ITK NetBlazer 8500

Use, Management and Configuration

Version 5.00

November 98

A subsidiary of Digi International

Table of Contents

Preface

Advantages of ITK NetBlazer 8500

Overview

Today, two different, separate networks are being used in the communications infrastructure of modern companies. On the one side, there are data networks with a powerful server or host computer as the focal point. This network is used by all departments in the company for performing various tasks using the respective terminal equipment that is connected (PCs and terminals). On the other side, the voice network with an analog or digital exchange as the control centre – all telephone and fax communications are conducted via this network.

So far there are usually two different network structures for data traffic and voice communication required. Each of these network structures meets different requirements concerning time for connection setup, throughput, availability, accessibility, quality of transmission etc. Any of these networks causes its own high costs for providing, administration and maintenance. Another fact is that possibilities which result from the integration of data and voice communication as well as from additional functions like video conferencing, cannot be used. Internet telephony allows companies, institutions and individuals to reduce their telecommunication costs considerably and at the same time to improve their communication possibilities. Internet telephony combines voice, video and data traffic by setting IP as a common protocol and joining together up to three different network structures.

This way network administration is considerably simplified and maintenance costs are reduced. The additional possibilities which are resulting from the extended communication abilities will raise efficiency and productivity.

Extension to ITK NetBlazer 8500

In the first place you will find in this preface a description of the „classical" Remote Access System ITK NetBlazer 8100. The extension of ITK NetBlazer 8100 to a powerful voice over IP gateway (ITK NetBlazer 8500) is described immediately behind. ITK NetBlazer 8500 therefore combines Remote Access via PPP with the ability to act as a gateway between IP and the telephone networks (PSTN/ISDN). In the sequel ITK NetBlazer 8500 with its data and voice communication capabilities is described in this manual.

ITK NetBlazer 8100

The constant growth in demand for information is a significant challenge for providers of corporate networks and online services as well as for carriers and multiprovider networks. The access system holds a key position for the flow of information from the provider to the end user. It must support the access processes used with their numerous different protocols. The access system must also accommodate future challenges; be flexible and scalable regarding to standards; and be future proven with regard to new technologies and application platforms.

ITK answers these challenges with ITK NetBlazer 8100 - the open solution for ISDN network access.

ITK NetBlazer 8100 uses ITK's proven second generation ISDN boards, multichannel digital modem, MVIP adapter technology and open system platform software to implement a range of products for present and future key system platforms. In addition to the system platform, ITK's strategy covers backbone connectivity, authentication, accounting and application servers.

ITK NetBlazer 8100 solution

How does ITK NetBlazer 8100 meet the key criteria and what are the benefits of a product range based on open standards?

Flexibility

For the connection with ITK NetBlazer 8100, it doesn't matter whether a remote access application is based on one or more servers (security/ authentication server, accounting server, application server).

Remote connections may be established via modems, cellular mobile clients, terminal adapter or ISDN controller. Backbone network connection may be established via Ethernet, Token Ring, FDDI, Frame Relay, X.25 or ATM. Furthermore, with up to 120/96 ports in only one system, ITK NetBlazer 8100 offers state-of-the-art flexibility. There are no fixed configuration restrictions or predetermined slot allocations.

ITK NetBlazer 8100 implements standard packet handling and routing procedures along with tunneling for use in complex multiproviding networks. With its support for L2F tunneling (Ciscos layer 2 forwarding), the optimized ITK NetBlazer 8100 integrates especially well into Cisco-based backbone networks.

L2F Tunneling

ITK NetBlazer 8100 is capable of handling the Layer 2 Forwarding Protocol (L2F). This protocol is a special tunneling protocol, which encapsulates PPP packets in L2F and sends these packets to a node in the net which is capable of unpacking and handling the raw PPP data. With this feature it is possible to build virtual private networks within the Internet or any carrier network.

ITK NetBlazer 8100 supports up to 120 L2F channels and therefore it is possible to drive all the physical connections with L2F.

This new feature fits very easily into environments with existing routers because it is capable of acting as a tunnel begin.

Security

The unique, flexible authentication of ITK NetBlazer 8100 allows the realization of different hierarchically organized security levels. ITK NetBlazer 8100 is your solution for a simple Intranet access as well as for complex multivendor networks via RADIUS and ADNS (ITK NetBlazer 8100 ***A**uthentication **D**omain **N**ame **S**ervice*).

ITK NetBlazer 8100 supports standardized and approved security procedures and protocols such as PAP, CHAP and RADIUS. ITK NetBlazer 8500 allows access to the ISDN number, the subscriber number and additional signaling information for the verification, identification and classification of the user.

Additionally, ITK NetBlazer 8100 offers its *Dynamic Allocation Packet Filter* providing extensive possibilities for the allocation of user or provider specific access rights.

Scaleability

ITK NetBlazer 8100 can be configured in a combination of digital and analog channels for parallel communication, including cellular mobile clients with V.110/V.120 on every channel. ISDN PRI,E1,T1 interfaces and/or digital modems can be added if necessary. ITK NetBlazer 8100 supports up to 120/96 digital and analog ports in a single system. If the channel number of one POP (Point of Presence) is greater than the maximum number of channels in a single ITK NetBlazer 8100, several systems can be cascaded. ITK NetBlazer 8100 offers the best appropriate configuration for each demand.

Future proofing

In cooperation with Cisco and others, ITK ensures that ITK NetBlazer 8100 will be up-to-date with support of new versions and enhancements. Through these partnerships, the interoperability for present and future protocols and processes will be guaranteed. The open approach to backbone connectivity means that new technologies can be supported as they become commercially available.

Special ITK NetBlazer 8100 features

Beside the features of usual access systems, ITK NetBlazer 8100 provides many special features which are very important - especially for inherent service providers, large enterprises and carriers. Some of these are the optimized data throughput, *short hold*, distributed Line Management and the flexible authentication in multi-provider networks.

Data throughput

With online connections on all 120 ports, ITK NetBlazer 8100 ensures complete data throughput of 64 Kbps on every channel without reduction.

Short Hold

Access via dial in networks results in several disadvantages for carriers and service providers as well as for the connected clients. To provide a highly available service, the carrier and service provider has to assign the port number of his PoP according to the maximum number of parallel sessions. This causes high initial costs and forces network congestion. The time dependent cycle of a dial-up connection to the PoP is a significant cost factor. The costs are proportional to the session period regardless of whether data is transferred or not. One single port in the central site access system is busy for the period of the logical session. ITK NetBlazer 8100 removes this disadvantage with its Short Hold and distributed Line Management features.

Short Hold ensures that a dial-up connection is established only during the period of data transmission. An established dial-up connection between Client and PoP is automatically taken down (Short Hold) if no data is transferred in a certain time interval. As soon as data is queued for transmission, the connection will be automatically established within 1-2 seconds. Short Hold does not influence logical network connections – the logical connection is up during the complete session.

Short Hold normally requires static IP addresses. In the past carrier and Internet service providers could not set up shorthold. ITK NetBlazer 8100 enables carrier and service providers to use the advantages of Short Hold even with dynamic IP addresses. The same IP address is allocated to the client for the connection after Short Hold. An assigned dynamic IP address is not released at the end of the session, but is still reserved for the client. When establishing a new dial-up connection, the original IP address is assigned to this client again. Shorthold allows the provider to service an estimated 10 times the current client base on the same number of physical lines.

Distributed Line Management

If only a single access system is used at one location, Short Hold is possible without limitations. All logical network connections and physical access ports are controlled by only one system. The allocation of dial-up connections to existing logical network connections can be carried out internally by the access system.

The number of ports a single access system can offer may not be sufficient for a carrier or service provider. For these requirements as well as for redundancy aspects, several independent access systems will be installed. All ports of all access systems are combined in a hunting group and can be reached via one single dial-in number. This normally results in a problem for Short Hold, because it cannot guarantee that a client reaches the same physical access system after Short Hold. ITK NetBlazer 8100 solves this problem with the distributed Line Management feature.

Extended Short Hold uses a special ITK NetBlazer 8100 tunneling protocol for communication between multiple access systems. For every new session ITK NetBlazer 8100 is assigned as a home router for this session. A home router manages the logical network connections for a session. When a client reactivates a Short Hold connection, the responsible ITK NetBlazer 8100 home router for this session is assigned during authentication procedure and a tunneling connection between ITK NetBlazer 8100 access system and ITK NetBlazer 8100 home router is established. This ensures that all physical and logical network connections of this session coincide on one ITK NetBlazer 8100.

Moreover, one ITK NetBlazer 8100 connected to a backbone can use any channel of another ITK NetBlazer 8100 in order to dial out.

Multiproviding

Multiproviding means the availability of several different services and service providers over one single access network. ITK NetBlazer 8100 is best suited for operation in such complex environments and offers the flexible authentication concept. This concept is based on ADNS and RADIUS and provides several steps of authentication. This proven concept considers the different responsibilities and security domains in complex multiproviding networks. The flexible authentication of ITK NetBlazer 8100 allows the adjustment of the access rights for the independent network resources by the responsible sections. By network resources such as for example several ISPs (Internet Service Provider), different departments in a company-wide net or single data services are meant.

ADNS runs on a central site server. This server knows all accessible services and service providers in the multiprovider network and is responsible for the initial service selection. If a call comes to one of the distributed access systems ITK NetBlazer 8100 asks ADNS for a routing path to the

required service or service provider. Therefore the addresses of the different services and service provider are managed by the ADNS data base and assigned to several selection criteria. If a client establishes a connection ITK NetBlazer 8100 forwards the available ISDN signaling information (dial-up number, address extension, digital or analog call, etc.) via RADIUS to the ADNS. The address extension can be used as selection criteria for the responsible service or service provider. Without any further action by the user a selection can be made before the connection to the client is established.

The following authentication of the subscriber is done independently by the responsible service or service provider.

Enhanced Logging

This is a dynamic logging facility allowing enabling and disabling of data and message logging while the processes (connections) are still active.

Callout

ITK NetBlazer 8100 establishes a connection to a customer. This offers certain definable clients the possibility of sending data to a destination computer which is absent. The charging applies at ITK NetBlazer 8100 site.

Distributed Callout

Distributed Callout offers the Callout feature. Additionally, one ITK NetBlazer 8100 connected to a backbone can use any port of another ITK NetBlazer 8100 in the same backbone in order to dial out.

Recall

This feature causes ITK NetBlazer 8100 to dial to a user just to *awake* his client software which must reject the call and should call back to the ITK NetBlazer 8100. The charging applies at user site.

Callback

Callback is the ideal solution for companies which want to supply their homeworkers with online access to the firm’s system.

All costs must be paid by the provider (company).

The client therefore dials ITK NetBlazer 8100. ITK NetBlazer 8100 rejects the call and calls back.

Distributed Multilink

With the PPP Multilink Protocol you can bundle multiple channels in order to increase the bandwidth. ITK NetBlazer 8100 allows the bundling of ISDN and modem links independent of which ITK NetBlazer 8100 the links arrive at.

All new incoming links of the same user are tunneled via SPC (**S**uprimo (ITK NetBlazer 8100) **P**rocess **C**ommunication) from the incoming ITK NetBlazer 8100 to the Home Gateway ITK NetBlazer 8100. There the EMAS process for this user accepts the new links and keeps a list of all active links.

Distributed Home Serving

For distributed Line Management and distributed Multilink, incoming calls are tunneled to the home server ITK NetBlazer 8100. Distributed home serving means: a corresponding home server is searched dynamically when a new call arrives.

If the user is known at the local ITK NetBlazer 8100, the call is processed locally (the local ITK NetBlazer 8100 is the home server).

If the user is not known at the local ITK NetBlazer 8100, all configured partner ITK NetBlazer 8100s are asked about the user. If one ITK NetBlazer 8100 knows the user, this one is used as the home server and the call is tunneled to this ITK NetBlazer 8100. If no ITK NetBlazer 8100 knows the user, the call is processed locally as above.

webMan

For easy monitoring and configuring ITK NetBlazer 8100 you can use webMan. This is a Web Management tool based on the WWW technology. Just use a web browser that supports html frames (for example: Microsoft Internet Explorer 3.x or Netscape Navigator 3.x). webMan shows you the current connections, the status of each B channel, statistic and logging data, accounting files and userlist. You also can show and edit the configuration files easily without using Unix editors. Furthermore, you have direct access to the online ITK NetBlazer 8100 manual.

ITK NetBlazer 8500

Voice over IP offers the key to overcoming the double infrastructure. It considerably facilitates network administration, and maintenance costs are dramatically reduced.

To begin with, Voice over IP was considered a fringe technology, but now the carriers are worried about drastic drops in long-distance calls which are their main source of income. Therefore, each carrier has conducted a research study on the potential threat of Internet technology. What are the reasons for the increasingly widespread acceptance of this novel technology for Internet service providers and carriers, as well as for companies of all sizes?

Voice over IP scenarios

Thanks to Voice over IP, Internet service providers and newly emerging carriers in Europe are now able to offer their customers voice services building on the existing infrastructure. This means that they are becoming serious competitors for the established carriers and monopoly companies in this area – and sooner than expected.

Voice over IP offers companies that are already operating TCP/IP networks considerable cost savings, as phone calls can be switched for the major part of the route via the IP data network. Based on their existing intranets, companies can implement voice services easily, and gradually migrate to the use of IP-based networks only. Support for video conferences and shared data applications offers added value while using the same infrastructure.

Another reason why more companies are becoming interested in Voice over IP are the increasing corporate bandwidth demands. Fast Ethernet and switching are now common technologies in most networks. With ATM and Gigabit Ethernet, two far more powerful successors are already in sight. This wide availability of bandwidth – particularly in local networks – forms the basis for new applications such as Voice over IP or video conferencing.

In addition, the innovative and fast developing PC industry is putting much effort into designing new applications such as PC-based PBXs, Web-based telephony support, network video conferencing solutions and customized call centre applications. They are competing with the manufacturers of proprietary PBXs, who to date have failed to successfully integrate PCs with their range of possibilities into the telecommunications infrastructure.

ITK NetBlazer 8500

The ITK NetBlazer 8500 is the ideal combination of a field-proven remote access server and a powerful voice over IP gateway, allowing the two hitherto separate worlds of tele-communications and information technology to unite.

As a remote access server, the ITK NetBlazer 8500 builds on the tried and tested, and globally used technology of the ITK NetBlazer 8100. All features supported by the ITK NetBlazer 8100 were included in the ITK NetBlazer 8500 from the outset.

In addition, the ITK NetBlazer 8500 offers the full functionality of a Voice over IP gateway. The Voice over IP gateway plays a central role in this innovative technology; it handles the conversion of voice data into TCP/IP packets and vice versa. This enables communications solutions such as phone-to-computer and phone-to-phone connections with the 700 million telephone terminals in use worldwide.

Voice Quality

The integrated high-performance MVIP switching architecture – which connects the primary rate card with the DSP-based voice compression card – ensures unlimited high performance and a stable voice quality, which is crucial when using a voice over IP gateway. Further enhancement of the voice quality is provided by integrated echo suppression and speech pause compensation.

Network management

The management mechanisms of the ITK NetBlazer 8500 are versatile. From easy and fast usable command line interfaces over SNMP up to WorldWideWeb-based management, everything is included that is needed for efficient and,even from the distance possible, system network management.

Cost advantages

With ITK NetBlazer 8500 you obtain an enormous potential of costs saving. The system enables intelligent Least Cost Routing. This way telephone calls are forwarded, depending from the dialed number, over the IP network to the local area of the desired subscriber. Consequently, charges are only caused for the switching to the public network if they are not dropped anyway, as some carriers are already doing. Many market research institutes which are engaged with the subject voice over IP, see a much bigger cost advantage in the integration of data and voice communication. Besides the unification of the network infrastructure, there is an enormous improvement of productivity, caused by 'multimedial' communication possibilities like shared applications with simultaneous voice or video connections.

Scaleability

The ITK NetBlazer 8500 can be scaled from 30 ports right up to 120 ports for every system. These ports support both dial-in from remote access clients via ISDN, Modem and GSM, as well as voice communication using conventional analog and digital telephones. If more than 120 ports are needed for one POP, or if failure-proofness is to be increased by redundancy, several systems can be cascaded to form one POP of any required size.

Standards

In addition, the ITK NetBlazer 8500 supports standards widely used in this field, such as H.323, G.723.1, G.729A and H.245. This ensures interoperability with products from other manufacturers. Integration into the existing backbone networks and connection to authentication, accounting and application servers is achieved using the widespread RADIUS standard.

1 Getting started

1.1 How this manual is organized

Advantages of ITK NetBlazer 8500 (Preface) provides an overview of the scope of the product.

Chapter 1 gives information about this manual and describes how to put ITK NetBlazer 8500 into operation.

Chapter 2 is a brief introduction to the operating system: Unix.

Chapter 3 informs about voice over IP.

Chapter 4 shows the possibilities for testing whether ITK NetBlazer 8500 is running correctly while being connected to the network.

Chapter 5 explains the PRAMON program, which is a user interface to work with ITK NetBlazer 8500 hard- and software.

Chapter 6 describes the *practrl* process.

Chapter 7 describes how to configure ITK NetBlazer 8500 software for special needs.

Chapter 8 deals with the hard- and software installation regarding hard- and software updates.

Appendix A deals with the technical data, troubleshooting and examples of the configuration files.

Appendix B describes what's new in ITK NetBlazer 8500 Version 5.00.

Appendix C describes briefly how to update to ITK NetBlazer 8500 Version 5.00.

Appendix D describes the *ix1.ini* file.

Appendix E contains a checklist to verify the steps during the installation of ITK NetBlazer 8500 soft- and hardware.

Appendix F informs about the Year 2000 compatibility.

The exhaustive Index allows you to find your way around quickly in the manual so you can answer questions that may occur during installation or operation.

1.2 How to use this manual

ITK NetBlazer 8500 is based on the „classical“ Remote Access via PPP (ITK NetBlazer 8100) and combines this functionality with the ability to act as a gateway between IP and the telephone networks (PSTN/ISDN). To distinguish between these 2 main functions where it is necessary the expressions ITK NetBlazer 8500 „data“ and ITK NetBlazer 8500 „data and voice“ are used.
Note that this manual describes features and functionality of ITK NetBlazer 8500 (data and voice).

The intent of this manual is to offer the user the possibility of a really quick start. To get the system to simply run, read Chapter 1.3, *Putting into operation* (page 1-4).

To go into detail and configure ITK NetBlazer 8500 for special needs which may change from time to time, read the following chapters:

Chapter 2, *Unix introduction* (page 2-1)

Chapter 4, *Testing ITK NetBlazer 8500* (page 4-1)

Chapter 5, *Pramon* (page 5-1)

Chapter 6, *PRACTRL* (page 6-1)

Chapter 7, *Individual software configuration* (page 7-1).

Note that the system you have bought from ITK is already preconfigured for your special software and hardware requirements.

Chapter 7, *Individual software configuration* (page 7-1) is of interest only in case of buying some new hardware which has to be plugged into ITK NetBlazer 8500 or to update the systems software.

Note that you will be informed by ITK if new software is available. To add new hardware to your system, you should contact your local distributor or ask ITK.

To facilitate its use the following features are employed consistently throughout the manual.

Header

The header on each page also contains the page numbers (“1-2” for example means: Chapter 1, page 2). On each page you will find the current chapter and section number and the *title of the current chapter* to guide you when you want to leaf through the manual. On the left of each page you will find the version number of the product.

Note

The gray background indicates an important point that you should not skip over!
You will also find Unix commands and entries in configuration and parameter files with gray background.

Special Note

Particularly important information that, if ignored, could easily lead to problems is also indicated by an exclamation mark symbol:

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

Bold or Italic Print

Bold or *italic* print is used in this manual to **highlight information** or *emphasize* it. In *italic* print you will also find directory names, file names and parameters.

Expressions in angle brackets <>

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

General Operating Steps

Operating steps are presented as follows:

(1) Turn on your PC.

(2) [next operating step]

(3) [... additional operating steps]

1.3 Putting into operation

Please check that the power select switch is adjusted correctly (110V/ 220V).

The pin assignment of the ISDN PRI connector is not standardized so compare yours with that of ITK NetBlazer 8500. See Appendix A.1, *Product highlights / Technical data* (page A-1).

Never touch any of the contact pins of the **interfaces** (e.g. serial ports, parallel ports, Ethernet port, ISDN connection) **without grounding** yourself!
The electronic components can be **damaged** by **static discharge**!

Make sure that the debug cable is connected to one ITK Primary (no specific board) and to the Com2 port. Connect the power supply cable and the network cable.

To test whether ITK NetBlazer 8500 is running correctly, also connect a VGA monitor and a keyboard (same for hardware configuration). For more detailed information see Chapter 4, *Testing ITK NetBlazer 8500* (page 4-1).

Turn on the main switch at the front and the system will run.

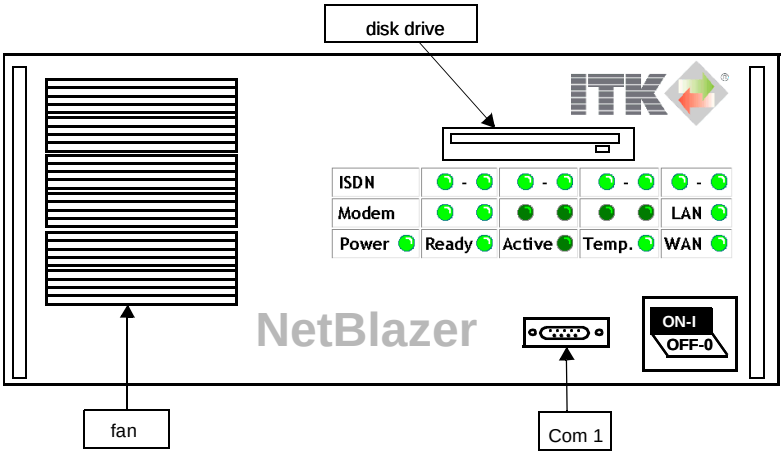


Fig. 1-1: Front panel of ITK NetBlazer 8500

The LEDs show the status of ITK NetBlazer 8500 and may be of interest for an operator or service technician.

The ITK NetBlazer 8500 software switches the LEDs automatically if the software is running. These LEDs can be green, orange or black (off).

For their meanings see Chapter 6.2, *LED status signaling (PCI)* (page 6-4)

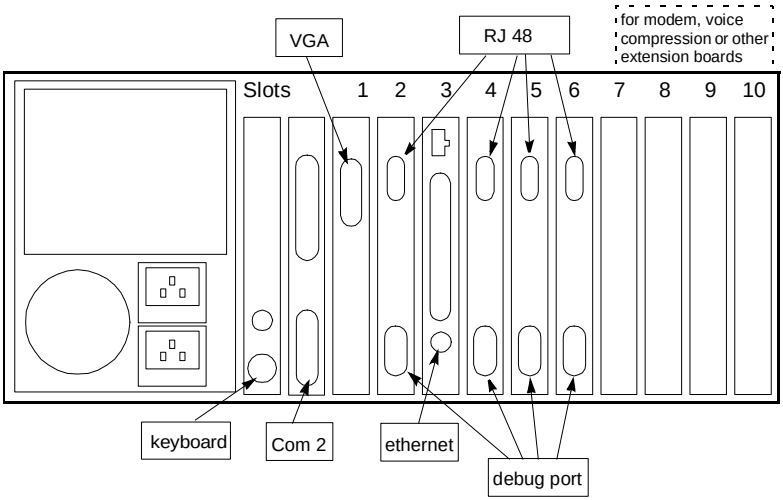


Fig. 1-2: Rear pannel of ITK NetBlazer 8500 PCI

2 Unix introduction

ITK NetBlazer 8500 is running under a Unix Operating System. Basic knowledge about Unix is necessary to manage and configure the system. This chapter is a short description of the most important tools.

2.1 Logging in, logging out

If the System is started a login screen appears. Please enter the user name and the password. The preconfigured users for ITK NetBlazer 8500 are:

username **pra**, password **pra**

and

username **root** password **itk**

pra is the standard user of the system. This user can do most things. The superuser **root** is only needed for special operations (for example changing the IP address).

To switch between up to four sessions (for example to log in as **pra** and **root**) use the Alt+F1 to Alt+F4 keys.

To log out from the system simply type:

```
exit
```

in the command line.

2.2 vi

To configure the ITK NetBlazer 8500 software it is necessary to use the standard Unix editor vi. The basic handling of vi is described in this chapter.

2.2.1 Introduction

Vi is a text editor based on the standard Unix editor called Ex. It is available on all Unix systems and versions. Instructions on how to change the text and modes are given below.

The way to learn about vi is not simply by reading a book or a manual. It is recommend that you read this document while sitting in front of a terminal using vi.

This section describes some of the basic concepts of vi.

For more detailed information about Unix and vi look at the SCO manuals included in the package.

2.2.2 Modes

Vi operates in a number of modes. The two main modes are command mode and input mode. Normally the way to insert text into a file is to switch vi into input mode. To issue commands vi must be switched back to command mode.

To summarize:

- in command mode any key is treated as a command
- in input mode any text typed is added to the file

When in doubt about whether vi is in command mode or input mode, press the <Esc> key. This activates the command mode.

2.2.3 The buffer

While editing a file vi does not work on the original file but on a copy. This temporary copy is called the buffer. When all changes are made the buffer must be saved to the original file otherwise all changes will be lost. If typing a lot of text or carrying out many changes the buffer should be saved at regular intervals (every 10 to 15 minutes).

2.2.4 The cursor

The cursor is the marker on the screen that indicates the current position in the buffer. It is quite often a square and sometimes an underscore. On some terminals it flashes. The cursor can be moved around the screen using the cursor keys and various other commands which will be described later.

2.2.5 Starting work with vi

To begin editing a file start vi by typing:

```
vi myfile
```

myfile is the name of the file being edited. If the file does not exist, vi creates it and saves it to the buffer. If the file already exists vi opens it and reads the contents into the buffer. When there are very few lines in the file (less than a screen) vi indicates empty lines beyond the end of the buffer with tildes (~) at the beginning of each line.

At this stage vi is in command mode.

To switch vi to input mode and insert some text, type **i**. Any text entered after this point is inserted into the file.

To switch back to command mode press <Esc>. In command mode any key is treated as a command.

2.2.6 Displaying the mode

Usually on Unix systems an input mode indicator can be displayed in the lower right corner of the screen. Make sure that the system is in command mode (by pressing Esc). Then type:

```
:set showmode
```

and press <Enter>. If an error message occurs this option is not available. Otherwise for the rest of the vi session whenever input mode is selected a message is displayed.

To set *showmode* every time using vi, create a file with the extension *.exrc* in the home directory containing the command:

```
set showmode
```

2.2.7 **Moving around** (use insert mode)

← ↑ → ↓	move gradually
ctrl-D	scrolls half page down
ctrl-F	scrolls one page down
ctrl-U	scrolls half page up
ctrl-B	scrolls one page up

2.2.8 **Altering text** (use command mode)

Capital Letters and small letters have **different** functions

S	deletes the line
x	deletes the character at the cursor position
u	undoes the last change
U	undoes the last changes in the whole topical line / repeats changes

2.2.9 Cutting / inserting text (use insert mode)

Capital Letters and small letters have **different** functions.

yw	puts the word into the buffer
yy	puts topical line into the buffer
ayy	puts topical line into the buffer *a* (possible with all letters)
dw	deletes the word into the buffer
dd	deletes topical line into the buffer
p	inserts text from the buffer after cursor position
ap	inserts text from the buffer *a*

2.2.10 Searching text (use insert mode)

/string	searches *string*
n	continues searching
N	continues searching in reverse order

2.2.11 Saving and leaving

:w [file]	writes the buffer to file; [file] is optional
:wq	writes the buffer to file and quits vi
:q!	quits vi without saving
:e!	undoes all changes since last saving/writing

2.3 Files and directories

Programs and data are stored in files. Each file has a name which can contain almost any character. The names can have a maximum length of 255 characters.

Files are organized with directories. Each directory acts as a container for files or directories usually known as subdirectories.

Directory names are in the same format as file names. The "/" character is used to separate the file part of a name from the directory part, for example fortran/prog.f identifies the file prog.f in the fortran directory.

Each user has a home directory for his or her files.

File names can be given relative to the current working directory, for example mydir/myfile are relative to the root directory (/) for example /home/sufs1/ru5/sw/swxxxxx/mydir/myfile

2.3.1 File management

The following commands are useful for working with files:

```
ls
```

Lists files (for more detailed information see below)

```
rm file
```

Erases file *file*

```
cp file1 file2
```

Copies *file1* to *file2*

```
cp file1 file2 dir
```

Copies files *file1* and *file2* into directory *dir*

```
mv file1 file2
```

Renames *file1* to *file2*

```
mv file dir
```

Moves *file* into directory *dir*

```
cat file1 file2
```

Lists contents of *file1* and *file2*

```
more file
```

Lists *file*, one page at a time, continue with space

```
compress file
```

Creates compressed *file.Z* from *file*

```
uncompress file.Z
```

Uncompresses *file* from *file.Z*

2.3.2 The ls command

The *ls* command is used to examine files and directories. Type *ls* followed by various options (starting with "-") and a list of files and directories appears.

- The -a option shows *all* files including the hidden ones.
- The -l option shows details for each file, especially owner, size and permissions. (same function with the alias command *l*).
- The -R option shows the contents of all subdirectory.

2.3.3 Special files

Each file beginning with a dot in its name is invisible. Such files usually contain the commands necessary to start a particular program and normally reside in a user's home directory for example

```
.profile
```

shell commands executed by the first log in

```
.logout
```

shell commands executed during exit

2.3.4 File and directory attributes

Unix recognizes three types of users when accessing files and directories.

- The files owner or user (u)
- Users in the same group as the owner (g)
- All other users (o)

Each type of user can have:

- Read permission (r)
- Write permission (w)
- Execute permission (x)

allowing to read from a file, write to a file or execute a program.

The execute permission of a directory allows the user to access but not to list the included files. To list the files, the read permission is required. While working with directories it is advisable to set read and execute permissions.

The following example may clarify it:

```
berlin:/u/pra>ls -l
total 7246
drwxrwxrwx 2 pra group  48    Okt 18 10:34 bin
drwxrwx--- 1 pra group  59619 Okt 18 10:34 dat
drwxrwx--- 1 pra group  59619 Okt 18 10:34 exe
drwxrwx--- 1 pra group  59619 Okt 18 10:34 log
-rwxrwx--- 1 pra group  59619 Okt 18 10:34 foo
berlin:/u/pra>
```

Note that the permissions are printed at the beginning of each line in a block of 10 characters if the long listing option is used.

If the first character of this block is a hyphen: "-" like in the last line of the listing, *foo* is an ordinary file; *d* means it is a directory. The other nine characters are arranged in blocks of three with each block showing a particular class of users, each with read (r), write (w) or execute (x) permission. The first of these blocks represents the permissions for the user, the second for the members of a group and the third for everyone else.

The chmod command changes permissions, for example:

```
chmod g+rx file
```

allows read and execute privilege to everyone in your group.

```
chmod go-rwx file
```

removes all privileges for anyone but yourself.

2.3.5 Directory management

The following commands are useful for organizing directories.

```
cd dir
```

Changes to directory *dir* relatively to the current directory. In Unix terms *dir* becomes the working directory. Files are accessed relatively to the working directory.

```
cd /dir
```

Changes to directory *dir* absolutely to root.

```
cd /
```

Changes to root

```
cd ..
```

Changes to parent directory

```
mkdir dir
```

Creates a directory called *dir.*

rmdir dir

Erases the directory called *dir*. The directory must be empty.

pwd

Print Working Directory. Shows the current path.

2.3.6 Special directories

bin, exe

Common names for directories containing executable programs.

lib

Common name for a directory containing libraries.

dat

Common name for a directory containing data files.

log

Common name for a directory containing log files.

doc

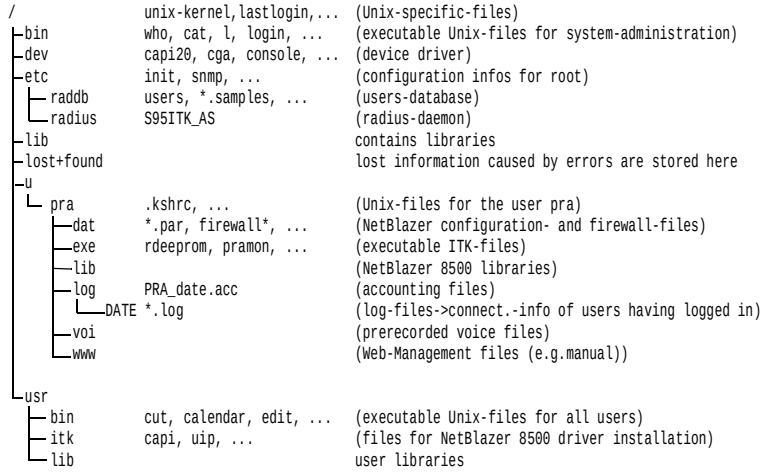
Common name for a directory containing documentation.

voi

Common name for a directory containing prerecorded voice files.

2.3.7 ITK NetBlazer 8500 directory tree

The following figure shows how the directories are organized.



2.3.8 Alias commands

Alias commands to change into the above mentioned directories:

bin=cd /u/$PROJ/bin

exe=cd u/$PROJ/exe

lib=cd /u/$PROJ/lib

dat=cd /u/$PROJ/dat

log=cd /u/$PROJ/log

logs=cd /u/$PROJ/log/`date +%y%m%d` (changes to log dir. with topical date)

voi=cd /u/$PROJ/voi

2.4 Some useful commands

Unix is bursting with commands and utilities which range from obscure to reasonably useful. Some of the more useful ones are listed below:

```
passwd
```

Changes your password.

```
telnet computer
```

Connects to another computer (insert computers name or IP).

```
uname -n
```

Prints the computer's name.

```
finger, who, w
```

Gives information about other users.

```
who am i
```

Prints out the user's name.

```
ps
```

Lists current running processes.

```
grep [-i] word file
```

Searches a file for a word or expression. The -i option means treat capital and small letters as equivalent.

2.5 The Korn Shell

The Korn Shell is a memory resistant program which makes it easier to work with Unix commands.

If a user logs in as pra the Korn Shell is active (preconfigured). If a superuser logs in as root it is not active. That should protect the superuser from making mistakes very easily by pressing certain keys which have short cut functions.

The Korn shell is initialized in the .profile and .kshrc files.

2.5.1 Using the Korn Shell

"^" means that the control key has to be pressed

The following keys and commands are available under the Korn Shell.

^P

Previous command

^N

Next command

^B

Back one character

^F

Forward one character

^A

Positions the cursor at the beginning of the line

```
^E
```

Positions the cursor at the end of the line

```
history
```

Prints command history

```
r
```

Repeats last command

```
r ls
```

Repeats last command starting with *ls*

```
^Rtext
```

Searches backwards for text

```
ESC  ESC
```

Completes a file name

```
ESC  *
```

Expands a file name matching pattern (for example f*.dat)

```
ESC-=
```

Lists possible file name completions.

The line editing is enabled for the *pra* user per default.

To start a korn shell and activate line editing for the root user enter the following command after login:

```
ksh  -o  emacs
```

3 Voice over IP introduction

Internet telephony which is also called IP Telephony or Voice over IP is a new technology that allows, among standard data packets, to transmit multimedia information like voice or video over the Internet or any other IP-based LAN or WAN.

This technology is based on open standards and recommendations which are passed by international standardization institutions like IETF or ITU and which are met by almost any supplier of Internet Telephony products. These standards define the transmission of multimedia information within IP-based networks.

This way it becomes possible to use the same network for the transmission of telephony, which is already used for the transmission of e-mail, web pages and all other packet oriented data.

3.1 Notations and technical information

Caller (user A): The user that wants to establish a call and calls the dialin gateway.

Callee (user B): The user that should be called from the caller (remote user).

Voice gateway: The system that processes the voice call and converts the voice data to IP packets.

Dial-in gateway: The (local) system where the telephone call arrives and where the voice data leaves the switched network (PSTN/ISDN) and enters the IP network.

Dial-out gateway: The (remote) system where the voice data leaves the IP network and enters the switched network (PSTN/ISDN).

Account code: Type of username, which is used to authenticate the caller. Must be numerically entered by DTMF keys.

Interactive Voice Response (IVR): A voice based menu like input system where the caller is guided to the different inputs by playback of prerecorded voicefiles. The inputs for identification and remote phone number are got by DTMF detection.

DTMF detection: The process of detecting digits pressed on a telephone touchpad. Only possible with tone dialing (not possible with pulse dialing).

2-stage-dialing: The process for the caller to call the number of the Dialin gateway 1st and to enter the wanted remote phone number in a 2nd step (guided by IVR).

Least Cost Routing (LCR): The process of finding the „best" dial-out gateway for the wished remote phone number. „Best" normally means the gateway that is nearest to the remote phone number and which causes the least costs by establishing the connection from the dial-out gateway to the callee phone (over PSTN/ISDN).

Codec: Coder/Decoder (in soft- or hardware) that converts audio or video signals in digital data (or back).

Compression (G.729A, G.723): The process of compressing the voice data in order to reduce the amount of data to be transmitted over the IP network.
The following codecs are supported:

- G.729A reduces the traffic to 8 kbit/s.
- G.723 reduces the traffic to 5.3 or 6.3 kbit/s.

Both compression protocols are NOT TRANSPARENT for data or fax. Only voice is compressed and decompressed with acceptable quality. (Data and fax is not.)

- G.711 is the uncompressed protocol and needs a bandwidth of 56 or 64 kbit/s.

Latency (Delay): The amound of time a multimedia packet takes to get from the source to the destination. The time is needed to compress the voice, packetizing it into IP packets, transferring the IP packet over the Intranet/Internet and to decompress the packet (time to transfer voice from caller to callee (or back)). The latency must be minimized in order to maintain a certain level of interactivity and avoid unnatural pauses in conversation. For a good quality the delay should be below 250 ms.

Jitter: (interarrival jitter): Real-time multimedia packets must arrive in order and on time to be of any use to the receiver. Variations in packet arrival time (jitter) must be below a certain threshold to avoid dropped packets (and therefore gaps in the call). The NetBlazer 8500 software keeps track of this problem by using an intelligent automatically adapted dynamic jitter buffer.

Echo Cancellation: To disable the audible echo caused by the delay of packet an echo cancellation process is necessary. This process reduces the input signal on one end by the output signal of the same end. The echo cancellation must be done on both sides.

DSP board: To fulfill the compression and echo cancellation requirements special computing power is necessary. In the NetBlazer 8500 a special hardware equipment with DSP (digital signal processors) is used. These DSP boards are connected to the MVIP bus and contain multiple DSP's. Each DSP processes one or more voice channels.
See Chapter 8.2.4, *Voice compression board* (page 8-6) for information about voice compression boards.

SPC Tunneling Protocol: The SPC protocol (Suprimo (ITK NetBlazer 8500) Process Communication) is a ITK NetBlazer 8500 proprietary protocol to exchange messages between multiple ITK NetBlazer 8500 processes. SPC is based on UDP. Therefore it has less communication overhead than for example L2F and is also useable between multiple systems (on the same network). SPC is used for example for tunneling (EMAS) the user data to the right process.

H.323 is an "umbrella recommendation" of the ITU which defines the multimedia communication in LANs that do not provide a guaranteed quality of service.
H.323 protocol uses TCP connections for the signaling protocol (H.245), for data transmission (T.120) and for connection control (Q.931).
H.323 uses RTP (Realtime Transport Protocol) for transmission of audio and video data, which is based on UDP (unprotected). Using intermediate buffers, time stamps and sequence numbers, RTP enables the receiving station to detect missing packets, double packets or packets which have been received in wrong order, and to correct the receiving flow in a suitable way.

Gatekeeper is a system in the H.323 network that is responsible for address translation (E.165 <=> IP address) and control of all network resources.

RAS: Registration, Admission, Status is the protocol in H.323 that defines the communication with the gatekeeper.

3.2 Voice over IP with H.323

The H.323 protocol is needed to establish voice connections from PC to PC, PC to phone, phone to PC and phone to phone when different gateways are involved. It allows the interoperability of systems from different vendors. The NetBlazer implementation in V5.00 is H.323V1 with some V2 enhancements.

The NetBlazer specific connection setup protocol SPC, that was introduced in V4.00, is still supported. Both protocols (SPC and H.323) can be selected dynamically on connection setup (See chapter 7.7.6, *Connection Setup* (page 7-76)).

A H.323 daemon (h323d) is used to realize call establishment by the ITU standard H.323 for Voice over IP.

The h323d is started and controlled by PRACTRL. If h323d uses a gatekeeper it registeres itself at the gatekeeper.

In the process table of PRAMON/webMan you can see the IP address of this gatekeeper (GK) or 'No GK' if no gatekeeper is used. Furthermore the number of sessions is shown (#s). For details see chapter 5.4, *Process Monitor* (page 5-10).

The parameters for the h323d are configured in h323.par (see chapter 7.7.3, *Configuring Voice over IP with H.323* (page 7-68)).

3.2.1 Country code substitution

This parameter is used to support an international dial number layout used by other vendors (e.g. Cisco). You can specify a country code and the substitution digits for your system. If the country code digits are found in the calling number they are exchanged by the substitution specified.

3.2.2 Prefix parameters

These parameters may be used if a gatekeeper needs to reference different gateways by calling number prefix. The gatekeeper forwards the calling number according this prefix. Thus the prefix must be cut off by the h323d. If the h323d gets a calling number, it will be checked if one of the configured prefixes is used. This prefix will be cut off and the calling number without prefix is used to establish the call. For external calls the 'PBXExternCallPrefix' is called first.

3.2.3 Call handling parameters

The h323d supports two different ways of connection establishment.

1. Offer own H.245 IP address and port in the first SETUP message to open H.245 channel with first round trip.
2. Wait for CONNECT message from remote phone before opening H.245 channel. (parameter only supported after V5.00b2)

3.2.4 Supported H.323 Clients

The following H.323 clients have been successfully tested with NetBlazer V5.00:

- Microsoft NetMeeting V2.0 / V2.1
- Intel ProShare V3.0 and Internet Video Phone 2.1 / 2.2
- Netspeak Webphone 4.0 / 4.01
- Vocaltec Internet Phone 5.0
- Netscape Conference 4.0
- VoxWare VoxPhone 3.0

3.3 Transparent Connection Setup

3.3.1 Voice dialog

The voice dialog defines how a user authenticates and enteres his destination phone number. The previous versions only supported Interactive Voice Response (IVR). V5.0 additionally supports One Stage dialing (OSD).

Interactive Voice Response (IVR)

IVR (or **V**oice **G**uided **I**nput VGI) is a 2-stage-dialing process: In the first step the user dials the number of the voice gateway and hears the welcome voice messages. In the second step the user enters his PIN and the destination number by DTMF digits.

During the IVR the following steps are necessary:

- Authentication of the caller (by account code, which is entered by DTMF digits)
- Recognition of the remote phone number (entered by DTMF digits)
- Determination of the dial-out gateway (by Least Cost Routing)
- Establishment of the connection
- Allowing multiple calls after authentication

The complete IVR is based on a menu like dialog which plays prerecorded voicefiles to guide the user and to get user inputs by DTMF digits entered on the caller phone-keypad (Only digits 0-9 and keys '*' and '#', tone dialing needed). In detail the IVR works as follows (most steps are configurable by parameters in the flexible authentication):

1. Playback „Welcome Message"
2. If Calling line ID is known (offline authentication): goto step 6
3. Playback „Prompt for account code"
4. Input account code (terminated by '#', by configured length or by timeout)
5. Check account code (online authentication): Not ok => Playback „Invalid Account" and goto step 4
6. Playback „Prompt for destination number"
7. Input destination number (terminated by '#' or by timeout)
8. Send least cost routing request to LCR server
9. Get answer from LCR server: Not ok => Playback voice message and goto step 7
10. Playback „Calling" tone
11. Connection setup to dial-out gateway: Errors => Playback voice mes-

sage and goto step 7

12. Compressing voice data during phone connection
13. After hangup of callee or callee is busy: go to step 6 (to allow further calls)

It is not necessary to wait for the completion of voice messages, they can be aborted by pressing a DTMF key. So a quick 2 stage dialing is possible (especially if the caller is authenticated by his calling line id and does not need to enter his account code).

During the IVR the input can be deleted by pressing the '*' key. The connection setup can be canceled with the '*' too.

All inputs in the IVR can be terminated by pressing the '#' key. The inputs are automatically terminated when no key is pressed during the timeout time (see parameter "vgi_timeout", default: 8 seconds).

After the termination of one call another call can be established. While hearing the busy signal (after the callee hung up or when the callee is busy) the '*' key can be pressed to delete the dialed number. Then the new called number can be entered.

The same procedure can be used to terminate a call that is not yet established (i.e. the callee is not reachable).

The entered account code is split into the username and the PIN: The last N digits of the account code are split off and are used as the PIN, the rest of the account code is used as the username. The username and the PIN (password) are used for online authentication.
(The length of the account code and of the PIN are configurable as NetBlazer parameters. See Chapter 7.3.11, *voip.par* (page 7-15))

The VoIP feature as well as the IVR is configurable by the flexible authentication of NetBlazer 8500, which is based on RADIUS. The selection between modem and voice calls are based on the offline authentication (i.e. on the DDI), because the ISDN signaling can not decide between modem/fax and voice.
I.e. the voicefiles can be changed depending on the dialed DDI (**d**irect **d**ial-**i**n, or DID **d**irect **i**n-**d**ialling) to present a multilingual voice menu.

Example:

DDI 10 may be used for an IVR with German voice files

DDI 11 may be used for an IVR with English voice files

Additionally the strategy of the IVR (flow control) may be selected by RADIUS attributes. Even customer specific IVR's are possible.

This voice dialog type has been enhanced with the following features:

- **WAV files**: All voice files are standard WAV files, that can be recorded or changed on a standard PC and activated on the NetBlazer by copying the files in the right directory (see Chapter 7.7.2, *Voice files for IVR* (page 7-66)).
- **Dynamic Dialing**: Additionally to the block dialing in V4.0 dynamic dialing is useable, where the termination of the destination number is not necessary. (see below)
- **Remote tone signalling**: During connection setup the dial tones that are generated at the dialout gateway are hearable from the caller at the dialin gateway. (see below)

To enable IVR the Radius attribute "ITK-Banner" must be set to one of the following values:

- "IVR"to enable IVR with block dialing (same as "VGI" in V4.0)
- "IVR_DYNDIAL"to enable IVR with dynamic dialing

One stage dialing (OSD)

One stage dialing allows the dialing of the destination number immediate after the access number of the voice gateway. There is no separator or pause necessary between the access number and the destination number. The digits are detected from the switch and received through the d channel (no DTMF digits necessary). The incoming call is not accepted until the callee has answered the call.

No PIN is entered in One Stage Dialing. So the authentication must be done by the calling line ID of the caller, or by doing no authentication at all.

To enable OSD the Radius attribute "ITK-Banner" must be set to one of the following values:

- "OSD"to enable OSD with block dialing
- "OSD_DYNDIAL"to enable OSD with dynamic dialing

3.3.2 Get Destination number

Block dialing

Block dialing describes the process where the NetBlazer collects all digits of the destination number, without knowing when it is complete. So a termination (by '#' key or timeout) is necessary.

As soon as the destination number is complete the NetBlazer establishes the connection.

Dynamic dialing (overlapped sending)

Dynamic dialing (also called overlapped sending) allows the transmission of dial digits during the dialing phase (one digit after the other). As soon as the remote switch signals the completion of the destination number the caller is signaled the calling signal.

No termination of the destination number is necessary.

If the connection setup is done by H.323 the remote gateway (or gatekeeper) must support H.323V2, because the overlapped sended digits, are sent by H.323V2.

To achieve the support of Dynamic dialing the D-channel Setup (dial-out) is done without any destination number. The destination number is transmitted to the PABX one after the other afterwards. This empty Setup may be rejected by some PABX (D-Channel Disconnect cause: „Information element is missing").

Setting the parameter *voip_empty_setup: 0* fixes the problem, but **disables** Dynamic dialing at the same time.

3.3.3 Remote Tone signaling

Remote tone signaling is used to hear remote status tones and announcements. The data path is switched starting with the connection setup (not after connection establishment).

3.3.4 Features

The following table describes all possible features in the several VoIP dialoges:

Feature \ VoIP-Dialog	IVR	IVR_DYNDIAL	OSD	OSD_DYNDIAL
Block dialing (termination necessary)	x		x	
Dynamic dialing (no Termination)		x		x
Authentication by PIN (entered as DTMF)	x	x		
Get destination number digits by DTMF	x	x		
Get destination number by DDI (d channel)			x	x
Interpretation '*' and '#' digits	x		x	
Additional calls after first	x			
Callback	x	x		
Remote tone signalling	x	x	x	x
Playback of voice files	x	x		
Accept call before connection established	x	x		

All other features are possible with all VoIP dialoges.

3.4 Address Translation

The address translation is necessary for two reasons:

1. Find the IP address of the dialout gateway that should be used for the entered destination number
2. Modify the destination number so that it can be used to establish a connection at the dialout gateway

The NetBlazer V5.0 supports two methods to do the address translation:

1. Use Least Cost Routing (LCR) requests to a Radius server (proprietary, same as in V4.0, useable for SPC and H.323 connection setup)
2. Use RAS (Registration Admission Status) requests to a Gatekeeper (H.323 compliant, only useable with H.323 connection setup)

Both address translation methods can be combined. If a LCR Radius server as well as a Gatekeeper is configured the following cases are possible:

(dial-no defines the number the user dialed,

called-no defines the number that should be used to establish the call (result of the address translation))

- Radius LCR knows the dial-no and though responds with a called-no: No RAS request will be done. The called-no from the Radius LCR response will be used to establish the connection.
- Radius LCR does not know the dial-no and though responds no called-no: A RAS request will be done. The called-no from the Gatekeeper will be used to establish the connection.
- No Radius LCR defined (service table empty or LCR dynamically disabled): A RAS request will be done. The called-no from the Gatekeeper will be used to establish the connection.

The LCR request can be disabled dynamically per call with the setting of the “ITK-Voip-Init-String” (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

With dynamic dialing the dialout gateway must be found dynamically. With every digit of the dial-no the LCR is asked if he knows the corresponding dialout gateway. As soon as a positive response has been received the connection is established, no further LCR requests are done and all further digits of the dial-no are transferred directly to the dialout gateway.

To minimize the LCR requests a minimal amount of digits is collected before the first LCR request is done, which can be configured with the parameter “.voip_lcr_min_digits” (Default: 3).

The same behaviour is used for address translation by RAS instead of LCR.

3.5 Codecs

V5.0 supports the following codecs:

- G.729A compression ratio 8:1
- G.723.1 compresion ratio 10:1
- G.711 uncompressed, a-law and µ-law supported

The codec to use is automatically negotiated between the dialin and the dialout gateway. The codecs supported by the NetBlazer can be configured with the parameter *.type_of_codec (Default: G711:G723:G729)*

The codec to use can be forced dynamically per call with the setting of the "ITK-Voip-Init-String" (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

The framesize can be configured to 30 or 60 ms with parameter ".frame_size". (Default: 60 ms)

The following table shows the different codecs, framesizes and packet sizes supported by V5.0:

Codec	Ratio	Framesize [ms]	Payload [bytes]	IP header [bytes]	IP packet size [bytes]	IP packets per sec	IP Bytes per sec [bytes]
G.729A	8:1	30	30	40	70	33,33	2334
G.729A	8:1	60	60	40	100	16,67	1667
G.723.1	10:1	30	24	40	64	33,33	2134
G723.1	10:1	60	48	40	88	16,67	1467
G.711	1:1	30	240	40	280	33,33	9333
G.711	1:1	60	480	40	520	16,67	8669

3.6 Coding / Transcoding

The NetBlazer supports the coding a-law (used in Europe) as well as µ-law (used in USA). Each DSP card must be configured to the right coding (depending on the switch) by setting the parameter ".pcm_companding".

Possible values:

1=µ-law

2=a-law (Default)

Transcoding: If the two communication gateways have different codings (i.e. one is located in Europe and one in the US) the different codings are converted/transcoded from the NetBlazer. This is only necessary for G.711, the other codecs automatically adapt the coding.

3.7 DTMF Relay

If DTMF relay is enabled the dialin gateway detects if DTMF keys are pressed and sends these digits to the dialout gateway, where they are processed (i.e. new DTMF tones generated). Thie mechanism is an outband transfer of recognized DTMF digits as specified in H.323V2. The DTMF keys are transferred by SPC or as H.245 User Input Indications to be H.323V2 compliant.

This feature is disabled by default but can be enabled dynamically per call with the setting of the “ITK-Voip-Init-String” (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

3.8 Selecting Dialout Line

Only lines with an active D channel and that are not disabled (status “up-on”) are selected for outgoing calls.

By default all available lines (physical interface, controllers) are investigated and the line with the highest number of free ports is used for an outgoing call.

This behaviour can be changed by manually selecting a special line (Provider selection). Each physical interface (primary rate, basic rate) is managed by a so called controller. If the dialout number is preceeded by a controller number and a pipe ('|') sign then the according physical interface is used for dialout. This modified dialout number may be retrieved from a least cost routing request (or from a gatekeeper). For details see chapter 7.7.10, *Selecting Dialout Line* (page 7-79)

3.9 CLIP

The Calling Line Identification (CLI) of the phone dialing into the NetBlazer 8500 (caller) is forwarded to the dialout gateway or H.323 client during the VoIP call setup. The dialout gateway presents the CLI at the remote phone (callee), and a H.323 client shows the CLI within its user dialog.

The CLI is transfered unchanged between the dialin gateway and the remote site. No adaptions of the phone number on the incoming or outgoing site (dependent on the phone number of the line) are done.

CLIP (CLI-**P**resentation) is disabled by default and can be enabled by setting the parameter ".capi20_clip" to 1.

3.10 Connection control

For detection of aborted connection the following mechanism is used:

If no voice data (RTP packets) are received during a specified amount of time (parameter ".voip_idle_tmo", default: 300 seconds) the session is disconnected.

3.10.1 Setting Type of Service (TOS)

The IP TOS (Type Of Service) field is part of the IP packet. Some routers use the IP TOS field for a precedence selection. IP packets with a matching type of service field are preferred delivered. To achieve the best transmission results this value can be adapted to the routers precedence selection. For Details see chapter , *Setting Type of Service (TOS)* (page 7-81).

4 Testing ITK NetBlazer 8500

Testing ITK NetBlazer 8500 connected to the network

Preconfigured system is already tested!

4.1 Debug ports

If the ITK NetBlazer 8500 software is running, the ports can be tested using the process monitor *pramon*. The *Infotext* field delivers the corresponding message: D channel up/down. Compare with Chapter 5.4, *Process Monitor* (page 5-10).

alternative

Perform the following steps:

(1) Connect ITK NetBlazer 8500 to PRI connector.

(2) Login as *pra*, password *pra.*

(3) Start *pramon.*

(4) Choose *7: Display PROCESS monitor.*

(5) Check infotext for *DEBUGLOG* process to read *D channel up*.

(6) Disconnect shortly PRI cable from controller and check display.

4.2 Testing ISDN / modem access

4.2.1 Testing ISDN access

To test ISDN access, perform the following steps:

(1) Connect a Windows 95 computer with ISDN board to ISDN BRI connector.

(2) Connect manually with *dial-up network* and user *itkSuprimo.*

(3) Type the following:

```
telnet 192.168.18.254
```

(4) Login as *pra*, password *pra* and start *pramon.*

(5) Check status control process (PRACTRL).

(6) Check PPP connection with *1*.

(7) Quit *pramon* typing *q* two times.

(8) Type the following:

```
exit
```

(9) Close connection.

(10) In case of any errors occuring, check the following files:

- */u/pra/log/*.acc*

(11) Enter daily-logging directory with *logs* and check:

- *isdn_ins*.log* and *debuglog*.log* (always the latest written file)

4.2.2 Testing modem access

To test modem access, perform the following steps:

(1) Connect Windows 95 computer with serial cable to modem.

(2) Test the connection several times (1 x per modem board) as described in Chapter 4.2.1, *Testing ISDN access* (page 4-1) but check files *pstn_ins*.log* and *debuglog*.log.*

4.3 Testing voice calls

To test the voice calls from a dial-out gateway the test utility „scon“ has been enhanced to support a new option („-voice“) to do a voice call to a normal phone.

Example:

The following command establishes a voice connection to the destination number „12345“:

```
scon 12345 <CTRL> -voice
```

To test a real phone-to phone-connection a PRI line and an analog phone is needed.

- Verify the file /etc/raddb/users for following entries:

*%_10 User-Password = "DIRECT_DIAL" #**(without leading hashmark)***
Service-Type = ITK-Voice-over-IP-Comp,
ITK-Banner="VGI",
ITK-Prompt="e"

123 User-Password = "VOICE-ACCOUNT"
ITK-Username = "W. Smith"

- Call PRI-line no. + DDI no. 10 to get the Interactive Voice Response of the NetBlazer.
- Key in the PIN 123#.
- Key in a reachable dial number (e.g. an analog phone in the local telephony network)

4.4 Testing WebManager

To test the WebManager, perform the following steps:

(1) Start the web browser on a computer with LAN connection or ISDN connection to ITK NetBlazer 8500.

(2) Go to URL: <ADDRESS of ITK NetBlazer 8500>.

4.5 Testing watchdog board

To test the watchdog board, perform the following steps:

(1) Start *pramon.*

(2) Choose the following options:

- **5** : Shutdown
- Change shutdown-state ? (y/n) **y**
- **5**-Cold-Reboot (Reset)
- timeout [s] : **0** (for immediate shutdown)

(3) Wait for Memory-Test after reboot.

4.6 D channel monitor (dcm)

The „dcm“ (D channel monitor) is a tool that allows the monitoring (tracing) of D channel activity.

Usage:

```
dcm<controller-no>[ -12][ -13 | -13x][ -dump][ -text]
```

<controller-no> must be replaced by the number of the ISDN board to monitor (See Chapter 5.10, *Displaying Cardtable* (page 5-25) for getting the controller-no).

Option ’-12’ (for layer 2) shows layer 2 messages.

Option ’-13’ (for layer 3) shows layer 3messages.

Option ’-13x’ (for layer 3 extended) shows extended layer 3 messages.

Option ’-dump’ writes the raw messages as data dump in a logfile (dcm_XXXXX_data.log).

Option ’-text’ shows additional Debug messages that have been activated on the ISDN board.

Defaultoptions: ’-13’ to show only the layer 3 messages (connection setup).

4.7 param_read

The tool „param_read“ is used to show the value of a ITK NetBlazer 8500 parameter.

Usage:

```
param_read [program name] <parameter name>
```

If „program name“ is given, the tool shows the value of parameter „parameter name“ for the context of the given program.

5 Pramon

5.1 Overview

Pramon is an interactive program for managing and monitoring the ITK NetBlazer 8500 software.

5.1.1 Pramon main screen

The main screen of *pramon* is displayed in the following figure.

```
NetBlazer 8500 connection-monitor V5.00
=======================================
(Copyright: ITK AG Dortmund/Germany)

hostname of NetBlazer 8500    : hannover.itk.de
state of the PRACTRL-process  : ok(running)

  1 : Display current connections
  5 : Shutdown
  7 : Display PROCESS-Monitor
  8 : Display SERVICE-Monitor
  c : Display Counters
  h : Hardware Information
  k : Display Cardtable
  z : Change time for display-refresh
  q : Exit

  your selection: ▮
```

Fig. 5-1: Pramon main screen

The choices are the following:

Entry	Meaning
1	Displays and controls active connections, informs about a specific connection (connection no. must be known), shows buffer data of a connection (connection no. must be known).

Entry	Meaning
5	Shutdown of ITK NetBlazer 8500 software or ITK NetBlazer 8500. Shuts down, restarts or reboots the ITK NetBlazer 8500 software or the ITK NetBlazer 8500 itself.
7	Process Monitor views all running processes.
8	Service Monitor looks at defined services, modems or IP pool addresses.
c	Shows the overall transferred bytes after the last start-up.
h	Shows the hardware information.
k	Informs about the installed ISDN, modem and voice compression boards.
z	Changes refresh rate of the terminal screen in order to adapt for example a slow terminal to ITK NetBlazer 8500.
q	Exit *pramon*

5.1.2 Direct jump

To jump from one display to another without returning to the main menu do the following:

(1) Press the key for the display that should be shown.

With this direct jump a switching between the following displays is possible:

Action	Meaning
1	display current connections

Action	Meaning
7	display process table
c	display total counters
h	display hardware information
k	display Cardtable

5.1.3 Show active users

If you start *pramon* from the shell with the parameter *-u*, a table with the active user connections is shown.

Example

pramon -u

```
Username   IP-Addr         Time    Con.-Type
-------------------------------------------------
User1     194.173.10.61  0:04:26  ISDN/HDLC_TRANSPRNT
User2     194.173.10.57  0:29:32  ISDN/X75SLP
User3     194.173.10.48  0:05:21  MODEM/ 33600
SCHMITT                  0:00:06  VOICE-IN
```

After this list has been shown, *pramon* exits.

This mechanism can be used to show the active user connection with the UNIX finger tool. To show the active user connections with any finger client used on the network the file */etc/inetd.conf* must contain the line:

finger stream tcp nowait pra /u/pra/exe/pramon-wrapper pramon-wrapper

5.2 Connections

By choosing option *f* it is possible to select a filter which is used to select the type of connections that will be displayed. The default value is 255 and will display all connections. This should normally be sufficient and can be accepted by pressing Return. A connection table is shown below.

```
NetBlazer 8500    Connection-Table        Filter:255          Page
1
CTE  t USRstat LANstat   USER -----> LAN         LAN -----> USER
 1  ii  DLISN            0/0         0/0         0/0        0/0
 2  ii  DATA   DATA     34/1934     34/1934     12/123     12/123
34  mi  DLISN            0/0         0/0         0/0        0/0
35  mi  DATA   DATA      2/123       2/123       9/987      9/987









------------------------------------------------------------
-
2:Con.-Data 3:Buffer-Data  6:Terminate-Con. m:Msg. f:Filter <RETURN>:exit
```

Fig. 5-2: Connection table

The connections *1ii* and *34mi* (*i* = ISDN, *m* = modem) are the listening processes waiting for incoming ISDN or PSTN connections. In this example two active connections are running (*2ii* and *35mi*). They are on the ISDN side (*USRstat*) and on the LAN side (*LANstat*) in the DATA status.

Connection *2ii* for example informs that ITK NetBlazer 8500 has received 34 data packets with 1934 bytes overall from the user and has sent all the data to the LAN (next column).

