

**BLACK BOX Catalogue Ltd**  
The Source for Connectivity



ISU9930 : Base Unit 2 Line Support  
ISU9931 : Fail Safe Relay Option  
ISU9932-SNMP : SNMP Option  
ISU9932-3PRI : 3<sup>rd</sup> Line Software Key  
ISU9932-4PRI : 4<sup>th</sup> Line Software Key  
ISU9932-CODE : Software Upgrade to Latest Code Version

## IntelliShare User Guide



**TECHNICAL:** (0118) 931 2233  
**SALES:** (0118) 965 5100  
**FAX:** (0118) 931 1727  
**ADDRESS:** 15 Cradock Road, Reading, Berkshire RG2 0JT  
**WEB:** [www.blackbox.co.uk](http://www.blackbox.co.uk)



## How To Contact your Local Black Box

**Austria:****Black Box gmbh****Tel: 01 256 98 56****Fax: 01 256 98 50-100****Web Site: [www.black-box.at](http://www.black-box.at)****Sweden:****Black Box AB****Tel: +46 8 44 55 870****Fax: +46 8 38 04 30****Web Site: [www.Blackbox.ab.se](http://www.Blackbox.ab.se)****France:****Black Box Catalogue****Tel: 01 45 60 67 00****Fax: 01 45 60 67 47****Web Site: [www.blackbox.fr](http://www.blackbox.fr)****Italy:****Black Box Italia s.p.a .****Tel: 02 27404 280****Fax: 02 27400 219****Web Site: [www.blackbox.it](http://www.blackbox.it)****Deutschland:****Black Box Deutschland****Tel: 0811/5541-0****Fax: 0811/5541-499****Web Site: [www.blackbox-deutschland.com](http://www.blackbox-deutschland.com)****Denmark:****Black Box Denmark****Tel: +45 5663 3010****Fax: +45 5665 0805****Web Site: [www.blackbox.dk](http://www.blackbox.dk)****Switzerland:****Black Box (Schweiz) AG****Tel: 055 451 70 70****Fax: 055 451 70 75****Web Site: [www.black-box.ch](http://www.black-box.ch)****Spain:****Black Box Comunicaciones S.A.****Tel: 91 659 0191****Fax: 91 623 9784****Web Site: [www.blackbox.es](http://www.blackbox.es)****Netherlands:****Black Box Datacom BV****Tel: 03032417700****Fax: 0302414746****Web Site: [www.blackbox.nl](http://www.blackbox.nl)****Belgium:****Black Box Communications S.A. N.V.****Tel: 02 725 85 50****Fax: 02 725 92 12****Web Site: [www.blackbox.be](http://www.blackbox.be)**

**Norway:**

**Black Box Norge as.**

**Tel: +47 55 300 700**

**Fax: +47 55 300 701**

**Web Site: [www.blackboxnorge.no](http://www.blackboxnorge.no)**

**Finland:**

**Black Box Finland Oy.**

**Tel: +358 (0) 201 888 888**

**Fax: +358 (0) 201 888 808**

**Web Site: [www.blackbox.fi](http://www.blackbox.fi)**

**U.S.A. :**

**Black Box Corporation**

**Tel: 724-746-5500**

**Fax: 724-746-0746**

**Web Site: [www.blackbox.com](http://www.blackbox.com)**

**Chile:**

**Black Box Chile**

**Tel: 00 562 6680 141**

**Fax: 00 562 6680 140**

**Web Site: [www.Blackbox.cl](http://www.Blackbox.cl)**

**Brazil:**

**Black Box Do Brasil.**

**Tel: (011) 5515-4000**

**Fax: (011) 5515-4002**

**Web Site: [www.blackbox.com.br](http://www.blackbox.com.br)**

**Australia:**

**Black Box Network Services Australia P/L**

**Tel: 03-9879-7100**

**Fax: 03-9870-2955**

**Web Site: [www.blackboxoz.com.au](http://www.blackboxoz.com.au)**



**SALES : 0870 90 10 750**

## Table of contents

<b>GENERAL DESCRIPTION.....</b>	<b>7</b>
INTRODUCTION.....	7
SAFETY CONSIDERATIONS .....	7
UNPACKING.....	8
SELECTING A SITE.....	8
INSTALLATION AND CONNECTION PRECAUTIONS.....	8
<b>PREFACE .....</b>	<b>9</b>
HOW TO USE THIS GUIDE .....	9
WHAT'S IN THE INTELLISHARE PACKAGE.....	9
OPTIONS.....	9
LED'S AND CONNECTORS ON THE INTELLISHARE.....	10
<b>GETTING STARTED.....</b>	<b>11</b>
THE COMMAND LINE AND THE SCREEN INTERFACE.....	11
THE WORLD ACCORDING TO INTELLISHARE.....	14
MOVING IN AND AROUND THE CONFIGURATION SCREENS. EDITING FIELDS.....	14
ACTIVATING AND RESTORING CONFIGURATIONS.....	15
THE FACTORY DEFAULTS.....	16
<i>The System configuration:</i> .....	17
<i>The Slot configuration:</i> .....	17
<i>The Line configuration:</i> .....	17
<i>The FixN64 configuration</i> .....	18
<i>The Route configuration:</i> .....	19
<i>The Operator configuration:</i> .....	19
<b>THE BASIC FACTORY APPLICATION.....</b>	<b>20</b>
CHECK YOUR CONFIGURATION AND YOUR PHYSICAL CONNECTION.....	22
CHECK THE DATALINK. SETTING THE TRACING LEVEL.....	23
ALARM FORWARDING.....	24
CHECK THE NETWORK LINK, TRYING OUT.....	25
STATUS SCREENS.....	25
FINAL COMPATIBILITY CHECKS .....	26
<b>SW UPGRADE &amp; SOFTKEY OPTIONS.....</b>	<b>27</b>
LOCAL SW UPGRADE ON THE INTELLISHARE .....	27
REMOTE SOFTWARE UPGRADE.....	28
SOFTKEY OPTIONS: VERIFICATION AND ACTIVATION .....	28
<b>MANAGING THE INTELLISHARE VIA THE LAN.....</b>	<b>31</b>
CONFIGURING AND INSTALLING FOR LAN ACCESS.....	31
BASIC TESTS FOR IP CONNECTIVITY .....	32
TELNET ACCESS TO INTELLISHARE.....	33
<b>PR-REDIAL: LEAST COST ROUTING USING CARRIER PREFIX.....</b>	<b>35</b>
THE APPLICATION.....	35
THE CONFIGURATION.....	35
ROUTING SCHEMES. RULES FOR MATCHING AND REPLACING PATTERNS.....	36
TESTING AND VERIFYING STATUS.....	36
<b>SAVING AND RESTORING CONFIGURATIONS WITH XMODEM.....</b>	<b>39</b>
<b>REMOTE CONTROL.....</b>	<b>42</b>
<b>MANAGING THE INTELLISHARE WITH A WEB BROWSER.....</b>	<b>48</b>
CONFIGURING YOUR BROWSER.....	48



THE INTELLISHARE WEB SERVER .....	49
<i>IntelliShare Home page</i> .....	49
<i>IntelliShare configuration, status and history pages</i> .....	49
REMARKS .....	51
<b>PR-SHARE: SHARING A SINGLE PRI WITH MULTIPLE USERS.....</b>	<b>52</b>
THE APPLICATION.....	52
THE CONFIGURATION. ....	52
RESTRICTING BANDWIDTH .....	53
<b>PR-CHOICE: LEAST COST SWITCHING TO AN ALTERNATIVE PRI.....</b>	<b>55</b>
THE APPLICATION.....	55
CONFIGURATION. ....	55
CLOCK SYNCHRONIZATION ISSUES. ....	56
<b>ADVICE OF CHARGE GENERATION .....</b>	<b>58</b>
WHAT IS ADVICE OF CHARGE ALL ABOUT? .....	58
GENERATION OF AOC BY THE INTELLISHARE. ....	58
CONFIGURING THE INTELLISHARE FOR GENERATING ADVICE OF CHARGE.....	59
CRITERIA FOR SELECTING A CHARGING PROFILE. ....	63
<b>CALLING LINE IDENTIFICATION(CLIP).....</b>	<b>64</b>
CONTROLLING THE CALLING LINE IDENTIFICATION (CLIP).....	64
<i>Using a CLI check on incoming calls</i> .....	64
<i>Controlling the CLI of outgoing calls</i> .....	65
<b>THE INTELLISHARE AS IP-ROUTER.....</b>	<b>66</b>
THE APPLICATION .....	66
THE CONFIGURATION .....	66
<i>Connecting to the Internet through a 64 kbit ISDN dial-up connection</i> .....	66
<i>Configuring your LAN for Internet access through the IntelliShare</i> .....	68
<i>Connecting to the Internet through a Fractional E1 leased line</i> .....	70
<i>Troubleshooting your Internet connection</i> .....	72
HOW TO SECURE YOUR NETWORK FROM MALICIOUS ATTACKS.....	73
ADVANCED IP-ROUTER CONFIGURATION.....	75
<i>Configuration of static routes</i> .....	75
<i>Enabling Port Forwarding on the IntelliShare</i> .....	75
REMARKS .....	76
<b>SNMP.....</b>	<b>77</b>
CONFIGURING THE INTELLISHARE FOR SNMP: BASIC SETTINGS.....	77
INSTALLATION AND VERIFICATION.....	77
ACCESSIBLE PARAMETERS. ....	79
TRAPS.....	79
<b>PR-COMBI: FRACTIONAL E1 AND ISDN ON A SINGLE PRI.....</b>	<b>80</b>
APPLICATION.....	80
CONFIGURATION. ....	80
<b>VXI MODULE: FRACTIONAL E1 ON A V35, V36 OR X21.....</b>	<b>82</b>
THE APPLICATION.....	82
ENABLING THE VX PORTS.....	82
V35, V36 AND X21 CABLES.....	83
CONFIGURATION. ....	83
<i>Example</i> .....	83
<i>Status indications and LED behaviour</i> .....	84
<i>Maintenance conditions</i> .....	85
SW UPGRADE ON THE VXI MODULE.....	85
<b>OTHER APPLICATIONS.....</b>	<b>86</b>



SALES : 0870 90 10 750

# Declaration of Conformity

issued according to ISO/IEC Guide 22 and EN45014 under the sole responsibility of the manufacturer

BLACK BOX declares that the product:

**Product name**

IntelliShare

provided that it is installed, maintained and used in the application for which it is intended for, with respect of the “professional practices“, relevant installation standards and manufacturer’s instructions is in conformity to all applicable essential requirements of all applicable directives and conform to the following Product Specifications:

- EN60950 : 1992 (A1+A2+A3) Class II
- EN55022 : 1994 (A1+A2:1997) Class B
- EN50082-1 : 1992

complies with the provision of the **R&TTE** Council Directive **1999/5/EC** annex II.

The product may be connected to the following EEC Operators Recognised Interface(s):

I-411, I-412, I-431, G703, G704, Q931, Q932

The product is compliant with:

TBR4

Additional information: The product has been tested in a typical configuration.  
The Technical File is kept at the Manufacturer’s Premises:  
15 Cradock Road, Reading, Berkshire RG2 OJT

March 2001



<b>Statement:</b>	The IntelliShare may be used in the European Community provided that it is installed , maintained and used in the application for which it is intended for , with respect to the professional practice , relevant installation standards and manufacturer's instructions (see also CE declaration of conformity).
<b>Destination of use:</b>	The IntelliShare allows direct connection of PRI and 10-BaseT Ethernet LAN
<b>Restricted use:</b>	No function featured by the IntelliShare is of restricted use in the European Community.
<b>Interfaces:</b>	The IntelliShare may be connected to the following EEC Operators Recognised Interfaces:I-411, I-412, I-431, G703, G704, Q931, Q932.
<b>Verklaring:</b>	De IntelliShare mag gebruikt worden binnen de Europese Gemeenschap op voorwaarde dat het wordt geïnstalleerd , onderhouden en gebruikt voor de toepassing waarvoor het ontworpen is , met betrekking tot het professioneel gebruik , de relevante installatie richtlijnen en de richtlijnen van de fabrikant (zie ook de CE verklaring van conformiteit).
<b>Toepassingsgebied:</b>	De IntelliShare laat directe verbinding toe met PRI en 10-BaseT Ethernet LAN.
<b>Beperkt gebruik:</b>	Er is geen enkele functie aanwezig op de IntelliShare die niet gebruikt mag worden binnen de Europese Gemeenschap.
<b>Interfaces:</b>	De IntelliShare mag aangesloten worden op de volgende door de EEC operatoren erkende interfaces: I-411, I-412, I-431, G703, G704, Q931, Q932.
<b>Déclaration:</b>	L' IntelliShare peut être employé dans la Communauté Européenne à condition qu'il soit installé, entretenu et utilisé dans la fonction pour laquelle il a été conçu, en suivant les règles de pratique professionnelles, les standards d'installation d'application et les instructions du fabricant (voyez aussi la déclaration CE de Conformité).
<b>Domaine d'utilisation:</b>	L' IntelliShare permet la connexion directe de PRI et de 10-BaseT Ethernet LAN.
<b>Restrictions d'usage:</b>	Aucune restriction d'usage n'est d'application dans la Communauté Européenne en ce qui concerne les fonctions offertes par le IntelliShare.
<b>Les interfaces:</b>	L' IntelliShare peut être connecté aux Réseaux des Opérateurs de la CEE offrant les Interfaces reconnues suivantes: I-411, I-412, I-431, G703, G704, Q931, Q932.
<b>Erklärung:</b>	Der IntelliShare darf in der europäischen Gemeinschaft benutzt werden, vorausgesetzt, er wird installiert, unterhalten und in der Funktion benutzt für die er entwickelt wurde, in dem die Regeln der Berufsausführung, sowie die vorgeschriebenen Installationsstandards und die Anweisungen des Fabrikanten berücksichtigt werden (siehe hierzu die Konformitätserklärung der EG).
<b>Anwendungsbereich:</b>	Der IntelliShare erlaubt die direkte Verbindung PRI und 10-BaseT Ethernet LAN.
<b>Anwendungsbeschränkung:</b>	In der europäischen Gemeinschaft gibt es keine Anwendungsbeschränkung bezüglich der Funktionen die der IntelliShare bietet.
<b>Verbindung:</b>	Der IntelliShare darf an die Operatorennetzwerke der EWG angeschlossen werden die folgende 'Interfaces' bieten: I-411, I-412, I-431, G703, G704, Q931, Q932.
<b>Declaración:</b>	El IntelliShare puede usarse en la Comunidad Europea con tal de que sea instalado, mantenido y usado en la aplicación para la cual ha sido destinado ,con el respeto del las prácticas profesionales, normas de la instalación pertinentes e instrucciones del fabricante (también vea declaración de CE de Conformidad).
<b>Destino de uso:</b>	El IntelliShare permite la conexión directa de PRI, redes Ethernet 10BaseT LAN.
<b>Uso restringido:</b>	Ninguna función ofrecida por el IntelliShare es de uso restringido en la Comunidad Europea.
<b>Interfaces:</b>	El IntelliShare puede conectarse a los Operadores de la CEE que ofrezcan los siguientes sinterfaces reconocidos: I-411, I-412, I-431, G703, G704, Q931, Q932.
<b>Dichiarazione:</b>	Il IntelliShare può essere usato nella Comunità Europea a condizione che sia installato, mantenuto ed usato nella applicazione per la quale è destinato, con rispetto delle pratiche professionali, degli standard di installazione attinenti e delle istruzioni del Costruttore (vedere anche la dichiarazione CE di Conformità).
<b>Destinazione di uso:</b>	Il IntelliShare permette il collegamento diretto di PRI, reti 10-BaseT Ethernet LAN.
<b>Uso ristretto:</b>	Nessuna funzione offerta dal IntelliShare è di uso ristretto nella Comunità Europea.
<b>Interface:</b>	Il IntelliShare può essere collegato agli Operatori di Telecomunicazione della CEE che offrono le seguenti interfacce: I-411, I-412, I-431, G703, G704, Q931, Q932.



**SALES : 0870 90 10 750**



## General description

### Introduction

Congratulations with the acquisition of your **IntelliShare: the BLACK BOX smart PR ISDN multiplexer**.

This equipment has been designed and produced by BLACK BOX according to our ISO 9001 certified quality system to assure a first quality and highly reliable product.

The IntelliShare is a smart ISDN multiplexer with up to 4 PRI interfaces and the capabilities to perform a wide range of applications. This unit can be used to perform **least cost routing** (LCR) on 1 or 2 PRI.

It can combine the LCR function with the sharing of a single PRI line from the network between 2 or 3 ISDN PRI based terminals.

The unit can also be configured to perform **least cost switching** (LCS), where it then switches ISDN calls to 2 different directly connected service providers.

Because of its **built-in TDM cross connecting functions**, one can also use the IntelliShare as a mini (4x4) crossconnect or to combine FE1 circuits with FPRI services on a single 2Mbits/s access line.

Finally, its **IP-Router** functionality makes it possible to connect a LAN transparently to the Internet over a dial-up or FE1 link.

### Safety considerations

The following safety considerations apply to the IntelliShare equipment:

Power adapter:	use only:	AC/DC: HITRON HES 40B-10 DC/DC: POWERTECHNICS PT314
Power cord:	use only:	HO5 VV F 3G 075 cord
Circuit classification:	PRI .. PR4:	TNV1
	Control:	SELV
	Ethernet:	SELV

#### **IMPORTANT SAFETY INSTRUCTIONS**

Unplug the unit from the wall power outlet before installing.

To assure the safety of this product, the protective earth terminal on the equipment's backpanel must be connected to earth. Properly fix an eyelet at the end of an earth wire of at least 0.75 mm<sup>2</sup>. Fasten the eyelet tightly to the terminal by means of the appropriate screw.

#### **SAFETY WARNING**

To avoid damage to the equipment, please observe all procedures described in this chapter.

Ensure that the unit and its connected equipment all use the same AC power and ground, to reduce noise interference and possible safety hazards caused by differences in ground or earth potentials.

## Unpacking

Rough handling during shipping causes most early failures. Before installation, check the shipping cardboard box for signs of damage. If the box is damaged, please place a claim to the carrier company immediately.

## Selecting a site.

### **WARNING**

Always place the unit on its feet without blocking the air vents.

Do not stack multiple units directly onto each other, as stacking can cause heat build-up that could damage the equipment.

Install the unit in an area free of extreme temperatures, humidity, shock and vibration.  
Position it so that you can easily see and access the front panel and its control indicators.  
Leave enough clearance at the back for cables and wires.  
Position the unit within the correct distances for the different accesses and within 2m of a power outlet.

## Installation and connection precautions.

- The installation of this equipment is to be performed by qualified service personnel.
- The content of this document is directed towards qualified service personnel.

### **ESD WARNING**

The circuit boards are sensitive to electrostatic discharges (ESD) and should be handled with care. It is advisable to ensure an optimal electrical contact between yourself, the working area and a safety ground before touching any circuit board. Take special care not to touch any component or connector on the circuit board.

### **EMC WARNING**

#### **EMC compliant installation**

The complete IntelliShare is fully EMC compliant. To ensure compliance with EMC directive 89/336/EEC, shielded cables have to be used.

### **NOTE**

This equipment may be powered by an IT power system.



## Preface

### How to use this guide

This User Guide has been organised as a series of hands-on sessions. We have tried to introduce only those elements that you need in order to obtain the desired result. You should use the Reference Guide (appendix to this User Guide) to obtain detailed information.

To start working with the IntelliShare, you need the following materials:

- The IntelliShare package.
- A PC with a serial (COMx) and a LAN interface.
- ISDN cables, LAN cables, maybe also a HUB.
- Access to one or more Primary Rate Interfaces.

If you use a real-world PRI interface, you should consider informing the PRI provider that you are going to do some testing so that he knows where the alarms come from. Those tests that require co-operation of the PRI provider will be indicated.

### What's in the IntelliShare package.

When you open the IntelliShare package, you should find the following elements:

- The IntelliShare box.
- An external power adapter with a power cord.
- This User Guide and Reference guide.
- A floppy disk containing an electronic copy of User and Reference guide (MANUAL), the current SW (binary BIN format and compressed CPR format), and the current MIB.

In addition, you should have ordered a set of ISDN cables. The exact amount and type of cables depend on your specific application. Have a look at the product codes on the ISDN cables:

- EIU146567 :           Straight ISDN cable 2.0 m to connect to the ISDN network.
- EIU153297 :           Crossed ISDN cable 2.0 m to connect to PR ISDN terminals.

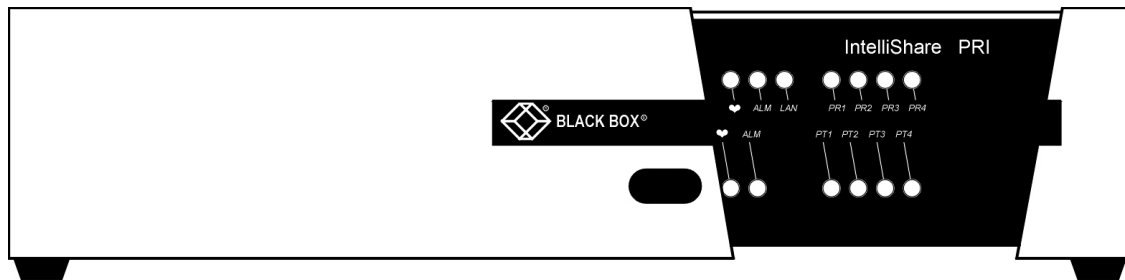
The Reference Guide shows the layout of these cables.

### Options.

When purchasing the IntelliShare, you should have selected some Software and Hardware Options. Be sure to have this information within reach. The verification and activation of options will be discussed later when it is needed.

In some cases, the IntelliShare may be equipped with a second card that is inserted in the lower half of the box. This can be either a Fail-Safe Relay Card or another extension card. Please refer to the respective manual appendices for these extensions.

## LED's and connectors on the IntelliShare.

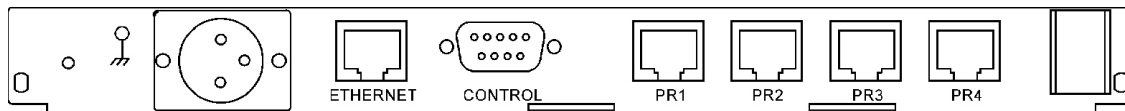


The front side features a number of LED indicators for the following functions:

- Heart beat: when the IntelliShare is operational, this LED beats in a 1-second rhythm.
- Alarm LED: this LED turns red when there is some error that renders the equipment non-operational.
- LAN LED: the LED turns green when the LAN is detected.
- PRI LED's: these tricolour LEDs indicate the physical status of the PRI lines. Green is normal, orange indicates reception of a remote alarm (RAI), and Red indicates other error conditions. If the LED is not green, then the corresponding PRI line is non-operational.

You may notice that the heart beat LED takes a long time (30 seconds) to come up. This is normal behaviour and will be explained later.

The backside features connectors for the PRI lines, the LAN connection, and a serial RS-232 connection.



