appear.

(5) Change to the *Local IP Address* entry in the following menu and specify your IP address for the ISDN connection.

The format consists of four decimal numbers between 0 and 255 separated by periods, for example, 192.89.4.1.

The corresponding *Subnet Mask of Connected Network* automatically will appear in the menu entry below.

(6) Accept the suggested entry.

(7) Exit the submenu by pressing the <Esc> key twice.

Continue in the following way:

- Configure Bindings for the Virtual Ethernet Interface - See the next chapter.
- Reinitialize the System - See Chapter 3.8, *Update Configuration changes* (page 3-19).
- Define WANODI Call Destinations - See Chapter 3.9, *Configure a WANODI Call Destination (X.75)* (page 3-21).

3.7 Configure Bindings for the Virtual Ethernet Interface

Configuring the Bindings for the IPX Network Protocol

Perform the following steps:

(1) In the INETCFG main menu, select the *Bindings* menu item.

(2) Press the <Ins> key to select the network protocol and choose *IPX*.

(3) Select whether to bind the protocol to a single interface or to an interface group.

(4) Select the *A Network Interface* entry to select a single interface, choose the desired interface and confirm your selection using <Enter>.

(5) In the *IPX network number* entry of the *Binding IPX to a LAN Interface* menu, specify the IPX network number that you are assigning to this Virtual Ethernet Driver. If you want to test your connection with the ITK_Test Router, you have to set the IPX network number to 9747298.

The IPX network number has to be unique for all systems you want to connect to. Only systems with the same Virtual Ethernet IPX Network number belong to the same “ISDN Network” and can exchange data!

(6) *Select the Frame Type entry. If necessary, change this entry to "ETHERNET_II".*

The IX1VETH driver supports **only** the “ETHERNET_II” frame type.

Do **not** change the RIP/SAP update intervals. Otherwise the installed filters will not operate properly.

(7) Select the *Expert Bind Options*.

(8) Select *RIP Bind Options* and change the *RIP State* to *On*.

(9) Select *SAP Bind Options* and change the *SAP State* to *On*.

SAP and RIP guarantee a correct exchange of the RIP and SAP information.

(10) Select *NLSP Bind Options* and change the *NLSP State* to *Off*.

The new routing protocol for IPX is called NetWare Link Service Protocol (NLSP). It is designed to reduce the traffic in large internetworks and to shorten the time for distributing information after network changes. For this purpose, each router polls its "neighbors" every 20 seconds. If no changes occur, the router will broadcast its knowledge about the Internet to EVERY other NLSP router in the network every 120 minutes.

Up to now we haven't implemented any filter for this, so if you use NLSP on the WAN routers, the data transfer may be very expensive.

We suggest using NLSP on LANs only and configure RIP/SAP for the ISDN routers.

(11) Exit the menus using <Esc> and confirm the *Save Changes message*.

Continue in the following way:

- Configure IP-Bindings for the Virtual Ethernet Interface - See the next section.
- Reinitialize the System - See Chapter 3.8, *Update Configuration changes* (page 3-19).

Configuring the Bindings for the IP Network Protocol

Perform the following steps:

(1) In the main menu, select the *Bindings* menu item and press the <Ins> key to select the network protocol. Select whether to bind the protocol to a single interface or to an interface group.

(2) Select the *A Network Interface* entry to select a single interface, choose the desired interface and confirm your selection using <Enter>.

(3) Select IP and press <Enter>.

A menu will appear.

(4) Change to the *Local IP Address* entry in the following menu, and specify the IP address that you want to assign to the Virtual Ethernet Driver.

The format consists of four decimal numbers between 0 and 255 separated by periods, for example, 192.89.4.1.

The corresponding *Subnet Mask of Connected Network* will automatically appear in the menu entry below.

(5) Accept the suggested entry.

(6) Exit the submenu by pressing the <Esc> key twice.

You have now completed activation of the Virtual Ethernet Driver using the INETCFG program.

Continue in the following way:

- Reinitialize the System - See Chapter 3.8, *Update Configuration changes* (page 3-19).

3.8 Update Configuration changes

Changes made in the router configuration are generally not activated immediately, but are activated by reinitializing the system. You have several options for making the changes active, as described below.

1. Option: Bring down and Restart the server (only NetWare 4.xx)

You should use this option after the initial configuration of the system and after major changes of the router configuration.

(1) From the Server *System Console* type:

```
down
```

```
restart server
```

2. Option: Initialize with CONNECT.NCF

The ITK NetBlazer 4400 software contains the file CONNECT.NCF, which first unloads all router related programs if necessary, and then performs a router restart including a download of the ISDN board software.

You should use this command after major Virtual Ethernet configuration changes.

(1) From the Server *System Console* type:

```
connect
```

3. Option: INETCFG menu “Reinitialize System”

This is the most common option if changes in the Internetworking Configuration of the system are performed.

(1) From the INETCFG Main Menu choose *Reinitialize System.*

(2) Press <Enter> three times for the changes made to take effect.

4. Option: Reinitialize with RI.NCF

The ITK NetBlazer 4400 software contains the file RI.NCF which forces the Reinitialize System process.

(1) From the Server *System Console* type:

```
ri
```

5. Option: Function Key <F2>

All subsequent configuration changes to the WANODI interface have to be imported into ITK NetBlazer 4400.

If you don’t perform a router restart as described in option 1 or 2, perform the following steps:

(1) Change to the IX1CCA ISDN Connection Manager and press the <F2> function key.

```
<F2>
```

Continue in the following way:

- Configure WANODI Call destinations- See the next chapter.
- Initial Virtual Ethernet Configuration Tasks - See Chapter 3.14, *Initial Virtual Ethernet Configuration Tasks* (page 3-36).

3.9 Configure a WANODI Call Destination (X.75)

For every connection using a WANODI driver, the remote partner has to be defined in the WAN Call Directory.

This chapter describes the necessary steps to configure a destination using an ITK NetBlazer product.

If you have to configure specific advanced parameters, see Chapter 5, *Reference for ITK NetBlazer 4400* (page 5-3). There you will find a detailed explanation of every parameter and its functionality.

In particular, the configuration of the Short Hold parameters should be done carefully to prevent expensive connection charges. See Chapter , section *Short Hold* (page 5-12).

Preliminary Tasks

- Setup the WANODI interface
- Configure Protocol Settings
- Configure Bindings for the WANODI interface

To configure a new remote partner or to change an existing entry, perform the following steps:

(1) From the INETCFG main menu, change to the *WAN Call Directory* submenu.

(2) Press <Ins> to enter a new remote partner, or use the cursor keys and <Enter> to change an existing entry.

(3) Enter a name for the ISDN remote partner and press <Enter>.

A list of the transfer media available is displayed.

(4) Select *ix1-ISDN* and press <Enter>. Choose *Board name* and select the entry of the WANODI board.

(5) Enter the *Remote ISDN Number*.

Use the following dial number scheme:

Country Code - Area Code - Subscriber number - PBX extension

Separate each of the parts with a hyphen.

> For detailed information on possible dial number schemes, see *Chapter* , section *Supported Dial Number Formats* (page 5-5).

The selection is made by using the cursor keys and the <Enter> key. Once you have finished all entries, press the <Esc> key to return to the previous menu.

Configure a Test WANODI Call Destination

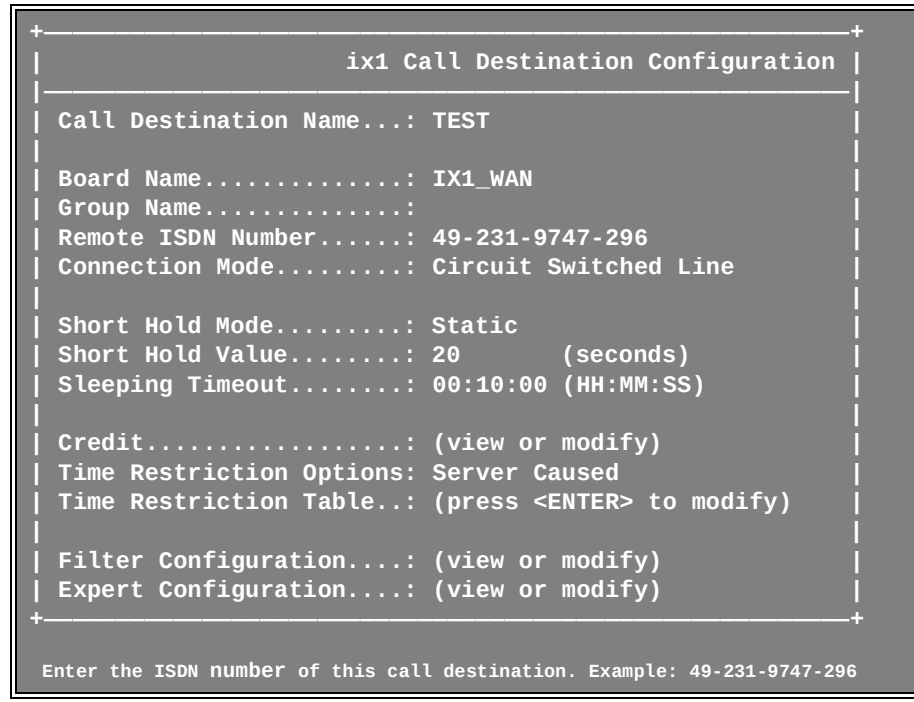
To perform an initial test of your system, you may define a destination for the ITK_TEST router in Dortmund, Germany.

This Call Entry requires the following settings:

- Call Destination Name: TEST
- Board name: <Your WANODI board name>
- Remote ISDN Number: 49 - 231 - 9747 - 296

All other parameters can remain in their default settings.

The ix1 Call Destination Configuration appears as follows:



Continue in the following way:

- Setup a WANODI Call - See Chapter 3.11, *Setup a WANODI Call* (page 3-26).
- Define a WANODI Call destination (PPP) - See Chapter 3.10, *Configure a WANODI Call Destination (PPP)* (page 3-24).
- Initial Virtual Ethernet Configuration Tasks - See Chapter 3.14, *Initial Virtual Ethernet Configuration Tasks* (page 3-36).

3.10 Configure a WANODI Call Destination (PPP)

ISDN connections to a destination using a system other than an ITK NetBlazer have to use the Point to Point Protocol (PPP). This Chapter describes additional configuration tasks for a destination using PPP and an optional authentication protocol.

Preliminary Tasks

- Setup the WANODI interface
- Configure Protocol Settings
- Configure Bindings for the WANODI interface

To setup a PPP call destination, perform the following steps:

(1) Define a Call destination as described in Chapter 3.9, *Configure a WANODI Call Destination (X.75)* (page 3-21).

(2) From the ix1 Call destination Configuration select *Expert Configuration*.

(3) Change the entry *Data Protocol* from *X.75 (ITK)* to *PPP (Point to Point Protocol)*.

If you want to configure a PPP authentication protocol, refer to the next section.

(4) Otherwise press <Esc> twice to leave the expert configuration menu and confirm the *Save Changes* message.

Optional: Configure a PPP authentication protocol

The ITK NetBlazer 4400 provides the authentication protocols CHAP and PAP. Depending on the destination, you may choose between a one-way and a two-way authentication.

For detailed explanations about the different authentication protocol settings, see *Chapter* , section *PPP Configuration* (page 5-19).

To configure the PPP authentication for a call destination, perform the following steps:

(1) In the Expert configuration menu of the ix1 Call destination configuration, select *PPP Authentication*.

(2) Choose the Authentication Protocol for this destination. If you select *Auto*, either PAP or CHAP is used, depending on the remote side settings.

(3) Change the Direction entry from *Allow own authentication* to *Peer have to authenticate* if you want to perform a two-way authentication. The setting *Call dependent* lets the particular calling peer identify itself.

(4) Insert the System IDs and the Password. By default, your router name is assigned as *Own System ID* and the Call destination Name is taken as *Remote System ID*. Change the entries according to your needs.

Remember that the system IDs and the Password have to agree on both sides. All entries are case sensitive!

(5) Press <Esc> twice to leave the expert configuration menu and confirm the *Save Changes message*.

Continue in the following way:

- Setup a WANODI Call - See the next chapter.

3.11 Setup a WANODI Call

To establish a WANODI connection manually to a remote partner, you use the Call Manager Utility. The Call Manager is part of Novell MPR 3.1.

> All manual WANODI calls are handled as described in this chapter.

To establish a connection using the Call Manager, perform the following steps:

(1) Start the WANODI Call Manager from the *System Console*:

```
load callmgr
```

(2) Press the <Ins> key, select the remote partner you want to connect to, and press <Enter>.

(3) Select the protocol you want to use for this connection and press <Enter> again.

The connection will be established. In the connection window, the status (on the far right) changes from *Out Connecting* to *Out Connected*.

Setup a WANODI Call to the ITK_TEST Router

You should establish a call to the ITK_TEST Router in Dortmund, Germany to check the functionality of your WANODI configuration.

Configure a WANODI partner TEST as described in Chapter 3.9, *Configure a WANODI Call Destination (X.75)*, section *Configure a Test WANODI Call Destination* (page 3-22).

Then start the Call Manager utility, select the Partner TEST, and choose the IPX protocol for the connection. If the call is OUT-CONNECTED, you have a physical and logical connection to the ITK_TEST router. You can check this by entering the command `display servers` on the server console. The ITK_TEST server will be among the servers displayed. From any client PC in your network, you can now log into the ITK_TEST server in Dortmund, Germany under the user name GUEST.

Release a WANODI Call

To manually terminate a call to a destination, change to the Call Manager screen. Now select the connection you want to release, and press <Del>.

The partner entry will change to OUT-DISCONNECTED.

If you have configured an IPX and an IP call for a destination, you have to release both connections separately.

Even if it is possible to release a WANODI call in the ISDN Communication Manager, we strongly recommend you handle WANODI calls via the Call manager utility.

Continue in the following way:

- Fine Tuning the WANODI Interface - See the next chapter.
- Fine Tuning WANODI Call destinations - See Chapter 3.13, *Fine Tuning WANODI Call Destinations* (page 3-30).

3.12 Fine Tuning the WANODI Interface

For operation of the ITK NetBlazer 4400 in some Private Branch Exchange Systems, it may be necessary to set some special parameters. It may also be useful to restrict the access to the system activating the basic security services by restricting the call acceptance to registered numbers only.

Enabling Basic Security Service

By default, the controller-dependent call acceptance is set to *Accept all numbers*. If you restrict this parameter, a connection is only established when a partner calls in with its corresponding configured dial number. Partners using a wrong dial number will be rejected.

For additional information on this parameter see Chapter , section *Basic Security Service / Call acceptance* (page 5-10).

To restrict the Call acceptance for WANODI connections, perform the following steps:

(1) From the INETCFG main menu, change to the *Network Interfaces* submenu.

(2) Choose the corresponding WANODI controller and press <Enter>.

(3) Change the entry *Call Acceptance* to *Accept Only Registered Numbers*.

(4) Save the changes and return to the INETCFG Main Menu.

(5) Switch to the *ITK NetBlazer 4400* Main Screen, the IX1CCA status screen, and press <F2> to import the changes to the router.

Adapt special WANODI Interface access parameters

If you have to change access codes or MSNs to establish calls from a Private Branch Exchange or if you want to change retry defaults, perform the following steps:

(1) From the INETCFG main menu change to the *Network Interfaces* submenu.

(2) Choose the corresponding WANODI controller and press <Enter>.

(3) Switch to *Expert Configuration* and press <Enter>.

(4) Change the corresponding entries according to your needs.

> For a detailed description of these parameters, refer to Chapter , section *Access Codes and MSNs* (page 5-7).

(5) Save the changes and return to the INETCFG Main Menu.

(6) Switch to the *ITK NetBlazer 4400* Main Screen, the IX1CCA status screen, and press <F2> to import the changes to the router.

Continue in the following way:

- Fine Tuning WANODI Call destinations - See the next chapter.
- Configure Static Routes for WANODI Call Destinations - See Chapter 3.13, *Fine Tuning WANODI Call Destinations* (page 3-30).

3.13 Fine Tuning WANODI Call Destinations

By default, WANODI call destinations are configured for standard use in a typical environment. It may be useful, and in some cases it is even necessary, to adapt parameters for individual needs. This section gives an overview of the tuning options for an individual WAN Call directory.

Detailed information about every parameter is given in *Chapter 5, Reference for ITK NetBlazer 4400* (page 5-3).

Configuring the Short Hold

You may define the Short Hold Mode as well as the Short Hold Value, that is the time interval before an inactivity timeout, if no user data is transferred for every dial number in the outgoing dial number list. Remember to set the Short Hold Value according to the charging interval. There is no need to release a line after 20 seconds, if the charging interval lasts 120 seconds. In this case, a Short Hold Value of 100 seconds may make sense.

If you have configured a Dynamic Short Hold mode and no charging indications are transferred during the connection, the static Short Hold value is taken instead.

If the Short Hold Values of a connection are different, the Call teardown will be processed after the shorter time.

If the Short Hold Mode is disabled, the connection remains active the entire time. This setting is only useful for leased lines, where connection-time-dependent charges do not occur.

Configuring the Sleeping Timeout

The Sleeping Timeout defines the time after which a sleeping connection is logically released, meaning the router stops packet spoofing.

Configuring Credits

Credits can be set to restrict outgoing calls to prevent uncoordinated connection costs. They can be restricted by charging units or connection times. They can be defined for different intervals and imposed by an expiration date.

If a credit is used up, all further connection requests will be rejected internally.

If more than one credit parameter is set, for example 100 units and a connection time of 2 hours, no further connection is possible when the first limit is reached.

Configuring Time Restrictions

The time restrictions are active either for outgoing, or for outgoing and incoming calls. A third setting restricts line establishment caused by NDS traffic. In a matrix, you may define time periods when connections are possible. It may be useful to restrict calls during weekend or evening hours. By default, no time restrictions are set. A detailed description on the Time Restriction functionality to suppress NDS data transfer is given in Appendix A.

Configuring Filters

The ITK NetBlazer 4400 has multiple filters for different IPX/SPX and IP control packets. In general, the pre-defined filter settings should not be changed unless it is absolutely necessary. An overview of the individual filters and their functionality are given in the reference chapter.

Expert Configuration

The following parameters may be changed in the *Expert Configuration* menu of the *Call Destination Configuration* window.

> Point to Point Protocol Settings and the PPP authentication are explained in Chapter 3.10, *Configure a WANODI Call Destination (PPP)* (page 3-24).

Changing the Call Type

If the Call Type is changed to *Permanent*, the corresponding connection will be established automatically at every time the router starts and remain logically active all times. Nevertheless, the Short Hold mechanism is still active. A permanent call also changes the defaults of the Retry Limit Handling and the Retry Interval Limit.

The permanent connection type is primarily used for leased lines and important network links that must always be active automatically.

Activating Channel Bundling

If you want to increase the transfer rate of one connection, you can bundle B channels to one virtual connection. The ITK NetBlazer 4400 offers three channel bundling options: static (that means the router tries to establish the maximum number of B channels), protocol dynamic, and load dynamic. When choosing Protocol Dynamic channel bundling, a B channel is added for every additional protocol to a destination. The load dynamic channel bundling depends on the amount of data to be transferred, and a B channel is added or removed automatically.

Prerequisites for a successful channel bundling are

- The channel bundling has to be activated on both sides.
- Sufficient B channels have to be present.
- The dial number has to be transmitted correctly.

Configure Static IPX Routing

To relieve you from manually initiating the establishment of a connection to a remote partner, the router is able to automatically establish connections. For this purpose, static IPX routing is used by Novell MPR 3.1. You can specify static routing information for every remote partner.

For a detailed description of the static IPX routing functionality, refer to the Novell MPR documentation.

To use static IPX routing, perform the following steps:

(1) In the INETCFG *Internetworking Configuration* menu, select the *Bindings* menu item and press <Enter>.

The *Protocol To Interface/Group Bindings* menu will appear.

(2) Select *IPX* for the appropriate ITK board and press <Enter>.

(3) In the *WAN Call Destinations* menu item, press the <Enter> key to display the configured remote partners. If you haven't configured a static IPX routing yet, an empty window will appear.

(4) Press the <Ins> key to display a list of available WAN Call destinations, choose the corresponding remote partner and press <Enter>.

In the *WAN Call Destination Entry* select the *Static Services* menu and press the <Ins> key to define a new service.

The following menu will appear:

```
+-------------------------------------------------------------+
|                Static Service Configuration                 |
|-------------------------------------------------------------|
| WAN Call Destination:    ITK_USA                            |
| Service Name:            SERVER_ITK_USA                     |
| Service Type:            (0004) FILE SERVER                 |
| Service Address Network: (Not Specified)                    |
| Service Address Node:    000000000001                       |
| Service Address Socket:  0451                               |
| Hops To Service:         1                                  |
| Ticks To Service:        70                                 |
+-------------------------------------------------------------+
```

(5) Enter the *Service Name* and define the *Service Type* for this service. Press <Ins> to display a list of supported services.

(6) In the *Service Address Network* field enter the internal IPX address of the remote server or router. The *Service Address Node* "1" is the default for all NetWare servers.

(7) Press <Esc> and <Enter> when prompted to save the configuration.

The service that you defined as the static route in the steps `WAN Call Destination` to `Service Address Network` will appear automatically in the list in the *Static Routes for on demand calls* menu item.

You do not need to change any other settings.

Using Permanent Calls

Permanent calls, once you have established them, are always maintained logically. The system attempts again and again to keep a logical connection established to this destination. You may configure *when* the connection is terminated and whether the connection is to be established manually or automatically when the router starts.

For this connection, one B channel is identified as busy at all times. This is independent of the physical state of the connection.

To use Permanent Calls, perform the following steps:

(1) From the INETCFG main menu select WAN call directory and choose the destination you want to edit.

(2) Select the *Expert Configuration* menu item and press <Enter>.

(3) Change the *Call Type* entry to `Permanent`.

(4) Press <Esc> and confirm the *Save Changes message* until you return to the *Internetworking Configuration* menu.

(5) Now Select the *Bindings* menu item and press <Enter>.

(6) Select the ITK board that you want to use to establish the permanent connection and press <Enter>.

(7) Press <Enter> again to configure or to change a `Permanent WAN Call Destination`.

(8) If there are no entries in the window, select a remote partner for permanent connections: First press <Ins> and then <Enter> in the next window under *WAN Call Destinations*.

(9) In the *WAN Call Type* menu item, you may now select when a connection is to be established to this remote partner.

There are two options:

- Manually

You manually establish the connection to the remote partner in the Call Manager.

- Automatically

  The connection is established immediately whenever the router starts.

  You do not need to change the settings in the *Expert Options* menu item.

(10) Press <Esc> to exit the menu, and confirm the changes with <Enter>.

Defining Backup Paths for Leased Line Connections (PPP)

For leased lines, you may define *one* backup path (backup call). For dial-up lines, you may not define any.

You may assign a second partner to a remote destination. This second partner accepts the connection if the connection to the first partner was interrupted.

Perform the following steps to specify a backup path:

(1) Define two WAN Call Directories to the corresponding remote partner. Enter different names and dial numbers for each.

(2) Define both WAN Call Directories in the *Expert Configuration* item as `Call Type` "Permanent" and as `Data Protocol` "PPP".

(3) Change to the *Backup Call Associations* item and press <Enter>.

(4) Press the <Ins> key to define a new backup path (Backup Call) and finally press the <Enter> key in the *Primary Destination* field.

(5) From the list, select the primary partner that will regularly establish the connection and press <Enter>.

(6) Select the *backup partner* in the *Backup Destination* field.