ITK NetBlazer 8500 has also received from the LAN (usually a server on the LAN) 12 packets with overall 123 bytes and all the packets have been transmitted to the user (last column).

The following entries (in column: *t*) are possible:

Entry	Meaning
ii	ISDN incoming connections
io	ISDN outgoing connections
mi	modem incoming connections
mo	modem outgoing connection
ll	leased line connections
e	emas connections used for tunneling

This screen offers the following possibilities:

- looking at a specific connection (2: Con.-Data)
- examining buffer data (3: Buffer-Data)
- terminating a connection (6: Terminate-Con.)
- sending message to connection number in order to switch on and off message and data logging (m:Msg.)
- selecting filter (f.Filter)
- returning to the main menu (just type return).

The buffer data is of no further interest for the common user.

5.2.1 Connection data

In the connection table menu choose option *2*. A monitor picture similar to the one below is displayed after the connection ID is specified (in this case 2).

```
CTE:002 Type:ii PID:3129   Age:   0:50:59  Log:E
USER-information                  LAN-information
Contr.No.     :            2      msgsize         :        2048
status        :        DLISN      status          :
overflow      :            0      more_data       :           0
resp_msgid_cnt:            0      snd_continue    :           0

cnt_snd_m     :            0      cnt_rcv_m       :           0
cnt_snd_b     :            0      cnt_rcv_b       :           0
cnt_rcv_m     :            0      cnt_snd_m       :           0
cnt_rcv_b     :            0      cnt_snd_b       :           0
plci          :       0x0000
ncci          :       0x0000      Auth.-Server    :     0.0.0.0
Service-Mask  :       0x80a0      Appl.-service   :
b2protocol    :                   Appl.-server    :     0.0.0.0
b3protocol    :                   IP-mode         :         0x0
ISDN-Call-ID  :                   IP-state        :
Called Subaddr:                   User-IP-address :
timeslot      :            0      IP-filter
                                  User:                 UNKNOWN

------------------------------------------------------------
-
3:Buffer-Data  m:Msg.  +:next  -:prev.  6:Terminate-Con.  <RETURN>:exit
```

Fig. 5-3: Connection information - ISDN

5.2.2 Meanings of ISDN connection entries

Entry	Meaning
Contr. No.	number of ISDN board
status	state of the connection on the ISDN and LAN side
cnt_*	transferred data for both directions

Entry	Meaning
SI/AddInfo	ISDN signalisation
b2/3protocol	protocols of digital connection (HDLC, X_75, V.110)
ISDN-Call-ID	Caller ID from the user (if determined)
Called Subaddr	Called Subaddress (DDI)
timeslot	timeslot on the primary rate interface
Auth.-server	IP address of the used authentication server
Appl.-service	used application service (TCP/IP, TELNET, TCP-Clear, SHELL, LOGIN)
Appl.-server	IP address of the application server
IP-mode	protocol used for the IP connection (sPPP, aPPP, PAP, CHAP)
IP-state	IP status of the connection (IP, LCP, IPCP, PAP, CHAP, EMAS) For the EMAS connection on the home gateway the number of calling connections is shown (number of MP links).
IP-state/Compr.	If compression is used, the used PPP compression is shown.
User-IP-address	IP address allocated to the user For distributed connections that are tunneled to a home gateway the IP address of this home gateway is shown.
IP-filter	IP packet filter (in this case 1, that means */u/pra/dat/firewall_1* is used as packet filter)

Entry	Meaning
User	user name of user of this connection

The connection data menu offers the possibility of viewing buffer data, of switching on/off message logging (*m*) for a connection and of switching forwards/backwards to further connections (+,-).

Leave this menu by pressing return.

5.2.3 Meanings of modem connection entries

```
b2protocol     :  MVIP -> MODEM
b3protocol     :   TRANSPARENT
Contr. / Modem :  1 / 1
ModPLCI / Baud :  0x0101 / 28800
Prot. / Compr. :  V.42 / V.42BIS
```

Fig. 5-4: Connection information - modem

Only the following entries differ from the terms explained above:

Entry	Meaning
b2protocol	connection to modem via MVIP bus
Contr. / Modem	number of modem board / number of modem on the board
Baud	baudrate
Prot. / Compr.	error correction protocol (V.42, MNP4) compression (V.42bis, MNP5)

5.3 Shutdown

There are several possibilities for shutting down the software or the system after choosing point 5 in the main menu.

Answer the question *change shutdown-state* with *y* (yes)

- **normal** means that the ITK NetBlazer 8500 software stops without restarting. Now ITK NetBlazer 8500 cannot accept calls from users. To start the software, type in at the command prompt: **start_practrl.**
- **capi-reload** means that the ISDN board software for the ITK Primary, ITK DigitalModem and voice compression boards are reloaded and the ITK NetBlazer 8500 software starts automatically.
- **reload ITK NetBlazer 8500 software** reloads the ITK NetBlazer 8500 software with new parameters
- **reboot system** stops the software and reboots the complete Unix system. The ISDN and ITK NetBlazer 8500 software start automatically.
- **cold-reboot** stops the ITK NetBlazer 8500 software and stops and resets the whole system (hardware reset). The ISDN and ITK NetBlazer 8500 software start automatically.
- **timeout**: inactivity time (after that time an inactive connection is aborted)

A negative value for the shutdown time is allowed, which means the shutdown should be done after N seconds at the latest. All active connections after that time are aborted. The normal inactivity shutdown time is activated with positive values.

5.4 Process Monitor

The Process Monitor shows all currently running processes and their status. This screen is also displayed when a shutdown is invoked.

```
Shutdown-state     :

Table of processes                                          page: 1

ID Name         PID    Start    Activity Start Exit- Infotext
                                         -Cnt  code
-----------------------------------------------------------------
 1 PRACTRL     3102    3:41:31   0:00:03    1     0
 2 ISDN_IN/0   3129    3:40:59   0:00:03    1     0
10 ISDN_OUT    3131    3:40:59   0:00:01    1     0
11 PSTN_IN/0   3125    3:40:59   0:00:03    1     0
19 PSTN_OUT    3127    3:40:59   0:00:01    1     0
22 PRAMODTEST  3147*   3:30:59   3:29:32    1     0
23 DEBUGLOG/0  3110    3:41:28   3:41:21    1     0 D-channel up
28 SNSP_SERVE  3133    3:40:59   0:00:01    1     0




-----------------------------------------------------------------
m: send message to process ▮
```

Fig. 5-5: Process Monitor

The entries have the following meanings:

Entry	Meaning
ID	ITK NetBlazer 8500 process number
Name	name of process
PID	Unix process ID *: process is not running
Start	process has been started *hh:min:sec* ago

Entry	Meaning
Activity	process has shown activity for the last time *hh:min:sec* ago
Start-cnt	displays how often the process has been started
Exit-code	error code
Infotext	gives additional information about the process

The following options are available:

Option	Meaning
m	sends a message to a process for example: to switch on/off message and data logging
ESC/Return	exit Process Monitor

Gatekeeper Information:

In the procss table of PRAMON (and webMan) you can see the IP address of the used gatekeeper (GK) or 'No GK' if no gatekeeper is used. Furthermore the number of sessions is shown ('s).

Example:

No GK - #s: 2	Not using a gatekeeper, two active H.323 sesions.
GK 123.45.67.89 #s: 0	Using a gatekeeper 123.45.67.89, no active H.323 session.
GK 0.0.0.0 #s: 0	Using a gatekeeper, but actual unregistered (e.g. gatekeeper is down), no active H.323 session.

5.5 Logging

The state of message and data logging can be changed (on/off) dynamically without restarting the software. Logging messages can be sent to processes/connections from PRAMON:

- A message to this connection must be sent to enable/disable the logging of a running connection.
- A message to the master connection (in *LISTEN* state) must be sent to enable/disable the logging for all further connections.

5.5.1 Changing/Showing Logging State

The current logging state (all active logging types) is shown in the connection data view.

Type the following characters to show the appropriate logging state:

Character	Meaning
E	Error logging is active
M	Message logging is active
D	Data logging is active
d	Data logging (only specified levels) is active

You can change the current logging states dynamically for current or future connections by sending a message to the specified connection (from connection table, connection data or process table view).

5.6 Sending a message to PRACTRL

To send a message to PRACTRL perform the following steps:

(1) Start *pramon*.

(2) Select *7:Display PROCESS-Monitor*.

(3) Type *m* to send a message to a process.

(4) Type *1* to select PRACTRL.

This menu offers the possibility to set the logging and to check running processes and the ISDN/modem hardware.

```
Msg.s to Process:

ID Name         PID    Start    Activity Start Exit- Infotext
                                          -Cnt  code
-------------------------------------------------------------------
1 PRACTRL     3102    3:41:31   0:00:03    1     0
-------------------------------------------------------------------
  m: Msg.-Logging on
  M: Msg.-Logging off
  d: Data-Logging on
  D: Data-Logging off
  l: Set Data-Logging-Level

  1: Check Process ISDN_IN         2: Check Process ISDN_OUT
  3: Check Process PSTN_IN         4: Check Process PSTN_OUT
  5: Check Process PSPDN           6: Check Process ISDN_LL
  7: Check Process SNSP-Server     9: Check Process L2F-Daemon
 10: Check Process H323-Daemon    11: Check Process ISS-Daemon
 15: Check ISDN-cards and Modem-cards
 16: Check Modem-cards (self-connecting)
 43: LAN/WAN-Test
 48: D-channel-Test

Type Message-No.: ▮
```

Fig. 5-6: Send Message to PRACTRL

Entry	Meaning
m	switch on message logging
M	switch off message logging
d	switch on data logging
D	switch off data logging
l	shows the Data-Logging-Level Menu

Entry	Meaning
1	checks the process ISDN_IN waiting for incoming ISDN connections.
2	checks the process ISDN_OUT handling the outgoing ISDN connections
3	checks the process PSTN_IN handling the incoming modem connections (analog)
4	checks the process PSTN_OUT handling the outcoming modem connections (analog)
5	checks the process PSPDN handling of the X.25 connections
6	checks the process ISDN_LL (leased line connections)
7	checks the SNSP server (ITK NetBlazer 8500 Name Server Protocol Server; explained below)
9	checks the L2F daemon
10	checks the H.323 Daemon
11	checks the ISS Daemon
15	checks ISDN boards and modem boards Initiates a self-test of the ISDN and modem boards to test the hardware. If an error occurs a trap is sent to the NMS and the boards are reloaded. This test is done in an automatic cycle of 60 sec (default).
16	*Check Modem-boards* additionally performs a self connection between two modems. With this feature all modems on all boards are checked. If a modem has an error it is disabled and a trap is sent to the NMS. This test is done in an automatic cycle of 10h.

Entry	Meaning
43	test whether a given IP address is reachable
48	checks the D channel

The meaning of ID, Name, PID, Activity, ... is explained in Chapter 5.4, *Process Monitor* (page 5-10).

5.6.1 Suprimo (ITK NetBlazer 8500) Name Service (SNS)

The new process *snsp_server* is the server for the Suprimo (ITK NetBlazer 8500) Name Service (SNS), which handles incoming requests (especially from other ITK NetBlazer 8500s) by finding the requested information and sending the response back. The requests and responses are transferred with the SPC protocol (see below). Incoming requests are expected on the UDP port 30000 (changeable with parameter *spc_sns_port*). Additionally, the SNS starts dial-out connections for received IP packets that have no active connection.

5.6.2 SPC Tunneling Protocol

The SPC protocol (Suprimo (ITK NetBlazer 8500) Process Communication) is a ITK NetBlazer 8500 proprietary protocol to exchange messages between multiple ITK NetBlazer 8500 processes. SPC is based on UDP. Therefore it has less communication overhead than for example L2F and is also useable between multiple systems (on the same network). SPC is used for example for tunneling (EMAS) the user data to the right process.

5.7 Service-Monitor

(1) To display or change the defined services, please use the Service-Monitor.

```
SERVICE-Menu:

1 : Display table of SERVICES
2 : Insert SERVICE-address
3 : Remove SERVICE-address
4 : Activate SERVICE-address
5 : Deactivate SERVICE-address
c : Display SERVICE-Comp.-Channels
i : Display SERVICE-UIP address
m : Display SERVICE-Modems
q : Terminate SERVICE-Monitor

your selection: ▮
```

Fig. 5-7: Service-Monitor

Entry	Meaning
1	Displays the configured services like an authentication server.
2	Inserts a service at runtime.
3	Removes a service.
4	Activates a service.
5	Deactivates a service.
c	Displays voice compression channels and state (in use, defined) see Fig. 5-8: *Voice compression* (page 5-18).

Entry	Meaning
i	Displays configured IP pools for dynamically IP address assignment. See Fig. 5-9: *IP pools* (page 5-20).
m	Displays configured modems and their status (in use, defective). See Fig. 5-10: *Modems* (page 5-21).
q	quits the service monitor

An inserted, removed, activated or deactivated service is only valid for the momentary runtime. In case of a restart changes are lost.

Service voice compression channels:

(1) In the Service Menu, type *c* to show the list of Service voice compression channels:

```
Service 11 (cchan): max. No. of entries :              page 1
 No: ctr dsp chan act err used start   end
307: 100  0     1 YES  NO  NO  16324 16230
308: 100  0     2 YES  NO  NO  16401 16401
309: 100  1     3 YES  NO  NO  16401 16401
310: 100  1     4 YES  NO  NO  16401 16401
311: 100  2     5 YES  NO  NO  16401 16401
312: 100  2     6 YES  NO  NO  16401 16401
313: 100  3     7 YES  NO  NO  16401 16401
314: 100  3     8 YES  NO  NO  16401 16401
315: 100  4     9 YES  NO  NO  16401 16401
316: 100  4    10 YES  NO  NO  16401 16401
317: 100  5    11 YES  NO  NO  16401 16401
318: 100  5    12 YES  NO  NO  16401 16401
319: 100  6    13 YES  NO  NO  16401 16401
320: 100  6    14 YES  NO  NO  16401 16401
321: 100  7    15 YES  NO  NO  16401 16401
322: 100  7    16 YES  NO  NO  16401 16401
323: 100  8    17 YES  NO  NO  16401 16401
324: 100  8    18 YES  NO  NO  16401 16401
325: 100  9    19 YES  NO  NO  16401 16401
326: 100  9    20 YES  NO  NO  16401 16401
------------------------------------------------------------
<ESC>:Start-Menu   <q>:Service-Menu  <RETURN>:next page
```

Fig. 5-8: Voice compression

The entries have the following meanings:

Entry	Meaning
No	index of service entry
ctr	controller number of voice compression board
dsp	number of DSP on the board
chan	number of voice compression channel on the board

Entry	Meaning
act	status if voice compression is activated
err	states occurred errors during connections
used	Yes, if voice compression channel is in use
start	time in sec. since the voice compression channel has been initialized
end	time in sec. since this voice compression channel has been last used

Service UIP addresses:

(1) In the Service Menu, type *i* to show the list of Service UIP addresses:

```
Service 9 < uip>: max. No. of entries: 30             page 1
No : uipaddr        pool-id inuse start    end  last-user
 59: 195.138.47.33        0  NO   16229  16146  guest1
 60: 195.138.47.34        0  NO   16317  16317
 61: 195.138.47.35        0  NO   16317  16317
 62: 195.138.47.36        0  NO   16317  16317
 63: 195.138.47.37        0  NO   16317  16317
 64: 195.138.47.38        0  NO   16317  16317
 65: 195.138.47.39        0  NO   16317  16317
 66: 195.138.47.40        0  NO   16317  16317
 67: 195.138.47.41        0  NO   16317  16317
 68: 195.138.47.42        0  NO   16317  16317
 69: 195.138.47.43        0  NO   16317  16317
 70: 195.138.47.44        0  NO   16317  16317
 71: 195.138.47.45        0  NO   16317  16317
 72: 195.138.47.46        0  NO   16317  16317
 73: 195.138.47.47        0  NO   16317  16317
 74: 195.138.47.48        0  NO   16317  16317
 75: 195.138.47.49        0  NO   16317  16317
 76: 195.138.47.50        0  NO   16317  16317
 77: 195.138.47.51        0  NO   16317  16317
 78: 195.138.47.52        0  NO   16317  16317
-------------------------------------------------------------
<ESC>:Start-Menu   <q>:Service-Menu  <RETURN>:next page
```

Fig. 5-9: IP pools

The entries have the following meaning:

Entry	Meaning
No	index of service entry
uipaddr / pool-id	list of IP addresses belonging to the pool ID
inuse	shows currently used IP addresses
start	time in sec. since a user has started using the IP address

Entry	Meaning
end	time in sec. since this IP address has been set free
last user	user having used this IP address

The available options are obvious.

Service Modems:

(1) In the Service Menu, type *m* to show the list of Service modems:

```
Service 5 <modem>: max. No. of entries : 38          page 1
No: ctr id pool act err used start   end
16:  0   1    0 YES  NO  NO  16324 16230
17:  0   2    0 YES  NO  NO  16401 16401
18:  0   3    0 YES  NO  NO  16401 16401
19:  0   4    0 YES  NO  NO  16401 16401
20:  0   5    0 YES  NO  NO  16401 16401
21:  0   6    0 YES  NO  NO  16401 16401
22:  0   7    0 YES  NO  NO  16401 16401
23:  0   8    0 YES  NO  NO  16401 16401
24:  0   9    0 YES  NO  NO  16401 16401
25:  0  10    0 YES  NO  NO  16401 16401
26:  0  11    0 YES  NO  NO  16401 16401
27:  0  12    0 YES  NO  NO  16401 16401
28:  0  13    0 YES  NO  NO  16401 16401
29:  0  14    0 YES  NO  NO  16401 16401
30:  0  15    0 YES  NO  NO  16401 16401
31:  0  16    0 YES  NO  NO  16401 16401
32:  0  17    0 YES  NO  NO  16401 16401
33:  0  18    0 YES  NO  NO  16401 16401
34:  0  19    0 YES  NO  NO  16401 16401
35:  0  20    0 YES  NO  NO  16401 16401
------------------------------------------------------------
<ESC>:Start-Menu   <q>:Service-Menu  <RETURN>:next page
```

Fig. 5-10: Modems

The entries have the following meanings:

Entry	Meaning
No	index of service entry
ctr	controller of modem board
id	number of modem on the board
pool	modem pool id
act	status if modem is activated
err	states occurred errors during the modem self-tests
used	states the current use of modems
start	time in sec. since the modem has been initialized
end	time in sec. since this modem has been last used

The available options are obvious.

5.8 Displaying counters

(1) In the main screen of *pramon*, type *c* to display the counters.

ITK NetBlazer 8500 will show the overall counters of transferred bytes and packets since the last start of the ITK NetBlazer 8500 software.

(2) By pressing *z* the counters are reset to 0.

```
SUM-COUNTERS:

Age:  30:06:18

Type     Con.#t #act  Sys      Received         Send
-------------------------------------------------------------
ISDN_IN  13        0  USR      211/3271       203/4367
                      LAN      203/4367       211/3271
ISDN_OUT 0         0  USR        0/0            0/0
                      LAN        0/0            0/0
PSTN_IN  9         0  USR      639/36599      580/69962
                      LAN      593/69962     1276/36595
PSTN_OUT 0         0  USR        0/0            0/0
                      LAN        0/0            0/0
EMAS     0         0  USR        0/0            0/0
                      LAN        0/0            0/0
-------------------------------------------------------------
Sum      22        0  USR      850/39870      783/74329
                      LAN      796/74329     1487/39866


z: delete sum-counters
```

Fig. 5-11: Display Counters

The entries have the following meanings:

Entry	Meaning
Age	Time since last restart in hh:mm:ss
Type	Connection type
Con.#t	Connection number in total
#act	Number of actual connections

5.9 Displaying hardware information

(1) In the main screen of *pramon*, type *h* to display the Hardware Information.

```
   Hardware Information

LED-State:
ISDN :     o --- o     ---     ---     ---
Modem:     o --- o                   LAN:  o
Power:  o Ready: o Active:  Temp: o  WAN:

Temperature  : 30.7 degrees C   87.2 degrees F

Voltages
           + 5V:   5.0 V
           +12V:  12.2 V
           - 5V:  -5.0 V
           -12V: -12.5 V
CPU-Load
last minute    :   0%
last 5 minutes :   0%
last 15 minutes:   0%
Operation-time : yy:mm:dd:hh:mm 00:01:05:16:30
License:
RAS     V50  Ports: 30    ExpireDate: key is unlimited
Voice   V50  Ports: 24    ExpireDate: key is unlimited
------------------------------------------------------------
                                                <RETURN>:Exit
```

Fig. 5-12: Hardware information

The following hardware information are shown

Hardware Information
LED-state (same as front-panel) with LAN/WAN, Ready, Active state and states for each communication board. The modem LEDs display the state of ITK DigitalModem and voice compression board(s).
temperature in ITK NetBlazer 8500 housing
current value of +5V voltage

Hardware Information
current value of +12V voltage
current value of -5V voltage
current value of -12V voltage
operation time of ITK NetBlazer 8500
CPU load
LAN status
WAN status
active licenses

5.10 Displaying Cardtable

(1) In the main screen of *pramon*, type *k* to display the Cardtable.

```
Table of communication-cards:
Shutdown-state     :

Ctr  Type               Stat.  MVIP    Ports     Active  cnt  last-ixload
-------------------------------------------------------------------------
  2 ITK Primary           up-on Master   30      0:00:08   1     1:12:40
  3 ITK Primary           up-on Slave    30      0:00:08   1     1:12:31
  0 ITK DigitalModem       up   Slave    30      0:00:07   1     1:12:20
  1 ITK DigitalModem       up   Slave    30      0:00:07   1     1:12:13
100 Viper Compression      up   Slave    48      0:00:07   1     1:12:07
101 Viper Compression      up   Slave    48      0:00:07   1     1:12:01




-------------------------------------------------------------------------
a:Activate card  d:Deact. card  t:Test cards  c:Test D-Channel  i:Card Info
```

Fig. 5-13: Cardtable

If pramon is started with the argument -k the cardtable is shown and pramon exits after the list has been shown.

The Cardtable shows some new information:

Entry	Meaning
Stat.	shows the state of the board up: enabled (board is loaded) down: disabled (board is not loaded) up-on: enabled and D channel active (layer-1 is on)
MVIP	shows the configured MVIP type (master or slave) of the board. The MVIP master is the master for the MVIP bus clock. Only one board on the same MVIP bus has to be configured to be the master. The other boards have to be configured as MVIP slaves.
Ports	shows the number of ports
Active	shows the time when the board was last active
cnt	shows how often the board has been loaded (ixload-count)
last-ixload	shows when the board has last been loaded

The following table shows you the possible actions:

Action	Meaning
i	information gives specific information about one selected board (for example used D channel protocol, language variant)

Action	Meaning
d	deactivate to disable To mark erroneous boards or run test configurations with fewer boards than configured, the boards in a ITK NetBlazer 8500 can be disabled on-the-fly in the Cardtable. A disabled board is not used for any new connection, but active connections on this board can be finished by the user normally.
a	activate to enable To mark erroneous boards or run test configurations with fewer boards than configured, the boards in a ITK NetBlazer 8500 can be re-enabled on-the-fly in the Cardtable. An enabled board is first loaded and then activated to be used for new connections.
t	sends a test message to each enabled board For each responding board the active timestamp is reset to zero.
c	tests D channel

The *practrl* process automatically disables a board if it is in an error state (for example not responding after some loads). Disabled boards have to be enabled manually (or have to be repaired).

5.10.1 Advanced Card-information

(1) Type *i* and then the Ctr. no. to show Advanced Card-information:

You find special entries that are only valid for a specific board in the following sections:

ITK DigitalModem (page 5-29)

ITK Primary (page 5-30)

Voice compression board (page 5-31)

The following entries are valid for ITK Primary, ITK DigitalModem and voice compression board:

Entry	Meaning
Ctrl. No	shows controller number
Ctrl. Type	shows the controller type (for example: ITK DigitalModem, ITK Primary, voice compression board)
Cardstate	shows the state of the board up: enabled (board is loaded) down: disabled (board is not loaded) up-on: enabled and D channel active (layer-1 is on)
MVIP-State	Master or Slave
Hardware-Version	shows hardware version (bus type, interface)
Hardware-Revision	shows hardware revision number
Serial-No.	shows the serial number
Maximum Channels	shows number of maximum channels

ITK DigitalModem

```
Advanced Card-information

Ctrl.No           : 0
Ctrl.Type         : ITK DigitalModem
Cardstate         : up
MVIP-State        : Slave
MVIP-Stream       : 0
Hardware-Version  : ISA Granite
Hardware-Revision : 1
Serial-No.        :
Maximum Channels  : 30




------------------------------------------------------------
+:next    -:previous                          <RETURN>:Exit
```

Fig. 5-14: Advanced Card-information for ITK DigitalModem

Entry	Meaning
MVIP-Stream	shows number of MVIP stream of ITK DigitalModem

ITK Primary

```
Advanced Card-information

Ctrl.No           : 2
Ctrl.Type         : ITK Primary
Cardstate         : up-on
MVIP-State        : Master
D-Chan.-protocol  : 1TR6
Voice-Coding      : a-law
Hardware-Version  : PCI S2m
Hardware-Revision : 1
Serial-No.        : 2288120095
Maximum Channels  : 30




------------------------------------------------------------

 +:next    -:previous                          <RETURN>:Exit
```

Fig. 5-15: Advanced Card-information for ITK Primary

Entry	Meaning
D-Chan.-protocol	shows the D channel protocol You will find all valid D channel protocols in Chapter D.2, *Parameters in the subsections* (page D-3).
Voice-Coding	shows the voice code The voice code standard can be: a-Law (European Standard) µ-Law (US Standard)

Voice compression board

```
Advanced Card-information

Ctrl.No           : 100
Ctrl.Type         : Viper Compression
Cardstate         : up
MVIP-State        : Slave
Hardware-Version  : Viper-12 542/PC
Hardware-Revision : B.0
Serial-No.        : 18114
#DSP              : 12
#DSP-Channel def. : 24
#DSP-Channel act. : 24




------------------------------------------------------------

 +:next    -:previous                          <RETURN>:Exit
```

Fig. 5-16: Advanced Card-information for voice compression board

Entry	Meaning
#DSP	number of DSPs
#DSP-Channel def.	defined number of voice compression channels
#DSP-Channel act.	number of useable voice channels

6 PRACTRL

The *practrl* process is checking the ITK NetBlazer 8500 software by executing the following tasks:

- According to the configuration several master processes may be started on ITK NetBlazer 8500 (ISDN_IN, ISDN_OUT, PSTN_IN , PSTN_OUT, ISDN_LL, L2F_DAEMON, SNSP_SERVER, WD_DAEMON, H323D, ISSD and DEBUGLOG).
- practrl starts, stops, watches, and restarts these master processes and evaluates program exit reasons. If a master process fails and stops more than m (parameter: .max_prc_restarts) times with an error within n (parameter: .time_prc_runok) milliseconds, than practrl reacts depending on the error code. If a card error is the reason for the program stop this/these board(s) will be reloaded. If a system fault is causing this reaction the system will reboot; all other reasons cause this process not to start again. practrl sends a SNMP trap to the NMS if a severe error occurs.
- Start of ITK NetBlazer 8500 software is not possible if software is already running.
- The most important adjustments of each board are determined after loading and can be displayed with *pramon*.
- practrl makes copies of all parameter files during startup which are stored in /u/pra/dat/.running. This enables a user to perform parameter file changes in /u/pra/dat without disturbance of ITK NetBlazer 8500.
- If an error occurs practrl shuts down the system in a specified way so all connections will be stopped after 1 minute (parameter: practrl.shuttime_abort) as well as all master processes. Afterwards practrl stops, too.
- If a shutdown is initiated at first all master processes are stopped, afterwards all established connections will be stopped after an inactivity time of 5 minutes (parameter: practrl.shuttime_normal). Inactivity time means a non interrupted period with no registered line activity.
- periodically practrl can perform defined commands.
- All boards are periodically tested and results are documented in log file (/u/pra/log/pramodtest*). Failing tests lead to a shorter time interval before the next test is started. After n (parameter:

.max_isdn_errors/ .max_modem_errors) successive failed tests only this board is reloaded.

- The PCs basic time is regularly checked and the PC will be restarted before this counter runs over. Basic time scale of ITK NetBlazer 8500 is milliseconds. A 32 bit counter collecting the milliseconds since system start runs over after about 490 days. Because this overrun may cause internal problems ITK NetBlazer 8500 is restarted some days before this counter runs over.
- A temperature sensor watches the temperature inside ITK NetBlazer 8500 housing. This regularly registered temperature inside the housing is written to a log file (practrl.info) if configured. If maximum temperature (parameter: .max_temp) is exceeded a trap is sent to NMS.
- If parameter .info_syslog_target is configured practrl will send information for a user to any configured syslog process beside the entry in /u/pra/log/practrl.info.
- practrl periodically checks the free disk space and sends a trap if the free space is below the defined limit (parameter: practrl.hdd_space_remaining).
- practrl determines CPU load of the PC for the last minute, the last 5 minutes and last 15 minutes.
- practrl periodically measures voltage values of the power supply and systems operation time.
- practrl counts the number of authentication failures that appeared in the last m minutes (parameter: check_auth_errors). A trap to NMS is generated if more than a defined number of authentication errors are recognized (parameter: .trap_auth_errors) (intruder recognition).
- practrl removes old log files periodically.
- A private MIB for ITK NetBlazer 8500 is available. A SNMP subagent is included in practrl and is responsible for communication with a Network Management System (NMS). This subagent receives SNMP get and put requests and answers these requests.

6.1 Dynamic reloading of boards

The *practrl* process automatically checks all communication boards. *practrl* periodically performs a download. This is done between 3:00 am (parameter: .night_begin_hour) and 5:00 am (parameter: .night_end_hour) if no connections are active. This default setting can be changed by setting parameter .restart to an interval n (in hours). Than this periodically download is performed every n hours. If parameter .restart = 0 is set no periodically download is performed.

Errors during download of boards are split in 2 categories:

a) administration error:

practrl performs a shutdown and an error message is written to file practrl.info. The administrator is asked to eliminate the error.

b) other error:

Is the faulty loaded board the last active MVIP master (clock generator for the system)? (All boards in ITK NetBlazer 8500 are connected via MVIP bus; one of these boards is MVIP master; if there are several MVIP busses in one system than each MVIP bus has its own MVIP master).

Yes (the board is the last active MVIP master):

Start shutdown/ixload and reload all communication boards. After n failed reload attempts a reboot (shutdown/coldboot) will be initiated because ITK NetBlazer 8500 needs at least one active MVIP master for proper operation. A SNMP trap is sent to the Network Management System (NMS).

No (another board is MVIP master):

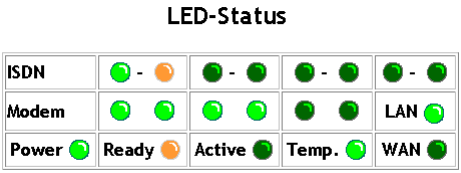
After n failed reload processes this board will be taken out of the availability list. This board is not useable till a successful download has been performed. Since there are other active MVIP master boards available ITK NetBlazer 8500 is useable with restrictions. A SNMP trap is sent to the NMS.

- Boards can manually be deactivated/ activated with *pramon*.

6.2 LED status signaling (PCI)

The *practrl* process is responsible for checking the LEDs at the ITK NetBlazer 8500 front. These LEDs can be green, orange or black (off).

The LED display on the ITK NetBlazer 8500 front contains 20 LEDs and is connected to the LED driver:



The LAN /WAN LEDs are set if the LAN/WAN interface is working correctly. The interface works correctly, if the network connected to this interface is reachable. practrl checks the connection to one IP address in this network (by a ping). If the IP adddress responds, the LED is set to green. If not, the LED is set to orange. If no IP address is specified the LED remains off.

ITK NetBlazer 8500 parameters that define the status checks:

practrl.time_check_net:	# Interval between two checks (in ms) (normally 60 sec)
practrl.cmd_start_check_net:	# Command to check the connection to an IP-address
practrl.lan_test_ip:	# IP-address to test for LAN-status
practrl.wan_test_ip:	# IP-address to test for WAN-status

If IP addresses (LAN and WAN) are not reachable within a certain time interval
(parameter: *practrl.time_check_net * practrl.max_test_failure msec*)
ITK NetBlazer 8500 reboots. If only one network (LAN or WAN) is configured decision is taken according to this network.

The modem LEDs show the status of installed modem and / or voice compression boards. Each modem and voice compression board is represented by one LED. You get the number of installed modem and voice compression boards from PRAMON (see Chapter 5.10, *Displaying Cardtable* (page 5-25)). From the left side with first LED(s) status of modem board(s) is set. Following LED(s) show the status of installed voice compression boards.

For each installed ISDN board 2 LEDs display the status. The LED on the left side is orange if board is not loaded. The LED is switched to green if board is loaded/active. The LED on the right side displays D channel status. This LED is green if D channel is up and orange if D channel is down. D channel is checked periodically and a trap is sent to NMS if D channel status changes.

The LEDs show a fast status of ITK NetBlazer 8500 and may be of interest for an operator or service-technician.
The ITK NetBlazer 8500 software switches the LED's automatically, if software is running.

Indicator	Color	Meaning
Power	green	ITK NetBlazer 8500 is turned **on**
	off	ITK NetBlazer 8500 is turned **off**
Ready	green	ITK NetBlazer 8500 is ready to accept **connections**
	orange	ITK NetBlazer 8500 is **unable** to accept calls
	off	ITK NetBlazer 8500 software is **not** running
Active	green	at least one connection is **running**
	off	**no** connection running

Indicator	Color	Meaning
Temp.	green	temperature in ITK NetBlazer 8500 housing is **ok**
	orange	temperature in ITK NetBlazer 8500 housing is **too high**
LAN	green	LAN connection is **working** (next-hop reachable)
	orange	LAN connection **not** working (configured next-hop not reachable)
	off	**no** LAN connection defined
WAN	green	WAN connection is **working** (configured next-hop reachable)
	orange	WAN connection **not** working (configured next-hop not reachable)
	off	**no** WAN connection defined
ISDN		2 LEDs (L=left/R=right) for each ISDN board
	L-green	ISDN board **ready**
	L-orange	ISDN board **not** ready
	L-off	ISDN board **not** configured
	R-green	ISDN board **running** (layer-1 ready)
	R-orange	ISDN board **not** ready (layer-1 not ready)
	R-off	ISDN board **not** configured

Indicator	Color	Meaning
Modem		1 LED for each modem and / or voice compression board
	green 	modem board **ready,** voice compression board **ready** (on front panel)
	blue 	voice compression board **ready** (only WebMan)
	orange 	modem / voice board **not ready**
	off 	modem / voice board **not configured**

6.3 SNMP Traps

To show special events practrl sends SNMP traps to the NMS, which has been configured for SCO Unix in the */etc/snmpd.trap* file.

The following enterprise specific traps are generated:

Traptext	Number	Cause
System ready	10	ITK NetBlazer 8500 has been restarted and is ready to accept connections
normal Shutdown	20	Normal (user caused) shutdown initiated
Shutdown with IXLOAD	21	Shutdown with CAPI-reload (reload of all ISDN, modem and voice compression boards) initiated

Traptext	Number	Cause
Shutdown with Reboot	22	Shutdown with warm-reboot initiated
Shutdown with Coldboot (Reset)	23	Shutdown with cold-reboot initiated
Shutdown with IXLOAD/ PRACTRL restart	24	Shutdown with software-restart initiated
Max. temperature exceeded: XX.Y Grad C	30	Temperature inside ITK NetBlazer 8500 housing is too high
ISDN-Card-Error, Card:X	31	Error with ISDN board
Modem-Card-Error, Card:X	32	Error with modem board
Modem-Error, Card:X Modem:Y	33	Error with modem on modem board
Process-Error, Process:X, PID:Y	34	Error with starting process
Packet-Handler-Connect-Error	35	Error connecting to X.25 packet handler
Appl-Server-Connect-Error	36	Error connecting to application server
HDD space (X) passed max. level of Y%	37	Too little free space on disk
Too many authentication errors : X	38	Too many authentication errors (intruder alarm)

Traptext	Number	Cause
ISDN-Card X: layer-1 active	39	PRI interface has been activated for ISDN board
ISDN-Card X: layer-1 deactive	40	PRI interface was deactivated for ISDN board
Voice compression-Card-Error, Card: X	41	Error with voice compression board
Error opening L2F tunnel to X	51	Error establishing l2f tunnel
Authentication Server is deactivated: IP-Addr.:	52	Error contacting RADIUS authentication server
Accounting Server is deactivated: IP-Addr.:	53	Error contacting RADIUS accounting server
LCR Server is deactivated: IP-Addr.:	54	Error contacting LCR server

6.4 pra_shutdown tool

A ITK NetBlazer 8500 shutdown is normally initiated with the *pramon* interactive program. Alternatively you can use the *pra_shutdown* tool. Call *pra_shutdown* with 2 command line parameters:

- shutdown-cause: integer that describes the action to take after the shutdown (1-5, as in *pramon*)
- inactivity-time: integer that describes the inactivity time for active connections (as in *pramon*)

This tool can be used to schedule an operatorless ITK NetBlazer 8500 shutdown, for example through the UNIX cron facility.

7 Individual software configuration

7.1 Shared Library

Since version 4.0 the ITK NetBlazer 8500 software uses a shared library concept. That means all executables are small in size and use one shared library („/u/pra/lib/libpra.so“), which contains all the code.

Further software upgrades (i.e. patches) only contain a new shared library and all executables use the new functionality. (Conflicts between executables of different versions should have come to an end now!)

7.2 Parameterization

The individual adjustment of the ITK NetBlazer 8500 software is done with parameter files described below. This allows the making of changes without altering any program code.

7.3 The parameter files

The software is already preconfigured for your needs.

All parameter files are stored in the directory:

/u/pra/dat

All files have the ending *par*, the short form of parameter.

The parameter files have the following meanings:

Parameter File	Meaning
param.par	includes all parameter files used
common.par	default values for all ITK NetBlazer 8500 parameters
isdn.par	parameters for ISDN PRI interfaces

Parameter File	Meaning
process.par	special parameters for processes, for example line-counters, PRACTRL parameters
uip_pool.par	pool of dynamic IP addresses for remote IP users
auth.par	parameters for authentication and accounting
ppp.par	parameters for PPP and SLIP
dlm.par	parameters for **D**istributed **L**ine **M**anagement (DLM)
misc.par	miscellaneous parameters
l2f.par	parameters for L2F tunneling
cards.par	parameters for communication cards (ISDN, modem and voice compression boards)
voip.par	parameters for voice over IP
h323.par	parameters for H.323 (VoIP)
iss.par	parameters for Internet Supplementary Services (Siemens EWSD features)

The *param.par* and *common.par* parameter files will be overwritten if you install a new software version. All the other files are customer specific and therefore will be left unchanged in future installations.

Setting parameters

You have several possibilities for setting parameters:

1. In the *common.par* file **all** parameters are set with default values. This file will be overwritten if you install a new software version.
2. You can set the parameters in the special parameter files. Then the specified values are used and not the values from the *common.par* file. The set parameters are left unchanged if you install a new software version.

Syntax for parameter files

The following syntax is valid for all parameter files:

- line-format: one parameter per line
- remarks start with #
- syntax: [<programname>].<parametername>: <value> [#remark]
- starts a macro: $(<macroname>)
- allowed characters for <programname> and <parametername>: [0-9], [A-Z], [a-z], _
- allowed characters for <value>: all except CR, LF, #
- max. length of <programname> and <parametername>: 40 characters
- max. length of <value>: 100 characters

If in a definition the <programname> is omitted, the parameter is interpreted as default for all programs. This default value is only used if a parameter required for a certain program is not specified.

You can change the parameter files using an editor, for example *vi* of Unix or webMan. For detailed information see Chapter 2, *Unix introduction* (page 2-1).

The files and their contents are described in the next sections.

Using macros

Macro substitution:

Parameter values can contain macros, which are inserted with $(macroname).

To determine the value for the macro, perform the following steps:

(1) Check if the macro name is an internal name:

PID:	macro value is process ID
PROGRAM:	macro value is program name
DATE:	macro value is date (JJJJMMDD)
TIME:	macro value is time (hhmmss)

(2) Check if macro name is an environment variable:

➟macro value is the value of the environment variable

(3) Determine macro name from parameterization

➟macro value is the parameter value

The macro substitution is recursive.

A lot of examples are given in Appendix A.6, *All parameters from common.par* (page A-51). The first section *Macros* defines the environment variables which are used in the following sections of *common.par*.

All changes in the parameter files take effect after starting software the next time.

Running/New Configuration

To differentiate between the running configuration (parameters the current system is running with) and a new configuration (parameters the system should run with after the next ITK NetBlazer 8500 start) there are two independent parameter file sets:

- The running parameter files (in */u/pra/dat/.running*) describe the current running system. Do not change these files.
- The new parameter files (in */u/pra/dat*) describe the new configuration. You can change these parameter files using an editor or using the new webMan tool. See Chapter 7.10, *Web Management (webMan)* (page 7-92). These parameter files are automatically copied to the running configuration and used at the next ITK NetBlazer 8500 startup (with shutdown actions).

7.3.1 param.par

The parameter file *param.par* is the main configuration file of ITK NetBlazer 8500. It includes all the special parameter files for the different purposes.

Do not change the *param.par* file.

This file will be overwritten if you install a new software version.

7.3.2 common.par

The file *common.par* configures **all** parameters with default values.

Do not change the *common.par* file. This file will be overwritten if you install a new software version.

You can change the parameters in any other parameter file described in the next sections.

If a parameter is set in one of the following parameter files, this specified value is used and **not** the one defined in *common.par.*

7.3.3 uip_pool.par

The *uip_pool.par* file contains the information about the IP addresses which are used for dynamic IP address assignment. A user gets an IP address from ITK NetBlazer 8500. This can be either a static one (defined in the RADIUS database) or a dynamic one. ITK NetBlazer 8500 offers the possibility of using more than one IP pool (for example to define the first IP pool with official addresses and a second one with unofficials). In the RADIUS database you can define which IP pool has to be used for which user.

A possible configuration of the addresses might be:

```
.ip_pool_cnt: 4
.ip_pool_1: 111.192.85.0    255.255.255.0   0
.ip_pool_2: 111.193.34.32   255.255.255.224 1
.ip_pool_3: 200.200.200.200 255.255.255.255 2
.ip_pool_4: 198.198.198.198 255.255.255.255 2
```

In this example four entries are used to define three IP pools.

The first entry: *.ip_pool_cnt* defines how many entries (not IP pools) follow after this line. The different entries have a keyword like: *.ip_pool_x*: where *x* means the entry number.

Every entry consists of three fields:

1. IP address
2. netmask for this IP address
3. pool ID

   ➟ The IP address is the result of the netmask "anded" with an IP address of the pool.

That means that there are three IP pools defined in the example above:

- A pool with the ID 0: A complete class C network with the address 111.192.85.
- A pool with the ID 1: A subnet using 3 bit subnetting (netmask = 255.255.255.224) and the subnet number 111.193.34.32.
- A pool with the ID 2: This pool consists only of two IP addresses.

The pool ID in the RADIUS database can be used to assign an IP pool to a user.

Note that the routes are automatically set by the software for this defined IP addresses.

Please set the routes of the configured uip addresses in your default router to the IP address of ITK NetBlazer 8500.

7.3.4 process.par

In the *process.par* file you configure the maximum number of incoming and outgoing connections (ISDN or PSTN). Additionally, the logging behavior of various processes can be defined (for example switch on message logging for modem connections).

The parameters have the following meanings:

Parameter	Meaning
.linecnt_isdn_in	maximum number of incoming ISDN (digital connections) If one ITK Primary is installed this value has to be 30. This parameter is set by the card_config tool.
.linecnt_isdn_out	maximum number of outgoing ISDN connections Normally this value is set to 0.
.linecnt_pstn_in	maximum number of incoming modem connections (must be adapted to the number of modems built in) Example: If 3 modem boards with 8 modems on each one are installed this value has to be 24. This parameter is set by the card_config tool.
.linecnt_pstn_out	maximum number of outgoing modem connections
.linecnt_pspdn	maximum number of X.25 connections Normally this value is set to 0.
.linecnt_pspdn_ph	number of permanent connections to the packet handler. Normally this value is set to 0.
.unpriv_chan_cnt	number of unprivileged B channels. This parameter is used to define channels which are reserved for special users (premium service). If you do not want to define reserved channels mark this parameter as a comment (# as first character of the line). Example: To reserve 5 of 30 available channels for special users set this value to 25.

Parameter	Meaning
.linecnt_emas	maximum number of tunnel connections
.linecnt_isdn_ll	maximum number of leased line connections
www_suprimon .www_refresh	to adjust default page-refresh of connection table, process table and LED table (webMan) Value: Time for refreshing page in seconds (0 = refresh off)
www_suprimon .www_reflines	count of lines shown at the end of file, if page-refresh is on

7.3.5 isdn.par

The *isdn.par* file configures special parameters to connect to the switch of PTT. This parameters are used to determine the right caller ID (CID telephone number of the user calling) and the right address extension (DDI = **D**irect **D**ial **I**n, digits after the normal telephone number of the primary interface).

Parameter	Meaning
.capi_callid_prefix	This parameter defines the caller ID prefix of the user's number. (Usually the 0 of the telephone number is not send by the switch. In this case this value can be set to 0).
.capi_subadd_ignore	Number of ignored digits to find the right DDI. Normally this value is set to the length of the telephone number (without country and area code) of ITK NetBlazer 8500 primary interface. Example: If the number of the interface is 0231/1234 then this value must be set to 4.
	If the ITK NetBlazer 8500 is connected to a PABX it might be that this value must be configured to 0.

Parameter	Meaning
.capi_subadd_cnt	The number of DDI digits of the address extension (Normally 2, Subaddress is in a range of 0 to 99).

7.3.6 auth.par

Compare with Chapter 7.6, *RADIUS* (page 7-23).

The *auth.par* file defines the authentication protocol which can be the RADIUS or the PSP protocol. Normally only RADIUS is needed for ITK NetBlazer 8500 three step authentication.

1. The ADNS (**A**uthentication **D**omain **N**ame **S**erver) is contacted by a client (ITK NetBlazer 8500) to find out which AS (**A**uthentication **S**erver) the client has to use (offline).
2. The AS is contacted by the client to authenticate the user's telephone number or parts of it (offline).
3. The AS is contacted by the client to authenticate the user's name and password (online).

The client is also called NAS (Network Access Server).

Usually only the second and third step are used.

The concept of ADNS is only needed in environments with multiple service providers.

Four inquiries can be sent to a RADIUS server from a client (ITK NetBlazer 8500).

In case of combination the test is ended after the first condition fits.

Each of the following character placed in the line *adns_req* / *auth_req* specifies an inquiry to the RADIUS server:

- A : The combination of caller ID (CID) and direct dial-in (DDI) is used
- B : Only the caller ID (CID) is used
- C : Only the direct dial-in (DDI) is used

- Z : The default entry is used

(CID = telephone number of the user dialing in)

(DDI = an extension to the dial-in number chosen by the user)

To configure a client only to use an AS, perform the following steps:

(1) To not use ADNS, configure:

```
.adns_prot:          NONE
```

```
.stab_adns_cnt:      0
```

(2) Configure the protocol to authenticate a user dialing in:

```
.auth_prot:          RADIUS
.auth_req:           BCZ     #Auth. Server Request Types
```

Service-Table-Entry for Authentication-Server (Offline):

```
.stab_offline_cnt:     1
.stab_offline_addr_1: $(RADIUS_SERVER)
```

Service-Table-Entry for Authentication-Server (Online):

```
.stab_online_cnt:      1
.stab_online_addr_1: $(RADIUS_SERVER)
```

Several entries for the authentication address are possible.

$(RADIUS_SERVER) is a free definable parameter which is defined at the beginning of this file (simply to replace the IP address).

Configuring ITK NetBlazer 8500 to use an ADNS

To use ADNS, define the IP address of the ADNS server in the last field:

```
.adns_prot:          RADIUS
```

```
.adns_req:              CZ

.stab_adns_cnt:         1

.stab_adns_addr_1:      $(RADIUS_SERVER)
```

The following lines are an example of entries delivered by the ADNS to the ITK NetBlazer 8500 in order to inform ITK NetBlazer 8500 how to inquire about the authentication server.

```
.auth_prot:    RADIUS
.auth_req:     BCZ      #Auth. Server Request Types
.stab_offline_cnt:1
.stab_offline_addr_1:$(RADIUS_SERVER)
```

Further it is possible to set for all Radius steps (ADNS, OFFLINE, ONLINE, LCR, ACCT) the RADIUS destination port and shared secret.

The default values are based on the following parameter macros:

for offline and online Radius server:	$(RADIUS_SERVER)	default: localhost
for all Radius secrets:	$(RADIUS_SECRET)	default: test
for Radius UDP ports:	$(RADIUS_ACCESS_PORT)	default: 1645

Shell login

The shell login doesn’t request a password if the password prompt is an empty string (Configured in auth.par or by RADIUS). In this case an empty password (null) string is used for authentication.

Accounting

The following configuration causes the ITK NetBlazer 8500 client to transmit the connection data between him and an user to an accounting server specified in the last line. This server writes the data into the following directory: /usr/adm/radacct/*clientname*

```
.acct_prot:          RADIUS

.stab_acct_cnt:      1

.stab_acct_addr_1:   183.88.100.77
```

Every connection between a RADIUS server (ADNS or AS) and a client (ITK NetBlazer 8500) must have an unique shared keyword. You have to configure this keyword at the client with the following line:

```
.radius_keyword: test
```

In this example the keyword is set to test. At the RADIUS server this keyword must be configured in the */etc/raddb/clients* file. For detailed information see Chapter 7.6, *RADIUS* (page 7-23).

All abbreviations used should be clear except *stab* (servicetable)

.stab_XXX_cnt: 1 means that one line with an IP addr. follows.

Changes only take effect if the software is restarted.

7.3.7 l2f.par

The goal of L2F is to separate the location of the initial dial-up NAS (**N**etwork **A**ccess **S**erver, for example a ITK NetBlazer 8500) from the location at which the dial-up protocol connection is terminated and access to the network is provided. In this way, users can dial into a NAS and gain access to their home networks. The home networks can then use their own methods of authentication, including security token, as well as filtering etc.

If an authentication entry enables L2F tunneling you have to set the following parameters in l2f.par of the NAS.

```
practrl.start_l2fd: 1
.SUPRIMO_nas_secret: test1
# NAS-Secret for Session with NAS-Name="SUPRIMO"
.ITK NetBlazer 8500_gw_secret:  test2
# Gateway-Secret for Session with NAS-Name="SUPRIMO"
```

The first entry starts the tunneling process (L2F daemon).

The next two entries specify the secret (password) for the L2F tunneling session. The tunnel name has to be defined in the radius database of the authentication server. The secret and the name must be known on the NAS side (**N**etwork **A**ccess **S**erver = begin of tunnel) and GW side (**G**ate**w**ay = Home Server = end of tunnel). Internally the identification is done via PAP, CHAP or SLIP.

With these methods, it is possible for users to authenticate at the ITK NetBlazer 8500 and have their authentication information forwarded to their home networks to prevent them from reauthenticating. L2F requires no change to PPP clients.

On demand of the authentication server the ITK NetBlazer 8500 tunnels the data to the corresponding home server, which handles the connection. The ITK NetBlazer 8500 drives only the link-portion of PPP and the home server handles the upper protocols. So the home server handles the authentication, assigns dynamic IP addresses and sends the resulting IP traffic to the home network.

L2F tunneling can be done between a L2F client (NAS, for example a ITK NetBlazer 8500) and a L2F server (home gateway) (for example a Cisco system). ITK NetBlazer 8500 can only be a L2F client.

The ITK NetBlazer 8500 implementation of L2F is based on UDP/IP.

The following figure gives an overview.

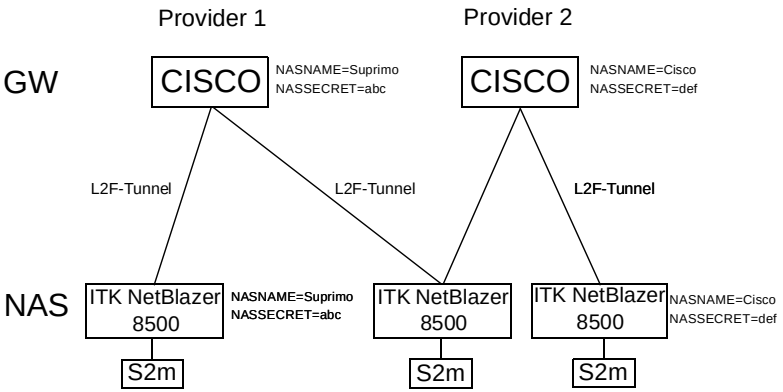


Fig. 7-1: L2F tunneling

The configuration of L2F tunneling is described in Chapter 7.6, *RADIUS* (page 7-23).

7.3.8 ppp.par

Use the *ppp.par* file to set the parameters for PPP and SLIP.

7.3.9 dlm.par

Use the *dlm.par* to set the parameters for Distributed Line Management (DLM).

7.3.10 cards.par

The parameter file cards.par is used by the card_config tool to set the parameters for communication cards and lines, ISDN-interfaces and voice compression boards. You find an example of cards.par in Appendix A.7, *All parameters from cards.par* (page A-74).

7.3.11 voip.par

In voip.par configuration parameter of ITK NetBlazer 8500 for voice over IP are specified.

Parameter	Meaning
.pcm_companding	voice (DSP) coding (a-law, µ-law)
.echo_canceller_flag	enable/disable echo cancellation
.vgi_accnt_l	maximum length of account code in voice guided input (IVR) including PIN
.vgi_pin_l	length of PIN (password) at end of account code (in IVR)
.vgi_autherr_max	max. number of authentication errors in IVR
.voip_lcr_ignore	ignore negative LCR answers
.vgi_timeout	timeout for IVR inputs (in milliseconds)
.voisam_*	sample files for messages used in IVR dialog
.stab_lcr_cnt	service table entry for LCR (number of LCR)
.stab_lcr_addr_1	IP Address of 1st LCR (one entry for each LCR)
.voicedialout_source_cnt	accept voice dialout requests from number of gateways (0 = accept from all gateways)
.voicedialout_source_1	IP Address of 1st gateway

Parameter	Meaning
.type_of_codec	Type of codecs supported by NetBlazer (default: G711:G723:G729)
.frame_size	frame size of codec (30 or 60 ms; default: 60 ms)

7.3.12 h323.par

In 323.par the parameters for the H.323 daemon (h323d) are configured. The H.323 daemon is used to realize call establishment by the ITU standard H.323 for Voice over IP. For details see chapter 7.7.3, *Configuring Voice over IP with H.323* (page 7-68).

Parameter	Meaning
h323d.use_gatekeeper	enable/disable the usage of a gatekeeper *0* = NOT using a gatekeeper *1* = Using a gatekeeper Note: If this parameter is *1* the parameter *h323d.ip_addr_gatekeeper* must be configured.
h323d.ip_addr_gatekeeper	If this parameter is left blank the h323d will try to find a gatekeeper by doing a RAS request broadcast. Alternatively you can configure the IP address of a known gatekeeper. In this case the h323d is trying to register itself at this gatekeeper by a RAS request. Example: h323d.ip_addr_gatekeeper: # Try to find a gatekeeper by broadcast or h323d.ip_addr_gatekeeper: 123.45.67.89 # IP address of gatekeeper

Parameter	Meaning
h323d.CountryCodeSubstitution	specifies a country code and the substitution digits for your system. If the country code digits are found in the calling number they are exchanged by the substitution specified. (e.g. *+49;0* leads to the result that country code '+49' is substituted by '0'*)*
h323d.PBXExternCallPrefix	Prefix for external calls using a PBX
h323d.AudioOnlyCallInternPrefix	Prefix for internal audio calls
h323d.AudioOnlyCallExternPrefix	Prefix for external audio calls
h323d.use_early_h245_tsap	Offer own H.245 IP address and port in the first SETUP message to open H.245 channel with first round trip. (no = 0/yes=1) (default = 1)
h323d.wait_for_remote_connect	Wait for CONNECT message from remote phone before opening H.245 channel. (parameter only supported after V5.00b2) (no=0/yes=1) (default: 0)
.spc_h323_setup	controls, which connection setup protocol should generally be used: 0 = use SPC 1 = use H.323
.voip_lcr_min_digits	minimal amount of digits collected before the first LCR request is done (Default: 3).

7.3.13 iss.par

In iss.par the parameters for the ISS daemon (ISSD) are configured. The ISS daemon is used to coordinate the ISS communication. For details and how to configure the ISS feature see chapter 7.11, *Internet Supplementary Services (ISS)* (page 7-96).

Parameter	Meaning
.start_iss	1= start ISS-Daemon, 0: do not start ISS-Daemon
.iss_uip_pool	IP-Pool-ID for ISS IP addresses of EWSD
.linecnt_isdn_ll	Parameter for ISS leased lines processes (LLP): Number of lesed lines (PRI links to EWSD)
.isdn_ll_1.service	Parameter for ISS leased lines processes (LLP): Service of 1st leased line
.isdn_1.controller	Parameter for ISS leased lines processes (LLP): Controller of 1st leased line
.isdn_ll_2.service	Parameter for ISS leased lines processes (LLP): Service of 2nd leased line
.isdn_ll_2.controller	Parameter for ISS leased lines processes (LLP): Controller of 2nd leased line

7.3.14 misc.par

Use the *misc.par* file to enter the license keys and to override parameters from *common.par* which are not set in the previously described files.

A list of important parameters is given in the Chapter 7.4, *Important parameters* (page 7-19).

7.4 Important parameters

All configurable parameters are described in the online helptexts of web-Man configuration.

List of important parameters (which can for example be set in *misc.par*)

Parameter	Meaning
.LICENSE_KEY_xxx	License keys for the major features of ITK NetBlazer 8500 (RAS, VOICE, ISS, see chapter 8.5.10, *Licenses* (page 8-46))
.practrl.max_temp	maximum temperature; when reached an SNMP trap is sent
.pra_language	language for the interactive managing program *pramon*. E = English, D = Deutsch (normally in *misc.par*)
.ppp_adrprompt1	Message to tell a SLIP client the server IP address.
.ppp_adrprompt2	Message to tell a SLIP client his IP address.
.ppp_dns1: 0.0.0.0	set primary DNS server address (for 0.0.0.0 put in the correct value) Set this parameter in *ppp.par*.
.ppp_dns2: 0.0.0.0	set secondary DNS server address (for 0.0.0.0 put in the correct value) Set this parameter in *ppp.par*.
.start_delay	Delay before sending/receiving data begins (in milliseconds). This is useful if a client is not fast enough to receive the first message.
.port_limit	This parameter defines the maximum number of simultaneous connections of one user to ITK NetBlazer 8500. If one is not allowed to dial-in ITK NetBlazer 8500 twice, set this value to one.

Parameter	Meaning
.subnetting	If subnetting is used for the dynamic IP address pool set this value to one.
.session_timeout	This value defines the maximum time of a session (in milliseconds) before it is closed. A value of 0 disables the option.
.idle_timeout	Maximum idle time per user (in milliseconds). This value is used to disconnect a user after xx milliseconds idle time.
.shell_banner	This defines the banner in case of a login screen.
.shell_usernameprompt	This defines the login prompt in case of a login screen.
.shell_passwordprompt	ditto for the password prompt.
.shell_prompt	ditto for the shell prompt.
.shell_welcomemsg	Welcome message in case of a successful login.
.set_static_routes	enables/disables the automatic setting or deleting of the routing entries for static UIP addresses.

7.5 Defining packet filters (firewalling)

Packet filters are used for security. A packet filter is used to determine whether an IP packet coming from a user is passed or not. As many IP packet filters as necessary can be configured on the client (ITK NetBlazer 8500).

It is very important to define these filters correctly to reach a maximum level of security.

You configure a packet filter in a file with:

/u/pra/dat/firewall_X

whereby X can be alphanumeric.

For example:

```
/u/pra/dat/firewall_group1
```

In the */u/pra/dat* directory there is also a file called *firewalldefault*. If no corresponding firewall file is found for a user, this file will be used. This means that this file should have a definition of a packet filter with a maximum level of security.

The extension (X) of the firewall file can be assigned to a certain user in the RADIUS database. For detailed information see Chapter 7.6, *RADIUS* (page 7-23).

A line in a firewall file has the following form:

```
(+/-) <IP address> <netmask> <TCP port> <UDP port>
```

(+/-) means whether the IP packet is passed (+) or not (-).

<IP address> and <netmask> create the IP pool that is allowed(+) or forbidden(-) for the users IP packet.

<TCP port> specifies the service a user belonging to this firewall may use. This field can be set to the keywords *ALL*, *NONE* or to a range of TCP ports such as *23-45*.

<UDP port> is the same as described above for <TCP port>.

To check a rule:

1. The users IP address is "anded" with the netmask and compared with the rule IP address. If TRUE go to step 2. If this rule doesn’t fit go to step 4.
2. The TCP or UDP portnumber is compared with the defined ones. If TRUE go to step 3; if this rule doesn’t fit go to step 4.
3. If (+) is defined then this IP packet is passed. If (-) is defined, it is si-

lently discarded.

4. The next line in the firewall file is checked beginning with step 1.

If a rule fits the checking is stopped.

The last line should always be the default rule (see example below).

If you are worried about the performance of ITK NetBlazer 8500 in case of firewall files with many rules, please note that a check of an IP packet is only carried out when the IP address or the port number differs from the last one.

Example

A firewall file might look like this:

```
+ 123.12.1.0 255.255.255.0  ALL    ALL
- 124.45.3.0 255.255.255.0  ALL    ALL
+ 123.4.4.1  255.255.255.255 23-23 NONE
- 0.0.0.0    0.0.0.0        ALL    ALL
```

- The first line defines a class C network 123.12.1.0 all TCP and UDP ports are allowed.
- The second line defines also a class C network but all TCP and UDP ports are forbidden.
- The third line defines only one host 123.4.4.1 with the TCP port 23 (telnet). That means that a user dialing in can telnet this host but nothing else.
- The last line defines a negative filter for the rest of the world.
- Do not forget to forbid the ITK NetBlazer 8500 itself and the IP address of the UIP device:

Example

```
-192.168.40.10  255.255.255.255 ALL ALL   #ITK NetBlazer 8500
-192.168.18.254 255.255.255.255 ALL ALL   #UIP device
```

Unknown IP protocols in packetfilter (firewall)

A parameter determines if unknown IP protocols are discarded (default) or are handled like ICMP packets and may pass the firewall.