## Getting started.

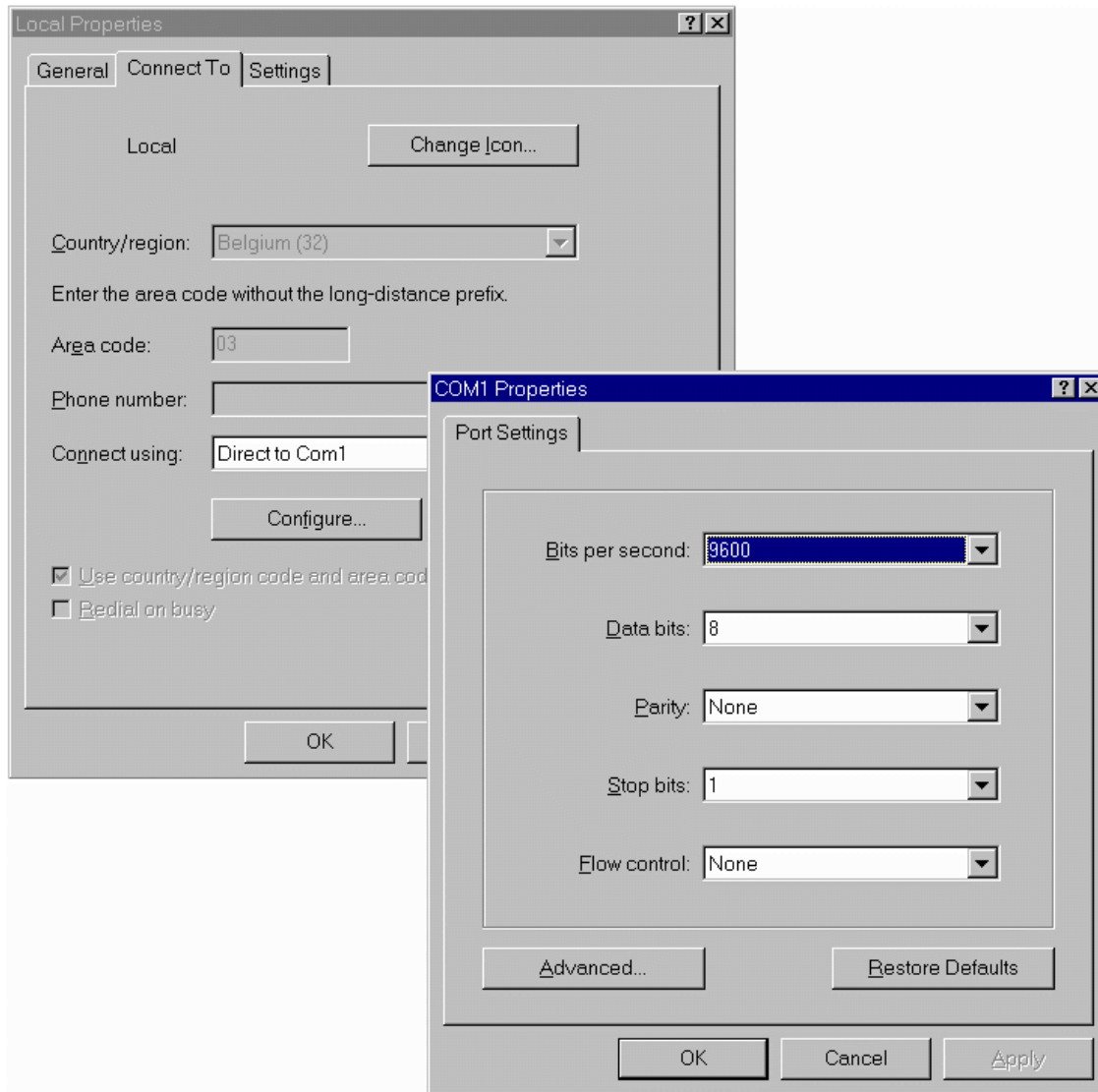
### The command line and the screen interface.

To start interacting with the IntelliShare, connect a (straight) serial cable from your PC to the Control Port, and use the following settings on your terminal emulation program:

9600 baud, 8bit, no parity, 1 stop bit, NO flow control.

In addition, select ANSI emulation with transmission of the function keys.

On a Win98 PC with Hyper-Terminal this results in the settings shown below.



Your first interaction with the IntelliShare may be something like this

```
                                -- ignore the boot messages before this
<enter>
? LOGIN
LOGIN ADM ADM <enter>
OK
<enter>
? LOGIN LOGOUT WIN SHOW CFG SET RESET MAINT REM
SHOW <enter>
SHOW ? TIME CFG STS HISTORY ID LOG
SHOW TIME <enter>
12:06:51,1999/03/22
SH TI <enter>
12:06:56,1999/03/22
SH ID <enter>
PRTA5314 4.1 (PMX)

PCode: PRTA/4000 1.1
Model: IntelliShare MPR-4
SerNr: 09700167
MacNr: 00E0DE FFFFE
                                -- <enter> stands for pressing the enter key
```

What you see is the command line interface of the IntelliShare. For this first example, we have explicitly indicated when you need to press the enter key. In the remainder of this manual, we will assume that you press enter when needed.

Note the following features of the command line interface:

- When you press <enter>, the IntelliShare will try to execute a command. If it does not find enough information, it prints out a help line starting with the part of the command that was understood, then a question mark, and then a list of words that it expects as valid continuation of the command. So, initially the IntelliShare shows that it expects you to log in, when you press 'show' with no arguments, then the IntelliShare shows the list of expected arguments.
- You can abbreviate commands. The rule is that you need to give enough of the word to make its interpretation unique. So you can use 'SH' for 'SHOW', but you cannot use 'S' because the IntelliShare does not know if you mean 'Show' or 'Set'.
- You can use the Up and Down arrow keys to call back previous lines.

This short example also shows you a few aspects of the IntelliShare:

- You need to log in. The different possibilities and restrictions will be explained later. For now just log in as the factory default administrator ADM.
- You can obtain information on the software release, the serial number of the product and some other identification elements using the command 'show id'. You will need this information whenever you need support with your IntelliShare.
- If the time is not correct then set it using the command SET TIME. By now, you should have learned enough to know how to do it.



One of the most used commands also happens to be one of the simplest: 'WIN'. This command gives you access to the configuration and status screens.

Type it in and follow the annotated example.

```

WIN <enter>          -- this calls the top level menu.

WIN
+-----+
| CFG          |          -- CFG is highlighted. With the arrow keys, you can
| STS         |          -- change the selected item.
| HISTORY     |
+-----+

                -- select CFG pressing <enter>.

CFG
+-----+
| Sys         |          -- you can move the selection using the arrow keys
| Slot       |
| Line       |
| FixN64     |
| Route      |
| Clip       |
| AOC_Profile|
| AOC_Holiday|
| Oper       |
| PPP        |
| IP_StatRoute|
| IP_PortFW  |
+-----+

                -- go back using the <esc> key. Or use <ctrl-X>

WIN
+-----+
| CFG        |
| STS       |
| HISTORY   |
+-----+

                -- go back using the <esc> key. Or use <ctrl-X>

OK

```

**Important:** Depending on the software key options you have purchased (see also chapter 0 on page 27), some of the menu options might not be visible on your IntelliShare. Throughout this manual, each screen snapshot shown applies to a IntelliShare with ALL software options installed.

There are a few things to be remarked here:

- The <esc> key may not work on your PC. Maybe you have an AZERTY keyboard and have CAPS-LOCK on, or your emulator does not support use of the <esc> key. In that case, use <ctrl-X> (pressing control and X simultaneously) to exit from the current level.
- When pressing the <esc> key twice in rapid succession, nothing happens at all. Indeed, the <esc> key cannot be correctly distinguished from the ANSI escape sequences unless there is some idle time after it. Be patient or use the <ctrl-X> key.

When referring to a sub menu or to a field in a sub screen, this will be indicated like this:

**WIN.CFG.SYSTEM.IP**

The above example refers to the configuration item that you can access by typing WIN first, then selecting CFG, then selecting System, and then finally moving to the IP field.

The instruction to set this field to a specific value will be given like this:

**WIN.CFG.SYSTEM.IP := 192.168.3.1**

**The world according to IntelliShare.**

Take a look at the items on the WIN.CFG menu. These items classify the building blocks used by the IntelliShare. Each class is really a small database:

Sys	This is a collection of general settings that have a system wide impact.
Slot	Each card in the IntelliShare is placed in a slot, and is assigned a slot number. The basic IntelliShare which consists of a single card (called MPR for multiple primary rate) is assigned slot 1. The extension card, if any, is placed in slot 2.
Line	The name line is used to indicate a PRI or E1 interface. There are 4 lines that can be individually configured.
FixN64	The name port is used to indicate a nailed-up datastream. There may be up to 64 nailed-up datastreams that may be individually configured.
Route	The route specifies how an ISDN call should be re-routed and redialed. There may be up to 300 route definitions.
Clip	Label is a name identifying a group of CLIP checks, Search and Replace are used in the same manner as in the route table, but work on the CGN information element
AOC_Profile	The AOC profile defines the charging pattern to be applied to a call, generated when Advice Of Charge is enabled. This entry will only be shown if you have the Advice Of Charge software option
AOC_Holiday	The AOC Holidays let you define the dates of the holidays for which a special charging profile can be configured. This entry will only be shown if you have the Advice Of Charge software option
Oper	The operator represents a user of the IntelliShare. Each user has an associated set of rights that determine the actions that are allowed. There may be up to 8 operators
PPP	The PPP entry defines various parameters to set up a PPP (Point to Point Protocol) - connection.
IP_StatRoute	The IP_StatRoute entry allows you to define how IP traffic is to be routed to the interfaces of the IntelliShare. This entry will only be shown if you have the IP routing software option
IP_PortFW	The IP_PortFW entry allows you to define how incoming IP traffic for certain IP services need to be sent to, in the case IP Masquerading is set. This entry will only be shown if you have the IP routing software option.

**Moving in and around the configuration screens. Editing fields.**

The IntelliShare provides two distinct views of the configuration databases:

- A browser oriented view. This shows multiple data entries on a single screen, be it with reduced information per record. The goal is to provide a quick overview and access.
- A record oriented view. This shows a single record with all available information.

As an example, select the route configuration screen (WIN.CFG.ROUTE).

This will show a configuration screen as shown below. Up to 10 entries are shown on a single page.

```

-Route-----0001--
N  Act  LineISearch      Replace      LineOCalltyp  FailMin
1   On   1--- *              *            -2-- ----- 0
2   On   -2-- *              *            1--- ----- 0
3   Off  ----              *            ---- ----- 0
4   Off  ----              *            ---- ----- 0
5   Off  ----              *            ---- ----- 0
6   Off  ----              *            ---- ----- 0
7   Off  ----              *            ---- ----- 0
8   Off  ----              *            ---- ----- 0
9   Off  ----              *            ---- ----- 0
10  Off  ----              *            ---- ----- 0
    
```





Moving the cursor up and down allows selecting other entries. You can move up or down a whole page at once using the keys <ctrl-F> (forward) and <ctrl-B> (backward).

With the <tab> key, the next field of an entry can be selected. Within the field you can use the arrows to move over the contents.

This screen shows all the basic types of configuration fields that are available on the IntelliShare, so this is a good moment to try your editing skills.

First go to entry 3 (N=3), and use the <tab> character to go to the type field. This field is a choice field, and you can see the different choices by pressing the <spacebar>. Select the 'On' choice.

Use <tab> to go to the next field, then use the right arrow to go to the third dash. When you press the <spacebar>, a '3' will be indicated. Pressing again will bring back the '-'. This is a bitmap field and allows specifying a set of on/off choices. The value '3' is just a reminder to indicate that you are changing the third element.

Use tab to go to the next field. This is a text entry field, where you can enter a search pattern. For now, enter your name, then erase it again. There is no error checking on this kind of field.

Finally, go to the last field (which is a numeric field), and enter a value. You will note that the values are automatically corrected when you leave the field. Non-numeric values are replaced by 0 and numeric values are limited to their range. Try to enter 99 for example.

The same actions are also possible in the record view.

To obtain this view press F2, or <ctrl-W> (window) to obtain a window like this.

```

--Route-----0002--
N      2
Act    On
LineIn -2--
Search *
Replace *
LineOut 1---
Calltyp -----
FailMin 0
ChgProf
CliProf

```

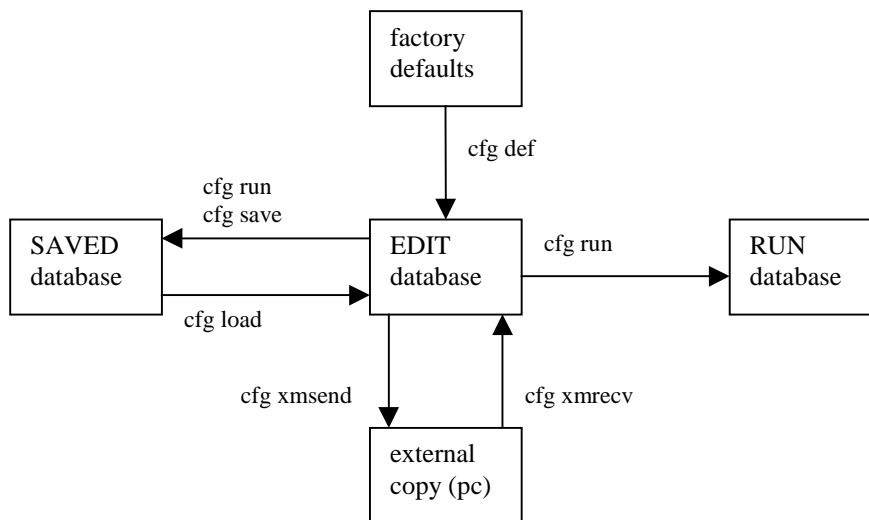
This view only shows the entry with index 2, but then it is a little more eloquent. Use the forward and backward commands (<ctrl-F> and <ctrl-B>) to go to the next or previous page. This time the jump is only 1 entry.

To go to route entry 145, the best thing to do is to use a sequence of <ctrl-F> commands in the browser view until you can place the cursor on entry N=145. Then switch to the record view and do whatever is needed on this entry.

### Activating and restoring configurations.

After all the changes you have made to the configuration, you may be wondering if you will ever get to the original state again. Well, the answer is yes.

First of all, all changes have been made to a "EDIT" copy of the configuration, which is different from the active ("RUN") configuration. To make it even more challenging, there is a third copy of the configuration, which is stored in flash memory. There are a number of commands that allow you to manipulate these copies, as shown here.



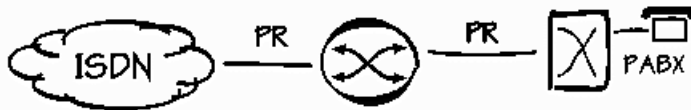
In general, you will either use the command CFG RUN to save and activate the new configuration, or the command CFG LOAD to revert to the previous configuration.

If things go really wrong, you can always reload the factory default by using the command CFG DEF.

### The factory defaults.

The factory defaults provide the basic configuration needed to be as transparent as possible.

This means that you should be able to place the IntelliShare between a PABX and the Public Network, and still be able to do all phoning as before: the IntelliShare will only forward calls with no modifications at all.



Before doing this, let us first look at the different screens and check their most important parameters.

To ensure that the factory defaults are loaded, perform the following tasks:

```

cfg def                                -- load defaults in edit base
OK
cfg run                                -- save and activate edit base
Activated
reset sys                              -- reboot the system
> BOOT PRTA5314 4.1
> ...
  
```

The reboot ensures that all changed settings are activated.



*The System configuration:*

```

-Sys-----
N          1
Type      MPR                AOCType  AOC-D
Name      PMX                AOCTyp  Unit
Log       20                 AOCCurr
Trp       50                 AOCMult 0.001
IP        192.168.004.001    IPRoute Off
SubMask   255.255.255.000    Masq    Off
Gateway   000.000.000.000    MasqIP  000.000.000.000
PrimMgr   000.000.000.000    RCNetIP 000.000.000.000
SecdMgr   000.000.000.000    RCMask  000.000.000.000
RdComm    public
WrComm    netman
TrpComm   trap
TLogOff   0
TFailSf   20
ClkSlve   AUTO
AlmTime   00:00:00
HttpRef   0
AOEnbl    Off

```

Most parameters are concerned with the LAN and Remote Management features of the IntelliShare, and will be considered further. At this time, the defaults are all we need.

There are two parameters that you may need to understand at this moment:

- **TLogOff:** this parameter specifies the maximum idle time in seconds before local control and telnet sessions will be disconnected. Set this value to 0 if you don't want to be disconnected during your tests. Set it to a value less than 240 seconds to be logged out after doing nothing during this time.
- **TFailSf:** this parameter specifies the boot start-up delay in seconds. This delay ensures that the operation of the equipment will be halted for at least TAFs seconds. Without this delay, the network would not necessarily be aware that the IntelliShare has been reset, and this might result in calls not broken down properly. If the network is ETSI compliant, then it will be able to correctly recover from a boot if the delay is set to at least 20 seconds. Otherwise, you may need to set the timer to a value up to 90 seconds. The reference guide gives a full account of the need for this start-up delay.

*The Slot configuration:*

```

-Slot-----0001--
N          1
Type      MPR
Name      S1

```

These parameters identify and name the different slots inside the IntelliShare.

*The Line configuration:*

```

-Line-----0001--
N Type Name          Act Sgn Tei NT Crc4
1 PR  TO NET         On  Isdn 0  TE NoCRC4
2 PR  TO USR         On  Isdn 0  NT NoCRC4
3 PR  L3             Off Isdn 0  TE NoCRC4
4 PR  L4             Off Isdn 0  TE NoCRC4

```

```

-Line-----0001--
N      1
Type   PR
Name   TO NET
Act    On
Sgn    Isdn
Tei    0
NT     TE
Idle   x49
Crc4   NoCRC4
StrInc 0
EndInc 0
StrOutg 0
EndOutg 0
AlmFrom ----
Options -----

```

The important parameters here at this moment (you don't need to change them) are:

- **Act:** this parameter specifies if the line can be used or not.
- **Sgn:** this parameter specifies if the line is connected to a network that allows signaling using ISDN. This will not be the case if the line is used for a pure Drop and Insert application.
- **NT:** This specifies the nature of the entity that is connected to the other side of the line. When the other side is the public network or some equipment behaving as a network, then this field should say 'TE'. That is, the line on the IntelliShare is configured as a ISDN Terminal Equipment (TE), whereas the other side (the network side) is configured as an ISDN Network Terminator (NT). In this case, the cable on this interface will most probably be a straight ISDN cable. When the other side is some user equipment, such as a PABX, then this field should say 'NT'. The cable on this interface will most probably be a crossed ISDN cable.
- **Crc4:** This parameter describes how the physical link is checked for quality. In many cases, the Network provides a PRI line that is not checked for quality. In this case, the CRC4 procedures do not apply, and the setting must read 'NoCRC4'. You should ask the PRI provider whether CRC4 is supported or not. Alternatively, you can try both possibilities as explained further.

#### *The FixN64 configuration*

```

-FixN64-----0001--
N Act Name          NrTLineITSILineOTSOPContrl
1 On  F1             8 L1  1  P1  1  ---
2 Off F2             0 NONE 1  NONE 1  ---
3 Off F3             0 NONE 1  NONE 1  ---
4 Off F4             0 NONE 1  NONE 1  ---
5 Off F5             0 NONE 1  NONE 1  ---
6 Off F6             0 NONE 1  NONE 1  ---
7 Off F7             0 NONE 1  NONE 1  ---
8 Off F8             0 NONE 1  NONE 1  ---
9 Off F9             0 NONE 1  NONE 1  ---
10 Off F10           0 NONE 1  NONE 1  ---

```

At this moment, since we do not use nailed-up channels, the default off setting is all we need.



*The Route configuration:*

```

-Route-----0001--
N  Act  LineISearch      Replace      LineOCalltyp  FailMin
1  On   1--- *              *            -2-- ----- 0
2  On   -2-- *              *            1--- ----- 0
3  Off  -----            ----- ----- 0
4  Off  -----            ----- ----- 0
5  Off  -----            ----- ----- 0
6  Off  -----            ----- ----- 0
7  Off  -----            ----- ----- 0
8  Off  -----            ----- ----- 0
9  Off  -----            ----- ----- 0
10 Off  -----            ----- ----- 0

```

The default provides two simple entries which have as effect that all calls coming in on line 1 are routed to line 2 with no modification, and vice versa.

The important parameters are:

- **Act:** On activates the entry, off ignores it.
- **LineIn:** This specifies that the route will be evaluated for calls that start at the indicated lines. Note that it is possible to specify routes that behave identically for several call sources.
- **LineOut:** This specifies the line to which the call will be routed whenever the route criteria are fulfilled.
- **Search:** This specifies a pattern that will be matched on the telephone number that is called. The '\*' indicates that all numbers will match with no exception.
- **Replace:** This specifies any modifications that will be done to the number when routing the call to the LineOut. The given search/replace combination specifies that the call will simply be forwarded with no modification.

*The Operator configuration:*

```

-Oper-----0001--
N Name      RightsInfo
1 ADM       x7777
2 SUP       x0333
3 SYS       x0222
4 USR       x0111
5           x0000
6           x0000
7           x0000
8           x0000

```

At this moment, we do not need to differentiate between several operators. So the default is ok.

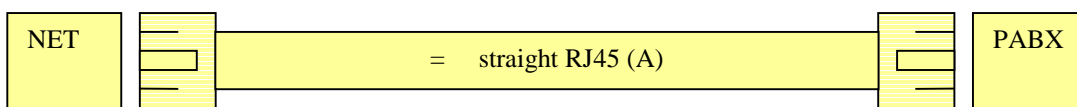
## The basic factory application.

As already noted before, the factory default allows to install the IntelliShare within the chain of USER to NET equipment (typically a PABX and a Public Network) without changing the current operation of the PABX in a significant way. We will spend a significant amount of pages on this simple case, because once you are able to make this work correctly, all other applications will be easy extensions.

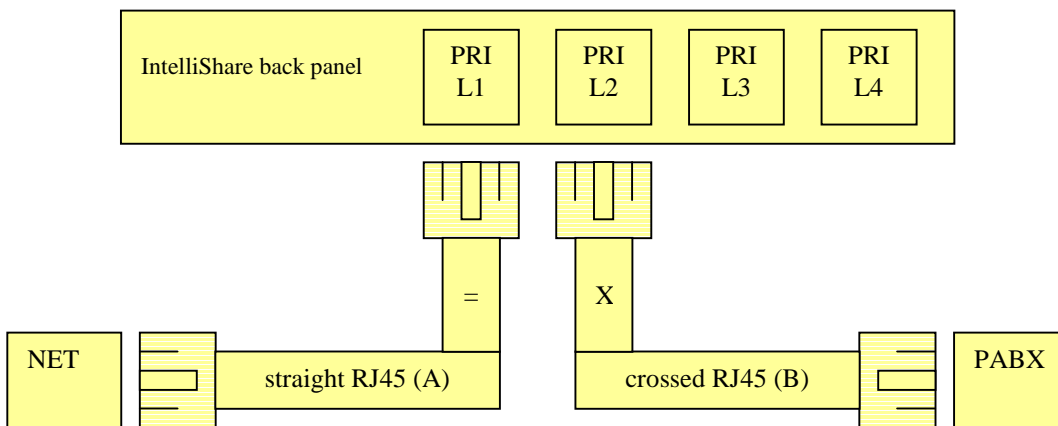
Before you do this test and those in the next chapters, ensure yourself that you have the PABX for yourself. Whenever you reset the IntelliShare (or the PABX for that matter), you will (and should) lose connection with the Network for at least 20 seconds. Inform whoever may be using the PABX.

Also, verify that the PABX is operational, and that you are able to make calls to the world.

Finally, you should prepare a note describing the actions to take to restore your original setup. In this way, you can revert to basic PABX operation in a minute. An example is shown here.



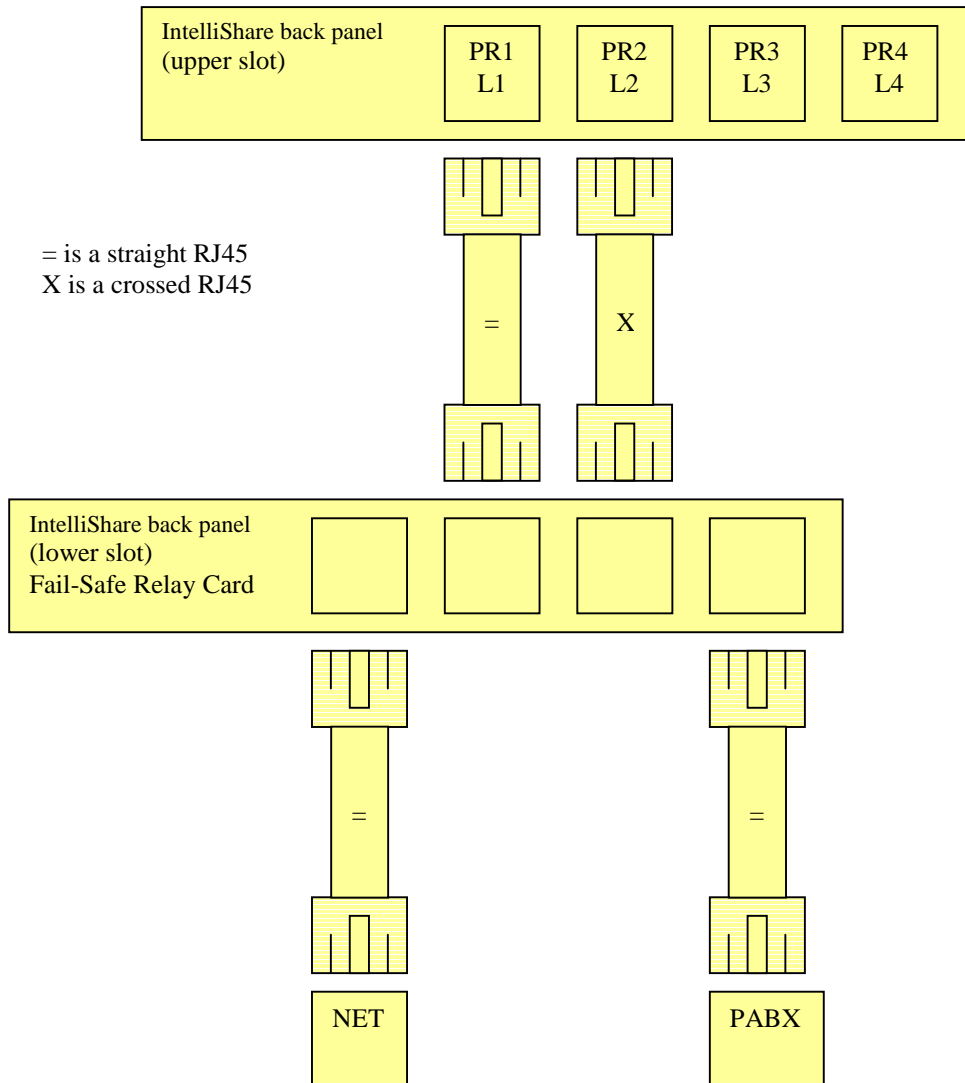
Basic installation: Original cabling



Basic installation: Cabling with IntelliShare inserted.