(7) You activate or deactivate backup operation in the *Status* field. In the fields below this, you can specify the times after which the backup number is to be dialed (*Backup Connect Delay*) or the time after which the connection is to be accepted again by the *Primary Destination*.

(8) Press <Enter> to confirm your selection.

3.14 Initial Virtual Ethernet Configuration Tasks

After you have activated the Virtual Ethernet Driver for the first time, you are prompted to enter the Product Key for your system. This Product Key is supplied within the software's standard delivery. You will find the Product Key on the enclosed CD.

Perform the following steps:

(1) Enter the *Product Key*, and press <Enter>.

(2) Choose the installed *ITK board* and edit the *command line* if necessary. The command line parameters are described in detail in the manual for the ISDN board.

> All drivers for the ITK boards are installed automatically at the same time with the ITK NetBlazer 4400.

(3) Switch to the *ITK NetBlazer 4400* Main Screen. You are asked to configure the driver and the global Virtual Ethernet settings.

The *Controller Configuration* menu initially opens automatically. You are requested to insert the Dial number for every controller in your system.

(4) Insert the dial number using the scheme mentioned in chapter 3.9, *Configure a WAN-ODI Call Destination (X.75)* (page 3-21), step **(5)**.

(5) Answer *Yes* to the question *Should the global Virtual Ethernet dial number be updated automatically?*

(6) If you have already configured a WANODI controller, you are only asked to insert the Virtual Ethernet Dial number.

> The configuration and administration of all Virtual Ethernet related issues is handled by one main router configuration window. You open this window by pressing <F10>.

Continue in the following way:

- Define a Virtual Ethernet Call destination (X.75) - See the next chapter.

3.15 Define a Virtual Ethernet Call destination (X.75)

Virtual Ethernet Call destinations are configured from the main status screen of the ITK NetBlazer 4400.

For example: for a simple standard configuration, a call to the ITK_TEST router is configured.

If you have to configure specific advanced parameters, see Chapter 5, *Reference for ITK NetBlazer 4400* (page 5-3). There you will find a detailed explanation of every parameter and its functionality.

In particular, the configuration of the Short Hold parameters should be done carefully to prevent expensive connection charges. See Chapter , section *Short Hold* (page 5-12).

To configure a Virtual Ethernet call destination perform the following steps:

(1) Press <F10> to open the *Router Configuration* menu.

(2) Select the Partner Configuration menu item and press <Enter>.

The *Configure Partner* window will appear with a list of available remote partners. All remote partners identified with a “V” in front of their name belong to the Virtual Ethernet Driver and can be edited here.

(3) If you wish to define a new remote partner, press the <Ins> key.

If you want to change the parameters of an existing remote partner, select the remote partner and press <Enter>.

(4) Enter a name for this Partner.

All WANODI and Virtual Ethernet destinations have to have unique names, meaning if you want to configure a partner name already present, you will get an error message.

(5) Choose the entry *Outgoing Dial number list* and press <Enter>.

(6) In the appearing window enter the dial number for this destination.

Use the following dial number scheme

Country code - Area Code - Subscriber number - PBX extension

Separate each of the parts from another with a hyphen.

> For detailed information on possible dial number schemes, see Chapter , section *Supported Dial Number Formats* (page 5-5).

(7) Press <Esc> and confirm the *Save changes message*.

The configured dial number will appear in the *Partner Configuration* menu. Different forms of this dial number are also stored in the Accepted number list.

> For additional information about the outgoing and accepted dial number list and their entries, see Chapter 3.22, *Fine Tuning Virtual Ethernet Call Destinations* (page 3-54).

Optional: Configure a static IP Address

If you want to use TCP/IP applications via an ISDN connection, you have to insert the destination's IP address in the corresponding entry.

Other tasks which have to be already completed:

- Configure the IP protocol.
- Bind the IP Protocol to your Virtual Ethernet Interface.
- Reinitialize the system.

Perform the following steps:

(1) In the *Partner Configuration* Menu, enter the IP Address of the destination in the corresponding field.

(2) Press <Esc> and confirm the *Save Changes message* to make the settings become active.

(3) Press <Esc> twice to leave the configuration window.

(4) Return to the *ITK NetBlazer 4400* main screen.

Configure a Test Virtual Ethernet Call Destination

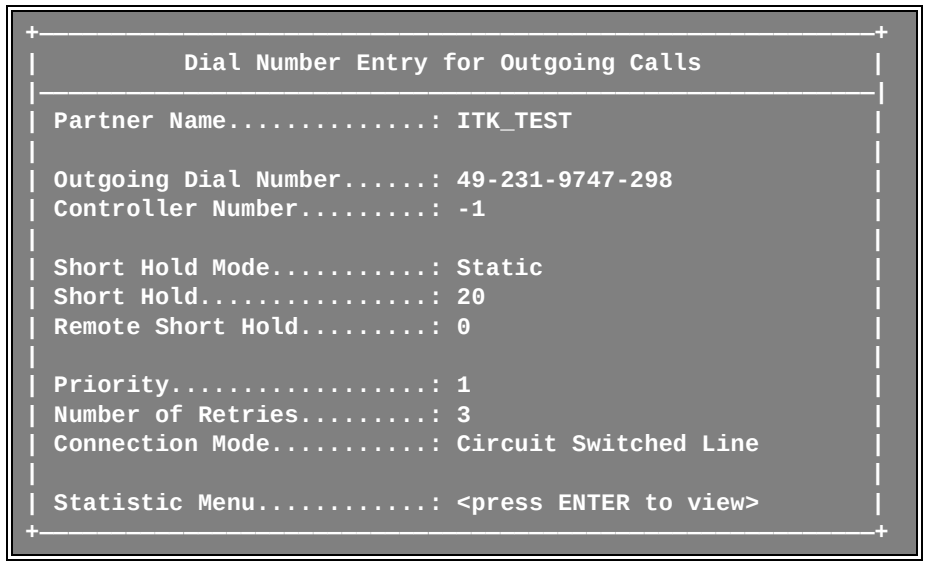
You should also setup a Virtual Ethernet Call destination to the ITK_TEST router in Dortmund, Germany to check the functionality of your Virtual Ethernet configuration.

The Call Entry requires the following settings:

- Name: ITK_TEST
- Outgoing Dial Number: 49 - 231 - 9747 - 298

All other parameters can remain in their default settings.

Enter the dial number in the *Dial Number Entry for Outgoing Calls* menu:



When you leave this menu, the *Partner Configuration* menu should look like this:

```
+-------------------------------------------------------------+
|              Partner Configuration                          |
|-------------------------------------------------------------+
| Name.....................: ITK_TEST                          |
| Virtual LAN Number.......: 0                                |
| Outgoing Dial Number List: 49-231-9747-298                  |
| Accepted Number List.....: 5 Entries                        |
| Callback.................: No                               |
| Protocol................. : Virtual-Ethernet                |
| PPP Parameter........... :                                  |
| Channel Bundling / MLP...: Disabled                         |
| Max Number of B channels :                                  |
| Media Type...............: 64 kbit/s                        |
| Action on Load...........: No Action                        |
| Sleeping Timeout.........: Disabled                         |
| Credit...................: No Limit                        |
| IP Address...............: 0.0.0.0                         |
| Time Restriction Options.: Disabled                         |
| Time Restriction.........: <press ENTER to modify>          |
| Connect Filters..........: <press ENTER to modify>          |
+-------------------------------------------------------------+
```

Before you establish a connection to ITK_TEST, verify that the IPX address you have bound to the Virtual Ethernet Interface is 9747298.

Perform the following steps:

(1) Switch to the *System Console* and type the following:

```
config
```

A list of all your defined network interfaces is displayed.

Your Virtual Ethernet Interface entries should look like the following:

```
IX1 Virtual-Ethernet  Driver for ISDN v2.00
Version 2.00 21 March 1997
Hardware Setting:
node address: 123456789012
Frame Type: ETHERNET_II
Board Name: VETHER_EII
LAN protocol: IPX network 09747298
```

If your LAN protocol entry differs, change it as described in Chapter 3.7, *Configure Bindings for the Virtual Ethernet Interface* (page 3-16).

Continue in the following way:

- Setup a Virtual Ethernet Call - See the next chapter.
- Define a Virtual Ethernet Call destination (PPP) - See Chapter 3.17, *Configure a Virtual Ethernet Destination (PPP)* (page 3-44).
- Fine Tuning Virtual Ethernet Calls - See Chapter 3.22, *Fine Tuning Virtual Ethernet Call Destinations* (page 3-54).

3.16 Setup a Virtual Ethernet Call

The call handling of Virtual Ethernet Calls is quite simple. It can be done from the *ITK NetBlazer 4400* main screen.

Perform the following:

(1) From the main screen, press the <Ins> key, select the remote partner you want to connect to, and press <Enter>.

The connection will be established. In the status screen window, the status changes from *going up* to *Outbound*.

Setup a Call to ITK_TEST

To check your system, setup a Virtual Ethernet call to the ITK_TEST router in Dortmund, Germany.

If you have already established a WANODI call to this destination, you have to release this connection first.

If your status screen displays an outgoing connection to ITK_TEST, you have a physical and logical connection to the router. You can check this by entering the command `display servers` on the server console. The ITK_TEST server will be among the servers displayed. From any client PC in your network, you may now log into the ITK_TEST server in Dortmund, Germany under the user name GUEST.

Release a Virtual Ethernet Call

To terminate a call to a destination manually, perform the following steps:

(1) Press <Del>.

(2) Select the partner you want to disable and press <Enter>.

The partner will be released and the call entry will disappear.

If you terminate a sleeping connection, the line will be set up before it is released to inform the partner about the end of connection.

3.17 Configure a Virtual Ethernet Destination (PPP)

The ITK NetBlazer 4400 supports various PPP features. There are special features for Virtual Ethernet Connections. Dynamic IP address allocation, Modem and GSM access, and Multilink features require a PPP connection.

This chapter describes additional configuration tasks for a destination using PPP and optionally, an authentication protocol.

Preliminary Tasks:

- Setup the Virtual Ethernet interface.
- Configure Protocol Settings.
- Configure Bindings for the Virtual Ethernet interface.

To setup a PPP call destination perform the following steps:

(1) Define a Call destination as described in Chapter 3.15, *Define a Virtual Ethernet Call destination (X.75)* (page 3-37).

(2) Change the Protocol entry from *Virtual Ethernet* to *PPP*.

(3) If you want to configure a PPP authentication protocol, refer to the next section.

Otherwise press <Esc> and confirm the *Save Changes message*.

Optional: Configure a PPP authentication protocol

The ITK NetBlazer 4400 provides the authentication protocols CHAP and PAP. Depending on the destination, you may select between a one-way and a two-way authentication.

For detailed explanations about the different authentication protocols, see Chapter , section *PPP Configuration* (page 5-19).

To configure the PPP authentication for a call destination, perform the following steps:

(1) In the *Partner Configuration* window, select *PPP Parameter*.

(2) Choose *Authentication method* and select the necessary protocol for this destination. If you select *Auto*, either PAP or CHAP is used, depending on the settings at the remote side.

(3) Change the direction entry from *Allow own authentication* to *Peer has to authenticate* if you want to perform a two-way authentication. If you select *Call Dependent,* the particular calling partner authenticates itself.

(4) Insert the System IDs and the Password.

By default, your router name is assigned as *Own System ID* and the Call destination Name is taken as *Remote System ID*.

(5) Change the entries according to your needs.

Remember that the system IDs and the Password have to agree on both sides.

All entries are case sensitive!

(6) Press <Esc> and confirm the *Save Changes message*.

Continue in the following way:

- Setup a Virtual Ethernet Call - See Chapter 3.10, *Configure a WANODI Call Destination (PPP)* (page 3-24).
- Fine Tuning Virtual Ethernet Calls - See Chapter 3.22, *Fine Tuning Virtual Ethernet Call Destinations* (page 3-54).

3.18 Leased Lines (D64S, D64S2)

The ITK NetBlazer 4400 is now capable of handing leased lines in a different way than previously. We can now access single B channels directly. This allows us to handle the channels more flexibly.

This new configuration is designed to be used with PPP only. On the other side of the line, there must be a router with the same functionality. This new way of handling D64S lines is not compatible with the way the ITK Basic controller handles leased lines without a B channel.

You can use the D64S2 with 2 B channels and PPP Multilink only in the virtual ethernet mode.

Configuration of the ISDN controller

Take the defaults and configure:

- use D-Channel Protocol DSS1
- use Point to Point
- use TEI =0

  To configure the controller, you have to edit the ix1.ini file for the controller handling of the leased line.

You have to change these lines:

- dProtocol= 2 ;2=DSS1 Euro-ISDN/NET3/ETSI
- lineAccess=2 ;1=Point to Multipoint, 2=Point to Point
- lineType=1 ;1=switched line, 2=leased line
- teiType=2 ;1=Auto TEI, 2=Fixed TEI
- teiValue=0 ;if TeiType = Fixed TEI, 0-63 are possible values

Configure the controller in the desktop of the router

Take the defaults and configure:

Choose any imaginary dialnumber.

- Enable Modem Access = "NO"

- Use for Virtual Ethernet = "NO"

Configuration of the Partner

Insert a new partner with any name.

Add the first dial number:

- Outgoing Dial Number "01"
- Controller Number <actual number of the controller used>
- Connection Mode "Semipermanent Line"
- Number of Retries "-1" (do forever)
- Short Hold Mode "Disabled"

Add a second dial number (only if you have D64S2)

- Outgoing Dial Number "02"
- Controller Number <actual number of the controller used>
- Connection Mode "Semipermanent Line"
- Number of Retries "3"
- Short Hold Mode "Disabled"

Configure the partner:

- Protocol "PPP"
- Channel Bundling "Disabled" for D64S
  "Static" for D64S2
- Action on Load "Call on Load"
- IP Address <IP Address of the partner>

  now you can establish a connection to the partner.

If you want to connect to the other router, you have to manually establish a connection from both sides! On both routers, you will find the information that the connection is listed as OUTBOUND.

3.19 Advanced Router Configuration features

This chapter describes settings which are responsible for the functionality of all Virtual Ethernet connections.

> For a detailed description of all parameters in the *Own Router Settings* menu, see Chapter 5.3, section *OWN Router Settings Menu* (page 5-40).

To make changes in the *Own Router Settings* menu, switch to the *ITK NetBlazer 4400* main screen, press <F10>, and select this item.

Defining an IP address range for Dynamic IP address allocation

Workstations or remote clients connecting the ITK NetBlazer 4400 via PPP may receive a dynamically assigned IP address instead of a fixed one. This feature reduces the configuration efforts on the client's side. During the call establishing process, the client receives an IP address from the pre-defined pool. This address remains active for the entire logical call duration, meaning even during Short Hold times. If a connection is released logically, the IP address returns to the pool and may be used by another partner.

The IP address range has to be within the IP net that you have assigned to the Virtual Ethernet Interface. Enter the start and the end address of the range, and additionally the IP address of the Virtual Ethernet interface of your system. The interface IP address has to be outside the IP address range. It is the same one you have bound to the Virtual Ethernet interface during your initial configuration in the INETCFG.

3.20 Advanced Controller Configuration features

The controller specific settings *Subscriber numbers* (MSN), *Access codes* and *Call acceptance* in this menu can only be edited if the controller is exclusively configured for Virtual Ethernet.

If a controller is used for WANODI and Virtual Ethernet connections simultaneously, these settings are established in the *Network Interface* section of the INETCFG program.

The configuration is described in Chapter 3.12, *Fine Tuning the WANODI Interface* (page 3-28).

In this menu, you configure the option for analog access, and a shared use of one controller for Virtual Ethernet and WANODI calls. If you have more than one controller and one of them is defined only for Virtual Ethernet, you may also edit subscriber numbers, Access codes, and Basic Security Services.

To make changes in the Controller Configuration menu, switch to the *ITK NetBlazer 4400* main screen, press <F10>, and select this item.

Enabling Modem Access

You should enable modem access only if you have installed an ITK MultiModem board or an ITK DigitalModem board, and you want remote access over analog media such as modem and/or GSM.

If you have enabled modem access, a shared use of the line with a telephone is no longer possible without advanced configuration efforts because the router also answers voice calls. In this case, a dedicated MSN has to be configured for the ITK NetBlazer 4400.

Reserve B channels for Virtual Ethernet Calls

By default, either a WANODI or a Virtual Ethernet connection can be established if a free B channel is present. You may reserve B channels for Virtual Ethernet connections, meaning a WANODI call request may be rejected even if a B channel is actually available. Enter the number of B channels reserved for Virtual Ethernet connections in the corresponding field.

If you don't want to connect Virtual Ethernet connections over this controller, change the entry *Use for Virtual Ethernet* to *No*.

Continue in the following way:

- Fine Tuning Virtual Ethernet Call destinations - See the next chapter.

3.21 Example of Masquerading Configuration

This section describes the most common configuration steps for connecting a network to the internet over a T-Online account.

Configuration Example: Connecting a network to the internet over a T-Online account (single account).

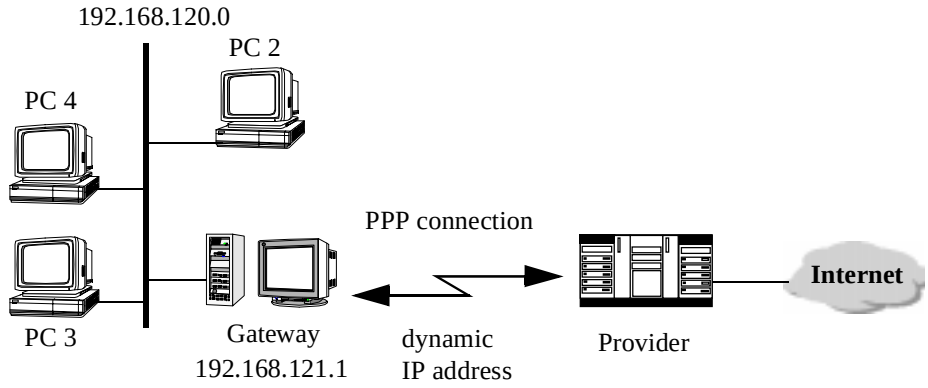


Fig. 3-2 Example for a network with IP masquerading

To configure the configuration example, perform the following steps:

Public IP address for the LAN

(1) Use for the LAN an public IP address, in our example, 192.168.120.0.

Define a pseudo IP address for the ISDN (Internet)

(1) Start the INETCFG program:

```
load inetcfg
```

(2) In the INETCFG *Internetworking Configuration* menu, select the *Bindings* menu item and press the <Ins> key to select the network protocol TCP/IP.

(3) Select the *A Network Interface* entry, choose the Virtual Ethernet interface and confirm your selection using <Enter>.

A menu will appear.

(4) Change to the *Local IP Address* entry in the following menu, and specify your IP address that you want to assign to the Virtual Ethernet Driver, in our example 192.168.121.1.

(5) Set *Subnet Mask of Connected Network* to entry (FF.FF.FF.00).

(6) Disable the options *RIP* and *OSPF*.

(7) Do not change The *Expert TCP/IP Bind Options*.

(8) Exit the submenu by pressing the <Esc> key, and confirm the settings with *Yes* and press <ESC> again.

Define a pseudo address for the Default Route

(9) In the INETCFG *Internetworking Configuration* menu, select the *Protocols* menu item and press <Enter>.

(10) Select the *TCP/IP* protocol and press <Enter>.

(11) Enable the option *Static Routing*.

(12) Select *Static Routing Table*.

(13) Insert a new Route.

(14) Select the menu item *Route to Network or Host* and press <Enter>, and choose *Default Route* and press <Enter>.

(15) Press <Ins> and select *Next Hop Router on Route,* and then enter the IP address 192.168.121.2.

Add the partner

(16) Start the IX1CCA program:

```
load ix1cca
```

(17) Press <F10>.

The *Own Router Settings* window appears.

(18) Select the menu item *Partner Configuration*, and press <Enter> and <Ins>.

(19) Enter a Name, for example, T-Online.

(20) Select the menu item *Outgoing Dial Number List* and then enter the dialnumber 0049-231-191011.

(21) Select the menu item *Protocol* and then *PPP*.

(22) Select the menu item *PPP Parameter,* and the submenu *Authentication Method* and then *PAP*.

(23) Select the menu item *Direction* and then *Call dependent*.

(24) Select the menu item *Password* and then enter *<your Password>*.

(25) Select the menu item *Own System ID* and then enter your *User ID*. This User ID will send you from your Internet Service Provider, in our example, T-Online.

The User ID contains the following parts:

- subscriber identification, subscriber number, # and co-owner identification.

(26) Select the menu item *Media Type* and then enter *64 kbit/s.*

(27) **Do not enter** an IP address.

Activate the dynamic IP acception

Select the *Own Router Settings* window.

(28) Choose in the *Own Router Settings* window the menu item *IP Configuration* and press <Enter>.

(29) Enable the menu option *IP Masquerading*.

(30) Enter as *Masquerading Partner* T-Online.

(31) Enable the *IP Acceptance*.

(32) Enter as *Routing Address* 192.168.121.2.

Now the configuration for the example is complete.

Reinitialize the system in order to activate the changes. Proceed as follows:

(33) From the Server *System Console* type:

```
ri
```

3.22 Fine Tuning Virtual Ethernet Call Destinations

By default, Virtual Ethernet call destinations are configured for a standard use in a typical environment. It may be useful and in some cases even necessary to adapt parameters to individual needs.

This chapter gives an overview of the tuning options for Virtual Ethernet connections.

> For a detailed description of the configurable parameters in the different menus, see the corresponding sections of *Chapter 5, Reference for ITK NetBlazer 4400* (page 5-3).

Configuring the _default partner

The _default partner is automatically initialized during router installation. The settings for this partner are the default ones for every newly configured destination. Unknown dial in partners will also take over the _default partners settings.

As the settings for different media may differ, the ITK NetBlazer 4400 has a _default partner for every supported medium.

Configuring an outgoing number list

The option of assigning more than one dial number to one destination guarantees a high degree of connection security. If a connection can’t be established over one dial number, the router tries to connect via the next number of the dial number list.

Every dial number entry contains information about the controller to be used to establish a call, Short Hold parameters, the Priority, Number of Retries, and the Connection Mode.

A simple example explains this functionality:

A connection between two partners is established via a permanent connection and a leased line. As a backup line and for a better security, a conventional circuit switched line is used.

As a permanent line connection requires a fixed defined controller; the controller number is changed from -1 (any controller may be used for calling) to a dedicated value, for example 0.

A dial number with a lower priority value has a higher priority, so the permanent dial number entry gets the priority 1, the backup line entry the value 2. If a connection fails after a certain number of retries, the router automatically tries to establish a line with the dial number entry of the next priority.

To configure additional dial numbers to a destination perform the following steps:

(1) From the *Router* main screen, press <F10> to open the *Router configuration* window and select *Partner configuration*.

(2) Choose the partner entry you want to edit, select *Outgoing dial number list,* and press <Ins>.

A list of already defined dial numbers with their corresponding configuration is displayed.

(3) Press <Ins> again and enter the values for the new dial number.

(4) Press <Esc> and confirm the *Save Changes message*s.

Configuring an accepted number list

For every configured outgoing dial number in the requested dial number format, different entries apply in the accepted number list as automatic entries. If the Basic Security Service of ITK NetBlazer 4400 is enabled (Call acceptance = accept only registered numbers) and the transmitted dial number doesn't correspond to the automatically configured entries, you may manually define additional accepted dial numbers.

Changing the Media Type

The ITK NetBlazer 4400 also supports remote access with a modem or a mobile phone (GSM). In this case, the system has to be equipped with an ITK MultiModem board or an ITK DigitalModem board. For some ISDN connections to or within the USA, the transfer rate has to be changed to 56 kbit/s.