Normally all IP packets with a protocol value unequal to ICMP, UDP or TCP are always discarded. If the parameter ".fw_unknown_prot" (e.g. in misc.par) is set to "PASS" these IP packets may pass the firewall according to the ICMP filter rules.

Examples:

```
.fw_unknown_prot: REJECT     # Always reject unknown IP protocols

.fw_unknown_prot: PASS       # Unknown IP protocols may pass the
                             # firewall according to the filter rules
```

7.6 RADIUS

This chapter describes the RADIUS protocol and the special needs when using ITK NetBlazer 8500 with the RADIUS authentication.

Compare with Chapter 7.3.6, *auth.par* (page 7-9).

Chapter 7.6.6, *Table of actions* (page 7-35) describes how to configure the users/customers data.

Examples for the various configurations are shown in Chapter 7.7.1, *Examples of RADIUS files* (page 7-59).

7.6.1 Introduction

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice; RFC 2058/2138) is a protocol designed to authenticate a user's dialing in. If a user dials in, ITK NetBlazer 8500 determines the user data (caller ID, username and password) and contacts the RADIUS server to obtain an authentication of the data.

The RADIUS server can be reachable by UDP anywhere in the network or it can even be on the same machine.

RADIUS uses attributes. Each attribute can have a value defined by the operator. ITK NetBlazer 8500 uses these attributes to configure a specific session.

No complicated configuration is necessary to install an authentication server. This feature is included in the ITK NetBlazer 8500 software.

To install an authentication server, perform the following steps:

(1) List the RADIUS clients (ITK NetBlazer 8500) in a certain file.

The RADIUS daemon will be started automatically.

(2) Define the users/customers data such as password etc.

RADIUS defines an amount of standard attributes which are described below. For special purposes ITK has defined ITK specific attributes to meet the advanced features of ITK NetBlazer 8500.

7.6.2 RADIUS daemon

To support the new requirements of the LCR request the delivered RADIUS daemon (radiusd) has been enhanced as follows (all changes concern only the LCR request and are not usable for other RADIUS requests):

- **Wildcard:** The wildcard character '*' can be used at the end of the defined destination number to correspond to all destination numbers that start with the defined number.

  Example:
  The following entry corresponds to all 1800 (US toll free) numbers:

  %1800* User-Password="LCR"

- **Adjusting the destination number:** The destination number must be adjusted in some cases: i.e. if the dialout gateway is connected to a PBX it may need a prefix digit to dial out to the PSTN.
  To **add digits** to the destination number the attribute „ITK-Dest-No" must be set to a value of the form „**+XXX**". The digits XXX are inserted at the beginning of the destination number.
  To remove digits from the beginning of the destination number the attribute „ITK-Dest-No" must be set to a value of the form „**-N**". The 1st N digits at the beginning of the destination number are removed.
  In both cases the RADIUS daemon returns the complete (modified)

destination number back to the requesting gateway.
Both adjusting mechanisms can be combined (e.g. „-2+0" removes 2 digits and adds a prefix of '0' afterwards.)

All RADIUS entries are searched sequentially, and the search stops at the 1st fitting entry. So care must be taken with defining LCR entries that contain wildcards.

Example:

```
%00*          # all foreign calls from Germany
%001*         # Calls from Germany to US
```

In this example the 2nd entry will never be used because for all foreign calls the 1st entry fits.

See Chapter 8.5.6, *Installing RADIUS server* (page 8-38) for further information.

7.6.3 Common attributes

In this chapter the common attributes used by ITK NetBlazer 8500 are described. All attributes are listed in Appendix A.5, *Supported RADIUS attributes* (page A-30).

Attribute	Meaning
Service-Type	The type of service configured for this user. This value can be for example: **Framed**: A user logs in with PPP or SLIP. **NAS-Prompt**: A user needs a login screen for login. **ITK-Voice-over-IP-Comp:** Use VoIP with compression **ITK-Voice-over-IP:** Use VoIP without compression
Framed-Protocol	The protocol used for this user: PPP, SLIP or CSLIP
Framed-IP-Address	A static IP address can be defined for the user

Attribute	Meaning
Filter-Id	This string defines the extension to the firewall file. For example if the filter Id = "12" the */u/pra/dat/firewall_12* file will be used for this connection.
Login-Service	The service which is switched on for example: **TCP-Clear**: open a transparent TCP connection. **telnet**: open a telnet session
Login-IP-Host	IP address of the server for telnet or TCP-clear connection.
Login-TCP-Port	The TCP portnumber for TCP-clear connections
Port-Limit	The number of ports are allowed for one user. This value should be set to 1 in the case of static IP address assignment.

The Service-Type „ITK-Voice-over-IP“ configures VoIP without compression and without echo cancellation and runs only on the ISDN board (without a DSP board). It is UNSUPPORTED and should only be used for demonstration or testing purposes because it has a lot of disadvantages:

- no compression (needs 64 kbit/s bandwidth)
- no echo cancellation
- high cpu load (only about 20 connections in one system)

Some RADIUS attributes have been renamed to comply with RFC2058 (**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice (RADIUS)) and RFC2059 (RADIUS Accounting). All old names are still supported and need not be changed.

Changes

Old Attribute	New Attribute
Password	User-Password
NAS-Port-Id	NAS-Port
Login-Port	Login-TCP-Port

Port Number

The UDP ports to use for RADIUS authentication and RADIUS accounting requests can be changed with the ITK NetBlazer 8500 parameters *radius_access_port* and *radius_accounting_port*.

The default values comply to the RADIUS RFC2058 (1645 for authentication and 1646 for accounting).

To use the new RADIUS RFC2138 ports the parameters must be changed to

radius_access_port=1812

radius_accounting_port=1813

The radius daemon uses the UDP ports specified in the */etc/services* file.

NAS-Port

This attribute indicates the physical port number of the NAS and is used in all requests. Because ITK NetBlazer 8500 has no physical port number the dynamic **C**onnection **T**able **E**ntry (CTE) is used as value for the NAS-Port.

NAS-Port-Type

Set this attribute in the online authentication requests and in accounting to differentiate between ISDN and modem calls.

The values used for *NAS-Port-Type* are:

- ASYNC for modem connections
- ISDN_SYNC for ISDN connections with synchronous protocols (HDLC and X.75)

- ISDN_ASYNC_V110 for ISDN connections with asynchronous protocols (V.110)

A complete listing with all parameters is given in Appendix A.5, *Supported RADIUS attributes* (page A-30).

7.6.4 Special ITK NetBlazer 8500 attributes

In this section all attributes defined by ITK are described. All special entries begin with *ITK-*.

Attribute	Meaning
ITK-Auth-Serv-IP	This entry is used for ADNS and defines the IP address of the authentication server ITK NetBlazer 8500 must use for the next authentication steps
ITK-Auth-Serv-Prot	This attribute tells ITK NetBlazer 8500 which authentication protocol is used for the next steps. (Normally RADIUS).
ITK-Provider-Id	This attribute defines the identifier of the provider the user belongs to. This identifier can be used for specific operations of a provider.
ITK-Usergroup	This attribute defines an identifier of a usergroup the user belongs to. The identifier will be used in conjunction with the ITK-Provider-Id for user specific operations.
ITK-Users-Default-Entry	This attribute defines the username of the default attribute section for the offline authentication.
ITK-Users-Default-Pw	This attribute defines the password of the default attribute section for the offline authentication.

Attribute	Meaning
ITK-Banner	This attribute defines the first text which is displayed to the user when a ITK NetBlazer 8500 Login is selected. VoIP: *IVR*: enable IVR with block dialing *IVR_DYNDIAL*: enable IVR with dynamic dialing OSD: enable OSD with block dialing *OSD_DYNDIAL*: enable OSD with dynamic dialing *RECORD*: Allows recording of new voice files (see chapter 7.7.4, *Transparent Connection Setup* (page 7-71)
ITK-Username-Prompt	This attribute defines the username prompt which is displayed to the user when a ITK NetBlazer 8500 Login is selected. VoIP: Specifies the name of the voice file for 'prompt for account code'.
ITK-Password-Prompt	This attribute defines the password prompt which is displayed to the user when a ITK NetBlazer 8500 Login is selected. VoIP: Specifies the name of the voice file for 'prompt for destination number'.
ITK-Welcome-Message	This attribute defines the welcome message which is displayed to the user after a successful login when the ITK NetBlazer 8500 shell is selected. VoIP (IVR): Specifies the name of the voice file for 'welcome message'. VoIP (RECORD): Specifies the name of the voice file for 'prompt for voice recording'.

Attribute	Meaning
ITK-Prompt	This attribute defines the command prompt which is displayed to the user when the ITK NetBlazer 8500 shell is selected. VoIP (IVR): The value is used to locate the voice files. The ITK NetBlazer 8500 already contains voice files in german and english, that can be selected with the values 'e' (for english) and 'd' (for german). VoIP (RECORD): Specifies the name of the voice file for the recording (output).
ITK-IP-Pool	This attribute defines an identifier of an IP pool from which an IP address will be assigned for the user. These pools have to be configured locally on the ITK NetBlazer 8500 in the file */u/pra/dat/uip_pool.par*.
ITK-Tunnel-Prot	This attribute defines the tunneling protocol (L2F).
ITK-Tunnel-IP	This attribute defines the system to which the user IP packets must be forwarded via an IP tunnel (home gateway). VoIP: Specifies the address of the dial-out gateway to use.
ITK-Acct-Serv-IP	This attribute defines the system to which the accounting data has to be sent.
ITK-Acct-Serv-Prot	This attribute defines the accounting protocol.
ITK-Filter-Rule	This Attribute indicates one entry of the filter list for this user. Identifying a filter list by a sample of rules allows the filter to be used on different NASes without local databases.

Attribute	Meaning
ITK-Channel-Binding	This attribute defines whether one of the reserved channels configured in */u/pra/dat/process.par* can be assigned to the user. Otherwise the user will be rejected if the number of unprivileged channels is exhausted.
ITK-Start-Delay	This attribute defines the delay in seconds before sending/receiving data.
ITK-NAS-Name	This attribute contains a string identifying the NAS. It is used for example to identify the NAS on the remote end in a tunneling protocol like L2F.
ITK-ISDN-Prot	This attribute indicates the B channel protocol. It should be used for outgoing calls. Possible values are given in the appendix.
ITK-PPP-Auth-Type	This attribute indicates the type of authentication via PPP.
ITK-Ftp-Auth-IP	This attribute defines the hostname or IP address of a FTP server that has to be used for online authentication.

Attribute	Meaning
ITK-Auth-Req-Type	This attribute defines the authentication request type, to use for the offline authentication. This is normally configured with the ITK NetBlazer 8500 *.auth_req* parameter, but can be selected also with this *ITK-Auth-Req-Type* RADIUS attribute. The mechanism to build the authentication request from caller ID and DDI remains the same: The request type is built up from a typed string. Each character in the request type specifies one request, which is formatted in the following way: A : The combination of caller-ID (CID) and direct-dialin (DDI) is used B : Only the caller-ID (CID) is used C : Only the direct-dialing (DDI) is used Z : The DEFAULT entry is used The first request that gives a positive answer terminates the offline authentication.
ITK-Dialout-Type	This attribute indicates the type of dial-out.
ITK-Modem-Pool-Id	Specifies the ID of the modem pool to use for the call. One free modem out of the specified modem pool is used for the call. If a special value of *1000* is used for the modem pool ID the controller number of the ISDN board is used as the modem pool ID.
ITK-Modem-Init-String	Specifies the modem init string that is used to initialize the selected modem on the ITK MultiModem board. The init string must specify a valid Rockwell command.

Attribute	Meaning
ITK-PPP-Client-Server-Mode	Specifies if the PPP software runs in PPP server (default) or PPP client mode for the connection. The following values are possible: • ITK-Mode-Server: In PPP server mode the connection setup must be initiated from the remote user (default) • ITK-Mode-Client: In PPP client mode the connection setup is initiated from ITK NetBlazer 8500 (necessary for some LAN-to-LAN connections).
ITK-PPP-Compression-Prot	Specifies a ':'-separated list of allowed ppp-compression-protocols, which can be defined in the ADNS and offline authentication steps. Possible compression protocols: STAC: STAC LZS Compression Protocol (RFC1974) PRED1: PPP Predictor type 1 Compression Protocol (RFC1978)
ITK-Username	Specifies an alphanumeric username for calls that are authenticated by caller-id. So far the caller-id (with a '%'-prefix) has been used as the username. Now a readable username is seen in *pramon*, webMan and accounting. On some Basic Rate Interfaces both B channels have different caller-id's. Normally the two possible connections from these interfaces cannot be bundled together, when authenticated by caller-id (in offline-authentication). Now these two different caller-id's can be mapped to one single alphanumeric username and a channel bundling will be possible.

Attribute	Meaning
ITK-Dest_No	This attribute defines the phone number that the user called. VoIP: Force an automatic connection setup to the specified destination number.
ITK-DDI	This attribute defines the Direct Dialling In (DDI) that the caller dialed.

A complete listing with all parameters is given in Appendix A.5, *Supported RADIUS attributes* (page A-30).

7.6.5 Special dial-in entries

Which of the following possible entries are selected to authenticate is laid down in the clients (ITK NetBlazer 8500) parameter file *auth.par*. For detailed information see Chapter 7.3.6, *auth.par* (page 7-9).

Assignments of requests and passwords:

Request	Password
Z	-SUPRIMO (DEFAULT entry)
C	-DIRECT_DIAL (DDI)
B	-ISDN_ADDRESS (CID)
A	-USER_DIAL (DDI + CID)

Sample RADIUS database

A sample for the RADIUS database is given in Appendix A.5, *Supported RADIUS attributes* (page A-30). A sample user's database is delivered with the ITK NetBlazer 8500 software.

7.6.6 Table of actions

For most of the following actions you will make entries in the user database.

User Database

The user database is located in */etc/raddb/users* on the RADIUS server.

There are four kinds of possible entries:

Compare Appendix A.4, *RADIUS authentication file "users"* (page A-23).

- ADNS Entries used for ADNS servers
- AUTH Entries used for AUTH servers to identify a caller
- AUTH Entries used for AUTH servers to authenticate name and password (Default Entry)

The first two entries are expansions of ITK NetBlazer 8500 while the last one is the usual standard entry.

You have to separate all attributes except the last one and the password by commas.

You have to separate all entries with a blank.

7.7 Configuring ITK NetBlazer 8500 features

What to do	How
Defining packet filters (firewalling)	configure a packet filter in a file: /u/pra/dat/firewall_X X can be alphanumeric and can be assigned to a certain user in the RADIUS database (Attribute Filter-Id). If no corresponding firewall file is found, the *firewalldefault* file in the same directory will be used.

What to do	How
Declaring RADIUS clients	configure each RADIUS client in the following file: /etc/raddb/client The first entry is the IP address of the RADIUS client (normally a ITK NetBlazer 8500) and the second entry is the RADIUS keyword which must match with the entry *.radius_keyword: test* of the ITK NetBlazer 8500 client in the following file: /u/pra/dat/auth.par There is no limit to defining clients. For detailed information see Chapter 7.3.6, *auth.par* (page 7-9). For an example see Client's declaration (page 7-59).
Starting RADIUS Daemon automatically	log in as superuser and type the following command: cp /etc/radius/S95ITK_AS /etc/rc2.d
Starting RADIUS Daemon manually	log in as superuser and type the following command: /etc/radius/S95ITK_AS
ADNS authentication offline	entry in user database in */etc/raddb/users*: %ADNS_YY Password="DIRECT_DIAL" This informs the client (ITK NetBlazer 8500) that for all users with the defined DDI the defined authentication server has to be contacted via RADIUS. All possible values are listed in Appendix A.5, *Supported RADIUS attributes* (page A-30). For an example see ADNS authentication, offline (page 7-59).

What to do	How
ADNS authentication, enabling L2F tunneling	entry in user database in */etc/raddb/users* Configure NAS-Name and NAS-Secret in *l2f.par*, see Chapter 7.3.7, *l2f.par* (page 7-13). In case of an ADNS request, the asking client (NAS) is instructed to build up a connection to a certain computer (usually a provider in a multiprovider network, home server). The authentication can take place either on- or offline. For an example see ADNS authentication, enabling L2F tunneling (page 7-59).
Authentication via CID	entry in user database in */etc/raddb/users*: %xxxx_ User-Password=“ISDN-ADDRESS“ or %xxxx_ YY User-Password=“USER_DIAL“ This informs the client (ITK NetBlazer 8500) that a user being identified with the defined telephone number (caller ID) has to be connected via PPP and that the packet filter with the defined ID has to be used. For additional information see Chapter 7.3.6, *auth.par* (page 7-9), Auth-Type “A“ For an example see Authentication via CID (page 7-60).
	Using the CID (password: *ISDN-ADDRESS*) or the combination of CID+DDI (password: *USER_DIAL*) no online authentication takes place **but** if only DDI (password: *DIRECT_DIAL*) is used as below the online authentication follows.

What to do	How
Authentication via DDI	entry in user database in */etc/raddb/users*: %_YY User-Password="DIRECT_DIAL" This informs the client (ITK NetBlazer 8500) that a user being identified with the defined extension address has to be connected via the defined protocol and the packet filter with the defined ID has to be used. For an example see Authentication via DDI (page 7-60).
Authentication with connection type	To differentiate between ISDN and modem calls, the RADIUS attribute *NAS-Port-Type* is used in online authentication requests and accounting. This can be used to allow some users access only with modem and others only with ISDN connections. The used values for *NAS-Port-Type* are: • ASYNC for modem connections • ISDN_SYNC for ISDN connections with synchronous protocols (HDLC and X.75) • ISDN_ASYNC_V110 for ISDN connections with asynchronous protocols (V.110)
Intruder Recognition and Alarm	The *PRACTRL* control process counts the number of authentication failures that have appeared in the last M minutes (configurable). A snmp trap is generated if more than one configured number of authentication errors is recognized. To enable the intruder recognition you have to set the following parameters: practrl.check_auth_errors: time interval to keep errors (in minutes); if not defined (default) no intruder recognition is done practrl.trap_auth_errors: send trap after this number of auth errors

What to do	How
Online authentication with FTP server	The flexible authentication is extended by the possibility of querying a standard FTP server in the online authentication step. If the FTP server allows access, the user is authenticated, otherwise the connection is aborted. Any FTP server that conforms to RFC959 can be used as an authentication server. To configure a FTP server as a 2nd authentication server, set the following parameters: 1. If all users to be authorized by the FTP server, are defined in the RADIUS users file (without a configured password) the RADIUS attribute *ITK-Ftp-Auth-IP* must be set for these users. The value of this RADIUS attribute must be the hostname or IP address of the FTP server. 2. If the users to be authorized by the FTP server are not defined in the RADIUS users file (or are configured with the wrong password) an ITK NetBlazer 8500 parameter can be set to configure a general FTP server authentication after a failed RADIUS online authentication. The *.ftp_auth_addr* parameter must be set to the hostname or IP address of the FTP server. For authentication checks with the FTP server you have to know the user password in readable form. The CHAP authentication protocol cannot be used, because it encrypts the password. You should set the RADIUS parameter *ITK-PPP-Auth-Type* to *ITK-Auth-PAP* to enforce PAP. For an example see Online authentication with FTP Server (page 7-60).

The dialog with the FTP server can be configured with the following parameters:

Parameter	Meaning
.ftp_accept_count	specifies the number of special accept messages from the FTP server that allow the user access (positive-list)
.ftp_accept_N	specifies the n-th accept message
.ftp_timeout	specifies the maximum time (in ms) to wait for answer messages from the FTP server

What to do	How
Select Modem Pool	entry in user database in */etc/raddb/users* RADIUS attribute: *ITK-Modem-Pool-Id* To configure a modem board into a different modem-pool, enter the pool ID in the *cards.par* parameterfile (default: *modem-pool-id: 0*). This entry specifies the ID of the modem pool to use for the call. One free modem out of the specified modem pool is used for the call. If different modem boards are installed in an ITK NetBlazer 8500, the modems of these boards can be configured into different modem pools. The flexible authentication can be used to specify (for example by DDI specific) which modem type (out of which modem pool) should be used for a modem call.

What to do	How
Initialize Modem	entry in user database in */etc/raddb/users* RADIUS attribute: *ITK-Modem-Init-String* Different modem init strings can be configured depending on the flexible authentication (for example DDI specific). For example, the modem training can be configured to start at 9.600 bps instead of 33.600 bps, tuning the modem connect times. The RADIUS attribute *ITK-Modem-Init-String* must be set to the corresponding modem init string, which must be given in Hayes AT command syntax. This feature is possible only with ITK MultiModem boards now. The init strings must specify valid Rockwell command strings.

What to do	How
Configuring Callback	entry in user database in */etc/raddb/users* If a user with the defined caller ID is recognized, ITK NetBlazer 8500 rejects the call and calls back (ITK-Dialout-Type = ITK-Callback). The same effect is achieved if the attribute *Service-Type = Dialback-Framed-User* is set. Then the *ITK-Dialout-Type* attribute can be omitted. If the ISDN B channel protocol is not specified, an automatic protocol recognition with fallback mechanisms will be carried out, but this does not work with all user software. The connection setup with a specified protocol is faster. If the dial number for the callback is not identical to the incoming caller ID, the callback number can be specified with *Callback-Number = ...* . This may be necessary if the ISDN switch or the PBX interface is not configured correctly. The user software must be able to initiate an outgoing call and accept an incoming call. This mechanism has been successfully tested with *ITK Columbus Pro* (formerly called *ITK connect/WS*). **Callback for modem** If the caller ID number is obtained from the carrier for modem calls, the offline authentication is carried out now before the connection is accepted (before the modem training). This tunes the modem callback in time (only one modem training) and costs (no connection setup cost for caller). All possible values are listed in Appendix A.5, *Supported RADIUS attributes* (page A-30). For an example see Configuring Callback (page 7-61).

What to do	How
Configuring Callout / Recall	entry in user database in */etc/raddb/users* For an efficient (active) Short Hold, the ITK NetBlazer 8500 is able to dial-out to a user if IP traffic has to be sent to this user. These dial-out features allow the ITK NetBlazer 8500 to call out. If an IP packet from the Intranet/Internet LAN arrives at the ITK NetBlazer 8500 and no connection to the corresponding user is active, an outgoing connection to the remote user is established. There are two possible dial-out types: 1. **Callout**: dials to the user to establish an outbound connection (charging applies at ITK NetBlazer 8500 site) 2. **Recall**: dials to the user just to 'awake' his client software which must reject the call and calls back to ITK NetBlazer 8500 (charging applies at user site) The dial-out works with static IP addresses and dynamic IP pools. The Callback feature can be combined with the Callout feature and is ideally suited for home offices. The complete charging (for incoming and outgoing calls) is applied at the ITK NetBlazer 8500 site. **Callout / Recall for modem** To enable the dial-out (Callout and Recall) for modem you have to start the *pstn_out* process by setting the ITK NetBlazer 8500 parameter *.linecnt_pstn_out* (in *process.par*) to the maximum number of outgoing modem connections. The mechanisms to enable dial-out for modem are the same as for ISDN connections. For an example see Configuring Callout (page 7-61).

Distributed Dial-out

The Distributed Dial-out is necessary if multiple ITK NetBlazer 8500s are configured in one ISDN hunting group. All these partner ITK NetBlazer 8500s can be used for a dial-out. If the ITK NetBlazer 8500 that should dial-out to the user has not enough resources (B channels) to make the call (for example all B channels are used) another ITK NetBlazer 8500 with free resources is searched for. All partner ITK NetBlazer 8500s (ITK NetBlazer 8500s that are in the same defined group) are asked for their resources and the one with the highest count of available resources is asked to make the dial-out. The callout to the remote user (and the incoming call from the user after a recall) must be tunneled to the home server ITK NetBlazer 8500 as described in the section *Distributed Line Management* (page 7-47).

What to do	How
Distributed Dial-out	To enable the dial-out feature set the following parameter in the *misc.par* file: .dialout:1#enable dialout additional parameters: .ignore_packet_time This prevents a callout burst for dial-out to an unreachable remote user. Specifies the time within further dial-outs to the same user (IP address) are not initiated. (normally set to 10 sec) .callout_tmo specifies the time after which a dynamic IP address expires (no callout will be done, if this IP address is not used in this time). (normally set to 1 hour)

What to do	How
Configuring Distributed Dial-out	Configure Partner ITK NetBlazer 8500 in *misc.par* file: .partner_cnt: N # number of partner ITK NetBlazer 8500 .partner_1: 1.2.3.4 # IP adress of 1st other ITK NetBlazer 8500 .partner_2: 5.6.7.8 # IP adress of 2nd other ITK NetBlazer 8500

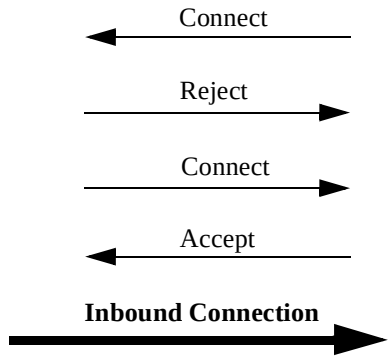
Actions on dial-out

1. An IP packet that has no active connection (checked with the IP address of the next hop) arrives in the ITK NetBlazer 8500 (in the SNS).
2. The SNS (**S**uprimo (ITK NetBlazer 8500) **N**ame **S**ervice) searches for this IP address in the IP pool (dynamic IP addresses). If it is found and the dial-out type is set for this entry, the SNS gets the caller number from this IP pool entry and initiates a dial-out for this dynamic IP address (see point 4. below).
3. If the IP address is not in the IP pool, the SNS asks the authentication server (RADIUS) for the caller number and starts a dial-out for this static IP address.
4. If the local ITK NetBlazer 8500 has available resources (B channels) the dial-out is made from process *isdn_out*.
5. If the local ITK NetBlazer 8500 does not have enough resources (free B channels), the SNS asks other ITK NetBlazer 8500 in the same group for free resources and one of these starts the dial-out (process *isdn_out*).

Dial-out types

The following chart gives an overview of the dial-out types explained above:

Connection Flow	Remarks
User **ITK NetBlazer 8500**	
ITK Callback: Connect → ← Reject ← Connect Accept → **Outbound Connection** ←	An incoming call will be rejected and the user is called back.
ITK Callout: ← Connect Accept → **Outbound Connection** ←	The ITK NetBlazer 8500 dials to an user to establish an outbound connection

Connection Flow	Remarks
ITK Recall:  	The ITK NetBlazer 8500 dials to an user just to 'awake' his client software which must reject the call and calls back to the ITK NetBlazer 8500. No outbound connection is established.

Distributed Line Management

Distributed Line Management guarantees that in a multiple access system a reactivated connection to or from a user is established with the same IP address as before, independent of which ITK NetBlazer 8500 calls out or accepts the call.

A client has dialed in the Home Agent and built up a TCP/IP connection which is presently physically down. If the connection is reactivated, the client is authenticated (on- or offline) by an authentication server that contains the following entry. Than the client is connected to a different ITK NetBlazer 8500 (called Access Agent) as before, the Access Agent builds up a tunnel via the ITK-EMAS process (**E**xtended **M**ultiple **A**ccess **S**ystem based on the SPC protocol). The Home Agent assigns the previously used IP address and the user is logically connected to the application server as before. The Access Agent drives the lower PPP protocols (for example LCP, PAP/CHAP) and the home server ITK NetBlazer 8500 drives the upper PPP protocols (IPCP).

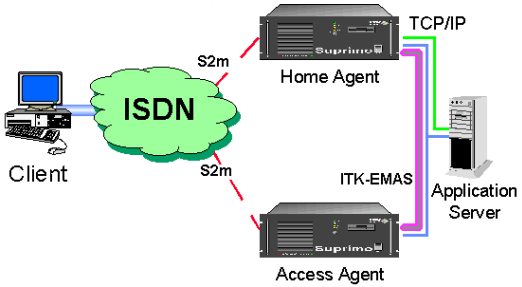


Fig. 7-2: Multiple Access System

What to do	How
Configuring Distributed Line Management	entry in user database in */etc/raddb/users* define maximum number of tunnel connections with the *.linecnt_emas* parameter in *process.par* The *ITK-Tunnel-IP* attribute indicates the home server to which the user IP packets must be forwarded via tunneling. The tunneling protocol is set by the attribute ITK-Tunnel-Prot. For Distributed Line Management it is called ITK-EMAS (**E**xtended **M**ultiple **A**ccess **S**ystem). The process which handles the connection on the home server is also called EMAS and can be seen in the connection table of the *pramon* and in the accounting file. For an example see Configuring Extended Shorthold (page 7-63).

Distributed Multilink PPP (MP)

The PPP Multilink Protocol (RFC1990) allows the bundling of multiple channels in order to increase the bandwidth. ITK NetBlazer 8500 allows the bundling of ISDN and Modem links independent of which ITK NetBlazer 8500 the links arrive at through the EMAS concept (**E**xtended **M**ultiple **A**ccess **S**ystem). See *Distributed Line Management* (page 7-47).

All new incoming links of the same user are tunneled via SPC (**S**uprimo (ITK NetBlazer 8500) **P**rocess **C**ommunication) from the incoming ITK NetBlazer 8500 to the Home Gateway ITK NetBlazer 8500. There the EMAS process for this user accepts the new links and keeps a list of all active links. The EMAS process reassembles the PPP frames, that are received through the different links, and sends the resulting IP packets to the LAN. IP Packets received from the LAN are packaged into PPP and split into several PPP fragments that are sent over the active links.

What to do	How
Propagation of DNS Address	The implementaion of RFC1977 PPP Internet Protocol Control Protocol Extension for Name Server Addresses allows to propagate the IP addresses of a primary and alternate (secondary) DNS from the ITK NetBlazer 8500 to the TCP/IP client software of the remote user. This makes the configuration of the user software easier, where now only the number of the ITK NetBlazer 8500 and user/password must be entered. Set the following ITK NetBlazer 8500 parameters with the correct values (normally in *ppp.par*): • .ppp_dns1: 0.0.0.0 # Primary DNS Server Address • .ppp_dns2: 0.0.0.0 # Secondary DNS Server Address

What to do	How
Distributed Multilink PPP (MP)	entry in user database in */etc/raddb/users* ITK NetBlazer 8500 accepts MP connections only if MP is activated and if it is supported and negotiated by the client software. To enable MP set the RADIUS attribute *Framed-Protocol* to *MP* (instead of *PPP*). You can do this at the Offline Authentication or in the DEFAULT entry of the RADIUS users file (not in Online Authentication). You can see the IP traffic and the number of active links of a MP connection with the *pramon* tool in the corresponding EMAS process. The maximum number of EMAS processes on one ITK NetBlazer 8500 must be set with the ITK NetBlazer 8500 *.linecnt_emas* parameter. The maximum number of channels which one user can use simultaneously is specified by the ITK NetBlazer 8500 *.port_limit* parameter (global value) and/or by RADIUS configuration (*Port-Limit* attribute). If the RADIUS *Framed-Protocol = MP* attribute is set in the DEFAULT entry of the RADIUS users file, all users can use MP if the ITK NetBlazer 8500 *.port_limit* parameter is > 1. This parameter can be overwritten by the RADIUS *Port-Limit* attribute. The reassemble algorithm for the received PPP fragments can be tuned by setting the following ITK NetBlazer 8500 parameters (normally the predefined values are sufficient): emas.mpra_max_frags: 100 # Max. number of MP fragments in reassembler table emas.mpra_frag_timeout: 1000 # Timeout of old MP fragments in MP reassembler table in ms For an example see Configuring Multilink PPP (MP) (page 7-63).

What to do	How
Enabling L2F tunneling	entry in user database in */etc/raddb/users* Configure NAS-Name and NAS-Secret in *l2f.par*, see *Chapter 7.3.7, l2f.par* (page 7-13). In case of an ADNS request, the asking client (NAS) is instructed to set up a connection to a certain computer (usually a provider in a multiprovider network, home server).
Verifying user's name and password	entry in user database in */etc/raddb/users*: USERNAME Password="PASSWORD" If a user has been identified by the extension address (DDI) this entry confirms the username and the password. For an example see AUTH Entries verifying user's name and password (page 7-64). Username and password can be followed by one or more attributes. For an example see Examples for attributes (page 7-64).
Distributed Line Management	For distributed connections that are tunneled to a home gateway the IP address of this home gateway is shown. For the EMAS connection on the home gateway the number of calling connections is shown (number of MP links). For further information see Chapter 5.2.2, *Meanings of ISDN connection entries* (page 5-6).
Send/Receive formatted IP Dump	A formatted dump of IP packets sent to / received from the user can be activated by starting a data logging with the appropriate levels. See Appendix A.3.2, *Logging* (page A-16).
Protocol Field Compression	The LCP option Protocol Field Compression is supported.

What to do	How
PPP Server / Client mode (passive/ active)	Enable *PPP Server/Client mode* by configuring ITK NetBlazer 8500 to *PPP client mode*. This is done with the flexible authentication by setting the RADIUS attribute *ITK-PPP-Client-Server-Mode* to *ITK-Mode-Client*. Normally the ITK NetBlazer 8500 is called from a remote user and the PPP software of ITK NetBlazer 8500 is passive, which means ITK NetBlazer 8500 waits for PPP connection establishment (for example configure requests) from the caller (client). That means normally ITK NetBlazer 8500 is in PPP Server mode. For LAN-to-LAN connection especially at least one side must be configured as PPP client to initiate the PPP connection. Please note that the *PPP Client Mode* is only possible without authentication.

What to do	How
Compression	The PPP compression is enabled by setting the ITK NetBlazer 8500 parameter *ppp_compression* (or the RADIUS attribute *ITK-PPP-Compression-Prot* in the authentication server) to a ':'-separated list of allowed compression protocols. **Example:** STAC:PRED1 To increase the throughput of PPP data enable the PPP compression. The negotiation of supported compression protocols is done with the PPP **C**ompression **C**ontrol **P**rotocol (CCP) as defined in RFC1962. ITK NetBlazer 8500 supports the following compression protocols in software (others may follow in future): • STAC: STAC LZS Compression Protocol (RFC1974) • PRED1: PPP Predictor type 1 Compression Protocol (RFC1978) The PPP compression works with single PPP connections as well as with multilink PPP (MP). The PPP compression is disabled for modem connections, because normally the modem protocols compress the data and a double compression is inefficient.

What to do	How
Distributed (Dynamic) Home Serving	For Distributed Line Management and distributed MP incoming calls are tunneled to the home server ITK NetBlazer 8500. Up to ITK NetBlazer 8500 software version V2.10 you had to configure the home server manually for each user (in the RADIUS database). This version introduces the distributed home server concept, which searches a corresponding home server dynamically when a new call arrives: • If the user is known at the local ITK NetBlazer 8500 (in connection table or UIP service table) the call is processed locally (the local ITK NetBlazer 8500 is the home server). • If the user is not known at the local ITK NetBlazer 8500, all ITK NetBlazer 8500s at the POP (all configured partner ITK NetBlazer 8500s) are asked about the user. If one ITK NetBlazer 8500 knows the user, this ITK NetBlazer 8500 is used as the home server and the call is tunneled to this ITK NetBlazer 8500. If no ITK NetBlazer 8500 knows the user, the call is processed locally as above. The *distributed home-serving* feature is normally disabled. You have to enable this feature by setting the ITK NetBlazer 8500 *.dist_homing* parameter to 1. The IP addresses of the partner ITK NetBlazer 8500 (ITK NetBlazer 8500 at one POP) must be configured with the ITK NetBlazer 8500 parameters *partner_cnt* (number of partner ITK NetBlazer 8500) and *partner_X* (IP address or name) (normally in *dlm.par*). The tunneling of calls to the home-server ITK NetBlazer 8500 is done automatically. The RADIUS attributes for tunneling (*ITK-Tunnel-Prot* and *ITK-Tunnel-IP*) need not be used.

What to do	How
CHAP	entry in user database in */etc/raddb/users* possible entries: ITK-PPP-Auth-Type: ITK-Auth-Auto|ITK-Auth-CHAP|ITK-Auth-PAP For detailed information see Appendix A.4, *RADIUS authentication file "users"* (page A-23). The **C**hallenge-**H**andshake **A**uthentication **P**rotocol (CHAP) is an alternative to PAP (**P**assword **A**uthentication **P**rotocol) in the authentication process of PPP. The password is transmitted encrypted. The authentication server decides which authentication protocol should be used: CHAP, PAP or AUTO. AUTO defines an automatic fallback from CHAP to PAP, if a dial-in user does not support CHAP.
Authenticate via DDI or CID	entry in *auth.par* For an example see Authentication via DDI (page 7-60). For an example see Authentication via CID (page 7-60).
Default entry for ITK NetBlazer 8500	entry in user database in */etc/raddb/users* Entry should define the attributes for the main user to avoid voluminous entries. The default entry for a ITK NetBlazer 8500 contacting a RADIUS server for authentication of users data is used to determine default attributes. If a required attribute is not given in a users entry, ITK NetBlazer 8500 uses the one from the default entry. The default entry is used during the offline authentication if no CID or DDI inquiry has been answered positively. For an example see Default entry for ITK NetBlazer 8500 (page 7-64).

What to do	How
Using DDI	entry in user database in */etc/raddb/users*: %_YY Password="DIRECT_DIAL" Entry authenticates users depending on their address extension (DDI = **D**irect **D**ial-**I**n). It is possible to define a special entry for every extension number For an example see Using DDI (page 7-64).
Using CID	entry in user database in */etc/raddb/users*: %XXX_ Password="ISDN_ADDRESS" The user will be authenticated by his telephone number (CID = **C**aller **I**D). When the user dials in, PPP is started automatically, the user gets the defined IP address and the appropriate packet filter file is used. No further authentication (such as online authentication) is required. For an example see Using CID (page 7-65).
Using DDI and CID	entry in user database in */etc/raddb/users*: %XXX_YY Password="USER_DIAL" Enabling DDI and CID at the same time can be useful if a user has the choice to select different services. For an example see Using DDI and CID (page 7-65).
Authentication Request Type from ADNS	In multiprovider scenarios the authentication request type, which is normally configured with the ITK NetBlazer 8500 parameter *.auth_req*, can be selected with the RADIUS Attribute *ITK-Auth-Req-Type*. The mechanism to build the authentication request from Caller ID and DDI remains the same.

What to do	How
Changing offline DEFAULT entry	entry in user database in */etc/raddb/users* Normally the entry with the default attributes for the offline authentication is read from the RADIUS user's file in the following section: DEFAULT User-Password = "SUPRIMO" If the RADIUS database is used for more RAS systems (not only for ITK NetBlazer 8500) the other systems need a DEFAULT section too. But the DEFAULT section can be defined only once. To solve this conflict the default attributes for the offline authentication can be read from a different section. The new section to use can be defined with the following ITK NetBlazer 8500 parameters: .users_default_entry# Username of the default-entry to use .users_default_pw# Password of the default-entry to use For an example see Changing offline DEFAULT entry (page 7-62).
Changing ID's for ITK RADIUS attributes	If the RADIUS database is used for more RAS systems (not only for ITK NetBlazer 8500) the other systems may need other proprietary attributes with RADIUS ID's that conflict with the ITK NetBlazer 8500 ones. To solve this conflict the ID's for the ITK NetBlazer 8500 attributes can be moved into a free range of attribute IDs. The RADIUS RFC allows ID's in the range 64 - 191. Normally the ITK attributes start with ID 100 but you can move them to a different place with the ITK NetBlazer 8500 parameter *.itk_radius_offset*, which is normally set to 100.

To change ID's for ITK RADIUS attributes perform the following steps:

(1) Change RADIUS dictionary:
- merge the ITK attributes into the dictionary file
- change the ITK attribute ID's manually to the destination range

(2) Restart RADIUS daemon to use the new dictionary.

(3) Change ITK NetBlazer 8500 parameter *.itk_radius_offset* to first ID in range.

(4) Restart ITK NetBlazer 8500 software.

7.7.1 Examples of RADIUS files

In this chapter you will find some examples of entries in RADIUS files. If no other file is given, the entries have to be made in the user database located in */etc/raddb/users*.

Client's declaration

Configure each RADIUS client in the */etc/raddb/client* file. An entry may look like this:

```
123.234.12.34 test
```

ADNS Entries used for ADNS servers

ADNS authentication, offline

```
%ADNS_10  Password  =  "DIRECT_DIAL"
            ITK-Auth-Serv-Ip=200.200.200.200,
            ITK-Auth-Serv-Prot  =  RADIUS
```

ADNS authentication, enabling L2F tunneling

```
%ADNS_20  Password  =  "DIRECT_DIAL"
              ITK-Tunnel-Prot = L2F,
              ITK-Tunnel-IP   = a.b.c.d,
              ITK-Tunnel-NAS-Name = NASNAME
```

The above-mentioned entry causes the inquiring client to build up a L2F tunnel to the IP address a.b.c.d. The Tunnel-NAS-Name is the home-servers name (name of server to be contacted with IP addr. a.b.c.d.).

NAS = Network Access Server: Begin of L2F tunnel

Home-Server = Gateway (GW): End of L2F tunnel

AUTH Entries verifying the user's caller ID

(offline authentication)

Authentication via CID

```
%1234_  Password  =  "ISDN-ADDRESS"
            Service-Type  =  Framed,
            Framed-Protocol  =  PPP,
            Framed-Filter-Id  =  "0"
```

Authentication via DDI

```
%_100  Password  =  " DIRECT_DIAL "
            Service-Type  =  Framed,
            Framed-Protocol  =  PPP,
            Framed-Filter-Id  =  "0"
```

Online authentication with FTP Server

1. Users defined in user file

```
testuser<SPACE>
            ITK-Ftp-Auth-IP = 1.2.3.4
            ... <Additional Attributes for testuser>
```

2. Users not defined in user file

```
testuser1<SPACE>
            ... <Additional Attributes for testuser1>
testuser2    Password="wrong password"
            ... <Additional Attributes for testuser2>
```

In the *auth.par* file insert:

```
.ftp_auth_addr: 1.2.3.4
```

Configuring Callback

```
%01234567_  Password = "ISDN_ADDRESS"
            Service-Type = Framed,
            Framed-Protocol = PPP,
            ITK-Dialout-Type = ITK-Callback,
            ITK-ISDN-Prot = ITK-HDLC,
            Filter-Id = "0"
```

Static IP addresses

The following entries could be used for users with **static IP addresses**:

Configuring Callout

```
%192.168.18.40 Password = "IP_ADDRESS"
            Callback-Number = "9876543",
            ITK-Dialout-Type = ITK-Callout
```

Offline authentication

```
%9876543_  Password = "ISDN_ADDRESS"
            Service-Type = Framed,
            Framed-Protocol = PPP,
            Framed-IP-Address = 192.168.18.40,
            ITK-ISDN-Prot = ITK-HDLC,
            Filter-Id = "0"
```

Online authentication

```
abcdef Password = "ghijklm"
            Framed-IP-Address = 192.168.18.41
```

Dynamic IP Adresses

The following entries could be used for users with **dynamic IP addresses**:

Offline authentication

```
%9876543_  Password = "ISDN_ADDRESS"
           Service-Type = Framed,
           Framed-Protocol = PPP,
           ITK-Dialout-Type = ITK-Callout,
           Filter-Id = "0"
```

In this case only the Dialout type has to be specified during the authentication (online is also possible, see below). ITK NetBlazer 8500 stores internally the last used IP address of this user. If someone sends IP packets to this IP address, ITK NetBlazer 8500 calls 9876... and reassigns the previously used IP address.

Online authentication

```
abcdef Password = "ghijklm"
           ITK-Dialout-Type = ITK-Callout
```

If instead of *ITK-Callout* the value *ITK-Recall* is used, the ITK NetBlazer 8500 **Recall feature** is activated. This means ITK NetBlazer 8500 calls the target PC but does not build up a B channel connection. The target rejects the call and calls back (do not forget to activate *Callback* on the target). This mechanism has been successfully tested with ITK connect/ WS.

Changing offline DEFAULT entry

If the following ITK NetBlazer 8500 parameters are defined

```
.users_default_entry:      SUPRIMO_DEFAULT
.users_default_pw:         SUPRIMO_PW
```

the offline authentication attributes are read from RADIUS user's section

```
SUPRIMO_DEFAULT   User-Password = „SUPRIMO_PW“
```

In multiprovider scenarios the values for the DEFAULT entry can be configured in the ADNS request with the following RADIUS Attributes:

```
ITK-Users-Default-Entry # Username of the DEFAULT entry to use
ITK-Users-Default-Pw    # Password of the default-entry to use
```

Configuring Extended Shorthold

The following example shows a sample entry in the RADIUS user's file of the authentication server which might be the Access Agent at the same time for offline authentication:

```
%01234567_  Password = "ISDN_ADDRESS"
            ITK-Tunnel-IP = 123.45.67.89,
            ITK-Tunnel-Prot = ITK-EMAS,
            Framed-Protocol = PPP,
            Service-Type = Framed
```

The above mentioned ITK attributes can also be used during an online authentication.

Configuring Multilink PPP (MP)

The following example shows a sample entry in the RADIUS user's file. The user with caller id *0123456* can use MP with a maximum of 3 links simultaneously:

```
#   Only Caller-ID known => Start PPP or MP:
          #   allow only 3 simultaneous connections,
          %0123456_ User-Password = "ISDN_ADDRESS"
                      Service-Type = Framed,
                      Framed-Protocol = MP,
                      Port-Limit = 3,
                      Filter-Id = "0"
```

The following example shows a sample entry in the RADIUS user's file. The user *guest10* can use MP with a maximum of 2 links simultaneously. The user *guest11* can use MP only if the ITK NetBlazer 8500 *.port_limit* parameter is > 1.

```
guest10 Password = "guest10"
            Port-Limit = 2
guest11 Password = "guest11"
DEFAULT Password = "SUPRIMO"
            Service-Type = Framed,
            Framed-Protocol = MP,
            Filter-Id = "0"
```

AUTH Entries verifying user's name and password

(online authentication)

```
peter Password = "susi"
        attribute1 = xxx,
        attribute2 = yyy
```

Username and password can be followed by one or more attributes.

All attributes except the last one and the password have to be separated by commas and all entries have to be separated with a blank.

Examples for attributes

Attribute	Meaning
Framed-Protocol = PPP	tells ITK NetBlazer 8500 to use the PPP protocol for this user
Service-Type = NAS-Prompt	tells ITK NetBlazer 8500 to pop up a log in screen for this user
Framed-IP-Address = 100.100.100.100	tells ITK NetBlazer 8500 to use this static IP address for the user

Default entry for ITK NetBlazer 8500

```
DEFAULT Password = "SUPRIMO"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Framed-Filter-Id = "0"
```

Using DDI

```
%_10 Password = "DIRECT_DIAL"
        Service-Type = NAS-Prompt
```

In this case a user who dials in ITK NetBlazer 8500 with an extension number of 10 gets a login prompt with predefined messages like *username* and *password.*

An online authentication will always follow.

Using CID

```
%12345_ Password = "ISDN_ADDRESS"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Framed-IP-Address = 1.2.3.4,
        Framed-Filter-Id = "1"
```

Using DDI and CID

```
%123_10 Password = "DIRECT_DIAL"
        Service-Type = NAS-Prompt

%123_20 Password = "DIRECT_DIAL"
        Service-Type = telnet,
        Login-Host = 1.2.3.4
```

In this case the user has two possibilities for dialing in. With the extension 10 a login screen is sent and with 20 a telnet connection to host 1.2.3.4 is established.

Additional accounting attributes

Some additional RADIUS attributes are used for accounting start and accounting stop requests.

The following table shows the accounting attributes of a sample ISDN session:

```
Fri Nov 14 09:03:36 1997
        Acct-Status-Type = Start
        NAS-IP-Address = 192.168.1.2
        User-Name = "itkSUPRIMO"
        Framed-IP-Address = 192.168.3.4
        Acct-Session-Id = "199711140903359460"
        NAS-Port = 3
        NAS-Port-Type = ISDN-Sync
        Calling-Station-Id = "4711"
        Acct-Authentic = RADIUS
        Service-Type = Framed
```

```
        Framed-Protocol = PPP
Fri Nov 14 09:03:45 1997
        Acct-Status-Type = Stop
        NAS-IP-Address = 192.168.1.1
        User-Name = "itkSUPRIMO"
        Framed-IP-Address = 192.168.3.4
        Acct-Session-Id = "199711140903359460"
        NAS-Port = 3
        NAS-Port-Type = ISDN-Sync
        Calling-Station-Id = "4711"
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Framed-Protocol = PPP
        Acct-Session-Time = 10
        Acct-Output-Octets = 203
        Acct-Input-Octets = 159
```

7.7.2 Voice files for IVR

The voice files used by the NetBlazer are located in the directory “/u/pra/voi”. The sample voice files contained in the NetBlazer kit are located in the directory “/u/pra/voi/samples”. During the installation the sample voice files are automatically copied into the working directory (but not overwritten if existant).

In previous version voice files in a special proprietary format were used for IVR (Interactive Voice Processing). Starting with V5.0 standard PC WAV files are used. These files can be recorded or changed with the NetBlazer or on a standard PC. After copying them into the directory “/u/pra/voi” (i.e. by FTP) they are used from by NetBlazer.

The used WAV files must conform to the following format (PCM 8.000 Hz; 16 Bit; Mono):

- Channels: Mono
- Resolution: 16 bit
- sample rate: 8000 Hz

There are different languages of voice files. They can be differentiated by their filenames:

```
Name_<Language>.<Type>
```

Name: corresponds to the contents of the file and can be selected by RADIUS attributes or ITK NetBlazer 8500 parameters. (e.g. “welcome” defines a file with a greeting message)

<Language>: Corresponds to the language of the file. The occurrence of “%s” in the filename is automatically substituted by the value of the RADIUS attribute “ITK-Prompt” (the language).

<Type>: Corresponds to the type of the voice file (wav).

Example: If the parameter “.voisam_welcome” has the (default) value “welcome_%s” than it may define the file “welcome_e.wav” (contains an English welcome message).

The ITK NetBlazer 8500 software kit contains sample voice files with English and German speech, which are located in the directory “/u/pra/voi/samples”.

Additional voice files for different languages or different contents can be recorded manually (see below).

Recording of new voice files

WAV files can be recorded with the NetBlazer by setting ITK-Banner to “RECORD”.

The following RADIUS entry allows the recording of a new file after dialing “42” as DDI:

```
%_42        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="RECORD",
            ITK-Welcome-Message="record_prompt_e",
            ITK-Prompt="record"
```

The recorded speech is found in the file “record.wav”.

7.7.3 Configuring Voice over IP with H.323

The H.323 protocol is needed to establish voice connections from PC to PC, PC to phone, phone to PC and phone to phone when different gateways are involved. It allows the interoperability of systems from different vendors. The NetBlazer implementation in V5.00 is H.323V1 with some V2 enhancements.

The NetBlazer specific connection setup protocol SPC, that was introduced in V4.00, is still supported. Both protocols (SPC and H.323) can be selected dynamically on connection setup.

A H.323 daemon (h323d) is used to realize call establishment by the ITU standard H.323 for Voice over IP.

The h323d is started and controlled by PRACTRL. If h323d uses a gatekeeper (see parameters below) it registeres itself at the gatekeeper.

In the process table of PRAMON/webMan you can see the IP address of this gatekeeper (GK) or 'No GK' if no gatekeeper is used. Furthermore the number of sessions is shown (#s).

Example:

“No GK - #s: 2”	->Not using a gatekeeper, two active H.323 sessions.
“GK 123.45.67.89 #s: 0”	->Using a gatekeeper 123.45.67.89, no active H.323 session.
“GK 0.0.0.0 #s: 0”	->Using a gatekeeper, but actual unregistered (e.g. gatekeeper is down), no active H.323 session

The parameters for the h323d are configured in h323.par.

Gatekeeper parameters

To enable/disable the usage of a gatekeeper the parameter 'h323d.use_gatekeeper' must be configured (no=0/yes=1):

Example:

```
h323d.use_gatekeeper: 0  # NOT using a gatekeeper
or
h323d.use_gatekeeper: 1  # Using a gatekeeper
```

Other values than 0 or 1 are not allowed. If the parameter 'h323d.use_gatekeeper' is 1 (using a gatekeeper) the parameter 'h323d.ip_addr_gatekeeper' must be configured. If you leave this parameter blank the h323d will try to find a gatekeeper by doing a RAS request broadcast. Alternatively you can configure the IP address of a known gatekeeper. In this case the h323d is trying to register itself at this gatekeeper by a RAS request.

Example:

```
h323d.ip_addr_gatekeeper:              # Try to find a gatekeeper by broadcast
or
h323d.ip_addr_gatekeeper: 123.45.67.89 # IP address of gatekeeper
```

Country code substitution

This parameter is used to support an international dial number layout used by other vendors (e.g. Cisco). You can specify a country code and the substitution digits for your system. If the country code digits are found in the calling number they are exchanged by the substitution specified.

If you do NOT want to use country code substitution the parameters can be left blank!

Example:

```
parameter setting:
h323d.CountryCodeSubtitution:  +49;0  # country code '+49' is substituted
                                      by '0'
```

1) If the h323d gets the calling number +4923197470:
The check of the prefix leads to the result 'it is an international call'. The prefix '+49' is cut off and the number '**0**23197470' is called.

2) If the h323d gets the calling number 023197470:
The check of the prefix leads to the result 'it NOT is an international call'. The number is unchanged.

Prefix parameters

These parameters may be used if a gatekeeper needs to reference different gateways by calling number prefix. The gatekeeper forwards the calling number according this prefix. Thus the prefix must be cut off by the h323d. If the h323d gets a calling number, it will be checked if one of the configured prefixes is used. This prefix will be cut off and the calling number without prefix is used to establish the call. For external calls the 'PBXExternCallPrefix' is called first.

If you do NOT want to use prefixes the parameters can be left blank!

Example:

Assuming the following parameter settings:
h323d.PBXExternCallPrefix: 0 # Prefix for external calls using a PBX
h323d.AudioOnlyCallInternPrefix: 92 # Prefix for internal audio calls
h323d.AudioOnlyCallExternPrefix: 93# Prefix for external audio calls

1) If the h323d gets the calling number 92123:
The check of the prefixes leads to the result 'it is an internal call'. The prefix is cut off and the number '123' is called.

2) If the h323d gets the calling number 93567890:
The check of the prefixes leads to the result 'it is an external call'. The prefix is cut off, the 'PBXExternCallPrefix' is called first and then the calling number is added. Thus '0-567890' is called in our example.

3) If the h323d gets the calling number 94789:
The call will be rejected because no matching prefix is found (normally the gatekeeper would not forward this call to the h323d).

Call handling parameters

The h323d supports two different ways of connection establishment. The behavior is selected by the following parameters:

1) h323d.use_early_h245_tsap: (no=0/yes=1) (default: 1)
Offer own H.245 IP address and port in the first SETUP message to open H.245 channel with first round trip.

2) h323d.wait_for_remote_connect: (no=0/yes=1) (default: 0)
Wait for CONNECT message from remote phone before opening H.245

channel.
(parameter only supported after V5.00b2)

NOTE: For support of the Ericsson gatekeeper the parameters should be set to:

h323d.use_early_h245_tsap: 0
h323d.wait_for_remote_connect: 1
and you have to change the '.type_of_codec' parameter in the 'voip.par':

.type_of_codec: G711:G723 #do NOT use G.729 with Ericsson gatekeeper

Further Parameters for H.323

The parameter ".spc_h323_setup" controls, which connection setup protocol should generally be used:

- 0 use SPC
- 1 use H.323

7.7.4 Transparent Connection Setup

Voice dialog

The voice dialog defines how a user authenticates and enteres his destination phone number. The previous versions only supported Interactive Voice Response (IVR). V5.0 additionally supports One Stage dialing (OSD).

Interactive Voice Response (IVR)

IVR (or **V**oice **G**uided **I**nput VGI) is a 2-stage-dialing process: In the first step the user dials the number of the voice gateway and hears the welcome voice messages. In the second step the user enters his PIN and the destination number by DTMF digits. This voice dialog type is still useable in V5.0 and has been enhanced with the following features:

- **WAV files**: All voice files are standard WAV files, that can be recorded or changed on a standard PC and activated on the NetBlazer by copying the files in the right directory (see Chapter 7.7.2, *Voice files for IVR* (page 7-66)).

- **Dynamic Dialing**: Additionally to the block dialing in V4.0 dynamic dialing is useable, where the termination of the destination number is not necessary. (see below)
- **Remote tone signalling**: During connection setup the dial tones that are generated at the dialout gateway are hearable from the caller at the dialin gateway. (see below)

To enable IVR the Radius attribute “ITK-Banner” must be set to one of the following values:

- “IVR” to enable IVR with block dialing (same as “VGI” in V4.0)
- “IVR_DYNDIAL” to enable IVR with dynamic dialing

The other Radius attributes to define the language, voice files, etc. remain unchanged.

One stage dialing (OSD)

One stage dialing allows the dialing of the destination number immediate after the access number of the voice gateway. There is no separator or pause necessary between the access number and the destination number. The digits are detected from the switch and received through the d channel (no DTMF digits necessary). The incoming call is not accepted until the callee has answered the call.

No PIN is entered in One Stage Dialing. So the authentication must be done by the calling line ID of the caller, or by doing no authentication at all.

To enable OSD the Radius attribute “ITK-Banner” must be set to one of the following values:

- “OSD” to enable OSD with block dialing
- “OSD_DYNDIAL” to enable OSD with dynamic dialing

Get Destination number

Block dialing

Block dialing describes the process where the NetBlazer collects all digits of the destination number, without knowing when it is complete. So a termination (by ‘#’ key or timeout) is necessary.

As soon as the destination number is complete the NetBlazer establishes the connection.

Dynamic dialing (overlapped sending)

Dynamic dialing (also called overlapped sending) allows the transmission of dial digits during the dialing phase (one digit after the other). As soon as the remote switch signals the completion of the destination number the caller is signaled the calling signal.

No termination of the destination number is necessary.

If the connection setup is done by H.323 the remote gateway (or gatekeeper) must support H.323V2, because the overlapped sended digits, are sent by H.323V2.

To achieve the support of Dynamic dialing the D-channel Setup (dial-out) is done without any destination number. The destination number is transmitted to the PABX one after the other afterwards. This empty Setup may be rejected by some PABX (D-Channel Disconnect cause: „Information element is missing“).

Setting the parameter *voip_empty_setup: 0* fixes the problem, but **disables** Dynamic dialing at the same time.

Remote Tone signaling

Remote tone signaling is used to hear remote status tones and announcements. The data path is switched starting with the connection setup (not after connection establishment).

Features

The following table describes all possible features in the several VoIP dialoges:

Feature \ VoIP-Dialog	IVR	IVR_DYNDIAL	OSD	OSD_DYNDIAL
Block dialing (termination necessary)	x		x	
Dynamic dialing (no Termination)		x		x
Authentication by PIN (entered as DTMF)	x	x		
Get destination number digits by DTMF	x	x		
Get destination number by DDI (d channel)			x	x
Interpretation '*' and '#' digits	x		x	
Additional calls after first	x			
Callback	x	x		
Remote tone signalling	x	x	x	x
Playback of voice files	x	x		
Accept call before connection established	x	x		

All other features are possible with all VoIP dialoges.

7.7.5 Address Translation

The address translation is necessary for two reasons:

1. Find the IP address of the dialout gateway that should be used for the entered destination number
2. Modify the destination number so that it can be used to establish a connection at the dialout gateway

The NetBlazer V5.0 supports two methods to do the address translation:

1. Use Least Cost Routing (LCR) requests to a Radius server (proprietary, same as in V4.0, useable for SPC and H.323 connection setup)
2. Use RAS (Registration Admission Status) requests to a Gatekeeper (H.323 compliant, only useable with H.323 connection setup)

Both address translation methods can be combined. If a LCR Radius server as well as a Gatekeeper is configured the following cases are possible:

(dial-no defines the number the user dialed,

called-no defines the number that should be used to establish the call (result of the address translation))

- Radius LCR knows the dial-no and though responds with a called-no: No RAS request will be done. The called-no from the Radius LCR response will be used to establish the connection.
- Radius LCR does not know the dial-no and though responds no called-no: A RAS request will be done. The called-no from the Gatekeeper will be used to establish the connection.
- No Radius LCR defined (service table empty or LCR dynamically disabled): A RAS request will be done. The called-no from the Gatekeeper will be used to establish the connection.

The LCR request can be disabled dynamically per call with the setting of the “ITK-Voip-Init-String” (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

With dynamic dialing the dialout gateway must be found dynamically. With every digit of the dial-no the LCR is asked if he knows the corresponding dialout gateway. As soon as a positive response has been received the connection is established, no further LCR requests are done and all further digits of the dial-no are transferred directly to the dialout gateway.

To minimize the LCR requests a minimal amount of digits is collected before the first LCR request is done, which can be configured with the parameter “.voip_lcr_min_digits” (Default: 3).

The same behaviour is used for address translation by RAS instead of LCR.

7.7.6 Connection Setup

SPC or H.323

The parameter ".spc_h323_setup" controls, which connection setup protocol should generally be used:

- 0 use SPC
- 1 use H.323

The connection setup protocol can be defined dynamically per call with the setting of the "ITK-Voip-Init-String" (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

Warning: Because of a lot of new features the SPC protocol has been enhanced so that there is no interoperability with NetBlazer 8500 V4.00

Automatic connection setup

A voice connection can automatically be established with the offline authentication by returning dest-no in the Radius response.

The following example establishes automatically a connection to a defined dest-no when the DDI '81' is dialed. An address translation will be done:

```
%_81        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="OSD",
            ITK-Dest-No = "023197470",
            ITK-Username="ITK"
```

The following example establishes automatically a connection to a defined H.323 client when the DDI '82' is dialed. An address translation is not done. The dummy dest-no is needed to force a connection setup to the defined IP address:

```
%_82        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="OSD",
            ITK-Dest-No = "xxx",
            ITK-Username="voip-test",
            ITK-Tunnel-IP = a.b.c.d,
            ITK-Voip-Init-String="H1"
```

7.7.7 Codecs

V5.0 supports the following codecs:

- G.729A same as in V4.0, compression ratio 8:1
- G.723.1 compresion ratio 10:1
- G.711 uncompressed, a-law and µ-law supported

The codec to use is automatically negotiated between the dialin and the dialout gateway. The codecs supported by the NetBlazer can be configured with the parameter *.type_of_codec (Default: G711:G723:G729)*

The codec to use can be forced dynamically per call with the setting of the "ITK-Voip-Init-String" (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

The framesize can be configured to 30 or 60 ms with parameter ".frame_size". (Default: 60 ms)

The following table shows the different codecs, framesizes and packet sizes supported by V5.0:

Codec	Ratio	Framesize [ms]	Payload [bytes]	IP header [bytes]	IP packet size [bytes]	IP packets per sec	IP Bytes per sec [bytes]
G.729A	8:1	30	30	40	70	33,33	2334
G.729A	8:1	60	60	40	100	16,67	1667
G.723.1	10:1	30	24	40	64	33,33	2134
G723.1	10:1	60	48	40	88	16,67	1467
G.711	1:1	30	240	40	280	33,33	9333
G.711	1:1	60	480	40	520	16,67	8669

7.7.8 Coding / Transcoding

The NetBlazer supports the coding a-law (used in Europe) as well as µ-law (used in USA). Each DSP card must be configured to the right coding (depending on the switch) by setting the parameter ".pcm_companding".