If you are using the Fail-Safe Relay Card, restoring the initial configuration is possible by simply turning off power to the IntelliShare. The cabling is shown below.



Basic Installation: Cabling with IntelliShare inserted and with use of Fail-Safe Relay Card.

## Check your configuration and your physical connection.

The default line configuration identifies L1 (our abbreviation for Line 1) as the line connected to the NET (NT field in Line Cfg == TE). You need a straight cable (a DX\_C2DMM\_R45\_R45) to connect from the IntelliShare L1 connector to the Network plug-in.

If everything is well, you should see that the corresponding PRI LED turns Green.

Also, the following indication appears on your screen (if you are in the WIN interface you need to go back to the Command interface first):

```
11:50:0162 L1 PH AI      -- after inserting cable to the NET
11:50:0166 L1 DL UP (TEI 0)
11:50:0592 L1 PH DI      -- after pulling out the cable
11:50:0592 L1 DL DOWN (TEI 0)
11:50:0592 L1 PH AR
11:50:5873 L1 PH AI      -- after inserting cable to the NET
11:50:5876 L1 DL UP (TEI 0)
```

What you see in action is the tracing feature of the IntelliShare. The IntelliShare has very extensive tracing facilities (check the reference guide), which are most helpful for trouble shooting.

The above trace tells something like this:

"At **11:50:01** (and **62/100** seconds), on line **L1** of the IntelliShare, a **PH**ysical event was detected. It concerned an Activation Indication (**AI**). At **11:50:01** (and **62/100** seconds), the same line showed a **Data Link** activation."

When you pull out the cable, the state of both the data link and physical link went down.

You may wonder why we did not simply tell at length that everything is OK. The reason is that the use of a well-defined format allows other software to interpret these traces easier. We will see an example later on.

If you did not see any such trace, then you have a problem at the physical layer. This means: your cabling is not OK. Maybe you did not use the correct cable. Or you are putting it into the wrong connector. If this is not the case and things are still not as shown, then you are out of luck and have to go to the trouble-shooting guide.

Now we need to connect the line to the PABX. This is a little tricky: the IntelliShare behaves as a USER equipment on the physical level, so if you connect it to another USER equipment then you need to use a crossed PRI ISDN cable (a DX\_C2XMM\_R45\_R45).

Because the default line configuration identifies L2 (Line 2) as the line connected to the USER (NT field in Line Cfg==NT), you need to connect the crossed cable from the IntelliShare L2 connector to the PABX plug-in. Note that the crossed cable is symmetrical, there is no "In" and "Out". This knowledge can be helpful if you have troubles: turn around the cable and insert it again. If you get another message, then something is wrong with one of the leads in the cable: throw it away.

Once again you should see a PH AI indication proving that the cabling is OK.

In some cases, you may see a rapid succession of PH AI or PH DI messages. One of the primary causes for this (apart from loose cables) is a mismatch in CRC4 settings at each side of the cable. In this case, go to the line configuration screen and change the setting of the field

**WIN.CFG.LINE.CRC4 := change it**

to the alternative selection. Do not forget to do "**CFG RUN**" after changing.

In the case of CRC4 changes, you also need to reset the equipment, either with power off or with the command "**RESET SYS**". Of course, if you asked the Network operator about CRC4, then you know, and you don't have to do this by trial and error.





## Check the datalink. Setting the tracing level.

Now that you are sure about the cabling, the time has come to have the IntelliShare do some talking. In fact, if all is well, then the IntelliShare has already made acquaintance with the network. To prove this, we need to adjust the level of tracing.

The tracing facilities of the IntelliShare are classified into a number of levels, each one more important than the previous one. For instance, the physical events shown above are considered rather important (level 40) which is why they are normally displayed. The casual talking of the IntelliShare with the Network is normally not very interesting (level 8), so it is not displayed.

You can change this setting, using the set trace command:

```
SET TRACE L 8
```

This command instructs the IntelliShare to show all Line-related traces with level above 8 on the screen. You could also have said

```
SET TRACE L1 8
```

which instructs the IntelliShare to do it only for L1 (others would remain at their current level).

If all is well, then you should now see something like this every 10 seconds:

```
23:51:0150 L1 DL T RR (00 01 01 01 x x 00 00)
23:51:0152 L1 DL R RR (00 01 01 01 x x 00 00)
                -- or
23:51:4161 L1 DL R RR (02 01 01 01 x x 00 00)
23:51:4161 L1 DL T RR (02 01 01 01 x x 00 00)
                -- or both
23:52:1163 L1 DL T RR (00 01 01 01 x x 00 00)
23:52:1167 L1 DL R RR (02 01 01 01 x x 00 00)
23:52:1168 L1 DL T RR (02 01 01 01 x x 00 00)
23:52:1168 L1 DL R RR (00 01 01 01 x x 00 00)
```

What you see here is that the IntelliShare and the Network are telling each other that they are ready to receive data (**R**eceiver **R**eady) on the datalink (**D**L). The **T** stands for transmit, the **R** for receive.

If you do not see this, then plug out the cable, wait 20 seconds, and plug it in again. You should see something like this (note that in some cases you may need to be patient for up to 1 minute):

```
23:54:4638 L1 PH AI
23:54:4656 L1 DL T SABME (00 01 7f 00 x x 00 00)
23:54:4659 L1 DL R UA (00 01 73 ab x x 00 00)
```

This trace shows that the datalink (DL) has been established normally. After this, the RR messages should be seen every 10 seconds.

Alternatively, you may see something like this:

```
12:08:5385 L1 PH AI
12:08:5385 L1 DL T SABME (02 01 7F )
12:08:5387 L1 DL R SABME (02 01 7F )
12:08:5485 L1 DL T SABME (02 01 7F )
12:08:5486 L1 DL R SABME (02 01 7F )
12:08:5585 L1 DL T SABME (02 01 7F )
12:08:5586 L1 DL R SABME (02 01 7F )
12:08:5685 L1 DL T SABME (02 01 7F )
12:08:5687 L1 DL R SABME (02 01 7F )
12:08:5785 L1 DL DOWN (TEI 0)
12:08:5787 L1 MDL Error L
```

Clearly something is wrong, and the reason is typically that both sides do not agree upon their role as either NET or USR (NT or TE). On the physical level it is possible to interwork by using crossed cables. On the higher levels however, it is necessary that one side acts as NET (NT) and the other side acts as USR (TE). If this happens, then check that the line configuration correctly identifies the peer entity (the entity at the other side of the cable in this case) as either NET or USR. If you are in doubt, then change the setting

**WIN.CFG.LINE.NT:= change it**

Do a CFG RUN, and then a RESET SYS and try if things are better. Of course, it is better to think and enquire about this if there are doubts: then you know.

After this validation of the datalink, you can set back the trace level to the default

**SET TRACE L 20**

### Alarm forwarding.

Suppose that something goes wrong between the IntelliShare and the Network, for instance that the ISDN cable is plugged out. Obviously, it will not be possible to make a call to the network. In fact, the PABX will be able to start the call, and will then receive a call clearing message indicating a temporary failure (cause 41). This is correct, but in some cases it may be desirable to generate a fault condition that can be detected by the PABX. This is where Alarm Forwarding comes in: this feature will translate a physical alarm on one line into a datalink failure on another line. The datalink failure will be generated by not responding to any received data on the link, and this is guaranteed to bring the line down within at most 15 seconds.

To check this out, change the line 1 configuration as follows:

```
-Line-----0001--
N          1
Type       PR
Name       TO NET
Act        On
Sgn        Isdn
Tei        0
NT         TE
Idle       x49
Crc4       NoCRC4
StrInc     0
EndInc     0
StrOutg    0
EndOutg    0
AlmFrom    @□□□
Options    -----
```

and similarly, line 2 configuration as follows:

```
-Line-----0002--
N          2
Type       PR
Name       TO USR
Act        On
Sgn        Isdn
Tei        0
NT         NT
Idle       x49
Crc4       NoCRC4
StrInc     0
EndInc     0
StrOutg    0
EndOutg    0
AlmFrom    1---
Options    -----
```



This instructs the IntelliShare to generate an alarm on Line1 (by not responding anymore to received data) whenever there is a physical problem on Line2.

In the same way, a physical problem on line L1 will force an alarm on L2.

Do **CFG RUN** and **RESET SYSTEM** to activate these.

Assuming that you started from a normal situation, you should see something like this when you pull out L1:

```

13:07:3200 L1 PH DI          -- Pull out L1 cable
13:07:3200 L1 DL DOWN (TEI 0)
13:07:3200 L1 PH AR
13:07:4230 L2 DL DOWN (TEI 0)  -- Datalink is forced down on L2
13:07:4232 L2 MDL Error I
13:07:4234 L2 MDL Error G
13:10:1310 L1 PH AI          -- Insert L1 cable
13:10:1339 L1 DL UP (TEI 0)
13:18:4777 L2 PH AI          -- L2 link re-established
13:18:4781 L2 DL UP (TEI 0)

```

When breaking the physical link to L1, the datalink is lost on L1, and the alarm is forwarded to L2. As a result, the datalink on L2 is lost some seconds later. When restoring the physical link, both datalinks come back on and the alarm disappears.

### Check the network link, trying out.

The network link is really concerned with the interaction between you and someone else at the other side of the network. So this is the correct time to make some outgoing calls.

If you succeed then this is a very good indication that the installation is successful. Otherwise, you will need to do some trouble shooting.

### Status screens.

The IntelliShare provides additional information that can help you identify problems if any. This information can be accessed using the screen interface (WIN.STS).

```

-Sys-----
N Sts  Date       Time       ClTrcHWErrs
1 ACT  2000/03/08 13:21:24  1 20 x0000

```

The System status screen shows the current date and time (which you can change with the SET TIME command). It defines the line on which clock slaving is performed, the trace level, and the number of hardware errors occurred.

The derivation of the system clock, and the consequent synchronisation of the whole system, will be discussed later. For now, just note that the IntelliShare always derives its clock from an NT, or goes into Free Run if no NT is available.

```

-Slot-----0001--
N Sts  SW          HW          LED
1 ACT  PRTA5314  4.1        09700630    g-GGG-----
2 ACT  PRTA5314  4.1        09700630    -----

```

The Slot status screen provides information that is associated to the particular card(s) in the IntelliShare box. The card in slot 1 is a MPR (Multiple Primary Rate – see WIN.CFG.SLOT), and it is enabled. The self-check of the card was OK, and there were no errors or warnings. The software running on this card is version 4.0 and the hardware serial number is as shown. The LED status shows the indicators as they appear on the front panel. Small letters indicate blinking LEDs, large letters indicate steady LEDs.

The second slot is occupied by the VXI card (V.X Interface card – see WIN.CFG.SLOT), and has a good status. It is interesting to pull out the ISDN cable on L2: after some seconds - at the next screen update - the screen shows:

```

-Slot-----0001--
N Sts SW HW LED
1 ACT PRTA5314 4.1 09700630 g-GGR-----
2 ACT PRTA5314 4.1 09700630 -----
    
```

The LED on Line L2 has become Red (check it). When reinserting the cable, the L1 LED turns Green again. By now, you will have remarked that the screen is redrawn at definite intervals. This refresh time is 10 seconds.

```

-Line-----0001--
N Sts PH DL BConn AlmFrom
1 ACT Up Down -----
2 ACT Up Up -----
3 IDLE Down Down ----
4 IDLE Down Down ----
    
```

The Line Status screen provides information on the current state of the PRI lines.

- **Sts:** Define the status of the line: if ACT, then the line has been activated in the WIN.CFG.LINE screen. If this field shows IDLE, then the line has been deactivated. If this field shows KEY, then you don't have a valid key to enable this line.
- **PH:** this shows the physical state according to the ETSI norms. If you see Up in it, then all is well. This indication is related with the "PH AI" traces we saw before.
- **DL:** this shows if the datalink is up (Up) or down (Down). This indication is related with the establishment of the datalink as we have seen before. If the datalink is down, then have a look at AlmFrom. If there is some line indicated here, then the origin of the problem is there.
- **BConn:** as we will see later, this shows which B channels are in use.
- **AlmFrom:** this indicates which - if any - alarms cause the datalink on this line to be dropped.

For now, this ends the overview of status screens. We will come back to these and others later.

### Final compatibility checks

Before configuring other applications, take the time to do some testing with the current installation because most problems that you may encounter will arise already at this stage. Try to use different kinds of telephone sets, isdn terminal adapters, fax machines and whatever you can put to use. Try outgoing and incoming calls.



## SW Upgrade & Softkey Options.

### Local SW Upgrade on the IntelliShare

Since the SW on IntelliShare resides in Flash EPROM, a SW upgrade is as simple as a file transfer.

In general following upgrade procedure may be applied:

1. Make a backup of the IntelliShare configuration using X-Modem.
2. Log in via terminal access on Supervisor or Administrator level and enter the 'MAINT' command from the Human Interface. Upon request of confirmation, enter 'Y' to proceed. The IntelliShare will confirm start-up of the maintenance menu.

Note that the HB LED stops blinking.

```
? LOGIN LOGOUT WIN SHOW CFG SET RESET MAINT REM
MAINT
Start Upgrade Procedure [Y/N]: Y
Active
```

3. To enter the maintenance menu press the enter-button. The following commands are available:

**ID:** shows the identification of the product

**UPGRADE:** starts the upgrade procedure

4. Enter the 'UPGRADE' command to start an X-modem file receive session (character 'C' will appear). After entering this command, the operator should send the 'PMX.BIN' file in the 'SW' subdirectory of the SW upgrade floppy.

```
? ID UPGRADE
UPGRADE
Erasing and waiting for <update>.BIN upload
C
```

5. As soon as the IntelliShare confirms receipt of the complete file, the new SW type and revision is displayed. At this point the operator should power down the IntelliShare to boot up the new software

```
? ID UPGRADE
UPGRADE
Erasing and waiting for <update>.BIN upload
C..
OK
PMX 4.1
```

6. Power on the IntelliShare again. After a successful selftest the IntelliShare will start up with the factory default settings for the configuration. Note that the HB LED starts blinking again.
7. Depending on the type of SW upgrade, a previously stored configuration can be recovered completely or partially.

#### REMARK!

If some fault occurs during the X-modem file transfer, you must repeat the upgrade procedure as described above, with the following differences :

2. Instead of logging-in and entering the 'MAINT' command, power down the system and place jumper JP85 on the IntelliShare (located behind the Ethernet connector).  
Power on the system again.
5. In addition to powering down the system remove jumper JP85 on the IntelliShare.



## Remote Software Upgrade

Apart from the possibility to upgrade the software through a local console port, you can also perform an upgrade remotely, i.e. over the LAN connection, or a remote PPP connection (see chapter 0 for configuring the IntelliShare for LAN access, chapter 0 for configuring the IntelliShare for a remote PPP connection). It allows you to upgrade the software from a distance, without the need for local access to the machine.

To perform a remote software upgrade, you need to follow following steps:

1. Log in on Supervisor or Administrator level
2. Enter the command:

```
maint remupgrade
```

3. The command will start an X-Modem session. ('C' characters will appear on your console). Send over the compressed **pmx.cpr** file (*not pmx.bin*), to be found on the SW directory of the SW upgrade floppy.
4. From the moment the file has been received completely by the IntelliShare, the IntelliShare brings up a message, and will stop its normal functionality, i.e. all ISDN call processing will be stopped, and you will loose connection to the IntelliShare (the heartbeat will stop blinking). At that moment, the IntelliShare will start decompressing the file, which will take *a couple of minutes* to complete.

**Important:** Please, do not power down the IntelliShare while the decompression process is going on. Powering down the IntelliShare while decompressing the software will result in a complete loss of the software. If such a loss occurs, you'll need to follow the steps as described in the remark section of previous paragraph.

5. Once the decompression of the software is completed, the IntelliShare will reset automatically, and the new software will boot up (the heartbeat starts blinking again). You will have to restore your connection to the IntelliShare, and log in with Telnet to access the device.

Remark that the previous configuration stored inside the IntelliShare will be retained. As such, there is no need to save the configuration before upgrading the device and restoring it afterwards. However, as a safety measure, it's always wise to back up the configuration before upgrading. For instructions on backing up and restoring the configuration, see chapter 0.

## Softkey Options: Verification and Activation

In the basic offering, the IntelliShare is restricted to the use of 2 PRI lines (L1-L2), and does not provide TCP/IP support (LAN access and remote control), Advice Of Charge (AOC) generation and IP-Router functionality. If you do not need the other PRI lines, TCP/IP or AOC, then this is the most economical solution for you. For more complex applications, you will require special software activation keys.

You may purchase additional options when ordering the IntelliShare, or later as an upgrade.

The following options can be purchased:

- ISU9931: Fail Safe Relay option.
- ISU9932-3PRI: Allows the use of L3.
- ISU9932-4PRI: Allows the use of L4.
- ISU9932-SNMP: Allows the use of TCP/IP for local and remote Telnet and SNMP.
- ISU9932-AOC: Allows the generation of Advice Of Charge Info
- ISU9932-IPR: Allows the IntelliShare to act as an IP Router
- ISU9932-CODE: Software Upgrade to latest Code version

To obtain information on the currently installed options, check the extended identification:



**show id x**

```

PRTA5314 4.1 (PMX)

PCode: PRTA/4000 1.1
Model: DAXIT MPR-4
SerNr: 09700630
MacNr: 00E0DE 00010F
Option [P16,H15,S3,K1682687753]
Mar 06 2000 16:54:02
ISDNQ=PRTA5303 1.2.001
ISDNI=BRTA5301 1.2.001
5353 1.0 04.04.97 003          5352 1.0 04.04.97 003

```

The options have been highlighted, and contain option information that is used by BLACK BOX:

- P16: this is a product identification code.
- H15: this is a hardware option set.
- S3: this is a software option set.
- K1682687753: this is the option activation key value, which is determined from the serial number and additional information residing at BLACK BOX.

The following are specific options:

- H3: support of L1 and L2.
- H7: support of L1, L2 and L3.
- H15: support of L1,L2,L3, L4.
- S1: support of basic software package
- S3: support of basic software plus TCP/IP (hence LAN and remote control).
- S7: support of basic software plus TCP/IP (hence LAN and remote control) plus AOC.
- S15: support of basic software plus TCP/IP (hence LAN and remote control), AOC and IP-Router.

Descriptive info about the options installed can be obtained with the *show keys* command:

**show keys**

```

Hardware Keys:
Line 1234
VXI Port 1234
Software Keys:
SNMP key
AOC key
IP Route key

```

When you choose to activate extended options, you need to contact BLACK BOX SALES Department to acquire new option settings. You will need to provide the following information:

- the current options, as shown above
- the serial number of the equipment
- the required options

After purchasing the additional options, you will receive a new option set from BLACK BOX comparable to the one above. The installation and activation of the new option is done with a maintenance command :

**maint opt**

```

Enter Option Sequence (SERNR=9700002)
P:64
H:527
S:3
K:1684587753
Option [P64,H527,S3,K1684587753]
OK

```



The options will be activated at the next power up. You can verify this on the boot screen, which shows the enabled lines:

```
> BOOT PRTA5314 4.1
> Option [P16,H4111,S3,K1548921915]
> TIME..... 15:11:44,2000/06/26
> NVRAM.....
> PIO..... OK
> L1: FALC OK,Enabled
> L2: FALC OK,Enabled
> L3: FALC OK,Enabled
> L4: FALC OK,Enabled
> MITEL..... OK
> Xilinx .... OK
> ESCC.....
> SMC..... OK
> VXI 1--- . Enabled
> Failsafe Timer..OK
```





## Managing the IntelliShare via the LAN.

Let us now consider management via the LAN interface.

For this to work, you need to have installed the Softkey option DX\_PMX\_SK\_SN (TCP/IP module).

If you have no LAN interface, or if you did not buy this option, then you can simply skip this chapter and proceed with the next chapter.

### Configuring and installing for LAN access.

Before connecting the IntelliShare to the LAN, you need to obtain the following information from your network manager:

- A free IP address (a unique identification that will represent the IntelliShare on the LAN).
- The netmask to be used (in most cases this will be 255.255.255.0 (class C network)).
- An access point to the LAN. In most cases this will be a port on a HUB.

If you want to try this out on your own, then you can create your own LAN. Proceed as follows:

- You need a HUB with a few ports. Alternatively you can use a crossed Ethernet cable to connect directly between your PC and the IntelliShare. The layout is specified in the Reference Guide.
- You need to define your IP domain. For testing, you can use one of the 'private' internet domains (RFC1918), for instance 192.168.4.0 with netmask 255.255.255.0. In this case, you should configure your PC so that it uses an IP address on this network, say 192.168.4.16. You will probably need to restart your PC.
- You can then assign the IP address of the IntelliShare, say 192.168.4.15.

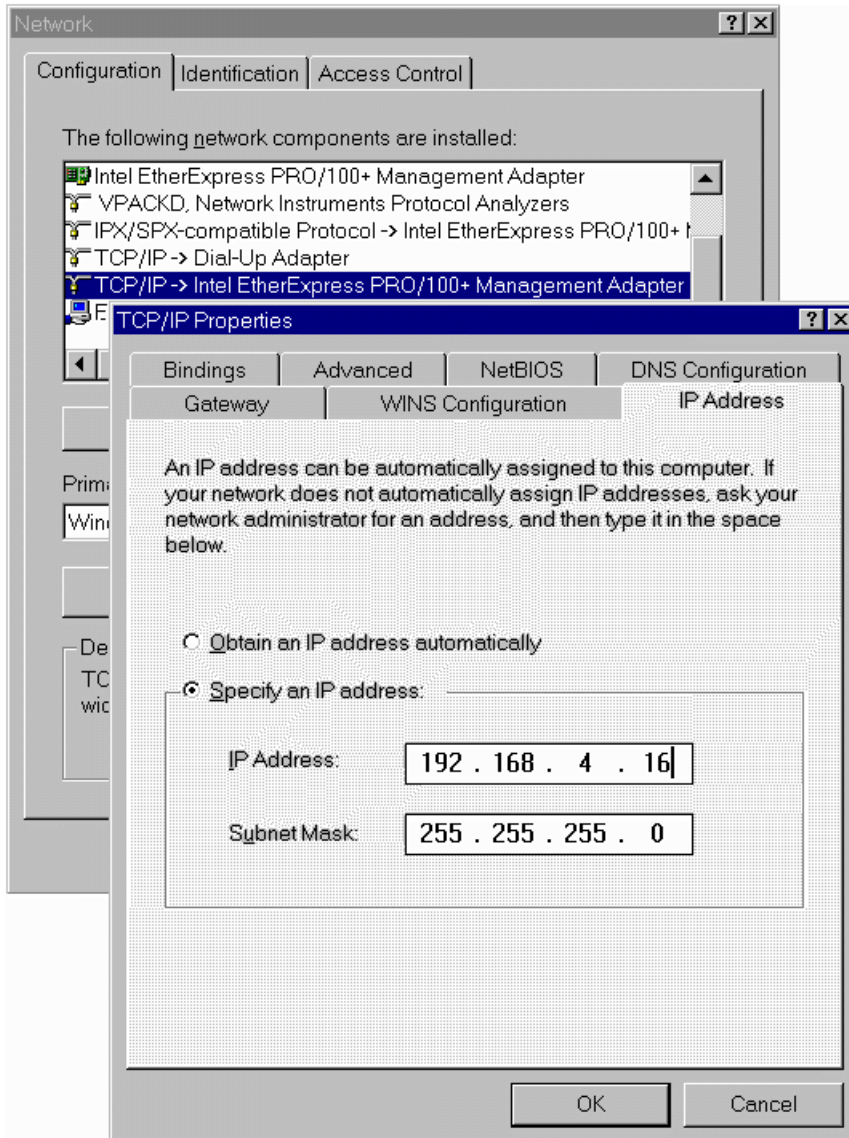
We are now ready to start the LAN configuration for the IntelliShare. This is done in the CFG.SYSTEM screen. Assuming the test LAN, the minimal configuration required to interact with the IntelliShare is shown below. The highlighted fields have been changed.

```

-----Sys-----
N          1
Type      MPR
Name      PMX
Log       20
Trp       50
IP      192.168.004.015
SubMask 255.255.255.000
Gateway   000.000.000.000
PrimMgr   192.168.004.016
SecdMgr   000.000.000.000
RdComm    public
WrComm    netman
TrpComm   trap
TLogOff   0
TFailsf   20
ClkSlve   AUTO
AlmTime   00:00:00
HttpRef   0
AOCEnbl   Off
AOCType   AOC-D
AOCCTyp   Unit
AOCCurr
AOCMult   0.001
IPRoute   Off
Masq      Off
MasqIP    000.000.000.000
RCNetIP   000.000.000.000
RCMask    000.000.000.000

```

On your PC, assuming that you are using Win98, you should be able to verify that the "Network Neighborhood Properties" resemble this:



Now power down the IntelliShare and the PC, and install one straight RJ45 cable between the PC and the HUB, and a second straight RJ45 between the IntelliShare LAN connector and the HUB. Be careful to select the correct connector on the IntelliShare, and verify that you did not connect to the Uplink port of the HUB. Note that you can use straight ISDN cables for this since they are the same for ISDN and for Ethernet. If you have no HUB, then connect the crossed Ethernet cable between the PC and the IntelliShare. Note in this case that a crossed Ethernet cable is different from a crossed PRI cable.