Preliminary Tasks:

- Enable Modem Access for the Controller - See Chapter 3.20, *Advanced Controller Configuration features* (page 3-49).
- Define a Virtual Ethernet Call destination - See Chapter 3.15, *Define a Virtual Ethernet Call destination (X.75)* (page 3-37).

Perform the following steps:

(1) From the *Router* main screen press <F3> to open the *Configure Partner* window.

(2) Choose the partner entry you want to edit and select *Media Type*.

(3) Change the media type for this partner according to your needs.

(4) Press <Esc> and confirm the *Save Changes* request.

The new media type applies in the Partner configuration.

Configuring the Action on Load

By default, all Virtual Ethernet calls have to be initialized manually after a router restart. For some connections it may be useful to change this parameter, meaning initiate an automatic call setup after a router restart or disable a partner automatically.

Configuring the Short Hold

You may define the Short Hold Mode as well as the Short Hold Value, that is the time interval before an inactivity timeout, if no user data is transferred for every dial number in the outgoing dial number list. Remember to set the Short Hold Value according to the charging interval. There is no need to release a line after 20 seconds, if the charging interval lasts 120 seconds. In this case, a Short Hold Value of 100 seconds may make sense.

If you have configured a Dynamic Short Hold mode and no charging *indications* are transferred during the connection, the static Short Hold value is taken instead.

If the Short Hold values of a connection are different, the inactivity timeout will be processed after the shorter time.

If both partners have configured a remote configured Short Hold, the feature is disabled!

If the Short Hold mode is disabled, the connection remains active the entire time. This setting is only useful for leased line, where connection- time- dependent charges do not occur.

Configuring the Sleeping Timeout

The Sleeping Timeout defines the time after which a sleeping connection is also released logically, meaning the router stops packet spoofing.

Configuring Credits

Credits can be set to restrict outgoing calls to prevent uncoordinated connection costs. They may be restricted by charging units or connection times, defined for different intervals and imposed by an expiration date.

If a credit is expired, all further connection requests will be rejected.

If more than one credit parameter is set, for example 100 units and a connection time of 2 hours, further connection is not possible after the first limit is reached.

Configuring Time Restrictions

The time restrictions are either configurable for outgoing, or for incoming and outgoing calls. Alternatively, you may restrict NDS caused connections. In a matrix, you may define time periods when outgoing connections are possible. It may be useful to restrict calls on weekends or during evening hours. By default, no time restrictions are set.

A detailed description of the Time Restriction functionality to suppress NDS data traffic is given in Appendix A.

Configuring Filters

The ITK NetBlazer 4400 has multiple filters for different IPX/SPX and IP control packets. In general, the pre-defined filter settings should not be changed unless absolutely necessary. An overview of the individual filters and their functionality is given in the reference chapter.

Changing the Connection Mode

The connection mode can be set for every entry in the outgoing dial number list. If you change the default, keep in mind that your controller has to be configured for the corresponding connection mode, and that the Controller number entry in the outgoing dial number list must not be -1 (any ISDN controller configured for Virtual Ethernet may be used). A semi-permanent line is only defined for the German 1TR6 ISDN protocol.

Activating Channel Bundling

If you want to increase the transfer rate of one connection, you may bundle B channels to one virtual connection. The ITK NetBlazer 4400 offers two channel bundling options: static (that means the router tries to establish the maximum number of B channels) and load dynamic. The load dynamic channel bundling depends on the amount of data to be transferred, and a B channel is added or removed automatically.

Prerequisites for a successful channel bundling are

- The channel bundling has to be activated on both sides.
- Sufficient B channels have to be present.
- The dial number has to be transmitted correctly.

Activating Callback

The callback functionality is a security mechanism as well as an option for collecting charges on one side. If callback is activated for a partner, an incoming connection request is considered and rejected by the system. The router then establishes a call by itself.

Do not activate the callback on both sides. If you do, the partners request and reject their connections mutually.

4 Supervising ITK NetBlazer 4400

4 Supervising ITK NetBlazer 4400

Convenient and detailed information about all actions concerning ISDN connections is an important feature of the ITK NetBlazer 4400. With its ISDN Communication Manager IX1CCA, you configure the partners using Virtual Ethernet connections. Furthermore, you can monitor **all** ISDN connections and view statistics for both WANODI and for Virtual Ethernet connections in the ISDN Communication Manager.

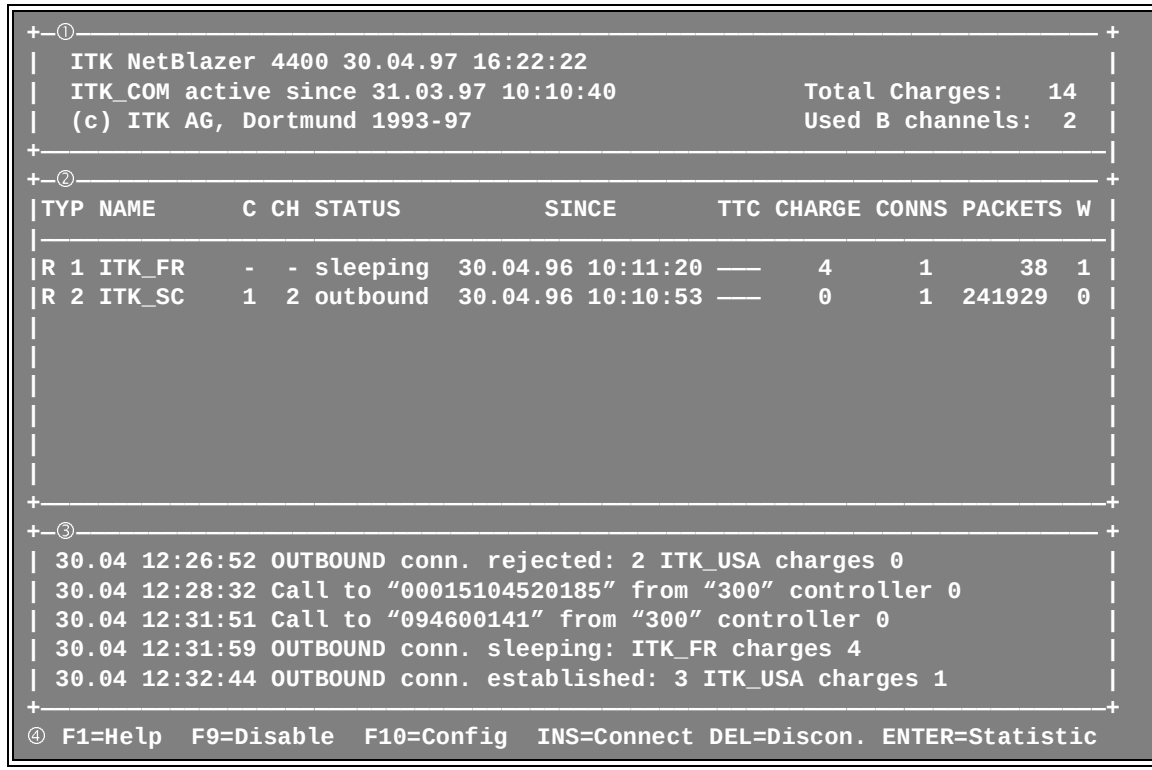
In particular, this chapter will introduce you to

- the Function Keys and their use
- the ISDN Communication Manager
- the Activity Log and the file IX1CCA.TRC
- the statistics and what they mean

4.1 The ISDN Communication Manager

IX1CCA Main Screen

The main screen of the IX1CCA ISDN Communication Manager is divided into four sections:



Section	The following is displayed here
①	left • Product name and version • Server name and starting time of the ISDN Communication Manager • Copyright information right • Date and time • The total charges incurred since starting the ISDN Communication Manager • Number of B channels currently being used
②	Current connection data
③	Information about actual router activities
④	Current operating help information

Section ② of the main window (the IX1CCA “status window”) displays connection status information. Active connections are listed in alphabetical order. To display more information concerning a particular connection, select the corresponding line with the <Enter> key.

The journal window ③,which is below the main window, displays, the five most recent router events logged during a connection or disconnection. To see earlier journal entries, press the <Tab> key. The journal window will be enlarged to show more entries. Using the <Pg Up> and <Pg Dn>, or the cursor keys, you can display up to 200 journal entries. For more information, please refer to Chapter 4.2, *Connection Journals and Activity Log* (page 4-11).

To return to the status window, press the <Tab> key.

Using the Function Keys

For manual call handling and configuration of the ITK NetBlazer 4400, you use different function keys. The most common keys and their meanings are listed as follows:

For a detailed description of all keys, see Chapter 5.4, *Reference for the ISDN Communication Manager* (page 5-57).

Common Keys

Key	Meaning
<Enter>	Select and Confirm *Router Actions*
<Tab>	Switch between *IX1CCA* Main Screen and *Activity Log* window
<F1>	Display *help topics*
<F2>	Import WANODI configuration changes
<F3>	Open the *Partner Configuration* menu
<F4>	Reset displayed statistic information
<F5>	Trace connection responsible packets
<F10>	Open *Router Configuration* window

Line Handling Keys

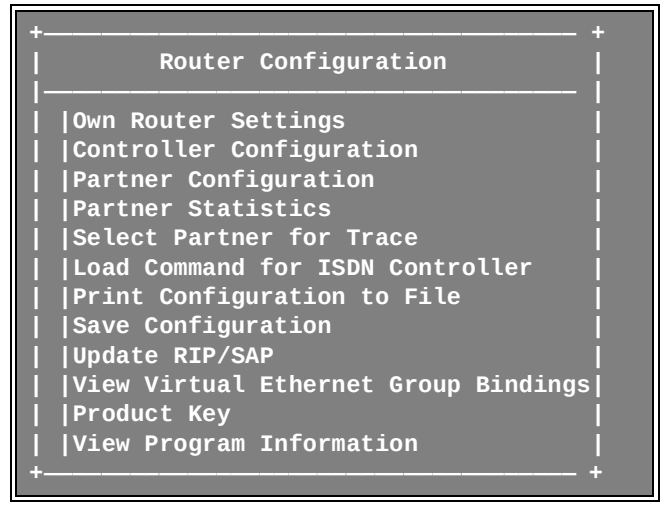
Key	Meaning
<Ins>	Establish a Virtual Ethernet connection
<Del>	Release a Virtual Ethernet connection
<F6>	Reset partner credits
<F9>	Disable a connection
<Alt>+<F9>	Force a connection Short Hold

Manual WANODI connections must be established and/or released by the Novell Call manager utility CALLMGR.

All other keys and their functionality may be used for both WANODI and VIRTUAL ETHERNET connections.

Main Router Configuration Menu

Press <F10> to enter the main *Router Configuration* menu.



The menu items *Own Router Settings*, *Controller Configuration* and *Partner Configuration* with their parameters are described in Chapter 5.3, *Reference for Virtual Ethernet Related Items* (page 5-40).

The menu item *Partner Statistics* makes it possible to display detailed statistics for each individual remote partner. For further information, see Chapter 4.3, *Statistics* (page 4-13).

In the Menu *Select Partners for Trace*, you may define those partners which will be traced by the IX1LANZ analyzer tool. For further information, see Chapter 4.2, *Connection Journals and Activity Log* (page 4-11).

Using the *Load Command for ISDN Controller* item, you can select and configure the hardware that is loaded automatically during system startup.

By selecting the *Print Configuration to File* menu item, you can save the current configuration of the router and the remote partners entered in the IX1CCA.PRN file.

The menu item *Save Configuration* stores the actual configuration and partner settings into the router database. This will also be performed automatically, if the router is unloaded and/or restarted.

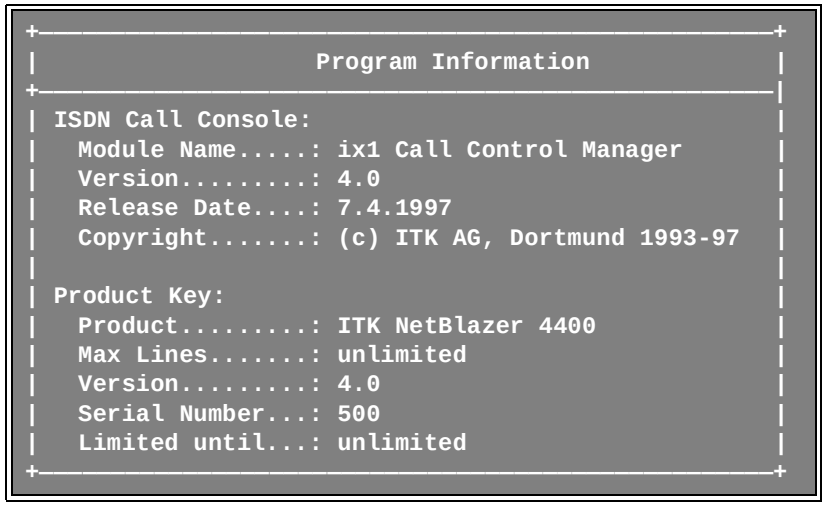
By selecting the menu item *Update RIP/SAP*, all of the Virtual Ethernet connections can be physically established in order to update all of the routing and service information.

By selecting the *View Virtual Ethernet Group Bindings* menu item, you open the *Virtual Ethernet Group Bindings* window, which displays the protocol bindings for the Virtual Ethernet groups you configured.

The entries in the *View Virtual Ethernet Group Bindings* window are described in detail in Chapter 5.3, *Reference for Virtual Ethernet Related Items* (page 5-40).

You can select the *Product Key* menu item to display the Product Key or re-enter it.

When you select the *View Program Information* menu item, the *Program Information* window will appear.



This window provides the following information on the installed router:

- Information on the currently running module of the ISDN Communication Manager:

- Module name
- Version number
- Release date
- Copyright

- Information on the Product Key:
  - Product name
  - Number of possible connections (unlimited means that the number of possible connections is limited only by the number of available B channels.)
  - Serial number
  - Software validity (unlimited; beta versions have “validity date” in this field)

Status Window

The Status Window is located in Section ② of the *ISDN Communication Manager* main screen. The entries may appear as in the following example:

```
+—②————————————————————————————————————————————————————————————+
|TYPE NAME   C CH  STATUS    SINCE           TTC  CHARGE CONNS  PACKETS W|
|———————————————————————————————————————————————————————————————|
|R 1 ITK_FR  -  -  sleeping 31.01.96 10:11:20 ——    4      1         38 1|
|R 2 ITK_SC  2  1  outbound 31.01.96 10:10:53  68    0      1     241929 0|
```

The following information about every logical active connection will be displayed:

Entry	Meaning
TYPE	Indicates the connection type: Virtual Ethernet (R), WANODI (X), PPP (P) or Remote Workstation (W), (G) V.110 (GSM) and (M) Modem.
NAME	Destination Name as configured in the partner configuration menu.
C / CH	Number of the used controller and the established B channels for this connection.

Entry	Meaning
STATUS / SINCE	Actual connection status and the date and time when this status was set.
TTC	Displays the remaining time until a call teardown for an active connection.
CHARGE /CONNS	Amount of charge units and number of physical connections since the router start.
PACKETS	Number of Data packets exchanged since the router start
W	Number of possible warning messages

A more detailed description of every parameter is given in Chapter 5.4, *Reference for the ISDN Communication Manager* (page 5-57).

4.2 Connection Journals and Activity Log

Although the *IX1CCA Main Screen* (page 4-3) displays only the last five lines of the connection journal, you can enlarge the journal window to approximately 20 lines by switching to the Activity Log window by pressing the <Tab> key. In addition, by using the cursor keys, you can scroll back through as many as 200 lines of the record. It is here you will also find important start and initialization messages generated when the router was restarted.

The journal window may look like the following example:

```
28.02 14:54:07 OUTBOUND conn. sleeping: ITK_FR charges 0
28.02 14:54:13 Connecting to Partner ITK_FR upon user request.
28.02 14:54:13 Call to “00033112345678” from “298” controller 0
28.02 14:54:13 OUTBOUND conn. established: ITK_FR
```

If you have to restart your router, the journal information recorded until that time is not lost.

Trace File IX1CCA.TRC

Every entry displayed in the Activity Log Window is simultaneously written into the IX1CCA.TRC journal file in ASCII format. Journal entries are added to this trace file up to a maximum size of 200 KB.

If IX1CCA.TRC exceeds the maximum size of 200 KB, it is automatically renamed IX1CCA.BAK. If an old IX1CCA.BAK file already exists, this file is automatically overwritten.

If you want to process your journal file “manually” or automatically using your own program, – for example, if you want to compute long term connection statistics or connection costs – you must make sure that you rename or process the IX1CCA.TRC file, or the IX1CCA.BAK file in time, that is, before it is overwritten.

In most cases, about 2,500 journal entries can be stored in the IX1CCA.TRC file. Every ISDN connection and disconnection generates at least one journal entry. If there are errors or if the line is busy, you will get several additional entries, so you can estimate how fast the journal file will reach its maximum size of 200 KB, based on your own typical traffic volume.

Accounting File IX1_ACC.DAT

Every inbound or outbound ISDN connection is recorded in the file SYS:SYSTEM/IX1_ACC.DAT.

Every connection generates a line in this file.

The lines have the following format:

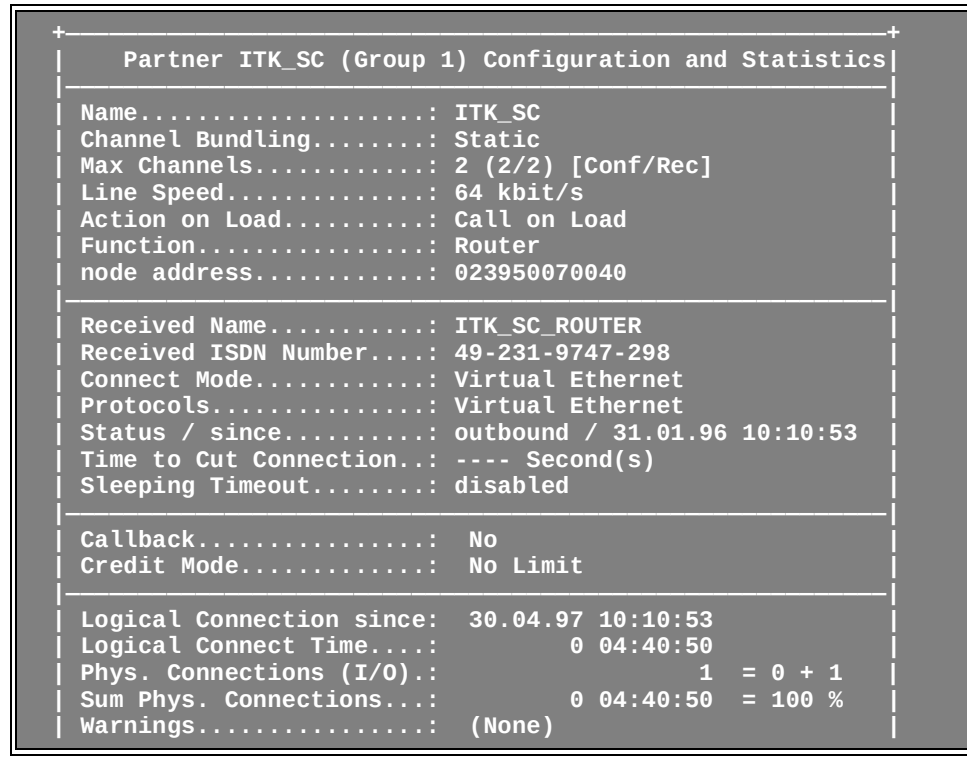
```
Starting  Ending    Duration    Fees  outbound  Partner      Connection Rate /
Time      Time                        or        name         Protocol
                                      inbound

17.04.97  17.04.97  0 00:01:04  1     OUT       ITK_BERLIN   64 kBit
04:15:39  04:16:43

17.04.97  17.04.97  0 00:01:50  0     IN        ITK_HAMBURG  33600 V.42 V.42bis
04:19:51  04:21:41

17.04.97  17.04.97  0 00:01:50  0     IN        ITK_HAMBURG  19200 V.42 V.42bis
04:21:51  04:23:41

17.04.97  17.04.97  0 00:01:50  0     IN        ITK_HAMBURG  33600 V.42 V.42bis
04:23:51  04:25:41
```

4.3 Statistics

Common Statistics

One of the special strengths of IX1CCA is that it provides detailed information to the network administrator on all current logical ISDN connections. It performs this function primarily in the Status Window, as discussed in detail in section *Status Window* on page 4-9, and provides important connection data, such as accumulated charges and connection information.

Further information is required in order to optimize the data throughput in the overall network and the accessibility of remote partners, while at the same time minimizing ISDN connection costs.



Call History	Current	Last	Total
Call Duration...	0 04:40:50	0 00:00:00	0 04:40:50
Short-Hold Pause	0 00:00:00	0 00:00:00	0 00:00:00
Channels.....	2	0	
Charges.....	0	0	0
Packets Tx.....	83.696	0	83.696
Packets Rx.....	70.468	0	70.468
Bytes Tx.....	23.252.515	0	23.252.515
Bytes Rx.....	4.986.340	0	4.986.340

Call Statistics	Minimum	Maximum	Average
Call Duration...	0 00:00:00	0 04:42:07	0 04:42:07
Short-Hold Pause	0 00:00:00	0 00:00:00	0 00:00:00
Channels.....	1	2	2,00
Charges.....	0	0	0,00
Packet Size Tx..	30	1.502	277
Packet Size Rx..	30	1.502	70
Packets Tx.....	0	83.696	83.696
Packets Rx.....	0	70.816	70.816
Bytes Tx.....	0	23.474.766	23.474.766
Bytes Rx.....	0	5.006.210	5.006.210

Performance	Actual Speed	Ø Curr. Call	Ø All Calls
Packets/sec Tx..	21	4,95	4,95
Packets/sec Rx..	14	4,16	4,16
Bytes/sec Tx....	8.681	1.381	1.381
Bytes/sec Rx....	666	294	294

The IX1CCA ISDN Communication Manager offers the aforementioned adjustment and statistical data, as well as a number of measurement values which may be useful for optimization purposes *for every connection*.

For an existing connection, you have two options for displaying the information:

Option 1

(1) Position the cursor in the connection line you are interested in, and press <Enter>.

(2) To display this detailed information for connections which are currently not in use, go to the Status Window and position the cursor *under the most recent connection*, and then press the <Enter> key.

(3) Using the connection partners dialog box, select a remote partner and instruct the program to display detailed information on previous connections.

Option 2

(1) From the *IX1CCA* main screen, press <F10> to open the *Router Configuration* menu.

(2) Choose the *Partner Statistics* entry and select the corresponding destination in the *Partner Statistics* menu.

The *Partner Configuration and Statistics* menu will appear.

The information displayed is initialized for every connection at the start of the router and measured from this time forward. You can also reset these statistics to zero using the <F4> function key.

The statistical information shown on page 4-13 and on page 4-14 are a single logical screen, in which you can move backwards and forwards using the cursor keys, and the <Pg Up> and <Pg Dn> keys. Values concerning an existing connection are updated every second.

The first block (*Call History*) on page 4-14 provides information on the existing connection in comparison with the preceding connection and with the overall values of all connections.

The second block (*Call Statistics*) on page 4-14 displays the minimum, maximum, and average value for all connections with regard to the same entries.

The third block (*Performance*) on page 4-14 provides a series of measurement values with respect to the throughput rates observed on the connections. It must be assumed that these throughput rates also contain all of the protocol elements transferred over the ISDN lines. Transfer pauses, during which the application or user is neither transferring nor downloading data, are also counted. Thus, depending on the application, the observed peak transfer speed values can differ considerably from the average values.