Possible values:

1=µ-law
2=a-law (Default)

Transcoding: If the two communication gateways have different codings (i.e. one is located in Europe and one in the US) the different codings are converted/transcoded from the NetBlazer. This is only necessary for G.711, the other codecs automatically adapt the coding.

7.7.9 DTMF Relay

If DTMF relay is enabled the dialin gateway detects if DTMF keys are pressed and sends these digits to the dialout gateway, where they are processed (i.e. new DTMF tones generated). Thie mechanism is an outband transfer of recognized DTMF digits as specified in H.323V2. The DTMF keys are transferred by SPC or as H.245 User Input Indications to be H.323V2 compliant.

This feature is disabled by default but can be enabled dynamically per call with the setting of the “ITK-Voip-Init-String” (see chapter 7.7.13, *Additional Parameters & Attributes for VoIP* (page 7-81)).

7.7.10 Selecting Dialout Line

Only lines with an active D channel and that are not disabled (status “up-on”) are selected for outgoing calls.

By default all available lines (physical interface, controllers) are investigated and the line with the highest number of free ports is used for an outgoing call.

This behaviour can be changed by manually selecting a special line (Provider selection). Each physical interface (primary rate, basic rate) is managed by a so called controller. If the dialout number is preceeded by a controller number and a pipe ('|') sign then the according physical interface is used for dialout. This modified dialout number may be retrieved from a least cost routing request (or from a gatekeeper).

Example:

192.168.100.31 is a gateway located in Dortmund/Germany. This gateway is connected to a city carrier via controller 2 and to a backup distance carrier via controller 3.
The least cost routing entry in the RADIUS users file may look like this:

```
%0231*      User-Password="LCR"
            ITK-Tunnel-IP = 192.168.100.31,
            ITK-Dest-No = "-4+2|",
            ITK-Tunnel-IP = 192.168.100.31,
            ITK-Dest-No = "-4+3|"
```

The RADIUS server strips the first four digits of the dialed number and adds the leading string "2|" respectively "3|": e.g. 0231987654 -> 2|987654; 3|987654. The dialout gateway first uses controller 2 (city carrier) for the dialout with number "987654". If this fails (all lines busy) then controller 3 (backup carrier) is used for the dialout with number "987654".

7.7.11 CLIP

The Calling Line Identification (CLI) of the phone dialing into the NetBlazer 8500 (caller) is forwarded to the dialout gateway or H.323 client during the VoIP call setup. The dialout gateway presents the CLI at the remote phone (callee), and a H.323 client shows the CLI within its user dialog.

The CLI is transfered unchanged between the dialin gateway and the remote site. No adaptions of the phone number on the incoming or outgoing site (dependent on the phone number of the line) are done.

CLIP (CLI-**P**resentation) is disabled by default and can be enabled by setting the parameter ".capi20_clip" to 1.

7.7.12 Connection control

For detection of aborted connection the following mechanism is used:

If no voice data (RTP packets) are received during a specified amount of time (parameter ".voip_idle_tmo", default: 300 seconds) the session is disconnected.

7.7.13 Additional Parameters & Attributes for VoIP

The Radius attribute “ITK-Voip-Init-String” can be used to configure special attributes for a voice connection. The following values are supported and can be combined to an initialization string (as AT like modem init strings):

H: Select connection setup protocol:
H1=H.323, H0=SPC
A: Select address translation protocol:
A1=RAS (Gatekeeper), A0=LCR (Radius)
D: Enable/disable DTMF Relay:
D1=enable, D0=disable
C: Select/force special codec:
C1=G.711, C2=G.723.1, C3=G.729A

The following Radius example shows the activation of a voice connection with H.323 connection setup and DTMF relay when the DDI “83” is dialed:

```
%_83        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="OSD",
            ITK-Voip-Init-String="H1D1"
```

Setting Type of Service (TOS)

To configure a NetBlazer 8500 for VoIP the following parameter can be adapted in “voip.par”:

- Configuration IP TOS (type of service) field — voip_ip_tos (description below)

The IP TOS (Type Of Service) field is part of the IP packet. Some routers use the IP TOS field for a precedence selection. IP packets with a matching type of service field are preferred delivered. To achieve the best transmission results this value can be adapted to the routers precedence selection.

The TOS field is defined in RFC 791:

Bit 0: 0x01 Reserved
Bit 1: 0x02 Low Monetary costs
Bit 2: 0x04 High Reliability
Bit 3: 0x08 High Throughput
Bit 4: 0x10 Low Delay
Bit 5-7:Precedence value

These flags are used to build the resulting TOS value:

Example:

If the ip packets should be transmitted with low delay and high reliability then the parameter
voip_ip_tos must be set to the value 0x14
Default value: 0x10

7.7.14 Examples for IVR

1. Offline authentication: Selecting a German IVR with voice compression when “40” is dialed as DDI:

```
%_40        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="IVR",
            ITK-Prompt="d"
```

2. Offline authentication: Selecting an English IVR with voice compression when “41” is dialed as DDI, use a special welcome message:

```
%_41        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="IVR",
            ITK-Prompt="e",
            ITK-Welcome-Message=”welcome_special”
```

3. Offline authentication: Selecting an English guided voice file recording when “42” is dialed as DDI, save recording in voice file “record”,

limit the recording to 30 seconds:

```
%_42            User-Password = "DIRECT_DIAL"
                Service-Type = ITK-Voice-over-IP-Comp,
                ITK-Banner="RECORD",
                ITK-Welcome-Message="record_prompt_e",
                Session-Timeout=30,
                ITK-Prompt="record"
```

4. Offline authentication: Selecting German IVR when a call from Calling line ID “0231555566” arrives and the caller “W.Smith” the DDI “40” dials (IVR does not ask for entering the account code because the caller is already authenticated by the calling line ID):

```
%0231555566_40 User-Password = "USER_DIAL"
                Service-Type = ITK-Voice-over-IP-Comp,
                ITK-Banner = "IVR",
                ITK-Prompt = "d",
                ITK-Username = "W.Smith"
```

5. Offline authentication: To enhance the previous entry for callback the following attribute must be added:

```
ITK-Dialout-Type = ITK-Callback,
```

   This means that the caller calls the Dialin gateway which rejects the connection, but calls back some seconds later. After that the caller hears the normal IVR and can enter the destination number to establish a connection. This solution is suitable for home workers because all charging will be done to the Dialin gateway.

6. Offline authentication: Enable an automatic call setup to destination number “12345” when “45” is dialed as DDI:

```
%_45            User-Password = "DIRECT_DIAL"
                Service-Type = ITK-Voice-over-IP-Comp,
                ITK-Banner="IVR",
                ITK-Dest-No = "12345",
                ITK-Username="Directcall",
                ITK-Prompt="d"
```

7. Online authentication: Accept the account code “18112001” (Length

of account code: 8, length of PIN: 4):

```
1811        User-Password="2001"
            ITK-Username="W.Smith"
```

8. Online authentication: Accept the account code “123” (which is too short to conform to the complete account code (with PIN)):

```
123         User-Password="VOICE-ACCOUNT"
            ITK-Username="W.Smith"
```

7.7.15 Least Cost Routing (LCR)

To find the best dial-out gateway for the connection setup one (or more) Least Cost Routers (LCR) maintain the defined routes and answer the LCR requests from Dialin gateways.

This version only supports LCR requests over the RADIUS protocol. As soon as the Dialin gateway knows the complete destination phone number a special RADIUS request is sent to a RADIUS server that queries his database in order to find the right entry and sends the result back to the calling gateway as a RADIUS access accept.

LCR-Request and -Answer:

The LCR request from the Dialin gateway to the RADIUS server contains the destination number as <username> and “LCR” as the predefined <password> (plus additional attributes, that can be used to restrict the query):

```
%dest_number    User-Password=”LCR”
                ITK-Username=”xxxx”,    # Username of the caller
                ITK-DDI=xx              # DDI the caller dialed
```

The access accept from the RADIUS server should contain the following attributes:

```
ITK-Tunnel-IP=a.b.c.d,
ITK-Dest-No=xxxx,
Session-Timeout
```

"**ITK-Tunnel-IP**" contains the IP-address of the dial-out gateway. It is optional, the default is to use the value of "ITK-Tunnel-IP" from previous offline- or online-authentication steps. If none was defined the call remains locally (the dialin gateway is used for the dial-out).

"**ITK-Dest-No**" contains the phone number that should be dialed at the dial-out gateway site in order to reach the callee. It is optional, the default is the same as the destination number the caller dialed.

"**Session-Timeout**": contains the timeout for the phone connection (in seconds). After this time the connection is terminated automatically. It is optional, the default is 0=no limit.

These three attributes may occur multiple times to define alternate dial-out gateways, i.e. if the 1st dial-out gateway is busy or out of order the 2nd gateway will be used with the special attributes (destination number and session timeout) for this gateway.

Voice message instead of connection setup:

If the LCR answer contains the attribute "ITK-Prompt" the connection is not established. Instead the voice file whose name corresponds to the value of "ITK-Prompt" is played and the caller remains in the state of entering the destination number.

This mechanism can be used to forbid special destination numbers for the caller. Instead a voice message is presented to inform the caller about this situation.

Example:

The following entry forbids long distance calls in Europe but plays the English voice message "nolongdist_e.<type>"

```
%00*        User-Password=”LCR”
            ITK-Prompt=”nolongdist_e”
```

Short dial numbers (shortcuts):

The LCR request performs a type of conversion or mapping of destination numbers. This can be used to define "short dial numbers" that make the dialing of long numbers easier.

Example:

The following entry makes a connection to the “cinema announcement” in Chelmsford and uses the defined dial-out gateway when using the destination number “1”:

```
%1          User-Password="LCR"
            ITK-Tunnel-IP = a.b.c.d,
            ITK-Dest-No = "19787443700"
```

Service table:

The IP addresses of the primary LCR server and multiple alternates are defined in a new service table “LCR”. This service table is initialized with the corresponding parameters in “voip.par” and can be viewed and changed dynamically with pramon.

Normally the 1st LCR server in the service table is queried, but if this fails (i.e. timeout waiting for LCR answers) this LCR server is disabled in the service table and a SNMP trap is sent. For this and all following LCR requests the 2nd LCR server is used. The re-enabling of the disabled LCR server has to be done manually after checking its functionality.

Testing LCR entries:

LCR entries can be tested with the tool “test_rad”.

Example:

The following command shows the LCR response for the previous shortcut example :

```
test_rad  -p LCR  -u  %1
```

Response:

```
Access-Accept Packet received

ID                = 44
LENGHT            = 39

ATTR_TYPE         = 110
ATTR_LEN          = 6
TUNNEL_IP         = a.b.c.d
```

```
ATTR_TYPE        = 130
ATTR_LEN         = 13
ITK_DEST_NO      = 19787443700
```

(The options ‘-a’ (for IP address) and ‘-k’ (for secret) are optional.)

7.8 Accounting file

- The daily files are in */u/pra/log*.
- The name of the accounting files are: *.acc
- All fields are divided by ’:’.
- You can import and analyze the accounting files into EXCEL.

For each VoIP connection there are two accounting entries: 1 on the dialin gateway and 1 for each dialout connection on the dialout gateway.

The accounting file shows the following additional fields for VoIP connections:

- **VoIP-Con-Setup** Connection setup protocol used (SPC, H.323)
- **VoIP-Dialog-Type** Type of VoIP dialog (IVR, OSD, with/without DYNDIAL)

For the other connections there is one entry per connection.

Alternative processing of ITK NetBlazer 8500 accounting data in billing system “iPhoneEX“ is possible. Conversion of accounting data into CDR (**C**all **D**etail **R**ecord) format is performed with tool “acc2cdr”.

7.8.1 acc2cdr

The new tool “acc2cdr” (accounting to CDR format) is used to convert the NetBlazer 8500 accounting format into the Call Detail Record (CDR) format of the billing system “iPhonEX” of the vendor MIND CTI Inc.

Usage:

```
acc2cdr  [-d  delimiter]  [<INPUT]  [>OUTPUT]
```

The delimiter defines the character between the several fields.
Default is ‘;’.

"acc2cdr" works like a UNIX pipe, which means the input (NetBlazer 8500 accounting format) is read from standard input and the output (CDR format) is written to standard output. Input/ouput from/to files must be done through I/O-redirection.

7.9 ITK NetBlazer 8500 MIB

There is a private MIB (**M**anagement **I**nformation **B**ase) for the ITK NetBlazer 8500. The objects (variables) from the MIB can be asked during running time from NMS (**N**etwork **M**anagement **S**ystem) via SNMP.

With ITK NetBlazer 8500 you have the following file, which explains all ITK NetBlazer 8500 MIB objects in ASN.1 syntax:

/u/pra/dat/pra.mib

You can import this file in an NMS system and list the ITK NetBlazer 8500 objects with their explanations.

List of ITK NetBlazer 8500 Objects

ITK NetBlazer 8500 Object	Meaning
praVersion	Version of ITK NetBlazer 8500 software
asIPTable	table of ApplicationServer IP Addresses
asIPEntry	one entry in *asIPTable*
asNumber	number of authentication server
asIPAddr	IP address of authentication servers
linecntPspdn	max. number of logical connections to PH (type X.25)
linecntPspdnPerBchannel	max. number of logical connections per B channel to PH
linecntPspdnPh	max. number of physical connections to PH

ITK NetBlazer 8500 Object	Meaning
linecntMax	Number of physical B channel
asIPAddrTableMaxIndex	max. number of AS-IP-Addresses
numberOfEngagedBchan	number of engaged B channel
numberOfFreeBchan	number of free B channel
numberOfTransToAs	number of transmission connections to AS
numberOfRecvToAs	number of receive connections to AS
temperature	temperature inside the ITK NetBlazer 8500 housing (in tenth degrees)
isdnMuxOk	status of ISDN board
modemAdapterTable	table of modems
modemEntry	entry in the *modemAdapterTable*
modemCardNumber	index
modemAdapterOk	status of modem adapter
modem x	status of Modem x
practrlOk	status of *PRACTRL* process
isdnInOk	status of *isdn_in* process
isdnOutOk	status of *isdn_out* process
pstnInOk	status of *pstn_in* process
pspdnOk	status of *pdpdn* process

ITK NetBlazer 8500 Object	Meaning
modemCardMax	maximum number of modem adapters
cpuCapacity	free capacity of CPU in percent
sessionTable	table of sessions
sessionEntry	entry in the session table
sessionNumber	session number to identify this session (1 - maxSessionNumber)
sessionType	session type of this session
b2Protocol	B2 channel protocol
cntRcvByteCapi	number of bytes received from T interface
cntSndByteCapi	number of bytes sent to T interface
cntRcvMsgCapi	number of messages received from T interface
cntSndMsgCapi	number of messages sent to T interface
cntRcvBytePsp	number of bytes received from R interface
cntSndBytePsp	number of bytes sent to R interface
cntRcvMsgPsp	number of messages received from R interface
cntSndMsgPsp	number of messages sent to R interface
cntRcvTotalByteCapi	number of total bytes [KBytes] received from T interface

ITK NetBlazer 8500 Object	Meaning
cntSndTotalByteCapi	number of total bytes [KBytes] sent to T interface
cntRcvTotalMsgCapi	number of total messages received from T interface
cntSndTotalMsgCapi	number of total messages sent to T interface
cntRcvTotalBytePsp	number of total bytes [KBytes] received from R interface
cntSndTotalBytePsp	number of total bytes [KBytes] sent to R interface
cntRcvTotalMsgPsp	number of total messages received from R interface
cntSndTotalMsgPsp	number of total messages sent to R interface
sessionTableMaxIndex	max. number of session number

Script pramibtest

There is a script file pramibtest in the */u/pra/exe* directory. This file gets all objects of the MIB via the SCO UNIX tool *getone* from the SNMP agent and saves the return value in the *pramib.test* file.

The command needs as parameter the IP address or the name of the called ITK NetBlazer 8500.

7.10 Web Management (webMan)

The ITK NetBlazer 8500 Web Management Tool (webMan) is a graphical configuration and monitoring tool for ITK NetBlazer 8500 that is based on the World Wide Web technology (HTML, http).

WebMan uses the scohttpd (**H**yper**T**ext **T**ransport **P**rotocol **D**aemon) of SCO OpenServer Release 5.

webMan can be used from every web browser that supports HTML frames (for example Microsoft Internet Explorer >=V3.x or Netscape Navigator >=2.x).

During installation of ITK NetBlazer 8500 the webMan software and files are automatically copied to the disk and configured into the SCO httpd.

WebMan is started just by entering the ITK NetBlazer 8500 name or ITK NetBlazer 8500 IP address as URL in the Web browser. Access rights are based on predefined webMan users. See Chapter 8.5.8, *Installing ITK NetBlazer 8500 WebManager* (page 8-40).

The following features on the ITK NetBlazer 8500 homepage are already implemented and can be used:

Feature	where / how to use
Action Menu	upper-left frame
LED status display	upper right frame includes hostname, IP address and software version Use the following hypertext-links: Click on an **ISDN** LED or **Modem** LED to show controller information Click on the **Power** LED or **Temp.** LED to show the hardware status Click on the **Ready** LED to show the process-table (all running daemons) Click on the **Active** LED shows the connection-table (all running connections)

Feature	where / how to use
Hardware Status	lower frame shows temperature, CPU load and voltages

The following table provides a summary of the features and their meanings.

Feature	Meaning
Connections	Shows the current connections (as *pramon* function 1). Click on the *Con-Id* to obtain detailed connection data (as *pramon* function 2).
Controller	Shows the status of each B channel (and modem) by colored LEDs. Click on an LED to show the corresponding connection data, if existing.
OS-Operations	Shows a sub-menu with the following options: • Start: Starts ITK NetBlazer 8500 software (as command *start_practrl*) • Shutdown: Does a ITK NetBlazer 8500 shutdown (as *pramon* function *5*) • IP-Routing-table: Shows the IP routing table (as command *netstat -r*)
Logging	Shows the logging directory where directories and logfiles can be selected. Click on a logfile to get its contents.

Feature	Meaning
Accounting	Shows the accounting files. Click on an accounting file to get its contents in a formatted table. Click on the PID to get the corresponding logfile (errors).
Userlist	Shows a list of all active users (as *pramon -u*)
Configuration	Allows ITK NetBlazer 8500 configuration with the following sub-menu: • Parameter: Shows a list of all parameterfiles with following options: •view: Shows the textual parameterfile •change (click on filename): •show all parameters and values •change parameter values (with online-help) • Packet Filter:Shows the packet filter files
Manual	Shows the online ITK NetBlazer 8500 manual (with hypertext links).

7.10.1 Refresh

It is possible to adjust page-refresh of Connection-table, Controller-table, Process-table and LED-table. Also page-refresh while viewing files (if refresh is off the complete file is shown, if refresh is on the last lines of file are shown).

In each frame that supports refresh 5 buttons are shown at the upper right that enable/disable the refresh at different times:

- 10s Enable refresh every 10 seconds
- 30s Enable refresh every 30 seconds
- 60s Enable refresh every 60 seconds
- stop Stop refresh
- default Set refresh to default

The following new parameters (process.par) can be configured:

```
www_suprimon.www_refresh: 0      # time for refreshing page in seconds
                                   ( 0 = refresh off )
www_suprimon.www_reflines: 15    # count of lines shown at the end
                                   of file, if refresh is on.
```

7.10.2 Show licenses

The active licenses are shown in the hardware information frame.

7.10.3 Security enhancements

For extended security in file *access* with password (".sysaccess", ".groupaccess") the access may be restricted additionally by IP address (net, host or both). See sample file *u/pra/www/sysddm/dotgroupaccess* for details.

7.10.4 Show other systemfiles

Other system files can be viewed (with or without refresh) by entering a link to them in the log directory ("/u/pra/log").

Example:

After creating the following link the syslog file (system messages) can be viewed in the webMan logging frame:

```
cd /u/pra/log
ln -s /usr/adm/syslog syslog
```

Remark: NetBlazers can be configured to sent their system messages to the syslog daemon of another system (or the same) by setting the parameter "practrl.info_syslog_target" to the IP address of the syslog system. So all NetBlazer system messages can be concentrated and viewed on one system.

7.11 Internet Supplementary Services (ISS)

The Internet Supplementary Services (ISS) are used to enable the following features to subscribers of a switch that supports the ISS requirements (i.e. SIEMENS EWSD).

- **ISCI: Subscriber Control via Internet**

  ISCI allows a subscriber to control the services assigned to his telephone by using the web browser. This is provided via a graphical PC based user interface for telephone feature management. It uses IP to set parameters for subscriber related EWSD features and to retrieve various journal as well as accounting and billing information.

- **EWI: E-Mail Waiting Indication**

  EWI informs a user immediately that an Internet mail message has been received – even if there is currently no active Internet session. This indication is brought to the subscriber's telephone, either by a specific dial tone, by an announcement or by display information as appropriate and supported by the respective terminal equipment.

- **CWIB: Call Waiting Internet Busy**

  CWIB informs the subscriber during an active Internet session that an incoming call is waiting. This event is visualized to the user by an additional window opening on his screen and the user is asked to either accept or refuse the call. If the user decides to accept the incoming call the Internet session is cleared and the call is switched to the telephone.

- **CCIB: Call Completion Internet Busy**

  The feature 'Call Completion on Internet Busy' allows a subscriber who is currently engaged in an internet session to receive a voice phone call on his PC using voice-over-IP technology. The internet session is not terminated. Voice call and internet traffic can simultanously be handled on one analoge line, or on the original used ISDN B-channel(s) respectively.

- **IAVoIP: Improved Access to Voice over IP**

The feature allows a subscriber using his normal phone (POTS/ISDN) to place a call (typically long distance call) to another normal phone (POTS/ISDN) using the internet as transmission medium between both PSTN (accessed A- and B- phone). The A subscriber has to add an access code in front of the usual E.164 number of the B subscriber. The call is initiated by one-stage-dialling. There is no interactive dialogue to any voice responding system in the system.

The ITK NetBlazer 8500 is connected to the EWSD by PRI circuit(s). The D-channel is used to carry the Internet specific communication between EWSD and NetBlazer 8500. This is accomplished by enhancing the D-channel protocol implementation and RAS functionality.

Briefly, the functionality to be provided by NetBlazer 8500 is as follows:

- Provide a local IP address for a D-channel on request by EWSD (RARP request and response)
- Issue RADIUS requests to EWSD and process the RADIUS response for authentication and accounting
- Provide EWSD with the dynamic IP address for a subscriber after successful login
- Accept IP messages encapsulated in D-channel messages – issued by EWSD - and forward to router entity
- Accept IP messages issued by router entity, encapsulate into D-channel messages and forward to EWSD
- Establish H.323 voice connection to remote gateways

Internally a new daemon (the ISS daemon ISSD) coordinates the ISS communication. All data that is sent/received to/from EWSD goes through this module that is running only when the ISS functionality is needed. The ISS daemon provides all the features to implement the requirements described above.

For each D-channel (ISDN-card) a leased line process (LLP) is started that works like a line driver between EWSD and the ISSD (for one d-channel link only). After the LLP processes have registered at the ISSD data can be exchanged between EWSD and the NetBlazer 8500.

The new daemon ISSD and the leased line processes are automatically started and controlled by the PRACTRL process. The process state can be seen in the process table (in PRAMON or webMan).

The ISSD show the following process information:

Reg LLP <N>/<M>
<N> is the number of LLP that have been registered at the ISSD (number of usable PRI links).
<M> is the max. number of possible PRI links.

The LLP processes show the following process informations:

ISS C:<C> registering during registering at ISSD
ISS C:<C> registered after registering at ISSD
ISS C:<C> <a.b.c.d> after RARP-Response has been sent to EWSD
<C> is the number of the ISDN PRI board (controller).
<a.b.c.d> is the IP address used for the PRI link.

To enable the ISS features the following parameters must be set:

Parameterfile “iss.par” (new):

```
.start_iss:              1      # 1: start ISS-Daemon, 0: do not start ISS-
                                   Daemon
.iss_uip_pool:           100    # IP-Pool-ID for ISS IP addresses of EWSD
# Parameters for ISS leased lines processes (LLP):
.linecnt_isdn_ll:        2      # Number of leased lines (PRI links to EWSD)
isdn_ll_1.service:       ISS    # Service of 1st leased line
isdn_ll_1.controller:    1      # Controller for 1st leased line
isdn_ll_2.service:       ISS    # Service of 2nd leased line
isdn_ll_2.controller:    2      # Controller for 2nd leased line
```

Parameterfile “auth.par” (Authentication & Accounting):

To enable the RADIUS server in EWSD for online authentication:

```
.radius_online_port:     1812      # UDP port number
.radius_online_keyword:  [xxx]     # Shared secret to access RADIUS
                                     server
.stab_online_cnt:        1         # No. of Authentication-Servers
.stab_online_addr_1:     localhost # IP-Address of 1st Authent.-Server
```

To enable the RADIUS server in EWSD for accounting:

```
.radius_account_port:                  1813# UDP port number
.radius_account_keyword:               [xxx]# Shared secret to access
```

```
RADIUS server
.stab_acct_cnt:      1          # No. of Accounting-Servers
.stab_acct_addr_1:   localhost  # IP-Address of 1st Accounting-Server
```

Parameterfile “uip_pool.par” (User IP address pools):

```
To define IP addresses for the ISS links:
.ip_pool_[X]:        a.b.c.d  [netmask]  100   # IP-address pool for ISS links
```

For offline authentication (service selection) the RADIUS server in the NetBlazer 8500 is used.

To enable PPP as the default service the following RADIUS entry must be defined in the corresponding RADIUS configuration file (“/etc/raddb/users”):

```
DEFAULT User-Password = "SUPRIMO"
        Service-Type = Framed,
        Framed-Protocol = MP,
        ITK-PPP-Auth-Type = ITK-Auth-PAP,
        Filter-Id = "0"
```

8 Installing ITK NetBlazer 8500

The system is already preconfigured. No further installation or configuration is recommended. To add or change a board you should contact ITK.

This chapter describes the hard- and software installation of ITK NetBlazer 8500 as well as the PCI and Unix configuration. Please use Appendix E, *ITK NetBlazer 8500 Installation Checklist* (page E-1) to verify the steps during installation.

An industry system (for example ITK NetBlazer 8500) with SCO Unix (SCO Open Desktop/SCO Open Server) as a preinstalled operating system is required.

8.1 SCO OpenServer Release 5

ITK NetBlazer 8500 Version 5.00 uses some features that need the SCO OpenServer Release 5.0.4 operating system. The SCO Open Desktop Lite Release 3.0 software which has been used so far is no longer available and supported from SCO. Install therefore the SCO OpenServer (Desktop) Release 5.0.4 (or later) before installing ITK NetBlazer 8500.

The SCO OpenServer Release 5 supports a lot of new features. For ITK NetBlazer 8500 the following features are useful:

- **Subnetting:** TCP/IP Subnetting is supported. This allows for example the LAN adapter and the UIP pool to be in the same Class C Network that is cut into some subnets. Furthermore, these subnet information and routes can be propagated to other systems.
- **New routing protocols:** The new routing protocols RIP2 and OSPF are supported and can be used to learn and propagate routing information of subnets.
- **Support of the PCI bus**
- **man pages:** The man pages that were ommitted in SCO Open Desktop Lite Release 3.0 are included and can be used to look up the online documentation.

- **scoadmin:** The administration tool for changing SCO parameters has been enhanced. It is named *scoadmin* and has an X11 or Window based textual user interface.
- **httpd:** A Web server is contained which can be used to support a Web based graphical user interface for managing and monitoring ITK NetBlazer 8500. For further information see Chapter 7.10, *Web Management (webMan)* (page 7-92).

For other features of SCO OpenServer Release 5 see the product descriptions from SCO (www.sco.com).

Before installing SCO OpenServer Release 5 save all ITK NetBlazer 8500 configuration files (parameter files, firewall files etc.). Use for example the *save_config* tool.

You have three options for installing SCO OpenServer Release 5:

Option 1

Installing SCO OpenServer Release 5 local from CD ROM: a CD ROM drive must be connected (temporarily) to the ITK NetBlazer 8500.

Option 2

Installing SCO OpenServer Release 5 remote: A network installation (netisl) can be done from a remote SCO OpenServer system. This is only possible with a supported LAN adapter (for example 3COM-Ethernet-ISA).

Option 3

Installing SCO OpenServer Release 5 from disk: Copy the complete disk from a master disk, on which SCO OpenServer Release 5 and possibly the newest ITK NetBlazer 8500 software is installed.

For detailed information see the *SCO Open Desktop/ SCO Open Server Installation and Upgrade Guide* and *SCO Hardware Compatibility Handbook* and the *SCO Open Systems Software Hardware Configuration Guide*.

8.2 Installing Hardware

The following steps are necessary to install ITK NetBlazer 8500 hardware:

- Install the ITK Primary board(s) in your system.
- Install the ITK DigitalModem(s) in your system.
- Install the voice compression board(s).
- Install the IFB board in your system.
- Install the LAN and/or WAN board(s) in your system.

These steps are described in detail below.

Switch off the **PC** and to **disconnect the mains plug from the mains socket** whenever the computer has to be opened!

Never touch any of the contact pins of the **interfaces** (e.g. serial ports, parallel ports, Ethernet port, ISDN connection) or the **electronic components** without grounding yourself!
The electronic components can be **damaged** by **static discharge**!

Do not forget to fix the rubber stoppers in the case's cover to protect the boards.

8.2.1 ITK Primary

The ITK Primary board is ITK's board for the primary rate interface based on the PCI bus. It has the same features as the predecessor ix1-primary (EISA) plus the following enhancements:

- T1 support for US switches that support 1.55 Mbit/s (23 B channels)
- US D channel protocols (4ESS, 5ESS, DMS-100)
- PCI plug and play mode for automatic board recognition

- Voice compression

A special doanloadfile for the Primary/PCI boards “ixdummy.bin” can be used to deactivate the d channel.

8.2.2 Interface Board (IFB)

The **I**nter**f**ace **B**oard (IFB) contains a VGA display adapter, a watchdog device and a LED driver on one (PCI plus extensions) board.

Watchdog

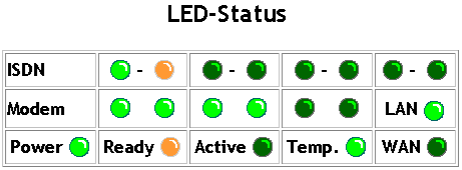
The watchdog device supports the following features:

- measuring the temperature inside the ITK NetBlazer 8500 housing
- measuring the power supply values (+5V, +12V, -5V, -12V)
- measuring operation time of the system
- Watchdog: resetting the system (coldboot), if a software trigger is not received periodically (about every 30 sec)

These informations are shown in pramon and webMan and can be used to detect errors.

LEDs

The LED display on the ITK NetBlazer 8500 front contains 20 LEDs and is connected to the LED driver:



These LEDs can be green, blue (only WebMan), orange or black (off).

The LEDs show a fast status of the ITK NetBlazer 8500 and may be of interest for an operator or service technician.

The ITK NetBlazer 8500 software switches the LEDs automatically if the software is running. For the meaning of the LED colors and additional information see Chapter 6.2, *LED status signaling (PCI)* (page 6-4).

The LED status can be displayed remotely with pramon and webMan, even if no PCI Interface Board is used (in EISA systems).

8.2.3 ITK DigitalModem

The ITK DigitalModem is a DSP board which supports 30 digital modems on one ISA board. The connection of an ISDN board and ITK DigitalModem boards over a MVIP bus is called MICA Technology (**M**odem **I**SDN **C**hannel **A**ggregation).

The DSP code on the ITK DigitalModem is downloaded from the ITK NetBlazer 8500 software. The new Portware (firmware for DigitalModem boards) supports the new V.90 protocol (56 kbit/s).

By default V.90 is enabled. To disable V.90 and support only V.34+ (33,6 kbit/s) or slower connections the following parameter must be set:

```
.capi_modem_initstring: ATS29=0
```

The DigitalModem II board is a low power variant of the already supported DigitalModem I board. The low power board has the same features and the same hardware and software interfaces as it's predecessor.

With the new DigitalModem II board up to 4 boards are supported in one system.

The DigitalModem boards must be configured with the card_config tool. Fully configured boards (30 modem ports) as well as partly configured boards (6, 12, 18 or 24 modem ports) are supported

In this version modem self-tests on ITK DigitalModem are not possible, but individual digital modems can be disabled/enabled in the ITK NetBlazer 8500 service table.

8.2.4 Voice compression board

To fulfill the compression and echo cancellation requirements special computing power is necessary. ITK NetBlazer 8500 uses a special hardware equipment with DSP (digital signal processing). These DSP boards are connected to the MVIP bus and contain multiple DSPs. Each DSP processes one or more voice channels. The DSP code on the voice compression board is downloaded from ITK NetBlazer 8500 software.

As DSP board the following boards can be used:

Name	Number of DSPs	Number of voice channels per DSP	Number of voice channels per board (with G.729A)
VIPER-12 542/PC	12	2	24
VIPER-12 548/PC	12	4	48

The new supported Viper C548 board contains DSP's with 80 Mips (C542 DSP's have 40 Mips). 4 DSP boards are supported in one NetBlazer system.

Mixed configurations: C548 and C542 boards can be mixed in one system, but C542 boards must be configured **before** C548 boards (related to I/O ports).

The voice compression boards must be configured with the card_config tool. Fully configured boards (12 DSP) as well as partly configured boards (4, 6 or 8 DSP's) are supported

The G.723.1 codec needs more processing power than G.729A, so less G.723.1 voice channels per DSP are possible than for G.729A. If the DSP resources are insufficient to support all voice channels the voice quality may diminish. If many G.723.1 connections will be used the DSP boards should be configured for less voice channels per DSP (in cards.par).

The following table shows the number of supported channels per DSP:

DSP type	number of G.729A channels [per DSP / per board]	number of G.723.1 channels [per DSP / per board]
C542	2 / 24	1 / 12
C548	4 / 48	3 / 36

8.2.5 Slot assignment

Slot assignment for ITK NetBlazer 8500 PCI

The slots are numbered this way: When looking from the front slot 1 is on the right side beside the power supply and slot 10 is on the left side. The following slot assignment is recommended:

Slot #	Slot assignment	Status
Slot 10	for modem / voice compression or other extension boards	optional
Slot 9		
Slot 8		
Slot 7		
Slot 6	4th ITK Primary	optional
Slot 5	3rd ITK Primary	optional
Slot 4	2nd ITK Primary	optional
Slot 3	LAN/WAN board	necessary
Slot 2	1st ITK Primary	necessary
Slot 1	IFB board	necessary

8.2.6 Installing LAN/WAN board

Install the 1st LAN/WAN board in slot 3.

ITK NetBlazer 8500 may be connected with different types of networks. Depending on the net, ITK NetBlazer 8500 can use one or more of the following LAN/WAN boards:

- Ethernet or Fast Ethernet board
- Token Ring board
- FDDI board
- Frame Relay board
- X25 board
- ATM board

8.2.7 Installing ITK Primary

No jumper setting is necessary to configure the ITK Primary board.

To install the ITK Primary board, perform the following steps:

(1) Install the 1st ITK Primary board.

(2) Connect interface COM2 and the 9 pin male connector of the ITK Primary board with the debug cable (9pin female connector on both sides).

(3) Compare the pin assignment of the S_{2m} connector with the one of the ITK Primary board. See Appendix A.1, *Product highlights / Technical data* (page A-1).

Optional: Install the 2nd board in slot 4 (PCI) / 2 (EISA).

Optional: Install the 3rd board in slot 5.

Optional: Install the 4th board in slot 6.

8.2.8 Installing ITK DigitalModem

PCI/ISA: Jumper setting is required for the installation.

To install the ITK DigitalModem board(s), perform the following steps:

(1) Install the 1st ITK DigitalModem (PCI: in Slot 10).

To install more than one ITK DigitalModem install the 2nd one in slot 9, the next ones in slot 8 and 7.

(2) Connect all the ITK Primary board(s) and ITK DigitalModem(s) with the MVIP cable. This cable is part of the shipment.

For ISDN boards that are connected to an MVIP bus the following configuration rules must be taken in consideration:

1. All ISDN boards need the same external clock
2. Configure only one ISDN board as MVIP master (use the external clock for the MVIP)
3. Configure all other boards as MVIP slave (inherit the clock from the MVIP bus)

8.2.9 Installing voice compression board

PCI: Jumper setting is required for the installation.

To install the voice compression board(s) perform the following steps:

(1) Install the 1st voice compression board in slot 9.

To install more than one voice compression board install the others in slot 8 and slot 7.

(2) Connect all the ITK Primary board(s), ITK DigitalModem(s) and voice compression board(s) with the MVIP cable. This cable is part of the shipment.

For ISDN, ITK DigitalModem and voice compression boards that are connected to an MVIP bus the following configuration rules must be taken in consideration:

1. All ISDN boards need the same external clock
2. Configure only one ISDN board as MVIP master (use the external clock for the MVIP)
3. Configure all other boards as MVIP slave (inherit the clock from the MVIP bus)

8.2.10 Additional information for slot usage and jumper setitings

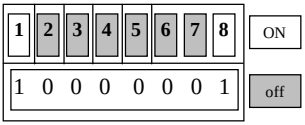
Slot 1 is the slot next to the CPU board; see Appendix A.2.1, *Slot-/IRQ-usage Overview* (page A-7) for further details.
Install metal springs between boards.

Adapter	Slot	Jumper / DIP-Switch *)	MVIP-Term. **)	Serial No.	RAM in MB
1. ITK Primary	2	E1/T1	X		64
2. ITK Primary	4	E1/T1	-		64
3. ITK Primary	5	E1/T1	-		128
4. ITK Primary	6	E1/T1	-		128
1. ITK DigitalModem	10	110011	(X)		
2. ITK DigitalModem	9	001011	-		
3. ITK DigitalModem	8	101011	-		
4. ITK DigitalModem	7	011011	-		
1. Voice compression board	9***)	0010	(X)		
2. Voice compression board	8***)	0110	-		
3. Voice compression board	7***)	1010	-		

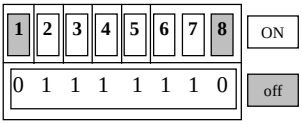
Annotations see next page.

*) **ITK Primary: DIP-switch setting for E1/T1 connection:**

Setting for E1 connection:



Setting for T1 connection:

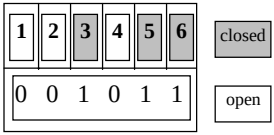


The setting must be according to the line connection used during the installation, configuration and testing. The appropriate setting according the customer requirements may differ, and must be adjusted before shipment (see 6.3.4). Please pay attention to use the right cable for E1 (RJ-48/RJ-45) resp. T1 (RJ-48/RJ-48).

ITK DigitalModem (Granite):

DIP-switch 6 to 1 is closed for „1“, open for „0“.

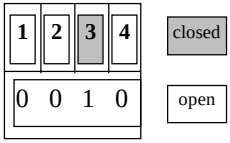
Example for 2nd ITK DigitalModem:



Voice compression board:

DIP-switch 4 to 1 is closed for „1", open for „0".

Example for 1st Voice compression board:



**) MVIP termination is set with jumper pairs near the MVIP connector on the boards. (jumper have to be installed).

For systems with five or fewer MVIP bus connections, it is adequate to place the circuit board that is the master clock source at one end of the cable and provide the termination on the circuit board which is physically at the other end of the cable.

On systems with more than five MVIP connections, both ends of the cable should be electrically terminated with jumpers. No other boards should terminate these lines. First ITK Primary in the rightmost position needs MVIP bus termination. On the other side only one board must be MVIP bus terminated. This is the ITK DigitalModem in slot 10. If no ITK DigitalModem is installed the ITK Voice compression (ITK VIPER) board in the leftmost position must be terminated.

Board	Jumper settings
ITK Primary (Jumper near MVIP connector)	 Jumper closed (MVIP bus terminated)
	 Jumper open (MVIP bus not terminated)
ITK DigitalModem	 Jumper J3 closed (MVIP bus terminated)
	 Jumper J3 open (MVIP bus not terminated)
ITK Voice compression board	 Jumper J2 and J4 closed (MVIP bus terminated)
	 Jumper J2 and J4 open (MVIP bus not terminated)

***) The slot numbers for voice compression boards must be adapted if ITK DigitalModem boards are also to be installed. Slot number is (10 minus *number of present ITK DigitalModem boards*):

1st ITK DigitalModem in slot 10, 2nd ITK DigitalModem in slot 9, 1st ITK Voice compression board in slot 8 and 2nd ITK Voice compression board in slot 7.

- Connect the boards with the MVIP-flat ribbon cable.

8.2.11 Finishing hardware installation

To finish hardware installation, perform the following steps:

(1) Connect COM 2 and first ITK Primary (MVIP master) with 9-pin Sub-D cable.

(2) Insert flat rubber blocks in the top cover (numbered places).

(3) Remount system cover.

8.2.12 Configuring PCI BIOS

To configure the PCI BIOS, perform the following steps:

(1) Plug in the keyboard, CRT display and power cord.

(2) Switch the main power on.

(3) Press <Del> key when prompted by BIOS message to enter BIOS setup.

(4) Check parameters and change if necessary.

For default parameter list see Appendix A.2.2, *ITK default BIOS Settings* (page A-8).

8.2.13 Configuring ISDN/modem board parameters

The ISDN/modem board parameters (for example D channel protocol, MVIP mode, language settings) you have to configure in the following file:

ix1.ini

(link in dat-directory to */usr/itk/ixload/ix1.ini*)

There is a section with parameters for each board with examples and possible values for each parameter. After a change of *ix1.ini* you have to reload the ISDN and modem boards with *ixload* or *shutdown-ixload*.

All possible parameters and values of *ix1.ini* you will find in Appendix D, *ix1.ini Configuration File* (page D-1).

MVIP modes for ITK Primary

If more than one ITK Primary board is installed the parameter <*mvipType*> must be set for each board as follows:

1st ITK Primary: mvipType=1 (Master)

2nd ITK Primary: mvipType=2 (Slave)

3rd ITK Primary: mvipType=2 (Slave)

4th ITK Primary: mvipType=2 (Slave)

CountryVersion codes

In the following table you find the CountryVersion codes for ITK DigitalModem:

Country	Coding	Code
US & Canada	µ-law	0x1
Taiwan	µ-law	0x103
International	a-law	0x200
Italy	a-law	0x201
Holland	a-law	0x205
Israel	a-law	0x206
Belgium	a-law	0x207
France	a-law	0x209
Sweden	a-law	0x210
Norway	a-law	0x211
Denmark	a-law	0x212
South Africa	a-law	0x213
Singapore	a-law	0x214
Austria	a-law	0x216

Country	Coding	Code
Germany	a-law	0x217
Switzerland	a-law	0x219
Russia	a-law	0x224
Turkey	a-law	0x227
Spain	a-law	0x231
Malaysia	a-law	0x234
Finland	a-law	0x237
Ireland	a-law	0x238
Portugal	a-law	0x241
Poland	a-law	0x253
Czech Republic	a-law	0x255
India	a-law	0x268
China	µ-law	0x273
International	µ-law	0x300
UK	a-law	0x400
Australia	a-law	0x402
New Zealand	a-law	0x403
Cyprus	a-law	0x417
Japan	µ-law	0x500

T1 Interface configuration

To configure the ISDN board from the default E1 interface to a T1 interface set the following parameters:

Parameter	Value
voiceCoding=2	µ-law
lineRate=2	PCM24 (T1)
lineCode=1	1=B8ZS or 2=AMI_WITH_ZCS
framingFormat=1	1=ESF, 2=SF(D3/D4), 3=F4, 4=F72
dsxPreemphasis=1	1= 0 - 115 feet, 2= 82 - 213 feet, ...
dProtocol=X	d-channel-protocol

After changing any board parameter that board (or all boards) must be reloaded to enable the new parameters. This can be done by PRAMON shutdown or by disabling/enabling the specific board.

8.3 Configuring new boards

To add (or remove) ISDN-, modem- or voice compression boards in (from) the ITK NetBlazer 8500 perform the following steps:

(1) Shut down and power down system.

(2) Open system cover.

Switch off the **PC** and to **disconnect the mains plug from the mains socket** whenever the computer has to be opened!

Never touch any of the contact pins of the **interfaces** (e.g. serial ports, parallel ports, Ethernet port, ISDN connection) or the **electronic components** without grounding yourself!
The electronic components can be **damaged** by **static discharge**!

(3) Insert new boards (or remove unused boards).

(4) See the Appendix E, *ITK NetBlazer 8500 Installation Checklist* (page E-1) to find the following information:

- slot usage
- Jumper and DIP switch settings
- MVIP termination
- hardware resources (IRQ, I/O port, shared memory)
- needed system memory (RAM)

(5) Close system cover.

(6) Power-up system and enter *single user mode*.

(7) Configure CAPI driver:

```
cd /usr/itk/capi
./card_config
```

(8) Enter boards. See *Reconfiguring CAPI20 driver* (page 8-42).

Hardware resources are read from hardware profiles (**.hw* files).

(9) The configuration file „/usr/itk/capi/cards.par“ is automatically generated and contains information about all boards and available ports. All ports are configured for the maximal variant of each board (i.e. 30 modems for ITK DigitalModem boards and 12 DSPs for voice compression boards).
If some boards support less ports the configuration file „cards.par“ must be changed manually.

(10) Reboot system:

```
reboot
```

(11) Login as *pra*.

If the ITK NetBlazer 8500 software is started automatically shut it down (pramon:5:1).

(12) Load all boards manually:

```
ixload
```

If ixload shows the warning

```
WARNING: No configuration file ix1.ini found, create a de-
fault file ix1.ini.
```

a new *ix1.ini* file with default values has been created.

Execute ixload again to check that all boards can be loaded (the hardware resources are configured correctly)

(13) Configure ISDN/modem board parameters (D channel protocol, language settings, coding, MVIP modes) in file *ix1.ini* as described in Chapter 8.2.13, *Configuring ISDN/modem board parameters* (page 8-13).

(14) Load all ISDN/modem boards with the new parameters

```
ixload
```

(15) Check that all boards have been loaded successfully.

(16) Load DSP boards with the command

```
viperload v54x.bin <Boardno> -1
```

where x is set to 2 for Viper 542 and 8 for Viper 548 board,
<Boardno> starts with 0 for the 1st DSP board.

(17) Start ITK NetBlazer 8500 software:

```
start_practrl
```

(18) Verify that all boards are running with the correct parameters:

```
pramon   (Cardtable: card info)
```

8.4 UNIX configuration

This chapter describes the adaptation of the Unix software because of hardware changes.

The following steps have to be performed in single user mode.

(1) Switch on the ITK NetBlazer 8500.

(2) As soon as the message:

INIT: SINGLE USER MODE

appears, type the root password (default is *itk*).

Hostname and boot mode adaptation

To adapt the hostname for ITK NetBlazer 8500 and to adapt the boot mode, perform the following steps:

(1) Set ITK NetBlazer 8500 system name:

```
uname -S <ITK NetBlazer 8500 name>
```

(2) Adapt */etc/hosts*

vi /etc/default/boot, should be set correctly as shipped; if not set add the following entries:

```
Set:    PANICBOOT=YES
Add:    TIMEOUT=10
```

8.4.1 Configuring TCP/IP

To configure TCP/IP, perform the following steps:

(1) Enter the following:

```
scoadmin
```

Installing a LAN/WAN board under Unix

The driver for the ethernet LAN board is on the disk labeled *SCO 3Com Driver.*

To install the LAN/WAN board under Unix, perform the following steps:

(1) Go to topic *Software Manager*.

software → install new → From <localhost> → Media Device: Floppy Drive

(2) Insert SCO Driver disk → continue

(3) Follow the instructions.

(4) Don't quit *scoadmin*.

Configuring TCP/IP layer

Follow these steps to integrate ITK NetBlazer 8500 into the local net:

(1) Go to topic *Networks*.

(2) *Network Configuration Manager* → Hardware → Add new LAN Adapter

(3) Choose *3com Etherlink XL PCI* adapter → Continue

(4) Add Protocol → SCO TCP/IP

(5) Enter the following

- hostname: [ITK NetBlazer 8500 name]
- IP-Address: [enter IP-address reserved for local testing]
- Netmask: 255.255.255.0
- Broadcast address: use default value
- Domain Name: _____ (see customer sheet)
- TCP connections: 1280
- Pseudo ttys: 64

(6) Quit.

(7) Answer the question *Do you want to relink* with YES.

(8) Answer the following questions during kernel rebuild with YES.

Set COM2: speed

Should be set correctly as shipped, otherwise, perform the following steps:

(1) mkdev serial → remove [r] → IBM-COM2 [2] → Create new Kernel [n]

(2) mkdev serial → install [i] → 1port card [1] → COM2 [2]
→ IBM-COM2 [2] → baud rate 9600 → again 9600 [1]
→ create a new kernel → No [n]

Create new kernel

To create a new kernel, perform the following steps:

(1) Type the following:

```
/etc/conf/bin/idbuild
```

(2) Kernel as default → yes [y]

(3) environment rebuild → yes [y]

(4) Boot system with:

```
reboot
```

(5) Wait until:

```
login:
```

appears.

(6) Check possible error messages. If necessary, review error messages after reboot with:

```
more /usr/adm/messages
```

8.4.2 Configuring user PRA

This user should be available as shipped, otherwise, perform the following steps:

(1) Login as *root* (password *itk*).

(2) Start *scoadmin*.

(3) Accounts → User → Add new user

(4) Enter the following:

- Login: pra
- comment: ITK NetBlazer 8500 standard user
- Modify defaults: yes
- login group: group
- login shell: ksh
- Homedirectory: /u/pra
- Home directory: Create Home
- User number: 200
- Type of User: Default
- create user: yes
- Password: now
- Force change: no

(5) pick Password: [Enter] → pra → pra

(6) Quit *scoadmin*.

8.4.3 Other useful system commands / options

Some other useful Unix commands / options to configure ITK NetBlazer 8500 are listed below:

Boot options (activates autoboot)

```
vi /etc/default/boot
set parameter "Timeout = 10" and "PANICBOOT = YES"
```

Activating SNMP support:

```
ln -s /etc/snmp /etc/rc2.d/S73snmp
ln -s /etc/snmp /etc/rc0.d/K73snmp
```

Making changes to the serial interface

```
mkdev serial → install → 1 port card → COM2 → IBM-COM2 →
baud rate 9600 → 9600
```

Configuring four virtual console screens and the first serial interface to login

```
enable tty1a; enable tty02
disable tty05; disable tty06; disable tty07; ...; disable tty12
```

Defining a user

The user *pra* is the predefined user to control the ITK NetBlazer 8500 software.

The user is already defined!

See Chapter 8.4.2, *Configuring user PRA* (page 8-21) to see how the user *pra* was defined.

Changing the IP address

To change ITK NetBlazer 8500 IP address, perform the following steps:

(1) Log in as *superuser* and type in at the Unix prompt:

```
netconfig
```

This is an interactive program which allows you to change the parameters of the IP stack.

The *Network Configuration Manager* window will appear.

The installed LAN adapters will be listed.

(2) Type <tab> to step into the window of current network configuration.

(3) Highlight entry „SCO TCP/IP“ for the network device to change.

(4) Type <tab> to come back to menu.

(5) Choose *Protocol* → *Modify protocol configuration*.

(6) The *SCO TCP/IP Configuration* window will appear.

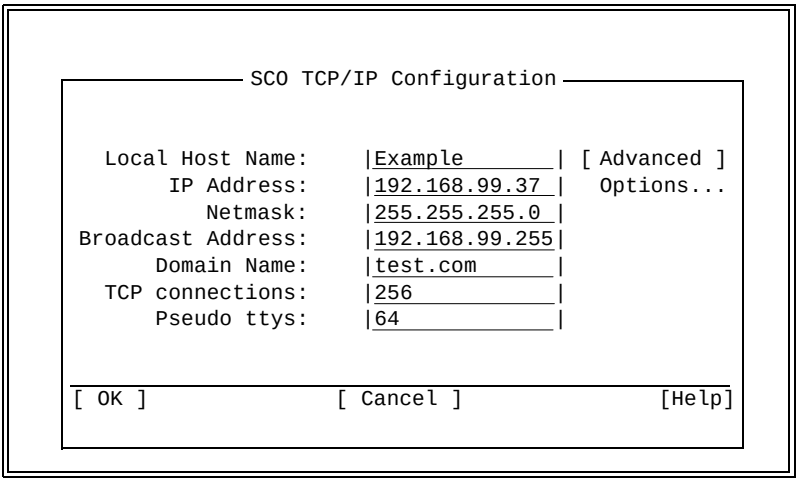


Fig. 8-1: *SCO TCP/IP Configuration* window

If necessary change the *Local Host Name*, *IP Address* and the *Netmask*. All other parameters should be set to default.

Remember:
If the *IP Address* is changed the IP addresses in
/u/pra/dat/auth.par and
/etc/raddb/clients
have to be changed too.
If *Local Host Name* or *IP Address* are changed verify new values in /etc/hosts.

Systemname

uname -s <your hostname>

prints ITK NetBlazer 8500 name

Changing ITK NetBlazer 8500 name

```
uname -U new_name
```

changes ITK NetBlazer 8500 name

Remember to correct the hostname in:
/etc/hosts

Adding or deleting routing entries

```
netstat -rn
```

the system lists the routing table

```
route add (net) <destination> <gateway> 1
```

adds a new entry in the routing table

This command adds a route to <destination> over the gateway <gateway>. If the keyword <net> is given. <destination> is a complete network.

```
route delete (net) <destination> <gateway>
```

deletes a route entry

```
route add default <dest.> <gateway> 1
```

adds a default entry into the routing table

The table located in */etc/rc2.d/S85tcp_default_route* is loaded while booting.

Adding symbolic hostnames (domains)

edit the file:

```
/etc/hosts
```

and add an entry like:

```
123.23.45.1          Peter Peter.default.com
```

where Peter is the name of the computer and default.com is the domain of the network.

Configuring DNS

DNS (**D**omain **N**ame **S**ervice) is used for identifying hosts with the help of a special Domain Name Server. The assignment of IP address and the Domain Name is configured in:

```
/etc/resolv.conf
```

with these two lines:

```
domain          itk.de
nameserver      123.456.1.2
```

Do not forget to enter your ITK NetBlazer 8500 name and IP address (for example ITKNetBlazer8500.default.com123.456.10.12)

Configuring the system to send SNMP traps to the NMS

edit the following file:

```
/etc/snmpd.trap
```

and insert a line with the SNMP community, the IP address of the NMS (Network **M**anagement **S**ystem) and the UDP port number 162.

Traps which are generated by ITK NetBlazer 8500 are sent to this node.

The ITK NetBlazer 8500 error trap numbers are in Chapter 6.3, *SNMP Traps* (page 6-7).

Restart the SNMP daemon.

Rebuilding the kernel

To take effect on changes of some of the above mentioned parameters a new kernel has to be build with the following command:

```
/etc/conf/bin/idbuild
```

After building a new kernel the system must be rebooted.

Rebooting the system

```
reboot
```

boots the system.

Before booting it is recommend to shutdown the ITK NetBlazer 8500 software using *pramon*. See Chapter 5, *Pramon* (page 5-1).

Or simply use the *pramon* shutdown option with reboot!

Halting the system

```
haltsys
```

stops the system immediately.

It is recommended to shut down the ITK NetBlazer 8500 software before executing *haltsys*.

Static routes

Static routes as well as the default router should be entered in the file */etc/rc2.d/S86tcp_default_route*. See man pages for *route*.

The current routes can be displayed with the command:

```
netstat -r
```

The following command can be used to show the routing-table of any other host, that has SNMP enabled:

```
/etc/getroute HOSTNAME public
```

To show the routes that are set from ITK NetBlazer 8500 the logfile of the *root_prog* daemon should be viewed. (*/u/pra/log/root_prog.log*)

Console terminal at COM1 port

The console terminal is used for UNIX console messages and as the only terminal port in single user mode. Normally a VGA display and a PC keyboard are used as the console terminal.

It is possible to configure a serial port (COM port) as console port. This serial console port can be used by every text terminal or terminal server device.

To change the console terminal to a COM port, perform the following steps:

(1) Enable the COM port for interactive login (getty daemon on device file):

```
enable  tty1a
```

(2) Edit file */etc/default/boot* to contain the following lines:

```
MAPKEY=YES      (mapping console keyboard)
SERIAL8=YES     (serial consol device)
SYSTTY=1        (enable serial port for console)
```

The changes take effect after the next reboot.

Routing daemons

To enable the (simple) routed (only RIP-1) the start of routed must be enabled in the */etc/rc2.d/S85tcp* file, that is normally commented out. See man pages for *routed*.

To enable the gated (routing protocols RIP, OSPF, EGP, BGP) a configuration file must be created. The following example shows a simple */etc/gated.conf* file for OSPF: (See man pages for *gated.*)

```
traceoptions internal external route rip update;
rip no;
ospf yes {
    backbone {
     interface net1 ; (interface name for LAN-adapter, see „netstat -i")
    } ;
} ;
```

SNMP daemon

The snmpd is configured in the following files (See man pages for *snmpd*):

File	Meaning
/etc/snmpd.conf	configuration file (with contact and location)
/etc/snmpd.comm	community configuration (who may access SNMP-objects)
/etc/snmpd.trap	trap-destination configuration
/etc/snmpd.peers	private-MIB configuration must contain the following entry for ITK NetBlazer 8500: "practrl" 1.3.6.1.4.1.1195 "pra")

To test the ITK NetBlazer 8500 MIB the *etc/getone* tool can be used. The following example gets the temperature:

/etc/getone HOSTNAME public 1.3.6.1.4.1.1195.3.2.2.1.0

See */u/pra/dat/pra.mib* to show the MIB objects and IDs.

DNS Resolver

For DNS resolution in the remote user clients the DNS resolver is not needed.

To ask a DNS (**D**omain **N**ame **S**erver) to resolve hostnames entered in the UNIX shell the resolver must be configured by editing the file */etc/resolv.conf*:

```
hostresorder local bind nis
nameserver a.b.c.d (IP-address of DNS)
```

The changes may influence ITK NetBlazer 8500 connections to authentication/accounting or other servers, especially if these servers are not entered in the DNS. The DNS resolver should be deactivated if some ITK NetBlazer 8500 features don’t work as expected.

8.5 Installing ITK NetBlazer 8500 software

The system is already preinstalled. Presently there is no further customer installation necessary.

The complete ITK NetBlazer 8500 software package is divided into two parts:

- **Root software**

  This part of the software contains all programs and files which can be executed by the user *root*. The installation can only be done by the *superuser*. The preconfigured password for *root* is *itk*.

- **PRA software**

  This part of the software contains all programs and files which can be executed by the user *pra*. The installation can only be done by the user *pra*.

First stop the running ITK NetBlazer 8500 software (user shutdown in PRAMON from user *pra*) then install the new ITK NetBlazer 8500 software.

The easiest way to install or update the ITK NetBlazer 8500 software is to use an installation host with the IP address A.B.C.D. (You will be informed by ITK if updates are available or if parts of a new installation are necessary. The required IP address will be given too).

8.5.1 Downloading software

Downloading Root software	Downloading PRA software
cd /tmp ftp A.B.C.D login as root cd /tmp get root.tar.Z get install_root get install_www bye	cd /tmp ftp A.B.C.D login as pra cd /tmp get pra.tar.Z get install_pra get pranotes.txt get Install.doc get update500.doc bye

The installation files are:

Installation File	Meaning
install_root	Installation script for the software running with root permissions
install_pra	Installation script for the software running with pra permissions
install_www	Installation script for the ITK NetBlazer 8500 web-Man software
root.tar.Z	Compressed tar archive containing the root software
pra.tar.Z	Compressed tar archive containing the ITK NetBlazer 8500 software
update500.doc	V5.0 Installation Guide & Release Notes (WinWord)
Install.doc	ITK NetBlazer 8500 PCI Hardware Installation Checklist (WinWord)

Installation File	Meaning
pranotes.txt	textfile containing the ITK NetBlazer 8500 release notes

These files have to be copied (by ftp or from distribution media) to the */tmp* directory of the ITK NetBlazer 8500.

Change the attributes of installation files with the following command:

```
chmod a+x install*
```

Now they are executable for the user *root* or *pra*.

8.5.2 Shutdown of running ITK NetBlazer 8500 software

Before installing the new ITK NetBlazer 8500 software stop the running ITK NetBlazer 8500 software. This is done with a user shutdown in the monitor program *pramon* (started from user *pra*).

8.5.3 Installing or updating

There are two possible modes of ITK NetBlazer 8500 installation:

Mode	ITK NetBlazer 8500 installation
Install	installs all files All device drivers are installed with default values or must be reconfigured manually.
Update	installs all files The device drivers need not be reconfigured (their old values retain). Update is not possible from versions < V5.00

In both ITK NetBlazer 8500 installation modes customer specific files are never overwritten by new files.

Customer specific configuration files are normally installed as sample files (extension: *.sample*). If a customer specific file does not already exist, the install process copies the sample file to the customer specific file (removes the *.sample* extension). Old customer specific files, which will be used no longer, are renamed to files with the extension *.old*.

ITK NetBlazer 8500 V5.0 contains a lot of new features in the device drivers. For this reason an update installation from ITK NetBlazer 8500 V1.xx, V2.xx, V3.xx or V4.xx to V5.xx is not possible and a complete installation with device driver configuration has to be done. See Chapter 8.5.4, *Installing/Updating root software* (page 8-33).

8.5.4 Installing/Updating root software

To install and update the *root software*, you have two possibilities:

- installing from **network**
- installing from **floppy disk**

In both cases you first have to log in as *root* (password: *itk*) and change to *tmp* directory.

Installing from network

To install ITK NetBlazer 8500 software from network, perform the following steps:

(1) Type the following

```
ftp [hostname/IP address of appropriate ITK NetBlazer 8500 software server]
```

(2) Login as *pra*.