### Basic tests for IP connectivity

Once you have finished this, check IP connectivity first using the PING program. For this, start a DOS session on the PC, and type the following commands:

**PING 192.168.4.15**

You should receive a message indicating that an echo has been received. If this does not work, then try the following first:

**PING 192.168.4.16**



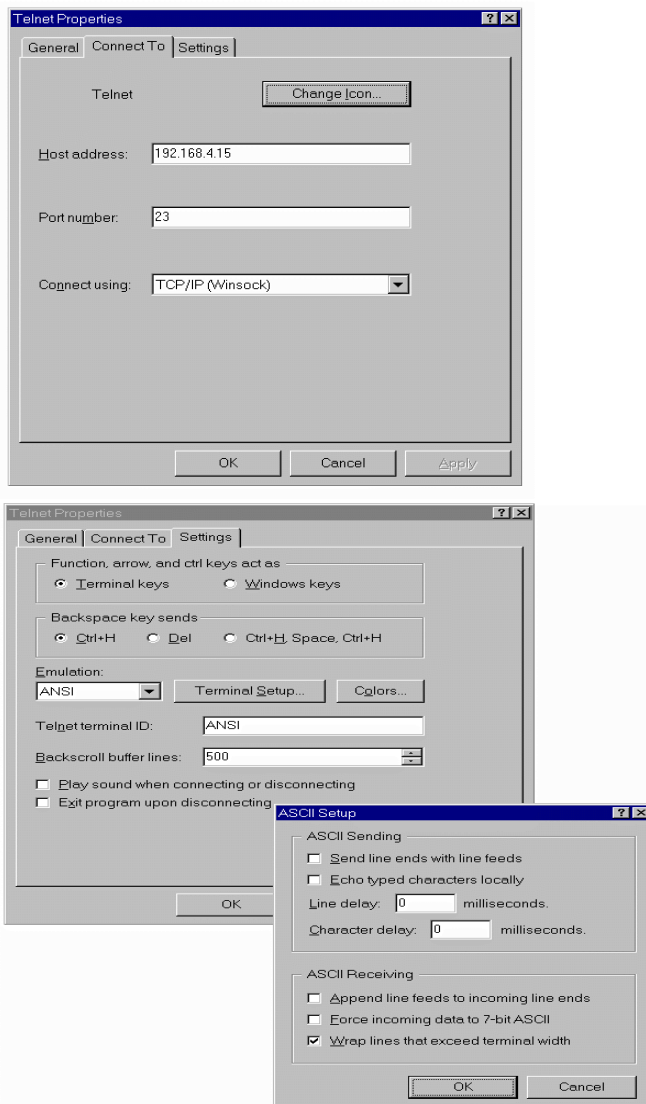
This is the IP address of the PC itself, so it should work. If it does not work, then you have a PC configuration problem. Otherwise you should first check the cable. Note also that the IntelliShare must be operational before pinging will work. During the boot delay, the IntelliShare will not respond to Ping requests. If this still not works, then refer to the trouble-shooting guide.

Assuming that everything got right, you are now ready to manage the IntelliShare via the LAN.

### Telnet access to IntelliShare.

To illustrate Telnet access, let us try it out using Win98 HyperTerminal.

The settings required for our test LAN are as shown below. Apart from this, the terminal emulation settings should indicate ANSI with use of function keys (like it was for the serial connection).



### Telnet: HyperTerminal configuration example

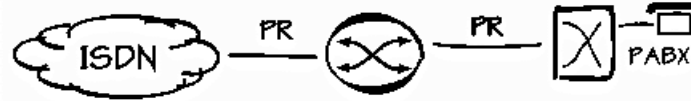
It is important to realize that a Telnet session cannot be executed simultaneously with a Local control port session. If you are logged in on the local control port, then starting Telnet will disconnect the local session, and display a message "Telnet Active". The reasoning behind this behavior is that the local user - if he wishes - can always force access by disconnecting the LAN.

After configuring HyperTerminal, select the connect command or simply start typing. This will establish a connection via TCP/IP. Apart from this, the interaction between the IntelliShare and the user is identical to the interaction via the serial control port.



## PR-REDIAL: Least Cost Routing using Carrier Prefix.

### The application



This application exploits the possibility to select an alternative network operator using a carrier prefix before the phone number, such as dialling 1234032302887 instead of 032302887. The prefix 1234 is called a carrier prefix, and specifies the network operator that will handle the call.

New license operators often specialise in specific types of connections such as long distance calls, which they can offer at significantly lower costs.

Routing these calls via the alternative operators is economically very attractive, but requires a change of habits and well informed users: every user has to know and decide which call should or should not be made using the carrier prefix.

The IntelliShare provides the means to relieve the users from this burden by analysing the called number and by adding the carrier prefix whenever desirable.

### The Configuration

Start from a working factory default (optionally modified for LAN access) as described before.

The only thing that needs to be added is information concerning the call destinations and the associated decision to add a carrier prefix. The place to add this information is the route configuration screen (WIN.CFG.ROUTE).

As a very simple example, consider the following configuration:

```

-Route-----0001--
N  Act  LineISearch      Replace      LineOCalltyp  FailMin
1  On   1--- *             *            -2-- ----- 0
2  On   -2-- *            1234*       1--- ----- 0
3  Off  ----             -----      ----- 0
4  Off  ----             -----      ----- 0
5  Off  ----             -----      ----- 0
6  Off  ----             -----      ----- 0
7  Off  ----             -----      ----- 0
8  Off  ----             -----      ----- 0
9  Off  ----             -----      ----- 0
10 Off  ----             -----      ----- 0

```

In this example, all outgoing calls are routed to the alternative carrier, by prefixing every called number with 1234.

A slightly more developed example is shown next. All inter-zonal and international calls are routed with carrier prefix, all the other calls use the original network.

```

-Route-----0001--
N  Act LineISearch          Replace          LineOCalltyp    FailMin
1  On  1--- *                    *                -2-- ----- 0
2  On  -2- 0*                  01234*          1--- ----- 0
3  On  -2-- *                    *                1--- ----- 0
3  Off -----                ----- ----- 0
4  Off -----                ----- ----- 0
5  Off -----                ----- ----- 0
6  Off -----                ----- ----- 0
7  Off -----                ----- ----- 0
8  Off -----                ----- ----- 0
9  Off -----                ----- ----- 0
10 Off -----                ----- ----- 0
    
```

This is a simple example showing the priority rules for subsequent routes: as long as route R2 remains possible, route R3 – which is always possible – is not selected. On a phone that dials digit after digit, the IntelliShare will not forward the call until it is sure that route R2 cannot match. Of course, on a phone that calls all digits at once, the decision can be taken immediately.

In general, the decision to use route N will not be taken unless all routes before N have been invalidated. As a consequence, default routes should be placed at the end of the routing table. More specific search patterns should come earlier, with the most specific on top.

**Routing schemes. Rules for matching and replacing patterns.**

The matching takes place on the number that is being called, which is referred to as CDN.

The matching rules are based on the following syntax elements:

- a '?' (question mark) can match any single digit in CDN
- a '\*' (asterix) can match with either the leading part or the trailing part of CDN.
- a digit matches with the same digit in CDN

During the match process, the wildcard elements obtain values. These values are used when the replacement is executed.

A few examples to make things clear:

CDN	Search	Replace	new CDN	note
123456	*	888*	888123456	
123456	12*	88812*	888123456	
123456	15*	88815*	No match	
123456	1??*	8881??*	888123456	
123456	1??*	10??0*	10230456	
123456	*56	*00	123400	note 1
123456	*??	*00??	12340056	note 1

- Note 1: Suffix matching is only possible if the called number is sent 'en bloc'. This is generally true for calls coming in from the network, but cannot be assumed for calls coming from the user.
- Search and Replace string can have 0 or 1 '\*' wildcard.
- If the Replace string contains wild cards, the Search string should have at least as many corresponding wildcards.

**Testing and verifying status**

The next trace (set the trace level at 10 to obtain this level of information: SET TRACE L 10) shows an example of a call using the above shown configuration (latter example).

Do not worry if you don't understand this: it's only to satisfy the experts.



```

17:15:4564 L2 CC R CR=-0007 ST00 Setup (0)
17:15:4565 L2 CC T CR=-0007 ST06 SetupAck (0)
17:15:4712 L2 CC R CR=-0007 ST25 Informatn (0)      -- digit '0'
17:15:4712 L1 CC T CR=0005 ST00 Setup (0)          -- route decided, replace done
17:15:4723 L1 CC R CR=0005 ST01 CallProc (0)      -- network has enough digits.
17:15:4724 L2 CC T CR=-0007 ST25 CallProc (0)
17:15:4728 L1 CC R CR=0005 ST03 Alert (0)
17:15:4728 L2 CC T CR=-0007 ST09 Alert (0)
17:15:4880 L1 CC R CR=0005 ST04 Connect (0)
17:15:4880 R2 Connect 38410                        -- the actually dialed number
17:15:4880 L2 CC T CR=-0007 ST07 Connect (0)
17:15:4884 L2 CC R CR=-0007 ST10 ConnectAck (0)

```

The status screen (WIN.STS.ROUTE) for the routes also provides some interesting information.

```

-Route-----0001--
N   Sts  StateDate      Time      CausCDN      LineOut
1   ACT  Ok    0000/00/00  00:00:00  0            0
2   ACT  Ok    1999/03/26  17:15:46  0   38410       1
3   ACT  Ok    1999/03/26  17:10:17  16  384720      1
4   IDLE Ok    0000/00/00  00:00:00  0            0
5   IDLE Ok    0000/00/00  00:00:00  0            0
6   IDLE Ok    0000/00/00  00:00:00  0            0
7   IDLE Ok    0000/00/00  00:00:00  0            0
8   IDLE Ok    0000/00/00  00:00:00  0            0
9   IDLE Ok    0000/00/00  00:00:00  0            0
10  IDLE Ok    0000/00/00  00:00:00  0            0

```

For each route the following information is shown:

- **CDN:** This is the most recent phone number that was dialed out on this route. It concerns the number after executing any replacements specified in the corresponding route configuration.
- **Cause:** This is the most recent call clearing cause that was received on this route. Refer to the reference guide for an overview of causes.
- **LineOut:** This is the most recent line selected for dialing out.

Finally, the history screens (WIN.HISTORY) provide you with additional statistics about the calls made. There is a line history screen (WIN.HISTORY.LINE) and a route history screen (WIN.HISTORY.ROUTE). Both screens show accumulated statistics since the reset of the IntelliShare.

The line history screen shows various statistics about calls occurred on a particular line.

```

-Line-----0001--
N           1
AMaxIn     0
AMaxOut    0
AMinFre    30
APHDown    2881
ACRCErr    0
AFrmErr    0
AConTim    0
AChrges    0
ErrSec     0
SErrSec    0
UnvlSec    0

```

This screen shows the maximum number (high watermark) of channels used for incalls and outcalls, the minimum number (low watermark) of free channels, the number of occurrences of level 1 going down on the line, the number of CRC errors and framing errors occurred since reset of the IntelliShare.

It also shows the total connection time and accumulative charges (if AOC is enabled).



It finally shows the 'Errored Seconds' (ErrSec), the 'Severely Errored Secs' (SErrSec) and 'Unavailable Seconds' (UnvlSec). These three statistics are defined in the ITU spec G.821, and give you an indication about the quality of the line. These statistics are only relevant on PRI lines.

- An 'Errored Second', as defined by the G.821 spec is a second during which at least one bit error was detected on the line.
- A 'Severely Errored Sec' is a second during which at least one bit per thousand bits was erroneously (i.e. a Bit Error Rate (BER) of  $10^{-3}$  was detected).
- An 'Unavailable Second' is the amount of seconds during which continually Severely Errored Seconds were detected, and this for at least 10 seconds in row.

The route history screen shows various statistics about routes selected for switching calls.

```

-Route-----0001--
N          1
ACllAtt  0
AScCall  0
AF1Call  0
AConTim  0
ADblCnt  0
AChrges  0
    
```

This screen shows for the first route the number of call attempts, the number of successful calls, the number of failed calls, the total connection time and the number of occurrences the route was disabled, since reset. It also shows the accumulated charges for all calls occurred on this route.

Remark that a call is considered successful if a B-channel could be established. This means that in general, the call is successful when the setup message is correctly answered by e.g. a call proceeding. This implies that a call that is set up correctly, but is not answered by the remote party is considered as a successful call.

There are two situations where the IntelliShare will not even try a route, even if the phone number matches:

- If LineOut for the route is not available: this happens for instance when the LineOut cable is plugged out. In this case, the IntelliShare will immediately reject the call with a temporary failure.
- If there are no channels available on the LineOut link: in this case, the IntelliShare will reject the call with a "No channels available" cause.

```

17:21:5506 L1 PH DI
17:22:0448 L2 CC R CR=-0008 ST00 Setup (0)
17:22:0448 L2 CC T CR=-0008 ST06 SetupAck (0)
17:22:0815 L2 CC R CR=-0008 ST25 Informatn (0)      -- digit 0, route decided
17:22:0815 L2 CC T CR=-0008 ST25 Disconnect (3)    -- L1 is in LOS, so No Route!
17:22:0854 L2 CC R CR=-0008 ST11 Release (16)
17:22:0854 L2 CC T CR=-0008 ST11 ReleasCmpl (0)
    
```





## Saving and restoring configurations with XModem.

After finalising the correct configuration and the complete routing table, you will certainly want to keep the resulting configuration somewhere on a PC disk as a backup. The IntelliShare provides the means to this, by using various upload and download features.

In this chapter, we will consider the XModem protocol.

The XModem protocol is an old but very simple and very commonly used protocol to upload or download files between PC's. With the IntelliShare you can use this protocol:

- CFG XMSEND sends the configuration from IntelliShare to PC
- CFG XMRECV receives on the IntelliShare from the PC.

Configuration uploads/downloads can be performed in two formats: text format and binary format. If you want an upload/download in text format, you need to specify as filename *cfg.txt*. If you want an upload/download in binary format, you need to specify as filename *cfg.bin*.

The IntelliShare supports Xmodem over a Telnet session. With HyperTerminal for instance, it is possible to do XModem just like on a local link. Note however that not all terminal emulation programs support this feature. The following example shows both kinds of transfer on a Win98 PC (using HyperTerminal).

To start a download of the configuration in binary format to the PC, enter the command

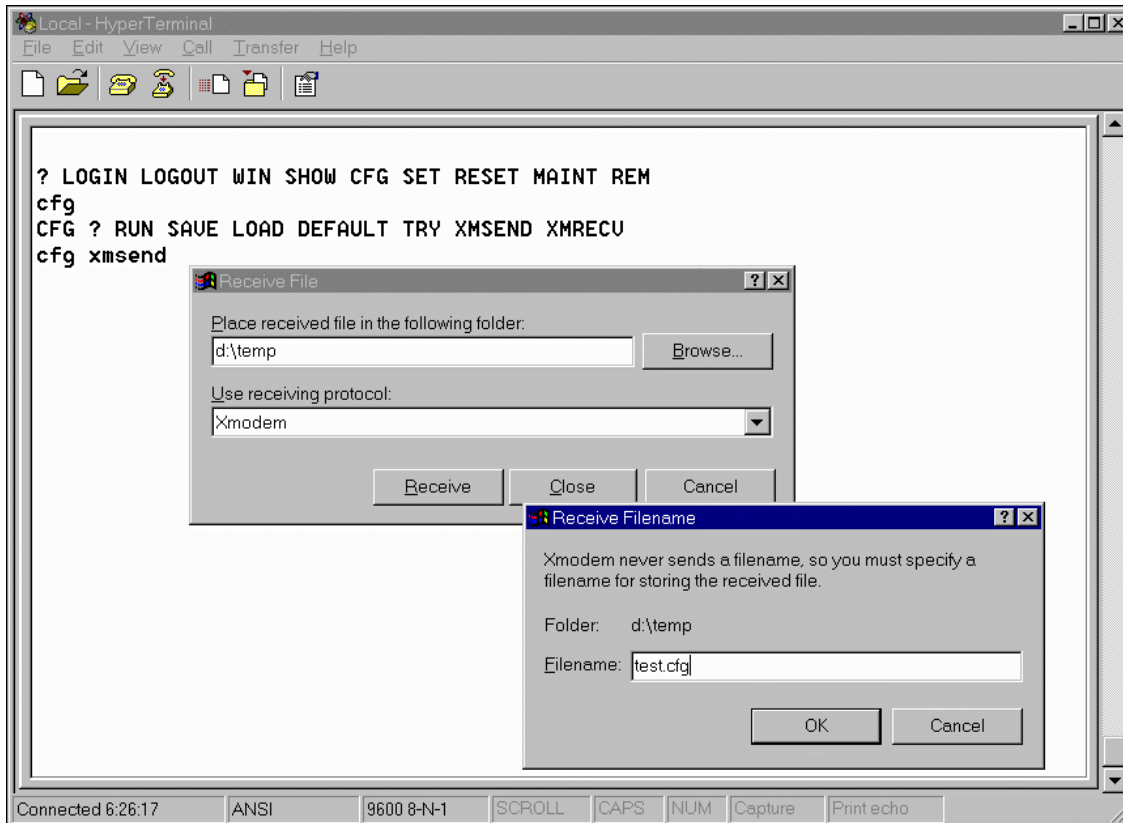
```
CFG XMSEND CFG.BIN
```

To start a download of the configuration in text format to the PC, enter the command

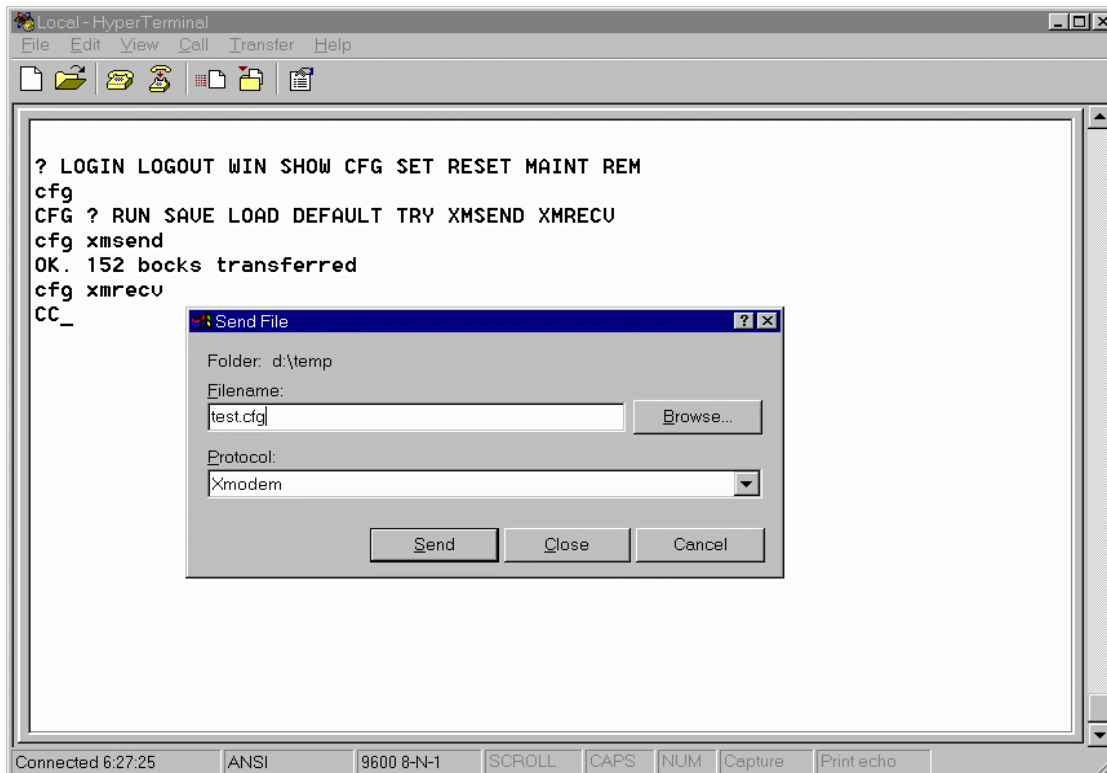
```
CFG XMSEND CFG.TXT
```

The IntelliShare is ready to start the transfer. On the PC, select the file transfer command, and choose to receive a file using the XMODEM protocol. Give a file destination and filename, and finally press the start button. After a few seconds, the file transfer will start.



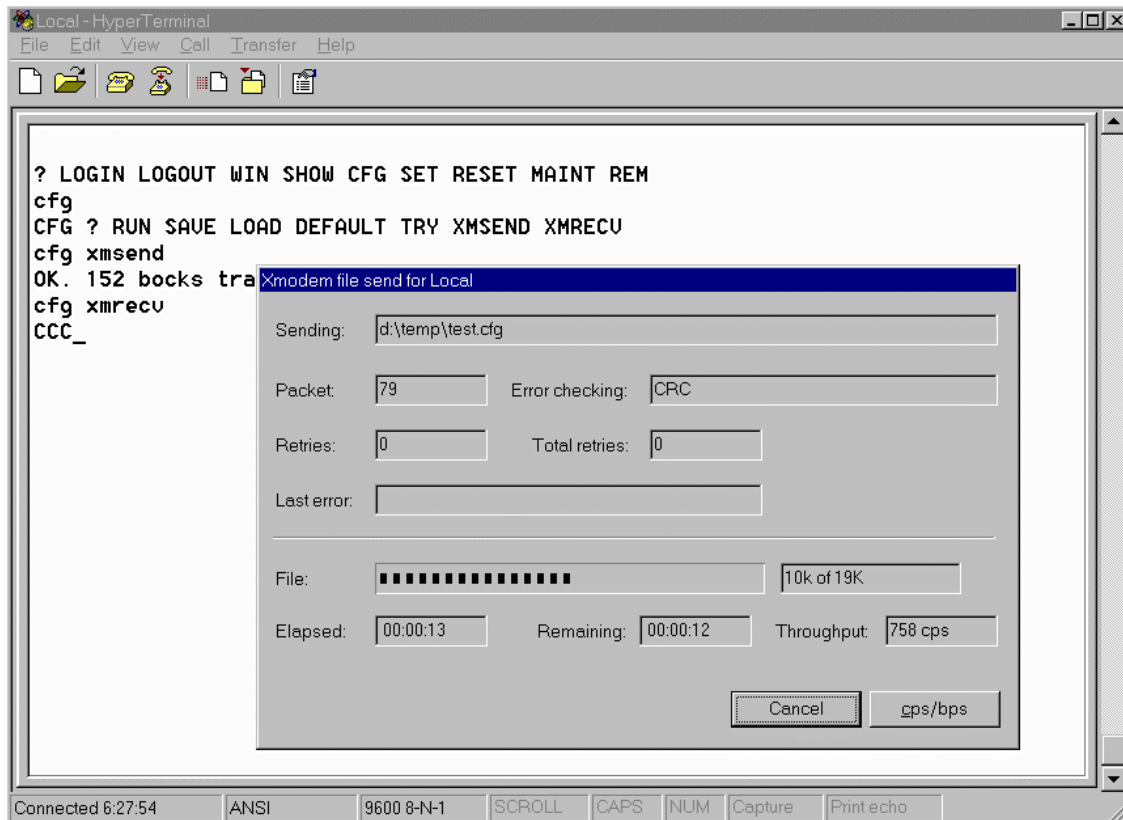


The procedure for uploading is almost the same. After entering the command "CFG XMRECV CFG.TXT" or "CFG XMRECV CFG.BIN", the IntelliShare is ready to start receiving. The 'C' characters that appear on the screen are normal, and indicate that the IntelliShare invites the PC to start sending the file.