Against this background, the performance measurement data block displays 3 columns:

`actual speed`	the transfer rate observed in the *last second*,
`ø curr call`	the average transfer rate of the current connection, and
`ø all calls`	the average transfer rate to this remote partner for *all connections*

If you observe these messages during operation, you will notice that the data rate achieved per second varies between 0 and about 23,000 bytes/s per connection direction, depending on the type of application, if you work with *one B channel*.

> These data rates correspond to bit rates of up to 180 kbit/s on a single B channel. Such values can be achieved only by using the “on-the-fly” data compression feature of the ITK boards.

The last block of the statistical information screen shows the number of IPX packets transferred and received for this connection, as well as their sums. By comparing the transfer rates of different types of packets, the filter’s effectiveness can be estimated, and the ratio between control data and payload data can be determined.

Outgoing Call Statistics

To display statistical information on every outgoing dial number used for an outbound connection to a remote partner, perform the following steps:

(1) In the main screen of the ISDN Communication Manager, press the <F3> function key.

(2) From the *Configure Partner* menu, select the partner you want and press <Enter>.

(3) Now select the entry ***Outgoing*** *Dial Number List* and press <Enter>.

(4) Select the dial number you want and press <Enter>.

The *Dial Number Entry for Outgoing Calls* menu will appear.

(5) Select the *Statistic Menu* entry and press <Enter> to display the statistics for the selected outgoing dial number.

A detailed explanation of the statistic parameters is given in Chapter 5.3, *Reference for Virtual Ethernet Related Items* (page 5-40).

Incoming Call Statistics

To display statistics on an **incoming** connection, perform the following steps:

(1) In the *ISDN Communication Manager* main screen, press the <F3> function key.

(2) From the *Configure Partner* menu, select the partner you want and press <Enter>.

The *Partner Configuration* menu will appear.

(3) Select the ***Accepted** Number List* entry and press <Enter>.

(4) Select the dial number you want and press <Enter> to display the statistical data for the selected incoming dial number.

A detailed explanation of the statistic parameters is given in *Chapter* *5.3, Reference for Virtual Ethernet Related Items* (page 5-40).

4.4 Evaluating Statistics

The control values mentioned in the preceding chapter cannot be evaluated according to a pre-determined method. Rather, the network administrator must evaluate each one individually, based on the overall configuration from the point of view of the LAN and ISDN, and applying customized criteria, depending on the requirements of the application and the company.

Nonetheless, certain measurement values are always important for evaluating the *Quality of Service* with regard to *costs*, *performance*, and *accessibility.*

To evaluate *accessibility*, we recommend studying the journal in the journal window, consulting a printout of the journal, or at least reviewing and evaluating the journal file (IX1CCA.TRC or IX1CCA.BAK) on screen with the aid of an ASCII Editor.

Some of the most important measurement values for evaluation purposes are shown in the following figure, which is taken from the screens shown on page 4-13 and on page 4-14 and are designated with ①, ②, ③, etc.

```
........
........
Sum Phys. Connections...:        0 00:12:02  =   5 %  ①
........

........
........

Call Statistics          minimum          maximum        average

Call Duration...     0 00:00:44       0 00:03:13  ②  0 00:01:52
Short-Hold-Pause     0 00:10:34    ③  0 01:46:23  ③  0 00:31:48
Channels........             1              ④  1         ④  1,00
Charges.........             3              10           4,05
Packet Size Tx..            40         ⑤  1.502        ⑥  1.212
Packet Size Rx..            45         ⑤  1.502           ⑥  928
Packets Tx......            15         ⑦  4.132        ⑦  3.879
Packets Rx......            27         ⑦  3.266        ⑦  2.920
.....
.....

Performance        actual speed      Ø curr call    Ø all calls

Packets/sec Tx..
Packets/sec Rx..
Bytes/sec Tx....       ⑧  16.012          11.545        ⑨  6.075
Bytes/sec Rx....       ⑧  5.724           4.684         ⑨  2.991
```

Fig. 4-1 Important measurement values for evaluating costs, performance and accessibility

Evaluating the accessibility of your router

Poor accessibility of the router can only occur if you use several Virtual Ethernet connections, and the B channels that are available to Virtual Ethernet are continually insufficient to meet the number of simultaneous call requests. There are several options for improving such a condition, although some of them may be costly. Thus, the first step is to analyze the situation carefully.

Complaints from users are one way of alerting you to insufficient router accessibility; but you can already be aware of this problem by simply consulting the status window:

Example:

> You have equipped your router with 2 ISDN controllers, and therefore 4 B channels are available. At the same time, however, 8 remote partners with Virtual Ethernet are using these 4 ISDN channels. If all 4 B channels are basically busy all the time, your accessibility is poor! On the other hand, if only 3 of the 4 B channels are busy about 60% of the time, you probably do *not* have an accessibility problem.

You may also find additional information on this subject in the journal. If you frequently come across entries indicating that your router was not able to establish Virtual Ethernet connections with remote systems, you probably have some congestion in your configuration.

If you do need to improve the accessibility, you have to add additional ISDN controllers. To save on costs, however, you should first check whether the existing channels can be used more efficiently. To do this, you first need to check all of the Virtual Ethernet connections to see whether users really need the B channels for as long as they do at a given time: reducing the short hold times could possibly lead to a substantial improvement of router accessibility! In addition, a WANODI connection could be possibly transformed into a Virtual Ethernet connection, thus freeing up a controller and improving the accessibility accordingly.

First of all, collect the statistical data for your connections over a sufficiently period of time (several hours of a typical workday) and then evaluate the following statistics values for all connection destinations:

① If the physical occupancy of a logical connection is very high (for example, over 50%), this line is certainly a good candidate for a WANODI connection, as opposed to a Virtual Ethernet connection. If the value is under 20%, you should definitely consider whether a Virtual Ethernet connection should be used, if you are not doing so already.

②, ⑦ If the ratio of the average connection duration and the average number of packets transferred per connection is unacceptable, it could be that the short hold value for this connection has been set too high. It often happens, in particular in communications with workstations, that only one mailbox access is being accessed

or one file is being copied, without any other data being exchanged during the rest of the time: in such application situations, it makes sense to set the short hold value to about 40 seconds, even for local calls, and not to wait for the full duration of a charge signal.

③ If the average and even the maximum short hold time between two connections is very short, you should arrange for this connection to be operated as a point-to-point connection, in order to establish this connection at any time independently of other connections.

Evaluating the performance to a remote partner

The actually achieved performance in terms of an average achieved transfer rate on a connection can be determined by using a number of parameters contained in the displayed statistical data; based on this information, deductions can be made and corrective measures for the optimization can be investigated.

⑧, ⑨ By observing this "line speed indicator" for the logical connection, you can get a good impression of the punctual performance. If the displayed value (which changes every second) never reaches a value greater than 8,000 byte/s, the remote partner probably does not have an ISDN adapter with compression. A displayed value that fluctuates between 5,000 and 17,000 bytes is typical for *one* B channel with compression. This value can be much higher if you also use channel bundling! Experience has shown that the average value for a logical connection (average of all physical connections) can be much lower than the displayed peak values, depending on the application.

④ If the maximum value of the bundled channels does not correspond to the value configured by you, the remote partner, or even your own router does not have enough (free) controllers, or the remote partner has not set the maximum number of channels requested by you. If the maximum value is the same as the maximum value selected by you, but the average value is significantly *below* this amount (for example maximum value = 4, average value = 1.2), and the connection in question is a Virtual Ethernet connection, this could be a sign that the desired number of B channels is almost never available because they are being occupied by other connections! You should then check the short hold parameters of the other connections!

③ If the average value of the short hold pauses is extremely short (only a few seconds, for example), it could be that the short hold value for this connection has been set too short, leading to unnecessary waiting times for setup. In this case, you should set the short hold parameter to a higher value, such that it does not immediately trigger a teardown during shorter transfer pauses.

⑤, ⑥ If the maximum and average packet sizes vary widely from each other (more than 50%), it could be that this connection is being used primarily by an application transporting very small quantities of data. If the user of this connection even notices the low performance, the router cannot optimize the performance, which can be improved only by improving the transport functionality of the application.

Is a connection incurring overly high costs?

To analyze the transfer efficiency of a connection:

⑤, ⑥ Check to see whether the average number of packets transferred is noticeably low! If you determine, at the same time, that connections are established quite frequently and only very few packets are transferred in every connection, it could be that a filter has not been set correctly, causing connections to be established that do not carry any useful data from the standpoint of the user. If you press <F5> and answer the following question *Start tracing connect packets?* with `Yes`, the program displays the following information in the Activity Log concerning packets that lead to a connection establishment:

- Transfer protocol
- Packet type
- Transmitter address
- Receiver address

If you are not able to prevent the undesired establishment of connections by adjusting the filter, you can proceed to determine which protocol or application is causing the permanent establishment of connections by “disconnecting” the protocols or applications one-by-one. You can then decide how to arrive at a permanent solution to the cost problem.

②, ⑤ If you are using channel bundling and the average call duration indicates that basically all of the calls can be made within a single charge signal, you should try to operate this connection without channel bundling! You will probably find that most of the connections can be established within the duration of a single charge unit, thus saving considerably on line charges!

③ If you observe that the average short hold pause lasts only a few seconds (in other words, the short hold pause is short compared to the charge signal), you should try to extend the short hold time, in order to use the charge signal more effectively, and therefore cut back on costs.

By reviewing this statistical data on a regular basis, you will develop a “feeling” for *good* and *bad* values, and probably discover even more ways of using the displayed data!

4.5 Trace Tool for LANalyzer for Windows

The IX1LANZ module records all of the packets between the ISDN Router and the remote partner, and stores them in the “sys:etc” registers in the file designated as a parameter when loading the program. Using the IX1LANZ trace tool, you record the packets in the *LANalyzer for Windows* format. The LANalyzer for Windows is a Novell product.

Select Partners for Trace

By default, the packet transfer for all configured and actually active partners will be traced when you activate the IX1LANZ tool. If you have multiple active connections at the same time, this may cause a large amount of unnecessary data.

Therefore you may exclude partners,so that you only trace those connections which may cause problems. To select the partners for trace perform the following steps:

(1) Press <F10> to open the *Router Configuration* menu.

(2) Select the *Select partners for trace* menu item and press <Enter>.

All configured partners will be displayed. Partners which will be traced are displayed in yellow, partners not traced are displayed in white.

(3) To exclude a partner from being traced, put the cursor to this partner and press <Enter> or <Del>.

The excluded partner flashes and will be displayed in white if the cursor is turned off.

(4) Repeat the previous step for every partner you want to exclude from being traced.

(5) Press <Esc> and <Enter> when recommended to save the changes and return to the *IX1CCA* main screen.

(6) Press <Esc> and confirm the *Save changes* request.

If you now start the IX1LANZ tool, only the data transfer to not-excluded partners will be traced.

Starting IX1LANZ

To load the trace tool, switch to the *System Console* under NetWare and run the IX1LANZ program:

```
load ix1lanz
```

The following two parameters are admissible:

- File name (maximum 4 characters)
- Number of trace files to be generated (maximum 999)

The program produces a trace file. The first 4 characters consist of your entry followed by a "_" and a three-digit series number. The trace file suffix is "`.tr1`".

If you save the file under an existing file name, it will be overwritten without a warning prompt.

If you do not indicate any parameters when calling IX1LANZ, the standard name `lanz_001.tr1` will be generated.

The maximum size of the trace file is 1 Mbyte. If this value is exceeded, a new trace file is generated automatically; in our example, the file name would be `lanz_001.tr1`.

IX1LANZ terminates automatically when you close the last trace file.

If you enter only the parameter *file name* when loading IX1LANZ, the number of trace files is set automatically to 10.

It is not possible to run the program **without** a *file name* and **with** an *indication of number.*

After recording the packets, LANalyzer for Windows decodes the packets received/ transferred over the ISDN line.

The following three problems can arise during operation:

Not enough main memory

IX1LANZ cannot create a buffer memory for intermediate storage and terminates.

Not enough hard-drive memory

Because up to 1 Gbyte of storage space is required in the sys volume in order to handle up to 999 trace files, the program checks the available hard-drive space when creating the trace files.

- A warning is displayed on the console when available memory falls below the 500 KB limit.
- IX1LANZ terminates automatically when available memory falls below the 100 KB limit.

Packet Loss

Packets can be lost under very high traffic conditions (several B channels used to full capacity). These packet losses are due to buffer overflow, as packets are placed in the internal buffer faster than they can be written to the trace file.

When this happens, the console shows the following error message:

```
packet lost !!!
```

5 Reference for ITK NetBlazer 4400

5 Reference for ITK NetBlazer 4400

In this chapter you will find a summary of all tables for the WANODI driver and the Virtual Ethernet driver (VETHER).

5.1 Reference for Common Configuration Items

The following tables provide a summary of valid router parameters for both ISDN interfaces. In the left column, the location of the parameters in the corresponding menus is displayed.

INETCFG: Internetworking Configuration Main Screen

Menu Item	Meaning
`Boards`	Here you specify the LAN or WAN drivers to be loaded when starting the router. For example, you set the following hardware parameters here: • Interrupts • Port addresses • Memory areas used You can activate and deactivate individual boards.
`Network Interfaces`	Here you configure the various parameters of a network interface.
`WAN Call Directory`	Here you define and configure the remote partners that you want to access using the WAN boards.
`Backup Call Associations`	Here you can link several WAN call destinations, such that one WAN call destination serves as a backup for another destination.
`Protocols`	Here you specify global parameters for the network protocols used.

Menu Item	Meaning
`Bindings`	Here you assign a network protocol to a specific LAN or WAN board.
`Manage Configuration`	Here you specify additional parameters: • Configuring the SNMP information • Reading and storing configuration information on diskette • Configuring remote access to the server • Editing the AUTOEXEC.NCF file This menu item has no significance when operating the ITK NetBlazer 4400.
`View Configuration`	Here you can display the following information: • All LOAD and BIND commands • LOAD and BIND commands for LAN boards • Protocol commands • Board, interface, and protocol assignments in a matrix format • Summary of the configuration (LAN boards, protocols, bindings) • This summary can be stored in a file. • Messages output by the modules loaded during system start This menu item has no significance when operating the ITK NetBlazer 4400.
`Reinitialize System`	When you select this menu item, the changes made in the INETCFG program are activated.
`Go To Fast Setup`	When you select this menu item, you go to Fast Setup. This simplifies configuration by accepting default parameters.

Supported Dial Number Formats

Entry	Meaning
`ISDN Number scheme` *WANODI:* *Network Interfaces* *AND* *WAN Call directory* *VETHER:* *Own Router Settings* *AND* *Controller Configuration* *AND* *Outgoing Dial Number list* *AND* *Accepted Number list*	The ITK NetBlazer 4400 provides three different dial number schemes. Every scheme requires unique handling. (1) Dial number in which the individual components are separated by a hyphen (“-”): Country Code / Area Code / Subscriber Number / PBX Extension 49 / -30 / -38493 / 1 / -510 / -769 / -5555 The dial number separates into a maximum of four parts. The first part of the dial number specifies the country code. This is “49” in Germany and “1” in the USA. The area code is the code for the appropriate local network without the “0” (for example, the area code for Alameda is “510”). This is followed by the actual dial number of your ISDN station connection. If there are no area codes in your ISDN network (for example, in Denmark), enter two consecutive hyphens. If your ISDN connection is located within a private branch exchange, enter the direct dial number of your extension, separated by a hyphen.

Entry	Meaning
	ITK NetBlazer 4400 generates all formats from the dial number and enters them into the “Accepted Number List”. **When using the 1TR6 protocol:** If your connection uses the 1TR6 protocol, the last digit specified is always interpreted as the media access digit. **The dial number(s) of your own system requires this dial number scheme!** If your connection uses the media access digit, specify the media access digit within the last block of digits without separating the media access digit by an additional hyphen. You may also enter the dial number in the following formats: (2) Dial number without added characters: 492319747298 The dial number is entered directly into the *Accepted Number List* without variations. (3) Dial number that begins with a period: `.9747298` The dial number is not automatically entered into the *Accepted Number List*. You may enter it manually. **Recommendation** Use format (1).

Access Codes and MSNs

Entry	Meaning
`Access Codes` *WANODI:* *Network Interfaces* → *Expert Configuration* *VETHER:* *Controller Configuration*	There are three different Access Codes: `Public, Long Distance, International` They are described below.
`Public` *(default=0)*	Prefix for access to the public network (only for private branch exchanges) or an outside line. Dial this digit to reach a public (local) telephone network, for example “9” for some private branch exchanges, “0” for others.
`Long Distance` *(default=0-0)*	Sequence of digits that you dial to make a long distance call. In general, this is the `Public Access Code` followed by the digit you dial for supra-regional connections. In Germany, this is the “0”, in the USA, this is the “1”. If you operate your system in a private branch exchange, separate the prefix for access to the public network from the `Long Distance Access Code` using a hyphen. **Example** When you call from San Francisco to New York, the `Long Distance Access Code is` “1”, the `Area Code` is “212” and the required dialing sequence is “1212”. When you call out from a private branch exchange, you must add the prefix for accessing the public network (usually a “9”) to leave the private branch exchange. In this case, you separate the `Access Code` using the “-”, for example, “9-1212”.

Entry	Meaning
`International` (*default*=`0-00`)	The sequence of digits you dial to make an international call. When you use your system from a private branch exchange, separate the prefix for accessing the public network (see `Public Access Code`) from the `International Access Code` by means of a hyphen. **Example** When you are calling from Germany to other countries, the `International Access Code is` "00". When you are calling out from a private branch exchange, you must add the `Public Access Code`, separated by means of a "-", for example "0-00". **Example** For subscribers of France Telecom, the `International Access Code is` "0-19".
`Own MSN` *(default=* `Auto-Detect`*)*	The router uses MSN for outgoing calls. A change of MSN is only important for some private branch exchanges when making outgoing calls. If you retain the *default* setting `of Auto-Detect`, MSN is the *calling number* for the outgoing call. In the Euro-ISDN Protocol, this is the part following the last hyphen. In the 1TR6 Protocol, the last digit of your own dial number (media access digit) serves as the *calling dial number* for the outgoing call. In some private branch exchanges, however, the complete dial number is not specified as your own calling number. For this reason, the required MSN or the dial number with media access digit used can be entered in this field. If you are not allowed to use an MSN for outgoing calls, enter the value "`No`".

Entry	Meaning
`Accepted MSN` *(default= *)*	This parameter is important for *incoming* calls for a few private branch exchange or with one BRI having several terminals. This parameter determines which ISDN board is addressed for which **M**ultiple **S**ubscriber **N**umber (MSN) on the BRI bus (in Euro-ISDN) or by which media access digit (in the case of 1TR6). If you only use one ISDN board on the connection, leave the default setting of "*". If you have connected several terminals with "Data Services" to one BRI, use the following settings: • If you enter a "*" in this field, your router will react to all (authorized) incoming calls with the service code *64 kbit/s data transmission.* • If you have entered `Auto-Detect` here, the router compares all digits received with the dial number of this controller. To make use of this feature, ISDN must have transmitted at least one digit as the "Requested Address". (The *Requested Address* is the dial number of the called partner that is transmitted to this partner when the connection is established.) • If you are using the Euro-ISDN protocol, enter the MSN (**M**ultiple **S**ubscriber **N**umber) specified for the ISDN board. • If you are using the 1TR6 protocol with media access digit, enter the *media access digit* specified for your ISDN board here.

Basic Security Service / Call acceptance

Entry	Meaning
`Call Acceptance` *WANODI:* *Network Interfaces* *VETHER:* *Controller Configuration*	In the case of *incoming* calls, this specifies whether all or only selected dial numbers are accepted. `Accept all Numbers` *`(default)`* An incoming call is accepted in all cases, regardless of the dial number. An incoming unknown Virtual Ethernet call will be compiled with the settings of the _DEFAULT partner. `Accept only registered Numbers` The dial number of the remote partner transmitted in the D channel is compared to the Remote ISDN Number of a Call Destination, respectively all entries of the *Accepted Number List* for a Virtual Ethernet Call destination. A connection will only be established when the corresponding number is present. This check is made before the connection is established because the dial number transmitted in the D channel is used for the check. For this reason, no charges are accrued for a rejected call.  During installation and configuration, always leave the parameters set to `Accept all Numbers` to avoid mistakes caused by rejected connections. The *default* is `Accept all Numbers`.

Callback

Entry	Meaning
`Callback` *WANODI:* *Network Interfaces (Expert Configuration* *VETHER:* *Partner Configuration*	`No` *`(default)`* Callback is disabled. `Yes` If you activate this function (`Yes`), a connection retry by a remote partner is initially rejected. In response to this, the router then establishes the connection to the remote partner. In this way, the connection charges are accrued at your router and not at the remote partner. In addition, the Callback mechanism provides an additional security instrument to prevent undesired access. Callback operates only if the dial number is transferred in the D channel.

Short Hold

Entry	Meaning
`Short Hold Mode` *WANODI:* *WAN Call Destination* *VETHER:* *Partner Configuration → Outgoing Dial number list* *(default =* `Static`*)*	This allows a call teardown. `Disabled` Switches off the Short Hold mode. This makes sense when your routers are connected within one private branch exchange in which no additional charges accrue due to long connection times. `Static` *(default)* The physical connection between two partners (router or workstation) is interrupted if no user data is transmitted in a specific time. However, the logical connection is retained so that the connection can be established again automatically and virtually without any time delay when data flows again. `Dynamic` The dynamic Short Hold is an extension of the static Short Hold. If charge signals are transmitted during a connection, the program calculates the actual clock time of these signals and initiates the call teardown if no data is transmitted before an expected new charge signal. If charge signals are not transmitted by your carrier, dynamic Short Hold does not operate and the router uses static Short Hold.

Entry	Meaning
	`Remote Configured` *(Only for Virtual Ethernet)* The Short Hold value will be taken from the partners setting. If both sides have activated a remote configured Short Hold, the resulting one will be disabled.  Dynamic Short Hold operates only when charge data is transmitted during a connection. You must have requested charge data during the connection from your carrier.
`Short Hold Value` (*default*=`20`)	This value specifies the time in seconds after which a teardown is performed that no user data is being transferred. The adjustable range is 10 to 9999 seconds. The *default* is 20 seconds. If the `Short Hold Value` of the remote partner is different, the smaller value is used.  Pay very close attention to the correct setting of the Short Hold parameters after entering a new setting. Carefully check the efficiency of your settings. Short Hold operation may result in unnecessarily high connection charges, in the event of an incorrect or “unsuitable” setting.

Sleeping Timeout Configuration

Entry	Meaning
`Sleeping Timeout` *WANODI:* *WAN Call Destination* *VETHER:* *Partner Configuration*	Format <Hours>:<Minutes>:<Seconds> Here you set the period of inactivity after which a connection is also logically terminated once the physical connection has already been terminated, that is, the connection was in Short Hold mode. The period of inactivity ranges from 00:00:00 to 18:12:15. To change the configuration, select the entry and press <Enter>. A window will appear with the following possible settings: `Disabled` The sleeping timeout is not active. The logical connection will never be automatically terminated, but rather remains in sleeping mode. `Enabled` The sleeping timeout is activated and a connection will be terminated following the set time. If you set the time to zero, the connection does not enter Short Hold mode, but rather is immediately terminated both logically and physically. The *default* is 10 minutes for WANODI and 60 minutes for Virtual Ethernet connections.