(3) Type the following (replace x.yy with version number):

```
cd/usr/itk/Vx.yy/kit
prompt
mget *
bye
```

Installing from floppy disk

To install ITK NetBlazer 8500 software from floppy disk, perform the following steps:

(1) Insert first floppy disk.

(2) Type the following:

```
tar xv
```

(3) Insert floppy disks as prompted.

Starting root installation

To start the *root installation*, perform the following steps:

(1) Log in as *root* (password: *itk*).

(2) Change to *tmp* directory or to the directory where the ITK NetBlazer 8500 software kit was installed.

(3) The install scripts must be made executable (If it hasn't been done yet):

```
chmod a+x install*
```

(4) Start the installation with:

```
./install_root
```

The script installs the root software uncompressing the file *root_tar.Z* and configures the various kernel drivers. An automatic CAPI configuration (described below) follows.

During the installation the following device drivers are automatically installed with default parameters:

•Watchdog driver

•PA30=2 for PA30 Watchdog board (ISA bus)

•IFB=1 (default=1) for Kontron interface board (PCI bus)

•UIP driver (Interface: 192.168.18.254, Mask: 255.255.255.0, Channelcount: 120)

•VOIP driver (for Voice Compression DSP boards)

If the defaults are not sufficient, the device drivers should be reconfigured later. (see below)

The following chapters describe the reconfiguration of the device drivers:

- *Reconfiguring CAPI20 driver* (page 8-42).
- *Reconfiguring UIP driver* (page 8-45).
- *Reconfiguring watchdog driver* (page 8-44).
- *Configuring VOIP driver* (page 8-46).

An automatic CAPI configuration follows. See *Reconfiguring CAPI20 driver* (page 8-42).

(5) At the end of the installation configure the CAPI driver by entering the following information:

•Hardware-Platform (KPR_PCI, or <Enter> for default)

•Line-Rate for ISDN cards (E1 (30 ports) or T1 (23 ports), or <Enter> for E1)

•Number of ITK Primary cards

•Number of ITK DigitalModem cards (30 Modems)

•Number of modem ports for each ITK DigitalModem card

•Number of 542 DSP voice compression cards

•Number of DSPs for each 542 card

•Number of 548 DSP voice compression cards

•Number of DSPs for each 548 card

•Build a new UNIX-Kernel (y/n)

See *Reconfiguring CAPI20 driver* (page 8-42) for an example CAPI configuration.

8.5.5 Installing / Updating ITK NetBlazer 8500 software

To install or update pra software you have to log in as user *pra* (preconfigured password: *pra*).

Perform the following steps:

(1) Log in as *pra*.

(2) Change to directory *tmp* or to the directory where the ITK NetBlazer 8500 software was installed and start the installation with:

```
./install_pra
```

The script installs the pra software uncompressing the following file: *pra.tar.Z*

Older customer files that are not longer used will be renamed to **.old*.

The names of all used samples (copied to the original filename) are shown after the installation. Verify these files or change them if necessary.

Have a look at */tmp/install_pra.log* after the installation.

Configuring parameter files

The following parameter files (in */u/pra/dat* directory) must not be changed, because they will be overwritten with each new installation:

Parameter File	Meaning
param.par	includes all parameter files used
common.par	default values for all ITK NetBlazer 8500 parameters

The following customer-specific parameter files (in */u/pra/dat* directory) should be checked and/or changed:

Parameter File	Meaning
isdn.par	parameters for ISDN PRI interfaces
process.par	special parameters for processes, for example line-counters, PRACTRL parameters

Parameter File	Meaning
uip_pool.par	pool of dynamic IP addresses for remote IP users
auth.par	parameters for authentication and accounting
ppp.par	parameters for PPP and SLIP
dlm.par	parameters for **D**istributed **L**ine **M**anagement (DLM)
misc.par	miscellaneous parameters
l2f.par	parameters for L2F tunneling
cards.par	parameter for communication boards (automatically generated from the card-config tool)
voip.par	parameter for voice over IP (VoIP)
h323.par	parameter for H.323 (VoIP)
iss.par	parameter for Internet Supplementary Services (Siemens EWSD features)

The customer-specific parameter files will be preserved (will not be changed) in future installations. (Only the samples will be overwritten.)

Configuring firewall files

The format of the firewall files (in directory */u/pra/dat*) has not changed, so a configuration is not necessary, if a previous ITK NetBlazer 8500 version has been used.

Adapting uip_pool.par

To adapt the *uip_pool.par* file, perform the following steps.

(1) Enter UIP-Pool Address defined for this system:

Start address UIP-Pool (see installation list)

```
vi uip_pool.par
```

(2) Remove comment sign # and adapt line:

```
ip_pool_1:    [Start address UIP-Pool]255.255.255.224
```

In some cases it is necessary to reconfigure the netmask entry.

Adapting auth.par

To adapt the *auth.par* file, perform the following steps:

(1) vi auth.par

(2) Adapt line:

```
.Radius_Server:      [ITK NetBlazer 8500 name]
```

(3) Remove comment sign #:

```
.auth_prot:          Radius
.auth_req:           ABCZ
```

8.5.6 Installing RADIUS server

If the ITK NetBlazer 8500 is not to run a local authentication server (but use a remote authentication or application server) this section can be skipped.

A description of all ITK NetBlazer 8500 supported RADIUS and ITK attributes is in the */etc/raddb/rad_attr.txt* file.

Configuration files

The RADIUS daemon configuration files are in */etc/raddb*:

Configuration file	Meaning
dictionary	the definition of all attributes and values (should not be changed)
clients	configuration file describing which RADIUS clients (hostnames) are allowed to access this RADIUS daemon (client (hostname) and secret (password))

Configuration file	Meaning
users	database with all usernames/passwords and service selections

All hosts (ITK NetBlazer 8500s) that should access this RADIUS daemon must be entered in the *clients* file. For each host the client name (host-name) and the secret (password) must be entered. ITK NetBlazer 8500 uses normally the secret *test*.

All users that should access this ITK NetBlazer 8500 must be entered in the *users* file.

Starting RADIUS daemon

To start the RADIUS daemon manually perform the following steps:

(1) Login as *root*, password *itk*.

(2) Type the following command:

```
/etc/radius/S95ITK_AS
```

If the RADIUS daemon should start automatically perform the following steps:

(1) Login as *root*, password *itk*.

(2) Type the following commands:

```
cp /etc/radius/S95ITK_AS   /etc/rc2.d
vi /etc/raddb/clients
```

(3) Adapt line for special configuration, default *localhost* should work in most cases.

```
#Client Name          Key (secret)
#----------------     -------------------
[ITK NetBlazer 8500 name]test
```

8.5.7 Verifying the software installation

To verify the software installation, perform the following steps.

(1) Login as *root*, password *itk*.

(2) Check if the following files exist:

dir: /etc/rc2.d/ :S85uip, S95ITK_PRA, S95ITK_AS

dir: /dev/ : uip, ucip, IFB, capi20

(3) Boot system with:

```
reboot
```

(4) Check if all device drivers are listed while booting (uip, watchdog driver, all ITK boards, voice compression board).

(5) Check that there are no error messages listed while booting.

8.5.8 Installing ITK NetBlazer 8500 WebManager

To use the ITK NetBlazer 8500 Web Management tool to configure the SCO httpd as follows:

(1) Login as *root*, password *itk*.

(2) Change to the *tmp* directory with:

```
cd /tmp
```

(3) Type the following:

```
./install_www
```

Default WebMan access rights

The default access rights for all webMan functions are based on a user/ password scheme that is not in junction with the UNIX user and group scheme:

- All users in the group *users* are allowed read-access.
- The administration functions (parameter changes, OS operations) are only allowed from user *admin.*

The pre-installed administration user is *admin* (with password *itk*).

The pre-installed standard user is *pra* (with password *pra*) in the group *users*.

Normally the ITK NetBlazer 8500 access should be restricted by packet filter and firewall mechanisms and the pre-installed webMan users need not be changed (only for expert users!).

Adding new WebMan users

All webMan users must be defined in the */u/pra/www/sysadm/.htpasswd* file, which should not be changed manually.

A new user in this file is created with the following command (from user *root*):

```
cd  /u/pra/www/sysadm
./htpasswd  .htpasswd  USERNAME
```

(The same command can be used to change the user password.)

The new user must be entered into the group *users* by manually changing the */u/pra/www/sysadm/groupaccess* file.

Using host access

By using host access the webMan usage can be restricted by IP host or IP network addresses.

To enable host-access the */u/pra/www/sysadm/.hostaccess* file must be changed manually. Additionally, the links in the WWW directories must be changed to point to the *.hostaccess* file instead of the *.groupaccess* file.

Configuring SCO http

The SCO http daemon is configured in the */var/scohttp/conf/scohttpd.conf*.

After changing the configuration the httpd must be stopped and started again:

```
/etc/scohttp  stop
/etc/scohttp  start
```

8.5.9 Manual driver reconfiguration

The following chapters describe the **manual** reconfiguration of drivers. This is only necessary, if the default configuration is not sufficient or if the configuration should be changed later.

Reconfiguring CAPI20 driver

The CAPI20 device driver (*/dev/capi20*) is necessary to have access to the ITK ISDN- and Modem-Cards and voice compression boards.

The CAPI driver configuration has been enhanced so that preconfigured board configurations with pre-defined slot and hardware resource usage (IRQ, I/O port, shared memory) can be used. So normally not every embedded communication board has to be specified.

The CAPI20 driver must be reconfigured for V5.00.

To install/update ITK NetBlazer 8500 software, perform the following steps:

(1) From user *root* install and configure the CAPI20 driver with the commands:

```
cd /usr/itk/capi
./card_config
```

(2) Follow the displayed instructions.

(3) Please answer the following questions according to your hardware installed:

(4) Select hardware platform from following list:

- 1. kpr_pci.hw: #!Platform: Kontron KPR-PCI
- Number of Hardware Platform (default:1): [select platform or just press <Enter>]
- PRI-Type (E1:30 ports,T1:23 ports) (default:E1): [enter option or press <Enter>]
- Number of ITK Primary cards: [enter number]

- Number of ITK DigitalModem cards (30 Modems): [enter number]
- Number of modem ports for each ITK DigitalModem card
- Number of 542 DSP voice compression cards (24 voice channels): [enter number]
- Number of DSPs for each 542 card
- Number of 548 DSP voice compression cards (48 voice channels): [enter number]
- Number of DSPs for each 548 card
- Build new UNIX-Kernel (y/n) ? [y]
- Kernel as default → yes [y]
- environment rebuild→ yes [y]

Configuration Example

The following example shows a configuration on a PCI system with 4 ITK Primary, 2 ITK DigitalModem and 1 DSP card:

```
card_config V1.3: Configurator for communication-cards
=======================================================
(Copyright ITK Telekommunikation AG)
   Hardware-Base: pci
   Select Hardware-Platform from following list:
      1. kpr_pci.hw:    #!Platform: Kontron KPR-PCI
Number of Hardware-Platform (default:1): 1
   Using Hard-Platform kpr_pci.hw
PRI-Type (E1:30 ports,T1:23 ports) (default:E1): E1
   Number of ports for PRI-interface: 30 (E1)
Number of ITK Primary/PCI-cards             : 4
Number of ITK DigitalModem-cards (30 Modems): 2
Number of ports on 1. ITK DigitalModem (default: 30):
Number of ports on 2. ITK DigitalModem (default: 30):
Number of ITK VIPER-XX 542-cards (max: 24 channel on 12 DSPs): 1
Number of DSPs on 1. ITK VIPER-XX 542 (default: 12):
Number of ITK VIPER-XX 548-cards (max: 48 channel on 12 DSPs):
  Enter card 1.DigitalModem:ISA
(slot:0,irq:0,io:0x0330,sm:0xD0000,ports:30)
   Enter card 2.DigitalModem:ISA
(slot:0,irq:0,io:0x0340,sm:0xD1000,ports:30)
   Enter card 1.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
   Enter card 2.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
   Enter card 3.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
```

```
   Enter card 4.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
  Enter card 1.VIPER-12_542:ISA (slot:0,irq:0,io:0x3280,sm:0,ports:12)
  configured: 4 ISDN-cards  with 120 ports
              2 Modem-cards with 60 ports
           1 Compression-cards with 24 channels an 12 DSPs
Installing capi20-Driver ...
   capi20-Driver has been installed successfully
Build new UNIX-Kernel (y/n) ? y
Building UNIX-Kernel ...
        The UNIX Operating System will now be rebuilt.
        This will take a few minutes.  Please wait.
        Root for this system build is /
        The UNIX Kernel has been rebuilt.
Do you want this kernel to boot by default? (y/n) y
Backing up unix to unix.old
Installing new unix on the boot file system
The kernel environment includes device node files and /etc/inittab.
The new kernel may require changes to /etc/inittab or device nodes.
Do you want the kernel environment rebuilt? (y/n) y
The kernel has been successfully linked and installed.
        To activate it, reboot your system.
Setting up new kernel environment
```

In the parameter file define the communication board configuration:

```
/usr/itk/capi/cards.par
```

which is automatically created, if a preconfigured standard configuration is used.

If other configurations are used, you have to edit this file manually. See Chapter A.7, *All parameters from cards.par* (page A-74).

Reconfiguring watchdog driver

Normally the watchdog driver is installed automatically and a reconfiguration is not necessary.

The watchdog device driver (*/dev/IFB* for PCI) allows access to the watchdog hardware (get hardware status (temperature, voltages), trigger the watchdog and light LEDs on the front panel) and is installed automatically.

The watchdog driver can be configured manually with the following commands:

- Kontron IFB board:

```
cd /usr/itk/IFB
./INSTALL
```

Reconfiguring UIP driver

Normally the UIP driver is installed automatically and a reconfiguration is not necessary.

The UIP device driver (user IP, */dev/uip*) allows the access to the IP-Routing-Layer of the operating system and is needed to access the IP routing stack for RAS services (PPP, SLIP). It has been enhanced to select the IP address for the connection from the ITK NetBlazer 8500 software instead of managing a pool of IP addresses in the driver (UIP pool).

This enhances the process of changing the UIP addresses, because in this case the UIP driver does not have to be reconfigured and no kernel has to be built (and no reboot).

Normally the default UIP values are sufficient and need not be changed. Changes are required only in configurations that use special LAN-to-LAN communications.

The UIP driver is automatically updated. If you want to specify special parameters, you have to reconfigure the UIP-driver as follows:

(1) To specify special parameters, reconfigure the UIP driver with the following commands:

```
cd /usr/itk/uip
./INSTALL
```

Standard Values are:

```
IP Address of UIP device      : 192.168.18.254
Netmask of UIP device         : 255.255.255.0
Maximum Number of Channels: 120
Do you want to do change any of these parameters (y/n) ?  n
Add driver to system
Your System is reconfigured.
Do you want to rebuild the system [y/n]?:  y
```

(2) In the parameter file define the UIP configuration:

```
/usr/itk/uip/uip.par
```

which is created automatically and must not be changed.

Configuring VOIP driver

Normally the VOIP driver is installed automatically and a reconfiguration is not necessary.

The VOIP device driver (*/dev/voip*) allows the access to the DSP boards (for voice compression) and is installed automatically.

The VOIP driver can be configured manually with the following commands:

```
cd /usr/itk/voip
./INSTALL
```

Building new UNIX kernel

This step is only necessary if a new kernel (system) has not been built in the previous steps.

(1) After configuring all device drivers a new UNIX kernel must be built with the following command:

```
/etc/conf/bin/idbuild
```

8.5.10 Licenses

The ITK NetBlazer 8500 V5.0 Software needs license keys for the following major features:

- RAS: Remote Access (ISDN and modem)

- VoIP: Voice over IP
- ISS: Internet Supplementary Services (for Siemens EWSD)

Before starting the software the license keys must be entered in the parameterfile „misc.par“(parameter „*.LICENCE_KEY_xxx*“)..

8.5.11 Restarting system

(1) After installing the new software restart ITK NetBlazer 8500 from the user „root“ with the following command:

```
reboot
```

8.5.12 Creating ix1.ini file after installing / updating Software

After installing or updating NetBlazer 8500 Software a new ix1.ini file has to be created.

(1) Login as „pra"

(2) If the NetBlazer 8500-software is started automatically, shut it down (pramon:5:1)

(3) Load all ISDN-/Modem-boards manually:

```
ixload
```

If the NetBlazer 8500-software wasn’t started automatically, ixload shows the Warning

„WARNING: No configuration file ix1.ini found, create a default file ix1.ini."

A new ix1.ini file with default values has been created, the original ix1.ini has been backuped as ix1.ini.xxx (where xxx is the highest number of saved ix1.ini files).

(4) Update the default values of the new ix1.ini file with the settings of the saved ix1.ini.xxx.

(5) Start NetBlazer 8500 software

```
start_practrl
```

(6) Verify that all boards are running with the correct parameters

(7) pramon (Cardtable: card info)

8.6 Cleanup

After successfully installing the ITK NetBlazer 8500 software the kit files can be removed from the install directory (normally */tmp*).

8.7 Saving / restoring configuration files

The *save_config* script saves / restores the necessary configuration files to / from a floppy disk or a tar file.

Perform the following steps:

(1) Log in as *root* and type the following at the Unix prompt

```
save_config
```

A self-explanatory menu with the options backup and restore to / from a floppy or tar file will appear.

(2) Save / restore your configuration files.

A Product Information

A.1 Product highlights / Technical data

Internet telephony

- Voice over IP gateway for ISDN and PSTN
- H.323, H.225, Q.931, H.245
- G.711, G.723.1, G.729A, G.165
- Echo cancellation
- RTP/RTCP
- Least-cost routing
- Phone-to-phone
- Phone-to-computer
- Call-back

ISDN

- PRI
- DSS-1, Q.931, 1TR6, 5ESS

Backbone

- Ethernet, Fast Ethernet, Token Ring, FDDI
- Frame Relay, X.25, ATM

X.25-PAD (X.3, X.28, X.29)
The concept for realizing a remote access to X.25 via PAD with ITK NetBlazer 8500 is described in the technical Concept ITK NetBlazer 8500 *X.25-PAD Solution*. Please contact your distribution partner.

Scaleability

- Up to 60 digital channels
- Up to 60 modem channels
- Up to 60 voice channels

- several systems may be cascaded

Protocols

- HDLC, X.75, V.110
- V.21-V.90, MNP2-5, MNP10, V.42/V.42bis
- PPP, PAP, CHAP, SLIP, CSLIP
- ML-PPP
- TCP/IP, TCP clear
- Tunnelling according to L2F method (Cisco's layer 2 forwarding)
- ITK NetBlazer 8500 tunnelling protocol
- X.25 access router (X.31, X.3, X.28, X.29)

Line management

- Dynamic and static IP addresses
- LAN/LAN connection
- Short Hold
- Distributed Line Management (multiple access system)

Authentication / Security

- RADIUS (**R**emote **A**ccess **D**ial-**I**n **U**ser **S**ervice)
- ADNS (**A**uthentication **D**omain **N**ame **S**ervice)
- Security Dynamics (SecurID)
- Flexible authentication (multiprovider support)
- Dynamic, session related packet filtering
- Extensive system control and recovery (watchdog)

Accounting

- Provider specific accounting (RADIUS)
- Session related accounting records
- Accounting files

Configuration / Management / Trouble-Shooting

- Easy configuration tools
- SNMP
- MIB I, MIB II, private ITK NetBlazer 8500-MIB
- TELNET, FTP
- Management via WWW

Sizes and weights

- 448 * 410 * 165 (w * d * h)
- front panel: 483 * 177 (w + h)
- weights:
  chassis, incl. Ethernet card: 16.0 kg
  ITK Primary: 300 g
  ITK DigitalModem: 400 g
  Viper C542 / C548 : 250 g

Environmental conditions

- temperature:
  5°C to 50°C (in operation)
  -20 °C to 60°C (non-operating)
- humidity:
  20% to 80% non condensing

Basic assenmbly requirements

- Horizontal air convection, supported by fan
- chassis stackable in 19'' rack
- Power supply:
  115/230 V(AC): 250W

Pin assignment of the S_{2m} connector

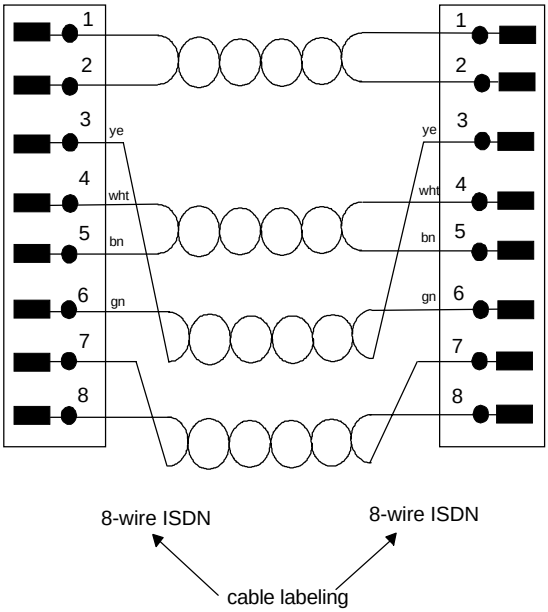


Fig. A-1 Cable assignment for symmetrical cable (RJ48C-RJ48C)

NT PRI CO				RJ45	RJ48C
contact no.	labeling		function	contact no.	contact no.
1 2 3			power supply		
4	FPE				
5 6 7	**a** PRI b s		ITK→NT	3 Tx 6 Tx	4 Tx 5 Tx
8 9 10	**a** PRI b s		ITK←NT	4 Rx 5 Rx	1 Rx 2 Rx
11 12 13	s **a** UK2 b				
14 15 16	s **a** UK2 b				

Fig. A-2 Structure and NT PRI terminal strip assignments for NT PRI CO (PCI)

Fig. A-2 shows the structure and terminal strip assignments for an NT PRI CO. The connection assignments are on the left side of the NT PRI CO and the assignments for the RJ 45 and the RJ48C jack on the right side.

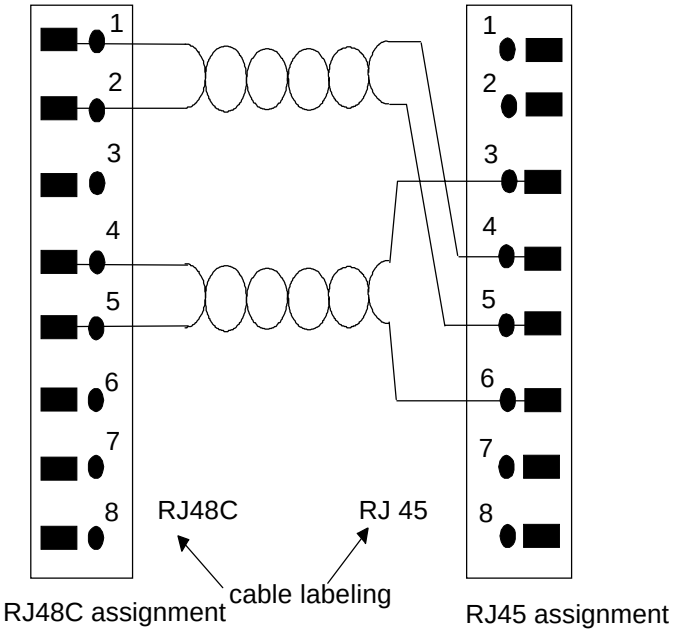


Fig. A-3 cable assignment for asymetrical cable (RJ48C-RJ45)

A.2 Configuring PCI BIOS

The following settings are shipped by default (Version 1.41):

Slot 1 is the slot next to the CPU board.

A.2.1 Slot-/IRQ-usage Overview

Slot-No.	Interface	IRQ	IRQ usage
1	Interfaceboard (IFB), fix	-	PCI
2	**1**. ITK Primary PCI	5	PCI
3	3c900 Ethernet, fix	9	PCI
4	2. ITK Primary PCI (opt.)	5	PCI
5	3. ITK Primary PCI (opt.)	5	PCI
6	4. ITK Primary PCI (opt.)	5	PCI
7	4. ITK DigitalModem / 3. Voice compression board (opt.)	7/-/-	ISA
8	3. ITK DigitalModem / 2. Voice compression board (opt.)	15/-/-	ISA
9	2. ITK DigitalModem / 1. Voice compression board (opt.)	11/-/-	ISA
10	**1**. ITK DigitalModem (opt.)	10/-	ISA

A.2.2 ITK default BIOS Settings

Setup

Standard

Pri Master

Entry	Setting
Type	Auto
LBA/Large Mode	ON
Block Mode	ON
32Bit Mode	Off
PIO Mode	4

Pri Slave

Entry	Setting
Type	Not Installed

Sec Master

Entry	Setting
Type	Not Installed

Sec Slave

Entry	Setting
Type	Not Installed

Date / Time

Entry	Setting
Date	check date
Time	check time

Floppy A

Entry	Setting
Type	1.44MB 3 1/2

Floppy B

Entry	Setting
Type	Not Installed

Advanced Setup

Entry	Setting
Quick Boot	Enabled
BootUP Sequence	A:, C:, CDROM
BootUP NumLock	Off
Floppy Drive Swap	Disabled
Floppy Drive Seek	Disabled
Mouse Support	Disabled
System Keyboard	Absent

Entry	Setting
Primary Display	VGA/EGA
Password Check	Always
OS/2 Compatible Mode	Disabled
Wait For ‘F1’ If Error	Disabled
Hit ‘DEL’ Message Disp.	Enabled
Internal Cache	Write back
External Cache	Enabled
System BIOS cache-able	Enabled
C000, 16k Shadow	Cached
C400,16k Shadow	Cached
other Shadows	Disabled

Chipset Setup

Entry	Setting
IRQ12/ Mouse Function	Disabled
8Bit I/O recovery time	1
16Bit I/O recovery time	1

Power Management

Entry	Setting
power management / apm	Disabled

PCI/PNP Setup

Entry	Setting
Plug and Play Aware O/S	NO
PCI Burst Mode	Enabled
PCI Concurrency	Enabled
PCI Streaming	Enabled
PCI Latency Timer (PCI clock)	64
PCI VGA Palette Snoop	Disabled
Allocate IRQ to PCI VGA	NO
PCI IDE BusMaster	Enabled
Offboard PCI IDE Card	Auto
PCI Slot 1 IRQ Priority	5
PCI Slot 2 IRQ Priority	5

Entry	Setting
PCI Slot 3 IRQ Priority	9
PCI Slot 4 IRQ Priority	5
DMA Channel 0	PnP
DMA Channel 1	PnP
DMA Channel 3	PnP
DMA Channel 5	PnP
DMA Channel 6	PnP
DMA Channel 7	PnP
IRQ3	PCI/PnP
IRQ4	PCI/PnP
IRQ5	PCI/PnP
IRQ7	ISA/EISA
IRQ9	PCI/PnP
IRQ10	ISA/EISA
IRQ11	ISA/EISA
IRQ14	PCI/PnP
IRQ15	ISA/EISA
Reserved Memory	Disabled

Peripheral

Entry	Setting
OnBoard FDC	Auto
OnBoard Serial Port 1	2F8
OnBoard Serial Port 2	3F8
Serial Port 2 Mode	Normal
OnBoard Parallel Port	Disabled
OnBoard PCI IDE	primary

In most cases the shipped configuration should work.

A.3 Troubleshooting

A.3.1 Accounting files

The accounting files list connection data (type, PID, caller ID, ...) of finished connections and are located in the directory */u/pra/log*. They are helpful for generating statistical reports or finding a certain log file in case of errors. See *section Finding logfiles* (page A-20).

The files look like:

pra_970226.acc, where 970226 stands for the date: 26/02/97

For an easy analysis an accounting file can be imported to Excel. (Download the file via ftp to PC, start Excel, choose file/open and select the file which should be opened, click continue and insert " : " in the field *others*.)

For further processing accounting data in billing system "iPhonEX" (vendor MIND CTI Inc.) a conversion of ITK NetBlazer 8500 accounting data into CDR (**C**all **D**etail **R**ecord) format is necessary. Conversion tool *acc2cdr* is described in Chapter 7.8.1, *acc2cdr* (page 7-87).

The following fields are displayed:

Field	Meaning
Type	connection type
PID	Unix process ID that handled the connection
Starttime	when the process was started
Endtime	when the process was stopped
Rcv- / SndBytes	number of received and sent bytes
Caller-ID	Caller ID of user
Username	
DDI	dial extension for **D**irect **D**ial-**I**n

Field	Meaning
ISDN-Prot	ISDN protocol (HDLC, MVIP (analog), V110, X75)
User-Prot	sPPP_PAP / CHAP, aPPP_PAP / CHAP
UIP-Addr	User IP address
V.110-Baud	baudrate of a V.110 connection (e.g. GSM)
M-Baud	baudrate of a modem connection
M-Prot	modem protocol
M-Comp	compression protocol of modem connection
M-Contr	number of used modem card
M-ID	number of modem on the board
AS-IP-Adr	IP address of the application server
Auth-IP-Adr	IP address of the authentication server
Errorcode	What happened to the process (e.g. shutdown)
Terminator	Who did sth. (e.g. operator stopped process)
Serv-Ind / Add-Info	Shows signaled service and the additional info corresponding to the 1TR6 norm
Timeslot	Number of the used ISDN timeslot
Direction	Direction of the connection (incoming, outgoing)
IP-Filter	Used packed filter
Tunnel-Prot	Used tunneling protocol (EMAS, L2F)
Tunnel-IP-Addr	IP address of tunnel end

Field	Meaning
Tunnel-Cause	Reason for closing tunnel (look at L2F-Draft specifications)
ISDN-Contr	Number of ISDN controller (1st / 2nd ITK Primary)
Charges	Number of monetary unit
Duration	Duration of the connection (in seconds)
Hostname	Hostname
PPP-Compr	Used ppp compression (STAC, PRED1 ...)
VoIP-Dial-No	Dialed destination number
VoIP-Called-No	Called number to reach callee (answer from LCR)
VoIP-Gateway	IP address of used dial-out gateway
Call-Duration	Duration of the dial-out call (in seconds)
VoIP-Compr	Compression protocol (G.711, G.729...)
DSP-Board	Number of used DSP board (1st board =100)
DSP-Chan	Number of used DSP voice channel (1-24)
Packet-Lost	Lost packet count (in percent)

A.3.2 Logging

If ITK NetBlazer 8500 does not work as expected, occurring errors can be pursued in the logging files.

Common.par predefines the logging facility but changes should only be made to the file process.par (data logging) or in h323.par (voice logging) because common.par is overwritten in case of a software update.

Note that the h323d (VoIP) is using an special logging interface (see section *Logging interface for H.323* (page A-19)).

Use the following syntax to switch on the logging:

```
process.log_kindoflogging_logparameter
```

with:

process:	process which is logged	
kindoflogging:	error, data, msg, info, fstart, fend	
	error:	all occurring errors are logged (switched on by default)
	data	logs all the data sent and received (default: off)
	msg	logs all messages built in by the developer (default off) Message logging is a tool for the ITK developers. If the problems cannot be solved, send the msg logging of the specific process where the error occurs to ITK.
	info	like error logging with additional connection infos (default off)
	fstart:	is only used by developers
	fend:	is only used by developers
logparameter:	_file, _format, _depth, _fname, _level	
	_file:	Name of Output device (Device, File, <STD-OUT> or <STDERR)) (no value → no Logging)
	_format:	Format of output (combinations possible): Z = show time z = show date Y = show logging type F = show name of function D = show name of module (filename) T = show calling-depth P = show Process ID (PID) X = show logging text

C = do buffer-clear (Flush) after logging output

O = write output additionally to STDOUT

S = show stack of calling functions

A = do not open logfile, if not already open

* = show all (no value → no logging)

depth: filter for calling depth (from-to)

_fname: filter for function names (separated by ',', skip function with '!', wildcard '*' at end)

_level: logging level (set bit for bit, combinations possible) (only for data logging)

The output of data logging can be filtered by selecting one or more data levels. Each level defines data in different places of the ITK NetBlazer 8500 software. You can select the following levels:

0x00000001	received SPC packets
0x00000002	sent SPC packets
0x00000004	received CAPI packets (from USER)
0x00000008	sent CAPI packets (to USER)
0x00000010	received Shell packets (from LAN)
0x00000020	sent Shell packets (to LAN)
0x00000040	received IP packets (LAN to USER)
0x00000080	sent IP packets (USER to LAN)
0x00000100	received PSP packets (from LAN)
0x00000200	sent PSP packets (to LAN)
0x00000400	received L2F packets
0x00000800	sent L2F packets
0x00001000	internal tables of L2F daemon
0xffffffff	log all levels
0x00000000	log no level

To select the kind of data logging:

- select the level **dynamically** within pramon

  or

- select the level **statically** by setting the ITK NetBlazer 8500 parameter *.log_data_level* to an appropriate bit mask

Normally all levels are logged if data logging is enabled.

Changes to the logging-facility take effect if the ITK NetBlazer 8500 software is restarted. Optionally a dynamically switching is possible using PRAMON.

Example

The following default entry enables error-logging for the process isdn_ll_1 (leased line) and the data is written to a file. $(MSG_LOGFILE) is a macro defined at the beginning of *common.par.*

isdn_ll_1.log_error_file: $(MSG_LOGFILE)

Logging interface for H.323

The h323d is using an special logging interface. It is possible to configure several logging levels and component masks.

Common.par predefines the logging facility but changes should only be made to the file *h323.par* because common.par is overwritten in case of a software update.

The following logging interface level are relevant to the h323d:

Error	0
Warning	1
Info	2
Commands (internal)	3
LAN messages	6
All details	8
Periodic events	19

The default logging interface level may be for example 10. That means all logging messages of level 0 to 10 are shown but not the periodic events (timer check, e.g.).

The following logging interface component masks are relevant to the h323d:

Log no components/modules	0x00000000
ASN	0x00000004
H.245	0x00000010
H.323	0x00000080
Q.931	0x00000100
Miscellaneous	0x00000200
Protocol handler	0x00000400
Main module	0x00000800
SPC wrapper	0x00001000
Log all components	0xffffffff

It is possible to set the logging interface component mask bit for bit and combinations are possible.

The default logging interface component mask may be e.g. 0xffffffff. That means all logging messages of all components are shown.

Note that the logging interface levels and component masks have only influence on the modules in the h323d using the interface, for example if message logging is on but the interface level is 0 there will be still appearing messages (from SPC, e.g.). The logging interface levels are different from the data logging levels!

If you use the dynamic enable/disable logging feature of the PRAMON you can switch message and/or data logging for h323d on or off. That means using of the logging interface is also switched on or off.

Note that the configured parameters for the logging interface are still valid. If you dynamically switch message logging on but the logging interface level is 0, you get only error messages or messages which do not use the interface (e.g. SPC).

Finding logfiles

1. Search for the specific entry in the accounting files and bear the PID in mind. The accounting files are located in the directory */u/pra/log*. Compare with *Chapter A.3.1, Accounting files* (page A-14).

   (Optional the PID can be determined using Pramon.)
2. The logfiles are in the */u/pra/log/date* directory. (date is for example:

19971202)

Example:

```
/u/pra/log/19961205
```

This directory contains the logfiles for the fifth of December of the year 1996.

Logfiles older than five days are automatically removed.

Every logfile has the following form:

PROCESS_PID_TYPE.log that means:

- PPOCESS is the type of connection, for example isdn_ins.
- PID is the unique Unix process ID for the program that serves the connection.
- TYPE is the logging type. This can be: *msg* for error and message logging and *data* for data logging.

The data or message logging is plain English text readable with vi for example.

A.3.3 Frequent errors

Error: no network connection is possible or the connection cannot be set.

Reason: wrong connector of the Ethernet board is selected.

Solution:

- Find out which board is inside:

  type netconfig at Unix-prompt:

  ISA-Card e3E0 Driver

  EISA-/PCI-Card e3G0 Driver

- Configure Port

  Boot the system with a DOS-Disk

  Use the following tools from your Ethernet-disk to configure the

Port correctly (BNC or Twisted Pair):

3C59Xcfg.exe for the 3COM-EISA/PCI-Card

3C5X9cfg.exe for the 3COM-ISA-Card

Error: no display output during the installation of the PRA-Software, hard disk is active but the installation does not continue.

Reason: wrong access to pra.tar.Z or the installation directory

Solution: the system administrator must change the permissions. (compare chapter UNIX)

Error: incoming calls are rejected, the error file contains the following entry: Error at gethostbyname()

Reason: ITK NetBlazer 8500 cannot assign an IP address to the hostname

Solution: */etc/hosts* must contain the entry: *hostname.domainname* (for example: *192.168.12.94 ITKNetBlazer8500.default.de*) and

if a Domain-Name-Server is added in */etc/resolv.conf*, the DNS must be able to resolve hostname.domainname and

check the permission of user pra concerning *resolv.conf* (*r* for group and others)

Other useful system commands / options are in Chapter 2.4, *Some useful commands* (page 2-12).

A.4 RADIUS authentication file "users"

(user database)

- Example of an Authentication-conf. in the file *users.sample*
- Example of an ADNS-configuration in the file *adns.sample*

A.4.1 Example of an authentication configuration

```
# RADIUS-authentication-file 'users'
#


#    Caller-ID and Direct-Dial-No known => Start Shell:
#    (Packet-filter '0' is used, when SLIP, CSLIP or PPP
#     is manually selected)
#%012345_67 User-Password = "USER_DIAL"
#            Service-Type = NAS-Prompt,
#            Filter-Id = "0"

#    Only Caller-ID known => Start PPP:
#%0123456_ User-Password = "ISDN_ADDRESS"
#            Service-Type = Framed,
#            Framed-Protocol = PPP,
#            Filter-Id = "0"

#    Only Caller-ID known => Start PPP or MP:
#    allow only 3 simultaneous connections,
#%0123456_ User-Password = "ISDN_ADDRESS"
#            Service-Type = Framed,
#            Framed-Protocol = MP,
#            Port-Limit = 3,
#            Filter-Id = "0"

#    Only Caller-ID known => Start PPP with static IP-Address,
#    allow only 1 simultaneous connection,
#    privileged user (if ISDN-Call):
#%2345678_ User-Password = "ISDN_ADDRESS"
#            Service-Type = Framed,
#            Framed-Protocol = PPP,
#       Framed-IP-Address = 192.168.20.13,
#            Filter-Id = "0",
#            Port-Limit = 1,
#       ITK-Channel-Binding = Reserved

#     IP-packet received => Callout to 2345678
#     (this entry belongs to the user above
#     or e.g. guest7)
#%192.168.20.13 User-Password = "IP_ADDRESS"
#       Callback-Number = "2345678",
#       ITK-Dialout-Type = ITK-Callout

#    Only Caller-ID known => Start PPP:
#    Callback-user (callback-number equals 01234567),
#    use HDLC as the ISDN protocol (synchronous PPP)
```

```
#%01234567_  User-Password = "ISDN_ADDRESS"
#            Service-Type = Callback-Framed,
#            Framed-Protocol = PPP,
#            ITK-ISDN-Prot = ITK-HDLC,
#            Filter-Id = "0"

#    Only Caller-ID known => Start PPP with static IP-Address:
#    Recall-user (callout-number equals 2345678),
#    use HDLC as the ISDN protocol (synchronous PPP)
#%2345678_  User-Password = "ISDN_ADDRESS"
#            Service-Type = Framed,
#            Framed-Protocol = PPP,
#            Framed-IP-Address = 192.168.20.13,
#            ITK-Dialout-Type = ITK-Recall,
#            ITK-ISDN-Prot = ITK-HDLC,
#            Filter-Id = "0"

#     IP-packet received => Recall to 2345678
#     (this entry belongs to the user above
#     or e.g. guest7)
#%192.168.20.13 User-Password = "IP_ADDRESS"
#            Callback-Number = "2345678",
#            ITK-ISDN-Prot = ITK-HDLC,
#            ITK-Dialout-Type = ITK-Recall

#    Direct-Dial-No '-10' => Start Shell with Login:
#    (Packet-filter '0' is used as default, when SLIP,
#     CSLIP or PPP is manually selected)
%_10         User-Password = "DIRECT_DIAL"
             Service-Type = NAS-Prompt,
             Filter-Id = "0"

#    Direct-Dial-No '-20' => Start Shell with Login and use
#    special Shell-Strings:
#    (Packet-filter '0' is used as default, when SLIP,
#     CSLIP or PPP is manually selected)
#%_20        User-Password = "DIRECT_DIAL"
#            Service-Type = NAS-Prompt,
#            Filter-Id = "0",
#            ITK-Banner = "XYZ Internet Services",
#            ITK-Username-Prompt = "Username:",
#            ITK-Password-Prompt = "Password:",
#            ITK-Welcome-Message = "Access OK",
#            ITK-Prompt = "XYZ>"

#    Direct-Dial-No '-50' => Start Special-TCP-Clear-Connection:
#%_50        User-Password = "DIRECT_DIAL"
#            Service-Type = Login,
#            Login-Service = TCP-Clear,
#            Login-IP-Host = 123.45.67.89,
#            Login-TCP-Port = 13

#    Normal User-1 with default packet-filtering:
#    (PPP with PAP -> PPP)
#    (Login        -> Shell)
guest1  User-Password = "guest1"

#    Normal User-2 with special packet-filtering:
#    (PPP with PAP -> PPP)
```

```
#    (Login        -> Shell)
guest2 User-Password = "guest2"
            Filter-Id = "6"

#    SLIP-User-3 with special packet-filtering (used after Login):
guest3 User-Password = "guest3"
        Service-Type = Framed,
        Framed-Protocol = SLIP,
        Filter-Id = "1"

#    CSLIP-User-4 with special packet-filtering (used after Login):
guest4 User-Password = "guest4"
        Service-Type = Framed,
        Framed-Protocol = SLIP,
        Filter-Id = "1",
        Framed-Compression = Van-Jacobson-TCP-IP

#       Callout user with dynamic IP-address -> if an IP-packet
#       with the last assigned dynamic user-IP-address of guest5
#       is received, the NetBlazer 8xxx dials to user guest5
#       (ISDN-dialnumber saved at dialin)
guest5 User-Password = "guest5"
        ITK-Dialout-Type = ITK-Callout

#       Recall user with dynamic IP-address -> if an IP-packet
#       with the last assigned dynamic user-IP-address of guest6
#       is received, the NetBlazer 8xxx dials to user guest6
#       (ISDN-dialnumber saved at dialin)
guest6 User-Password = "guest6"
        ITK-Dialout-Type = ITK-Recall

#       User with static IP-address
guest7 User-Password = "guest7"
            Framed-IP-Address = 192.168.20.13

########## L2F tunneling ##########

# Enable L2F tunneling in Offline-Authent. (DDI):
#%_60 User-Password = "DIRECT_DIAL"
#        Service-Type = Framed,
#        Framed-Protocol = PPP,
#        ITK-Tunnel-Prot = L2F,
#        ITK-Tunnel-IP = 123.45.67.89,
#        ITK-NAS-Name = Suprimo

# Enable L2F tunneling in Online-Auth.:
#guest8 User-Password = "guest8"
#        ITK-Tunnel-Prot = L2F,
#        ITK-Tunnel-IP = 123.45.67.89,
#        ITK-NAS-Name = Suprimo

########## end L2F tunneling ##########


######### Lan to Lan connection #######

## clientside

#%UIPDEVICE_IP_SERVER Password = "IP_ADDRESS"
```

```
#        Callback-Number = "Dialnumber_server",
#             ITK-ISDN-Prot = ITK-HDLC,
#             ITK-Dialout-Type = ITK-Callout

#%Dialnumber_server_ Password = "ISDN_ADDRESS"
#             Service-Type = Framed-User,
#             Framed-Protocol = PPP,
#             Filter-Id = "xx",
#             Framed-IP-Address = UIPDEVICE_IP_SERVER

## serverside in other users

#%Dialnumber_client_ Password = "ISDN_ADDRESS"
#             Service-Type = Framed-User,
#             Framed-Protocol = PPP,
#             Filter-Id = "xx",
#             Framed-IP-Address = UIPDEVICE_IP_CLIENT

########## End of Lan to Lan connection ##

########## Extended Short Hold ##########

# Enable Extended Short Hold in Offline-Authent. (DDI):
#%_70 User-Password = "DIRECT_DIAL"
#        Service-Type = Framed,
#        Framed-Protocol = PPP,
#        ITK-Tunnel-Prot = ITK-EMAS,
#        ITK-Tunnel-IP = 123.45.67.89

# Enable Extended Short Hold in Online-Auth.:
#guest9 User-Password = "guest9"
#        ITK-Tunnel-Prot = ITK-EMAS,
#        ITK-Tunnel-IP = 123.45.67.89

########## end Extended Short Hold ##########


########## Voice over IP ####################

#    Direct-Dial-No '-40' => Start compressed Voice over IP:
#    select german IVR
#%_40    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="IVR",
#        ITK-Prompt="d"

#    Direct-Dial-No '-41' => Start compressed Voice over IP:
#    select english IVR with a special welcome message
#%_41    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="IVR",
#        ITK-Prompt="e",
#        ITK-Welcome-Message="welcome_special"

#    Direct-Dial-No '-42' => Start compressed Voice over IP:
#    select english guided voice file recording,
#    limit the recording to 30 seconds
#%_42    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
```

```
#        ITK-Banner="RECORD",
#        ITK-Welcome-Message="record_prompt_e",
#        Session-Timeout=30,
#        ITK-Prompt="record"

#    Direct-Dial-No '-43' => Start compressed Voice over IP:
#    select english IVR with overlapped sending
#%_43    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="IVR_DYNDIAL",
#        ITK-Prompt="e"

#    Direct-Dial-No '-44' => Start compressed Voice over IP:
#    select One Stage Dialing (transparent call setup)
#%_44    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="OSD"

#    Direct-Dial-No '-45' => Start compressed Voice over IP:
#    select One Stage Dialing (transparent call setup) with
#    overlapped sending
#%_45    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="OSD_DYNDIAL"

#    Direct-Dial-No '-46' => Start compressed Voice over IP:
#    enable automatic call setup to destination number "12345",
#    assign the username "Directcall" to this connection
#%_46    User-Password = "DIRECT_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="IVR",
#        ITK-Dest-No="12345",
#        ITK-Username="Directcall",
#        ITK-Prompt="d"

#    Caller-ID and Direct-Dial-No known => Start compressed Voice over IP:
#    select a german IVR and assign the username "W.Smith"
#    (no further authentication is needed)
#%0231555566_10User-Password = "USER_DIAL"
#        Service-Type = ITK-Voice-over-IP-Comp,
#        ITK-Banner="IVR",
#        ITK-Prompt="d",
#        ITK-Username="W.Smith"

#    IVR authentication of account code "18112001"
#    (length of account code: 8, length of PIN: 4)
#1811        User-Password = "2001"
#       ITK-Username="W.Smith"

#    IVR authentication of account code "123"
#    (the password "VOICE-ACCOUNT" is used, if the entered account
#    code is shorter than the defined PIN-length (e.g. PIN-length: 4))
#123     User-Password="VOICE-ACCOUNT"
#        ITK-Username="W.Smith"

#    LCR-Request for dialed number "12345":
#    use 192.168.14.12 as dialout-gateway,
#    replace "12345" by "9876"
#%12345  User-Password="LCR"
```

```
#        ITK-Tunnel-IP = 192.168.14.12,
#        ITK-Dest-No = "9874"

#    LCR-Request for dialed number "23456":
#    use 192.168.14.12 as primary and 192.168.14.15
#    as secondary dialout-gateway
#%23456  User-Password="LCR"
#        ITK-Tunnel-IP = 192.168.14.12,
#        ITK-Tunnel-IP = 192.168.14.15

#    LCR-Request for any dialed number beginning with "001":
#    use a dialout-gateway in the USA, remove two leading digits
#    ("0018001234" -> "18001234")
#%001*   User-Password="LCR"
#        ITK-Tunnel-IP = itk_usa,
#        ITK-Dest-No = "-2"

#    LCR-Request for any dialed number beginning with "0":
#    use "0" as prefix digit (e.g. gateway is connected to a PBX)
#    ("0231555566" -> "00231555566")
#%0*     User-Password="LCR"
#        ITK-Dest-No = "+0"

########## end Voice over IP #################


#    Direct-Dial-No '-97' (for support from ITK) => Start Shell with Login:
#     (should not be propagated to users, only for ITK)
%_97         User-Password = "DIRECT_DIAL"
             Service-Type = NAS-Prompt

#    Special User for ITK-Support
itkSuprimo  User-Password = "2high4you"
             Filter-Id = "97"

#    Default Connection => PPP with CHAP/PAP and packet-filter '0':
DEFAULT User-Password = "SUPRIMO"
             Service-Type = Framed,
             Framed-Protocol = MP,
             Filter-Id = "0"

# ITK-PPP-Auth-Type: ITK-Auth-Auto | ITK-Auth-CHAP | ITK-Auth-PAP
```

A.4.2 Example of an ADNS configuration

```
# RADIUS-authentication-file 'users'
#
# Example of an ADNS-'users'-file


#    Direct-Dial-No '-10' => Provider 1
%ADNS_10 Password = "DIRECT_DIAL"
             ITK-Auth-Serv-IP = 123.45.67.89,
             ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-11' => Provider 1
%ADNS_11 Password = "DIRECT_DIAL"
```

```
            ITK-Auth-Serv-IP = 123.45.67.89,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-12' => Provider 1
%ADNS_12 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 123.45.67.89,
            ITK-Auth-Serv-Prot = RADIUS



#    Direct-Dial-No '-20' => Provider 2
#    Multiple Authentication-Servers -> Successive usage
#    of these servers in case of breakdown
%ADNS_20 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 100.100.100.100,
            ITK-Auth-Serv-IP = 100.100.100.101,
            ITK-Auth-Serv-IP = 100.100.100.102,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-21' => Provider 2
%ADNS_21 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 100.100.100.100,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-22' => Provider 2
%ADNS_22 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 100.100.100.100,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-23' => Provider 2
%ADNS_23 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 100.100.100.100,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-24' => Provider 2
%ADNS_24 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 100.100.100.100,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-30' => Provider 3
%ADNS_30 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 192.192.192.192,
            ITK-Auth-Serv-Prot = RADIUS

#    Direct-Dial-No '-40' => Provider 4
%ADNS_40 Password = "DIRECT_DIAL"
            ITK-Auth-Serv-IP = 200.200.200.200,
            ITK-Auth-Serv-Prot = RADIUS

#    Default ADNS-Entry => e.g. Carrier
ADNS_DEFAULT Password = "SUPRIMO"
            ITK-Auth-Serv-IP = 134.135.136.137,
            ITK-Auth-Serv-Prot = RADIUS
```

A.5 Supported RADIUS attributes

```
RADIUS Attributes (from Network Working Group RFC 2058,2059) State:14.05.1998

This are all RADIUS -and ITK-Attributes supported by NetBlazer 8XXX

# standard RADIUS-attributes:

1             User-Name
2             User-Password
4             NAS-IP-Address
5             NAS-Port
6             Service-Type
7             Framed-Protocol
8             Framed-IP-Address
11            Filter-Id
13            Framed-Compression
14            Login-IP-Host
15            Login-Service
16            Login-TCP-Port
19            Callback-Number
27            Session-Timeout
28            Idle-Timeout
31            Calling-Station-Id
61            NAS-Port-Type
62            Port-Limit

# Accounting Attributes:

40              Acct-Status-Type
42              Acct-Input-Octets
43              Acct-Output-Octets
44              Acct-Session-Id
45              Acct-Authentic
46              Acct-Session-Time
47              Acct-Input-Packets
48              Acct-Output-Packets
49              Acct-Terminate-Cause
50              Acct-Multi-Session-Id


# ITK Attributes:

100             ITK-Auth-Serv-IP
101             ITK-Auth-Serv-Prot
102             ITK-Provider-Id
103             ITK-Usergroup
104             ITK-Banner
105             ITK-Username-Prompt
106             ITK-Password-Prompt
107             ITK-Welcome-Message
108             ITK-Prompt
109             ITK-IP-Pool
110             ITK-Tunnel-IP
111             ITK-Tunnel-Prot
112             ITK-Acct-Serv-IP
113             ITK-Acct-Serv-Prot
```

```
114             ITK-Filter-Rule
115             ITK-Channel-Binding
116             ITK-Start-Delay
117           ITK-NAS-Name
118           ITK-ISDN-Prot
119           ITK-PPP-Auth-Type
120           ITK-Dialout-Type
121           ITK-Ftp-Auth-IP
122                   ITK-Users-Default-Entry
123           ITK-Users-Default-Pw
124           ITK-Auth-Req-Type
125           ITK-Modem-Pool-Id
126           ITK-Modem-Init-String
127           ITK-PPP-Client-Server-Mode
128             ITK-PPP-Compression-Prot
129             ITK-Username
130           ITK-Dest-No
131           ITK-DDI


Datatype        content
-------------------------------------------------------------------------------
string        0-253 octets

address       32 bit value, most significant octet first.

integer       32 bit value, most significant octet first.

time          32 bit value, most significant octet first -- seconds since
                00:00:00 GMT,January 1, 1970. The standard Attributes do not
                use this data type but it is presented here for possible use
                within Vendor-Specific attributes.



1   User-Name
-----------------

    Description

      This Attribute indicates the name of the user to be authenticated. It
      is only used in Access-Request packets.

    String

      The String field is one or more octets. The NAS may limit the maximum
      length of the User-Name but the ability to handle at least 63 octets
      is recommended.


2   User-Password
--------------------

    Description

      This Attribute indicates the password of the user to be authenticated,
      or the user's input following an Access-Challenge. It is only used in
      Access-Request packets.
```

String

The String field is between 16 and 128 octets long, inclusive.

4 NAS-IP-Address

Description

This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user. It is only used in Access-Request packets. Either NAS-IP-Address or NAS-Identifier SHOULD be present in an Access-Request packet.

Address

The Address field is four octets.

5 NAS-Port

Description

This Attribute indicates the physical port number of the NAS which is authenticating the user. It is only used in Access-Request packets. Note that this is using "port" in its sense of a physical connection on the NAS, not in the sense of a TCP or UDP port number. EitherNAS-Port or NAS-Port-Type (61) or both SHOULD be present in an Access-Request packet, if the NAS differentiates among its ports.

Value

The Value field is four octets. Despite the size of the field, values range from 0 to 65535.

6 Service-Type

Description

This Attribute indicates the type of service the user has requested, or the type of service to be provided. It MAY be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these service types, and MUST treat unknown or unsupported Service-Types as though an Access-Reject had been received instead.

Value

The Value field is four octets.

1	Login
2	Framed
4	Callback-Framed
7	NAS-Prompt
100	ITK-Voice-over-IP
101	ITK-Voice-over-IP-Comp

The service types are defined as follows when used in an Access-Accept. When used in an Access-Request, they should be considered to be a hint to the RADIUS server that the NAS has reason to believe the user would prefer the kind of service indicated, but the server is not required to honor the hint.

Login The user should be connected to a host.

Framed A Framed Protocol should be started for the User, such as PPP or SLIP.

Callback-Framed The user should be disconnected and called back, then a Framed Protocol should be started for the User, such as PPP or SLIP.

NAS-PromptThe user should be provided a command prompt on the NAS from which non-privileged commands can be executed.

ITK-Voice-over-IP Use VoIP without compression

ITK-Voice-over-IP-Comp Use VoIP with compression

7 Framed-Protocol

Description

This Attribute indicates the framing to be used for framed access. It MAY be used in both Access-Request and Access-Accept packets.

Value

The Value field is four octets.

1 PPP
2 SLIP

8 Framed-IP-Address

Description

This Attribute indicates the address to be configured for the user. It MAY be used in access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.

Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (e.g. Negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g. Assigned from a pool of addresses kept by the NAS). Other valid values indicate that the NAS shoulduse that value as the user’s IP address.

11 Filter-Id

Description

This Attribute indicates the name of the filter list for this user. Zero or more Filter-Id attributes MAY be sent in an Access-Accept packet. Identifying a filter list by name allows the filter to be used on different NASes without regard to filter-list implementation details.

String

The String field is one or more octets.

13 Framed-Compression

Description

This Attribute indicates a compression protocol to be used for the link. More than one compression protocol Attribute MAY be sent. It is the responsibility of the NAS to apply the proper compression protocol to appropriate link traffic.

Value

The Value field is four octets.

0	None
1	VJ-TCP-IP header compression

14 Login-IP-Host

Description

This Attribute indicates the system with which to connect the user, when the Login-Service Attribute is included. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint to the server, that the NAS would prefer to use that host, but the server is not required to honor the hint.

Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS SHOULD allow the user to select an address. The value 0 indicates that the NAS SHOULD select a host to connect the user to. Other values indicate the address the NAS SHOULD connect the user to.

15 Login-Service

Description

This Attribute indicates the service which should be used to connect the user to the login host. It is only used in Access-Accept packets.

Value

The Value field is four octets.

0	Telnet	Telnet connection
2	TCP-Clear	Transparent TCP connection
100	ITK-UDP-Clear	Transparent UDP connection

16 Login-TCP-Port

Description

This Attribute indicates the TCP port with which the user is to be connected, when the Login-Service Attribute is also present. It is only used in Access-Accept packets.

Value

The Value field is four octets. Despite the size of the field, values range from 0 to 65535.

19 Callback-Number

Description

This Attribute indicates a dialing string to be used for callback. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint to the server that a Callback service is desired, but the server is not required to honor the hint.

String

The String is one or more octets. The actual format of the information is site or application specific, and a robust implementation should support the field as undistinguished octets. The codification of the range of allowed usage of this field is outside the scope of this specification.

27 Session-Timeout

Description

This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. This Attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge.

Value

The field is 4 octets, containing a 32-bit unsigned integer with the maximum number of seconds this user should be allowed to remain connected by the NAS.

28 Idle-Timeout

Description

This Attribute sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. This Attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge.

Value

The field is 4 octets, containing a 32-bit unsigned integer with the maximum number of consecutive seconds of idle time this user should be permitted before being disconnected by the NAS.

31 Calling-Station-Id

Description

This Attribute allows the NAS to send in the Access-Request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. It is only used in Access-Request packets.

String

The String field is one or more octets, containing the phone number that the user placed the call from.
The actual format of the information is site or application specific.
Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.
The codification of the range of allowed usage of this field is outside the scope of this specification.

61 NAS-Port-Type

Description

This Attribute indicates the type of the physical port of the NAS which is authenticating the user. It can be used instead of or in addition to the NAS-Port (5) attribute. It is only used in Access-Request packets. Either NAS-Port (5) or NAS-Port-Type or both SHOULD be present in an Access-Request packet, if the NAS differentiates among its ports.

Value

The Value field is four octets.

0	Async
1	Sync
2	ISDN-Sync
3	ISDN-Async-V.120

```
       4       ISDN-Async-V.110


62  Port-Limit
------------------

    Description

      This Attribute sets the maximum number of ports to be provided to the
      user by the NAS. This Attribute MAY be sent by the server to the client
      in an Access-Accept packet. It is intended for use in conjunction with
      Multilink PPP or similar uses. It MAY also be sent by the NAS to the
      server as a hint that that many ports are desired for use, but the
      server is not required to honor the hint.

    Value

      The field is 4 octets, containing a 32-bit unsigned integer with the
      maximum number of ports this user should be allowed to connect to on the
      NAS.


100 ITK-Auth-Serv-IP
------------------------

    Description

      This Attribute indicates the system which host should be used to
      authenticate the user. It MUST be used in Access-Accept packets from
      ADNS.

    Address

      The Address field is four octets and indicates the IP address of the
      authentication server.


101 ITK-Auth-Serv-Prot
--------------------------

    Description

      This Attribute indicates the authentication protocol. It MUST be used
      in Access-Accept packets from ADNS.

    Value

      The Value field is four octets.

       0      None
       1      PSP
       2      RADIUS


102 ITK-Provider-Id
----------------------

    Description
```

This Attribute indicates the identifier of the provider, the user belongs to. This identifier can be used for provider specific operations. It MAY be used in Access-Accept packets from ADNS.

Value

The Value field is an integer of four octets.

103 ITK-Usergroup

Description

This Attribute indicates an identifier of a usergroup the user belongs to. The identifier will be used in conjunction with the ITK-Provider-Id for user specific operations. It MAY be used in Access-Accept packets from ADNS.

Value

The Value field is an integer of four octets.

104 ITK-Banner

Description

This Attribute indicates the first text which is displayed to the user when a NetBlazer 8xxx-Login is selected. It is only used in Access-Accept packets.

VoIP extension:

String: VGI: The Interactive Voice Response (IVR) (or Voice Guided Input VGI) is used to provided the caller with a 2-stage-dialing method to establish a telephone connection to the callee.

String: RECORD: Allow recording of new voice files

String

The String field is one or more octets, and its contents are intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

105 ITK-Username-Prompt

Description

This Attribute indicates the Username-Prompt which is displayed to the user when a NetBlazer 8xxx-Login is selected. It is only used in Access-Accept packets.

VoIP extension:

Specifies the name of the voice file for ’prompt for account code’

String

The String field is one or more octets, and its contents are intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

106 ITK-Password-Prompt

Description

This Attribute indicates the Password-Prompt which is displayed to the user when a NetBlazer 8xxx-Login is selected. It is only used in Access-Accept packets.

VoIP extension:

Specifies the name of the voice file for ’prompt for destination number’

String

The String field is one or more octets, and its contents are intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

107 ITK-Welcome-Message

Description

This Attribute indicates the Welcome message which is displayed to the user after a successful login when the NetBlazer 8xxx-Shell is selected. It is only used in Access-Accept packets.

VoIP extension:

ITK-Banner: ’VGI’: Specifies the name of the voice file for ’welcome message’

ITK-Banner: ’RECORD’: Specifies the name of the voice file for "prompt for voice recording"

String

The String field is one or more octets, and its contents are intended to be human readable and MUST NOT affect operation of the protocol. It is

recommended that the message contain displayable ASCII characters from the range 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

108 ITK-Prompt

Description

This Attribute indicates the Command Prompt which is displayed to the user when the NetBlazer 8xxx-Shell is selected. It is only used in Access-Accept packets.

VoIP extension:

ITK-Banner: 'VGI': The value is used to locate the voice files. The NetBlazer already contains voice files in german and english, that can be selected with the values "e" (for english) and "d" (for german).

ITK-Banner: 'RECORD': Specifies the name of the voice file for the recording (output)

String

The String field is one or more octets, and its contents are intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

109 ITK-IP-Pool

Description

This Attribute indicates an identifier of an IP-Pool from which an IP-address will be assigned for the user. This Pools have to be configured locally on the NetBlazer 8xxx. The Attribute MAY be used in Access-Accept packets.

Value

The Value field is an integer of four octets.

110 ITK-Tunnel-IP

Description

This Attribute indicates the system to which the user IP-packets must be forwarded via an IP-tunnel. It MAY be used in Access-Accept packets.