The progress of the file transfer may or may not be shown depending on the PC program.





The syntax of the configuration in text format is similar to the syntax of the LISP programming language, and is described fully in the reference guide.

While a binary configuration file is generally useful to make a backup of the IntelliShare configuration in case its configuration gets lost, the text configuration file will normally be used to edit remotely the configuration of the IntelliShare, and upload it afterwards.

## Remote Control.

And now for something completely different...

If the IntelliShare is installed at customer premises, the manager of the IntelliShare's may be interested in having remote access to the equipment via an ISDN B channel. The reasons for this can be the wish of the manager to check the operation of the equipment, or to provide remote support, or to control the routing table, etc...

The IntelliShare offers a standard way to do this, by providing TCP/IP connectivity over PPP via an ISDN B channel. This means that, once a PPP link has been established between the IntelliShare and the peer entity (read, the PC equipped with a ISDN adapter supporting PPP), all normal TCP/IP applications are possible: Telnet, SNMP.

There are two ways of establishing a Remote Control session: you dial in to the IntelliShare, or the IntelliShare dials a predefined number at a predefined hour of the day. We'll first discuss dialling into the IntelliShare.

To support remote control from your PC to the IntelliShare, the IntelliShare must be able to identify the incoming call as a remote control call. This is achieved by specifying the phone number to be used for Remote control. Moreover, for security reasons, you can specify the phone number of the calling device, which will be verified by the IntelliShare.

To simplify the PPP settings for the manager, the IntelliShare behaves as a PPP server, and if necessary assigns a IP address to the calling PPP client. As a result, the configuration required on a typical PC is pretty much the same as the one required to interact with a typical Internet Service Provider.

Finally, during establishment of the PPP connection, the IntelliShare will require a login verification using PAP (Password Authorization Protocol).

To support Remote Control, you will need to configure various PPP settings, which you can find in the PPP configuration table (WIN.CFG.PPP). The configuration tasks required on the IntelliShare are shown below.

```
-PPP-----  
N          1  
IPAddr    192.168.003.001  
TimeOut   0  
InCDN     *99  
InCLI     *123  
RemUser  
RemPwd  
OutCDN  
OutCLI  
OutLine   ----  
LLine     NONE  
LLStrTS   0  
LLEndTS   0
```

In this example, the phone number used for remote control (InCDN) is specified as \*99. Note that this is a search pattern in the same way as search patterns were defined for the SHARE application (see chapter 0). If this setting is too general, you can change it to be more specific. The example setting can be used to preconfigure an equipment in a more generic way allowing easier installation.

When a call is received with a *called* number that matches the pattern \*99, the calling line identifier (CLI) (if present in the call setup) will be verified against the pattern \*123 (as defined in the InCLI field).

The IP address assigned to the remote control port of the IntelliShare is specified as 192.168.3.1.



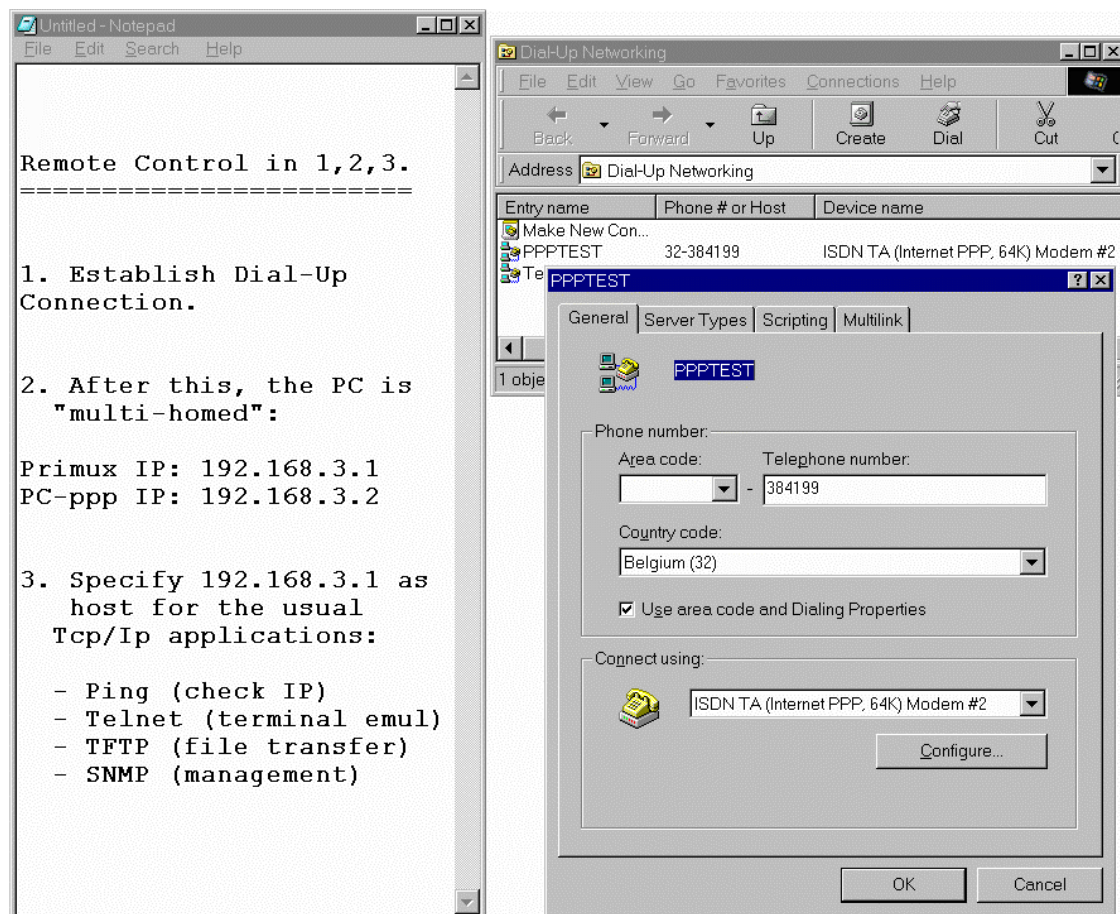
This is an address that belongs to the so-called private networks. This address can normally be used safely, unless the LAN network used by the client happens to be this same network (in this case, select another private network on the IntelliShare). As noted above, the IntelliShare will use this IP address in the negotiation with the client: by our convention, the IntelliShare will assign address IP+1 (192.168.3.2) to the PPP link at the client side, if the client side is not configured for an own PPP address.

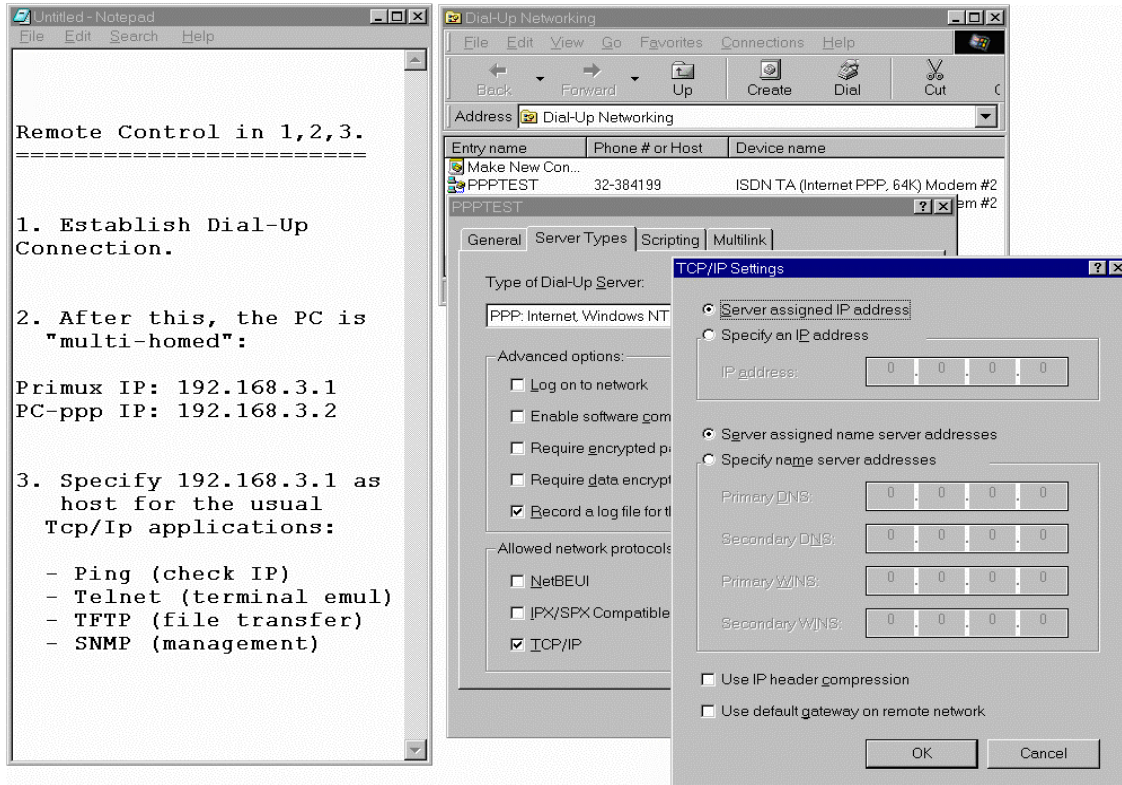
Once connected to the client, the IntelliShare will be identified to the client by the address 192.168.3.1.

This is all that is needed on the IntelliShare side.

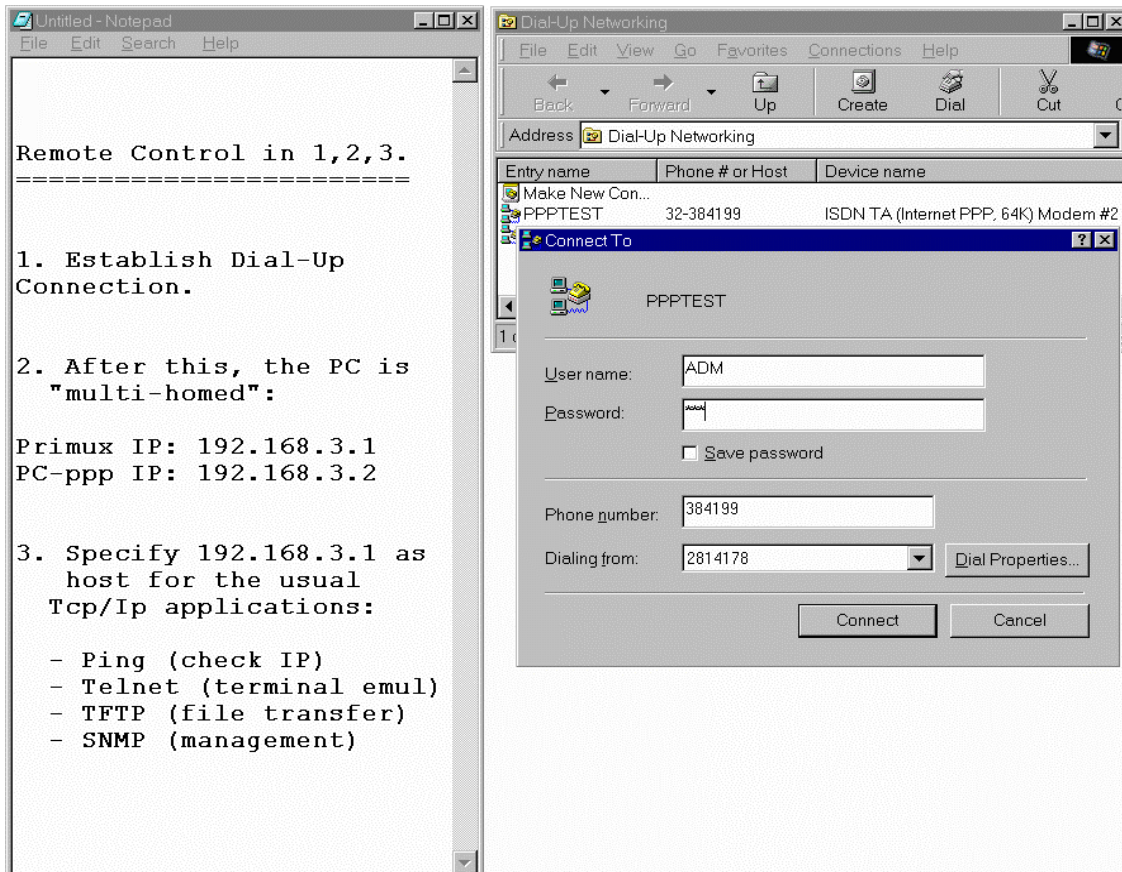
On the PC side, you need to have an installed ISDN TA adapter. External models are cheap, flexible and generally easy to install. You should ensure that the equipment supports basic PPP, which will be the case if it is able to connect to an Internet Service Provider.

Assuming a Win98 PC, a typical configuration may look as follows:

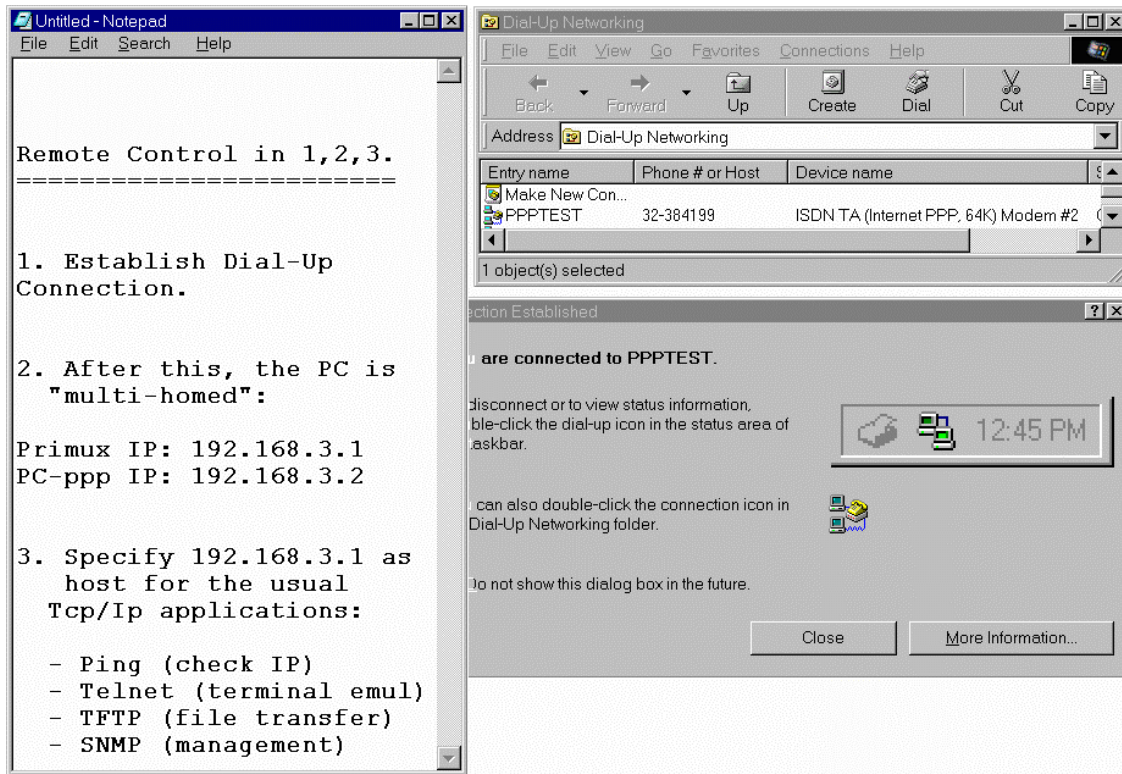




To establish the connection, select the Dial-Up entry, fill in the password, and connect.