Connection Modes

Entry	Meaning
`Connection Modes` *WANODI:* *WAN Call Directory* *VETHER:* *Partner Configuration → Outgoing Dial Number list*	This defines the type of connection used to access the remote partner. `Circuit Switched Line` *`(default)`* The ISDN connection is established using a standard dial-up line. Connection charges accrue for the time of the connection depending on the distance. `Semi-permanent Line` *`(only with 1TR6)`* The connection between the two subscribers is cleared established by the carrier (for example, Deutsche Telekom AG in Germany) for a specific time and with specified charges (permanent dial-up line ordered in advance). No additional connection charges accrue for this type of connection. Also, select Semi-permanent Line if you want to use the leased line together with PPP as described in chapter 3.18, *Leased Lines (D64S, D64S2)* (page 3-46).

Entry	Meaning
	`Permanent Line` The remote partner is addressed by means of a leased line (dedicated line). The connection is available without restriction to these two remote partners only, regardless of the data traffic. No additional connection charges accrue for this type of connection. If you have selected `Permanent Line`, a dial number cannot be entered (leased line) and *Short Hold Mode* (see page 5-12) and *Sleeping Timeout* (see page 5-14) are automatically disabled.  For semi-permanent or permanent lines the controller number must not be “-1”. The controller number must be assigned to the corresponding ISDN connection. You will find additional information in the *ix1 Installation and Interfaces* manual.  If you want to use the permanent line together with PPP, you have to switch this parameter to Semi-permanent, as described in chapter 3.18, *Leased Lines (D64S, D64S2)* (page 3-46) The *default* is `Circuit Switched Line`.

Channel Bundling

Entry	Meaning
`Channel Bundling/MLP`	This allows channel bundling to use several B channels for one connection. If you have selected the PPP protocol, the channel bundling will be performed using the **M**ulti **L**ink **P**rotocol. `Disabled` *(default)* No channel bundling is performed. `Load Dynamic` Channel bundling is used as a function of the quantity of data to be transferred. B channels are established or terminated as needed. In the dynamic channel bundling version, the number of B channels is limited by the *Max Number of B channels* (see page 5-18). `Protocol Dynamic` *(only for WANODI)* An additional B channel is established for every protocol used for a remote partner. `Static` It is always attempted to establish the number of channels entered under *Max Number of B channels* (see page 5-18). `Manual` The number of channels used for bundling can be changed manually while the connection is established.The number of B channels is limited by the *Max Number of B channels* (see page 5-18) To change the number of channels highlight the connection on the IX1CCA Main Screen and press ➪ <Alt>+<F7> to decrement the number of channels. ➪ <Alt>+<F8> to increment the number of channels. **Prerequisites for a successful channel bundling** • the channel bundling must be activated on both sides • sufficient B channels must be present • the dial number must be transmitted correctly

Entry	Meaning
`Max Number of B channels`	The maximum number of B channels to be used simultaneously to this ISDN remote partner. You can only enter a value if you have selected one of the following values: `Static`, `Protocol Dynamic`, `Manual`, or `Load Dynamic`.  Please keep in mind that the maximum value for channel bundling naturally assumes a corresponding number of ISDN controllers in your router *and at the remote partner.* You should understand that, when using *n* B channels, *n times* the charges accrue, but n times the throughput rate occurs only in the best case. If you have entered different values on both sides, only the **smaller** number of B channels is used for channel bundling.

PPP Configuration

Entry	Meaning
`PPP Compression` *(default=`Stac Compression`)*	(only for PPP) This parameter specifies whether a compression should be requested for this connection. If the compression is selected, this router will try to bring up compression while establishing the connection. Compression will only be used if the partner is capable of using it.
`PPP Authentication Method` *(default=`None`)* *WANODI:* *WAN Call Destination → Expert Configuration* *VETHER:* *Partner Configuration → PPP Parameter*	(only for PPP) `None` *`(default)`* Switches **off** subscriber authentication. `CHAP` With CHAP (**C**hallenge-**H**andshake **A**uthentication **P**rotocol) switched on, the partners exchange encrypted password information when establishing the connection. A connection is only established when this information is identical for both sides. During this process, the password entered is not transferred itself but rather only internally used as an encoding key so that decoding externally is impossible. This version ensures high security against unauthorized router access. However, data compression is not available in this version of the protocol. `PAP` PAP, the (**P**assword **A**uthentication **P**rotocol) acts similarly to CHAP with the only difference being that the password and IDs are not encrypted during the transmission over the ISDN line. `Auto` The authentication protocol will be negotiated between the peers. In a first step the router tries to connect via CHAP. If the peer doesn't respond the CHAP request, the system then tries to negotiate PAP.

Entry	Meaning
`Direction`	`Allow own authentication` The authentication is performed in one direction, for example the system authenticates to the remote peer, but it doesn't expect an authentication from the peer. (One way authentication) `Peer must authenticate` The system authenticates itself and expects authentication information from the remote peer at the same time. `Call dependent (only Virtual Ethernet)` The particular calling system authenticates itself, but doesn't expect an authentication from the remote peer.  If both partners have configured "Allow own authentication", no PPP authentication takes place.
`Password`	The password necessary to establish a PPP connection to a remote partner. This password must be identical to the one the remote partner uses for this connection. The password can be 1 - 47 ASCII characters long. The entry is case sensitive. The recommended password length is 6 to 8 characters.

Entry	Meaning
`Own System ID`	The name or identification key of your own router that is transmitted to the remote partner during outgoing calls. The local server name is automatically specified here and you may change this entry. Format The ID consists of 1 - 48 ASCII characters. The *default* is your own server name.
`Remote System ID`	Here, you specify the system IDs of all remote partners defined in INETCFG. The *default* is the name of the remote partner.

Credit Configuration

Entry	Meaning
`Credit` *WANODI:* *WAN Call Destination* *VETHER:* *Partner Configuration*	With this parameter, you limit the connection establishment to a remote partner, in terms of time or charges, in the case of *outgoing* connections. `Credit Mode` This configures the type of credit. Press <Enter> to select from the following entries: `no credit` No outgoing connections can be established. `no limit` *`(default)`* There are no limits. `one time` Connections are established until the allowed credit has been used. `per day, per month, per year` The credit is allowed for the set period of time. `Credit Charge Units` Number of charge units. Once this value has been reached: • no more outgoing connections can be established • existing outgoing connections are terminated (switched to the sleep phase). `Credit Connection Time` Time period format: <Hours>:<Minutes> Once this value is reached, • no more outgoing connections can be established • existing outgoing connections are terminated (switched to the sleep phase). `Credit expires` Date after which no more connections to a remote partner can be established. Format: <Day>.<Month>.<Year> The *default* is `never`.

Time Restriction Configuration

Entry	Meaning
`Time Restriction Options`	Here you define which connections are meant to be restricted. You have the following options: `Outbound` Outgoing connections are restricted during the configured times, while incoming calls are possible. `In- and Outbound` Neither incoming nor outgoing calls are possible during the configured times. `Server Caused` Server and/or NDS caused connection establish requests are suppressed during the configured times. `Disabled` The Time Restriction is disabled.

Entry	Meaning
`Time Restriction Table` *WANODI:* *WAN Call Destination* *VETHER:* *Partner Configuration*	This specifies the times at which connections may be established to this remote partner. The minimum setting range is 30 minutes. The time period selected is displayed below the time window.  These time limits apply to the parameters configured in the *Time Restriction Options* menu. Asterisk (“*”) — Identifies those times in which connection establishment is allowed. Blank — Identifies those times in which connection establishment is suppressed. To change the settings of the time ranges, press: <Del> key — Erases the time range marked with the “*” and identifies it as *disabled.* <Ins> key — Identifies the range as *enabled* and inserts a “*”. <Spacebar> key — Changes the value of the selected range (toggle function). <F7> function key — Switches off the time restriction, a connection is allowed at *all* times. <F8> function key — Blocks the remote partner, a connection is not allowed at *any* time. To change the settings in blocks, first switch on the marker mode using the <F5> function key. Then, you can select the desired time ranges using the arrow keys or the <Home>, <End>, <Pg Up> and the <Pg Dn> keys.

Filter Configuration

Entry	Meaning
`Filter Configuration` *WANODI:* *WAN Call Destination* *VETHER:* *Partner Configuration*	Press <Enter>. The menu for configuring the filter appears. The different filters of the ITK NetBlazer 4400 are described below.

By using connect filters, you can control the Short Hold mode without impairing the transmission of data packets over an established connection.

There are two types of filters:

- Simple filters
- Filters that spoof

Simple filters check whether the corresponding data packets establish a sleeping connection again. If the connection is active, the filters decide whether the timeout counter (TTC) is to be reset again by the packets. The TTC (**T**ime **T**o **C**ut) specifies the number of seconds after which the connection is again to be terminated.

Filters that spoof have the additional task of generating *Response Packets* and to respond locally.

You switch the filters on with `Yes` and off with `No.`

Yes/No	Meaning
`Yes`	A sleeping connection is not established again for these packets. The timeout counter (TTC) of an active connection is not reset.

Yes/No	Meaning
No	A sleeping connection is automatically established again for these packets. The timeout counter (TTC) of a connection is reset.

You can reduce unnecessary data traffic using the filters. We recommend configuring the applications in such a way that this data traffic is not generated in the first place.

IPX Diagnostic Packets

are used to test the network.

ARCserve from Cheyenne and NetExplorer (ManageWise) from Novell generate IPX Diagnostic Packets.

If you are using ARCserve or NetExplorer, leave this filter set to the default of `Yes`.

IPX Ping Packets

are usually used to test a connection to another host.

IPX Ping Packets are generated by workstations, hosts or other applications that test connections.

> A successful test using IPX Ping Packets is only possible with an existing connection. The test fails for a sleeping connection.
>
> Please keep this in mind if you change the default from `No` to `Yes`.

IPX NDS Ping Packets

are sent before synchronizing the NDS (**N**etWare **D**irectory **S**ervices) by the Novell NetWare 4.1 server to check whether the other server is ready for operation.

> Change this filter from the default `No` to `Yes` only if you know how NDS works.

IPX NDS Packets

Change this filter from the default `No` to `Yes` only if you know how NDS works.

IPX NCP Exchange Time Packets

Change this filter from the default `No` to `Yes` only if you know how NetWare time synchronization works.

IPX NetBIOS Packets

are used to communicate between workstations and Microsoft servers by way of IPX.

If you are using a Microsoft server with the IPX protocol in the LAN and set the defaults from `Yes` to `No`, your WAN connection is always active.

IPX SNMP Packets

are used to check routers and other network devices (SNMP = **S**imple **N**etwork **M**anagement **P**rotocol).

IPX SNMP Packets are generated by SNMP servers and SNMP clients, such as IPXCON.NLM or ManageWise from Novell.

If you would like to perform remote maintenance by way of ISDN, leave the default set to `No`. The RCONSOLE program does not use IPX SNMP but rather IPX SPX Packets.

IPX Watchdog Packet Spoofing

IPX Watchdog Packets are generated by every file server to ensure that the connected workstations are still “up and running”. The server routinely checks all workstations, even those connected by way of ISDN, every 5 minutes.

The mechanism of IPX Watchdog Spoofing responds to these packets locally to avoid establishing a connection. If you change the default from `Yes` to `No`, the server checks all connected workstations at intervals of 5 minutes and results in unnecessary costs.

IPX NLSP Packets

are generated by the local router for communication with its neighbor.

We recommend using RIP and SAP for the ISDN connection, and NLSP in the local network.

If you want to use IPX NLSP Packets with the default `Yes`, the IPX NLSP Hello Packets (see the following filter) must remain set to the default `No`, because you cannot use both filters at the same time.

IPX NLSP Hello Packet Spoofing

IPX NLSP Hello Packets are generated by the IPX software on the local router to test the availability of its neighbors. The test packets are transmitted every 20 seconds to each active partner.

We recommend using IPX NLSP Hello Packet Spoofing if you want to use NLSP on ISDN connections.

You can only activate this filter if IPX NLSP Packets (see the preceding filter) are set to `No` (default). You cannot use both filters at the same time.

SPX NetWare for SAA Inter-Server Packets

synchronize two NetWare SAA Gateways connected to the same hosts. This communication is not necessary if both SAA Gateways are connected to different hosts.

If you are using two NetWare for SAA applications at both ends of one ISDN connection, leave this filter set to the default of `Yes` to avoid unnecessary data transfers.

SPX Spoofing

The SPX protocol is used by various applications that require a secure connection on the network level. Beyond securing the data packets, both sides are participating in the communication check, at short intervals, and the accessibility of the other terminal system. To make Short Hold possible, the SPX Watchdog Packets must be answered locally. A few examples of applications that use SPX are NetWare for SAA, RCONSOLE, and BTRIEVE applications.

The default for this filter is `Yes`.

IP Ping Packets

can be used to check whether the addressed host or the workstation is ready for operation, and whether a path to this destination has been found in the network.

If you filter IP Ping Packets, the result of a ping by way of ISDN will be different depending on whether the ISDN connection is established or not. Testing using IP Ping Packets will only be successful if the ISDN connection is active. If the connection is sleeping, the test will fail. Please keep this in mind if you change the default from `No` to `Yes`.

IP RIP Packets

are used by the local TCP/IP router for communicating with its neighbor.

If you would like to use RIP only in the local network but not in ISDN, leave the default set to `Yes`.

For the ISDN connection, we recommend the use of static IP routing.

IP NetBIOS Packets

are used for communication between Microsoft servers and workstations using IP.

If you are using a Microsoft server with the IP protocol in the LAN and you set the default from `Yes` to `No`, your WAN connection is always active.

IP SNMP Packets

are used to check routers and other devices in the network.

IPX SNMP Packets are generated by SNMP servers and SNMP clients, such as TCPCON.NLM or ManageWise from Novell.

If you require access to a remote server using the SNMP protocol, leave the default set to `No`.

IP Sun RPC Packets

announce various IP services in the network. For example, the XCONSOLE program (the remote console via IP) generates these packets to announce its services in the network.

If you use XCONSOLE in your LAN, leave the default set to `Yes` because otherwise Short Hold operation will not operate properly.

5.2 Reference for WANODI Related Items

Network Interface Configuration Parameters

Entry	Meaning
`Board Name`	Name of the board to which you have assigned a WANODI Driver and are now configuring.You cannot edit this entry.
`Group Name`	This allows you to combine several available controllers into one group. Instead of using one specific controller, an ISDN connection can be established using any free channel of a controller group. For example, you can combine the four controllers of one ITK Octo board into one group.
`Board Status`	This specifies driver initialization during system start. Enabled The driver is loaded automatically during system start. Disabled The driver is not loaded during system start. The *default* is Enabled.
`Own ISDN Number`	Enter the dial number for your own ISDN connection here.The correct dial number scheme is described in section *Supported Dial Number Formats* (page 5-5).
`Call Acceptance`	Facilitates the Basic Security Services. For an explanation of these, see section *Basic Security Service / Call acceptance* (page 5-10).
`Expert Configuration`	The parameters of the Expert Configuration menu are primarily important for private branch exchanges and are usually not changed.This menu is described in the next section.

Network Interface Expert Configuration Parameters

Entry	Meaning
`Access Codes`	The three different Access Codes Public, Long Distance and International are described in section *Access Codes and MSNs* (page 5-7).
`Subscriber Numbers`	The parameters Own MSN and Accepted MSN are described in section *Access Codes and MSNs* (page 5-7).
`Number of Retries` *(default=3)*	Number of connection establishment retries (0-10) if the retry to establish a connection was unsuccessful.
`Pause between Retries` *(default=3)*	Delay between connection establishment retries in seconds. The time interval range is between 1 and 30 seconds.

WAN Call Directory Configuration Parameters

Entry	Meaning
`Call Destination Name`	The remote partner name is displayed here (cannot be edited).
`Board Name`	If you want to assign a single board to the remote partner (`Call Destination Name`) by which this partner can be reached, select this menu item using <Enter>. A list of all available ix1 WANODI controllers appears. Select the desired entry and confirm your selection using <Enter>.
`Group Name`	To assign a controller group and thus several boards instead of one single board to the remote partner, press <Enter>. A list of the connected groups appears. Select the desired group and confirm your selection using <Enter>.

Entry	Meaning
`Remote ISDN Number`	Dial number of the ISDN remote partner Enter the dial number as suggested in section *Supported Dial Number Formats* (page 5-5).
`Connection Mode`	For an explanation of the supported connection modes, see section *Connection Modes* (page 5-15).
`Short Hold Mode and Short Hold Value`	For an explanation of the Short Hold functionality of the ITK NetBlazer 4400, see section *Short Hold* (page 5-12).
`Sleeping Timeout`	For an explanation of the Sleeping Timeout functionality of the ITK NetBlazer 4400, see section *Sleeping Timeout Configuration* (page 5-14).
`Credit`	For an explanation of the Credit configuration of the ITK NetBlazer 4400, see section *Credit Configuration* (page 5-22).
`Time Restriction Options / Time Restriction Table`	For an explanation of the Time Restriction functionality of the ITK NetBlazer 4400, see section *Time Restriction Configuration* (page 5-23).
`Filter Configuration`	For an explanation of the Filter configuration options of the ITK NetBlazer 4400, see section *Filter Configuration* (page 5-25).
`Expert Configuration`	This menu is for setting special connection parameters. You will find a detailed description in the next section.

WAN Call Directory Expert Configuration Parameters

Entry	Meaning
`Call Type`	`On Demand` *(default)* The on demand connection is established • manually or • by way of data (if static routes have been defined) and terminated • manually or • if the sleeping timeout counter has reached zero. An on-demand connection is not automatically established again in the event of termination. `Permanent` The system tries to maintain permanently a logical connection once it is established. This connection is either established immediately when starting the router or manually later. This depends on the protocol used and can be set for IPX and TCP/IP. One B channel is reserved for this connection during the entire time of operation. The sleeping timeout counter is not used but the Short Hold mechanism is available without restriction. This type of connection is primarily used for leased lines and important network links that must always be active automatically.

Entry	Meaning
`Data Protocol`	The data protocol used to the remote partner To allow an exchange of data, the same data protocol must be used on both remote partners. `ITK X.75 (default)` This protocol highlights the advantages of ITK boards and should be used to connect ITK Remote Access products `PPP (Point to Point Protocol)` You set PPP to use the Point-to-Point Protocol. This protocol is used to communicate with third-party routers.
`Channel Bundling` *AND* `Max Number of B channels`	For an explanation of the Channel Bundling configuration, see section *Channel Bundling* (page 5-17). A channel bundling for WANODI connections is only possible if you have selected the ITK X.75 protocol.
`Line Speed`	The standard international transfer rate of ISDN is 64 kbit/s. In the case of connections to or within the USA, it may be necessary to reduce the transfer rate to 56 kbit/s because some exchanges between the different carriers only allow this transfer rate.
`Callback`	For an explanation of the Callback functionality of the ITK NetBlazer 4400, see section *Callback* (page 5-11).

Entry	Meaning
`Retry Mode`	This specifies the cases for which a new retry is to be started after an retry to establish a connection has failed. The interval between these retries is programmable from 8 seconds to the Retry Interval Limit. `Never Retry` No new retry is made after the first attempt to establish a connection has failed. `Retry Self Correcting Failures` *(default)* A new retry is made for all failures that do not depend on the router configuration, for example, if the remote partner is busy. `Retry All Failures` Independent of the failures that occur, new retries at establishing a connection are made periodically.  This setting results in high charges if the routers establish physical connections but are differently configured, so that a data connection is not possible. `Stop at limit` *(default for on demand connections)* After the time limit has been reached, no further retries are made at establishing a connection.

Entry	Meaning
`Retry Interval Limit`	Maximum interval between two retries when establishing a connection. *Default* • 10 minutes for *permanent* connections • 2 minutes for *on demand* connections Interval Range: 00:00:00 - 24:00:00 Format: <Hours>:<Minutes>:<Seconds>
`PPP Authentication parameters`	For an explanation of the PPP authentication configuration, see section *PPP Configuration* (page 5-19).

Static IPX Routing Configuration Menu

Entry	Meaning
`WAN Call Name`	Name of the remote partner *(cannot be edited)*
`WAN Call Type`	`static on demand` *(recommended)* The static routes entered are used. During an existing connection, no additional routing information is exchanged. `routed on demand` The static routes entered are used. In addition to this, routing information is transferred and stored during an existing connection. All newly available routing information is stored only until the connection is terminated.
`WAN Call Status`	This defines whether connections to a remote partner are allowed. `Enabled` Connections are possible to a remote partner. `Disabled` Connections to a remote partner are **not** possible.

Static Service Configuration Menu

Entry	Meaning
`WAN Call Destination`	Name of the remote partner that you are configuring.
`Service Name`	With static IPX routing, you can directly address a specific device in a remote corporate network (server, router, etc.). Enter the name of the device here that you want to announce in the local network.

Entry	Meaning
`Service Type`	Press <Ins> to define the function to be assumed by the device, selected in `Service Name,` of the remote network. Select an entry from the displayed list and press <Enter>.
`Service Address Network`	Specify the internal IPX address of the remote server or router.
`Service Address Node`	Specify the node address that the device has in the network interconnection. The *default* is "`1`" for all NetWare servers.

5.3 Reference for Virtual Ethernet Related Items

The following tables provide a summary of the entries and their meanings.

OWN Router Settings Menu

Entry	Meaning
`Own Name`	Name of the local server *(cannot be edited)*
`Virtual Ethernet Dial Number`	Group dial number that the Virtual Ethernet remote partners use to access the router. The group dial number serves to identify this router to Virtual Ethernet remote partners. Enter the dial number as suggested in section *Supported Dial Number Formats* (page 5-5).
`Pause between Retries` *(default=3)*	The pause between retries at establishing a Virtual Ethernet connection in seconds. The interval range is from 1 to 30 seconds.
`Connect on RIP/SAP-Change`	`Yes` *(default)* A sleeping connection is activated if entries were changed in the local routing table. `No` The Short Hold mode is not interrupted.

Entry	Meaning
`Maximal Workstation Sleeptime`	The time the router waits before checking whether a workstation with a sleeping connection is still active. • If the workstation is still active, the time is reset and checked again after the set time interval. • If the workstation does not react, the router repeats the attempt to establish a connection at intervals of about 5 minutes until the set retry rate (`Workstation Connect Retries`) is reached. Then, the connection is terminated completely. The default is 14 400 seconds (4 hours).
`Workstation Connect Retries`	Number of retries to change a sleeping connection to a workstation again. If the workstation does not react to any of the retries to re-establish a connection, the router terminates the logical connection to this workstation.
`Use SNMP Traps`	The ITK NetBlazer 4400 sends SNMP Traps (SNMP = Simple Network Management Protocol) for different router-relayed actions. Managing systems, such as Novell NMS, can report these traps which are listed by severity. A description of the SNMP traps can be found in appendix D, *Information about SNMP Traps*. If you set this item to *No*, no SNMP Trap information will be sent.
`IP Configuration`	In this section you can configure the IP address assignment and masquerading.

IP Configuration Menu

Entry	Meaning
`IP Address Assignment`	The ITK NetBlazer 4400 is capable of assigning IP addresses dynamically to clients. This functionality can be enabled or disabled.
`IP Masquerading`	The ITK NetBlazer 4400 can translate all internal IP addresses to an external one. This is described in chapter 1.8, *Masquerading* (page 1-33). You can enable or disable this feature.
`IP Address Pool`	
`Interface IP Address`	IP address of the Virtual Ethernet interface. This address must be within the same network, but outside the IP address range. This address is used in PPP connection establishment to configure the remote side. This functionality is active independent of IP address assignment.
`IP address range - START`	First IP address that should be used for clients requesting a dynamic IP address from ITK NetBlazer 4400.
`IP address range - END`	Last IP address that should be used for clients requesting a dynamic IP address from ITK NetBlazer 4400.
`Masquerading`	
`Masquerading Partner`	IP Masquerading is done only on the connection to your Internet Service Provider. After you have configured the partner, you have to select it here.
	If the *Select Masquerading Partner* list is empty, the ITK drivers might be not loaded. hence the ix1cca hasn't opened the partner database.
`IP Address Acception`	You can configure Masquerading using a dynamically assigned IP address for the route of the Internet Service Provider (enabled) or you can configure the IP address used manually (disabled).