VoIP extension:

Specify the address of the dialout-gateway to use

Address

The Address field is four octets and indicates the IP address of the tunneling endpoint.

111 ITK-Tunnel-Prot

Description

This Attribute indicates the tunneling protocol. It MAY be used in Access-Accept packets.

Value

The Value field is four octets.

1	L2FLayer 2 Forwarding	
2	FR-DLCIFrame Relay DLCI	
3	ITK-EMAS	Extended Multiple Access System

112 ITK-Acct-Serv-IP

Description

This Attribute indicates the system to which the accounting data is to be send. It MAY be used in Access-Accept packets.

Address

The Address field is four octets and indicates the IP address of the accounting server.

113 ITK-Acct-Serv-Prot

Description

This Attribute indicates the accounting protocol. It MAY be used in Access-Accept packets.

Value

The Value field is four octets.

0	None
1	RADIUS

114 ITK-Filter-Rule

Description

This Attribute indicates one entry of the filter list for this user. Zero or more ITK-Filter-Rule attributes MAY be sent in an Access-Accept packet.

Identifying a filter list by a sample of rules allows the filter to be used on different NASes without local databases.

String

The String field is one or more octets.

115 ITK-Channel-Binding

Description

This Attribute indicates whether one of the reserved channels can be assigned to the user. Otherwise the user will be rejected, if the number of unpriviledged channels exceeds the limit. The Attribute MAY be used in Access-Accept packets.

Value

The Value field is four octets.

0	NormalNormal User
1	ReservedPriviledged User

116 ITK-Start-Delay

Description

This Attribute indicates the delay before beginning of sending/receiving data in sec.

Value

The Value field is an integer of four octets.

117 ITK-NAS-Name

Description

This Attribute contains a string identifying the NAS. It is used for example to identify the NAS on the remote end in a tunneling protocol like L2F.

String

The String field is one or more octets.

118 ITK-ISDN-Prot

Description

This Attribute indicates the B-Channel protocol. It should be used for outgoing calls.

Value

The Value field is an integer of four octets.

0	ITK-Auto-Detection
1	ITK-HDLC
2	ITK-X.75
3	ITK-X.25
4	ITK-V.110
5	ITK-V.120
6	ITK-Modem-Async
7	ITK-Modem-Sync

ITK-Auto-Detection:Automatic detection of the ISDN protocols. At incoming calls the protocol will be recognized by the ISDN signaling. Moreover an detection of the possibly equal signaled protocols HDLC, X.75 and V.110 is tried.

ITK-HDLC:Used for PPP over ISDN (synchronous PPP) as specified in RFC 1618.

ITK-X.75:Solely use of the X.75 protocol. (e.g. for asynchronous PPP)

ITK-X.25:The X.25 protocol.

ITK-V.110:Solely use of the V.110 protocol. (e.g. for asynchronous PPP)

ITK-Modem-Async: Used for asynchronous Modem connections.

119 ITK-PPP-Auth-Type

Description

This Attribute indicates the type of authentication via PPP.

Value

The Value field is an integer of four octets.

1	ITK-Auth-Auto (At first we try CHAP and then PAP)
2	ITK-Auth-CHAP (We only try CHAP)
3	ITK-Auth-PAP (We only try PAP)
4	ITK-Auth-NONE

120 ITK-Dialout-Type

Description

This Attribute indicates the type of Dialout.

Value

The Value field is an integer of four octets.

1 ITK-Callback
2 ITK-Callout
3 ITK-Recall

ITK-Callback:An incoming call will be rejected and the
user is called back.

ITK-Callout: The NetBlazer 8xxx dials to an user to establish
an outbound connection.

ITK-Recall: The NetBlazer 8xxx dials to an user just to 'awake'
his client software. The user must reject
the call and should call back.
No outbound connection is established.

121 ITK-Ftp-Auth-IP

Description

This Attribute indicates the system the ipaddress or the name to FTP-authentication-server.
Any FTP-server that conforms to RFC959 can be used as an authentication-server.

Address

The Address field is four octets.

122 ITK-Users-Default-Entry

Description

This Attributes indicates a possibility to chance the default entry username in
RADIUS file users. Default username is DEFAULT.

String

The String field is one or more octets.

123 ITK-Users-Default-Pw

Description

This Attributes indicates a possibility to chance the default entry password in
RADIUS file users. Default password is SUPRIMO.

String

The String field is one or more octets.

124 ITK-Auth-Req-Type

Description

This Attributes indicates a possibility to set the order of authentication request
in offline phase. For example we want at first a authentication request with
combination of caller-id (CID) and direct-dialin (DDI) and second an access request
with default-entry. So we must set this attribute "AZ".

String

The String field is one or more octets.

125 ITK-Modem-Pool-Id

Description

This Attributes indicates a possibility to select a modem pool.

Value

The Value field is an integer of four octets.

126 ITK-Modem-Init-String

Description

This Attributes indicates a possibility to send a initstring to a modemcard.

String

The String field is one or more octets.

127 ITK-PPP-Client-Server-Mode

Description

This Attributes indicates a possibility to chance the reaction against an other system.

Value

The Value field is an integer of four octets.

```
      0      ITK-Mode-Server   (default)
      1      ITK-Mode-Client   (without PAP/CHAP)


128 ITK-PPP-Compression-Prot
----------------------------

   Description

     With this Attribute it is possible to set the PPP compression protocol.
     More than one compression protocol can be set with a separator ':'. For exam-
ple
     you want to set two PPP compression protocol. The entry in file users is
     ITK-PPP-Compression-Prot = "COMP1:COMP2". The default entry is no compression
protocol.


   String

     The String field is one or more octets. In the current state Predictor type 1
(PRED1)
     and Stac LZS (STAC) are supported.


129 ITK-Username
----------------

   Description

     This Attributes indicates a possibility to assign a username to a dialnumber.

     VoIP extension:

     Specify the alphanumeric username to appear in pramon/webMan and accounting

   String

     The String field is one or more octets.


130 ITK-Dest-No
---------------

    Description

     This Attributes indicates the phone number that the user called.

     VoIP extension:

     Force an automatic connection setup to the specified destination number

   String

     The String field is one or more octets.


131 ITK-DDI
-----------
```

Description

This Attributes indicates the Direct Dialling In (DDI) that the caller dialed. This Attribute is only used in Access Accept packet.

String

The String field is one or more octets.

40 Acct-Status-Type

Description

This attribute indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
It MAY be used by the client to mark the start of accounting (for example, upon booting) by specifying Accounting-On and to mark the end of accounting (for example, just before a scheduled reboot) by specifying Accounting-Off.

Value

The Value field is four octets.

1	Start
2	Stop
7	Accounting-On
8	Accounting-Off

42 Acct-Input-Octets

Description

This attribute indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Value

The Value field is four octets.

43 Acct-Output-Octets

Description

This attribute indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Value

The Value field is four octets.

44 Acct-Session-Id

Description

This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Acct-Session-Id. It is strongly recommended that the Acct-Session-Id be a printable ASCII string.

For example, one implementation uses a string with an 8-digit upper case hexadecimal number, the first two digits increment on each reboot (wrapping every256 reboots) and the next 6 digits counting from 0 for the first person logging in after a reboot up to 2^24-1, about 16 million. Other encodings are possible.

String

The String field SHOULD be a string of printable ASCII characters.

45 Acct-Authentic

Description

This attribute MAY be included in an Accounting-Request to indicate how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol. Users who are delivered service without being authenticated SHOULD NOT generate Accounting records.

Value

The Value field is four octets.

1 RADIUS

46 Acct-Session-Time

Description

This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Value

The Value field is four octets.

47 Acct-Input-Packets

Description

This attribute indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Value

The Value field is four octets.

48 Acct-Output-Packets

Description

This attribute indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Value

The Value field is four octets.

49 Acct-Terminate-Cause

Description

This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Value

The Value field is four octets, containing an integer specifying the cause of session termination, as follows:

1 User-Request
2 Lost-Carrier
3 Lost-Service
4 Idle-Timeout
5 Session-Timeout
6 Admin-Reset
7 Admin-Reboot
8 Port-Error
9 NAS-Error
10 NAS-Request
11 NAS-Reboot
12 Port-Unneeded
13 Port-Preempted
14 Port-Suspended
15 Service-Unavailable
16 Callback
17 User-Error
18 Host-Request

The termination causes are as follows:

User-Request:	User requested termination of service, for example with LCP Terminate or by logging out.
Lost-Carrier:	DCD was dropped on the port.
Lost-Service:	Service can no longer be provided; for example, user's connection to a host was interrupted.
Idle-Timeout:	Idle timer expired.
Session-Timeout:	Maximum session length timer expired.
Admin-Reset:	Administrator reset the port or session.
Admin-Reboot:	Administrator is ending service on the NAS, for example prior to rebooting the NAS.
Port-Error:	NAS detected an error on the port which required ending the session.
NAS-Error:	NAS detected some error (other than on the port) which equired ending the session.
NAS-Request:	NAS ended session for a non-error reason not otherwise listed here.
NAS-Reboot:	The NAS ended the session in order to reboot non administratively ("crash").
Port-Unneeded:	NAS ended session because resource usage fell below low-water mark (for example, if a band-width-on-demand algorithm decided that the port was no longer needed).
Port-Preempted:	NAS ended session in order to allocate the port to a higher priority use.
Port-Suspended:	NAS ended session to suspend a virtual session.
Service-Unavailable:	NAS was unable to provide requested service.
Callback:	NAS is terminating current session in order to perform callback for a new session.
User-Error:	Input from user is in error, causing termination of session.
Host-Request:	Login Host terminated session normally.

A.6 All parameters from common.par

```
#=============================================================================
# ITK AG                       III   TTTTT   K  K        All rights reserved
#                               I      T     K K
# Joseph-v.-Fraunhofer-Str. 23 I      T     KK
# D - 44227 Dortmund           I      T     K K
# Phone. (0231) 9747-0        III     T     K  K
#=============================================================================
#
# Description:      Global Parameterfile
#
# Product/Project:  NetBlazer 8xxx
#
# Filename:         common.par
#                   (should not be changed by customer)
#                    ================================
#
# Subject:          Definition of global (default) Parameters
#
#                   Macro-Substitution:
#                   Parametervalues can contain Macros, which are inserted
#                   with $(macroname). The value for the macro will be
#                   determined in the following order:
#                     1. Check if macroname is internal name:
#                           PID:       macrovalue is process-ID
#                           PROGRAM:   macrovalue is programname
#                           DATE:      macrovalue is date (JJJJMMDD)
#                           TIME:      macrovalue is time (hhmmss)
#                     2. Check if macroname is environment-variable:
#                           => macrovalue is value of environment-variable
#                     3. Determine macroname from parametrisation
#                           => macrovalue is parametervalue
#                   The macro-substitution is recursiv.
#
#
# Version:          @(#) $Revision: 1.150 $ $Date: 1998/07/10 15:12:20 $
#=============================================================================
# Update-History:
#  Date      User  Description of Change
# ----------------------------------------------------------------------------
# 10.10.1996  TH   Creation
# 11.10.1996  KP   No Msg-Logging in Master-processes
# 21.11.1996  KP   New parameter: subnetting
# 27.11.1996  TH   New process:   l2fd
#                  New parameter: practrl.start_l2fd
# 12.12.1996  KP   New parameter: capi_callback_delay
# 12.12.1996  Fi   New parameter: l2fd.ign_mid_seq
# 16.12.1996  TH   New parameters: practrl.ctrl_temperature_log &
#                                  practrl.info_syslog_target
# 17.12.1996  steins New parameter: pramon.refresh_default
# 06.01.1996  TH   New parameter: practrl.restart
# 09.01.1997  KP   New parameter: linecnt_isdn_ll
# 10.01.1997  mb   New parameter: practrl.command_events_cnt
# 24.01.1997  mb   New Parameter: practrl.cmd_start_practrl
# 29.01.1997  mb   New Parameters: .isdn_local_id_%d
# 11.02.1997  TH   New parameter: linecnt_emas
# 14.02.1997  KP   New process:   isdn_ll
```

```
# 19.02.1997  KP   Setting infomasks of Slave-processes
# 07.03.1997  MB   New parameters: ignore_packet_time and callout_tmo
# 07.03.1997  Fi   New parameter: l2fd.timer_len
# 11.03.1997  Fi   New parameters: l2fd.max_tunnels, l2fd.max_callers
# 24.03.1997  mb   New parameters: partner_cnt and partner_%d
# 25.03.1997  Fi   New parameter: .log_data_level
#                  New process: snsp_server
# 02.04.1997  Fi   New process: emas
# 18.04.1997  mb   New Parameter: dialout
# 28.04.1997  TH   New Parameters: ftp_accept_count, ftp_timeout, ftp_auth_addr,
#                                  check_auth_errors, trap_auth_errors
# 29.04.1997  KP   New process:   pstn_out
# 07.05.1997  KP   New parameter: .dist_homing
# 16.05.1997  fl   New parameter: .ppp_dns1, .ppp_dns2
# 23.05.1997  mb   New parameter: snsp_server.snsp_max_timeout
# 04.06.1997  Fi   New parameter: emas.mpra_frag_timeout
# 05.06.1997  Fi   New parameter: emas.mpra_max_frags
# 09.06.1997  thg  New parameter: .isdn_local_id_4
# 11.06.1997  KP   New parameters: modemtest_initstring, modemtest_dlpdblocklen
# 19.06.1997  Fi   New process: pra_shutdown
#   09.07.1997     mb        New   parameter:   practrl.cmd_start_check_net,   prac-
trl.time_check_net
#                                ,practrl.lan_test_ip,practrl.wan_test_ip
# 18.07.1997  fl   New parameter: PPP_Client_Server_Mode
# 28.07.1997  mb   New parameter: itk_radius_offset
# 14.08.1997  mb   New parameter: cpuload_check_1,cpuload_check_2,cpuload_check_3
# 28.08.1997  mb   New parameter: akt_pjdat (directory for actual parameters)
# 02.09.1997  fl   New parameter: users_default_entry and users_default_pw
# 02.09.1997  thg  New parameters for www_suprimon (logging)
# 25.09.1997  fl   New parameter: ppp_compression (PRED1)
# 26.09.1997  mb   New parameter: parameter_actual_flag
# 29.09.1997  fl   New parameter: radius_access_port and radius_accounting_port
# 07.10.1997  TH   New parameter: set_uip_routes
# 20.10.1997  fl   New parameter: uip_address_strategy
# 04.11.1997  mb   New Parameter: debuglog%d.card
# 11.11.1997  fl   New parameter: ppp_compression (STAC)
# 13.11.1997  mb   Added default entries for: .APPL_SERVER and .RADIUS_SERVER
# 17.11.1997  mb   New parameter: time_d_channel
#                  add name of parameterfile to all parameters that can be changed
#                  removed debuglog%d.card,akt_pjdat
# 20.11.1997  mb   New parameter: practrl.restart_type
# 19.12.1997  mb   New parameter: dcm.log_data_file,dcm.log_data_format,
#                  dcm.log_msg_format
# 30.12.1997  KP   New parameter: .capi_datablklen_b2_voip
# 20.01.1998  TH   Parameters for VoIP
# 20.01.1998  fl   New parameter: .radius_resend_count
# 27.01.1998  fl   New parameter: .voip_pkt_analyze_flag
#                                 .voip_pkt_src_delay
#                                 .voip_pkt_variation
# 29.01.1998  fl   New parameter: .voip_echo_resp_tmo
#                                 .voip_wait_for_any_con_msg
# 04.02.1998  KP   New parameter: .capi_eaz
# 05.02.1998  mb   New parameter: practrl.max_test_failure
# 10.02.1998  mb   New parameter: .netblazer_name
# 12.02.1998  mb   New parameter: practrl.cmd_viperload
# 24.02.1998  KP   New parameter: .ccard_cnt (and also .ccard_xx)
# 09.03.1998  fl   New parameter: .pcm_companding
#                                 .echo_canceller_flag
#                                 .jitter_hdr_seq_flag
```

```
# 23.03.1998  fl   New parameter: .voip_dialout_count
# 02.04.1998  fl   New parameter: .stab_lcr_cnt
#                                 .stab_lcr_addr_1 (see voip.par)
#             mb   New parameter: snsp_server.voicedialout_source_cnt
#                                 snsp_server.voicedialout_source_ (list)
# 03.04.1998  mb   New macro: HOST_ADDRESS
#                  new values for snsp_server.voicedialout_source_cnt and
#                                 snsp_server.voicedialout_source_
# 08.04.1998  KP   'localhost' is default for lcr_addr and auth_addr
# 05.06.1998  mb   New parameter: .top_linecnt_pspdn, .top_linecnt_pspdn_ph ,
#                                 .top_stab_adns_cnt, .top_stab_auth_cnt ,
#                                 .top_stab_lcr_cnt, .top_stab_acct_cnt,
#                                 .top_number_uip, .top_stab_isdn_cnt ,
#                                 .top_stab_pstn_cnt and .top_stab_pspdn_cnt
# 15.06.1998  mb   New Parameter: .start_iss
# 18.06.1998  KP   New Parameter: .voip_ip_tos
# 26.06.1998  KP   New parameter: .set_static_routes
# 01.07.1998  fl   Rename: stab_auth_cnt -> stab_offline_cnt
#                         stab_auth_addr_x -> stab_offline_addr_x
#                         top_stab_auth_cnt -> top_stab_offline_cnt
#                  New parameter: .stab_online_cnt
#                                 .stab_online_addr_x
#                                 .top_stab_online_cnt
#             mb   New Parameter: .start_llp
# 07.07.1998  fl   New macros: RADIUS_ACCESS_PORT, RADIUS_SECRET
#                  New parameter: .radius_adns_keyword, .radius_offline_keyword
#                                 .radius_online_keyword, .radius_lcr_keyword
#                                 .radius_adns_port, .radius_offline_port
#                                 .radius_online_port, .radius_lcr_port
# 08.07.1998  KP   New: CAPI20 parameters
#   20.07.1998      mb         Renamed   parameter:   practrl.cmd_viperload=>prac-
trl.cmd_viper542load
#                  New parameter: practrl.cmd_viper548load,
#                                 practrl.cmd_viper549load
# 20.07.1998  fl   Delete parameter: .radius_keyword
#                  New parameter: .radius_account_keyword
# 23.07.1998  steins New parameter:www_suprimon.www_refresh
# 28.07.1998  TH   Set bit 0x20000000 in capi20_infomasks (forward facility-msg)
# 29.07.1998  steins New parameter:www_suprimon.www_reflines
# 13.08.1998  steins New parameter for license-keys
# 20.08.1998  KP   Changed values for capi20_infomasks
# 31.08.1998  steins New parameter: .LICENSE_KEY_ISS
# 01.09.1998  KP   New parameter: .fw_unknown_prot
# 04.09.1998  mb   cmd_viperXXXload needs now 2 parameters ( Card + Dsp )
# 09.09.1998  fl   New parameter: .voip_autocon_discon
# 14.09.1998  mb   Added all parameters of h323.par.sample :
#                    h323d.log_component_mask,h323d.use_early_h245_tsap,
#                    h323d.use_gatekeeper,h323d.ip_addr_gatekeeper,
#                    h323d.PBXExternCallPrefix,h323d.AudioOnlyCallInternPrefix,
#                    h323d.AudioOnlyCallExternPrefix
# 14.09.1998  ES   added bits in infomask to enable CALL PROCEEDING
# 21.09.1998  fl   Rename voip_echo_resp_tmo to voip_idle_tmo
# 30.09.1998  fl   New default value for voip_idle_tmo: 5 Minutes
# 30.09.1998  KP   Added default values for leased line session/idle-timeouts
# 15.10.1998  KP   New parameter: .voip_empty_setup
# 16.10.1998  mb   New parameter: h323d.wait_for_remote_connect
# 02.11.1998  UF   New parameter: h323d.Q931CallingPartyNoOctet3a
#
#==============================================================================
```

```
#
################################################################################
# Macros
################################################################################
.PJSRC:                         /u/pra/src/
.PJDAT:                         /u/pra/dat/
.PJBIN:                         /u/pra/bin/
.PJLOG:                /u/pra/log/$(DATE)/
.PJEXE:                /u/pra/exe/
.PJSPC:                 /u/pra/spc/
.PJVOI:                 /u/pra/voi/
.ERROR_LOGFILE:        $(PJLOG)$(PROGRAM)_$(PID)_msg.log
.MSG_LOGFILE:          $(PJLOG)$(PROGRAM)_$(PID)_msg.log
.FSTART_LOGFILE:$(PJLOG)$(PROGRAM)_$(PID)_msg.log
.FENDE_LOGFILE:        $(PJLOG)$(PROGRAM)_$(PID)_msg.log
.DATA_LOGFILE:         $(PJLOG)$(PROGRAM)_$(PID)_data.log
.APPL_SERVER:
.RADIUS_SERVER:         localhost
.RADIUS_ACCESS_PORT:    1645   # port:1645 (RFC2058) port:1812 (RFC2138)
.RADIUS_SECRET:         test   # Shared RADIUS-Secret
.LICENSE_KEY_VOICE:
.LICENSE_KEY_RAS:
.LICENSE_KEY_FAX:
.LICENSE_KEY_ISS:
#
#
################################################################################
# Parameter for isdn_in (Master-process for accept. incoming ISDN-connections)
################################################################################
isdn_in.capi_b2protocol:         0x02  # CAPI-B2-Protocol
isdn_in.capi_b3protocol:         0x04  # CAPI-B3-Protocol
isdn_in.capi_simask:           0x80a0  # CAPI-Service-Indicator-Mask
isdn_in.capi_infomask:           0x40    # Info-Mask

isdn_in.capi20_b1protocol:       0x00  # CAPI-B1-Protocol HDLC
isdn_in.capi20_b2protocol:       0x01  # CAPI-B2-Protocol transp
isdn_in.capi20_b3protocol:       0x00  # CAPI-B3-Protocol transp
isdn_in.capi20_cipmask:    0x00000104  # CAPI-Compatibility-Information-Profile
isdn_in.capi20_infomask:   0x20010381    # Info-Mask

isdn_in.capi_callback_delay:        0    # Delay before a callback is
                                                 # initiated in msec [dlm.par]
isdn_in.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
#isdn_in.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
isdn_in.log_msg_file:            # No Msg-Logging
#isdn_in.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
isdn_in.log_data_file:           # No Data-Logging
################################################################################
# Parameter for isdn_ins (slave-process for serving an incoming ISDN-connect.)
################################################################################
isdn_ins.capi_infomask:          0x01    # Info-Mask

isdn_ins.capi20_infomask:  0x20010381    # Info-Mask

isdn_ins.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
#isdn_ins.log_msg_file:$(MSG_LOGFILE) # Msg-Logging => Logfile
isdn_ins.log_msg_file:           # No Message-Logging
#isdn_ins.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
isdn_ins.log_data_file:          # No Data-Logging
```

```
#
################################################################################
# Parameter for isdn_out (master-process for accept. outgoing ISDN-connections)
################################################################################
isdn_out.capi_b2protocol:         0x01  # CAPI-B2-Protocol
isdn_out.capi_b3protocol:         0x04  # CAPI-B3-Protocol
isdn_out.capi_outgservice:        0x07  # CAPI-Outgoing service

isdn_out.capi20_b1protocol:       0x00  # CAPI-B1-Protocol HDLC
isdn_out.capi20_b2protocol:       0x00  # CAPI-B2-Protocol X.75
isdn_out.capi20_b3protocol:       0x00  # CAPI-B3-Protocol transp
isdn_out.capi20_cipvalue:         0x02   # unrestricted digital info(64 kbit/s)

isdn_out.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
#isdn_out.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
isdn_out.log_msg_file:          # No Msg-Logging
#isdn_out.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
isdn_out.log_data_file:         # No Data-Logging
################################################################################
# Parameter for isdn_outs (slave-process for serving one outgoing ISDN-conn.)
################################################################################
isdn_outs.capi_infomask:         0x01    # Info-Mask

isdn_outs.capi20_infomask: 0x20000341    # Info-Mask

isdn_outs.log_error_file:$(ERROR_LOGFILE)# Error-Logging => Logfile
#isdn_outs.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
isdn_outs.log_msg_file:         # No Message-Logging
#isdn_outs.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
isdn_outs.log_data_file:  # No Data-Logging
#
################################################################################
# Parameter for pstn_in (master-process for accept. incoming Modem-connections)
################################################################################
pstn_in.capi_b2protocol:         0x0e  # CAPI-B2-Protocol B2_MVIP
pstn_in.capi_b3protocol:         0x04  # CAPI-B3-Protocol B3_TRANSPARENT
pstn_in.capi_simask:           0x0006  # CAPI-Service-Indicator-Mask
pstn_in.capi_infomask:           0x40    # Info-Mask

pstn_in.capi20_b1protocol:       0x81  # CAPI-B1-Protocol MVIP
pstn_in.capi20_b2protocol:       0x01  # CAPI-B2-Protocol transp
pstn_in.capi20_b3protocol:       0x00  # CAPI-B3-Protocol transp
pstn_in.capi20_cipmask:    0x04010032    # CAPI-Compatibility-Information-Profile
pstn_in.capi20_infomask:   0x60010381    # Info-Mask

pstn_in.capi_callback_delay:     5000    # Delay before a callback is
                                                 # initiated in msec [dlm.par]
pstn_in.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
#pstn_in.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
pstn_in.log_msg_file:           # No Msg-Logging
#pstn_in.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
pstn_in.log_data_file:          # No Data-Logging
################################################################################
# Parameter for pstn_ins (slave-process for serving one incoming Modem-conn.)
################################################################################
pstn_ins.capi_infomask:          0x01    # Info-Mask

pstn_ins.capi20_infomask:  0x60010381    # Info-Mask
```

```
pstn_ins.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
#pstn_ins.log_msg_file:$(MSG_LOGFILE) # Msg-Logging => Logfile
pstn_ins.log_msg_file:          # No Message-Logging
#pstn_ins.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
pstn_ins.log_data_file:         # No Data-Logging
#
##############################################################################
# Parameter for pstn_out (master-process for accept. outgoing Modem-conn.)
##############################################################################
pstn_out.capi_b2protocol:         0x0e  # CAPI-B2-Protocol
pstn_out.capi_b3protocol:         0x04  # CAPI-B3-Protocol
pstn_out.capi_outgservice:        0x01  # CAPI-Outgoing service
pstn_out.capi_addinfooctett:      0x02  # Additional information octet

pstn_out.capi20_b1protocol:         0x81 # CAPI-B1-Protocol MVIP
pstn_out.capi20_b2protocol:         0x01 # CAPI-B2-Protocol transp
pstn_out.capi20_b3protocol:         0x00 # CAPI-B3-Protocol transp
pstn_out.capi20_cipvalue:           0x04 # 3.1 kHz audio

pstn_out.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
#pstn_out.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
pstn_out.log_msg_file:          # No Msg-Logging
#pstn_out.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
pstn_out.log_data_file:         # No Data-Logging
##############################################################################
# Parameter for pstn_outs (slave-process for serving one outgoing Modem-conn.)
##############################################################################
pstn_outs.capi_infomask:         0x01    # Info-Mask

pstn_outs.capi20_infomask:   0x20000351  # Info-Mask

pstn_outs.log_error_file:$(ERROR_LOGFILE)# Error-Logging => Logfile
#pstn_outs.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
pstn_outs.log_msg_file:         # No Message-Logging
#pstn_outs.log_data_file:$(DATA_LOGFILE) # Data-Logging => Logfile
pstn_outs.log_data_file:  # No Data-Logging
#
##############################################################################
# Parameter for pspdn (process for serving all X.25-connections)
##############################################################################
pspdn.capi_b2protocol:         0x01      # CAPI-B2-Protocol
pspdn.capi_b3protocol:         0x02      # CAPI-B3-Protocol
pspdn.capi_outgservice:        0x08      # CAPI-Outgoing service

pspdn.capi20_b1protocol:         0x00    # CAPI-B1-Protocol HDLC
pspdn.capi20_b2protocol:         0x00    # CAPI-B2-Protocol X.75
pspdn.capi20_b3protocol:         0x02    # CAPI-B3-Protocol ISO8208
pspdn.capi20_cipvalue:           0x07    # packet mode

pspdn.capi_timeout_conf:      30000   # Timeout for Confirm-wait in msec
pspdn.capi_timeout_ind:       60000 # Timeout for Indication-wait in msec
pspdn.log_error_file:$(ERROR_LOGFILE)    # Error-Logging => Logfile
#pspdn.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
pspdn.log_msg_file:             # No Msg-Logging
#pspdn.log_data_file:$(DATA_LOGFILE)  # Data-Logging => Logfile
pspdn.log_data_file:            # No Data-Logging
#
##############################################################################
# Parameter for l2fd (L2F-Daemon for IP-Tunneling)
```

```
#############################################################################
l2fd.log_error_file:$(ERROR_LOGFILE)     # Error-Logging => Logfile
#l2fd.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
l2fd.log_msg_file:               # No Msg-Logging
#l2fd.log_data_file:$(DATA_LOGFILE)  # Data-Logging => Logfile
l2fd.log_data_file:              # No Data-Logging
#
l2fd.ign_mid_seq:         0     # Ignore MID sequencing(no=0/yes=1)[l2f.par]
l2fd.timer_len:        5000     # Timer length in ms [l2f.par]
l2fd.max_tunnels:        30     # Max. number of L2F tunnels [l2f.par]
l2fd.max_callers:        30     # Max. number of callers in all [l2f.par]
#                                       # L2F tunnels [l2f.par]
#
#############################################################################
# Parameter for isdn_ll (process for serving one leased line connection)
#############################################################################
isdn_ll_1.log_error_file: $(MSG_LOGFILE) # Error-Logging => Logfile
#isdn_ll_1.log_msg_file:  $(MSG_LOGFILE) # Msg-Logging => Logfile
isdn_ll_1.log_msg_file:          # No Msg-Logging
#isdn_ll_1.log_data_file: $(DATA_LOGFILE)# Data-Logging => Logfile
isdn_ll_1.log_data_file: # No Data-Logging
isdn_ll_1.service:                PPP    # Service: PPP, ISS
isdn_ll_1.capi_b2protocol:  0x02    # HDLC-TRANSPARENT
isdn_ll_1.capi_b3protocol:       0x04    # TRANSPARENT
isdn_ll_1.capi20_b1protocol:     0x00    # HDLC
isdn_ll_1.capi20_b2protocol:     0x01    # TRANSPARENT
isdn_ll_1.capi20_b3protocol:     0x00    # TRANSPARENT
isdn_ll_1.controller:               0    # Controller for leased line
isdn_ll_1.timeslot:                29    # Timeslot of leased line
isdn_ll_1.dialnumber:                    # Dialnumber for dialout
#
isdn_ll_2.log_error_file: $(MSG_LOGFILE) # Error-Logging => Logfile
#isdn_ll_2.log_msg_file:  $(MSG_LOGFILE) # Msg-Logging => Logfile
isdn_ll_2.log_msg_file:          # No Msg-Logging
#isdn_ll_2.log_data_file: $(DATA_LOGFILE)# Data-Logging => Logfile
isdn_ll_2.log_data_file: # No Data-Logging
isdn_ll_2.service:                PPP    # Service: PPP, ISS
isdn_ll_2.capi_b2protocol:  0x02    # HDLC-TRANSPARENT
isdn_ll_2.capi_b3protocol:       0x04    # TRANSPARENT
isdn_ll_2.capi20_b1protocol:     0x00    # HDLC
isdn_ll_2.capi20_b2protocol:     0x01    # TRANSPARENT
isdn_ll_2.capi20_b3protocol:     0x00    # TRANSPARENT
isdn_ll_2.controller:               0    # Controller for leased line
isdn_ll_2.timeslot:                28    # Timeslot of leased line
isdn_ll_2.dialnumber:                    # Dialnumber for dialout
#
# Leased Line Timeout-Defaults:
isdn_ll_1.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_1.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_2.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_2.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_3.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_3.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_4.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_4.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_5.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_5.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_6.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_6.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
```

```
isdn_ll_7.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_7.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_8.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_8.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_9.session_timeout:  0   # Maximum session time (in msec)(0=endless)
isdn_ll_9.idle_timeout:     0   # Maximum idle time    (in msec)(0=endless)
isdn_ll_10.session_timeout: 0   # Maximum session time (in msec)(0=endless)
isdn_ll_10.idle_timeout:    0   # Maximum idle time    (in msec)(0=endless)
#
##############################################################################
# Parameter for snsp_server (Suprimo Name Service Protocol Server)
##############################################################################
snsp_server.log_error_file: $(ERROR_LOGFILE)     # Error-Logging => Logfile
#snsp_server.log_msg_file: $(MSG_LOGFILE)        # Msg-Logging => Logfile
snsp_server.log_msg_file:        # No Msg-Logging
#snsp_server.log_data_file: $(DATA_LOGFILE)      # Data-Logging => Logfile
snsp_server.log_data_file:       # No Data-Logging
snsp_server.snsp_max_timeout: 3000               # Timeout for responses in ms.
#                                                    # [dlm.par]
##############################################################################
# Parameter for emas (Extended Multiple Access Server)
##############################################################################
emas.log_error_file: $(ERROR_LOGFILE)     # Error-Logging => Logfile
#emas.log_msg_file: $(MSG_LOGFILE)        # Msg-Logging => Logfile
emas.log_msg_file:                 # No Msg-Logging
#emas.log_data_file: $(DATA_LOGFILE)      # Data-Logging => Logfile
emas.log_data_file:                # No Data-Logging
#
emas.mpra_frag_timeout:  1000 # Timeout old Multilink PPP (MP) fragments [in ms]
#                             # [ppp.par]
emas.mpra_max_frags:      100 # Max. number of MP fragments in reassembler table
#                             # [ppp.par]
#
##############################################################################
# Parameter for pramon
##############################################################################
pramon.log_error_format:FXC
pramon.log_msg_file:             # No Msg-Logging
pramon.refresh_default:2000      # Monitor refreshtime in ms [process.par]
#
##############################################################################
# Parameter for www_suprimon
##############################################################################
www_suprimon.log_error_format:  FXC
www_suprimon.log_msg_file:   /dev/null           # No Msg-Logging
www_suprimon.log_error_file: $(ERROR_LOGFILE)    # Error-Logging => Logfile
www_suprimon.www_refresh:   0  # time for page-refresh in seconds [process.par]
www_suprimon.www_reflines: 15  # count of lines from the end of file shown while
#                               # refreshing page [process.par]
#
##############################################################################
# Parameter for www_sysadm
##############################################################################
www_sysadm.log_error_format:  FXC
www_sysadm.log_msg_file:   /dev/null           # No Msg-Logging
www_sysadm.log_error_file: $(ERROR_LOGFILE)    # Error-Logging => Logfile
#
##############################################################################
# Parameter for www_param_get
```

```
#############################################################################
www_param_get.log_error_format:  FXC
www_param_get.log_msg_file:   /dev/null           # No Msg-Logging
www_param_get.log_error_file: $(ERROR_LOGFILE)    # Error-Logging => Logfile
#
#############################################################################
# Parameter for www_param_put
#############################################################################
www_param_put.log_error_format:  FXC
www_param_put.log_msg_file:   /dev/null           # No Msg-Logging
www_param_put.log_error_file: $(ERROR_LOGFILE)    # Error-Logging => Logfile
#
#############################################################################
# Parameter for debuglog
#############################################################################
#
#
# Parameter for debuglog0
debuglog0.device:            /dev/tty2a   # serialport of ISDN-Card-Debugport
#                                         # [process.par]
debuglog0.poll_tmo:          10000        # Poll-Timeoutzeit
#                                         # according to list in cards.par
debuglog0.log_error_file: $(ERROR_LOGFILE)# Error-Logging => Logfile
debuglog0.log_msg_file:   $(MSG_LOGFILE)  # Msg-Log (ISDN-Debugdata) => Logfile
debuglog0.log_msg_format:    XzZC
debuglog0.log_msg_depth:     1-1
# Parameter for debuglog1
debuglog1.device:            /dev/tty1a   # serialport of ISDN-Card-Debugport
#                                         # [process.par]
debuglog1.poll_tmo:          10000        # Poll-Timeoutzeit
#                                         # according to list in cards.par
debuglog1.log_error_file: $(ERROR_LOGFILE)# Error-Logging => Logfile
debuglog1.log_msg_file:   $(MSG_LOGFILE)  # Msg-Log (ISDN-Debugdata) => Logfile
debuglog1.log_msg_format:    XzZC
debuglog1.log_msg_depth:     1-1
#
#############################################################################
# Parameter for dcm  (D-channel-monitor)
#############################################################################
#
dcm.log_data_file: $(DATA_LOGFILE)        # Data-Logging => Logfile
dcm.log_data_format:    ZXC
dcm.log_msg_format:     ZX
#
#############################################################################
# Parameter for practrl
#############################################################################
practrl.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
practrl.log_error_format: zZYFDTPXC      # Errors with Date and time
#practrl.log_msg_file:$(MSG_LOGFILE)   # Msg-Logging => Logfile
practrl.log_msg_file:            # No Msg-Logging
#
practrl.max_temp:             40  # Max. Temperature (in degree C) [process.par]
practrl.check_auth_errors:        # time-interval to keep errors (in minutes)
#                              # [process.par]
practrl.trap_auth_errors:    10   # send trap after this number of auth-errors
#                              # [process.par]

practrl.debuglog_cnt: 1           # number of debuglog-daemons [process.par]
```

```
practrl.ctrl_temperature_log:     # Time to log Temp in practrl.info (opt,in ms)
#                               # [process.par]
practrl.start_l2fd:            0  # Start Tunnelprocess L2FDaemon (1=yes,0=no)
#                               # [process.par]
practrl.cmd_ixload:       cd /usr/itk/ixload; ./ixload %s && sleep 2
#                                 Command: Download of ITK-cards
practrl.cmd_viper542load:   /usr/itk/ixload/viperload  /usr/itk/ixload/v542.bin  %d
%d
#                                 Command: Download of Viper-Board type 542
practrl.cmd_viper548load:   /usr/itk/ixload/viperload  /usr/itk/ixload/v548.bin  %d
%d
#                                 Command: Download of Viper-Board type 548
practrl.cmd_viper549load:   /usr/itk/ixload/viperload  /usr/itk/ixload/v549.bin  %d
%d
#                                 Command: Download of Viper-Board type 549
practrl.cmd_wdstart:      $(PJEXE)wd_daemon
#                                 Command: Start Watchdog-Daemon
practrl.cmd_dlstart:      $(PJEXE)debuglog
#                                 Command: Start DebugLog-Daemon
practrl.cmd_del_log: find /u/pra/log -mtime +5 -print | xargs rm -f; rmdir /u/pra/
log/*; exit 0
#                                 Command: Remove old Logfiles [process.par]
practrl.cmd_start_practrl: $(PJEXE)start_practrl
#                                 Command: Start Practrl
practrl.infofile: /u/pra/log/practrl.info # Name of PRACTRL-Informationfile
practrl.info_syslog_target:       # IP-Addr. of SYSLOG-Host (opt.) [process.par]
practrl.restart:                  # Restart-Time: [process.par]
#                                     empty: default (once per day)
#                                     0:     never
#                                     N:     every N hours
practrl.restart_type: 2           # Restart-Type: [process.par]
#                                 # Legal values are : 2 = Capi-Reload
#                                   # (Shutdowntypes)    3 = Reload NetBlazer 8xxx
Software
#                                 #                    4 = Reboot
#                                 #                    5 = Coldboot
practrl.time_prc_runok:   600000  # Timeinterval, where process-restarts are
#                                   counted as failed [ms] [process.par]
practrl.max_prc_restarts:      5  # Max. number of Process-Restarts [process.par]
practrl.time_prc_tests:   300000  # Time between process-checks [ms] [process.par]
practrl.shuttime_abort:   -60000  # Shutdown-Inactivitytime after Errors [ms]
#                                 # [process.par]
practrl.shuttime_normal:  300000  # Inactivitytime for normal Shutdown [ms]
#                                 # [process.par]
practrl.night_begin_hour:       03   # Start-hour of Night-Time (Restarts) [pro-
cess.par]
practrl.night_end_hour:       05  # End-hour   of Night-Time [process.par]
practrl.time_modemtests: 36000000 # Time between Modemtests [ms] [process.par]
practrl.time_modemtest1:  600000  # Time for first Modemtest after Restart [ms]
#                                 # [process.par]
practrl.time_isdntests:    30000  # Time between ISDN-Cardtests [ms] [process.par]
practrl.time_tempcheck:    120000   # Time between Temperature-tests [ms] [pro-
cess.par]
practrl.time_shutdowncheck:10000  # Time between Shutdown-complete-tests [ms]
practrl.time_hddcheck:    300000  # Time between HDD-freespace-tests [ms]
#                                 # [process.par]
practrl.hdd_space_remaining:   2  # Minimal free HDD-space [%]
#                                 # [process.par]
practrl.max_ixloads:           5  # Max. number of succeeding IXLOADS => REBOOT
#                                 # [process.par]
```

```
practrl.max_ixloads_night:    10  # After N IXLOADS + nighttime => Reboot
#                                 # [process.par]
practrl.max_ixloads_day:      20  # After N IXLOADS + daytime   => Reboot
#                                 # [process.par]
practrl.max_isdn_errors:       5  # Max. errorcount at ISDN-card  => IXLOAD
#                                 # [process.par]
practrl.max_modem_errors:     10  # Max. errorcount at Modem-card => IXLOAD
#                                 # [process.par]
practrl.reboot_typ:            0  # Reboot-Type: 0=Warm+Cold-Reboots allowed
#                                 #              1=do only Warm-Reboots
#                                 #              2=do only Cold-Boots
#                                 # [process.par]
practrl.capi_debug_isdn: #cmt l3; cmt l3x # CAPI-Debug-Command for ISDN-Cards
#                                       # [process.par]
practrl.capi_debug_modem: #at 60 s91=15    # CAPI-Debug-Command for Modem-Cards
#                                          # [process.par]
#
practrl.command_events_cnt:    0  # Number of User-defined commands executed by
#                                 # practrl after a defined interval [process.par]
# example for one user-defined command
# every 5 minutes date is send to file test.txt
# start time is 14:30 ,but this start time will be ignored for intervalls
# smaller than one day (86400 seconds)  !!!
practrl.command_event_1: date > test.txt   # command to execute [process.par]
practrl.command_event_interval_1: 300        # interval for event in sec. [pro-
cess.par]
practrl.command_event_starttime_1: 14 30    # hour minute of first start [pro-
cess.par]
# the LEDs named WAN /LAN are green when special IP-addresses respond
# when no IP-Address is defined the LED will be off
practrl.cmd_start_check_net: $(PJEXE)check_net # command to start test for IP-
address
practrl.time_check_net: 60000 # interval to check IP-adresses of LAN/WAN LEDs
#                             # [process.par]
practrl.lan_test_ip:   # IP-address to check LAN-interface [misc.par]
practrl.wan_test_ip:   # IP-address to check WAN-interface [misc.par]
practrl.max_test_failure: 10 # number of failed interface-checks to start a Shut-
down
#                          # Coldboot [misc.par]
# practrl evaluates cpuload for three intervals
practrl.cpuload_check_1: 60000          # interval for Cpuload checks in ms
practrl.cpuload_check_2: 300000         # interval for Cpuload checks in ms
practrl.cpuload_check_3: 900000         # interval for Cpuload checks in ms
# practrl checks d-channel status of all ISDN-cards
practrl.time_d_channel: 15000 # interval for D-channel checks
##############################################################################
# Parameter for pramodtest
##############################################################################
pramodtest.log_error_file: $(ERROR_LOGFILE) # Error-Logging => Logfile
#pramodtest.log_msg_file:  $(MSG_LOGFILE)   # Msg-Logging => Logfile
pramodtest.log_msg_file:                    # No Msg-Logging
pramodtest.log_info_format:       XC        # Infologging: Create Logfile
#
##############################################################################
# Parameter for fw_check
##############################################################################
fw_check.log_error_file:        <STDOUT> # Error-Logging => stdout
fw_check.log_error_format:      YX
#fw_check.log_msg_file:         <STDOUT> # Msg-Logging => Logfile
```

```
fw_check.log_msg_file:                  # No Message-Logging
#
###############################################################################
# Parameter for wd_daemon
###############################################################################
wd_daemon.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
wd_daemon.log_msg_file:          # No Msg-Logging
#
###############################################################################
# Parameter for modemtest
###############################################################################
modemtest.log_error_file:       <STDOUT>         # Error-Logging => stdout
modemtest.log_error_format:     YX
#modemtest.log_msg_file:        <STDOUT> # Msg-Logging => stdout
modemtest.log_msg_file:                 # No Message-Logging
#
###############################################################################
# Parameter for qciser
###############################################################################
qciser.log_data_file:           <STDOUT>
qciser.log_data_fname:  main*,handle*,Get*
qciser.log_msg_file:    <STDOUT>
qciser.log_msg_format:  FXC
qciser.log_msg_fname:   main*,handle*,Get*
qciser.log_msg_depth:   0-2
qciser.log_error_file:  <STDOUT>
qciser.log_error_format:        FXC
#
###############################################################################
# Parameter for pra_shutdown
###############################################################################
pra_shutdown.log_error_file:        <STDOUT>  # Error-Logging => stdout
#pra_shutdown.log_msg_file: $(MSG_LOGFILE)        # Msg-Logging => Logfile
pra_shutdown.log_msg_file:        # No Msg-Logging
#pra_shutdown.log_data_file: $(DATA_LOGFILE)      # Data-Logging => Logfile
pra_shutdown.log_data_file:       # No Data-Logging
#
###############################################################################
# Parameter for iss (ISS-Daemon for communication to EWSD)
###############################################################################
issd.log_error_file:$(ERROR_LOGFILE) # Error-Logging => Logfile
.start_iss: 0             # 1 : start ISS-Daemon,0 : do not start ISS-Daemon
.iss_uip_pool:  100       # IP-Pool-ID for ISS IP addresses of EWSD
#
###############################################################################
# Parameters for h323d (H.323 demon)
###############################################################################
##### Logging format #####
# (For the meaning of the format see in common.par)
# (e.g. H = show Thread-ID (TID) )
h323d.log_error_format:  ZYFDTPXCH
h323d.log_msg_format:    ZYFXCH
h323d.log_fstart_format: ZYFTCH
h323d.log_fende_format:  ZYFTCH
#
##### Logging output #####
h323d.log_error_file:   $(ERROR_LOGFILE) # Error-Logging => Logfile
#h323d.log_msg_file:    $(MSG_LOGFILE)   # Msg-Logging => Logfile
h323d.log_msg_file:                     # No Msg-Logging
```

```
#h323d.log_data_file:   $(DATA_LOGFILE)  # Data-Logging => Logfile
h323d.log_data_file:                     # No Data-Logging
#h323d.log_direct_file: $(DATA_LOGFILE)  # Direct-Logging => Logfile
h323d.log_direct_file:                   # No Direct-Logging
#
##### Logging level of intermediate logging interface #####
# (Only relevant levels are shown here!)
#
# Error                   0
# Warning                 1
# Info                    2
# Commands (internal)     3
# LAN messages            6
# All details             8
# Periodic events        19
#
h323d.log_level: 10
#
##### Logging component mask of intermediate logging interface #####
# (Only relevant masks are shown here!)
#
# (Set bit for bit, combinations possible)
# Log no components           0x00000000
# ASN                         0x00000004
# H.245                       0x00000010
# H.323                       0x00000080
# Q.931                       0x00000100
# Miscellaneous               0x00000200
# Protocol handler            0x00000400
# Main module                 0x00000800
# SPC wrapper                 0x00001000
# Log all components          0xffffffff
#
h323d.log_component_mask: 0xffffffff
#
##### Connection handling parameters ####
h323d.use_early_h245_tsap:  1            # Using early connect of call control
#                                        # channel (no=0/1=yes)
#
h323d.wait_for_remote_connect: 0         # (no=0/yes=1)
#
h323d.Q931CallingPartyNoOctet3a: 0x80    # H.225 shall not use Q.931 octet 3a of
#                                       # calling party number information element
#                                        # but you can configure it here for
#                                        # the SNSP_DO_DIALOUT_REQ
##### Gatekeeper parameters #####
h323d.use_gatekeeper:      0             # Using gatekeeper (no=0/yes=1)
#h323d.ip_addr_gatekeeper:               # Try to find a gatekeeper by broadcast
#h323d.ip_addr_gatekeeper: 123.45.67.89  # IP address of gatekeeper
#
##### Prefix parameters #####
# (e.g. may be needed for referencing gateways in a gatekeeper)
h323d.PBXExternCallPrefix:          0    # Prefix for extern calls using a PBX
h323d.AudioOnlyCallInternPrefix:         # No prefix for intern audio calls
#h323d.AudioOnlyCallInternPrefix:  92    # Prefix for intern audio calls
h323d.AudioOnlyCallExternPrefix:         # No prefix for extern audio calls
#h323d.AudioOnlyCallExternPrefix:  93    # Prefix for extern audio calls
#
################################################################################
```

```
# DEFAULT-PARAMETER
################################################################################
# Show Parameter-Values: (0=off, 1=on (to stdout))
.param_show: 0
################################################################################
# Logging:
# *_file:    Name of Output-Device (Device, File, <STDOUT> or <STDERR))
#                   (no value => no Logging)
# *_format:  Format of outputline (combinations possible):
#                   Z = show Time
#                   z = show Date
#                   Y = show Logging-Type
#                   F = show Name of Function
#                   D = show name of Module (Filename)
#                   T = show calling-depth
#                   P = show Process-ID (PID)
#                   H = show Thread-ID (TID)
#                   X = show Logging-Text
#                   C = do Buffer-Clear (Flush) after Logging-Output
#                          O = write outputline additionally to STDOUT
#                   S = show Stack of Calling-Functions
#                          A = do not open Logfile, if not already open
#                   * = show all
#                   (no value => no Logging)
# *_depth:   Filter for Calling-depth (from-to)
# *_fname:   Filter for Functionnames
#                      (separated by ',', skip Function with '!', wildcard '*' at
end)
# *_level:      Logging level (set bit for bit, combinations possible)
#               (until now only for data logging)
#                   0x00000001    received SPC packets
#                   0x00000002    sent SPC packets
#                   0x00000004    received CAPI packets
#                   0x00000008    sent CAPI packets
#                   0x00000010    received Shell packets
#                   0x00000020    sent Shell packets
#                   0x00000040    received IP packets
#                   0x00000080    sent IP packets
#                   0x00000100    received PSP packets
#                   0x00000200    sent PSP packets
#                   0x00000400    received L2F packets
#                   0x00000800    sent L2F packets
#                   0x00001000    internal tables of L2F daemon
#                   0x00002000    RADIUS requests and answers
#                   0xffffffff    log all levels
#                   0x00000000    log no level
#
.log_error_file:<STDERR> # Error-Logging-Output => stderr
.log_error_format:      ZYFDTPXC
.log_error_depth:       0-10000
.log_error_fname:*
.log_fstart_file:# No Functionstart-Logging
.log_fstart_format:ZYFTC
.log_fstart_depth:      0-10000
.log_fstart_fname:*
.log_fende_file:# No Functionend-Logging
.log_fende_format:ZYFTC
.log_fende_depth:       0-10000
.log_fende_fname:*
```

```
.log_msg_file:         <STDOUT> # Message-Logging-Output => stdout
.log_msg_format:        ZYFXC
.log_msg_depth:        0-10000
.log_msg_fname:        *
.log_data_file:        # No Data-Logging-Output
.log_data_format:       ZXC
.log_data_depth:0-10000
.log_data_fname:*
.log_data_level:0xffffffff
.log_info_file:        $(log_error_file) # Info-Logging => Error-Logging
.log_info_format:       XCA
.log_info_depth:0-10000
.log_info_fname:*
.log_direct_file:       # No Data-Logging-Output
.log_direct_format:     XC
.log_direct_depth:      0-10000
.log_direct_fname:      *
###############################################################################
###############################################################################
# global NetBlazer 8xxx Parameter (process-independent)
###############################################################################
.netblazer_name: # Name of NetBlazer (default: NetBlazer 8100 or 8500)
.pra_language: E        # NetBlazer 8xxx-Language: D=german, E=english [misc.par]
.accounting_file:  /u/pra/log/$(DATE).acc   # File for Accounting-Records
# Message-Buffer-Parameter:
.msgsize:          2048# max. message-length
.capi_maxcount:        20      # max. number of msgs in TO_CAPI-Msg-Buffer
.capi_low_water:2       # Lowwater-Mark      in TO_CAPI
.capi_high_water:4       # Highwater-Mark     in TO_CAPI
.capi_windowsize:3       # Windowsize         in TO_CAPI
.psp_maxcount:         20      # max. number of msgs in TO_LAN-Msg-Buffer
.psp_low_water:        3       # Lowwater-Mark      in TO_LAN
.psp_high_water:8       # Highwater-Mark     in TO_LAN
# PSP-Parameter:
.psp_timeout_open_recv:  30000 # Timeouttime for psp_open_recv-Wait in msec
.psp_timeout_call_recv:  30000  # Timeouttime for psp_call_recv-Wait in msec
.psp_timeout_call_conf:  30000  # Timeouttime for psp_call_conf-Wait in msec
# PPP-Parameter:
.ppp_fifo_size:           5000  # Length of FIFO-Stream-Buffer for PPP/SLIP
.ppp_firewall_file:    $(PJDAT)firewall        # Begin of Packetfilter-Filename
.ppp_firewall_default: $(PJDAT)firewalldefault # Name of Default-Packetfilter
.fw_unknown_prot:        REJECT # Always reject unknown IP protocols
#                                 (If set to "PASS" they may pass the
#                                  firewall according to the filter rules)
.ppp_adrprompt1:        Server address is %s   # SLIP-Output for Server-IP-Adr.
#                                              # [ppp.par]
.ppp_adrprompt2:        Your address is %s     # SLIP-Output for Client-IP-Adr.
#                                              # [ppp.par]
.ppp_patch_ip:                 # no IP-Adr.-Patch
#                              # [ppp.par]
#
# Misc Parameter
.start_delay:               0  # Delay before beginning of sending/receiving
#                                       data in msec
.port_limit:              1000  # Per User Limit of simultaneous connections
.subnetting:                0  # Must be set to 1, if any of the UIP-Pool
#                                 subnets belongs to the Class-C net of any
#                                         LAN/WAN interfaces
.set_uip_routes:            1  # Must be set to 0 if no routes should be set
```

```
#                                # for UIP-address-pools [uip_pool.par]
.set_static_routes:           0  # Must be set to 1, if routes should be set
#                                  (and deleted) for static UIP addresses
.dist_homing:          0     # Distributed Home Serving (0 disabled, 1 enabled)
#                            # [dlm.par]
.dialout:              0     # 0 disabled , 1 enables Dialout [dlm.par]
.ignore_packet_time:  10000 # time in msec to ignore further Dialoutrequests
#                            # after sending one [dlm.par]
.dialout_tmo: 3600000        # maximum time in msec between last use of
#                            # an address and a Dialout [dlm.par]
# Delegation of Dialouts via SNSP-Server
#
.partner_cnt: 0 # no partners [dlm.par]
.partner_broadcast: # not available
#.partner_cnt: 4 #number of NetBlazers 8xxx to delegate callout to
#.partner_1:  192.168.17.42  #  list  of  IP-adresses  of  other  NetBlazers  8xxx
[dlm.par]
#.partner_2: 192.168.18.45
#.partner_3: 192.168.17.23
#.partner_4: 192.168.19.45
#
# User-Timeout-Defaults:
.session_timeout:       0   # Maximum session time per user(in msec)(0=endless)
.idle_timeout:          0   # Maximum idle time per user   (in msec)(0=endless)
#
# CAPI-Parameter:
.capi_timeout_conf:  3000  # Timeouttime for Confirm-Wait in msec
.capi_timeout_ind:       30000# Timeouttime for Indication-Wait in msec
.capi_fallback_tmo:       5000  # Timeout for Fallback to V.110 in ms [isdn.par]
.capi_callback_delay:        0  # Delay before a callback is initiated in msec
#                               # [dlm.par]
.capi_level3cnt:      1 # Max number of B3-Connections
.capi_datablkcnt_b3:     7 # Number of B3-Datablocks
.capi_datablklen_b3:      2048 # Max length of B3-Datablock (X.75 + HDLC)
.capi_datablklen_b3_v110:  400 # Max length of B3-Datablock (V.110)
.capi_datablklen_b3_sbv:  2048 # Max length of B3-Datablock (SBV:X.25)
.capi_numbchannel:           1 # Number of B-Channels
.capi_maxbchannel:           1 # Max. B-Channels
.capi_b2protocol:         0x01 # B2-Protocol for 64kbit-connections: X.75
.capi_b2protocol_v110:    0x08 # B2-Protocol for V.110-connections:  V.110
.capi_b2protocol_sbv:     0x01 # B2-Protocol for SBV-connections:    X.75
#                                          0x01 B2_X75_SLP
#                                          0x02 B2_HDLC_TRANSPARENT
#                                          0x03 B2_BITTRANSPARENT
#                                          0x04 B2_SNA_SDLC
#                                          0x05 B2_X75_BTX
#                                          0x06 B2_T30_FAX
#                                          0x08 B2_V110
#                                          0x0b B2_BITTRANS_SEND_ONLY
#                                          0x0c B2_MODEM
#                                          0x0d B2_PPP
#                                          0x0e B2_MVIP
.capi_b3protocol:         0x04 # B3-Protocol for 64kbit-connections: transp.
.capi_b3protocol_v110:    0x04 # B3-Protocol for V.110-connections:  transp.
.capi_b3protocol_sbv:     0x02 # B3-Protocol for SBV-connections:    X.25
#                                          0x01 B3_T70_NL
#                                          0x02 B3_ISO_8208
#                                          0x03 B3_T90
#                                          0x04 B3_TRANSPARENT
```

```
#                                       0x05 B3_T30_FAX
.capi_simask:           0x0080 # Service-Indicator-Mask
#                                       [bit]:
#                                    1  : telephonie
#                                    2  : a/b-Services
#                                           5  : Btx (64 kbit/s)
#                                           7  : Data (64 kbit/s)
#                                           8  : X.25-Service
#                                   15  : BTX (new standard) (SBV)
.capi_infomask:           0x00 # Info-Mask
.capi_eazmask:          0x03ff # EAZ-Mask
.capi_compresssel:        0x00 # Compression Selection
#                                       0: No Compression
#                                       1: V.42bis
.capi_compressmode:       0x00 # Compression-Mode
#                                       0: Optional
#                                       1: mandatory
.capi_outgservice:        0x07 # Outgoing service for 64kbit-data-connections
.capi_outgservice_sbv:    0x0f # Outgoing service for SBV-connections
.capi_addinfooctett:      0x00 # Additional information octet
.capi_origtypplan:        0xa1 # Origin Typ / Plan
.capi_desttypplan:        0x81 # Destination Typ / Plan
.capi_eaz:                   0  # Source EAZ for outgoing calls
.capi_datablklen_b2:      2056 # Max length of B2-Datablock (X.75 + HDLC)
.capi_datablklen_b2_v110:  512 # Max length of B2-Datablock (V.110)
.capi_datablklen_b2_sbv:  2056 # Max length of B2-Datablock (SBV:X.25)
.capi_datablklen_b2_voip:  512 # Max length of B2-Datablock (Voice over IP)
.capi_link_add_a:      3 # link address a
.capi_link_add_b:      1 # link address b
.capi_modulo_mode:     8 # Modulo mode (B2 Packetnumbering)
.capi_window_size:     7 # Max number of unacknowledged B2 Packets
.capi_xid_length:         0x00 # Length of XID-Block
#
.capi20_b1protocol:         0x00 # B1-Protocol for 64kbit-connections: HDLC
.capi20_b2protocol:         0x00 # B2-Protocol for 64kbit-connections: X.75
.capi20_b1protocol_v110:    0x02 # B1-Protocol for V.110-connections:  V.110 async
.capi20_b2protocol_v110:    0x01 # B2-Protocol for V.110-connections:  transp
.capi20_b1protocol_x25:     0x00 # B2-Protocol for X.25-connections:   HDLC
.capi20_b2protocol_x25:     0x01 # B2-Protocol for X.25-connections:   X.75
.capi20_b3protocol:         0x00 # B3-Protocol for 64kbit-connections: transp.
.capi20_b3protocol_v110:    0x00 # B3-Protocol for V.110-connections:  transp.
.capi20_b3protocol_x25:     0x02 # B3-Protocol for X.25-connections:   X.25
.capi20_cipmask:          0x0004 # Compatibility information profile
.capi20_cipvalue:         0x0002 # Compatibility information profile
.capi20_infomask:         0x0141 # Info-Mask
.capi20_origtypplan:        0xa1 # Origin Typ / Plan
.capi20_desttypplan:        0x81 # Destination Typ / Plan
.capi20_window_size_b2:     7 # Max number of unacknowledged B2 Packets
.capi20_window_size_b3:     2 # Max number of unacknowledged B3 Packets
.capi_datablklen_b3_x25:  2048 # Max length of B3-Datablock X.25
.capi_datablklen_b3_voip:  512  # Max length of B3-Datablock voip
.capi20_clip:                0  # Calling Line Id presentation (1:on 0:off)
#
.capi_modem_initstring: AT      # Modem-Init-String
.modemtest_initstring:  AT      # Modem-Init-String for the modem selftests
.modemtest_dlpdblocklen:  2048  # Max length of Modem Datablock (selftests)
#
##############################################################################
# Parameters for Suprimo Process Communication (spc)
```

```
#############################################################################
.spc_commtype:              2  # SPC-Communication-Type (1=FIFO, 2=UDP)
.spc_snsp_port:         30000  # spc-port for Suprimo Name Service Protocol (snsp)
#############################################################################
# Parameters for Communication-cards (see cards.par)
#############################################################################
# ISDN-Cards:
# .icard_*: Controller Channel-Count
.icard_cnt:  1                 # No. of ISDN-Cards
.icard_1:    0      30 # Controller 0 (30 Channels)
# Modemcards:
# .mcard_*: Controller Modem-Count
.mcard_cnt:  0                 # No. of Modemcards
#.mcard_1:   1       8 # Controller 1 (8 Modems)
#
# Compression cards:
# .ccard_*: Board-Id, Number of DSPs, Channels on DSP
.ccard_cnt:  0                 # No. of Compression cards
#.ccard_1:   0      12      2   # Board 0, 12 DSPs, 2 Channels on each DSP
#
#############################################################################
# ISDN-Parameters (for s2m- and s0-Interface) (see isdn.par)
#############################################################################
.capi_subadd_ignore:         0  # Number of digits that should be ignored from
#                               #   the direct-dialin-number [isdn.par]
.capi_callid_prefix:           # Digits used as the caller-id-prefix [isdn.par]
.capi_subadd_cnt:     2# Number of direct-dialin-digits to read [isdn.par]
.capi_subadd_tmo:  3000  # Timeouttime waiting for direct-dialin-digits
#                               # [isdn.par]
#.isdn_local_id_0: 4     12345  # transfer EAZ 4 to multiple subscriber
#                               # number 12345 [isdn.par]
.isdn_local_id_0:               # controller-0: set default nothing
.isdn_local_id_1:               # controller-1: set default nothing
.isdn_local_id_2:               # controller-2: set default nothing
.isdn_local_id_3:               # controller-3: set default nothing
.isdn_local_id_4:               # controller-4: set default nothing
.isdn_local_id_5:               # controller-5: set default nothing
.isdn_local_id_6:               # controller-6: set default nothing
.isdn_local_id_7:               # controller-7: set default nothing
.isdn_local_id_8:               # controller-8: set default nothing
.isdn_local_id_9:               # controller-9: set default nothing
#
#############################################################################
# Special process-Parameters (see process.par)
#############################################################################
# Maximal number of connections:
.linecnt_isdn_in:30  # max. number of ISDN-IN-Connections  (ISDN-In)
#                           # [process.par]
.linecnt_isdn_out:30  # max. number of ISDN-OUT-Connections (ISDN-Out)
#                           # [process.par]
.linecnt_pstn_in:30  # max. number of PSTN-IN-Connections  (Modem-In)
#                           # [process.par]
.linecnt_pstn_out: 0  # max. number of PSTN-OUT-Connections (Modem-Out)
#                           # [process.par]
.linecnt_pspdn:        30  # max. number of log. X.25-Connections [process.par]
.linecnt_pspdn_ph:      0  # Number of phys. X.31 Connections to Packet-Handler
#                           # [process.par]
.linecnt_isdn_ll: 0  # Number of ISDN_LL Connections (Leased Lines)
#                           # [process.par]
```

```
.linecnt_emas:          0  # Number of EMAS Conn. (extended multiple Access)
#                             # [process.par]
.unpriv_chan_cnt:     1000  # No. of unprivileged B-channels, all remaining chan-
nels
#                           # are reserved for privileged users [dlm.par]
#
##############################################################################
# IP-Address-Pool for dial-in-IP-users (User-IP) (see uip_pool.par)
##############################################################################
# Pools with User-IP-Addresses:
# .ip_pool_x: IP-Address Netmask [Pool-ID]
# If the Pool-ID is omitted, the default of 0 is chosen
.ip_pool_cnt: 0          # [uip_pool.par]
#.ip_pool_1: 194.172.85.32 255.255.255.224 0 # [uip_pool.par]
#
.uip_address_strategy: 0 # Strategy to search/reserve addresses in UIP-pool
#                        #  0: reserve UIP-address in pool after online-
#                        #     authentication just before IPCP-phase (default)
#                        #  1: reserve UIP-address before online-authentication
#                        #    advantages(+)/disadvantages(-):
#                        #     + UIP-address contained in Radius-access-request
#                        #       for online-authentication)
#                        #     - distributed-line-management features (extended
#                        #       short-hold,Multilink-PPP) may not work entirely
##############################################################################
# IP-Address for two DNS-Server (see misc.par)
##############################################################################
.ppp_dns1:             # primary DNS-IP-Address [ppp.par]
.ppp_dns2:             # secondary DNS-IP-Address [ppp.par]
#
##############################################################################

##############################################################################
# PPP Client/Server Mode (Default: MODE_SERVER) (see auth.par)
##############################################################################
.PPP_Client_Server_Mode:         # MODE_CLIENT or MODE_SERVER

##############################################################################
# With this two parameter it is possible to chance the default entry
# in RADIUS file users (see auth.par)
##############################################################################
.users_default_entry: DEFAULT# default is DEFAULT [auth.par]
.users_default_pw: SUPRIMO# default is SUPRIMO [auth.par]

##############################################################################
# With this parameter it is possible to set the PPP compression protocol.
# You can set more than one compression protocol with a separator ':'.
# The default entry is no compression protocol
##############################################################################
.ppp_compression:                    # PRED1:STAC [ppp.par]
#                                    # PRED1 = Predictor type 1
#                                    # STAC  = PPP Stac LZS
##############################################################################
# Parameters for Authentication and Accounting (see auth.par)
##############################################################################
##############################################################################
# Request-Types:
#   The ADNS- and Authentication-Server-Requests can be done in a predefined
#   multiple-step way:
```

```
#   Each character in the Request-Type specifies one Request, which is
#   formatted in the following way:
#     A : The combination of caller-id (CID) and direct-dialin (DDI) is used
#     B : Only the caller-id (CD) is used
#     C : Only the direct-dialin (DDI) is used
#     Z : The default-entry is used
#   The first request that gives a positive answer terminates the process.
#   Example: With Request-Type=BCZ:
#               1. B: A request with the caller-id is used,
#          if this gives no answer then:
#               2. C: A request with the direct-dialin is used
#          if this gives no answer then:
#               3. Z: The request for Default-Parameters is used
##############################################################################
# ADNS-Protocol for selecting the responsible Authentication-Server
# (optional, only for Multiproviding (Service-Selection))
##############################################################################
.adns_prot:            NONE             # ADNS-Protocol (NONE or RADIUS) [auth.par]
.adns_req:             CZ               #     ADNS-Request-Types     (see     above)
[auth.par]
# Service-Table-Entry for ADNS:
.stab_adns_cnt:         0# No. of ADNS-Servers [auth.par]
#.stab_adns_addr_1:             # IP-Address of 1st ADNS-Server [auth.par]
#
##############################################################################
# if no ADNS is used one Authentication-Server-Protocol must be specified:
#   (1) RADIUS    or
#   (2) PSP)
#
# (1) RADIUS-Authentication-Protocol:
.auth_prot:            RADIUS   # PSP or RADIUS [auth.par]
.auth_req:             BCZ              # Auth.-Server-Request-Types (see above)
#                                        # [auth.par]
# Service-Table-Entry for Authentication-Server (Offline):
.stab_offline_cnt:    1# No. of Authentication-Servers [auth.par]
.stab_offline_addr_1: $(RADIUS_SERVER)# IP-Address of 1st Authent.-Server
#                                        # [auth.par]
# Service-Table-Entry for Authentication-Server (Online):
.stab_online_cnt:    1 # No. of Authentication-Servers [auth.par]
.stab_online_addr_1: $(RADIUS_SERVER)# IP-Address of 1st Authent.-Server
#                                        # [auth.par]
#
# (2) PSP-Authentication/Application-Protocol:
#.auth_prot:    PSP             # PSP or RADIUS
# Service-Table-Entry for Application-Servers:
.stab_isdn_cnt:         3               # No. of ISDN-Appl-Server [auth.par]
.stab_isdn_1:          $(APPL_SERVER)  # IP-Address of 1st ISDN-Appl-Server
#                                        # [auth.par]
.stab_isdn_2:
.stab_isdn_3:
.stab_pstn_cnt:         3               #   No.   of   PSTN-Appl-Servers   (Modem)
[auth.par]
.stab_pstn_1:          $(APPL_SERVER)  # IP-Address of 1st PSTN-Appl-Server
#                                        # [auth.par]
.stab_pstn_2:
.stab_pstn_3:
.stab_pspdn_cnt: 3             # No. of PSPDN-Appl-Servers (X.25) [auth.par]
.stab_pspdn_1:         $(APPL_SERVER)  # IP-Address of 1st PSPDN-Appl-Server
#                                        # [auth.par]
```

```
.stab_pspdn_2:
.stab_pspdn_3:
###############################################################################
#
###############################################################################
# Accounting-Protocol (optional)
###############################################################################
#
.acct_prot:     NONE            # NONE, RADIUS [auth.par]
# Service-Table-Entry for Accounting-Server:
.stab_acct_cnt:   0             # No. of Accounting-Servers [auth.par]
#.stab_acct_addr_1:                      # IP-Address of 1st Accounting-Server
#                                        # [auth.par]
#
###############################################################################
# Parameters for RADIUS-Requests:
###############################################################################
.radius_account_keyword: $(RADIUS_SECRET)# Shared RADIUS-Secret [auth.par]
.radius_adns_keyword:    $(RADIUS_SECRET)
.radius_offline_keyword: $(RADIUS_SECRET)
.radius_online_keyword:  $(RADIUS_SECRET)
.radius_lcr_keyword:     $(RADIUS_SECRET)
.radius_timeout: 3000  # Timeout for requests (in msec) [auth.par]
.radius_resend_count: 3         # Number of trials to send RADIUS packet
#                                 to the same RADIUS Server [auth.par]

.radius_adns_port:   $(RADIUS_ACCESS_PORT)
.radius_offline_port:$(RADIUS_ACCESS_PORT)
.radius_online_port: $(RADIUS_ACCESS_PORT)
.radius_lcr_port:    $(RADIUS_ACCESS_PORT)
.radius_account_port: 1646   # port:1646 (RFC2059) port:1813 (RFC2139) [auth.par]

#
# Shell-Messages:
.shell_banner:             NetBlazer 8500 Authentication Server    # Login-Message
[auth.par]
.shell_usernameprompt:  Username: # Login-Prompt [auth.par]
.shell_passwordprompt:  Password:# Password-Prompt [auth.par]
.shell_prompt:          ITK-NetBlazer>#  Shell-Prompt [auth.par]
.shell_welcomemsg:      Access ok. Type help ...# First Shell-Message
#                                                 # [auth.par]
.itk_radius_offset:   100   #   allowed   values   64-191(depends   on   RADIUS   and
pra_software)
#                       # [auth.par]
#
###############################################################################
# Parameters for FTP-Request:
###############################################################################
.ftp_auth_addr:          # Name/Addr of FTP-Server to use for authentication
#                        # [auth.par]
.ftp_accept_count:   1   # number of special accept-messages from FTP-server
#                        # [auth.par]
.ftp_accept_1: 530-The password has expired.         # 1st accept-message
#                        # [auth.par]
.ftp_timeout:  60000     # max. time to wait for answer-msgs from FTP-server
#                        # [auth.par]
###############################################################################
# Actuality Flag for Parameters
###############################################################################
```

```
.parameter_actual_flag: /u/pra/dat/.running/.actual_flag # if this flag exists
#                                                  # actual parameters are ready
##############################################################################
# Parameters for VoIP:
##############################################################################
.voip_max_dtmf:     15 # Max. number of concurrent DTMF-detections on ISDN board
.voip_jitter_buffer: 1 # Jitter buffer on ISDN card (in bytes)
.voip_pkt_analyze_flag: 0 # 0:NO 1:YES only for test
.voip_pkt_src_delay: 180 # only for test (in ms)
.voip_pkt_variation:  50 # only for test (in ms)
#
#If the NetBlazer does't not receive voice data during voip_idle_tmo
#the session is disconnected. The NetBlazer gets the information for
#this check at regular intervals from voip_rtcp_tmo.
.voip_idle_tmo: 300 # default 300 (in second)
#
.voip_rtcp_tmo: 10000  # Timeout for RTCP request (in msec)
#
.voip_wait_for_any_con_msg: 3000 # Timeout for any setup connection
#                                  messages (in ms) default 3000
#
.voip_empty_setup:   1 # VoIP dialout: D-Channel Setup without a destination
#                        number; needed for DYNDIAL (Enable:1 Disable:0)
.voip_dialout_count: 3 # Max number of dialout_req resends(default: 3)
.voip_ip_tos:     0x10 # IP type of service flags (used by RTP) (see RFC 791)
#                        Bit   0: 0x01 reserved
#                        Bit   1: 0x02 Low Monetary costs
#                        Bit   2: 0x04 High Reliability
#                        Bit   3: 0x08 High Throughput
#                        Bit   4: 0x10 Low Delay
#                        Bit 5-7: Precedence
#
.voip_autocon_discon: 1 # 1: After the automatic connection it is not allowed
#                           for the caller to dial again (default).
#                         0: It is allowed (Only for test)
# DSP compression parameters: [voip.par]
.pcm_companding: 2      # DSP coding: 2=a-law(Europe),1=u-law(US)
.echo_canceller_flag: 1 # Echo Canceller (Enable:1 Disable:0)
.sub_frame_hdr_flag: 0  # The Sub-Frame header (Enables:1 Disables:0)
.vad_flag: 0            # Voice Activity Detection (Enables:1 Disables:0)
.dtmf_det_flag: 0       # DTMF Detector (Enable:1 Disable:0)
.dtmf_relay_flag: 0     # DTMF Tone Passer (DTMF Relay) (Enable:1 Disable:0)
.frame_size: 60         # Frame transfer time (in msec, only 30 or 60 allowed)
.spc_h323_setup: 0      # SPC or H323 stack (SPC:0 H323:1)
##############################################################################
# With this parameter it is possible to set all types of codecs that the
# NetBlazer 8XXX is supported.
# You can set more than one codecs with a separator ':'.
# The default entry is all codecs are set (G711:G723:G729)
##############################################################################
.type_of_codec: G711:G723:G729 # Voice compression codec (G711, G723, G729)
# Parameters for IVR (Interactive Voice Response)(VGI=Voice Guided Input):
.vgi_accnt_l:      12 # Max. length of account-code in Voice-Guided-Input (VGI)
#                       (including the PIN)
.vgi_pin_l:         4 # Length of PIN (Password) at end of account-code (in VGI)
.vgi_autherr_max:   3 # Max. number of authentication-errors in VGI
.voip_lcr_ignore:   1 # Ignore negative Least-Cost-Router (LCR) answers
#                       # (Connection-setup although no info from LCR)
.vgi_timeout:   8000 # Timeout for VGI inputs [ms]
```

```
# Voice sample files for Voice Guided Input in directory $(PJVOI):[voip.par]
.voisam_welcome:      welcome_%s       # voice sample: Welcome
.voisam_account:      account_%s       # voice sample: Account
.voisam_destno:       destno_%s        # voice sample: Dest. phone-number
.voisam_inv_account:  inv_account_%s   # voice sample: invalid Account
.voisam_inv_destno:   inv_destno_%s    # voice sample: invalid phone-number
.voisam_calling:      calling_%s       # voice sample: state "calling"
.voisam_lines_busy:   lines_busy_%s    # voice sample: state "all lines busy"
.voisam_callee_busy:  callee_busy_%s   # voice sample: state "callee busy"
#
.voip_lcr_min_digits: 3           # Minimal digits for LCR for dynamic dialing
# Service-Table-Entry for Least Cost Router(LCR):[voip.par]
.stab_lcr_cnt:         1# No. of LCR
.stab_lcr_addr_1:      $(RADIUS_SERVER) # IP-Address of 1st LCR
#
# number of acceptable Voice-Dialout sources: [voip.par]
snsp_server.voicedialout_source_cnt: 0  # (0 = accept dialout from all gateways)
# list of acceptable sources for voice dialout
#snsp_server.voicedialout_source_1: 127.0.0.1  # IP-address of 1st gw

################################################################################
# These Parameters are used to calculate the size of our SHM-segment
################################################################################
# Each of these values sets a maximum for an other parameter
# .top_linecnt_pspdn sets a maximum for .linecnt_pspdn
# If the value of .linecnt_pspdn is bigger than .top_linecnt_pspdn,
# the software will use the value of .top_linecnt_pspdn instead.
.top_linecnt_pspdn:      30  # .linecnt_pspdn does not accept bigger values
.top_linecnt_pspdn_ph:    2  # .linecnt_pspdn_ph does not accept bigger values
.top_stab_adns_cnt:       5  # .stab_adns_cnt does not accept bigger values
.top_stab_offline_cnt:    5  # .stab_offline_cnt does not accept bigger values
.top_stab_online_cnt:     5  # .stab_online_cnt does not accept bigger values
.top_stab_lcr_cnt:        5  # .stab_lcr_cnt does not accept bigger values
.top_stab_acct_cnt:       5  # .stab_acct_cnt does not accept bigger values
.top_number_uip:        300  # The number of UIP-adresses in all uip-pools must not
#                            # be bigger than this value(SOFTWARE does not start!)
.top_stab_isdn_cnt:       5  # .stab_isdn_cnt does not accept bigger values
.top_stab_pstn_cnt:       5  # .stab_pstn_cnt does not accept bigger values
.top_stab_pspdn_cnt:      5  # .stab_pspdn_cnt does not accept bigger values
```