Entry	Meaning
Masqueraded IP address	If you want to use a static IP address for Masquerading and you have disabled *IP Address Acception,* you have to specify it here.
Routing Address	If you use a dynamical assigned IP address (IP Address Acception = enabled), you need to configure a pseudo-Default Router for TCP/IP in the INETCFG, and insert this IP address of the Default Router here.

Controller Configuration Menu

The entries in the Controller Configuration window are handled differently, depending on the controller usage.

```
+-------------------------------------------------------------------------
|              Controller Configuration
|-------------------------------------------------------------------------
| Controller Number..........: 0
| Controller Type............: ITK BasicISA-UP04MB, Version:1.2
| Firmware Version...........: Basic V2.43-B(11)
| Line Interface.............: point to multipoint, TEI=AUTO
| D channel Protocol.........: DSS-1, Euro-ISDN/NET3, ETSI
| Number of B channels.......: 2
| Dial Number................: 49-231-9747-298
| Own MSN....................: Auto-Detect
| Accepted MSN...............: *
| Public Access Code.........: 0
| Long Distance Access Code..: 0-0
| International Access Code..: 0-00
| WANODI Board Name..........: (None)
| Call-Acceptance............: Accept all Numbers
| Enable Modem Access........: Yes
| Use for Virtual Ethernet...: Yes
| Reserved B channels VEther.: 0
+-------------------------------------------------------------------------
```

What follows are the different cases:

Case1 You use the controller only for Virtual Ethernet:
Then you may edit all parameters.

Case2 You use the controller for WANODI connections.
Then you may view the controller settings but not edit them.

Case3 You use the controller both for WANODI and for Virtual Ethernet.
Change the *Use for Virtual Ethernet* entry to `Yes` and enter the number of B channels reserved for this case in the `Reserved B channels VEther` entry.

The explanation of the parameters Dial Number, MSNs and Access Codes is given in the corresponding sections of this chapter. Please refer to them if you need additional information.

This section describes this menu's entries that are related to Virtual Ethernet:

Entry	Meaning
`WANODI Board Name`	If you have loaded the WANODI Driver for a controller, the name of the WANODI board is displayed here. This entry cannot be changed.
`Enable Modem Access`	`Yes` *`(default)`* Here you can specify whether the router should answer telephone (modem and GSM) calls.
`Use for Virtual Ethernet`	`Yes` *`(default)`* Here you can specify whether you also want to use this controller for Virtual Ethernet connections.
`Reserved B channels Vether`	Here you set the number of B channels that you want to reserve for Virtual Ethernet connections. This parameter prevents the WANODI Driver from seizing these B channels.

Partner Configuration Menu

Entry	Meaning
`Name`	Name for the partner system If possible, this name should be the server name of the other router in the case of routers, and the name of the remote partner in the case of workstations. The first 12 characters of the name appear with a “V” for *Virtual Ethernet* in the list of configured remote partners. **Example** “ITK_DO” appears as “V ITK_DO”.
`Virtual LAN Number`	As ISDN is considered an autonomous network for Virtual Ethernet connections, it is also possible to divide this ISDN network into subnetworks. For this reason, you can combine different remote partners by groups into one “ISDN subnetwork”. You can assign appropriate configuration parameters (protocol, network number, etc.) to this subnetwork and address it directly. Up to 10 (0-9) different virtual LANs are available.
`Outgoing Dial Number List`	In this list you can create and edit all dial numbers to reach the specified remote partner. The entries of the Outgoing dial number list menu are described in section *Supported Dial Number Formats* (page 5-5).
`Accepted number list`	This list contains all those dial numbers that allow partners call in access. Apart from automatic created entries when using the suggested dial number scheme, you can add manual call entries.
`Callback`	The Callback functionality is described in section *Callback* (page 5-11).

Entry	Meaning
`Protocol`	This parameter designates the transfer protocol to your remote partner. In order to make data exchange possible, the same transfer protocol must be configured for both sides. `Virtual Ethernet (default)` The standard ISDN protocol for the ITK boards. While establishing the connection, the routers exchange “Welcome Packets” to identify each other. With this transfer protocol, different network protocols such as IP or IPX can be transferred at the same time over one connection. `PPP` Set this protocol to use the Point-to-Point Protocol (PPP) in ISDN when you want to transfer IPX and IP Packets.
`PPP Configuration`	In this menu you define parameters for the PPP Authentication such as Password and System IDs. For an explanation of the PPP authentication configuration, see section *PPP Configuration* (page 5-19).
`Channel Bundling / MLP`	This allows channel bundling to use several B channels for one connection.
`Max Number of B channels`	For an explanation of the Channel Bundling configuration, see section *Channel Bundling* (page 5-17).

Entry	Meaning
`Media Type`	In this parameter, you define the media a partner uses to dial in to your system. The standard international transfer rate for SDN is 64 kbit/s. This is the default value for ISDN connections. In the case of connections to or within the USA, it may be necessary to reduce the transfer rate to 56 kbit/s because some exchanges between the different carriers only allow this transfer rate. Choose Modem if the partner connects to your system via an analog modem line. Choose GSM (V.110) if a partner connects via a GSM (mobile phone) connection.
`Action on Load`	This defines the status that the connection uses when you start your system. `No action` *`(default)`* The connection to this remote partner is not automatically established. You must "manually" dial the partner. `Call on Load` The connection is automatically established during system start. Please keep in mind that with the exception of leased lines, charges accrue immediately after the connection has been established.

Entry	Meaning
	`Disable on Load` The connection is set in the `disabled` state at system start. This means that neither outgoing nor incoming connections can be established until you remove this lock. `Sleep on Load` The connection is automatically established logically without implementing a physical connection. In this way, connection charges do not accrue until data is exchanged between the remote partners. The selection of this parameter only makes sense in the case of static routing between IP remote partners.
`Sleeping Timeout`	Format <Hours>:<Minutes>:<Seconds> The Sleeping Timeout Configuration is described in Chapter , section *Sleeping Timeout Configuration* (page 5-14).
`Credit`	The Credit configuration is described in section *Credit Configuration* (page 5-22).
`IP Address`	The IP address of the remote partner. The IP address consists of a total of 4 bytes each separated from one another by means of a period. The entries can be made using decimal or hexadecimal numbers, but the value must be between 0 and 255 or 00 (hex) and FF (hex), respectively. If you enter the values in hexadecimal, you must precede the value with the characters “0X”. **Example** 210.21.21.21. or 0xD2.0x15.0x15.0x15. This address is used to simulate the ARP (**A**ddress **R**esolution **P**rotocol) used in Ethernet.

Entry	Meaning
`Time Restriction Options / Time Restriction Table`	The Time Restriction functionality of the ITK NetBlazer 4400 is described in section *Time Restriction Configuration* (page 5-23).
`Connect Filters`	The Filter configuration options of the ITK NetBlazer 4400 are described in section *Filter Configuration* (page 5-25).

Outgoing Dial Number List Menu

Entry	Meaning
`Outgoing Dial Number`	Dial number of the remote partner. For the different dial number schemes, see section *Supported Dial Number Formats* (page 5-5).
`Controller Number` (*default*=`-1`)	Here you enter the number of the controller used to establish this connection. If you enter "-1" *(default)*, the router searches for an unused B channel to establish the connection on a controller configured for Virtual Ethernet.
`Short Hold Mode` *AND* `Short Hold`	The Filter configuration options of the ITK NetBlazer 4400 are described in section *Short Hold* (page 5-12).
`Remote Short Hold`	The value that was entered as the Short Hold by the remote partner. This value is only available if you are using the Virtual Ethernet protocol and a connection was already established. In the case of different Short Hold times, the connection always enters the sleeping state in accordance with the smaller value. The displayed value cannot be changed.

Entry	Meaning
`Priority`	The priority assigned to the connection establishment with this dial number. The smaller the value (0-9), the higher the priority. 0 has the highest priority. If you enter different dial numbers with different priorities, the router attempts to establish a connection in the sequence of the priorities. In the case of several dial numbers having the same priorities, the router uses that number with which the last successful connection was established. The *default* is `1`.
`Number of Retries` *(default=3)*	Number of connection establishment retries (0-10) when the attempt to establish a connection failed.
`Connection Mode`	The supported connection modes of the ITK NetBlazer 4400 are described in section *Connection Modes* (page 5-15).
`Statistic Menu`	This menu, accessed by means of <Enter>, provides information about the remote partner having this dial number. The different entries are described in the next section.

Statistic Menu for Outgoing Calls

Entry	Meaning
`Last Call Successful`	Indication of whether the last retry to establish a connection with this dial number was successful.
`Last CAPI Cause`	In the case of a failed connection attempt, this entry displays a 4-digit error code provided by the CAPI. The error description are found in Appendix C, *Messages*.
`Last Successful Connect Req.`	Date and time of the last successful attempt to establish a connection.
`Connect Requests Total`	The sum of all attempts to establish connections, independent of success.
`Last Charging Interval`	This displays the last charging interval. The dynamic Short Hold value is computed from this charge signal.
`Total ISDN Errors`	The number of all errors preventing an ISDN line establishment. These general errors can have particular reasons that are documented in the following entries.
`Count 'No User Responding'`	This shows the failed retries to establish a connection resulting from the fact that the remote partner did not respond. Normally, this error occurs when the remote system is switched off.
`Count 'Remote User Busy'`	The number of retries to connect that were refused because all available B channels are used at the remote partner – comparable to the “busy” signal when making a telephone call.

Entry	Meaning
`Count 'Call Rejected'`	The number of retries to connect rejected by the remote partner. Possible reasons for this are • unregistered dial number • Callback is activated • a partner was “disabled”
`Count 'No channel available'`	The number of failed attempts to connect caused by a missing ISDN channel.
`Establish Protocol Errors`	This is the number of failed attempts to initialize the data transfer protocol to the remote partner. Errors could occur here, for example: • if the transfer protocols are different (the remote partner is using PPP instead of Virtual Ethernet) • when the remote partner is configured as a WANODI connection while it is initialized locally as a Virtual Ethernet connection.

Accepted Dial Number List Menu

Entry	Meaning
`Accepted Dial Number`	Dial number that is transferred to your own router when you are called by the remote partner.
`Controller Number`	Here you specify the controller through which the remote partner can call you.
`Short Hold` (*default*=`20`)	Here you may enter the Short Hold value for this specific dial number. For detailed information on the Short Hold functionality of the ITK NetBlazer 4400 operation, see section *Short Hold* (page 5-12).
`Remote Short Hold`	This is the value that was entered by the remote partner as the Short Hold. This value is only accessible if you are using the Virtual Ethernet protocol and a connection has already been established. The connection always enters the sleeping state in the case of different times, in accordance with the smaller value. The value displayed cannot be changed.

Statistic Menu for Accepted Dial Number Entries

Entry	Meaning
`Last Successful Connect`	Date and time of the last successful connection establishment
`Total Connect Indications`	Number of all connection attempts
`Total ISDN Errors`	Number of errors that prevented a connection from being established with this remote partner The total number is analyzed further in the following entries.
`Total Call Rejection`	Number of connection retries that were rejected by the remote partner, for example because the dial number was not accepted.
`Protocol Errors`	Number of connection retries that were physically established, but did not lead to the establishment of a B channel, for example because the two parties had entered different transfer protocols.

View Virtual Ethernet Group Bindings Menu

Entry	Meaning
#	Number of the Virtual Ethernet group
LOD	Indication of whether the corresponding drivers have been loaded, that is, are active
FRAME-TYPE	Network protocol assigned to the group
IPX	Indication of whether IPX packets are being transferred in this group
NETWORK	IPX address of the current network that you entered in the INETCFG program under BINDINGS, if you bound IPX on the Virtual Ethernet Driver
NODE ADDRESS	Address assigned to this group
ACT	Number of active connections in this group
CNF	Number of remote partners assigned to this group

5.4 Reference for the ISDN Communication Manager

The following tables provide a summary of the entries and their meanings.

The IX1CCA Status Window

The entries in the status window have the following meanings:

Entry	Meaning
TYPE	Type and remote partner of the connection One of four possible letters will be displayed in the **first column**: R The router is being used for a Virtual Ethernet connection X The router is being used for a WANODI connection W The connection is with a remote workstation P The Point-to-Point Protocol is being used for the connection (both for WANODI and Virtual Ethernet and for workstation and router) G The router is being used for a V.110 connection (GSM) M The router is being used for a Modem connection The **second column** displays the number of B channels which have been set for this connection.
NAME	The first twelve characters of every active remote partner
C	Controller number of the ISDN Controller for this connection If several B channels are being used in different controllers for a connection, the program displays only the first controller number used.
CH	Number of B channels being used for this connection

Entry	Meaning
STATUS	Current connection status of a connection `outbound` An outbound connection exists with the indicated destination; your router is incurring connection charges in the public ISDN. `inbound` An inbound connection exists with the indicated destination; your router is incurring no charges. `sleeping` Teardown took place, leaving a logical, but not a physical connection to the remote partner. Your router incurs no charges in this condition. `going up` The router is trying to establish a physical connection. If it is successful, the connection reverts to `outbound` or `inbound` after about one second. `going down` An existing connection is being terminated. Once the connection termination is completed, the entry disappears from the status screen. `disabled` You have disabled this connection with the <F9> or <D> key.
SINCE	Date and time from which the current status of the logical connection exists.

Entry	Meaning
TTC	TTC Timeout counter (**T**ime **T**o **C**ut) This counter provides a dynamic description of the current Short Hold situation. It indicates the remaining time in seconds until a teardown occurs if no additional data is transferred in the meantime. If the data flow is resumed, the counter is reset to the adjusted Short Hold time (static Short Hold). In the case of a dynamic Short Hold, the counter indicates the time until the next charge signal and is not reset by the resumption of data flow.
CHARGE	Charge units incurred since the start of the router for this connection. These charges are incurred by the calling subscriber in each case and are displayed only for outbound connections.
CONNS	Number of physical connections since the start of the router to a remote partner.
PACKETS	Number of data packets exchanged on these connections since the start of the router. If this value exceeds 999,999, the overflow (greater than) sign “>” is shown in front of the number.
W	Number of possible warning messages when operating this connection. Warning messages can appear if there are discrepancies in the network numbers in the Virtual Ethernet connections.

Function Keys

Key	Meaning
<F1> function key	As in all other NetWare applications, this key is used to display a help screen on the screen entry or command which has just been selected.
<F2> function key (Refresh)	This key is active in the status window only if you have also configured the WANODI Driver. By pressing this key, you can implement possible configuration changes that you may have made in the meantime in the INETCFG program. You can perform the same action by pressing the <R> key.
<F3> function key (Partner config)	The <F3> function key opens the partner configuration menu. Select the partner you want to configure from the displayed list.
<F4> function key (Reset Counts)	The <F4> function key resets all statistic entries for a selected partner. This key is only active if you are in the *Configuration and Statistic* screen of this partner.
<F5> function key (Trace-Mode)	By pressing this key, you can indicate whether you want the program to display packets that establish a connection from Short Hold. By activating the *Trace and Connect Packets* features, you can view information on the type of packet transferred, as well as its source and destination address.
<F6> function key (Reset Credits)	This key resets the remaining credits, that is, the full configured credits for a partner are at its disposal again. This key is only active if you are in the *Configuration and Statistic* screen of this partner.

Key	Meaning
<F9> function key (Disable)	You can use this key to disable a particular connection. This may be useful, for example, if technical problems are encountered on the router or when performing configuration work. This key will also terminate an existing connection and prevent it from being activated again in either direction until you explicitly release the disabled condition. You can perform the same action by pressing the <D> key. To disable a connection, press the <F9> function key, select the remote partner to be disabled, and confirm your selection with <Enter>. To release the disabled condition, press the <Del> key. After pressing this key, a new connection can be established.
<Alt>+<F9> function key (Force Short Hold)	This key combination places an existing connection into the Short Hold condition. You can use this combination if you wish to conduct testing, and if you previously entered a long time period for the Short Hold and do not want to wait. You can perform the same action by pressing the <S> key.
<F10> function key (Configuration)	This key is used to display the configuration of all connections and to change the parameters of Virtual Ethernet connections. WANODI parameters can be set in the INETCFG program. You can perform the same action by pressing the <M> key.
<INS> key (Connection establishment)	By using this key, you can manually establish a connection to a remote partner that you select. You can perform the same action by pressing the <I> key.
<Del> key (Connection termination)	With this key, you can manually terminate a selected connection. You can perform the same action by pressing the <T> key.

Key	Meaning
<Esc> key	You can use this key to exit the current window at any time. To end your session with the ISDN Communication Manager, press <Esc> from the main screen. You can perform the same action by pressing the <X> key.
<Enter> key (Statistic)	This key is used for confirming and selecting a wide range of parameters in the configuration menus. If you select an existing connection with <Enter> in the status window, extensive information on this connection will be displayed. To view statistics concerning a non-active connection, position the cursor under the last active connection and press <Enter>. You can view the same information by selecting the entry *Partner Statistics* in the main menu.
<TAB> key (Toggle Window)	Press the <Tab> Key to switch between the IX1CCA Main screen and the activity log window of the ISDN communication manager. To view earlier entries in the Activity Log window, use the <Pg Up> and <Pg Dn> keys.

Statistic Window Information

The statistic entries provided for every call destination have the following meanings:

Entry	Meaning
Name	The name of the remote partner selected as determined by you in the configuration.
Channel Bundling	This entry shows whether the connection to this remote partner is established using several channels.

Entry	Meaning
`Max Channels`	Channels used to this remote partner Values in parenthesis mean 1st value: Number of locally configured channels 2nd value: Number of channels configured on the remote partner.
`Line Speed`	Rate of transfer on the ISDN line to this remote partner
`Action on Load`	Condition of the connection at the time when the router is restarted
`Function`	This field indicates whether the remote partner is a router or a remote workstation. This and the following values can be displayed only if there has already been a first connection to this remote partner.
`node address`	MAC address of the remote partner
`Received Name`	Name of the remote partner as configured there. This value can be completely different from the designation you selected.
`Received ISDN Number`	Dial number which the remote partner has configured as its own dial number. It could happen, especially if the connection is made to a PBX with trunk line numbers, that the dial number received in the D channel is different from the actual dial number.
`Connect Mode`	Type of connection: Virtual Ethernet or WANODI connection.

Entry	Meaning
`Protocols`	Transfer protocol used For Virtual Ethernet connections, either `Virtual Ethernet` or `PPP` is displayed. For WANODI connections, either `over Virtual Ethernet` or `over PPP` is displayed. Instead of IP or IPX, another network protocol can be displayed as well.
`Status / since`	Status information of the Status Window (see Entry *STATUS*, page 5-58). In addition, the `Released` status may also be displayed, if there is neither a physical nor a logical connection to the selected destination address at the present time.
`Time to Cut Connection`	Timeout Counter for Short Hold operation. This corresponds to the *`TTC`* entry of the Status Window (see page 5-59).
`Sleeping Timeout`	Time after which a sleeping connection is logically terminated.
`Callback`	This displays whether the callback mechanism was activated.
`Credit Mode`	Type of credit of this remote partner to the router
`Logical Connection since`	Time from which the current logical connection exists. This field displays the date and time at which the logical connection was established.
`Logical Connect Time`	Duration of a logical connection since the start of the router in days, hours, minutes and seconds.

Entry	Meaning
`Phys. Connections (I/O)`	Number of physical ISDN connections used since the start of the router. If multi-channel connections were also used, each channel is counted individually. The total number of physical connections is analyzed according to *inbound* and *outbound* connections: For example, `8 = 2 + 6` means that 2 of the 8 connections were *inbound* and 6 were *outbound* connections.
`Sum Phys. Connections`	Duration of all physical connections to this remote partner in days, hours, minutes and seconds. The percentage value indicated after the duration shows the ratio of physical to logical connection times. You can use this value to determine whether a given connection should be established via the Virtual Ethernet Driver or whether a point-to-point connection would be more appropriate.
`Warnings`	This field can display warnings if connections are recognized as being inefficient. (The possible messages that can be shown in this field were not yet determined as of the publication of this manual.)
`Call Duration`	Duration of the current and latest *physical* ISDN connection and the total connection duration of all connections in days, hours, minutes and seconds. The second block shows the corresponding minimum, maximum and average values.

Entry	Meaning
`Short Hold Pause`	The Short Hold pause before the current and latest connection, as well as the total accumulated Short Hold duration. The second block shows the corresponding minimum, maximum, and average values.
`Channels`	Number of channels used in the current and preceding connection. The second block shows the corresponding minimum, maximum, and average values.
`Charges`	Number of charge units (if appropriate for the line in question) for the current and the preceding connection, and for the total accumulated charges incurred since the router to this remote partner was started. The second block shows the corresponding minimum and maximum values of the most extreme connections and the average connection value for all connections
`Packets Tx,` `Packets Rx`	Number of data packets transferred (Tx) and received (Rx) in the current and last connection, and the number of the total data packets transferred and received in all previous connections. The size of a data packet depends on various conditions. It ranges from a few bytes to over 1500 bytes (for IPX). The second block shows the corresponding minimum and maximum values of the most extreme connections and the average connection value for all connections.

Entry	Meaning
`Bytes Tx,` `Bytes Rx`	The number of bytes transferred (Tx) and received (Rx) in the current connection and the preceding connection. The last column shows the total number of bytes exchanged during all connections. The second block shows the corresponding minimum and maximum values of the most extreme connections and the average connection value for all connections.
`Packets/sec Tx` `Packets/sec Rx`	Packet rates in transmitting and receiving directions
`Bytes/sec Tx` `Bytes/sec Rx`	Transfer rates in the transmitting and receiving directions, in bytes per second The effective bit rate can easily be determined by multiplying the byte rate by 8.

Appendix: A NDS over WAN Connections

A NDS over WAN Connections

This chapter contains recommendations and tips for using *ITK NetBlazer 4400* in a NetWare 4.1x environment.

The following topics are covered:

- NDS design
- time synchronization
- options for reducing NDS traffic over WAN connections

A.1 Understanding NDS Synchronization

Since the 4.x servers from Novell, NDS (**N**ovell **D**irectory **S**ervices) has provided a substantial innovation in network management.

Using a common NDS data base structure within a network, a user can access all network resources that he has access rights to, independent of where these domains are physically located.

To do this, objects are assigned to all resources in NDS. These include both the actually available resources (for example, printers, servers, users, etc.) and the logical resources (for example, user groups, print queues, etc.). All objects are managed in a common NDS data base so that even a complex network consisting of several servers is seen as a single information system by a user.

The objects can be arranged hierarchically using a directory tree. In turn, the entire tree can be subdivided again into *directory partitions*. These partitions are logical divisions or parts of the NDS data base that serve to increase system performance and to make network management easier.

> The terms *directory tree* and *directory partition*, as used with NDS, are independent of the directory structure on a physical drive. They only designate logical structures, not existing network resources.

To obtain a consistent NDS data base and to ensure data security within the NDS structure, copies, known as *replicas*, of every partition are created on different servers. A writable *master replica* is stored for every partition of the corporate network. This *master replica* contains all object information of the partition. Copies of this replica can be created as read-write replicas, as read-only replicas, or as subordinate reference replicas on different servers.

If the object structure within a partition changes, for example, when new users are created or passwords changed, all replicas of the partition are automatically synchronized. The change is time stamped so that a number of changes to one object can be arranged in chronological order. The time stamp avoids, for example, the phenomenon of a previously deleted user still having access rights to the network.

Time synchronization and possible configurations are discussed in Chapter A.3, *Understanding Time Synchronization* (page A-12).

Detailed information about the Novell Directory System (NDS) can be found in the Novell documentation.

NDS Synchronization via ISDN Connections

If segments connected to one another by way of ISDN are to be incorporated into common NDS data base structures in a corporate network, three factors are important in principle. These factors have a great influence on the functionality of the entire system:

- It must be possible to synchronize the NDS data base in principle between all the servers of one partition.
- The connection short hold must not be interrupted if there is a change to a replica on one side of the WAN.
- A uniform network time must exist throughout the entire corporate network to provide the changes to the NDS data base with a precise time stamp.

Within a corporate network, enough data traffic can be created to constantly maintain an ISDN dial-up connection just to synchronize the NDS data and a synchronized network time. This consequently causes immense connection charges.

Carefully planning the network partitions and replicas can greatly reduce this data traffic. The remaining, necessary data traffic can be further optimized by some configuration measures.

These measures include planning the directory tree and the partitions in accordance with the circumstances of your company or its geographic separation. Next, you have to plan the replica strategy of the partitions.

Before you plan to spread a directory tree among WAN connected locations, evaluate the necessity of such an action. In some cases it may be useful to create separate NDS trees for every location and then access the remote site(s) as bindery.

Two aspects must be kept in mind during the planning process:

- Fault tolerance must be ensured.
- Data traffic over the ISDN connections to synchronize the NDS must be kept to a minimum.

Novell considers 3 replicas sufficient for one partition. The replicas of a partition may also be configured by way of WAN connections.

The following two examples should explain this strategy:

Example 1

Small computer networks exist in a company with a central office and a subsidiary located in different cities. These networks are connected together by way of ISDN and are to be incorporated into a common NDS. To meet the requirements listed above, one common partition is configured for the entire company.

The replicas of both partitions are distributed over the entire network. The master replica is created in the central office. On all other 4.x servers in the network, a read-write replica is created.

The following figure illustrates this scheme:

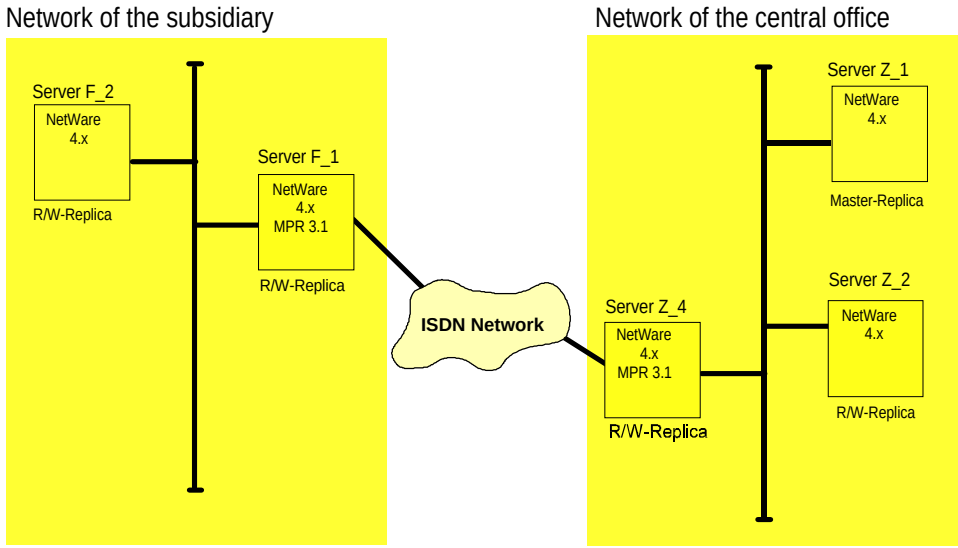


Fig. A-1 NDS Synchronization Example 1

Example 2

Another strategy for avoiding ISDN data interchange to the greatest possible degree is to allocate one partition to each segment of the company that has a network connected to other segments by way of ISDN. Then, the replicas of each partition are distributed within the LAN.

A company consists of a large central office and several small subsidiaries. A small network with a server is installed in each of the subsidiaries. The central office itself has a computer network with a number of servers. The subsidiaries are connected to the central office computer network by way of ISDN and are to be incorporated into an NDS structure.

With these requirements, one partition is configured for the central office and one for each subsidiary. The subsidiary partitions are subordinate to the partition of the central partition.

The master replica of the subsidiary partition is always created locally on the server of the subsidiary. The master replica of the central partition is created on one server in the central office. A read-write replica of this partition is created on all other servers of the central office.

In addition, a *subordinate reference replica* of each individual subsidiary is created automatically on every server of the central office containing a replica. These replicas contain a reference to the fact that a Master Replica of this partition is located on server x (see Fig. A-2, *NDS Synchronization Example 2*).

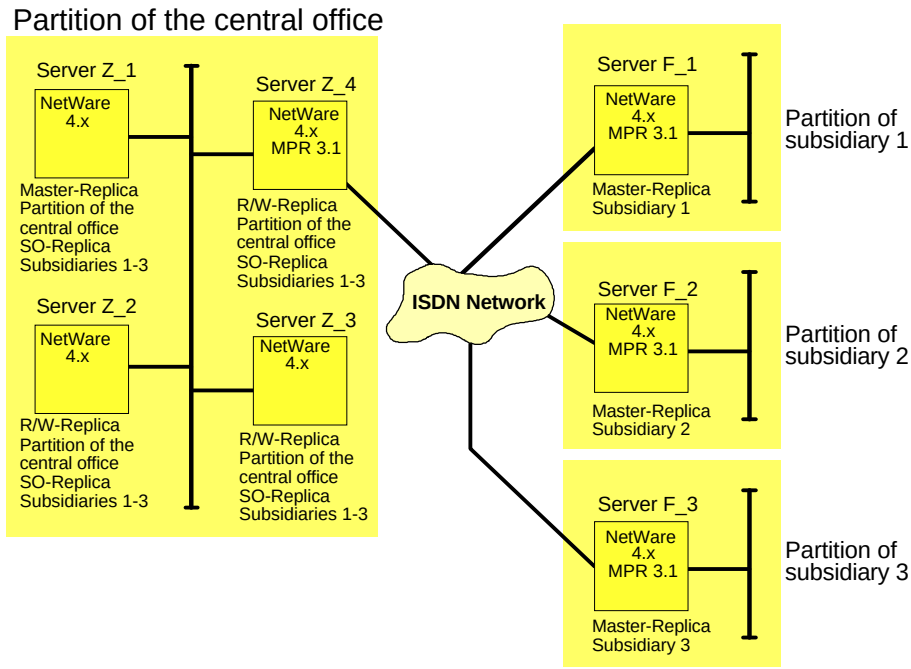


Fig. A-2 NDS Synchronization Example 2

A.2 Measures for NDS traffic reduction

By default, the replicas of a partition are synchronized every 30 minutes, even if there have been no changes to the objects.

If you have distributed replicas of a network partition by way of ISDN connections, every change to the NDS data base is also performed via this connection.

The uncoordinated filtering of NDS traffic may cause severe problems in network functionality and must be planned carefully. There are different options for suppressing NDS data traffic over ISDN connections:

- Using the Time Restriction functionality of ITK NetBlazer 4400
- Using the PINGFILT.NLM tool provided by Novell

We recommend you use the Time Restriction functionality of ITK NetBlazer 4400, as the PINGFILT utility is only effective and suited for systems with up to five servers storing replicas. Nevertheless, we will give you a brief description of the utility in this chapter.

Using the Time Restriction Functionality

The time restriction feature of the ITK NetBlazer 4400 is available for every configured partner and restricts call establishment in the way defined in the *Time Restriction Options* menu. Whereas the settings *Inbound* and *In- and Outbound* suppress every connection request, the entry *Server Caused* suppresses only requests sent by and bound for a server.

As a result, all NDS Packets will be filtered during the configured times. This admittedly prevents the server replicas from being updated, but the replica synchronization will be checked every 30 minutes and be performed as soon as it is possible.

Remarks for the Time Restriction Configuration:

1. Plan the restriction times carefully and restrict especially non-productive time periods, such as evenings and the weekend.
2. Select the same restriction times on every partner holding a replica to prevent the possible problem of “One Way Synchronization”.
3. Activate time restriction also on the remote side for the same periods. If you have systems in different time zones, adapt them to the local times.

4. If you perform the following steps for the _Default partner, all newly-configured Virtual Ethernet destinations will adapt this configuration.
5. The complete replica synchronization after a time restricted period may last up to 30 minutes.

Perform the following steps to suppress NDS synchronization by way of ISDN:

(1) From the *IX1CCA* main screen press <F10>, choose *Partner Configuration* and select the partner you want to edit.

(2) From the *Partner Configuration* window choose *Time Restriction Options* and select *Server Caused*.

(3) Leave the Restriction Parameter menu by pressing <Esc> and switch to the *Time Restriction Table* menu.

(4) Here you edit the Time Restriction matrix according to your needs using the space bar and the arrow keys. Connections are allowed in periods with an asterisk and suppressed when blank.

For a detailed description about the editing options, refer to Chapter , section *Time Restriction Configuration* (page 5-23).

(5) Press <Esc> and confirm the *Save Changes* message when recommended to return to the *IX1CCA* main screen.

Using the Novell PINGFILT Utility

Novell supplies the two programs DSFILTER.NLM and PINGFILT.NLM to suppress constant synchronization. These programs are stored on your ITK NetBlazer 4400 CD in the <drive:>\UPDATES\<os_version>\PINGFILT directory. They must be copied into the system directory of your server.

Times for a permitted NDS synchronization and the addresses of the servers to be filtered are specified using the DSFILTER.NLM program. The PINGFILT.NLM program starts the filter.

As the PINGFILT.NLM program suppresses all NDS information interchange, it is only possible, with the filter activated, to access the NDS partitions that are *locally* present. This means that, in Example 2, you can access the central office from the subsidiary only when the filter is not active.

In order to display the current UTC and the local server time, enter the command `TIME` on the *`System Console`*. In central Europe, the local time CET is one hour ahead of UTC.

Perform the following steps to suppress NDS synchronization by way of ISDN:

(1) Open the DSFILTER.NLM file and select the *Filter Pass Through Times* menu item.

(2) Specify the times in which the server can exchange NDS information.

Please note that the *filter pass through times* are specified in the World Standard Time of UTC (United Time Coordinated).

(3) Now select the *List Filter Address* menu item and press <Ins> to enter the internal IPX numbers of the remote partners to which the NDS information is to be filtered (as a rule, these are all WAN remote partners that have a replica of a partition).

If you press <Ins> twice, all servers known to the System are displayed and you may select them directly from the table.

(4) Save your configuration, end the DSFILTER program, and load the PINGFILT.NLM program with this command:

```
load pingfilt
```

A.3 Understanding Time Synchronization

A standard network time is necessary for smooth data transfer and the synchronization of the NDS data base in a LAN with several servers. As the internal clocks of the individual servers operate only with limited precision, time synchronization among these machines is required.

For this, it is possible to assign a time server status to the servers. In general, there are two different cases:

- secondary servers and
- time sources (primary, reference and single reference servers).

The time sources in a network specify a network time, and relay this time to the secondary time servers and all workstations. In this way, an unambiguous time stamp can be set for the NDS data bases in the network.

One important criterion in time synchronization is synchronization among the time servers. Only when all servers behave in a “network synchronous manner” can they interchange correct NDS information. This synchronization is indicated when the *time synchronization flag* is set. A server that is not operating in a network synchronous manner, results in the situation where no NDS information can be interchanged.

In the default configuration, all servers make use of the **S**ervice **A**dvertising **P**rotocol (SAP) to interchange time information with one another. In this case, all servers integrated into the network are connected into the process.

While this form of time synchronization is simple, it is not practical for networks connected to one another by means of ISDN. If the SAP packets are filtered in the router, the necessary time synchronization cannot take place. If they are not filtered, time synchronization will use ISDN connections and this will cause plenty of calls.

A suitable time synchronization strategy is to configure the time servers separately. This means that each server is told the servers with which it is to synchronize. In this way, it is possible to synchronize the servers within one LAN. Then, time synchronization by way of ISDN can be handled directly by the participating routers.

Example Time Server Combination

To configure your network into such a time server combination, you may specify the following parameters in the SERVMAN program. These changes must be made on all servers connected in the same NDS system.

One server on each side is configured as a single reference server. This type of time server does not interchange time information with other time sources, but rather represents its time as the absolute network time. It is recommended that you use the Router PC as the machine to maximize the ITK NetBlazer 4400 time exchange functionality.

All other servers are configured as secondary servers, both in the central office and in the subsidiary, to follow the local single reference servers.

The following figure explains this time server combination:

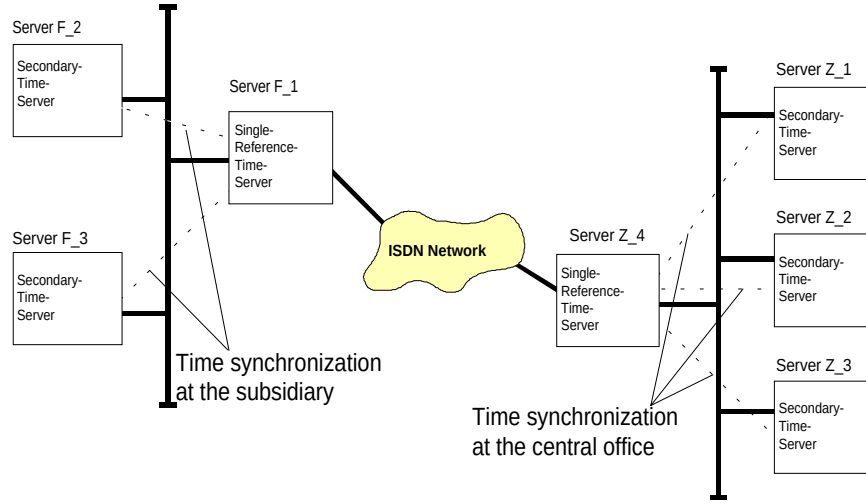


Fig. A-3 Time Synchronization – Example Time Server Combination

To supply the same time to the two independent single reference servers, you can now assign an atomic clock as the time source to the single reference servers. However, in the case of a large WAN network, this can lead to considerable costs.

The ITK NetBlazer 4400 provides the alternative for polling the set time for each individual server when establishing the connection and to accept this time as its internal time. In this case, it is useful to assign an atomic clock on one side and tell all other stations to get their time via ISDN from this server.

A.4 Configuring Time Synchronization

The configuration of the described time synchronization strategy is performed in two steps:

- Adapt the necessary Time Synchronization parameters on every participating server
- Assign one Single Reference server as the “master clock” and let all other routers get their time from this destination.

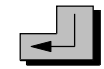
Adapt Time Synchronization Parameters

You have to perform these changes on **all** servers that are connected into the NDS system.

Perform the following steps to operate your network in the time server combination mentioned above:

(1) Load the Servman program using the command:

```
load servman
```



(2) Select the *Server parameters* menu item.

(3) Change to the *TIME* submenu and press <Enter>.

(4) To disable time synchronization by way of SAP, change the following entries:

```
TIMESYNC Configured Sources = ON
TIMESYNC Service Advertising = OFF
```

(5) To specify or change the type of a time server, specify the appropriate value in the following entry:

`TIMESYNC Type = xxxx`

For the single reference servers: `TIMESYNC TYPE = SINGLE`

For the secondary servers: `TIMESYNC TYPE = SECONDARY`

You have to change the following entries only for the secondary servers:

(6) To increase the interval between time synchronization operations, change this entry:

`TIMESYNC Polling Interval = xxxx`

(The time is in seconds, for example, 43200 seconds = 12 hours.)

(7) To increase the time interval for which a time server still operates in a "network synchronous manner," change this entry:

`TIMESYNC Synchronization Radius = xxxx`

(The time is in milliseconds, for example, 1200000 milliseconds = 2 minutes.)

(8) Enter the server names to be used as the time source.

For the secondary servers in the central office:

`TIME SOURCE =` <Name of the single reference server of the central office>

For the secondary servers in the subsidiary:

`TIME SOURCE =` <Name of the single reference server of the subsidiary>

(9) Save the changes by exiting the submenu, selecting the following lines one after another, and confirming your selection with <Enter>:

`Update AUTOEXEC.NCF and STARTUP.NCF now`

`Update TIMESYNC.CFG now`

As it cannot always be ensured that the configuration changes were indeed included in the TIMESYNC.CFG file, you should check whether this file contains the correct values.
Use the following command to do this:

```
LOAD EDIT SYS:SYSTEM/TIMESYNC.CFG
```

If necessary, change the values there so that they correspond to your configuration. The configuration changes are properly included in any case in the `AUTOEXEC.NCF` and `STARTUP.NCF` files.

It may also be necessary to erase existing entries. If, for example, you want to change a reference server into a single reference server, you must erase the entries specified as `TIME SOURCE = xxxx`.

If you are using a German version of the server, the comment lines are not automatically identified as such by means of a “#”! You must manually enter this character into the appropriate lines.

Determining the Server Time by Way of ISDN

This feature is only available if the ITK NetBlazer 4400 acts as Single time server! If another server should act as time source, you must equip it with an external clock.

Define one single server in your NDS tree as master clock, for example by use of an atomic clock, and let the other time servers get their server time from this station. To do this, you must expand the IX1CCA.CFG parameter file on these machines.

In the case of the slave clock server, you have to change one entry. To do this, please perform the following steps:

(1) Load the IX1CCA.CFG file into the editor from your *System Console* using this command:

```
load edit sys:system/ix1cca.cfg
```

(2) Remove the REM in this entry:

```
REM SetServerTimeFromPartner = <Partner Name>
```

(3) Replace the <Partner Name> field with the name of the single server functioning as the master clock.

(4) Save the changed file.

Changes in the time server configuration do not take effect until the system is rebooted.

B ISDN Boards and ITK Modem Boards for ITK NetBlazer 4400

This appendix offers recommendations for selecting ISDN boards and adapters to use with your *ITK NetBlazer 4400* product.

The following sections describe which ISDN boards are recommended in given scenarios (see table on page B-2).

High data throughputs and maximum functionality cannot be achieved unless the router products and ISDN boards are optimally matched. ITK NetBlazer 4400 has therefore been fully optimized for the specific performance features of the *active* ITK boards (including analog modem extensions) and of the *passive* ITK board (ITK Micro).

The driver software of all ITK boards will install simultaneously with the ITK NetBlazer 4400 installation.

The following table shows the supported ITK boards and their important features:

ITK Boards	ISDN Ports (B channels)	ESS	Channel Bundling	Fax	Modem	GSM	MVIP	Data Compression	Leased Line
ITK Basic PCI	2	no	yes	yes[1]	yes[1]	yes	no	yes	yes
ITK Basic 1MB	2	no	yes	yes[1]	yes[1]	yes	no	yes	yes
ITK Basic 4MB	2	yes	yes	yes[2]	yes[2]	yes	no	yes	yes
ITK Octo	8	yes	yes	yes[2,4]	yes[2,4]	yes[3]	yes	yes	yes
ITK Primary	30	yes	yes	yes[4]	yes[4]	yes	yes	yes	yes
ITK Primary PCI	30	yes	yes	yes[4]	yes[4]	yes	yes	yes	yes
ITK Micro	2	no	yes	no	no	yes	no	yes[5]	no
ITK MultiModem[6]	-	-	-	yes	yes	yes	yes	-	-
ITK DigitalModem[7]	-	-	-	no	yes	yes	yes	-	-
ITK FaxModem	-	-	-	yes	yes	yes	-	-	-

[1] with ITK FaxModem; Due to memory limitations on the ITK Basic 1MB / PCI, either fax or modem support is available

[2] with ITK FaxModem

[3] with ITK FaxModem; Please check the manual of your GSM card for information about analog modem connections.

[4] with ITK MultiModem or ITK DigitalModem;
ITK DigitalModem supports modem only.
ITK MultiModem supports fax and modem.

[5] Data compression of ITK NetBlazer 4400 software

[6] The ITK MultiModem is available with 8 modem channels.

[7] The ITK DigitalModem is available in five configurations with 6, 12, 18, 24, or 30 digital modem ports.

Appendix: C Messages

C Messages

A large number of the error messages that may occur are produced by the ISDN exchange or the PBX. These messages point to errors during connection establishment. The *ITK NetBlazer 4400* accepts these messages and displays them on the screen in the journal information frame. They are also stored accordingly in the journal file. See Chapter 4.2, *Connection Journals and Activity Log* (page 4-11).

Other error messages that usually occur before or after connection establishment are reactions to errors in the internal configuration or occur during operation because of special situations.

C.1 Messages before a Connection to the ISDN Switching Node could be established

`0x3301: Error D channel Layer 1: No ISDN`

A connection could not be established from your ITK board to the ISDN exchange.

Possible causes

- One end of the cable to the ISDN junction box is not connected or the cable is defective.
- The ISDN connection to the exchange is not operating or defective.

Remedies

- Check that the ISDN cable is connected properly and test it for mechanical damage.
- Check – for example, using a different ISDN device on the same BRI bus – whether the connection to the ISDN exchange is operating properly.
- As a last resort, try replacing the ISDN cable of your PC board.

`0x3302: Error establish D channel Layer 2`

A *D channel layer 2* connection could not be established from your ITK board to the ISDN exchange.

Possible causes

- The ITK board is not configured correctly, or
- the ISDN line is not configured correctly, particularly in the case of private branch exchanges.

Remedy

- Make sure that the configuration of the ISDN line corresponds to the configuration of the terminal (ISDN board). Pay attention that the point-to-point or point-to-multipoint connection is set correctly.

`0x3307: Error abortion D channel Layer 3`

A *D channel layer 3* connection could not be established from your ITK board to the ISDN exchange.

Possible cause

- The D channel protocol for your ITK board is not identical to the settings at the exchange.

Remedy

- Determine which protocol your exchange or private branch exchange is using for your connection and set your ITK board to this protocol. You can find more detailed information in the *Installation and Interfaces* manual of your ITK board.

C.2 Messages from the ISDN Switching Node

`0x3403: bearer service not implemented`

The *data transfer 64 kbit/s* service is not configured for you or the connection you called.

Remedies

- Check the number you dialed. The number you dialed can be displayed on the router screen.
- Find out from your carrier or from the service organization for your private branch exchange whether this service is enabled for your ISDN connection.
- Ask your communications partner whether this service is enabled for him.

`0x3426: Network out of order`

The network is not capable at this time of establishing the connection.

Remedy

- Try to establish the connection again. If this message appears again, report it to the telecommunication repair services of your carrier.

`0x3432: Requested fac. not subscr.`

The *data transfer 64 kbit/s* service has not been requested for you or for the connection you called.

Remedies

- Check the number you dialed.
- Find out from your carrier or from the service organization for your private branch exchange whether this service is enabled for your ISDN connection.
- Also ask your communications partner whether this service is enabled for him.

`0x3435: Destination not obtainable`

The ISDN connection could not be established because the called destination address is not valid.

Remedy

- Check the number you dialed for the corresponding remote partner and dial it again. The current number dialed is displayed in the Journal Window and in the IX1CCA.TRC file.

`0x3438: Number changed`

The telephone number of the remote partner has changed.

Remedies

- Check the telephone number.
- Find out the new telephone number.