A.7 All parameters from cards.par

In this chapter you will find an example of the *cards.par* file for your system. This example is specially for the following configuration:

- 2 ITK Primary
- 2 ITK DigitalModem
- 2 Voice compression boards

Take care, that you have choosen the right number of ISDN boards (icard_cnt and mcard_cnt). The spare entries will then be ignored, nevertheless you find them in the example file.

```
#================================================================
# ITK Telekommunik. AG III   TTTTT   K  K  All rights reserved
# Joseph-von            I      T     K K
#   Fraunhofer-Str.23   I      T     KK
# D - 44227 Dortmund    I      T     K K
# Phone (0231) 9747-0  III     T     K  K
#================================================================
# Description:         Cards-Parameterfile
# Product/Project:     NetBlazer8xxx
# Filename:            cards.par
# Subject:             Parameterfile for Communicationcards
#                      and lines, ISDN-interfaces
#================================================================
# ISDN-Cards:
#  .icard_cnt: Count-of-ISDN-Cards
#  .icard_N:     Controller-No   Count-of-B-Channels
# Modemcards:
#  .mcard_cnt: Count-of-Modemcards
#  .mcard_N:     Controller-No   Count-of-Modems      [Modem-pool-id]
# Compressioncards:
#  .ccard_cnt: Count-of-Compression-cards
#  .ccard_N:     Board-Id        Count-of-DSPs        Channels on DSP
#
# Parameter  Ctrl /    Chan /   [M-PoolID]Remark
#                      BoardID  DSPs    Chan/DSP
#----------------------------------------------------------------
.mcard_1:    0         30                          # 1.DigitalModem:ISA
.mcard_2:    1         30                          # 2.DigitalModem:ISA
.ccard_1:    100       12       4                  # 1.VIPER-12_548:ISA
.ccard_2:    101       12       4                  # 2.VIPER-12_548:ISA
.icard_1:    2         30                          # 1.Primary_____:PCI
.icard_2:    3         30                          # 2.Primary_____:PCI
#
.icard_cnt: 2          # Number of ISDN-Cards
.mcard_cnt: 2          # Number of Modem-Cards
.ccard_cnt: 2          # Number of Compression-Cards
#
.PORTS_ISDN:  60 # Number of ISDN-Ports
.PORTS_MODEM: 60 # Number of Modem-Ports
.PORTS_COMP:  60  # Number of Compression-Ports
.PORTS_PSTN:  60 # Number of analog ports (modem+voice)
```

A.8 RADIUS Dictionary

```
#
# Last Updated 96/7/9 for ComOS 3.3.2 and RADIUS 1.16
#
#           This file contains dictionary translations for parsing
#           requests and generating responses.  All transactions are
#           composed of Attribute/Value Pairs.  The value of each attribute
#           is specified as one of 4 data types.  Valid data types are:
#
#           string - 0-253 octets
#           ipaddr - 4 octets in network byte order
#           integer - 32 bit value in big endian order (high byte first)
#           date - 32 bit value in big endian order - seconds since
#                     00:00:00 GMT,  Jan.  1,  1970
#
#           Enumerated values are stored in the user file with dictionary
#           VALUE translations for easy administration.
#
#           Example:
#
#           ATTRIBUTE         VALUE
#           ---------------   -----
#           Framed-Protocol= PPP
#           7                = 1   (integer encoding)
#
#
#
# Obsolete names for backwards compatibility with older users files
#
ATTRIBUTE    Password           2       string
ATTRIBUTE    Client-Id          4       ipaddr
ATTRIBUTE    NAS-Port-Id        5       integer
ATTRIBUTE    Client-Port-Id     5       integer
ATTRIBUTE    User-Service-Type  6       integer
ATTRIBUTE    Framed-Address     8       ipaddr
ATTRIBUTE    Framed-Netmask     9       ipaddr
ATTRIBUTE    Framed-Filter-Id   11      string
ATTRIBUTE    Login-Host         14      ipaddr
ATTRIBUTE    Login-Port         16      integer
ATTRIBUTE    Old-Password       17      string
ATTRIBUTE    Port-Message       18      string
ATTRIBUTE    Dialback-No        19      string
ATTRIBUTE    Dialback-Name      20      string
ATTRIBUTE    Challenge-State    24      string

VALUE        Service-Type       Login-User           1
VALUE        Service-Type       Framed-User          2
VALUE        Service-Type       Dialback-Login-User  3
VALUE        Service-Type       Dialback-Framed-User 4
VALUE        Service-Type       Outbound-User        5
VALUE        Service-Type       Shell-User           6

VALUE        Framed-Routing     Broadcast            1
VALUE        Framed-Routing     Listen               2
VALUE        Framed-Routing     Broadcast-Listen3

VALUE        NAS-Port-Type      ISDN                 2
```

```
VALUE       NAS-Port-Type      ISDN-V120           3
VALUE       NAS-Port-Type      ISDN-V110           4

#
#           Configuration Values
#           uncomment to turn account expiration on
#

#VALUE      Server-Config      Password-Expiration  30
#VALUE      Server-Config      Password-Warning     5

ATTRIBUTE   User-Name          1       string
ATTRIBUTE   User-Password      2       string
ATTRIBUTE   CHAP-Password      3       string
ATTRIBUTE   NAS-IP-Address     4       ipaddr
ATTRIBUTE   NAS-Port           5       integer
ATTRIBUTE   Service-Type       6       integer
ATTRIBUTE   Framed-Protocol    7       integer
ATTRIBUTE   Framed-IP-Address  8       ipaddr
ATTRIBUTE   Framed-IP-Netmask  9       ipaddr
ATTRIBUTE   Framed-Routing     10      integer
ATTRIBUTE   Filter-Id          11      string
ATTRIBUTE   Framed-MTU         12      integer
ATTRIBUTE   Framed-Compression 13      integer
ATTRIBUTE   Login-IP-Host      14      ipaddr
ATTRIBUTE   Login-Service      15      integer
ATTRIBUTE   Login-TCP-Port     16      integer
ATTRIBUTE   Reply-Message      18      string
ATTRIBUTE   Callback-Number    19      string
ATTRIBUTE   Callback-Id        20      string
ATTRIBUTE   Expiration         21      date
ATTRIBUTE   Framed-Route       22      string
ATTRIBUTE   Framed-IPX-Network 23      ipaddr
ATTRIBUTE   State              24      string
ATTRIBUTE   Session-Timeout    27      integer
ATTRIBUTE   Idle-Timeout       28      integer
ATTRIBUTE   Termination-Action 29      integer
ATTRIBUTE   Called-Station-Id  30      string
ATTRIBUTE   Calling-Station-Id 31      string
ATTRIBUTE   NAS-Identifier     32      string
ATTRIBUTE   Proxy-State        33      string
ATTRIBUTE   Acct-Status-Type   40      integer
ATTRIBUTE   Acct-Delay-Time    41      integer
ATTRIBUTE   Acct-Input-Octets  42      integer
ATTRIBUTE   Acct-Output-Octets 43      integer
ATTRIBUTE   Acct-Session-Id    44      string
ATTRIBUTE   Acct-Authentic     45      integer
ATTRIBUTE   Acct-Session-Time  46      integer
ATTRIBUTE   Acct-Input-Packets 47      integer
ATTRIBUTE   Acct-Output-Packets48      integer
ATTRIBUTE   Acct-Terminate-Cause49     integer
ATTRIBUTE   Acct-Multi-Session-Id50    string
ATTRIBUTE   Acct-Link-Count    51      integer
ATTRIBUTE   CHAP-Challenge     60      string
ATTRIBUTE   NAS-Port-Type      61      integer
ATTRIBUTE   Port-Limit         62      integer

#           ITK specific Attributes
```

```
ATTRIBUTE    ITK-Auth-Serv-IP   100     ipaddr
ATTRIBUTE    ITK-Auth-Serv-Prot 101     integer
ATTRIBUTE    ITK-Provider-Id    102     integer
ATTRIBUTE    ITK-Usergroup      103     integer
ATTRIBUTE    ITK-Banner         104     string
ATTRIBUTE    ITK-Username-Prompt105     string
ATTRIBUTE    ITK-Password-Prompt106     string
ATTRIBUTE    ITK-Welcome-Message107     string
ATTRIBUTE    ITK-Prompt         108     string
ATTRIBUTE    ITK-IP-Pool        109     integer
ATTRIBUTE    ITK-Tunnel-IP      110     ipaddr
ATTRIBUTE    ITK-Tunnel-Prot    111     integer
ATTRIBUTE    ITK-Acct-Serv-IP   112     ipaddr
ATTRIBUTE    ITK-Acct-Serv-Prot 113     integer
ATTRIBUTE    ITK-Filter-Rule    114     string
ATTRIBUTE    ITK-Channel-Binding115     integer
ATTRIBUTE    ITK-Start-Delay    116     integer
ATTRIBUTE    ITK-NAS-Name       117     string
ATTRIBUTE    ITK-ISDN-Prot      118     integer
ATTRIBUTE    ITK-PPP-Auth-Type  119     integer
ATTRIBUTE    ITK-Dialout-Type   120     integer
ATTRIBUTE    ITK-Ftp-Auth-IP    121     ipaddr
ATTRIBUTE    ITK-Users-Default-Entry122     string
ATTRIBUTE    ITK-Users-Default-Pw 123     string
ATTRIBUTE    ITK-Auth-Req-Type       124     string
ATTRIBUTE    ITK-Modem-Pool-Id       125     integer
ATTRIBUTE    ITK-Modem-Init-String   126     string
ATTRIBUTE    ITK-Voip-Init-String    126     string
ATTRIBUTE    ITK-PPP-Client-Server-Mode 127integer
ATTRIBUTE    ITK-PPP-Compression-Prot   128  string
ATTRIBUTE    ITK-Username               129  string
ATTRIBUTE    ITK-Dest-No                130  string
ATTRIBUTE    ITK-DDI                    131  string

#            ITK specific Values

VALUE        ITK-Auth-Serv-Prot         None         0
VALUE        ITK-Auth-Serv-Prot         RADIUS       1
VALUE        ITK-Auth-Serv-Prot         PSP          2

VALUE        ITK-Acct-Serv-Prot         None         0
VALUE        ITK-Acct-Serv-Prot         RADIUS       1

VALUE        ITK-Channel-Binding     Normal          1
VALUE        ITK-Channel-Binding     Reserved2

VALUE        ITK-Tunnel-Prot    L2F                  1
VALUE        ITK-Tunnel-Prot    FR-DLCI              2
VALUE        ITK-Tunnel-Prot    ITK-EMAS             3

VALUE        ITK-ISDN-Prot      ITK-Auto-Detection   0
VALUE        ITK-ISDN-Prot      ITK-HDLC             1
VALUE        ITK-ISDN-Prot      ITK-X.75             2
VALUE        ITK-ISDN-Prot      ITK-X.25             3
VALUE        ITK-ISDN-Prot      ITK-V.110            4
VALUE        ITK-ISDN-Prot      ITK-V.120            5
VALUE        ITK-ISDN-Prot      ITK-Modem-Async      6
VALUE        ITK-ISDN-Prot      ITK-Modem-Sync       7
```

```
VALUE       ITK-Dialout-Type   ITK-Callback        1
VALUE       ITK-Dialout-Type   ITK-Callout         2
VALUE       ITK-Dialout-Type   ITK-Recall          3

VALUE       ITK-PPP-Auth-Type  ITK-Auth-Auto       1
VALUE       ITK-PPP-Auth-Type  ITK-Auth-CHAP       2
VALUE       ITK-PPP-Auth-Type  ITK-Auth-PAP        3
VALUE       ITK-PPP-Auth-Type  ITK-Auth-None       4

VALUE       ITK-PPP-Client-Server-ModeITK-Mode-Server0
VALUE       ITK-PPP-Client-Server-ModeITK-Mode-Client1


#
#           Integer Translations
#

#           User Types

VALUE       Service-Type       Login                1
VALUE       Service-Type       Framed               2
VALUE       Service-Type       Callback-Login       3
VALUE       Service-Type       Callback-Framed      4
VALUE       Service-Type       Outbound             5
VALUE       Service-Type       Administrative       6
VALUE       Service-Type       NAS-Prompt           7
VALUE       Service-Type       Authenticate-Only    8
VALUE       Service-Type       Callback-NAS-Prompt  9
VALUE       Service-Type       ITK-Voice-over-IP      101
VALUE       Service-Type       ITK-Voice-over-IP-Comp 101

#           Framed Protocols

VALUE       Framed-Protocol    PPP                  1
VALUE       Framed-Protocol    SLIP                 2
VALUE       Framed-Protocol    MP                   100

#           Framed Routing Values

VALUE       Framed-Routing     None                    0
VALUE       Framed-Routing     Send-routing-packets    1
VALUE       Framed-Routing     Listen-for-routing-packets 2
VALUE       Framed-Routing     Send-and-Listen          3

#           Framed Compression Types

VALUE       Framed-CompressionNone                 0
VALUE       Framed-CompressionVJ-TCP-IP            1
VALUE       Framed-CompressionVan-Jacobson-TCP-IP  1
# misspelled but kept for backwards compatibility
VALUE       Framed-CompressionVan-Jacobsen-TCP-IP  1

#           Login Services

VALUE       Login-Service      Telnet               0
VALUE       Login-Service      Rlogin               1
VALUE       Login-Service      TCP-Clear            2
VALUE       Login-Service      PortMaster           3
VALUE       Login-Service      LAT                  4
```

```
VALUE       Login-Service      ITK-UDP-Clear      100

#           NAS Port Types, available in 3.3.1 and later

VALUE       NAS-Port-Type      Async              0
VALUE       NAS-Port-Type      Sync               1
VALUE       NAS-Port-Type      ISDN-Sync          2
VALUE       NAS-Port-Type      ISDN-Async-V.120   3
VALUE       NAS-Port-Type      ISDN-Async-V.110   4
VALUE       NAS-Port-Type      Virtual            5
VALUE       NAS-Port-Type      ITK-Transparent     100


#           Status Types

VALUE       Acct-Status-TypeStart                 1
VALUE       Acct-Status-TypeStop                  2
VALUE       Acct-Status-TypeAccounting-On         7
VALUE       Acct-Status-TypeAccounting-Off        8

#           Authentication Types

VALUE       Acct-Authentic     None               0
VALUE       Acct-Authentic     RADIUS             1
VALUE       Acct-Authentic     Local              2
VALUE       Acct-Authentic     Remote             3

#           Termination Options

VALUE       Termination-ActionDefault             0
VALUE       Termination-ActionRADIUS-Request      1

#           Acct Terminate Causes, available in 3.3.2 and later

VALUE       Acct-Terminate-Cause    User-Request           1
VALUE       Acct-Terminate-Cause    Lost-Carrier           2
VALUE       Acct-Terminate-Cause    Lost-Service           3
VALUE       Acct-Terminate-Cause    Idle-Timeout           4
VALUE       Acct-Terminate-Cause    Session-Timeout        5
VALUE       Acct-Terminate-Cause    Admin-Reset            6
VALUE       Acct-Terminate-Cause    Admin-Reboot           7
VALUE       Acct-Terminate-Cause    Port-Error             8
VALUE       Acct-Terminate-Cause    NAS-Error              9
VALUE       Acct-Terminate-Cause    NAS-Request            10
VALUE       Acct-Terminate-Cause    NAS-Reboot             11
VALUE       Acct-Terminate-Cause    Port-Unneeded          12
VALUE       Acct-Terminate-Cause    Port-Preempted         13
VALUE       Acct-Terminate-Cause    Port-Suspended         14
VALUE       Acct-Terminate-Cause    Service-Unavailable    15
VALUE       Acct-Terminate-Cause    Callback               16
VALUE       Acct-Terminate-Cause    User-Error             17
VALUE       Acct-Terminate-Cause    Host-Request           18
```

B New Features of ITK NetBlazer 8500 V5.0

B.1 Voice over IP (VoIP, Internet-Telephony)

Internet telephony which is also called IP Telephony or Voice over IP is a new technology that allows, among standard data packets, to transmit multimedia information like voice or video over the Internet or any other IP-based LAN or WAN.

This technology is based on open standards and recommendations which are passed by international standardization institutions like IETF or ITU and which are met by almost any supplier of Internet Telephony products. These standards define the transmission of multimedia information within IP-based networks.

This way it becomes possible to use the same network for the transmission of telephony, which is already used for the transmission of e-mail, web pages and all other packet oriented data.

B.1.1 Notations and technical information

Caller (user A): The user that wants to establish a call and calls the dialin gateway.

Callee (user B): The user that should be called from the caller (remote user).

Voice gateway: The system that processes the voice call and converts the voice data to IP packets.

Dial-in gateway: The (local) system where the telephone call arrives and where the voice data leaves the switched network (PSTN/ISDN) and enters the IP network.

Dial-out gateway: The (remote) system where the voice data leaves the IP network and enters the switched network (PSTN/ISDN).

Account code: Type of username, which is used to authenticate the caller. Must be numerically entered by DTMF keys.

Interactive Voice Response (IVR): A voice based menu like input system where the caller is guided to the different inputs by playback of prerecorded voicefiles. The inputs for identification and remote phone number are got by DTMF detection.

DTMF detection: The process of detecting digits pressed on a telephone touchpad. Only possible with tone dialing (not possible with pulse dialing).

2-stage-dialing: The process for the caller to call the number of the Dialin gateway 1st and to enter the wanted remote phone number in a 2nd step (guided by IVR).

Least Cost Routing (LCR): The process of finding the „best" dial-out gateway for the wished remote phone number. „Best" normally means the gateway that is nearest to the remote phone number and which causes the least costs by establishing the connection from the dial-out gateway to the callee phone (over PSTN/ISDN).

Codec: Coder/Decoder (in soft- or hardware) that converts audio or video signals in digital data (or back).

Compression (G.729A, G.723): The process of compressing the voice data in order to reduce the amount of data to be transmitted over the IP network.
The following codecs are supported:

- G.729A reduces the traffic to 8 kbit/s.
- G.723 reduces the traffic to 5.3 or 6.3 kbit/s.

Both compression protocols are NOT TRANSPARENT for data or fax. Only voice is compressed and decompressed with acceptable quality. (Data and fax is not.)

- G.711 is the uncompressed protocol and needs a bandwidth of 56 or 64 kbit/s.

Latency (Delay): The amound of time a multimedia packet takes to get from the source to the destination. The time is needed to compress the voice, packetizing it into IP packets, transferring the IP packet over the Intranet/Internet and to decompress the packet (time to transfer voice from caller to callee (or back)). The latency must be minimized in order to maintain a certain level of interactivity and avoid unnatural pauses in conversation. For a good quality the delay should be below 250 ms.

Jitter: (interarrival jitter): Real-time multimedia packets must arrive in order and on time to be of any use to the receiver. Variations in packet arrival time (jitter) must be below a certain threshold to avoid dropped packets (and therefore gaps in the call). The NetBlazer 8500 software keeps track of this problem by using an intelligent automatically adapted dynamic jitter buffer.

Echo Cancellation: To disable the audible echo caused by the delay of packet an echo cancellation process is necessary. This process reduces the input signal on one end by the output signal of the same end. The echo cancellation must be done on both sides.

DSP board: To fulfill the compression and echo cancellation requirements special computing power is necessary. In the NetBlazer 8500 a special hardware equipment with DSP (digital signal processors) is used. These DSP boards are connected to the MVIP bus and contain multiple DSP's. Each DSP processes one or more voice channels.
See Chapter 8.2.4, *Voice compression board* (page 8-6) for information about voice compression boards.

H.323 is an "umbrella recommendation" of the ITU which defines the multimedia communication in LANs that do not provide a guaranteed quality of service.
H.323 protocol uses TCP connections for the signaling protocol (H.245), for data transmission (T.120) and for connection control (Q.931).
H.323 uses RTP (Realtime Transport Protocol) for transmission of audio and video data, which is based on UDP (unprotected). Using intermediate buffers, time stamps and sequence numbers, RTP enables the receiving station to detect missing packets, double packets or packets which have been received in wrong order, and to correct the receiving flow in a suitable way.

Gatekeeper is a system in the H.323 network that is responsible for address translation (E.165 <=> IP address) and control of all network resources.

RAS: Registration, Admission, Status is the protocol in H.323 that defines the communication with the gatekeeper.

B.1.2 Voice over IP with H.323

The H.323 protocol is needed to establish voice connections from PC to PC, PC to phone, phone to PC and phone to phone when different gateways are involved. It allows the interoperability of systems from different vendors. The NetBlazer implementation in V5.00 is H.323V1 with some V2 enhancements.

The NetBlazer specific connection setup protocol SPC, that was introduced in V4.00, is still supported. Both protocols (SPC and H.323) can be selected dynamically on connection setup.

A H.323 daemon (h323d) is used to realize call establishment by the ITU standard H.323 for Voice over IP.

The h323d is started and controlled by PRACTRL. If h323d uses a gatekeeper (see parameters below) it registeres itself at the gatekeeper.

In the process table of PRAMON/webMan you can see the IP address of this gatekeeper (GK) or 'No GK' if no gatekeeper is used. Furthermore the number of sessions is shown (#s).

Example:

“No GK - #s: 2”	->Not using a gatekeeper, two active H.323 sessions.
“GK 123.45.67.89 #s: 0”	->Using a gatekeeper 123.45.67.89, no active H.323 session.
“GK 0.0.0.0 #s: 0”	->Using a gatekeeper, but actual unregistered (e.g. gatekeeper is down), no active H.323 session

The parameters for the h323d are configured in h323.par.

Gatekeeper parameters

To enable/disable the usage of a gatekeeper the parameter 'h323d.use_gatekeeper' must be configured (no=0/yes=1):

Example:

```
h323d.use_gatekeeper: 0  # NOT using a gatekeeper
or
h323d.use_gatekeeper: 1  # Using a gatekeeper
```

Other values than 0 or 1 are not allowed. If the parameter 'h323d.use_gatekeeper' is 1 (using a gatekeeper) the parameter 'h323d.ip_addr_gatekeeper' must be configured. If you leave this parameter blank the h323d will try to find a gatekeeper by doing a RAS request broadcast. Alternatively you can configure the IP address of a known gatekeeper. In this case the h323d is trying to register itself at this gatekeeper by a RAS request.

Example:

```
h323d.ip_addr_gatekeeper:              # Try to find a gatekeeper by broadcast
or
h323d.ip_addr_gatekeeper: 123.45.67.89 # IP address of gatekeeper
```

Country code substitution

This parameter is used to support an international dial number layout used by other vendors (e.g. Cisco). You can specify a country code and the substitution digits for your system. If the country code digits are found in the calling number they are exchanged by the substitution specified.

If you do NOT want to use country code substitution the parameters can be left blank!

Example:

```
parameter setting:
h323d.CountryCodeSubtitution:  +49;0  # country code '+49' is substituted
                                        by '0'
```

1) If the h323d gets the calling number +4923197470:
The check of the prefix leads to the result 'it is an international call'. The prefix '+49' is cut off and the number '**0**23197470' is called.

2) If the h323d gets the calling number 023197470:
The check of the prefix leads to the result 'it NOT is an international call'. The number is unchanged.

Prefix parameters

These parameters may be used if a gatekeeper needs to reference different gateways by calling number prefix. The gatekeeper forwards the calling number according this prefix. Thus the prefix must be cut off by the h323d. If the h323d gets a calling number, it will be checked if one of the configured prefixes is used. This prefix will be cut off and the calling number without prefix is used to establish the call. For external calls the 'PBXExternCallPrefix' is called first.

If you do NOT want to use prefixes the parameters can be left blank!

Example:

Assuming the following parameter settings:
h323d.PBXExternCallPrefix: 0 # Prefix for external calls using a PBX
h323d.AudioOnlyCallInternPrefix: 92 # Prefix for internal audio calls
h323d.AudioOnlyCallExternPrefix: 93# Prefix for external audio calls

1) If the h323d gets the calling number 92123:
The check of the prefixes leads to the result 'it is an internal call'. The prefix is cut off and the number '123' is called.

2) If the h323d gets the calling number 93567890:
The check of the prefixes leads to the result 'it is an external call'. The prefix is cut off, the 'PBXExternCallPrefix' is called first and then the calling number is added. Thus '0-567890' is called in our example.

3) If the h323d gets the calling number 94789:
The call will be rejected because no matching prefix is found (normally the gatekeeper would not forward this call to the h323d).

Call handling parameters

The h323d supports two different ways of connection establishment. The behavior is selected by the following parameters:

1) h323d.use_early_h245_tsap: (no=0/yes=1) (default: 1)
Offer own H.245 IP address and port in the first SETUP message to open H.245 channel with first round trip.

2) h323d.wait_for_remote_connect: (no=0/yes=1) (default: 0)
Wait for CONNECT message from remote phone before opening H.245

channel.
(parameter only supported after V5.00b2)

NOTE: For support of the Ericsson gatekeeper the parameters should be set to:

h323d.use_early_h245_tsap: 0
h323d.wait_for_remote_connect: 1
and you have to change the '.type_of_codec' parameter in the 'voip.par':

.type_of_codec: G711:G723 #do NOT use G.729 with Ericsson gatekeeper

Logging interface

The h323d is using an special logging interface. It is possible to configure several logging levels and component masks. The following logging interface level are relevant to the h323d:

Error	0
Warning	1
Info	2
Commands (internal)	3
LAN messages	6
All details	8
Periodic events	19

The default logging interface level may be for example 10. That means all logging messages of level 0 to 10 are shown but not the periodic events (timer check, e.g.).

The following logging interface component masks are relevant to the h323d:

Log no components/modules	0x00000000
ASN	0x00000004
H.245	0x00000010
H.323	0x00000080
Q.931	0x00000100
Miscellaneous	0x00000200
Protocol handler	0x00000400
Main module	0x00000800
SPC wrapper	0x00001000
Log all components	0xffffffff

It is possible to set the logging interface component mask bit for bit and combinations are possible.

The default logging interface component mask may be e.g. 0xffffffff. That means all logging messages of all components are shown.

Note that the logging interface levels and component masks have only influence on the modules in the h323d using the interface, for example if message logging is on but the interface level is 0 there will be still appearing messages (from SPC, e.g.). The logging interface levels are different from the data logging levels!

If you use the dynamic enable/disable logging feature of the PRAMON you can switch message and/or data logging for h323d on or off. That means using of the logging interface is also switched on or off.

Note that the configured parameters for the logging interface are still valid. If you dynamically switch message logging on but the logging interface level is 0, you get only error messages or messages which do not use the interface (e.g. SPC).

Supported H.323 Clients

The following H.323 clients have been successfully tested with NetBlazer V5.00:

- Microsoft NetMeeting V2.0 / V2.1
- Intel ProShare V3.0 and Internet Video Phone 2.1 / 2.2
- Netspeak Webphone 4.0 / 4.01

- Vocaltec Internet Phone 5.0
- Netscape Conference 4.0
- VoxWare VoxPhone 3.0

Further Parameters for H.323

The parameter ".spc_h323_setup" controls, which connection setup protocol should generally be used:

- 0 use SPC
- 1 use H.323

B.1.3 Transparent Connection Setup

Voice dialog

The voice dialog defines how a user authenticates and enteres his destination phone number. The previous versions only supported Interactive Voice Response (IVR). V5.0 additionally supports One Stage dialing (OSD).

Interactive Voice Response (IVR)

IVR is a 2-stage-dialing process: In the first step the user dials the number of the voice gateway and hears the welcome voice messages. In the second step the user enters his PIN and the destination number by DTMF digits. This voice dialog type is still useable in V5.0 and has been enhanced with the following features:

- **WAV files**: All voice files are standard WAV files, that can be recorded or changed on a standard PC and activated on the NetBlazer by copying the files in the right directory (see Chapter 7.7.2, *Voice files for IVR* (page 7-66)).
- **Dynamic Dialing**: Additionally to the block dialing in V4.0 dynamic dialing is useable, where the termination of the destination number is not necessary. (see below)
- **Remote tone signalling**: During connection setup the dial tones that are generated at the dialout gateway are hearable from the caller at the dialin gateway. (see below)

To enable IVR the Radius attribute “ITK-Banner” must be set to one of the following values:

- “IVR” to enable IVR with block dialing (same as “VGI” in V4.0)
- “IVR_DYNDIAL” to enable IVR with dynamic dialing

The other Radius attributes to define the language, voice files, etc. remain unchanged.

One stage dialing (OSD)

One stage dialing allows the dialing of the destination number immediate after the access number of the voice gateway. There is no separator or pause necessary between the access number and the destination number. The digits are detected from the switch and received through the d channel (no DTMF digits necessary). The incoming call is not accepted until the callee has answered the call.

No PIN is entered in One Stage Dialing. So the authentication must be done by the calling line ID of the caller, or by doing no authentication at all.

To enable OSD the Radius attribute “ITK-Banner” must be set to one of the following values:

- “OSD” to enable OSD with block dialing
- “OSD_DYNDIAL” to enable OSD with dynamic dialing

Get Destination number

Block dialing

Block dialing describes the process where the NetBlazer collects all digits of the destination number, without knowing when it is complete. So a termination (by ‘#’ key or timeout) is necessary.

As soon as the destination number is complete the NetBlazer establishes the connection.

Dynamic dialing (overlapped sending)

Dynamic dialing (also called overlapped sending) allows the transmission of dial digits during the dialing phase (one digit after the other). As soon as the remote switch signals the completion of the destination number the caller is signaled the calling signal.

No termination of the destination number is necessary.

If the connection setup is done by H.323 the remote gateway (or gatekeeper) must support H.323V2, because the overlapped sended digits, are sent by H.323V2.

To achieve the support of Dynamic dialing the D-channel Setup (dial-out) is done without any destination number. The destination number is transmitted to the PABX one after the other afterwards. This empty Setup may be rejected by some PABX (D-Channel Disconnect cause: „Information element is missing“).

Setting the parameter *voip_empty_setup: 0* fixes the problem, but **disables** Dynamic dialing at the same time.

Remote Tone signaling

Remote tone signaling is used to hear remote status tones and announcements. The data path is switched starting with the connection setup (not after connection establishment).

Features

The following table describes all possible features in the several VoIP dialoges:

Feature \ VoIP-Dialog	IVR	IVR_DYNDIAL	OSD	OSD_DYNDIAL
Block dialing (termination necessary)	x		x	
Dynamic dialing (no Termination)		x		x
Authentication by PIN (entered as DTMF)	x	x		
Get destination number digits by DTMF	x	x		
Get destination number by DDI (d channel)			x	x

Feature \ VoIP-Dialog	IVR	IVR_DYNDIAL	OSD	OSD_DYNDIAL
Interpretation '*' and '#' digits	x		x	
Additional calls after first	x			
Callback	x	x		
Remote tone signalling	x	x	x	x
Playback of voice files	x	x		
Accept call before connection established	x	x		

All other features are possible with all VoIP dialoges.

B.1.4 Address Translation

The address translation is necessary for two reasons:

1. Find the IP address of the dialout gateway that should be used for the entered destination number
2. Modify the destination number so that it can be used to establish a connection at the dialout gateway

The NetBlazer V5.0 supports two methods to do the address translation:

1. Use Least Cost Routing (LCR) requests to a Radius server (proprietary, same as in V4.0, useable for SPC and H.323 connection setup)
2. Use RAS (Registration Admission Status) requests to a Gatekeeper (H.323 compliant, only useable with H.323 connection setup)

Both address translation methods can be combined. If a LCR Radius server as well as a Gatekeeper is configured the following cases are possible:

(dial-no defines the number the user dialed,

called-no defines the number that should be used to establish the call (result of the address translation))

- Radius LCR knows the dial-no and though responds with a called-no: No RAS request will be done. The called-no from the Radius LCR response will be used to establish the connection.
- Radius LCR does not know the dial-no and though responds no called-no: A RAS request will be done. The called-no from the Gatekeeper will be used to establish the connection.
- No Radius LCR defined (service table empty or LCR dynamically disabled): A RAS request will be done. The called-no from the Gatekeeper will be used to establish the connection.

The LCR request can be disabled dynamically per call with the setting of the “ITK-Voip-Init-String” (see below).

With dynamic dialing the dialout gateway must be found dynamically. With every digit of the dial-no the LCR is asked if he knows the corresponding dialout gateway. As soon as a positive response has been received the connection is established, no further LCR requests are done and all further digits of the dial-no are transferred directly to the dialout gateway.

To minimize the LCR requests a minimal amount of digits is collected before the first LCR request is done, which can be configured with the parameter “.voip_lcr_min_digits” (Default: 3).

The same behaviour is used for address translation by RAS instead of LCR.

B.1.5 Connection Setup

SPC or H.323

The parameter “.spc_h323_setup” controls, which connection setup protocol should generally be used:

- 0 use SPC
- 1 use H.323

The connection setup protocol can be defined dynamically per call with the setting of the “ITK-Voip-Init-String” (see below).

Warning: Because of a lot of new features the SPC protocol has been enhanced so that there is no interoperability with NetBlazer 8500 V4.00

Automatic connection setup

A voice connection can automatically be established with the offline authentication by returning dest-no in the Radius response.

The following example establishes automatically a connection to a defined dest-no when the DDI ‘81’ is dialed. An address translation will be done:

```
%_81        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="OSD",
            ITK-Dest-No = "023197470",
            ITK-Username="ITK"
```

The following example establishes automatically a connection to a defined H.323 client when the DDI ‘82’ is dialed. An address translation is not done. The dummy dest-no is needed to force a connection setup to the defined IP address:

```
%_82        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="OSD",
            ITK-Dest-No = "xxx",
            ITK-Username="voip-test",
            ITK-Tunnel-IP = a.b.c.d,
            ITK-Voip-Init-String="H1"
```

B.1.6 Codecs

V5.0 supports the following codecs:

- G.729A same as in V4.0, compression ratio 8:1
- G.723.1 compresion ratio 10:1
- G.711 uncompressed, a-law and u-law supported

The codec to use is automatically negotiated between the dialin and the dialout gateway. The codecs supported by the NetBlazer can be configured with the parameter .type_of_codec (Default: G711:G723:G729)

The codec to use can be forced dynamically per call with the setting of the “ITK-Voip-Init-String” (see below).

The framesize can be configured to 30 or 60 ms with parameter ".frame_size". (Default: 60 ms)

The following table shows the different codecs, framesizes and packet sizes supported by V5.0:

Codec	Ratio	Framesize [ms]	Payload [bytes]	IP header [bytes]	IP packet size [bytes]	IP packets per sec	IP Bytes per sec [bytes]
G.729A	8:1	30	30	40	70	33,33	2334
G.729A	8:1	60	60	40	100	16,67	1667
G.723.1	10:1	30	24	40	64	33,33	2134
G723.1	10:1	60	48	40	88	16,67	1467
G.711	1:1	30	240	40	280	33,33	9333
G.711	1:1	60	480	40	520	16,67	8669

B.1.7 Coding / Transcoding

The NetBlazer supports the coding a-law (used in Europe) as well as µ-law (used in USA). Each DSP card must be configured to the right coding (depending on the switch) by setting the parameter ".pcm_companding".

Possible values:

1=µ-law
2=a-law (Default)

Transcoding: If the two communication gateways have different codings (i.e. one is located in Europe and one in the US) the different codings are converted/transcoded from the NetBlazer. This is only necessary for G.711, the other codecs automatically adapt the coding.

B.1.8 DTMF Relay

If DTMF relay is enabled the dialin gateway detects if DTMF keys are pressed and sends these digits to the dialout gateway, where they are processed (i.e. new DTMF tones generated). Thie mechanism is an outband transfer of recognized DTMF digits as specified in H.323V2. The DTMF keys are transferred by SPC or as H.245 User Input Indications to be H.323V2 compliant.

This feature is disabled by default but can be enabled dynamically per call with the setting of the “ITK-Voip-Init-String” (see below).

B.1.9 Voice files for IVR

In previous version voice files in a special proprietary format were used for IVR (Interactive Voice Processing). Starting with V5.0 standard PC WAV files are used. These files can be recorded or changed with the NetBlazer or on a standard PC. After copying them into the directory “/u/pra/voi” (i.e. by FTP) they are used from by NetBlazer.

Of course WAV files can be recorded with the NetBlazer with the same mechanism as in previous versions (by setting ITK-Banner to „RECORD“).

The used WAV files must conform to the following format (PCM 8.000 Hz; 16 Bit; Mono):

- Channels: Mono
- Resolution: 16 bit
- sample rate: 8000 Hz

The voice files used by the NetBlazer are located in the directory “/u/pra/voi”. The sample voice files contained in the NetBlazer kit are located in the directory “/u/pra/voi/samples”. During the installation the sample voice files are automatically copied into the working directory (but not overwritten if existant).

B.1.10 Selecting Dialout Line

Only lines with an active D channel and that are not disabled (status “up-on”) are selected for outgoing calls.

By default all available lines (physical interface, controllers) are investigated and the line with the highest number of free ports is used for an outgoing call.

This behaviour can be changed by manually selecting a special line (Provider selection). Each physical interface (primary rate, basic rate) is managed by a so called controller. If the dialout number is preceeded by a controller number and a pipe ('|') sign then the according physical interface is used for dialout. This modified dialout number may be retrieved from a least cost routing request (or from a gatekeeper).

Example:

192.168.100.31 is a gateway located in Dortmund/Germany. This gateway is connected to a city carrier via controller 2 and to a backup distance carrier via controller 3.

The least cost routing entry in the RADIUS users file may look like this:

```
%0231*      User-Password="LCR"
            ITK-Tunnel-IP = 192.168.100.31,
            ITK-Dest-No = "-4+2|"
            ITK-Tunnel-IP = 192.168.100.31,
            ITK-Dest-No = "-4+3|"
```

The RADIUS server strips the first four digits of the dialed number and adds the leading string "2|" respectively "3|": e.g. 0231987654 -> 2|987654; 3|987654. The dialout gateway first uses controller 2 (city carrier) for the dialout with number "987654". If this fails (all lines busy) then controller 3 (backup carrier) is used for the dialout with number "987654".

B.1.11 CLIP

The Calling Line Identification (CLI) of the phone dialing into the NetBlazer 8500 (caller) is forwarded to the dialout gateway or H.323 client during the VoIP call setup. The dialout gateway presents the CLI at the remote phone (callee), and a H.323 client shows the CLI within its user dialog.

The CLI is transfered unchanged between the dialin gateway and the remote site. No adaptions of the phone number on the incoming or outgoing site (dependent on the phone number of the line) are done.

CLIP is disabled by default and can be enabled by setting the parameter ".capi20_clip" to 1.

B.1.12 Connection control

For detection of aborted connection the following mechanism is used:

If no voice data (RTP packets) are received during a specified amount of time (parameter ".voip_idle_tmo", default: 300 seconds) the session is disconnected.

B.1.13 Additional Parameters & Attributes for VoIP

The Radius attribute "ITK-Voip-Init-String" can be used to configure special attributes for a voice connection. The following values are supported and can be combined to an initialization string (as AT like modem init strings):

H: Select connection setup protocol:
H1=H.323, H0=SPC

A: Select address translation protocol:
A1=RAS (Gatekeeper), A0=LCR (Radius)

D: Enable/disable DTMF Relay:
D1=enable, D0=disable

C: Select/force special codec:
C1=G.711, C2=G.723.1, C3=G.729A

The following Radius example shows the activation of a voice connection with H.323 connection setup and DTMF relay when the DDI "83" is dialed:

```
%_83        User-Password = "DIRECT_DIAL"
            Service-Type = ITK-Voice-over-IP-Comp,
            ITK-Banner="OSD",
            ITK-Voip-Init-String="H1D1"
```

Setting Type of Service (TOS)

To configure a NetBlazer 8500 for VoIP the following parameter can be adapted in "voip.par":

- Configuration IP TOS (type of service) field — voip_ip_tos (description below)

The IP TOS (Type Of Service) field is part of the IP packet. Some routers use the IP TOS field for a precedence selection. IP packets with a matching type of service field are preferred delivered. To achieve the best transmission results this value can be adapted to the routers precedence selection.

The TOS field is defined in RFC 791:

Bit 0: 0x01 Reserved
Bit 1: 0x02 Low Monetary costs
Bit 2: 0x04 High Reliability
Bit 3: 0x08 High Throughput
Bit 4: 0x10 Low Delay
Bit 5-7:Precedence value

These flags are or'ed to build the resulting TOS value:

Example:

If the ip packets should be transmitted with low delay and high reliability then the parameter
voip_ip_tos must be set to the value 0x14
Default value: 0x10

B.2 License Keys

With V5.00 a license schema is introduced, where all major features must be activated with valid license keys. The following features are limited to a valid license key:

- RAS: Remote access (ISDN and modem)
- VOICE: Voice over IP
- ISS: Internet Supplementary Services (for Siemens EWSD)

A RAS only system needs only a license key for RAS operations, a VOICE only system only a key for VOICE operations. A System that supports RAS and VOICE needs two license keys.

All licenses contain the following informations:

- Product ID and feature(NetBlazer 8500 with RAS / VoIP / ISS)
- Version (a key of V50 is useable for all versions V5.x)

- number of ports
- termination date (for evaluation)

Before starting the software the license keys must be entered in parameterfile “misc.par” (parameter “.LICENSE_KEY_xxx”).

The active licenses are shown in pramon and webMan in the hardware information list.

The following example shows a unlimited RAS license for 30 ports and a limited (evaluation) VOICE license for 24 ports. Both license can be used for NetBlazer software versions V5.x:

```
RAS     V50     Ports: 30     ExpireDate: key is unlimited
VOICE   V50     Ports: 24     ExpireDate: 1998 12 30
```

B.3 New communication boards

B.3.1 DSP Viper C548

The new supported Viper C548 board contains DSP’s with 80 Mips (C542 DSP’s have 40 Mips). 4 DSP boards are supported in one NetBlazer system.

Mixed configurations: C548 and C542 boards can be mixed in one system, but C542 boards must be configured **before** C548 boards (related to I/O ports, see hardware checklist).

The new C548 DSP board must be configured with the card_config tool. Fully configured boards (12 DSP) as well as partly configured boards (4, 6 or 8 DSP’s) are supported

The G.723.1 codec needs more processing power than G.729A, so less G.723.1 voice channels per DSP are possible than for G.729A. If the DSP resources are insufficient to support all voice channels the voice quality may diminish. If many G.723.1 connections will be used the DSP boards should be configured for less voice channels per DSP (in cards.par).

The following table shows the number of supported channels per DSP:

DSP type	number of G.729A channels [per DSP / per board]	number of G.723.1 channels [per DSP / per board]
C542	2 / 24	1 / 12
C548	4 / 48	3 / 36

B.3.2 DigitalModem II

The new DigitalModem II board is a low power variant of the already supported DigitalModem I board. The low power board has the same features and the same hardware and software interfaces as it's predecessor.

With the new DigitalModem II board up to 4 boards are supported in one system.

The DigitalModem boards must be configured with the card_config tool. Fully configured boards (30 modem ports) as well as partly configured boards (6, 12, 18 or 24 modem ports) are supported

B.4 V.90

The new Portware (firmware for DigitalModem boards) supports the new V.90 protocol (56 kbit/s).

By default V.90 is enabled. To disable V.90 and support only V.34+ (33,6 kbit/s) or slower connections the following parameter must be set:

.capi_modem_initstring: ATS29=0

B.5 PRAMON Enhancements

B.5.1 card table

If pramon is started with argument '-k' the card-table is shown and pramon exits.

Example:

pramon -k

```
Ctr Type                Stat. MVIP      Ports  Active cnt last-ixload
-------------------------------------------------------------------------------
2 ITK Primary           up-on Master    30     0:00:08   2   11:19:40
0 ITK DigitalModem      up Slave        24     0:00:08   2   11:19:31
1 ITK MultiModem        up Slave        8      0:00:08   2   11:19:20
100 Viper Compression   up Slave        24     0:00:07   2   11:19:11
```

B.5.2 Show licenses

The active licenses are shown in the hardware information view.

B.5.3 Show modem pool id

The modem pool id is shown in the modem service table.

B.6 webMan Enhancements

B.6.1 Refresh

It is possible to adjust page-refresh of Connection-table, Controller-table, Process-table and LED-table. Also page-refresh while viewing files (if refresh is off the complete file is shown, if refresh is on the last lines of file are shown).

In each frame that supports refresh 5 buttons are shown at the upper right that enable/disable the refresh at different times:

- 10s Enable refresh every 10 seconds
- 30s Enable refresh every 30 seconds
- 60s Enable refresh every 60 seconds
- stop Stop refresh
- default Set refresh to default

The following new parameters (process.par) can be configured:

```
www_suprimon.www_refresh: 0      # time for refreshing page in seconds
```

```
                                        ( 0 = refresh off )
www_suprimon.www_reflines: 15     # count of lines shown at the end
                                    of file, if refresh is on.
```

B.6.2 Show licenses

The active licenses are shown in the hardware information frame.

B.6.3 Security enhancements

For extended security in file “access” with password (“.sysaccess”, “.groupaccess”) the access may be restricted additionally by IP address (net, host or both). See “dotgroupaccess” for details.

B.6.4 Show other systemfiles

Other system files can be viewed (with or without refresh) by entering a link to them in the log directory (“/u/pra/log”).

Example:

After creating the following link the syslog file (system messages) can be viewed in the webMan logging frame:

```
cd /u/pra/log
ln -s /usr/adm/syslog syslog
```

Remark: NetBlazers can be configured to sent their system messages to the syslog daemon of another system (or the same) by setting the parameter “practrl.info_syslog_target” to the IP address of the syslog system. So all NetBlazer system messages can be concentrated and viewed on one system.

B.7 Accounting-Enhancements

For each VoIP connection there are two accounting entries: 1 on the dialin gateway and 1 for each dialout connection on the dialout gateway.

The accounting file has been enhanced to show the following new fields for VoIP connections:

- **VoIP-Con-Setup** Connection setup protocol used (SPC, H.323)

- **VoIP-Dialog-Type** Type of VoIP dialog (IVR, OSD, with/without DYNDIAL)

B.8 PRACTRL Enhancements

- Support for loading and controlling the new communication boards
- The H323 daemon (h323d) is started/stopped and controlled
- The ISS daemon (issd) is started/stopped and controlled, if configured

B.9 RADIUS Enhancements (Authentication & Accounting)

B.9.1 Separating Authentication into offline and online (auth.par)

In previous versions the offline and online authentication steps were done with the same Radius servers, defined in the authentication service table. From this version this two steps are split and two separate Radius servers can be configured (in two service tables). The parameters stab_auth_cnt and stab_auth_addr_x are no longer used. Instead the parameter stab_auth_cnt is split into stab_offline_cnt and stab_online_cnt and the parameters stab_auth_addr_x (x = [1, Number of IP Addresses]) are splitting into stab_offline_addr_x and stab_online_addr_x.