0x3439: Out of order

The terminal on the remote end is not operating.

Remedy

- Dial again. If the error occurs again, check whether the remote partner is operational.

0x343A: No user responding

The called terminal is not responding.

Remedies

- Make sure that the remote router is switched on.
- Check the telephone number of the called remote partner.

0x343B: User busy

The called terminal is busy.

Remedy

- Make sure that the remote partner is activated and that at least one B channel is available for data communication.

0x343E: Call rejected

The remote partner (the other router or the remote PC) has rejected your incoming call.

Remedies

- This is normal if callback is set at the other end.
- Check the communications authorization at the remote partner. Possibly, the entries for authorized remote partners were not made properly at your communications partner.

0x3459: Network congestion

Congestion has occurred in the ISDN network of your carrier.

Remedy

- Try to establish the connection again. If this message appears again, please report it to the telecommunication repair services of your carrier.

0x3471: Remote procedure error

The connection was interrupted by the ISDN exchange because of an undefined problem in the switching node.

Remedy

- Try to establish the connection again. If this is unsuccessful, try to bring the router into a defined initial state by means of a reboot.

C.3 Messages when loading the ISDN Drivers

Error: `ix1 adapter not found`

The driver could not access the ITK board(s) when starting.

Possible cause

- The correct loading procedure for the software was probably not performed for the ITK board.

Remedies

- Unload all associated modules, and then reload them by executing the connect batch file.
- Shut down your router and perform the complete loading procedure again.
- Check the hardware configuration of your ITK boards.

Error: `cannot allocate accepted dial number list`

Error: `cannot allocate outgoing dial number list`

Error: `System out of memory`

Error: `could not allocate resource tag`

During start up, the driver could not obtain sufficient system resources, and then ceased operation.

Remedies

- Boot the server to reorganize all system resources and try to load the drivers again.
- Expand the main memory of your router.

C.4 Messages during Operation

Error: `Run out of connection slots`

The ISDN Communication Manager cannot define an additional remote partner because more than 250 communications partners exist.

Remedy

- Delete some of the partners that are no longer needed or contact your system vendor.

D Information about SNMP Traps

The ITK NetBlazer 4400 can send SNMP Traps (SNMP = Simple Network Management Protocol) for different router relayed events. Management systems, such as Novell NMS, can report these traps which are listed by severity.

You find the description of the possible SNMP traps in the following table:

Trap name	Short description	Description
ix1cmDriverLoaded	ix1cca loaded	The ISDN connection manager is started.
ix1cmDriverUnloaded	ix1cca unloaded	The ISDN connection manager is unloaded.
ix1cmISDNControllerUp	ISDN controller is up	The ISDN board is up and running.
ix1cmISDNControllerDown	ISDN controller is deactivated	ISDN board is deactivated (temporarily or permanently).
ix1cmModuleLoaded	module loaded	A module used by the ISDN connection manager was loaded.
ix1cmModuleUnloaded	module unloaded	A module used by the ISDN connection manager was unloaded.
ix1cmLoadError	error loading module	An error occurred while loading a module of the router
ix1cmConnectEstablished	connection established	An ISDN connection is established.

Trap name	Short description	Description
ix1cmConnectSleeping	connection sleeping	An ISDN connection is physically disconnected.
ix1cmConnectReleased	connection released	An ISDN connection is released.
ix1cmConnectDisabled	connection disabled	An ISDN connection is disabled.
ix1cmDChannelError	D channel error	An ISDN connection is disconnected due to a D channel Error.
ix1cmBChannelError	B channel error	An ISDN connection is disconnected due to a B channel Error.
ix1cmProtocolError	protocol error	An ISDN connection is disconnected due to a protocol Error.
ix1cmUserAction	user action	The operator of the console initiates a command.
ix1cmCSLAction	CSL action	The CSL of the Novell router initiates a command.
ix1cmBChannelAdded	B channel added	A B channel is added to an existing connection.
ix1cmBChannelRemoved	B channel removed	A B channel is removed from an existing connection.
ix1cmWakeUpPacket	wake up packet	A connection is established due to a packet that should be send.

Trap name	Short description	Description
ix1cmCLIAuthenticationError	CLI authentication error	A partner with unknown CLI tried to dial into the router.
ix1cmPPPAuthenticationError	PAP/CHAP authentication error	A partner with unknown PPP Name and Password tried to dial into the router.
ix1cmESSAuthenticationError	ESS authentication error	A partner with wrong EES tried to dial into the router.
ix1cmChargeLimitReachedPartner	partner charge limit reached	The limit of charges allowed for this partner was reached.
ix1cmTimeLimitReachedPartner	partner time limit reached	The limit of outgoing connection time allowed for this partner was reached.
ix1cmTimeRestrictedPartner	connection time restricted	A connection to this partner cannot be established due to configured time restrictions.
ix1cmAccountExpired	account expired	A connection to this partner can not be established as the credit has expired.
ix1cmResetCredit	reset credit	The credit for this partner is initialized again.
ix1cmChargeLimitReachedRouter	charge limit reached for the router	The total number of charges allowed is reached. An outgoing connection can no longer be established.

E Install Novell NetWare 3.2

Prerequisites

Installation involves bringing down the server. Schedule this installation accordingly.

If you have previously installed NetWare, you don’t need to remove previously installed patches because the installation program compares patches on a per-file basis

- Make sure that all users are logged out and there are no open files.
- NetWare 3.12 must be running on the server.
- Make sure the server boots from a hard disk, not from diskette.
- Back up all data on server volumes and DOS partitions.

Several files in SYSTEM, PUBLIC, and LOGIN are overwritten during NetWare 3.2 install. As an extra precaution, BACKUP.BAT has been provided to back up these files. To perform the backup, insert the ITK NetBlazer 4400 CD in a workstation, log in as Supervisor, and run <CD-ROM drive letter>:\32ENH\BACKUP.BAT.
Files in the DOS partition, except SERVER.EXE, are not backed up.

The following conditions may require you to bring down the server before installation:

- The command "REMOVE DOS" must not have been used prior to installing this product. If DOS has been removed, you must reboot the server to restore it, first ensuring that it is not automatically removed by a command in the AUTOEXEC.NCF file.
- Installation requires 15 MB of free space on the server’s DOS partition. If you are not sure how much space is available on the server’s DOS partition, you can check the amount of free space using DOS after bringing down the server.

Loading NetWare 3.2 Installation Files from Server:

(1) Insert the ITK NetBlazer 4400 CD in the server's CD-ROM drive. If the CD-ROM is a DOS device, go to *Install NetWare 3.2* (page E-3); otherwise go on with step 2.

(2) Make sure the driver for your CD-ROM is loaded. Drivers are usually loaded in the STARTUP.NCF. (For example: *LOAD AICxxxx.DSK, LOAD ASPICD*)

(3) At the server console, type *LOAD CDROM.NLM*.

(4) Type *CD DEVICE LIST* to verify that the ITK NetBlazer 4400 CD is recognized.

(5) Mount the CD-ROM as a volume. Type *CD MOUNT* NETBLAZER4400.

Loading NetWare 3.2 Installation Files from Workstation:

(1) Insert the ITK NetBlazer 4400 CD into the workstation's CD-ROM drive.

(2) Log in to the target server as Supervisor.

(3) Map a drive to a volume with at least 15 MB of free space, and create a directory named **32ENH** on that volume.

(4) Copy the CD's 32ENH directory with subdirectories to the mapped drive. (For example*: xcopy D:\32ENH*.* G:\32ENH /s*)

Either go to the server or run RCONSOLE from the workstation to access the server console screen. If you use RCONSOLE, you must copy *\32ENH\PUBLIC\RCONSOLE.EXE* manually to *SYS:PUBLIC* after installation.

Install NetWare 3.2

(1) Type *LOAD INSTALL* at the server console.

(2) Choose *Product Options* and press *Insert* to install a new product.

(3) When asked for a location of the source files, delete *A:* and specify one of the following:

- If the CD-ROM is a DOS device, type *<CD-ROM drive letter>:32ENH* (for example, *D:32ENH*)
- If the CD-ROM is mounted as a volume, type *<CD-ROM volume name>:32ENH* (for example, *NETBLAZER4400:32ENH*)
- If installing from a server directory, specify the path to the directory where you copied the files. (For example, *SYS:32ENH*)

(4) When the installation is complete, close all applications and connections, bring down the server, and reload the server to update all files.

Glossary

1TR6	Technical directive describing the D channel protocol of the German ISDN. This ISDN protocol allows subscriber number display, call diversion and three-party conferences, for example.
a/b interface	Designation for interfaces (two-wire) used in analog telephone, modem, fax, exchange or network lines.
Account	User ID Logon authorization for a mailbox or a network consisting of the user's name or pseudonym, and a password.
Analog	Mode of transmission of signals or information Criteria for analog signals are how high/low they are (frequency) and their intensity (amplitude).
ASCII	American Standard Code for Information Interchange International standard which specifies the characters which can be displayed on computers.

Authentication	Check of logon authorization for a system. Authentication may be carried out either by the hardware, for example through the serial numbers of the ISDN cards, or by the software. In both cases, information is stored which can be coded and exchanged more than once if necessary until a connection is made. Such security mechanisms are particularly important if previously closed networks are opened up via ISDN and therefore have a high security requirement.
B channel (basic access)	Transmission channel of an ISDN system via which useful data (voice, data, video) can be transmitted in digital form at 64 kbit/s. An ISDN basic access (S_0 line) comprises two B channels. A primary rate access (S_{2m} line) consists of 30 B channels.
Bandwidth on Demand	Provided when required for optimal utilization of links. Various channel bundling variants are available for this in the ITK router products.
Base contact	The S_0 line (or BRI line) of the ISDN is also known as the base contact.
Basic access	See “B channel“
Baud	Measurement of the signal rate at which data is transferred. It specifies the number of signal exchanges per second, in contrast to bps (**b**its **p***er* **s**econd).
Bit rate adaptation	The bit rates of conventional data interfaces are generally lower than those in the ISDN and need to be adapted when such terminal equipment is connected.

Bit rate	Measurement of the transmission speed of signals in digital systems.
BRI	Basic Rate Interface Basic ISDN and basic Euro-ISDN line, also referred to as S_0 line. This is the most commonly used ISDN system offering one D channel and two B channels. The two B channels can be used independently of one another to transmit voice, text, data and graphical information. The D channel is a control channel. It establishes and terminates the connection.
BSS	Basic Security Service Security mechanism controlling network access via the ISDN using the dial number transferred.
CAPI 2.0	See “CAPI“
CAPI	Common ISDN Application Programmable Interface A software interface which allows the ISDN board to communicate with applications and vice versa (for example, ITK Columbus Client). CAPI is an international standard: Version 2.0 is based on the European ISDN standard DSS-1.

Channel bundling

Intelligent use of the maximum bandwidth available in ISDN.

If needed, the B channels of an ISDN basic access are bundled so that they can be used in parallel.

With 2 B channels, the seeming result for the application software is a transmission channel having a speed of 2 x 64 kbit/sec, that is, 128 kbit/s.

CHAP

Challenge Handshake Authentication Protocol

An authentication procedure used in the Point-to-Point Protocol (PPP), consisting of a system ID and a password exchanged during the establishment of the ISDN connection between two remote terminals.

In CHAP the information is exchanged in encrypted form.

Closed User Group

Also known as CUG.

In DSS-1 groups of subscribers can use certain agreed services solely amongst themselves.

Compression

Coding of data in order to save storage space or shorten transfer times. Compressed data has to be decompressed again before it can be used. There are a large number of compression algorithms and utilities. Common utilities include zip, pkzip and arj.

The active ITK ISDN boards also have efficient compression during data transmission. This enables the transfer rates of an ISDN B channel to be increased significantly.

D channel

In the ISDN, the channel structure divides the interfaces into several speech/data channels (B channels) and a service channel (D channel).

The D channel has a bandwidth of 16 kbit/s or 64 kbit/s for transmission of the D channel protocol depending on the nature of the interface.

D channel protocol

Communication in the ISDN is regulated by protocols. In the D channel protocol, information on the dial numbers of the remote terminals or the transmission bandwidth are transferred and swapped if necessary. In Germany, the D channel protocols “Euro-ISDN DSS-1” and “1TR6” are used.

Data bit

A bit is the smallest digital unit, corresponding to a binary information “1” or “0”. In digital transmission, the data bits contain the actual information section of a packet which is required for transferring information. Compare with: parity bit, stop bit.

Data transfer rate

Speed at which data is transferred, measured in bit/s.

Decoder

Electronic circuit or computer program for de-encrypting message which has previously been coded (example: T Online Decoder).

DHCP

Dynamic Host Configuration Protocol

Instead of static assignment of an IP address to an IBM PC in a network, DHCP allows dynamic IP address allocation. An application assigned to an IP address is allocated this automatically on request. In order to use permanently assigned IP addresses in the network in parallel, a particular range of addresses can be reserved for the DHCP by the Network Administrator.

Digital	Information transfer via discrete values. Digital information is represented by the two states “1” and “0”. In the ISDN, information is transferred digitally, that is, signals are transferred using discrete (whole) numerical values. This enables voice and data to be transferred in a single network.
Download	Receipt of data from an outside computer to one’s own computer.
DSS-1	Digital Subscriber Signaling System No. 1 (formerly E-DSS-1) Protocol which realizes communication in the ISDN network across Europe.
DTMF	Dual Tone Multi Frequency See "Dual Tone Multi Frequency Signaling"
EAZ	Endgeräte-Auswahl-Ziffer (Terminal Selection Digit / Terminal Selection Number) The EAZ is a feature of the German ISDN D channel protocol 1TR6. It enables terminals to be selected directly. The terminal selection digit can be set via the application software (for example ITK Columbus Client) or via switches on the terminal equipment.
E-DSS-1	See "DSS-1"

EFT

Euro File Transfer

File transfer standardized by ETSI. Standardization enables different file transfer programs to communicate with each other.

Open communication protocol based on ETS 300-075 for manufacturer-neutral and system-neutral file transfer, initiated by the European ISDN User Forum (EIUF).

E-Mail

Abbreviation for "Electronic Mail", mainly sent and received over the Internet.

ESS

Extended Security Services

ESS is a security mechanism for data transmission (only with active ISDN boards).

Euro-ISDN

The "MoU" (Memorandum of Understanding), also known as E-DSS-1 or DSS-1, is a D channel protocol which was specified in order to create a uniform ISDN standard throughout Europe. ISDN network operators across Europe use this protocol for digital information communication.

Extension

Telephones or other communication devices (for example fax) connected to telecommunications systems are extensions.

Fax

Abbreviation for facsimile.

Electronic transmission of data in pictorial form.

Fax G3

Group 3 fax machine

These machines are the most widespread. In group 3 faxes, the principle of transmission is as follows: the “image” to be communicated (text, drawings, etc.) is first scanned, similar to in a photocopier, and coded as electronic information. This coded information is provided with a transmission carrier (modulation) and transferred via the telephone network. At the receiving end the transmission carrier is removed (demodulation), the information is decoded and finally the original “image” is recorded.

Fax G4

Group 4 fax machine

Group 4 fax machines are used in the ISDN. Compatibility with group 3 should be guaranteed. Both digital and analog connection to the network are possible.

File transfer

Data communication.

Transfer of files by data communication.

Fossil driver

Fido/Opus/Seadog Standard Interface Layer

Driver for serial interfaces used in the area of mailboxes. Its counterpart for ISDN boards is CAPI.

FTP

File Transfer Protocol (for example TCP/IP)

FTP is used to transmit data between a wide variety of systems. FTP is a very efficient application, but only provides basic data transmission commands.

Gateway	Interface between two networks working with different network protocols. Also interface between two communications systems, for example, from videotext to fax.
HDLC	High Level Data Link Control Protocol of OSI layer 2 for recognition of data transmission errors. The data to be transmitted is divided into packets.
Host	Host computer; system in which users log on for data transfer. Databases, mailboxes, videotext centers and other remote partners may serve as the host.
Internet	Worldwide data network with services such as the WWW, E-Mail, FTP, etc. Communication takes place in accordance with specified rules. IP is used as the communications protocol.
Intranet	Network offering an organization similar services as the Internet, but not necessarily linked to the Internet. For example, companies which set up one or more WWW servers on an internal network in order to distribute information internally.

ISDN	Integrated Services Digital Network A group of standards used to simultaneously transmit voice, text, data and video in digital form. The most frequently used ISDN system (in Germany: BRI) carries one D channel for signaling and two B channels for user data over the same copper wires. The transfer rate is 64 kbit/sec, in the USA, it is sometimes 56 kbit/sec. The transfer follows uniform transport standards and protocols (Germany: 1TR6, Europe: DSS-1).
ISDN board - active	ISDN board with on-board processor. Has a separate processor and a separate memory, thereby relieving the PC.
ISDN board - passive	ISDN board without a separate processor and memory. The ISDN protocols are processed by the processor of the PC.
ITK Connectivity Protocol	An extremely efficient data transfer protocol developed by ITK AG.
IP	Internet Protocol Protocol used on an international level which transports data to a receiver across various networks.
IPX	Internet Package eXchange A network protocol used by Novell.
LAN	Local Area Network A "local" computer network within a corporate site connecting many computer terminals.
Link	Cross-reference to other pages in the WWW.

Login

Regular entry into a data communications system or a local network stating name, and if necessary, a personal password.

Establishing a data communication contact.

Mail

Also known as: Private Mail (PM).

Personal message. In contrast to news, private mails cannot be seen by all users but instead are personally addressed to a particular communication partner - just as in the case of a regular mailed letter.

Mailbox program

Also known as mailbox software.

Program controlling access to a mailbox and for management of mailbox data.

MLB

Mac Layer Bridging

Control of data in a network via the node address (MAC address) of a connected client PC.

Modem

Modulator/Demodulator

A modem converts digital bit patterns into analog tones (modulation, reverse process = demodulation). This enables the digital signals of an EDP (Electronic Data Processing) system to be transferred via the telephone network.

MSN	Multiple Subscriber Number A feature of DSS-1 The Multiple Subscriber Number replaces the EAZ in the national ISDN protocol 1TR6. Up to 10 independent subscriber numbers from the subscriber number household of the DIVO can be switched to a Euro-ISDN line. Each of the subscriber numbers can be dialed individually.
Multi-device line	Deutsche Telekom AG defines a multi-device line as an S_0 line with Euro-ISDN protocol in a bus configuration. Up to eight devices can be connected to this S_0 bus.
Multilink PPP	Multilink describes the bundling of B channels in the ISDN using the Point-to-Point Protocol (PPP). In the multilink procedure, the data is divided between the B channels and merged again later. This channel bundling can be used to make a connection with your Internet provider via the NDIS-WAN Miniport.
NDIS	Network Device Interface Specification Programming interface for network driver software.
NDIS-WAN-Miniport	Software interface which communicates between the ISDN board and the applications. Supports RAS and TCP/IP applications, amongst others.

NT

Network Terminator

The NT is a module which coordinates the secure interaction of the protocols on the user network interface in the ISDN subscriber line area. It matches the U and S reference points with each other and is divided into two areas, NT1 and NT2. NT1 carries out adaptation of electrical and physical variables (for example 2-wire to 4-wire). NT2 carries out security and address tasks.

Offline

State in which no data link exists.

Online

Data link and data exchange with remote partners.

PABX, aka PBX

Private Automatic Branch Exchange or
Private Branch Exchange

See "Telecommunications system"

PPP

Point-to-Point Protocol

ISDN communications protocol adapted to international standard. This standardization allows communication with devices from different manufacturers. All the leading hardware and software manufacturers as well as the Internet service providers use this standard, which allows interactive access to the Internet via dial-up lines such as telephone or ISDN.

Primary rate access (PMX)

Special type of access offering a total of 30 B channels each with a transfer speed of 64 kbit/s and a D channel, likewise with a speed of 64 kbit/s. In the ISDN the S_{2m} line is designated as PMX. Here all the channels of the S_{2m} interface have the same dial number.

Protocol	In transmission technology, rules and agreements (protocols) are necessary in order to reach consensus on the time and type of information transfer and its interpretation. Distinctions are made between, for example, network protocols such as IPX and TCP/IP, data transfer protocols such as PPP or X.75 and authentication protocols such as PAP or CHAP.
Provider	Regional or cross-regional provider of Internet accesses.
Q.931	Q.931 is the name of a recommendation by CCITT which is used to designate the signaling protocol in the ISDN.
RFC	Request for Comments Standard of a series of numbered Internet information documents and standards. For example, the RFC 822 standard is accepted as a format for Internet Electronic Mail.
RJ45	Designation for an eight-pin plug technology used in the ISDN area for the S_0 line. In Germany, this technology is also known as UAE. The designation “Western plug” is also commonly used.
Router	A Router is used as an interface between networks and is a connector between different network segments. If these networks use different protocols, then a multiprotocol router must be used.

Routing	Control and steering of network traffic. Also management and generation of transmission paths between Internet computers.
S_0	Designation for the basic contact of the ISDN and the Euro-ISDN, also referred to as BRI. The line has two B channels and one D channel. The two B channels can be used independently of each other for communicating voice, data, text and video information. Transfer speed: 64 kbit/s. The D channel is used as a control channel and can be used, for example, for establishing and terminating the connection. Transfer speed of the D channel: 16 kbit/s or 64 kbit/s depending on interface design.
S_{2m}	Designation for the primary rate access of the ISDN. The access has 30 B channels and one D channel. The 30 B channels can be used independently for communicating voice, data, text and video information. The D channel is used as a control channel and can be used, for example, for establishing and terminating the connection for the B channels.
Service channel	See “D Channel“
SLIP	Serial Line Internet Protocol Data communication procedure on the Internet. Adaptation of the Internet protocol for dialed connections, for example telephone or ISDN connections.
SMTP	Simple Mail Transport Protocol Data communication procedure for E-Mails.

Speech/data channel	See “B channel“
SPID	Service Profile Identifier For US D channel protocols NI-1, 5ESS at least one SPID is required per ISDN line. Each SPID is assigned to an ISDN service (for example voice, data…).
SPX	Sequenced Packet eXchange Connection-oriented network protocol in Novell networks.
T.70	Network-independent transport protocols for telematic services.
TCP/IP	Transmission Control Protocol / Internet Protocol Two frequently used protocols for data transmission and Internet connections which can be used for different transport media.
Telecommunication	Transfer of analog or digital data.
Telecommunications system	Analog telecommunications systems are telephone systems used for voice communication which can also be used for transmission of the analog fax service. Digital telecommunications systems, which are now widespread, are also suitable for transmission of telematic services.
Terminal adapter	Allows non-ISDN capable terminal equipment to be used in the ISDN.
Unix	Network operating system.

V.110	Bit rate adaptation, defined up to 9600 Baud; available for most terminal adapters up to 38400, and for some also up to 57600 Baud. Each bit on the V24 or X.21bis page is mapped to a bit of the 64 kbit stream of the B channel. In some implementations, slower speeds can be multiplexed, that is, there are several valid mappings.
V.120	Similar to V.110, but additional removal of start and stop bits in the B channel data stream. The theoretically possible data speed (without compression) is therefore 76800 Baud.
WAN	Wide Area Network In contrast to a LAN, the extent of a WAN is not limited by physical boundaries. Local networks are made into a WAN by connecting them via public networks such as ISDN.
WWW	World Wide Web (also W3) An Internet service which uses graphically designed pages and "hyperlinks". Hyperlinks can be text or graphics. Clicking on a hyperlink takes the user to other pages containing additional information.
X.25	Interface for accessing packet-switched data networks.
X.75	Protocol for the link between packet-switched networks.

Index

Bold page numbers contain detailed information.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X