That means the parameters must be set separate for offline and online authentication.

Example:

```
# Service-Table-Entry for Authentication-Server (Offline):
.stab_offline_cnt:    1                  # No. of Authentication-Servers
.stab_offline_addr_1: $(RADIUS_SERVER)   # IP-Address of 1st
                                           Authent.-Server

# Service-Table-Entry for Authentication-Server (Online):
.stab_online_cnt:     1                  # No. of Authentication-Servers
.stab_online_addr_1:  $(RADIUS_SERVER)   # IP-Address of 1st
                                           Authent.-Server
```

Further it is possible to set for all Radius steps (ADNS, OFFLINE, ONLINE, LCR, ACCT) the RADIUS destination port and shared secret.

The default values are based on the following parameter macros:

for offline and online Radius server:
$(RADIUS_SERVER) default: localhost
for all Radius secrets:
$(RADIUS_SECRET) default: test
for Radius UDP ports:
$(RADIUS_ACCESS_PORT) default: 1645

B.9.2 Shell login

The shell login doesn't request a password if the password prompt is an empty string. (Configured in auth.par or by RADIUS). In this case an empty password (null) string is used for authentication.

B.10 Miscellaneous

B.10.1 Setting routes for UIP addresses

The NetBlazer 8500 is able to set and delete the routing entries for static UIP addresses automatically. This functionality must be enabled by setting the following parameter (e.g. in misc.par):

```
.set_static_routes: 1
```

B.10.2 Unknown IP protocols in packetfilter (firewall)

A new parameter determines if unknown IP protocols are discarded (default) or are handled like ICMP packets and may pass the firewall.

Normally all IP packets with a protocol value unequal to ICMP, UDP or TCP are always discarded. If the parameter ".fw_unknown_prot" is set to "PASS" these IP packets may pass the firewall according to the ICMP filter rules.

Examples:

```
.fw_unknown_prot: REJECT    # Always reject unknown IP protocols

.fw_unknown_prot: PASS      # Unknown IP protocols may pass the
```

```
# firewall according to the filter rules
```

B.10.3 D channel deactivation

A special downloadfile for the Primary/PCI boards “ixdummy.bin” can be used to deactivate the d channel.

B.11 ISDN Programming Interface (CAPI)

The internal ISDN interface has changed from CAPI1.1 to CAPI2.0. These changes shouldn't affect the behavior of the NetBlazer software at all. There are just new (different) disconnect causes according to the Euro-ISDN (DSS1 Euro-ISDN/NET3/ETSI) specification. Not to mention, that the message logging differs from previous NetBlazer 8500 versions (especially the call establishment).

B.12 Internet Supplementary Services (ISS)

The Internet Supplementary Services (ISS) are used to enable the following features to subscribers of a switch that supports the ISS requirements (i.e. SIEMENS EWSD).

- **ISCI: Subscriber Control via Internet**

  ISCI allows a subscriber to control the services assigned to his telephone by using the web browser. This is provided via a graphical PC based user interface for telephone feature management. It uses IP to set parameters for subscriber related EWSD features and to retrieve various journal as well as accounting and billing information.

- **EWI: E-Mail Waiting Indication**

  EWI informs a user immediately that an Internet mail message has been received – even if there is currently no active Internet session. This indication is brought to the subscriber’s telephone, either by a specific dial tone, by an announcement or by display information as appropriate and supported by the respective terminal equipment.

- **CWIB: Call Waiting Internet Busy**

CWIB informs the subscriber during an active Internet session that an incoming call is waiting. This event is visualized to the user by an additional window opening on his screen and the user is asked to either accept or refuse the call. If the user decides to accept the incoming call the Internet session is cleared and the call is switched to the telephone.

- **CCIB: Call Completion Internet Busy**

  The feature 'Call Completion on Internet Busy' allows a subscriber who is currently engaged in an internet session to receive a voice phone call on his PC using voice-over-IP technology. The internet session is not terminated. Voice call and internet traffic can simultanously be handled on one analoge line, or on the original used ISDN B-channel(s) respectively.

- **IAVoIP: Improved Access to Voice over IP**

  The feature allows a subscriber using his normal phone (POTS/ISDN) to place a call (typically long distance call) to another normal phone (POTS/ISDN) using the internet as transmission medium between both PSTN (accessed A- and B- phone). The A subscriber has to add an access code in front of the usual E.164 number of the B subscriber. The call is initiated by one-stage-dialling. There is no interactive dialogue to any voice responding system in the system.

The ITK NetBlazer 8500 is connected to the EWSD by PRI circuit(s). The D-channel is used to carry the Internet specific communication between EWSD and NetBlazer 8500. This is accomplished by enhancing the D-channel protocol implementation and RAS functionality.

Briefly, the functionality to be provided by NetBlazer 8500 is as follows:

- Provide a local IP address for a D-channel on request by EWSD (RARP request and response)
- Issue RADIUS requests to EWSD and process the RADIUS response for authentication and accounting
- Provide EWSD with the dynamic IP address for a subscriber after successful login
- Accept IP messages encapsulated in D-channel messages – issued by EWSD - and forward to router entity

- Accept IP messages issued by router entity, encapsulate into D-channel messages and forward to EWSD
- Establish H.323 voice connection to remote gateways

Internally a new daemon (the ISS daemon ISSD) coordinates the ISS communication. All data that is sent/received to/from EWSD goes through this module that is running only when the ISS functionality is needed. The ISS daemon provides all the features to implement the requirements described above.

For each D-channel (ISDN-card) a leased line process (LLP) is started that works like a line driver between EWSD and the ISSD (for one d-channel link only). After the LLP processes have registered at the ISSD data can be exchanged between EWSD and the NetBlazer 8500.

The new daemon ISSD and the leased line processes are automatically started and controlled by the PRACTRL process. The process state can be seen in the process table (in PRAMON or webMan).

The ISSD show the following process information:

Reg LLP <N>/<M>
<N> is the number of LLP that have been registered at the ISSD (number of usable PRI links).
<M> is the max. number of possible PRI links.

The LLP processes show the following process informations:

ISS C:<C> registering during registering at ISSD
ISS C:<C> registered after registering at ISSD
ISS C:<C> <a.b.c.d> after RARP-Response has been sent to EWSD
<C> is the number of the ISDN PRI board (controller).
<a.b.c.d> is the IP address used for the PRI link.

To enable the ISS features the following parameters must be set:

Parameterfile “iss.par” (new):

.start_iss: 1 # 1: start ISS-Daemon, 0: do not start ISS-

```
                                        Daemon
.iss_uip_pool:          100     # IP-Pool-ID for ISS IP addresses of EWSD
# Parameters for ISS leased lines processes (LLP):
.linecnt_isdn_ll:       2       # Number of leased lines (PRI links to EWSD)
isdn_ll_1.service:      ISS     # Service of 1st leased line
isdn_ll_1.controller:   1       # Controller for 1st leased line
isdn_ll_2.service:      ISS     # Service of 2nd leased line
isdn_ll_2.controller:   2       # Controller for 2nd leased line
```

Parameterfile "auth.par" (Authentication & Accounting):

```
To enable the RADIUS server in EWSD for online authentication:
.radius_online_port:        1812        # UDP port number
.radius_online_keyword:     [xxx]       # Shared secret to access RADIUS
                                          server
.stab_online_cnt:           1           # No. of Authentication-Servers
.stab_online_addr_1:        localhost   # IP-Address of 1st Authent.-Server

To enable the RADIUS server in EWSD for accounting:
.radius_account_port:                   1813# UDP port number
.radius_account_keyword:                [xxx]# Shared secret to access
RADIUS server
.stab_acct_cnt:         1           # No. of Accounting-Servers
.stab_acct_addr_1:      localhost   # IP-Address of 1st Accounting-Server
```

Parameterfile "uip_pool.par" (User IP address pools):

```
To define IP addresses for the ISS links:
.ip_pool_[X]:       a.b.c.d  [netmask]  100   # IP-address pool for ISS links
```

For offline authentication (service selection) the RADIUS server in the NetBlazer 8500 is used.

To enable PPP as the default service the following RADIUS entry must be defined in the corresponding RADIUS configuration file (“/etc/raddb/users”):

```
DEFAULT User-Password = "SUPRIMO"
        Service-Type = Framed,
        Framed-Protocol = MP,
        ITK-PPP-Auth-Type = ITK-Auth-PAP,
        Filter-Id = "0"
```

C Installing/Updating to V 5.0

All keyboard input is marked as shaded und must be entered as shown.

C.1 Prerequisite

The ITK NetBlazer 8500 Version 5.00 uses some features that need the **SCO OpenServer Release 5.0.4** operating system. The SCO Open Desktop Lite Release 3.0 software which has been used so far is no longer available and supported from SCO. Before installing ITK NetBlazer 8500 V5.00 the SCO OpenServer (Desktop) Release 5.0.4 (or later) has to be installed.

Before installing SCO OpenServer Release 5 all ITK NetBlazer 8500-configuration-files (parameter files, firewall files, etc.) should be saved (i.e. with the 'save_config'-tool).

The installation of SCO OpenServer Release 5 can be done in three different ways:

- local from CD-ROM: a SCSI host adapter and a SCSI-CD-ROM must be connected (temporarily) to the ITK NetBlazer 8500.
- remote: A network installation (netisl) can be done from a remote SCO OpenServer system. This is only possible with a supported LAN-adapter (e.g. 3COM-Ethernet-ISA).
- Diskcopy: The complete disk can be copied from a master-disk, on which SCO OpenServer release 5 (and possibly the newest ITK NetBlazer 8500 software) is installed.

C.2 Preparation

C.2.1 Installation Files (ITK NetBlazer 8500 Software Kit)

The ITK NetBlazer 8500 Software kit consists of the following files:

Installation File	Meaning
install_root	install script for the root software
install_pra	install script for the ITK NetBlazer 8500 software
install_www	install script for the ITK NetBlazer 8500 webMan software
root.tar.Z	compressed tar archive containing the root Software
pra.tar.Z	compressed tar archive containing the ITK NetBlazer 8500 software
update50.doc	V5.00 Installation Guide & Release Notes (Winword Format)
Install.doc	ITK NetBlazer 8500 PCI Hardware Installation Checklist (WinWord)
pranotes.txt	textfile containing the ITK NetBlazer 8500 release notes

These files should be copied (by ftp or from distribution media) to the */tmp* directory of the ITK NetBlazer 8500. The install scripts must be made executable:

```
chmod a+x install*
```

C.2.2 Shutdown running ITK NetBlazer 8500 software

Before installing new ITK NetBlazer 8500(Suprimo) software the running ITK NetBlazer 8500 software must be stopped. This is done with a user shutdown in the monitor program PRAMON (started from user *pra*).

C.3 Installing/Updating root software

The installation and update of root Software must be done from the user *root*. The preconfigured password for *root* is *itk*.

C.3.1 Installing or updating

There are two possible modes of ITK NetBlazer 8500 installation:

Mode	Meaning
Install	installs all files All device drivers are installed with default values or must be reconfigured manually.
Update	installs all files The device drivers need not be reconfigured (retain their old values). Update is not possible from older versions than V 5.00.

In both ITK NetBlazer 8500 installation modes **customer specific files are never overwritten by new files**. Customer specific configuration files are normally installed as sample files (Extension: *.sample*). If a customer specific file does not already exist the install process copies the sample file to the customer specific file (removes the .sample extension). Old customer specific files, which will be used no longer, are renamed to files with the extension *.old*.

C.3.2 Installing/updating root software

The ITK NetBlazer 8500 root software is installed with the command:

```
./install_root
```

executed in the directory, where the ITK NetBlazer 8500 Software Kit was installed (usually */tmp*).

During the installation the following device drivers are automatically installed with default parameters:

- Watchdog driver:
  - ➟ PA30 for PA30 watchdog board (ISA bus)
  - ➟ IFB for Kontron interface board (PCI bus)
- UIP driver (Interface: 192.168.18.254, Mask: 255.255.255.0, Channelcount: 120)
- VOIP driver (for voice compression DSP boards)

If the defaults are not sufficient, the device drivers should be reconfigured later. (see below)

At the end of the installation the CAPI driver must be configured by entering the following information:

- Hardware platform (KPR_PCI or KPR_EISA, or <RETURN> for default)
- Line rate for ISDN boards (E1 (30 ports) or T1 (23 ports), or <RETURN> for E1)
- Number of ITK Primary boards
- Number of ITK DigitalModem boards (30 modems)
- Number of modem ports for each ITK DigitalModem card
- Number of 542 DSP voice compression cards
- Number of DSPs for each 542 card
- Number of 548 DSP voice compression cards
- Number of DSPs for each 548 card
- Build a new UNIX-Kernel (y/n)

See *Reconfiguring CAPI20-Driver* (page C-5) to watch an example CAPI configuration.

C.3.3 Manual driver reconfiguration

The following chapters describe the manual reconfiguration of drivers. This is only necessary, if the default configuration is not sufficient or if the configuration should be changed later.

Normally you can continue with chapter “Install/Update NetBlazer 8500-Software”.

Reconfiguring CAPI20-Driver

The CAPI20 device driver (/dev/capi20) allows the access to the ITK ISDN- and Modem-Cards.

This driver is compliant to the CAPI-2.0 specification.

The CAPI driver configuration has been enhanced so that pre-configured card configurations with pre-defined slot and hardware-resource usage (IRQ, IO-port, shared memory) can be used. So normally not every embedded communication-card has to be specified.

The CAPI20 driver must be reconfigured for V5.00.

Configuration (from user “root”):

```
cd  /usr/itk/capi
./card_config
```

The following information must be entered:

- Hardware-Platform (KPR_PCI or KPR_EISA, or <RETURN> for default)
- Line-Rate for ISDN-cards (E1 (30 ports) or T1 (23 ports), or <RETURN> for E1)
- Number of ITK Primary-cards
- Number of ITK DigitalModem cards (30 Modems)
- Number of modem ports for each DigitalModem card
- Number of 542 DSP voice compression cards
- Number of DSP’s for each 542 card
- Number of 548 DSP voice compression cards
- Number of DSP’s for each 548 card
- Build a new UNIX-Kernel (y/n)

The following example shows a configuration on a PCI-system with 4 Primary, 2 DigitalModem and 1 DSP card:

```
card_config V1.3: Configurator for communication-cards
======================================================
(Copyright ITK Telekommunikation AG)

   Hardware-Base: pci
   Select Hardware-Platform from following list:
      1. kpr_pci.hw:    #!Platform: Kontron KPR-PCI
Number of Hardware-Platform (default:1): 1
   Using Hard-Platform kpr_pci.hw
PRI-Type (E1:30 ports,T1:23 ports) (default:E1): E1
   Number of ports for PRI-interface: 30 (E1)
Number of ITK Primary/PCI-cards             : 4
Number of ITK DigitalModem-cards (max: 30 Modems): 2
Number of ports on 1. ITK DigitalModem (default: 30) :
Number of ports on 2. ITK DigitalModem (default: 30) :
Number of ITK VIPER-XX 542-cards (max: 24 channel on 12 DSPs) : 1
Number of DSPs on 1. ITK VIPER-XX 542 (default: 12)   :
Number of ITK VIPER-XX 548-cards (max: 48 channel on 12 DSPs) :
   Enter card 1.DigitalModem:ISA (slot:0,irq:0,io:0x0330,sm:0xD0000,ports:30)
   Enter card 2.DigitalModem:ISA (slot:0,irq:0,io:0x0340,sm:0xD1000,ports:30)
   Enter card 1.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
   Enter card 2.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
   Enter card 3.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
   Enter card 4.Primary_____:PCI (slot:0,irq:0,io:0,sm:0,ports:30)
   Enter card 1.VIPER-12_542:ISA (slot:0,irq:0,io:0x3280,sm:0,ports:12)
   configured: 4 ISDN-cards  with 120 ports
               2 Modem-cards with 60 ports
               1 Compression-cards with 24 channels on 12 DSPs
Installing capi20-Driver ...
   capi20-Driver has been installed successfully
Build new UNIX-Kernel (y/n) ? y
Building UNIX-Kernel ...
        The UNIX Operating System will now be rebuilt.
        This will take a few minutes.  Please wait.
        Root for this system build is /
        The UNIX Kernel has been rebuilt.
Do you want this kernel to boot by default? (y/n) y
Backing up unix to unix.old
Installing new unix on the boot file system
The kernel environment includes device node files and /etc/inittab.
The new kernel may require changes to /etc/inittab or device nodes.
Do you want the kernel environment rebuilt? (y/n) y
The kernel has been successfully linked and installed.
        To activate it, reboot your system.
Setting up new kernel environment
```

The communication-card-configuration must be defined in the parameter-file

/usr/itk/capi/cards.par

which is automatically created, if a preconfigured standard-configuration is used.

If other configurations are used, this file must be edited by hand.

Reconfiguring Watchdog Driver

Normally the watchdog driver is installed automatically and a reconfiguration is not necessary.

The watchdog device driver (/dev/PA30 for EISA or /dev/IFB for PCI) allows the access to the watchdog hardware (get hardware-status (temperature, voltages), trigger the watchdog and light LED's on the front panel) and is installed automatically.

The watchdog driver can be configured manually with the following commands:

- Kontron IFB card:

```
cd /usr/itk/IFB
./INSTALL
```

- PA30 watchdog card:

```
cd /usr/itk/PA30
./INSTALL
```

Reconfiguring UIP-Driver

Normally the UIP-Driver is installed automatically and a reconfiguration is not necessary.

The UIP-Device-Driver (User-IP, /dev/uip) allows the access to the IP-Routing-Layer of the operating-system and is needed to access the IP routing stack for RAS services (PPP, SLIP). It has been enhanced to select the IP-Address for the connection from the NetBlazer 8500 software instead of managing a pool of IP-addresses in the driver (UIP-Pool).

This enhances the process of changing the UIP-Addresses, because in this case the UIP-Driver does not have to be reconfigured and no kernel has to be built (and no reboot).

Normally the default UIP-values are sufficient and need not be changed. Changes are required only in configurations, that use special LAN-to-LAN-communications.

The UIP-driver is automatically updated. If you want to specify special parameters, you have to reconfigure the UIP-driver as follows:

```
cd /usr/itk/uip
./INSTALL
```

Standard Values are:

IP Address of UIP-Device : 192.168.18.254

Netmask of UIP-Device : 255.255.255.0

Maximum Number of Channels : 120

Do you want to change any of these parameters (y/n) ? n

Add driver to system

Your System is reconfigured.

Do you want to rebuild the system [y/n]?: y

The UIP-configuration must be defined in the Parameterfile */usr/itk/uip/uip.par* which is created automatically and must not be changed.

Reconfiguring VOIP-Driver

Normally the VOIP-Driver is installed automatically and a reconfiguration is not necessary.

The VOIP-Device-Driver (/dev/voip) allows the access to the DSP boards (for voice compression) and is installed automatically.

The VOIP driver can be configured manually with the following commands:

```
cd /usr/itk/voip
./INSTALL
```

Building new UNIX-Kernel

This step is only necessary if a new kernel (system) has not been built in the previous steps.

After configuring all Device-Drivers a new UNIX-kernel must be built with the following command:

```
/etc/conf/bin/idbuild
```

C.4 Installing/Updating NetBlazer 8500 Software

The installation and update of NetBlazer 8500 software must be done from the user “pra”. The preconfigured password for “pra” is “pra”.

Installing Files

The files for the NetBlazer 8500 software will be installed with the command:

```
./install_pra
```

executed in the directory, where the NetBlazer 8500 Software Kit was installed (usually /tmp).

Older customer-files, that are not longer used, will be renamed to *.old.

The names of all used samples (copied to the original filename) are shown after the installation. These files should be verified/changed by the customer after the installation.

Have a look at “/tmp/install_pra.log” after the installation.

C.4.1 Configuring Parameterfiles

The following parameter files (in */u/pra/dat* directory) must not be changed, because they will be overwritten with each new installation:

Parameter File	Meaning
param.par	includes all parameter files used
common.par	default values for all ITK NetBlazer 8500 parameters

The following customer-specific parameter files (in */u/pra/dat* directory) should be checked and/or changed:

Parameter File	Meaning
isdn.par	parameters for ISDN PRI interfaces
process.par	special parameters for processes, for example line-counters, PRACTRL parameters
uip_pool.par	pool of dynamic IP addresses for remote IP users
auth.par	parameters for authentication and accounting
ppp.par	parameters for PPP and SLIP
dlm.par	parameters for **D**istributed **L**ine **M**anagement (DLM)
misc.par	miscellaneous parameters
l2f.par	parameters for L2F tunneling
cards.par	parameter for communication boards (automatically generated from the card-config tool)
voip.par	parameter for voice over IP (VoIP)
h323.par	parameter for H.323 (VoIP)
iss.par	parameter for Internet Supplementary Services (Siemens EWSD features)

The customer-specific parameterfiles will be preserved (will not be changed) in future installations. (Only the samples will be overwritten.)

C.4.2 Configuring firewall files

The format of the firewall files (in directory /u/pra/dat) has not changed, so a configuration is not necessary if a previous NetBlazer 8500 version has been used.

C.4.3 Configuring webMan

To use the NetBlazer 8500-Web-Management-Tool (webMan) (see Release-Notes below) the httpd of SCO must be configured as root with the command

```
./install_www
```

executed in the directory where the NetBlazer 8500-Software-Kit was installed (normally /tmp).

Default webMan Access Rights

The default access rights for all webMan-functions are based on a user/ password-scheme that is not in junction with the UNIX user and group scheme:

- All users in the group “users” are allowed read-access.
- The administration functions (parameter changes, OS operations) are only allowed from user “admin”.

The pre-installed administration-user is “admin” (with password “itk”).

The pre-installed standard-user is “pra” (with password “pra”) in the group “users”.

Normally the NetBlazer 8500 access should be restricted by packet filter and firewall mechanisms and the pre-installed webMan-users need not be changed (only for expert-users!).

Adding new webMan users

All webMan-users must be defined in the file “/u/pra/www/sysadm/ .htpasswd”, which should not be changed manually.

A new user in this file is created with the following command (from user “root”):

```
cd  /u/pra/www/sysadm
./htpasswd  .htpasswd  USERNAME
```

(The same command can be used to change the user password.)

The new user must be entered into the group “users” by changing the file “/u/pra/www/sysadm/groupaccess” manually.

Using host-access

By using host-access the webMan usage can be restricted by IP-host or IP-network-addresses.

To enable host-access, the file “/u/pra/www/sysadm/.hostaccess” must be changed manually. Additionally, the links in the www-directories must be changed to point to the “.hostaccess”-file instead of the “.groupaccess”-file.

SCO-httpd-configuration

The SCO-http-daemon is configured in the file “/var/scohttp/conf/scohttpd.conf”.

After changing the configuration the httpd must be stopped and started again:

```
/etc/scohttp  stop
/etc/scohttp  start
```

C.4.4 RADIUS-Authentication-Server

If the NetBlazer 8500 is not to run a local Authentication-Server (but use a remote-authentication- or application-server) this section can be skipped.

A description of all NetBlazer 8500-supported RADIUS- and ITK-attributes is in the file “/etc/raddb/rad_attr.txt”.

Configuring RADIUS-daemon

The RADIUS-daemon configuration files are in /etc/raddb:

- dictionary - the definition of all attributes and values (should not be changed
- clients - configuration-file describing which RADIUS clients (hostnames) are allowed to access this RADIUS-daemon (client (hostname) and secret (password))
- users - database with all usernames/passwords and service-selections

All hosts (NetBlazer 8500) that should access this RADIUS-daemon must be entered in the file '**clients**'. For each host the client-name (hostname) and the secret (password) must be entered. NetBlazer 8500 uses normally the secret "test".

All users that are allowed to use this NetBlazer 8500 (as a data or voice gateway) must be entered in the file '**users**'.

Starting RADIUS-daemon

The RADIUS-daemon is started manually with the following command:

```
/etc/radius/radiusd
```

If the RADIUS-daemon is to start automatically, the file "/etc/radius/S95ITK_AS" must be copied to "/etc/rc2.d" (from user "root").

C.4.5 Licenses

V5.00 needs license keys for the following major features:

- RAS: Remote access (ISDN and modem)
- VoIP: Voice over IP
- ISS: Internet Supplementary Services (for Siemens EWSD)

Before starting the software the license keys must be entered in parameterfile "misc.par".

C.4.6 Restarting System

After installing the new software the NetBlazer 8500 must be restarted (from user "root"):

```
reboot
```

C.4.7 Creating ix1.ini file after updating Software

After updating NetBlazer 8500 Software a new ix1.ini file has to be created.

(1) Login as "pra"

(2) If the NetBlazer 8500-software is started automatically, shut it down (pramon:5:1)

(3) Load all ISDN-/Modem-boards manually:

```
ixload
```

If the NetBlazer 8500-software wasn't started automatically, ixload shows the Warning
"WARNING: No configuration file ix1.ini found, create a default file ix1.ini."
a new ix1.ini file with default values has been created, the original ix1.ini has been backuped as ix1.ini.xxx (where xxx is the highest number of saved ix1.ini files).

(4) Update the default values of the new ix1.ini file with the settings of the saved ix1.ini.xxx.

(5) Start NetBlazer 8500 software

```
start_practrl
```

(6) Verify that all boards are running with the correct parameters (Card-table: card info)

```
pramon
```

C.5 Cleanup

After successfully installing the NetBlazer 8500-Software the Kit-Files can be removed from the install-directory (normally /tmp).

D ix1.ini Configuration File

In this chapter you will find the description of the *ix1.ini* configuration file.

The *ix1.ini* configuration file is an ASCII file. If you want to use settings other than the default settings for the ISDN interface, it is necessary to edit the appropriate parameter in the configuration file. The following section describes the structure and the parameters of the configuration file.

D.1 Structure of the ix1.ini configuration file

ix1.ini only need to be changed if you have created a new *ix1.ini* file by running *ixload* and you don't want to use the ISDN interface default settings.

The *ix1.ini* configuration file is structured in various sections:

- **Section:** is described with the "**[**" and "**]**" symbols, for example `[section]`.

  This description is repeated for each installed ITK-board.

  For example:

  You have installed 2 ITK-boards. In the configuration file you will find 2 sections with the symbols "**[**" and "**]**".
  In these sections you can configure general parameters for your ITK-boards.

- **Subsection:** is described **for example** with the following:

  ;----------

  ; general adapter settings

  ;----------

  In this section you can configure parameters for the appropriate line of your ITK-board(s).

- **(line x) section** Every (line x) section is described with "(line x)" and has several subsections. There are boards with only one (line x) section and boards with several (line x) sections (not supported in version 5.0).

  For example:

  - ITK Primary = 1 line (PRI), which means that the configuration section has only one (line x) section called (line 1).

- **Parameter:** is displayed on the left side of your screen with a "=" symbol at the end.

  If a parameter is displayed **without a value**, your board uses the **default value** as described in the tables later.

  For example:

  `mvipType=` parameter without value
  meaning: default value is chosen

  `mvipType=1` parameter with value

- **possible values:** are described after the "**;**" symbol with further information.

  For example:

  possible values of parameter `mvipType` are:
  `;1=master,2=slave`

  For example:

  `mvipType=` parameter without value

D.2 Parameters in the subsections

The parameters in the subsections of the configuration file have the following meanings:

Subsection: firmware

parameters	meanings
`<bootFile>`	Spezifies the bootfile for the board. Because in this version no bootfile is necessary this parameter has no entry. **Default: The default is depending on the board type and is automatically set.**
`<downloadFile>`	Every ITK board has its own download file, named *.bin You only have to change the name of the *.bin in the appropriate section if you have different versions of ITK boards in your system. **Default: The default is depending on the board type and is automatically set.**

Subsection: general adapter settings

parameters	meanings
<mvipType>	The MVIP clock mode can be set: 1 = Master meaning: The board is the clock master of the MVIP system (usually the board that is connected to the ISDN line is the master board) 2 = Slave meaning: Another board, perhaps from another manufacturer, is the clock master of the MVIP system. In this case our MVIP clock synchronizes with the clock of another board. **Default: 1 =Master (for ITK ISDN Line Boards, 1st ITK Primary)** **Default: 2 =Slave (for ITK DigitalModems, additional ITK Primary boards)**
<voiceCoding>	The voice code standard can be set: 1 = a-Law (European Standard) 2 = µ-Law (US Standard) For ISDN Line Boards: The voice code standard should be set according to the chosen D channel protocol. **Default: 1 = a-Law**

parameters	meanings
`<countryVersion>`	This parameter is only used for the ITK DigitalModem. The following values are supported: **Country** **Code** **Country** **Code** Australia 402 Japan 500 Austria 216 Malaysia 234 Belgium 207 New Zealand 403 China 273 Norway 211 Cyprus 417 Poland 253 Czech Republic 255 Portugal 241 Denmark 212 Russia 224 Finland 237 Singapore 214 France 209 South Africa 213 Germany 217 Spain 231 Holland 205 Sweden 210 India 268 Switzerland 219 International 300 Taiwan 103 Ireland 238 Turkey 227 Israel 206 UK 400 Italy 201 US & Canada 001 **Default: 217=Germany**

parameters	meanings
<compression>	The type of compression is set with this parameter. (The compression takes only effect if your remote partner also has ITK boards.) The following variants are supported: 1 = none (switches off compression) 2 = V.42bis (no standard; throughput better for multiple channels < 4) 3 = ITK_COMP - ITK compression (throughput better for multiple channels > 4) 4 = optional (Board offers V.42bis and ITK compression.) In this case the called subscriber can choose the compression method to be used. In case the calling and called subscriber have chosen “optional”, the ITK compression is chosen. 5 = capiPlus defined The compression is defined by the CAPIplus application, for example ITK NetBlazer 4400. **Default: 1 = none (ITK Primary)** **2 = V.42bis (ITK DigitalModem)**

Subsection: general line infos

The following parameters are important only for ISDN boards (not for the ITK DigitalModem board).

parameters	meanings
`<dProtocol>`	You can set your appropriate D channel protocol. When this manual went to print, the following codes were valid or will be valid in the near future: **1** = 1TR6, Deutsche Telekom (old national protocol) **2** = DSS-1/Euro-ISDN/NET3, ETSI **3** = VN2 (France) **4** = VN3 (France) **5** = 5ESS (AT&T/USA) **6** = DSS-1 PBX (with SETUP_ACK) **7** = DMS-100 (USA) **8** = CORNET-N (Siemens Pbx) **9** = DSS-1 (Norway Phase 1) **10** = CORNET-T (Siemens Pbx) **11** = National ISDN 1 = NI-1/USA **12** = Q.931 Blue Book (CCITT) **13** = Q.SIG, ECMA **14** = National ISDN 2 USA (not yet implemented) **15** = TS013/TS014, Australia **16** = DSS-1 for the Netherlands (type national) **17** = DSS-1 PBX (no sending complete) **18** = DSS-1 for ALCATEL PBX **19** = INS64 (Japan) (not yet implemented) **20** = 5ESS (G3_PBX) (not yet implemented) **21** = DSS-1 with no RESTART **22** = 4ESS (USA/AT&T - T1 long distance) **Default: 2 = DSS-1**

parameters	meanings
`<sasStateMask>`	Here you can set the properties of ESS (Extended Security Service). In order to use ESS you need a certified ISDN board. ESS is per default disabled. If you want to activate ESS, the value **0x1D** is recommended. See the following table for possible values. The headings in the table have the following meaning: **Authentication:** Enables identity check of remote ITK board. **Encryption:** Enables DES encryption of transmitted data. **Closed user group:** Enables access control. Only connections to remote ITK boards of identical group are accepted. **ESS optional mode:** Enables connections to remote ISDN boards without ESS. NOTE: To maintain security, mode has to be **disabled**. **Default: 0x00**

	VALUE	ESS enabled	Authentication	Encryption	Closed user group	ESS optional mode
Default	**0x00**	-	-	-	-	-
	0x01	x	-	-	-	-
	0x1D	x	x	x	x	-
	0x0D	x	x	x	-	-
	0x15	x	x	-	x	-
	0x05	x	x	-	-	-
	0x19	x	-	x	x	-
	0x09	x	-	x	-	-

VALUE	ESS enabled	Authen-tication	En-cryption	Closed user group	ESS optional mode
0x11	x	-	-	x	-
0x1F	x	x	x	x	x
0x0F	x	x	x	-	x
0x17	x	x	-	x	x
0x07	x	x	-	-	x
0x1B	x	-	x	x	x
0x0B	x	-	x	-	x
0x13	x	-	-	x	x
0x03	x	-	-	-	x

parameters	meanings
`<sasEventMask>`	Here you can define what happens if a security error occurs. To enhance security, parameters should be enabled. 0x00 = no abort 0x01 = only abort on authentication error 0x02 = only abort on signature error 0x03 = abort on authentication or signature error **Default: 0x03 = abort on authentication or signature error**

parameters	meanings
<sasDESMode>	Here you can set DES mode (Data Encryption Standard). CBC mode is recommended for most applications. 0x00 = DES-ECB (**E**lectronic **C**ode **B**ook) 0x01 = DES-CBC (**C**ipher **B**lock **C**haining) 0x02 = DES-CFB (**C**ipher **F**eed **B**ack) 0x03 = DES-OFB (**O**utput **F**eed **B**ack) **Default: 0x01 = DES-CBC**
<sasHashMode>	Here you can set the Hash Mode, used by signature generation. You can set the following two types of algorithms: 0x00 = MD4 (Message Digest) 0x01 = SQRMN (Square MOD n) **Default: 0x00 = MD4**
<sasAutoChgSessionKey>	Here you can set the level of encryption security: DES key is changed automatically every transmitted # blocks. Possible values for signature generation are: 0 to 65535 # blocks < 100 may reduce system performance # blocks > 500 is recommended # blocks = 65535 is maximum **Default: 1000**

parameters	meanings
<sasAutoSign>	Here you can secure data integrity: electronic signature is generated automatically every transmitted # blocks. Possible values for signature generation are: 0 to 65535 # blocks < 100 may reduce system performance # blocks > 500 is recommended # blocks = 65535 is maximal **Default: 1000**
<eazToMsn0> ... <eazToMsn9>	You need these parameters if you use a CAPI 1.1 application and DSS-1. Outgoing calls: The source EAZ (outgoing EAZ) can be mapped into a MSN of DSS-1. Incoming calls: The MSN of DSS-1 (that is called) can be mapped into a requested EAZ. Without mapping the requested EAZ will be the last digit of the called MSN. This will cause problems if you have two or more MSNs with identical last digit. Maximum 8 digits are possible. Type “x” if you want no digit to be transmitted with D channel. **Defaults:** **eazToMsn0 = 0** **eazToMsn1 = 1** **eazToMsn2 = 2** **...** **eazToMsn9 = 9**
<signalingMode>	1 = CCS **C**ommon **C**hannel **S**ignaling (only supported; do not change) The whole D channel is used for the signaling messages of all B channels. **Default: 1 = CCS**

parameters	meanings
<lineAccess>	1 = point-to-multipoint 2 = point-to-point **Default: 2 =point-to-point (for ITK Primary)**
<lineType>	1 = switched line = ISDN standard (dial-up connection) 2 = ISDN leased line **Default: 1 = switched line**
<leasedLineType>	This parameter is necessary only if you have set <lineType> = 2 1 = leased line with D channel and single B channel (for example 30 channels with 64 kbit/sec each) 2 = leased line with no D channel and single B channel 3 = leased line with D channel and bundled B channel (for example 1 channel with 1.92 Mbit/sec) 4 = leased line with no D channel and bundled B channel **Default: 1 =leased line with D channel and single B channel**
<teiType>	Stipulates which TEI (**T**erminal **E**ndpoint **I**dentifier, protocol element at level 2 of the ISDN D channel) is used. 1 = Auto TEI 2 = Fixed TEI This parameter is ignored if you have configured the line access as Point to Point. **Default: 2 =Fixed TEI (ITK Primary)**
<teiValue>	If <teiType> is set to Fixed TEI, select a number between 0 and 63 for <teiValue> of your ITK board for the ISDN connection. **Default = 0**

parameters	meanings
<NT_TE_Side>	The parameter is only important for leased lines. 1 = TE side 2 = NT side **Default: 1 = TE-side**

Subsection: parameters for primary rate interface only

The following parameters are **only** valid for the **primary rate interface**:

parameters	meanings
`<clockGenera-tor>`	Sets the clock. 1 = clock is generated by line 2 = clock is generated by adapter **Default: 1 = clock is generated by line**
`<firstBChan>`	If you use an ISDN interface with less B channels than the default ISDN interface, define the first B channel to be used upon connection establishment. Possible values: For the **E1** interface: 1-30 For the **T1** interface: 1-23 **For example:** You want to use an ISDN interface with 10 B channels from B channel 5 to B channel 14. You must define the `<firstBChan>` on 5. When this manual went to print, only the value 1 for the `<firstBChan>` parameter was supported. Please refer to the README.TXT file. **Default: 1 (for the E1 interface)** **Default: 1 (for the T1 interface)**

parameters	meanings
<lastBChan>	If you use an ISDN interface with less B channels than the default ISDN interface, define the last B channel to be used upon connection establishment. Possible values: For the **E1** interface: 1-30. For the **T1** interface: 1-23. For example: You want to use an ISDN interface with 10 B channels from B channel 5 to B channel 14. You must define the <lastBChan> on 14. **Default: 30 (for the E1 interface)** **Default: 23 (for the T1 interface)**
<bChanMask>	When this manual went to print, the parameter was not supported. Please refer to the README.TXT file.
<bChanSelection>	There are different sequences of B channel activation upon connection establishment: 1 = RoundRobin up 2 = RoundRobin down When this manual went to print, the parameter was not supported. Please refer to the README.TXT file. 3 = fix up When this manual went to print, the parameter was not supported. Please refer to the README.TXT file. 4 = fix down When this manual went to print, the parameter was not supported. Please refer to the README.TXT file. **Default: 1 = RoundRobin up**

parameters	meanings
`<lineRate>`	If you want to use an ISDN interface according to European Standard with 30 B channels and 1 D channel (E1) define the value 1. 1 = PCM30 (E1) If you want to use an ISDN interface according to American Standard with 23 B channels and 1 D channel (T1) define the value 2. 2 = PCM24 (T1) **Default: 1 = PCM30 (E1)**
`<lineCode>`	Line codes supported for the **T1** interface: 1 = B8ZS (**B**ipolar **8 Z**ero **S**ubstitution) 2 = AMI_WITH_ZCS (Alternate Mark Inversion with Zero Code Suppression) Line codes supported for the **E1** interface: 3 = HDB3 (High Density Bipolar of Order 3) 4 = AMI (Alternate Mark Inversion) **Default: 1 = B8ZS (for the T1 interface)** **Default: 3 = HDB3 (for the E1 interface)**

parameters	meanings
<framingFormat>	Framing formats supported for the **T1** interface: 1 = ESF (Extended Superframe Format) 2 = SF (Superframe Format) or D3/D4 Format 3 = F4 (4 - Frame Format) 4 = F72 (72 - Frame Format) Framing formats supported for the **E1** interface: 5 = CRC4_MULTI_FRAME (Cyclic Redundancy Check 4 Multi Frame) is used in most European countries 6 = DOUBLE_FRAME is sometimes used in France, the Netherlands and Sweden **Default: 1 =ESF (for the T1 interface)** **Default: 5 =CRC4_MULTI_FRAME (for the E1 interface)**
<dsxPreemphasis>	The parameter is necessary for the **T1** interface. Defines values from 1 to 7 depending on your cable length. If your cable is longer than 689 feet, define the value 8. With this setting an appropriate preemphasis of your outgoing signal is activated. **For example:** Value 8 = preemphasis 18 dB 1 = 0 - 115 feet 2 = 82 - 213 feet 3 = 180 - 312 feet 4 = 279 - 410 feet 5 = 377 - 509 feet 6 = 476 - 607 feet 7 = 574 - 689 feet 8 = 18 dB **Default: 1 = 0 - 115 feet**

Subsection: parameters for basic rate interface only

The parameters in this subsection are **only** valid for the **basic rate interface** if it is configured for a US D channel protocol.
In this version these parameters are not in use and you should not change them.

D.3 Important parameters for ITK DigitalModem

The following parameters are important only for the ITK DigitalModem:

Subsection firmware :

<downloadfile> (see page D-3)

Subsection general adapter settings:

<mvipType> (see page D-4)

<voiceCoding> (see page D-4)

<countryVersion> (see page D-5)

<compression> (see page D-6)

E ITK NetBlazer 8500 Installation Checklist

E.1 Personal checklist

For proper installation of ITK NetBlazer 8500 please fill in the following form.

- **Shipping address:**

  Company: _____

  Name/Dept.: _____

  Street: _____

  City & Zip Code: _____

  Country: _____

- **Technical contact:**

  Company: _____

  Name: _____

  Phone: _____

  Fax: _____

  E-Mail address: _____

❒ **functioning PRI connection:**

Connection to PABX (yes/no/type of PABX): _____

Line Rate (E1 (30 channels) or T1 (23 channels)):_____

D channel protocol (DSS1, 1TR6 or other): _____

Telephone number (with national code): _____

NT Connection: (RJ45, RJ48, fixing screw): _____

Support of direct dial-in (DDI): ❒

- **Country**, where the system should be installed: _____

❒ VGA monitor and PC keyboard (PS/2 connector) available (only for setup)

- **Physical connection to backbone:**

❒ **Ethernet:**

(BNC, UTP, AUI, 100Base-T): _____

❒ **Token Ring (opt):**

Speed (4 or 16 Mbit/s): _____

Cable type (STP or UTP): _____

Adapter type (9-pin or RJ45): _____

- **Backbone connection:**

IP address: _____._____._____._____

Subnet mask: _____._____._____._____

Default router: _____._____._____._____

Domain name: _____

Hostname for ITK NetBlazer 8500 (max. 8 chars.): _____

- **Frame-Relay (opt.):**

Speed: _____

DTE or DCE: _____

Interface (X.21, V.35, V.36): _____

FR switch (e.g. Cisco): _____

DLCI IP addresses: _____ _____._____._____._____

_____ _____._____._____._____

_____ _____._____._____._____

❒ **IP pool with dynamic IP address assignment:**

(If you wish to use more than one IP pool, please use comments below)

IP address: _____._____._____._____

Subnet mask: 255. 255. 255._____

or

From IP number: _____._____._____._____

to IP number: _____._____._____._____

- **Authentication:**

  Protocol (RADIUS, PSP): _____

  IP address of external Auth. Server (or local): _____._____._____._____

- **Routing:**

  On all used computers or routers the routing table entries for user IP addresses (static and dynamic) have to refer to ITK NetBlazer 8500.

- **IP address of the NMC (for SNMP traps):**

  _____._____._____._____

- **Comments/special considerations:**

  _____

  _____

  _____

  _____

  _____

  _____

  _____

- **Date of Installation/Training:** _____

E.2 Hardware Installation:

Date: _____

Name:_____

Kontron-SN:_____

E.2.1 Preparation:

- Remove system cover
- Harddisk type + Ser.-No.: Western Digital Caviar 11200
  Ser.No.:_____
- Network Adapter Type: 3com 3c900_____

E.2.2 Installing Primary, Digitalmodem and Voice compression Adapters

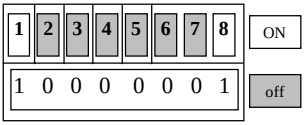
Slot 1 is the slot next to the CPU board; see Appendix A.2.1, *Slot-/IRQ-usage Overview* (page A-7) for further details.
Install metal springs between boards.

Adapter	Slot	Jumper / DIP-Switch *)	MVIP-Term. **)	Serial No.	RAM in MB
1. ITK Primary	2	E1/T1	X		64
2. ITK Primary	4	E1/T1	-		64
3. ITK Primary	5	E1/T1	-		128
4. ITK Primary	6	E1/T1	-		128
1. ITK DigitalModem	10	110011	(X)		
2. ITK DigitalModem	9	001011	-		
3. ITK DigitalModem	8	101011	-		
4. ITK DigitalModem	7	011011	-		
1. Voice compression board	9***)	0010	(X)		
2. Voice compression board	8***)	0110	-		
3. Voice compression board	7***)	1010	-		

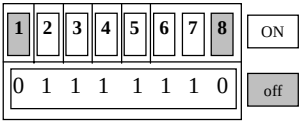
Annotations see next page.

*) **ITK Primary: DIP-switch setting for E1/T1 connection:**

Setting for E1 connection:



Setting for T1 connection:

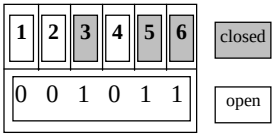


The setting must be according to the line connection used during the installation, configuration and testing. The appropriate setting according the customer requirements may differ, and must be adjusted before shipment (see 6.3.4). Please pay attention to use the right cable for E1 (RJ-48/ RJ-45) resp. T1 (RJ-48/RJ-48).

ITK DigitalModem (Granite):

DIP-switch 6 to 1 is closed for „1“, open for „0“.

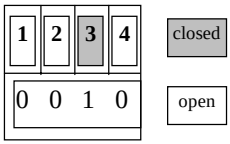
Example for 2nd ITK DigitalModem:



Voice compression board:

DIP-switch 4 to 1 is closed for „1", open for „0".

Example for 1st Voice compression board:



**) MVIP termination is set with jumper pairs near the MVIP connector on the boards. (jumper have to be installed).

For systems with five or fewer MVIP bus connections, it is adequate to place the circuit board that is the master clock source at one end of the cable and provide the termination on the circuit board which is physically at the other end of the cable.

On systems with more than five MVIP connections, both ends of the cable should be electrically terminated with jumpers. No other boards should terminate these lines. First ITK Primary in the rightmost position needs MVIP bus termination. On the other side only one board must be MVIP bus terminated. This is the ITK DigitalModem in slot 10. If no ITK DigitalModem is installed the ITK Voice compression (ITK VIPER) board in the leftmost position must be terminated.

Board	Jumper settings
ITK Primary (Jumper near MVIP connector)	 Jumper closed (MVIP bus terminated)
	 Jumper open (MVIP bus not terminated)
ITK DigitalModem	 Jumper J3 closed (MVIP bus terminated)
	 Jumper J3 open (MVIP bus not terminated)
ITK Voice compression board	 Jumper J2 and J4 closed (MVIP bus terminated)
	 Jumper J2 and J4 open (MVIP bus not terminated)

***) The slot numbers for voice compression boards must be adapted if ITK DigitalModem boards are also to be installed. Slot number is (10 minus *number of present ITK DigitalModem boards*):

1st ITK DigitalModem in slot 10, 2nd ITK DigitalModem in slot 9, 1st ITK Voice compression board in slot 8 and 2nd ITK Voice compression board in slot 7.

- Connect the boards with the MVIP-flat ribbon cable.

E.2.3 Finish Hardware Installation

- Connect COM 2 and first ITK Primary board (MVIP-master) with 9-pin Sub-D cable.
- Insert flat rubber blocks in the top cover (numbered places)

E.3 PCI-BIOS Configuration

- Plug in keyboard, CRT-display and power cord
- Switch main power on
- press <DEL>-key when prompted by BIOS-message to enter BIOS setup
- Check parameters and change as necessary. For default parameter list see Appendix A.2.2, *ITK default BIOS Settings* (page A-8).

E.4 Unix configuration

E.4.1 Hostname and boot-mode adaptation

- Set NetBlazer 8500 system name: *uname -S <NetBlazer 8500 name>* **and adapt /etc/hosts**
- *vi /etc/default/boot*, should be set correctly as shipped; if not:
  Set: PANICBOOT=YES
  Add: TIMEOUT=10

E.4.2 TCP/IP Configuration

- Enter *scoadmin*

Install 3Com Ethernet adapter

Should be installed correctly as shipped, otherwise:

- Topic ***Software Manager***

- *Software* ⇒ *install new* ⇒ From <localhost> ⇒ Media Device: Floppy Drive
- Insert SCO Driver disk ⇒ Continue
- Follow installation advice
- **Don't** quit scoadmin

Configure TCP/IP Layer

- Topic ***Networks***
- *Network Configuration Manager* ⇒ Hardware ⇒ Add new LAN Adapter
- Choose *3com Etherlink XL PCI* adapter ⇒ Continue
- Add Protocol ⇒ SCO TCP/IP
- hostname: [*NetBlazer 8500* name]
- IP-Address: [enter IP-address reserved for local testing]
- Netmask: 255.255.255.0
- Broadcast address: use default value
- Domain Name: _____ (see customer sheet)
- TCP connections: 1280
- Pseudo ttys: 64
- Quit
- Do you want to relink: YES
- Answer following questions during kernel rebuild with YES.

Set COM2: speed

Should be set correctly as shipped, otherwise:

- *mkdev serial* ⇒ remove [r] ⇒ IBM-COM2 [2] ⇒ Create new Kernel [n]
- *mkdev serial* ⇒ install [i] ⇒ 1port card [1] ⇒ COM2 [2] ⇒ IBM-COM2 [2] ⇒ baud rate 9600 ⇒ again 9600 [1] ⇒ create a new kernel ⇒ No [n]

Create new kernel

- /etc/conf/bin/idbuild
- Kernel as default ⇒ yes [y]

- environment rebuild⇒ yes [y]
- Boot system with '*reboot*' and verify BIOS version of the KONTRON box as 1.41 (minimum). If BIOS version is lower than 1.41, use BIOS update diskette, reboot the system with pressing Ctrl +<Home> (Strg + <Pos1> with german keyboard) and waiting for a 4-tone signal. After automatic restart the BIOS entry should be 1.41 (or newer).
  Wait until 'login:' appears.

  Check possible error messages. If necessary, review error messages after reboot with:
  more /usr/adm/messages

E.4.3 Configure user „PRA“

This user should be available as shipped, otherwise configure as following

- Login as root (Password *itk*)
- Start *scoadmin*
- Accounts ⇒ User ⇒ Add new user
- Login: pra
- comment: NetBlazer 8500 standard user
- Modify defaults: yes
- login group: group
- login shell: ksh
- Homedirectory: /u/pra
- Home directory: Create Home
- User number: 200
- Type of User: Default
- create user: yes
- Password: now
- Force change: no
- pick Password: [Return] ⇒ pra ⇒ pra
- Quit *scoadmin*

E.5 NetBlazer 8500 software installation

Version: __.____

E.5.1 Copy root / NetBlazer 8500 software

- Login: root (Password itk)
- cd /tmp

Network based installation

- *ftp* [hostname/IP-address of appropriate NetBlazer 8500 software server]
- login as pra
- *cd /usr/itk/Vx.yy /kit* (replace *x.yy* with version number)
- prompt
- mget *
- bye

Floppy disk based installation

- insert first floppy disk
- tar xv
- insert floppy disks as prompted

E.5.2 Start root installation

- chmod +xxx install*
- ./install_root
- choose installed watchdog board and answer question :
  available drivers: Kontron IFB = 1 PA30 = 2 (default= 1):
- Number of Hardware-Platform (default:1):
  [select platform or just press ENTER]
- PRI-Type (E1:30 ports,T1:23 ports) (default:E1):
  [enter option or press ENTER]
- Number of ITK Primary/PCI-cards:
  [enter number]

- Number of ITK DigitalModem-cards (30 Modems):
  [enter number]
- Number of ITK VIPER-12 542-cards (24 channel):
  [enter number]
- Number of ITK VIPER-12 548-cards (48 channel):
  [enter number]
- Build new UNIX-Kernel (y/n) ? **[*y*]**
- Kernel as default ⇒ yes **[*y*]**
- environment rebuild⇒ yes **[*y*]**

E.5.3 NetBlazer 8500 software installation

- Login as pra, password pra (please do not use *su pra* !)
- ***cd /tmp***
- ***./install_pra***
- *exit* ⇒ login again as pra

Adapt „UIP_POOL.PAR“

- Enter UIP-Pool Address defined for this system:
  Start address UIP-Pool (s. installation list)

  _____._____._____._____
- *vi uip_pool.par*
- Remove comment sign „#“ and adapt line:
  .ip_pool_1: ***[Start address UIP-Pool]*** **255.255.255.224**

  In some cases it is necessary to reconfigure the netmask entry.

Adapt „AUTH.PAR“

- *vi auth.par*
- Adapt line:
  .Radius_Server: ***[Authentication server name]***
- Remove comment sign „#“:
  .auth_prot: Radius
  .auth_req: ABCZ

E.5.4 Install Radius Server

- Login as root, Password itk
- *cp /etc/radius/S95ITK_AS /etc/rc2.d*
- *vi /etc/raddb/clients*
- Adapt line for special configuration, default „localhost“ should work in most cases.

#Client Name	Key
#----------	----------
[Authentication server name]	**test**

E.5.5 Software verification

- Login as root, Password itk
- Do the following files exist?
  Directory **/etc/rc2.d/** : S85uip, S95ITK_PRA, S95ITK_AS
  Directory **/dev/ :** uip, ucip, IFB, capi20
- Boot system with *reboot*
- Check boot messages for loading of the following drivers: **uip driver, watchdog driver, all ITK-adapters**
- Check for possible error messages

E.5.6 Start NetBlazer 8500-WebManager installation

- Login as root, Password itk
- *cd /tmp*
- *./install_www*

E.6 NetBlazer 8500 testing

E.6.1 Debug Ports

- Connect NetBlazer 8500 to PRI connector
- Login as pra, Password pra
- start pramon
- ***7*:** Display PROCESS-monitor

- check infotext for process DEBUGLOG to read „D-channel up“
- Disconnect shortly PRI cable from controller and check display

E.6.2 ISDN access test

- Connect Win95 computer with ISDN-Adapter to ISDN-BRI-Connector
- Manual Connection with *DialUp-Network* and User *itkSuprimo*
- *telnet 192.168.18.254*
- Login as pra and start *pramon*
  - Check Status control process (PRACTRL)
  - Check PPP-connection with [1]
  - Quit pramon [q][q]
- *exit*
- close connection

in case of any errors occuring, check the following files:

- /u/pra/log/practrl.info

enter daily-logging directory with *logs* and check

- isdn_ins*.log and debuglog*.log (always the latest written file)

Voice access test

- To test the voice calls from a dial-out gateway the test utility “scon” has been enhanced to support a new option (“-voice”) to do a voice call to a normal phone.

  Example:
  The following command establishes a voice connection to the destination number “12345”:

  scon 12345 <CTRL> -voice
- To test a real phone-to phone-connection a PRI line and an analog phone is needed.
- Verify the file /etc/raddb/users for following entries:

*%_10 User-Password = "DIRECT_DIAL" #**(without leading hashmark)***
Service-Type = ITK-Voice-over-IP-Comp,
ITK-Banner="VGI",
ITK-Prompt="e"

123 User-Password = "VOICE-ACCOUNT"
ITK-Username = "W. Smith"

- Call PRI-line no. + DDI no. 10 to get the Interactive Voice Response of the NetBlazer.
- Key in the PIN 123#.
- Key in a reachable dial number (e.g. an analog phone in the local telephony network)

Modem access test

- Win95 computer with serial cable to modem
- Test the connection several times (1 x per Modem adapter) as described in Chapter E.6.2, *ISDN access test* (page E-13)
  but check files pstn_ins*.log and debuglog*.log

WebManager test

- start web browser on computer with LAN connection or ISDN connection to NetBlazer 8xxx
- go to URL: *NETBLAZER 8500_IP_ADDRESS*

Watchdog adapter test

- *pramon*

Chose the following options:

- ***5*** : Shutdown
- Change shutdown-state ? (y/n) ***y***
- ***5***-Cold-Reboot (Reset)
- `timeout [s] : 0` (for immediate shutdown)

- wait for Memory-Test after reboot

E.7 Configure NetBlazer 8500 for shipment

E.7.1 Change hardware (card_config)

- The CAPI 2.0 configuration is already part of the root installation. If later the hardware will be changed, the tool “card_config” (as user root) could be used:
- cd /usr/itk/capi
- *./card_config*
  Please answer the following questions according to your hardware installed, see Chapter E.5.2, *Start root installation* (page E-10).

E.7.2 Change TCP/IP System

- Login as root, Password itk
- netconfig
- Select *3com Etherlink XL PCI (3c900)* subtopic *SCO TCP/IP*
- *Protocol* → *Modify Protocol Configuration*
- *SCO TCP/IP Configuration*
- Enter Internet address for this NetBlazer 8500:
  Internet address (s. installation list) _____._____._____._____

  Netmask (s. installation list): 255 . 255 . 255 ._____
- Leave other entries at *default*
- Choose *Ok*
- Quit netconfig , rebuild kernel when asked to do so,
  answer following questions with YES
- check /etc/hosts for missing, wrong or double entries of hostname

deactivate route daemon

Should be configured correctly as shipped.

- *vi /etc/rc2.d/S85tcp*
- Comment out 4 lines:

  # Choice of routing daemons.

  #

```
# if [ -x /etc/routed -a ! -f /etc/gated.conf ]; then
#         routed &
#         echo "routed \c"
# fi
```

Enter default route

Enter router IP-address:
Router IP-address (s. installation list)**:** _____._____._____._____

- Create new file:
  vi /etc/rc2.d/S86tcp_default_route
- Enter line:
  /etc/route add default <*IP-address router*>
- *chmod 711 /etc/rc2.d/S86tcp_default_route*

Check / change Radius server usage (local/remote)

- check/remove (for remote server) Radius server start (see Chapter E.5.4, *Install Radius Server* (page E-12))
- check /u/pra/dat/auth.par
  (see section *Adapt „AUTH.PAR“* (page E-11))

E.7.3 Set localized parameters (if applicable)

select desired language in „MISC.PAR“

Default language is english „E“

- Login as pra, password pra, change to directory *dat*
- *vi misc.par*
- adapt line:
  .pra_language: E
  or
  .pra_language: D (for german)

Set localized parameters of Modem adapters

- *cd /usr/itk/ixload*
- *vi ix1.ini*

- for each paragraph *granite MICA (*ITK DigitalModem*)* adapt the line *countryVersion=*
- ITK DigitalModem country codes:

Country	Coding	Code
US & Canada	µ-law	0x1
Taiwan	µ-law	0x103
International	a-law	0x200
Italy	a-law	0x201
Holland	a-law	0x205
Israel	a-law	0x206
Belgium	a-law	0x207
France	a-law	0x209
Sweden	a-law	0x210
Norway	a-law	0x211
Denmark	a-law	0x212
South Africa	a-law	0x213
Singapore	a-law	0x214
Austria	a-law	0x216
Germany	a-law	0x217
Switzerland	a-law	0x219
Russia	a-law	0x224
Turkey	a-law	0x227
Spain	a-law	0x231
Malaysia	a-law	0x234
Finland	a-law	0x237
Ireland	a-law	0x238
Portugal	a-law	0x241
Poland	a-law	0x253
Czech Republic	a-law	0x255
India	a-law	0x268
China	µ-law	0x273
International	µ-law	0x300
UK	a-law	0x400
Australia	a-law	0x402
New Zealand	a-law	0x403
Cyprus	a-law	0x417
Japan	µ-law	0x500

Set MVIP-Master and D-Channel parameters of ITK Primary adapters

- *cd /usr/itk/ixload*

- *vi ix1.ini*

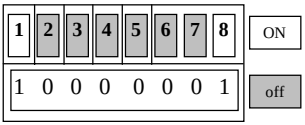
For each paragraph ITK Primary adapt the lines
mvipType= , voiceCoding= , dProtocol= ,
and whatever else is appropriate for your site.

For more than one ITK primary you **must** set the mvipType-Parameters, for only one adapter this is optional.

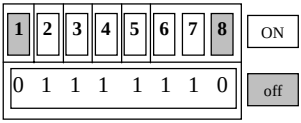
For US protocol ***T1*** enter the correct values for
lineRate= , lineCode= , framingFormat= and *dsxPreemphasis= .*

Check the on-board-settings for *E1/T1* of the ITK primary board

Setting for E1 connection:



Setting for T1 connection:



Please pay attention to use the right cable for E1 (RJ-48/RJ-45) resp. T1 (RJ-48/RJ-48).

Change keyboard layout

- Login as root (Password *itk*)
- Start *scoadmin*
- System ⇒ International Settings Manager
- Select Language and Keyboard as necessary

E.7.4 Others

- Login as root, Password itk and enter SINGLE-USER mode with ***init S***

- Enter new SCO-License (if applicable):
  - start *scoadmin*
  - *License Manager*
  - Select Product *SCO OpenServer Desktop System*
  - *remove License* ⇒ Yes
  - *License Product*
  - Enter license data and code as appearing on SCO license certificate
- Logout to leave single-user mode
- Copy applying registration card with „Activation Key“
- **Note SCO-Serial Number here:** _____
- **The NetBlazer license data has to be edited in** */u/pra/dat/misc.par***. Note them here:**

  _____:_____

  _____:_____

  _____:_____

  _____:_____

Remove files

- Login as pra, Password pra
- *pramon*
  - ***5*** : Shutdown
  - Change shutdown-state ? (y/n)***y***
  - ***1***-normal (User-caused)
  - `timeout [s]` ***0*** (inactivity timeout in sec.)
- **Change to directory /u/pra/log with *log***
- *rm -rf **

Reset operation counter and power down

- Login as root, Password itk

- insert disk with „hardware counter reset program“ into floppy disk drive
- ***reboot***
- Wait until computer is rebooted to DOS
- set_rtm
- Wait for completion message and switch system power off
- Write NetBlazer 8500 name on package.

Remount system cover

For shipment into USA change the power supply

- **Change voltage selection switch to 110V**

E.8 Check List

Computer	
Power cable	
Debug cable (mounted)	
3com EtherLink XL 3c900 PCI Configuration Disk (DOS based)	
RJ-45/RJ-48C and RJ-48/RJ-48 cables	
SCO-License	
Kontron KPR ITK II- User Manuals	
AMI-BIOS User Manual	
PIC Pentium CPU-Board Hardware Description	
NetBlazer 8xxx manual (if applicable)	
Copy installation script	
Update installations list	
Ship computer (delivery note-pretext, delivery note, forwarding agent)	

Date: _____

Installed by: _____

Signature: _____

Shipping date: _____

Appendix F Year 2000 compliance

F Year 2000 compliance

This feature has become an issue in the computer industry. Without Year 2000 compliance, computer products with internal clocks will have difficulties at the turn of the century.

ITK NetBlazer 8500 has been tested for year 2000 compliance without any problems. That means that neither performance nor functionality is affected by dates prior to, during and after the year 2000.

All references of the year are extended from 2 to 4 digits (Especially in the accounting- and logging-files).

Index

Bold page numbers contain detailed information.

Symbols

Numerics

A

B

C

D

E

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X