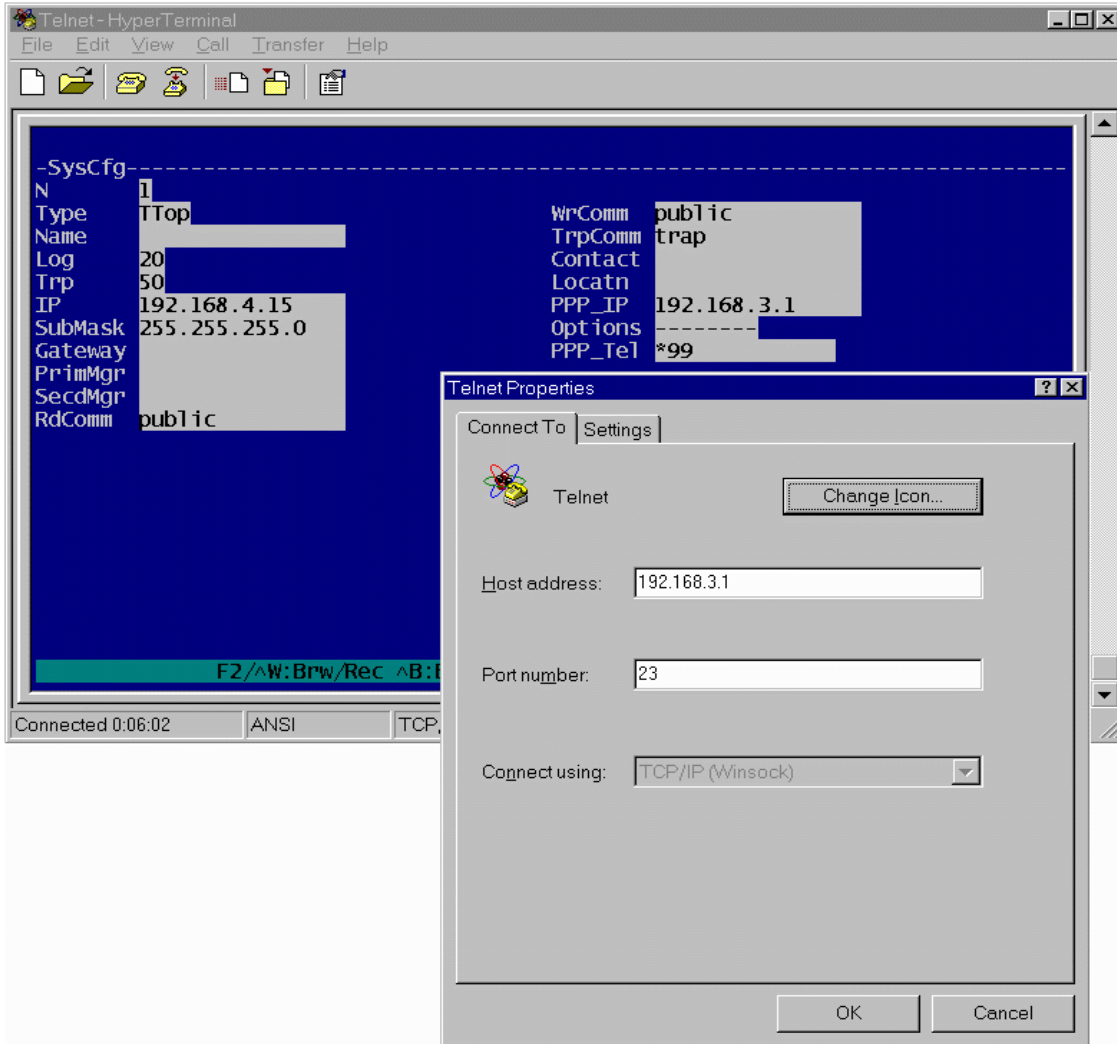
Now, IP-connectivity between the PC and the IntelliShare has been established. Of course you don't believe it. Open a DOS Box and try this:

```
C:\WINDOWS>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:

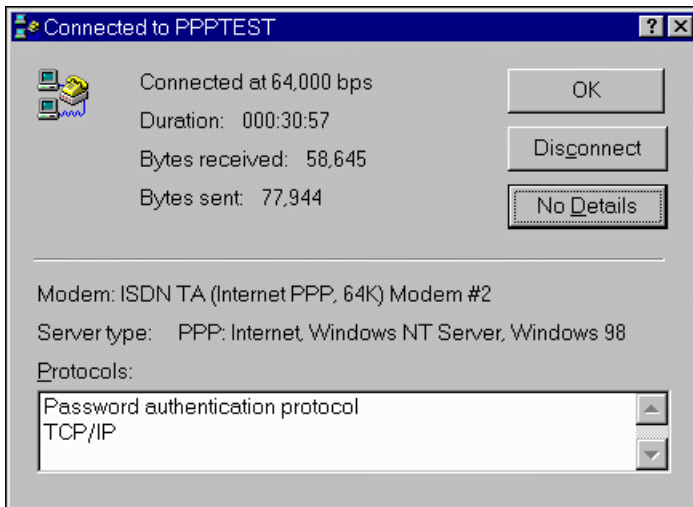
Reply from 192.168.3.1: bytes=32 time=96ms TTL=32
Reply from 192.168.3.1: bytes=32 time=100ms TTL=32
Ping statistics for 192.168.3.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```

To start a Telnet session, set the remote host address to the IntelliShare IP. And make a connection.

Note that you do not need to log in again: the log in from the PPP session is also valid for all other interactions over the PPP link, provided of course that you do not log out.



To end the PPP session, select the Dial-Up status window and choose disconnect:





As already mentioned, it is also possible to configure the IntelliShare to dial a predefined number at a certain moment in time, and establish a PPP session. Usually, you will want this kind of remote control, for example for collecting daily statistics through an SNMP management station.

To configure this, you will have to change some parameters in the System Configuration Menu and PPP menu. First you need to set the AlmTime (WIN.CFG.SYS.ALMTIME) parameter to a certain time of day, which will cause the IntelliShare to set up a call at that moment. The number that should be called is defined by the parameter OutCDN (WIN.CFG.PPP.OUTCDN).

In addition, you can define your own number, by filling in the OutCLI field (Calling Line Identifier) (WIN.CFG.PPP.OUTCLI). This can be handy for example to identify the IntelliShare that is calling the management station. The Timeout (WIN.CFG.PPP.TIMEOUT) parameter can be filled in if you want the IntelliShare to cut the connection when nothing is received from the other side. If you keep the field to zero, then the connection stays up, regardless if traffic is received on the line or not.

You should also define the lines on which a remote control call is initiated, by filling in the OutLine bitmask (WIN.CFG.PPP.OUTLINE). Flag in the OutLine bitmask the lines on which a remote control call should be attempted. The IntelliShare will, when initiating the call, choose whatever line is free from the list of marked lines.

At last, make sure that the SNMP parameters are set correctly (for a full explanation on how to configure your IntelliShare for SNMP access, please refer to chapter 0). This implies that you need to set at least the PrimMgr and TrpComm parameters correctly in the System configuration table.

When the alarm time is reached, an SNMP trap will be sent to the SNMP management station, which allows the management station to automatically retrieve statistics from the IntelliShare.

Remark that the same fields also apply when a trap is generated to a management station that is not located on the local LAN. In this case, an outcall will be attempted to the number specified, and an SNMP trap will be sent. This trap is generated when an important event happens which requires the attention of an operator or management system. In other words, such a trap will be generated when a certain event has an importance level that is equal or higher than the system parameter 'Trp' (WIN.CFG.SYS.TRP). For a list of the possible events, and their corresponding levels, see the chapter on 'Tracing, Logs and Traps' in the Reference Guide.

## Managing the IntelliShare with a web browser

Besides the ability to manage your IntelliShare through a Telnet connection, you have also the possibility to manage the IntelliShare through a built in web-interface. With the web-interface, managing the IntelliShare is user-friendlier than through a Telnet interface.

To be able to reach the IntelliShare with your web browser, you'll need to have installed the Softkey option ISU9932-SNMP (TCP/IP module), as your web browser connects to the IntelliShare using the TCP/IP protocol.

### Configuring your browser.

There are two ways you can access the web server of the IntelliShare. Or you have a direct LAN connection with your IntelliShare, or you remote dial-in to the IntelliShare.

In case you are directly connected to the IntelliShare, you must ensure that your TCP/IP stack is set up correctly. This basically means that you should follow the steps as described in chapter 'Managing the IntelliShare via the LAN.'

In case you have to dial in to the IntelliShare to reach it, you need to follow the steps as described in chapter 0 'Remote Control.'

Once you are sure you can reach the IntelliShare through TCP/IP (e.g. by pinging it), verify that your browser is configured correctly. This generally implies that your browser needs to be configured or for 'direct' (LAN) access, or that it uses a specific dial-up configuration, whatever is applicable.

Once you have verified this, open your Internet browser and point it to the IntelliShare. The simplest way to do this is by supplying the full IP-address of the IntelliShare as the Web Address, as in following example:

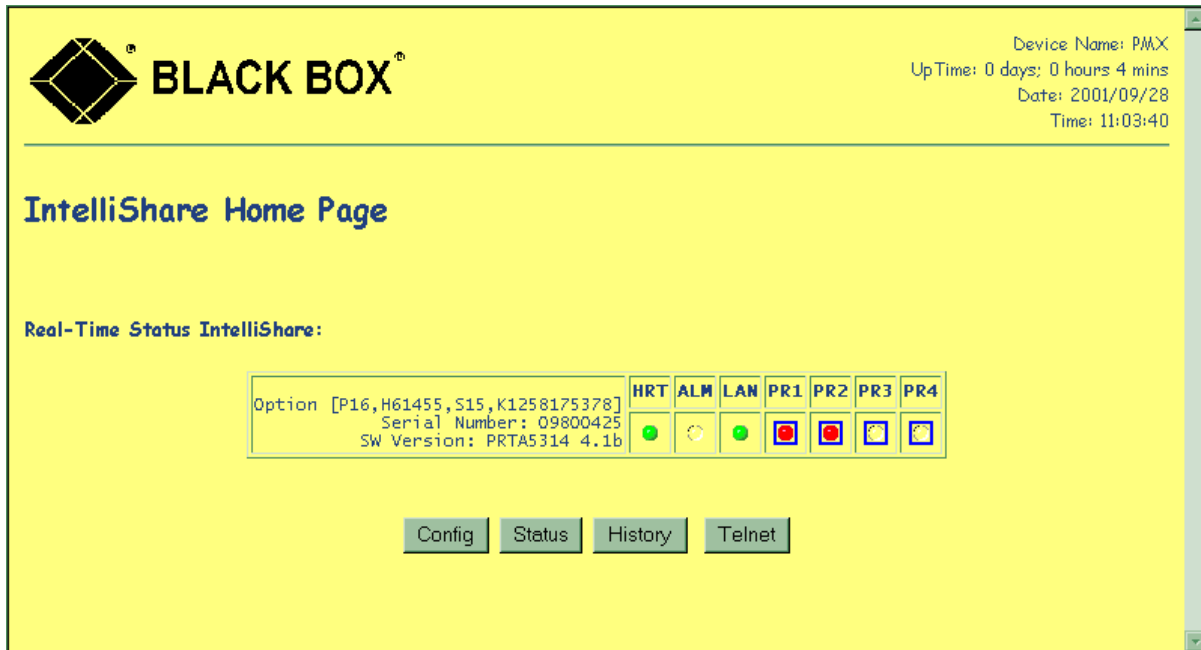
Address: <code>http://192.168.004.015</code>
--

Of course, if you have updated your Domain Name Server or hosts file with a name alias for your IntelliShare's IP address, you can fill in this alias in the Address field of your web browser.

If you have problems connecting to the IntelliShare, verify that you entered the IP-address correctly. If your web browser is configured for using a proxy server, and your IntelliShare is connected to your local LAN, verify that you are allowed to reach local web servers from your browser (if you are using Microsoft's Internet Explorer, verify that in the LAN settings of the Internet Options dialog box, you checked the box 'Bypass proxy server for local addresses').

If you are able to connect to the HTTP server, you'll get an authentication box in which you need to enter a username and password. This username needs to be one of the operators defined in the WIN.CFG.OPERATOR menu. If you logged in successfully, the IntelliShare will show you its 'home' page, as in following example:





Now you are ready to control the IntelliShare using your web browser.

## The IntelliShare web server.

*IntelliShare Home page.*

The home page contains following items:

- a simulated front panel of the IntelliShare. This front panel shows you the LEDs equivalent as the ones on the IntelliShare itself. If you have a VXI module installed, the corresponding LEDs will also be shown. It also shows the hardware and software options installed, the serial number, and the software version. Remark that you can click on the LEDs (for which a hyperlink is enabled) to jump to a summary page showing you the configuration, status, and history of the corresponding line.
- Links to the IntelliShare's configuration, status and history pages.
- A telnet button which launches your Telnet client and attaches it automatically to the IntelliShare.

*IntelliShare configuration, status and history pages*

The IntelliShare configuration, status and history pages can be accessed through a series of buttons on the home page. All these pages provide a menu interface similar to what the ANSI interface gives you if you connect with Telnet.

### *Configuration pages*

The configuration menu shows you the information contained in the "RUN" database. This is in contrast with the Telnet ANSI interface, which shows the config contained in the "EDIT" database.



Besides the config menu, the page contains also a link to download and/or upload *text* configuration information, as shown in following figure:

The 'Download Config' hyperlinks bring you to a new page containing the relevant configuration information in plain text format. You can store the info in this page to disk by saving it to a text file, using the 'File – Save As' function of your browser.

The 'Upload Config' field and buttons allow you to upload a configuration file to the IntelliShare. Supply the name of the file in the editable field directly, or click the browse button to search your local drive for it. Remark that you can only upload a *text* configuration file, with a syntax as described in the Reference Guide (see also chapter 'Saving and restoring configurations with XModem.').

Once you selected a file, click the 'Go!' button to upload the file. Depending on the size of the file, this can take a couple of minutes. When the page is uploaded, the browser returns the success or failure status of the upload process in a new page.

**Remark:** The Config upload command uploads the *edit* database to the device. Similarly, the Config download command downloads the *edit* database from the device. In particular, if you want to make the uploaded configuration the running configuration, it's necessary to perform a 'cfg run' command from the Telnet console. Alternatively, you can supply the 'cfg run' command together with the configuration file. Simply add the line '(Command, "cfg run")' after the 'Database' section. If the IntelliShare has stored successfully the configuration, the cfg run command will be performed automatically.

### **Status and History Pages**

The Status and History buttons on the Home Page bring you to a page containing a menu allowing you to view status and history information. Additionally, they contain a hyperlink to download the Status and History information in text format.

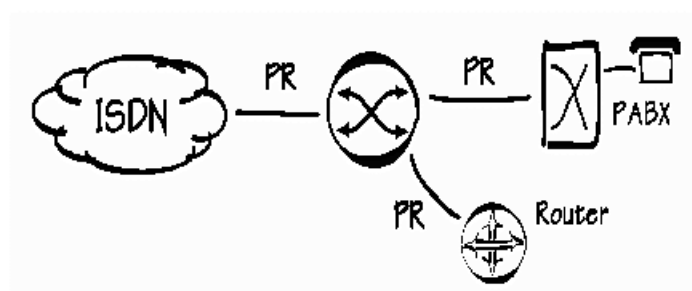


## Remarks

- The HttpRef field in the system configuration (WIN.CFG.HTTPREF) allows you to supply the IntelliShare with an interval in seconds at which the IntelliShare web server will refresh pages with dynamic data (such as status tables). A value of 0 in this field disables the refreshing of pages. Make sure that you take a value large enough not to overload the communications link or the web server. It is advised that you set the timeout to at least 20 seconds.
- The IntelliShare currently allows up to 3 simultaneous HTTP connections. This means that only three web browsers can consult simultaneously web pages of the IntelliShare. If a fourth web browser tries to reach the IntelliShare, it will be refused by the IntelliShare, saying that no connection was possible to the IntelliShare.

## PR-SHARE: Sharing a single PRI with multiple users.

### The application.



Today, most PRI access lines are used to feed a PABX. With the more common use of other equipment working on PRI lines (video conferencing systems, routers, etc..), the need has arisen to be able to share a single PRI equipment with multiple user terminals. Consider as an example sharing the PRI interface between the company PABX and a company WAN router with PRI interface. In some cases, it is also interesting to have multiple PABX's on the same PRI.

The IntelliShare provides possibilities to split the assigned range of phone numbers over multiple User (TE) equipment, so that the Net PRI can effectively be re-used.

In addition, the IntelliShare provides the possibility to impose limits on the number of B channels that can be used by the respective users.

### The configuration.

Start from a working factory default (optionally modified for LAN access) as described before.

As a first example, NT lines L2 and L3 share the single Net line L1 (note that you will need the L3 Soft-Key option to use at least three lines).

```

-Line-----0001--
N Type Name           Act Sgn Tei NT Crc4
1 PR   TO NET          On  Isdn 0  TE CRC4
2 PR   TO PABX         On  Isdn 0  NT CRC4
3 PR   TO ROUTER      On  Isdn 0  NT CRC4
4 PR   L4              Off  Isdn 0  TE NoCRC4
    
```

```

-Route-----0001--
N  Act LineISearch      Replace           LineOCalltyp  FailMin
1  On  1--- *98          *                --3- ----- 0
2  On  1--- *            *                -2- ----- 0
3  On  -23- *           *                1--- ----- 0
4  Off -----          -----          ----- 0
5  Off -----          -----          ----- 0
6  Off -----          -----          ----- 0
7  Off -----          -----          ----- 0
8  Off -----          -----          ----- 0
9  Off -----          -----          ----- 0
10 Off -----          -----          ----- 0
    
```

In this case, the route specifies that the incoming called number should be analyzed, and that the routing is to be made based on the last 2 digits. This assumes that the incoming calls will provide the full called number at once



(incoming setup is en bloc). This is normally the case, although it is theoretically possible that the network does not give adequate called number information.

The trace shows that calls are routed to R2, except when the called number ends with 98.

```
09:38:1478 R2 Connect 384720
09:38:3177 R1 Connect 384798
```

## Restricting bandwidth

In the above example, the resources on the Net PRI are used on a first-come first-serve basis. If L2 uses up all B channels, then L3 will not be able to make any calls.

So you may wish to restrict the number of calls that can be made by each User (PABX or router).

What needs to be done is to restrict the number of available B-channels on the line to the PABX (L2) and the router (L3).

Two methods can be used to achieve this: by restricting the channel range for incoming and outgoing calls on the PRI line for the PABX and the router, or by creating a nailed-up loopback for a number of channels on those lines.

The first method relies on the ability to reserve channels for incoming calls and outgoing calls, but works only if the User1 PRI line has a line configuration set to NT (which is usually the case). In our example, this would mean that we make only the first 22 channels available for incalls and outcalls, as configured in the next example:

```
-Line-----0002--
N          2
Type      PR
Name      TO USR
Act       On
Sgn       Isdn
Tei       0
NT        NT
Idle      x49
Crc4      NoCRC4
StrInc    0
EndInc    21
StrOutg   0
EndOutg   21
AlmFrom   1---
Options   -----
```

Line 2 is configured to use B-channels 0 to 21 for incoming calls (StrInc = 0, EndInc = 21), as well as for outgoing calls (StrOutg = 0, EndOutg = 21), which will force the IntelliShare to select a B-channel in this range for incoming and outgoing calls

Remark that *'Incoming'* and *'Outgoing'* is defined with respect to the IntelliShare, i.e. an incoming call is a call *entering* the IntelliShare, whereas an outgoing call is defined as a call *leaving* the IntelliShare. This effectively restricts the usage of B-channels to the first 22, and frees up 10 channels on the NET line for use by line 3.

Line 3 should be configured in the same way to have only 22 B-channels available, as such freeing up 10 channels on the NET line for use by line 2.

Remark that another practical usage of the fields StrInc, EndInc, StrOutg, EndOutg is for defining a range of B-channels for incoming calls, and a range of B-channels for outgoing calls. If for example you want to reserve B-Channels 0 to 15 for incoming calls, and B-channels 16 to 31 for outgoing calls, you would configure StrInc = 0, EndInc = 15, StrOutg = 16, EndOutg = 31. Certain types of PABX's sometimes require such a configuration.

Please be careful when restricting B-channels for incoming or outgoing calls. If this is done inadvertently, wrong settings can result in a failure of the line to accept or originate calls!

The second method is actually a kind of trick, which consists of making the IntelliShare believe that some channels are reserved for nailed up channels. The normal use of nailed up channels will be seen further. In this case just consider the following configuration

```

-FixN64-----0001--
N Act Name                NrTLineITSILineOTSOPContrl
1 On  Restr PABX acc      10 L2  22 L2  22 ----
1 On  Restr Rter acc      10 L3  22 L3  22 ----
3 Off F3                   0 NONE 1 NONE 1 ----
4 Off F4                   0 NONE 1 NONE 1 ----
5 Off F5                   0 NONE 1 NONE 1 ----
6 Off F6                   0 NONE 1 NONE 1 ----
7 Off F7                   0 NONE 1 NONE 1 ----
8 Off F8                   0 NONE 1 NONE 1 ----
9 Off F9                   0 NONE 1 NONE 1 ----
10 Off F10                 0 NONE 1 NONE 1 ----
    
```

Generally, nailed up channels are routed from one line (say L2) to another line (say L3).

The above configuration however specifies that 10 timeslots on L2 - starting with channel B22 - will be forced connected to themselves. This means that channels B22 to B31 are routed back to where they come from, thus creating a nailed-up (or fixed or forced) loopback.

The same setting has also been realised for L3.

In fact, these loopbacks are not the interesting aspect. The main result is that these 10 channels are not available anymore for switched ISDN calls. So this leads to the following situation:

- L2 will be able to use at most 20 B channels (30 – 10 used for the nailed-up loopback)
- L3 will be able to use at most 20 B channels (30 – 10 used for the nailed-up loopback)
- L1 will be able to use 30 channels (no restriction imposed).

In other words, both L2 and L3 will have a guaranteed 10 B channels at any time, and the remaining 10 channels (30 – 10 – 10) will be used on a first-come first-serve basis.

After reconfiguration and reset, the line status shows this as follows:

```

show sts l1 l4
N|Sts |PH|DL|BConn                |AlmF
1|ACT |Up|Up|-----|-----|----
2|ACT |Up|Up|-----|-----NNNNNNNNNN|----
3|ACT |Up|Up|-----|-----NNNNNNNNNN|----
4|IDLE|Dn|Dn|-----|-----|----
OK
    
```

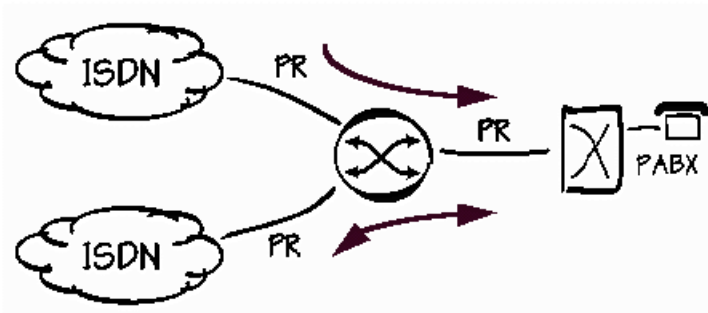
This same approach can also be used when the operator provides a Fractional PRI (in this case, only a limited number of B channels on the PRI can be used by the customer). In this case however, the network operator will need to specify which channels need to be blocked.





## PR-CHOICE: Least Cost switching to an alternative PRI.

### The application.



Providing telephone lines to the customer has finished being the monopoly of a single company. This creates the situation where multiple PRI lines are provided at the customer site, so that the customer is confronted with the need to choose between different operators.

This is where the CHOICE application comes in. As for the basic REDIAL application, the called number is analyzed. Based on specifications in the routing table an alternative PRI line can be selected.

The IntelliShare goes even further on this by providing the means to specify Fallback routes should the first choice be unavailable at the moment of making the call.

### Configuration.

Start from a working factory default (optionally modified for LAN access) as described before.

The alternative network operator is configured on L4.

All non-local calls are routed to L4, and all other calls are routed to L1 (compare this with the Carrier Prefix example).

```

-Line-----0001--
N Type Name          Act Sgn Tei NT Crc4
1 PR  TO NET1         On  Isdn 0  TE CRC4
2 PR  TO PABX        On  Isdn 0  NT CRC4
3 PR  L3              Off Isdn 0  TE NoCRC4
4 PR  TO NET2        On  Isdn 0  TE CRC4

```

```

-Route-----0001--
N  Act LineISearch      Replace          LineOCalltyp  FailMin
1  On  1--4 *              *                -2--          0
2  On  -2-- 0*            0*              ---4          0
3  On  -2-- *              *                1---          0
4  Off ----              -                -            0
5  Off ----              -                -            0
6  Off ----              -                -            0
7  Off ----              -                -            0
8  Off ----              -                -            0
9  Off ----              -                -            0
10 Off ----              -                -            0

```

The trace shows that numbers starting with 0 are routed using route R2, while the other numbers are routed using R3.

```
12:29:3467 R3 Connect 384060
12:30:2906 R2 Connect 0384060
```

What happens when L4 is not available?

Plug out the L4 cable, and dial the non-zonal number again: the call is now immediately routed using R3. In this case the call is disconnected because the number is not known on network L1.

```
12:35:1693 L4 PH DI
12:35:2306 R3 Disconnect cause 1, Fail=0
```

The explanation is as follows.

When choosing the route, the IntelliShare checks that the route is available.

If there is a physical problem or if all channels are in use, the route is not taken into account. Since route R3 is a default route, it will always match if no other routes are possible.

We may go further in defining fallback options, as is shown in the next example. Here, there is an intermediate fallback: if line L4 is not available, then the IntelliShare will route the call over L1 but will add a carrier prefix to select an alternative network operator.

```
-Route-----0001--
N  Act LineISearch      Replace          LineOCalltyp  FailMin
1  On  1--4 *                *              -2-- ----- 0
2  On  -2-- 0*              0*             ---4 ----- 0
3  On  -2-- *              12340*         1--- ----- 0
4  On  -2-- *                *              1--- ----- 0
5  Off -----                ----- ----- 0
6  Off -----                ----- ----- 0
7  Off -----                ----- ----- 0
8  Off -----                ----- ----- 0
9  Off -----                ----- ----- 0
10 Off -----                ----- ----- 0
```

When using alarm forwarding in this context, care should be taken to avoid that the user equipment (the PABX) comes into an alarm condition because one of the network routes (L1 or L4 in this example) becomes unavailable.

### Clock synchronization issues.

When using multiple networks, the issue of clock synchronization arises. Public networks are synchronized between them, so it is not really important which network will act as a provider of a clock source.

The IntelliShare always tries to slave on a NET line (line which are configured on the IntelliShare as TE), because the networks are supposed to give the clock. In the above example, L1 and L4 are possible clock sources.

The default rule for clock slaving is that at startup, the IntelliShare will first try to select the first PRI network on which a clock is detected (L1 in the example).

The selected clock can be checked in the System status screen as shown below.

```
-Sys-----
N Sts Date      Time      ClTrcHWErrs
1 ACT 2000/03/08 17:50:53 1 20 x0000
```



If for some reason the clock from L1 is lost (because the cable is plugged out), the IntelliShare will automatically switch to another available NET clock, in this case L4.

When the clock from L1 comes back, it will not be re-used as source, because the IntelliShare considers this NET line as less reliable than L4 (consider the case of L1 being loosely connected: resynchronizing on L1 might lead to a repetitive cycling between L1 and L4 with possibly undesirable side effects).

One can overrule this default action by specifying a line on which clock slaving needs to take place. In this case, the IntelliShare will first try the specified line for clock slaving. If the clock slaving is impossible on the specified line (because e.g. the line is non-operational), then the default action, as previously described will be taken by the IntelliShare. If the specified slaving line becomes operational again, then this line will be selected again as the line to slave the clock on.

The selection of the line to slave on can be done in the *ClkSlve* field in WIN.CFG.SYSTEM.

In the case where there is no clock source on any of the PRI lines, the IntelliShare will use an onboard oscillator (Free Run).

## Advice Of Charge Generation

### What is Advice Of Charge all about?

The generation of Advice of Charge (AOC) info allows an ISDN network to provide the caller with billing information about the current call. As such, the user can get notifications about the amount that he will get charged for his current phone-call. Remark that the Advice of Charge feature within ISDN only gives an *advice* about the amount that will be charged to the customer. For example, in some circumstances the network won't be able to retrieve all charging information about the current call, so the charging information given could be incomplete or not present at all.

There are three possible forms of AOC:

- AOC-S: Advice of Charge at the start of the call. The network provides at the beginning of the call (e.g. in response to a Setup request) information on the billing that the network provider will apply to the call. It won't give any information about the amount billed, but supplies the user with a method to 'calculate' the bill, as function of various parameters. AOC-S is seldom used, and as such not often implemented in ISDN-equipment.
- AOC-D: Advice of Charge during the call. The network provides information about the charges for the call in progress at fixed time intervals. At the end of the call, the total charges for a call are also given (as AOC-E would do).
- AOC-E: Advice of Charge at the end of the call. This AOC form supplies the caller with the total amount charged for a call at the end of the call.

The charging info can be provided in *Currency* format or in *Charging Units* format. AOC supplied in *Currency* format returns charging info in the form of an amount of money in a well specified currency. AOC supplied in *Charging Units* returns charging info in the form of an amount of units charged, where one unit corresponds to a certain pre-defined amount of money.

There exist different methods to supply AOC information within the ISDN community: one is within a keypad information element, another is within a facility information element. The IntelliShare only supports AOC within facility information elements.

### Generation of AOC by the IntelliShare.

The IntelliShare has the capability to generate Advice Of Charge information on its own, based on several configuration options. This way, you can supply your customers with information about the charges you apply to calls that they make.

The IntelliShare is capable of generating AOC-info during the call (AOC-D), and at the end of the call (AOC-E). This info can be supplied in both currency and units format.

Following are some situations where you might want to have the IntelliShare generate AOC information:

- When the network itself is not capable of generating AOC information on its own.
- When an alternative operator is reached by using a Carrier Select Prefix and the incumbent operator blocks any AOC info sent by the NLO. To circumvent this, the IntelliShare can supply the AOC information on its own.
- When adjustments are needed to the AOC info given by the network. For instance, for hotel chains, hotel customers are usually charged more for their phone calls than what is charged to the hotel-owner. In this case the IntelliShare could provide its own billing information to the hotel customers, regardless of what is charged to the hotel-owner.

Within the IntelliShare, the generation of AOC-info is done per route. This means that you configure a route for generating a certain charging pattern. So, if a call is switched through by the IntelliShare, the route taken for switching the call also determines the charges that will be sent to the originator of the call. This way, you can vary the charging depending on the number prefixes that are dialled, as well as on the type of the call (voice, data, ...), as a route is selected based on these two criteria.



It is obvious that only the originator of the call will receive AOC information, and only if the line to which he is connected is configured as an NT (network) line.

Remark that for calls for which AOC is enabled, AOC messages received by the IntelliShare from the network side of the call will be filtered out, such that the originator of the call only receives AOC information generated by the IntelliShare itself. On the other hand, for routes for which no AOC is configured, AOC information received by the network will be passed through transparently.

As a safety measure, there is a built in mechanism that will restrict the number of AOC messages on a particular line to one AOC message per second, regardless of the actual AOC messages. This prevents that equipment receiving AOC information gets swamped with AOC messages.

Each call for which AOC is enabled will generate at the end of the call a trace message stating the total amount of money that has been charged for the call. Also, the history database has a *Chrges* entry for each line and each route, showing the total cumulative charges applied to a line or route, since reset of the system.

### Configuring the IntelliShare for generating Advice of Charge.

Before you start configuring the IntelliShare for generating Advice of Charge, make sure you have purchased the ISU9932-AOC softkey (see chapter "AOC generation").

To configure the IntelliShare for generating Advice of Charge info, you need to follow a couple of steps:

Start by checking that some system level parameters are set correctly, as shown in following figure:

```

-Sys-----
N          1
Type      MPR          AOCType AOC-D
Name      PMX          AOCCTyp Unit
Log       20          AOCCurr
Trp       50          AOCMult 0.001
IP        192.168.004.001  IPRoute Off
SubMask   255.255.255.000  Masq    Off
Gateway   000.000.000.000  MasqIP  000.000.000.000
PrimMgr   192.168.004.111  RCNetIP 000.000.000.000
SecdMgr   000.000.000.000  RCMask  000.000.000.000
RdComm    public
WrComm    netman
TrpComm   trap
TLogOff   0
TFailsf   20
ClkSlve   AUTO
AlmTime   00:00:00
HttpRef   0
AOCEnbl   Off

```

First, make sure that the flag *AOCEnbl* is set to *On*. This flag will enable or disable the generation of AOC information for all calls. It is a convenient way to disable the generation of AOC info globally in case for example the PABX becomes overloaded due to the generation of AOC messages.

Secondly, you need to define in the *AOCType* field the type of AOC information to be generated: AOC-D or AOC-E. AOC-D enables the generation of AOC information while the call is in progress, while AOC-E only supplies a total amount charged at the end of the call. AOC-D has the advantage that the caller gets regular notifications about the amount he has been charged already, but has the disadvantage that the equipment receiving the info needs to be powerful enough to interpret the AOC messages quick enough. AOC-E only gives an amount at the end of the call, but poses a lesser load on the equipment.

Thirdly, you define the type of AOC information to be generated in the *AOCCtyp* field. If you choose *Currency*, AOC info will be generated in currency format. In this case, the *AOCCurr* and *AOCMult* fields apply. The *AOCCurr* field allows you to specify the abbreviated string (max. 4 characters) for the currency type string applied (e.g. BEF, USD, FRF, ...). The *AOCMult* field defines the multiplier that should be used for the charged amount. For example, if you define a charging of 625 per time interval in the charging profile (see further on)



and a multiplier of 0.01 is chosen, then the real charge applied will be an amount of 6.25 of the currency defined in the *AOCCurr* field per time interval.

If you choose *Unit* as the type of AOC information to be generated, then all charging will be supplied in units, in which a unit corresponds with a predefined amount of money. Remark that in this case, the *AOCCurr* and *AOCMult* fields are not applicable.

Once the system parameters are defined correctly, you need to configure each route with the necessary information about the charging applied to that route. The information about the conditions in which charging needs to be generated, and the amount of charges is actually contained in what is called a 'Charging Profile'. The 'Charging Profile' defines all the characteristics of the charging applied to a call, and as such determines the complete charging pattern for the call. A route record will refer to this charging profile to generate the necessary AOC charging for a call established on that route.

The IntelliShare stores charging profiles in a separate 'Charging Profile' database, which can be retrieved from the *AOC\_Profile* menu option (WIN.CFG.AOC\_PROFILE). The layout is shown in following example:

```

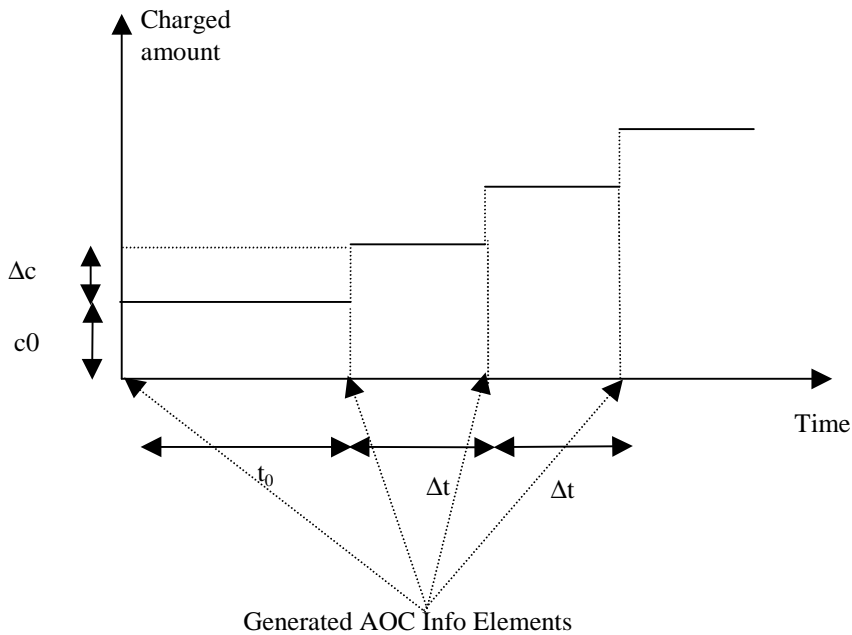
-AOCProf-----0001--
N  Act Label          Days      StrEndc0me  t0      DeltaCDeltaT
1  On  weekday peak    -MTWTF--  8  18  165  60      80      60
2  On  weekday off-peak -MTWTF--  18 8  165  120     80     120
3  On  weekend         S-----SH 0  24  100  120    100    120
4  Off
5  Off
6  Off
7  Off
8  Off
9  Off
10 Off
  
```

A Charging profile has the following parameters:

- **Act:** Activates the charging profile
- **Label:** a name that defines the charging profile, and through which it will be referenced from the route configuration (see further on)
- **Days:** bitmask of the days of the week for which the charging profile will apply. It has the format SMTWTFSH, where the first S stands for Sunday, M stands for Monday, and so on. The H stands for Holiday, and allows the user to select the profile for holidays. The holidays are defined in a separate database (see further on).
- **StrTime:** Start hour of the day for which the profile applies.
- **EndTime:** End hour of the day for which the profile applies. The time zone defined by the StrTime and EndTime parameters starts at StrTime and runs *until* the defined EndTime hour; that is not including the EndTime hour. Remark that the time zone defined by the StrTime and EndTime parameters can cross the midnight boundary, i.e. one can define a period from 18 h in the evening (6 pm) to 8 h the next morning (8 am).
- **c0:** The initial charged amount, which will be applied as soon as the call is connected.
- **t0:** The initial time interval in seconds for which the initial charging c0 applies.
- **DeltaC:** The incremental charge applied to a time interval DeltaT.
- **DeltaT:** The time interval in seconds after which a new increment DeltaC is applied.

The last four parameters define the charging pattern over time. With those parameters, one can define a charging profile as shown in following figure:





You define a 'free of charge' charging profile by setting the  $c_0$  and  $\Delta c$  parameters to 0. The  $t_0$  and  $\Delta t$  parameters will be ignored in this case.

You define a 'flat rate' charging profile by setting the  $\Delta c$  parameter to 0. The  $t_0$  and  $\Delta t$  parameters will be ignored in this case.

Looking back at the previous example, you can see that the first profile 'weekday peak' defines a charging profile for the week days at peak hours (between 8 am and 6 pm), with an initial charging of 165 units or currencies (depending on the system level parameter  $AOCCTyp$ ) during the first 60 seconds, and then an incremental charging of 80 units or currencies. The second profile, 'weekday off-peak' defines a charging profile during off-peak hours (between 6 pm and 8 am next morning), which is half as expensive as the 'weekday peak' profile.

Once you have defined all charging profiles that apply to your case, it is time to configure the routes to use a certain charging profile. This is done by setting the  $ChgProf$  field in the Route configuration to the label of the charging profile. The following example sets the first route entry to use the charging profile labeled 'weekday peak'.

```

-Route-----0001--
N          1
Act       On
LineIn    1234-----
Search    *
Replace   *
LineOut   -----9-
Calltyp   -----
FailMin   0
ChgProf   weekday peak
CliProf

```

It's of course possible to have multiple routes referring to the same charging profile.

You can configure holidays through the menu 'Holiday' (WIN.CFG.AOC\_HOLIDAY). The format is shown in following figure:

```
-AOCHDay-----0001--
N  Act Date
1  Off 01/01
2  Off 01/01
3  Off 01/01
4  Off 01/01
5  Off 01/01
6  Off 01/01
7  Off 01/01
8  Off 01/01
9  Off 01/01
10 Off 01/01
```

The Date field allows a month and day (in this order!) to be entered for the holiday you want to configure.

Remark that you can (and mostly will) define multiple charging profiles with the same label in the charging profile database.

In this case, if a route refers to a charging profile label, the first charging profile will be selected that matches the label *and* matches the time of day and day of the week. This way, you can define different charging profiles for different time zones, or for different days of the week.

For example, you might define two charging profiles with the label 'USA charging', one for peak hours, and one for off-peak hours, as in following figure:

```
-AOCProf-----0001--
N  Act Label          Days      StrEndc0me  t0      DeltaCDeltaT
1  On  USA charging    SMTWTFSH 8 18 25    60      15      60
2  On  USA charging    SMTWTFSH 18 8 25    30      15      30
3  Off                    ----- 0 0 0      0        0        0
4  Off                    ----- 0 0 0      0        0        0
5  Off                    ----- 0 0 0      0        0        0
6  Off                    ----- 0 0 0      0        0        0
7  Off                    ----- 0 0 0      0        0        0
8  Off                    ----- 0 0 0      0        0        0
9  Off                    ----- 0 0 0      0        0        0
10 Off                    ----- 0 0 0      0        0        0
```

If your route table contains a route that routes calls to the USA (e.g. by having a called number prefix that matches the international call prefix for the USA), you set the charging profile label for this route to 'USA charging', as shown in following figure:

```
-Route-----0004--
N          4
Act       On
LineIn    1234-----
Search    001*
Replace   001*
LineOut   -----9-
Calltyp   -----
FailMin   0
ChgProf   USA charging
CliProf
```

Each call on this route will have associated a 'USA charging' profile which matches the time of day and day of the week.





### Criteria for selecting a Charging Profile.

When a route is activated for a call, a charging profile needs to be selected for that route. The selection of a charging profile is based on the following:

The charging profile database is searched for the first profile that matches the label defined in the route configuration. Then, the current time of day and the day of the week are verified if they match the StrTime, EndTime and Days fields. If they match, then this profile will be selected. If not, the charging profile database is searched further on for an entry with the same label.

If no charging profile is found, then the IntelliShare will assume a *free of charge* call, i.e. this means that a charging info will be generated of 0 currencies or units at the end of the call.

If a charging profile is selected for a certain route, and the time of the day by-passes the time zone of the charging profile, another profile will be selected with the same label, as described in previous procedure. Because of the fact the charging profile database is searched from top to bottom, it is important that you order charging profiles with the same label such that the most specific ones come first.

## Calling Line Identification (CLIP)

### Controlling the Calling Line Identification (CLIP).

The CLI (calling line identifier) identifies the originator (his phone number) of a call. A check on the CLI is often used in end equipment as an additional security check. By verifying that the originator of the call is a known party, the risk of unwanted 'visitors' is reduced.

A second instance where the CLI is important is to identify the calling part towards the remote side for charging purposes. If the end user equipment specifies its own phone number in the CLI, then a more refined charging is possible.

In the situation where multiple customers are sharing a single PRI line, a control of the CLI is necessary to ensure that phone costs will be correctly assigned to the customer who makes the call.

A third case where control over the CLI is helpful occurs when calls are routed to two different networks. As each network uses its own subscriber numbers, a replacement of CLI numbers may be needed depending on the network to where the call is routed.

*Using a CLI check on incoming calls.*

Suppose that you wish to limit the routing of incoming calls to a well-defined group of remote users (which we call GROUP1 in this example). To do this, we need to specify that there is a CLIP check on the route, and we need to specify the CLIP check.

In the example below, we specify that route 1 will be enabled for all remote users in the DDI range 2325600 to 2325699, and to the remote user with phone number 2321357. As there are no other Clip checks with this label, an incoming call from a remote user other than those specified will be rejected.

```

-Route-----0001--
N      1
Act    On
LineIn 1234
Search *10
Replace *10
LineOut ---4
Calltyp -----
FailMin 0
ChgProf
CliProf GROUP1

```

```

-Clip-----0001--
N  Act  Label      Search      Replace
1  On   GROUP1     *23256??   *23256??
2  On   GROUP1     *2321357   *2321357
3  Off

```

If the CLIPprofile in the route entry is not specified, then no CLIP check is made.

If the CLIPprofile is specified, then it is required that the incoming call contains a valid CLI information, and that this CLI matches one of the Clip checks specified in the Clip table.

The CLIP check is part of the routing decision. If the Clip check fails, then an alternative route may be valid (in the example for instance, you could specify a default route to Lineout 9 without CLIPprofile which would route the other incoming calls to Line 9 instead of Line 10).



*Controlling the CLI of outgoing calls.*

Assume that two customers are sharing a single PRI line.

The first customer (CUST1) is connected on the second primary rate (line L10) and has subscriber number 2329900 to 2329999.

The second customer (CUST2) is connected on basic rate line L1 and has subscriber number 2311111 and a MSN number 2315555.

To ensure that outgoing calls from either customer will always have a correct CLI information, the following configuration may be used:

```
-Route-----0001--
N          1
Act       On
LineIn    ---4
Search    *
Replace   *
LineOut   ---4
Calltyp   -----
FailMin   0
ChgProf
cliProf CUST1
```

```
-Route-----0002--
N          2
Act       On
LineIn    1---
Search    *
Replace   *
LineOut   ---4
Calltyp   -----
FailMin   0
ChgProf
cliProf CUST2
```

```
-Clip-----0001--
N  Act  Label      Search      Replace
1  On   CUST1      23299??   23299??
2  On   CUST1      *         2329900
3  On   CUST2      2311111  2311111
4  On   CUST2      2315555  2311555
5  On   CUST2      *         2311111
3  Off
```

In this case, valid CLI's from customer1 and 2 will be passed through, while invalid or missing CLI information will be replaced by their respective base subscriber number.

## The IntelliShare as IP-Router

### The Application

Suppose you want to connect your internal LAN to the Internet through an ISDN connection. Until now, you had to have a dedicated router equipped with an ISDN BRI port, configured to dial up your Internet Service Provider (ISP) whenever you wanted to reach the Internet. Moreover, it required in many cases every host on your LAN to have a unique Internet address. As Internet addresses are nowadays very scarce (and expensive...), this approach is not feasible anymore if you have a lot of hosts on your LAN that need to be connected to the Internet.

With the BLACK BOX IP Routing software option, you have everything to solve your Internet access problems. With this software option, you can transform your IntelliShare into a performant Internet access router. The IP Routing software option allows every host on your LAN to connect to the Internet through an ISDN dial-up connection or fractional E1 leased line, without the need to acquire an Internet IP address for each connected host.

### The configuration

*Connecting to the Internet through a 64 kbit ISDN dial-up connection.*

This configuration example shows you how to configure the IntelliShare to dial up an ISP whenever traffic needs to be routed to the Internet. All you need for this is an Internet account from your ISP, and a telephone number to dial in. Of course, verify that your ISP is accessible through ISDN. Because most of the ISP's today offer free dial-up Internet access, this is a very economical way to connect all the hosts on your LAN to the Internet.



Configuring the IntelliShare for Internet access basically involves the activation of the IP router functionality, and the configuration of the information you received from your ISP into the PPP configuration table.

Before you start configuring the IntelliShare, make sure you have purchased the ISU9932-IPR Soft key. Next, you need to configure some systems level parameters, as shown in following figure:



```

-----Sys-----
N          1
Type      MPR
Name      PMX
Log       20
Trp       50
IP       192.168.099.001
SubMask 255.255.255.000
Gateway   000.000.000.000
PrimMgr   000.000.000.000
SecdMgr   000.000.000.000
RdComm    public
WrComm    netman
TrpComm   trap
TLogOff   0
TFailsf   20
ClkSlve   AUTO
AlmTime   00:00:00
HttpRef   0
AOCEnbl   Off
AOCType   AOC-D
AOCCTyp   Unit
AOCCurr
AOCMult   0.001
IPRoute On
Masq    On
MasqIP  000.000.000.000
RCNetIP 000.000.000.000
RCMask  000.000.000.000

```

- The IP field is the LAN IP address of your IntelliShare. Make sure that this is a unique IP address on your LAN, and belongs to your LAN's network IP address. The Network IP address is determined by masking the IP address with the bitmask as defined in the SubMask field. The network address in the above example is 192.168.099.000.
- Make sure that the IPRoute flag is set to on. This flag will enable the router functionality within the IntelliShare. This means that IP packets received on the LAN/ISDN interface, can be routed to the ISDN/LAN interface.
- In most cases, you will want the Masq field set to on. This flag will give you the possibility to activate IP Masquerading. IP Masquerading (also called Network Address and Port Translation (NAPT), sometimes Port Address Translation (PAT)), is a technique, described in RFC 2663, to translate private IP addresses of internal hosts into one unique Internet address. As such, it is a technique to allow multiple hosts to have connections to the Internet, using only one public Internet address. If you dispose of only one Internet IP address (either explicitly given by your ISP, or negotiated between your ISP's router and the IntelliShare when you set up a connection), you surely want this field to be set to on. However, if you want to connect two *private* IP networks together through a leased line, you don't necessarily need this feature.

The MasqIP, RCNetIP and RCMask fields in the System configuration table are not important for dialup connections, so let's take a look now at some settings in the PPP configuration table. The Point to Point Protocol (PPP) is the most important protocol to connect a device to an Internet Service Provider over a WAN link (in our case the ISDN dialup link). To connect successfully to your ISP provider, it is important that you set some PPP attributes correctly.

For dialup purposes, the highlighted PPP fields are important:

```

-----PPP-----
N          1
IPAddr   000.000.000.000
Timeout 300
InCDN     *99
InCLI     *
RemUser  MyISPAccount
RemPwd   MyISPPassword
OutCDN   031234567
OutCLI
OutLine  1---
LLine     NONE
LLStrTS   0
LLEndTS   0

```

- In most instances, the first parameter, IPAddr should be set to 000.000.000.000. This parameter denotes the IP address of the IntelliShare's side of the ISDN connection. As your ISP normally provides this IP address as part of the PPP negotiation process, you can safely set this parameter to 000.000.000.000.
- The Timeout parameter is an idle timeout in seconds after which the ISDN connection will be dropped.
- The RemUser and RemPwd parameters refer to the account you received from your ISP. Remark that these entries are case-sensitive.
- The OutCDN parameter is the phone-number to be dialled to reach your ISP
- The OutCLI parameter is 'your' phone-number, which you only want to provide in case the other side does a security check on it.
- The OutLine is the bitmask of lines on which the dial-up connection will be tried. The first free line in the bitmask will be tried.

If you configured these parameters correctly, you should now be able to make a connection to the Internet. Remark however that the IntelliShare won't make a connection as such. It will only start the connection setup when it received a packet on its LAN interface for which he decides that it should be routed to the Internet. This connection method is called *Dial On Demand*, which means that connections are only set up when there is a need for.

Now how will the computers on your LAN know that they should forward IP packets destined for the Internet to your IntelliShare? That's a topic for next paragraph.

### *Configuring your LAN for Internet access through the IntelliShare*

To allow your computers on the LAN to talk to the Internet through the IntelliShare, it is important that some IP parameters are set correctly on them. You will need to configure following parameters:

- You can choose the *IP address* of your computer as you want, but be sure that it belongs to the same subnet as the LAN IP address of your IntelliShare. It is advisable that the LAN's subnet is a private subnet (i.e. a subnet belonging to the range 192.168.0.0 to 192.168.255.255).
- The *Default Gateway* on your computer should point to your IntelliShare. More specifically, this means that the Default Gateway should be equal to the *LAN IP-address* of the IntelliShare. This is the IP-address as found in the WIN.CFG.SYS.IP field. Remark that this is *not* the IP address you received from your ISP.
- The *Primary and secondary DNS server* address must be set to the DNS addresses you received from your ISP. These addresses point to hosts of your ISP that are responsible for translating Internet 'names' (such as [www.BlackBox.co.uk](http://www.BlackBox.co.uk)) to real IP addresses.

As an example, suppose you decide to take for your LAN a network address of 192.168.4.0. Then, you could assign the LAN IP address of your IntelliShare 192.168.4.1, and your PC's LAN IP address 192.168.4.16. If your ISP Primary and Secondary DNS addresses are respectively 195.130.132.17 and 195.130.132.18, you should configure your Windows 98 computer's network card's TCP properties as follows:



IP Address:

**TCP/IP Properties** [?] [X]

Bindings | Advanced | NetBIOS  
DNS Configuration | Gateway | WINS Configuration | IP Address

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

Obtain an IP address automatically

Specify an IP address:

IP Address:

Subnet Mask:

OK Cancel

Gateway:

**TCP/IP Properties** [?] [X]

Bindings | Advanced | NetBIOS  
DNS Configuration | Gateway | WINS Configuration | IP Address

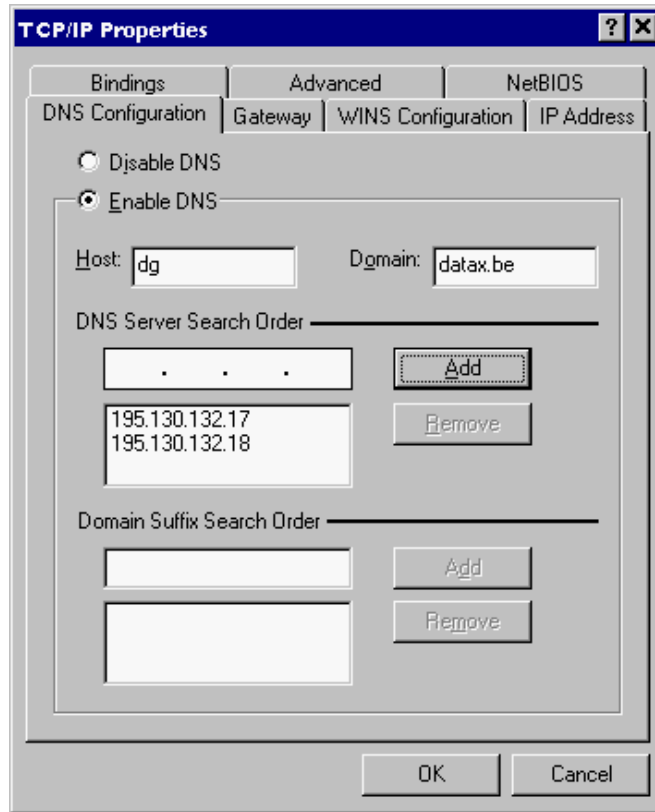
The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway:

Installed gateways:

OK Cancel

*DNS Configuration:*



*Connecting to the Internet through a Fractional E1 leased line.*

Although a 64 kbit dialup connection will be more than sufficient for small offices, larger offices will probably want to connect to the Internet using higher speeds. Moreover, if the Internet is frequently accessed, it will be more cost effective to have a permanent Internet connection. In this case, you might want to opt for a dedicated Fractional E1 leased line. The IntelliShare currently supports Fractional E1 connections with a speed of up to 256 kbps.



Configuring your IntelliShare for this setup is very similar to configuring it for dial-up access. First, set the parameters in the system configuration table the same way as for dial-up access. Second, you need to configure the PPP settings corresponding to the screen snapshot below:





```

-PPP-----
N          1
IPAddr    192.168.003.001
TimeOut   0
InCDN     *99
InCLI     *
RemUser   MyISPAccount
RemPwd    MyISPPassword
OutCDN
OutCLI
OutLine   ----
LLine     L1
LLStrTS   1
LLEndTS   4

```

- In a leased line configuration, the IP address of the local WAN interface normally will be fixed and given by your ISP beforehand. In this case, you will have to enter this IP address into the IPAddr field of the PPP configuration table.
- As the access to the Internet is through a leased line, the Access field needs to be set to *Leased*.
- The RemUser and RemPwd fields need to contain the username and password of your ISP account.
- The LLine field should contain the line on which the PPP connection needs to be initiated.
- The LLStrTS should contain the first timeslot of your fractional E1. (timeslots on the IntelliShare are assigned from 0 to 31; remark however that timeslot 0 is unavailable, as it is the timeslot that contains the framing signals of the E1).
- The LLEndTS should contain the last timeslot of your fractional E1. As the IntelliShare supports a maximum throughput of 256 kbps, only a maximum of 4 consecutive timeslots can be assigned.

In a leased line configuration, a couple of additional fields in the system configuration table require some attention. These are highlighted in the following screen snapshot:

```

-Sys-----
N          1
Type      IMX
Name      IMX
Log       20
Trp       50
IP        192.168.004.015
SubMask   255.255.255.000
Gateway   000.000.000.000
PrimMgr   000.000.000.000
SecdMgr   000.000.000.000
RdComm    public
WrComm    netman
TrpComm   trap
TLogOff   0
TFailsf   20
ClkSlve   AUTO
AlmTime   00:00:00
HttpRef   0
AOCEnbl   Off
AOCType   AOC-D
AOCCTyp   Unit
AOCCurr
AOCMult   0.001
IPRoute   On
Masq      On
MasqIP    000.000.000.000
RCNetIP   194.007.215.000
RCMask    255.255.255.000

```

- The MasqIP field denotes the IP address that will be used for Masquerading, i.e. it is the address that will be used in translating IP addresses of your internal private IP network to a public Internet address. If you don't fill an IP address in this field, the Masquerading IP address taken will be the IP address of the WAN interface of the IntelliShare, i.e. it will be the IP address filled in the WIN.CFG.PPP.IPAddr field. You should only fill in the MasqIP field when you want the Masquerading address to be different from the WAN Interface address (for example because the WAN Interface address belongs to a private network), and you have a public Internet address at your disposal that can be used as the Masquerading address.



- Once the IntelliShare has a connection to the Internet, you can manage the IntelliShare from the Internet using your web browser or telnet program. In this case, you should point your browser or telnet program to the Masquerading IP address your IntelliShare uses. This is of course very handy, but poses also a potential security problem, as every Internet user would be able to connect to your IntelliShare. This is especially true in a leased line configuration, where the IntelliShare is permanently connected to the Internet, and uses a fixed Internet IP-address.

To cope with this security issue, you can fill in the RCNetIP and RCMask fields. These fields denote the network address from which remote control is allowed. In the above example, this would mean that only hosts on a 194.007.215.000 network are allowed to have a telnet or web browser connection with the IntelliShare. All accesses from other networks will be blocked. We'll discuss security issues in greater detail in a next paragraph.

### Troubleshooting your Internet connection.

To verify your connection with the Internet, a IPRoute status table is provided with various status information on your Internet connection:

```

-IIPRoute-----
N Sts  MsqAddr      WANConn  MsqSess
1 ACT  000.000.000.000 Off      0
    
```

- The MsqAddr field is the address to which all source addresses of outgoing packets are translated to. If you have enabled Masquerading, you should see here a public Internet address (if you didn't configure your own Masquerading address, this will be an address received from your ISP).
- The WANConn field denotes the type of access you have to the Internet. Values are *Off* (no connection established), *Dialup* or *Leased*.
- MsqSess: This gives you an indication on the number of connections currently established with the Internet. Each TCP connection results in an equivalent internal Masquerading session.

If you encounter problems connecting to the Internet, here are some guidelines you can follow:

### If your IntelliShare is configured for Internet dial-up access

No dialup connection is made when I want to reach the Internet

- Verify that the following parameters are set on your IntelliShare:
  - IP Router functionality is enabled (WIN.CFG.SYS.IPROUTE field is set to on).
  - The PPP access method is set to dial-up (WIN.CFG.PPP.ACCESS field is set to Dialup)
  - In the IP Routing table, there is a route defined to the WAN, i.e. verify that you have a default route set to the WAN
- Verify that the network address of your host and of the IntelliShare is the same.
- Verify that your host's default gateway points to the LAN IP address of the IntelliShare.

A dialup connection is made, but when I look in the IPRoute Status menu, I see that the WANAccess field is set to 'off'.

This indicates that the PPP negotiation process with your ISP's router failed. Here are some reasons:

- Your account's username or password is incorrect. On your IntelliShare, you should see the following message: *'PPP remote login: Invalid user/pwd'*. Verify the WIN.CFG.PPP.REMUSER and WIN.CFG.PPP.REMPWD settings.
- Your ISP's router doesn't support Password Authentication Protocol (PAP). Check with your ISP.

A dialup connection is made, and in

The PPP negotiation process was successful, but there is a routing



<p>the IPRoute Status menu, I see that the WANAccess field is set to 'dialup'. However, I don't get any response from the Internet to my queries.</p>	<p>problem between the IntelliShare and the ISP. Here are some reasons:</p> <ul style="list-style-type: none"> <li>• Verify that Masquerading is enabled (WIN.CFG.SYS.MASQ field is set to on).</li> <li>• Check that the MasqAddress field in the IPRoute status menu (WIN.STS.IPROUTE.MSQADDR) is set to a public Internet address.</li> <li>• Verify that your host is configured with the DNS IP addresses you received from your ISP.</li> </ul>
---	---

#### If your IntelliShare is configured for leased-line Internet access

<p>When I look in the IPRoute Status menu, I see that the WANAccess field is set to 'off'.</p>	<p>This indicates that the PPP negotiation process with the remote router failed. Here are some reasons:</p> <ul style="list-style-type: none"> <li>• The remote router is not configured for PPP over HDLC. Both HDLC and PPP should be enabled on your remote router.</li> <li>• The range of timeslots assigned for IP-routing doesn't match the range defined on your remote router.</li> <li>• Your account's username or password is incorrect. On your IntelliShare, you should see the following message: <i>'PPP remote login: Invalid user/pwd'</i> Verify the WIN.CFG.PPP.REMUSER and WIN.CFG.PPP.REMPWD settings.</li> <li>• The remote router was unsuccessful in its authentication towards the IntelliShare. In this case, you'll see on the IntelliShare logger the following message: <i>'PPP local login: Invalid user/pwd'</i>. For security reasons, the IntelliShare always requests authentication from the remote. The account should be an operator as defined in the OPER configuration table, which has PPP privileges (i.e. the first bit of its Rights field of the operator should at least be 1).</li> <li>• Your remote router doesn't support the Password Authentication Protocol (PAP).</li> </ul>
<p>In the IPRoute Status menu, I see that the WANAccess field is set to 'leased'. However, I don't get any response from the Internet to my queries.</p>	<p>The PPP negotiation process was successful, but there is a routing problem between the IntelliShare and the ISP. Here are some reasons:</p> <ul style="list-style-type: none"> <li>• The IP address negotiation between the IntelliShare and the remote router was unsuccessful. Verify the WIN.CFG.PPP.IPADDR field on the IntelliShare, and the settings on your remote router.</li> <li>• If Masquerading is required, verify that Masquerading is enabled (WIN.CFG.SYS.MASQ field is set to on).</li> <li>• If Masquerading is required, verify the MasqAddress field in the IPRoute status menu (WIN.STS.IPROUTE.MSQADDR).</li> <li>• Verify the IP routing table of the IntelliShare. At least one route should point to the remote router.</li> <li>• Verify that your host is configured with the DNS IP addresses you received from your ISP.</li> </ul>

#### How to secure your network from malicious attacks.

As you are probably aware of, connecting your LAN to the Internet means that your network becomes vulnerable to malicious attacks from the Internet. Therefore, it is of a great importance that you spend a great



deal of time to secure your network and the IntelliShare. In this paragraph, we want to give you an overview of potential security issues, and how the IntelliShare can cope with those.

The most common attack on your network is what is called an *intrusion*, which means that some malicious Internet user is able to use your computer on your LAN for whatever reason. To be able to do this, the attacker must have the possibility to set up a direct TCP connection from his computer to your computer. For this, one thing he needs to know is your computer's IP address, and the type of TCP services your computer runs. Moreover, he must be able to establish an incoming TCP connection to a host on your LAN.

Therefore, a basic defense strategy is to

- disallow incoming connections from the Internet.
- hide your internal IP addresses and internal TCP services for an ordinary Internet user.

The Masquerading technique, used by the IntelliShare, has the pleasant feature that incoming Internet connections are impossible. Moreover, the Internal LAN IP addresses and services are effectively invisible from the Internet, as Masquerading translates the internal IP addresses into one public Internet address. As such, enabling Masquerading on the IntelliShare effectively protects your network from intrusion. This also means that you need to be aware of the following:

**Important: when Masquerading is disabled, the IntelliShare can *not* guarantee the security of your network. If you configure your IntelliShare to act only as an IP router without Masquerading, you need to add a security device - such as a Firewall - to your network, to protect it against malicious attacks.**

A next step in securing your network is to make sure that your gateway to the Internet (in your case the IntelliShare), is secured on itself, i.e. that no one can break into the device and change your configuration. The IntelliShare provides two protection mechanisms for attacks to itself:

- by restricting access to the device
- by protecting access with username / passwords.

The first is assured by configuring the RCNetIP and RCMask fields correctly, as already explained in previous paragraph. These fields allow control to the device only from hosts with an address belonging to the network specified by them. If you want to restrict access to one host, simply specify its IP address in the RCNetIP and set the RCMask field to 255.255.255.255.

Remark that if these fields are set, they apply to *all* types of access from *all* types of interfaces. More specifically, a Telnet or HTTP access originating from your local network will also be checked against these fields. If you want access from your local network, you will need to enter into these fields the network IP address of your local network.

The second protection mechanism involves setting the usernames and passwords to appropriate values. Remark that the default IntelliShare configuration is supplied with standard users, for which their password has been set default to the username.

**Important: It is strongly advised that you review all the default user accounts of the IntelliShare, and set their user names and passwords to appropriate values.**

Remark also that you can set each user with read / right / execute and protocol permissions. It is important that you choose carefully which users have what types of permissions on your IntelliShare.

For a complete explanation of the different types and levels of permissions, please refer to the reference guide.



## Advanced IP-Router configuration

### Configuration of static routes

The IntelliShare allows you to define up to 10 static routes. An IP route entry basically defines on what criteria the IntelliShare uses to route packets to a particular interface. You can enter IP routes in the IP\_StatRoute configuration table.

```

-IP_StatRoute-----0001--
N  Act NetAddr          NetMask          Gateway          Intface
1  On  000.000.000.000  000.000.000.000  000.000.000.000  WAN
2  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
3  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
4  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
5  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
6  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
7  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
8  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
9  Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN
10 Off 000.000.000.000  000.000.000.000  000.000.000.000  WAN

```

How does this routing work?

Suppose the IntelliShare receives a packet with a destination address of 194.7.215.16. First it will verify the address against the network address of its local LAN. If the destination address belongs to the network address of its LAN, it will send the packet to its LAN interface. If there is no match, the IntelliShare will scan the routing entries defined in the IP\_StatRoute configuration table, from top to bottom. The destination address of the packet is checked against the NetAddr and NetMask fields of each entry.

If the packet's destination address belongs to the network address as defined by the NetAddr and NetMask fields, the packet will be sent to the Gateway address as filled in the Gateway field on the configured interface (WAN or LAN). If no match is found, the packet is dropped, and the IntelliShare returns an ICMP 'host unreachable' packet.

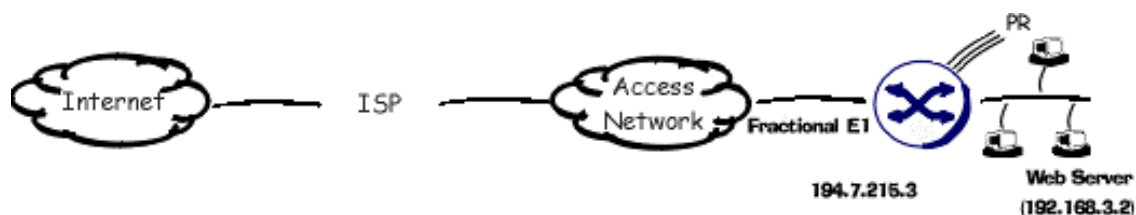
If the route points to the WAN interface, it is not necessary to fill in the Gateway address, as this is always the address of the remote router on the WAN link, which the IntelliShare has discovered during the PPP negotiation process.

Remark that one entry is by default already filled in: a default route to the WAN interface. This basically means that all packets that are not destined for the local LAN are routed to the WAN (dialup or leased-line) interface. This is exactly the purpose of an Internet access router.

In most circumstances, you won't need to change the default settings in the IP\_StatRoute configuration table. The only circumstance where you want to add a route is when you have multiple routers on your network, connecting other IP networks. In this case, you will need to add a route for each network that is behind the router on your network. The gateway will in that case be the router itself.

### Enabling Port Forwarding on the IntelliShare.

As already mentioned in a previous paragraph, Masquerading only allows outgoing connections (from your local network to the Internet). This is in many cases sufficient and even desirable. However, in some circumstances, you still want to allow incoming traffic, for example to provide access to an internal web server.



Suppose you have a web server on your LAN with address 192.168.3.2, that you want access from the Internet. To allow this, add an entry to the Port forwarding table as in following screen snapshot:

```
-IP_PortFW-----0001--
N  Act  DstPorAddress
1  On   80    192.168.003.002
2  Off  0     000.000.000.000
3  Off  0     000.000.000.000
4  Off  0     000.000.000.000
5  Off  0     000.000.000.000
6  Off  0     000.000.000.000
7  Off  0     000.000.000.000
8  Off  0     000.000.000.000
9  Off  0     000.000.000.000
10 Off  0     000.000.000.000
```

The DstPort field denotes the type of service, denoted by its TCP port number. For HTTP, the TCP port number is 80. The Address field denotes the IP address of the server that hosts the TCP service to be accessed from the Internet.

To access the web server, you have to point your browser to the Masquerading IP address, *not* the IP address of the web server itself. In our case, the address of the web server, as seen from the Internet is 194.7.215.3, not 192.168.3.1. As you see, Masquerading still masks the internal IP address of the host, even if it is accessible from the Internet.

A DstPort value of 0 acts as a wildcard, i.e. all services will be routed to the designated server. This is useful if you have an internal firewall, which is configured to block all unwanted services.

There is a potential conflict if you activate port forwarding for services also supported by the IntelliShare itself, namely telnet and HTTP. In this case, remote control to the IntelliShare for these services is not possible, except if the request came from a host that belongs to network as designated by the system fields RCNetIP (WIN.CFG.SYS.RCNetIP) and RCMask (WIN.CFG.SYS.RCMask). Instead, the request will be forwarded to the host defined in the port forwarding table.

## Remarks

- The IntelliShare can only support one PPP session at a time. In particular, this means that if your IntelliShare has a dial-up or leased line connection with a remote router, you can *not* have a dial-in remote control session. In other words, if a router connection is established, you can not manage the IntelliShare at the same time with a dial-in connection. In that case, you should manage the IntelliShare with HTTP or Telnet through the router connection it established. For example, if the IntelliShare has a connection with the Internet, you should manage the IntelliShare over the Internet.
- Remark that Masquerading is not transparent for all Internet applications. In particular, all applications that contain in their packets references to IP addresses are not sure to work correctly when Masquerading is enabled. Examples of applications that are not working reliably with Masquerading are:
  - RealAudio
  - H.323 (i.e. Microsoft Netmeeting)
  - Quake
- If Port Forwarding is enabled for one of the services with which you manage the IntelliShare (such as HTTP or Telnet), you can only access the IntelliShare if the network from which you want to access the IntelliShare has a network address equal to the one filled in the RCNetIP and RCMask fields of the system configuration table. Otherwise, requests will be transferred to the server referred to by the entry in the Port Forwarding table.
- If you enable Port Forwarding for FTP services, please remind that you should forward both TCP ports 20 AND 21 to have FTP functional. Also, remark that in this case only *passive* FTP connections will be allowed.



## SNMP

SNMP or "Simple Networking Management Protocol" is a standard that has been developed to allow the management of equipment in a uniform way.

To achieve this, every manageable object (read: configuration parameter) is uniquely identified using a sequence of numbers. For instance, the field WIN.STS.SLOT.SW is specified as:

```
1.3.6.1.4.1.1398.1.9.3.2.2.1.9          -- (the field WIN.STS.SLOT.SW)

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).BlackBox(1398).
BlackBox Products(1).IntelliShare(9).STS(3).SlotSts(2).
slotStsTable(2).slotStsEntry(1).slotStsSW(9)
```

The definition of these numbers, along with additional information on the associated fields, is collected in a file which is known as a MIB ("Management Information Base"). For IntelliShare, this file is called IntelliShare.MIB. This file must be loaded in the NMS (Network Management System), so that this system is able to access and represent the defined objects.

The example below shows the use of SNMP over a PPP Dial-Up connection.

The remainder of this section assumes that you have basic understanding of SNMP management.

### Configuring the IntelliShare for SNMP: basic settings

```
-Sys-----
N          1
Type      MPR                AOCType AOC-D
Name      PMX                AOCCTyp Unit
Log       20                 AOCCurr
Trp       50                 AOCMult 0.001
IP        192.168.004.015    IPRoute Off
SubMask   255.255.255.000    Masq    Off
Gateway   192.168.004.111    MasqIP  000.000.000.000
PrimMgr   000.000.000.000    RCNetIP 000.000.000.000
SecdMgr   000.000.000.000    RCMask  000.000.000.000
RdComm    public
WrComm    netman
TrpComm   trap
TLogOff   0
TFailsf   20
ClkSlve   AUTO
AlmTime   00:00:00
HttpRef   0
AOCEnbl   Off
```

The following elements can (must) be defined:

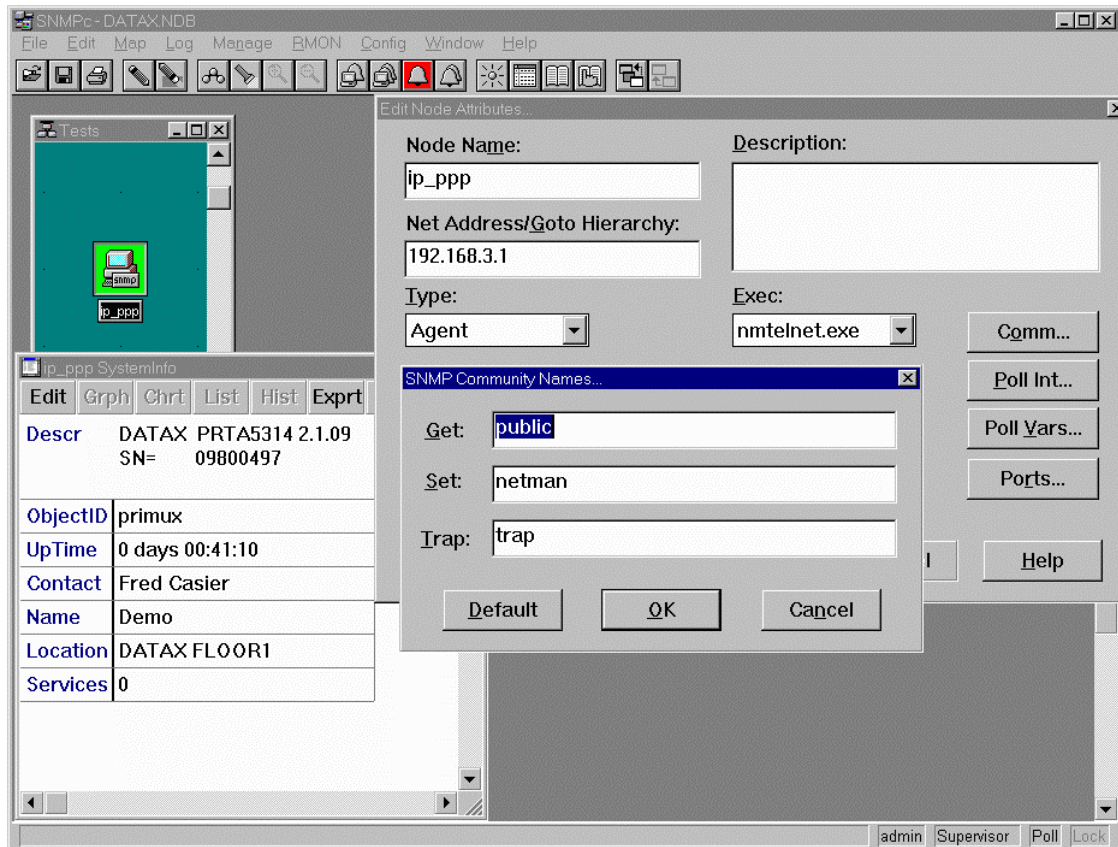
- **IP**            the IP address assigned to the unit. Ask your network manager.
- **SubMask:**    defines the local subnet. On a class C network: 255.255.255.0
- **Gateway:**    only required if the NMS is not on the same subnet.
- **PrimMgr:**    NMS IP address. Only required if traps must be sent to the NMS.
- **SecdMgr:**    Required if access is limited to 2 NMS's. Otherwise, any NMS passes.
- **RdComm:**    This must correspond to the read community on the NMS station.
- **WrComm:**    This must correspond to the write community on the NMS station.
- **TrpComm:**    The trap community name is given by IntelliShare along with the traps.
- **Trp:**        The trap detail level (0-99, a lower value gives more traps).

The fields Contact and Location are used by IntelliShare in the Mib-II system group. After modification the configuration must be activated, and the system must be reset.

### Installation and verification

Apart from the above configuration on the IntelliShare equipment, it is necessary to install the private IntelliShare MIB on the NMS. This MIB is delivered on the disk accompanying the equipment. In general, there is some option such as "LOAD MIB" which can be executed on the NMS.

The example below shows a basic SNMP access to the standard MIB-II system group, along with some of the required configuration settings. You may notice that this example uses SNMP over a Dial-Up PPP connection.



Verification of the installation can be done in the following steps:

- **PING:** Verification of the network connectivity. Enter PING <ip> from the NMS and check that the IntelliShare is sending replies. If not, then check cabling, the IP address and subnet mask. This test must succeed.
- **SNMP-MIB2:** Verification of basic SNMP access. On most NMS's there is a generic interface to the Mib-II system group. Perform a GET for this group and check that the equipment responds with the relevant information. If not, then check that the community names used by the NMS correspond with those configured on the unit. Note that small/capital case is significant.
- **SNMP-IntelliShare MIB:** Verification of the MIB integration within the NMS. One of the parameters in the system group is the System Object Identifier (ObjectID). This is a number which identifies the kind of equipment. Most NMS stations will translate this number to the symbolic string defined in the private MIB ("IntelliShare" for the IntelliShare). If this is not the case, it may be an indication that the MIB was not loaded or that some syntax error was encountered. Reload the mib and check any warnings. Most NMS have a "MIB-Browser" which allows to navigate the private mib and execute GET commands for groups and tables. Check that GET operations are possible. Do not worry at this moment if the response contains all '\*' characters (see operational issues). If GET's do not succeed, then there may still be MIB compilation problems. Check that the MIB corresponding with the equipment has been loaded.
- **SNMP-Traps:** If a primary manager (= manager to whom the IntelliShare will send traps) is configured, then check that traps are successfully handled. A simple test for this is to perform a "RES SYS" command on the IntelliShare. This will generate a standard WARM-BOOT trap. Note that the trap manager should not be a Dial-Up IP!





On most NMS's it is possible to define custom menu's and icons. You may wish to do this at this instant. Also, if possible, associate a Telnet command with the icon: this is generally an easier way to configure the equipment than using SNMP.

### Accessible parameters.

The IntelliShare MIB is divided into the following main sections:

- CFG: the read-only copy of the configuration (running configuration)
- STS: the read-only status information
- HISTORY: the read-only history information
- TRP: the last generated trap

The IntelliShare parameters cannot be changed through SNMP. Changing the configuration must be done either via Telnet (the most common approach), or via a HTTP file upload (containing the "CFG RUN" command), as described in chapter 0.

The only parameters that can be modified through SNMP are the writable MIB-II System Group parameters (e.g. name, contact, location).

### Traps

Traps are messages that are sent by the equipment to a "primary" network management system.

On the IntelliShare, these messages correspond to the Trace messages that are also shown on the screen. In order to limit the amount of traffic generated in this way, it is possible to specify a level of importance (WIN.CFG.SYS.TRP).

This level is used in the same way as the Trace level and as the Log level: every event which has an importance that is equal to or more than the level specified by TRP will be sent to the manager whose IP address is specified in WIN.CFG.SYS.PrimMgr (if not specified, then traps are disabled).

A simple test for this is to perform a "RES SYS" command on the IntelliShare. This will generate a standard WARM-BOOT trap

If the Primary Manager's IP address belongs to the local subnet, then traps will be sent on the local LAN. However, if you specify a trap manager IP address that is not belonging to the local subnet (i.e. for which the subnet doesn't correspond to the subnet address of the IP address specified in the WIN.CFG.SYS.IP field) *and* you didn't specify a gateway address (i.e. the WIN.CFG.SYS.GATEWAY field is 0), then an ISDN outcall will be tried to the ISDN number supplied in the WIN.CFG.PPP.OUTCDN field. This ISDN number should correspond to the ISDN call-in number of the trap manager.

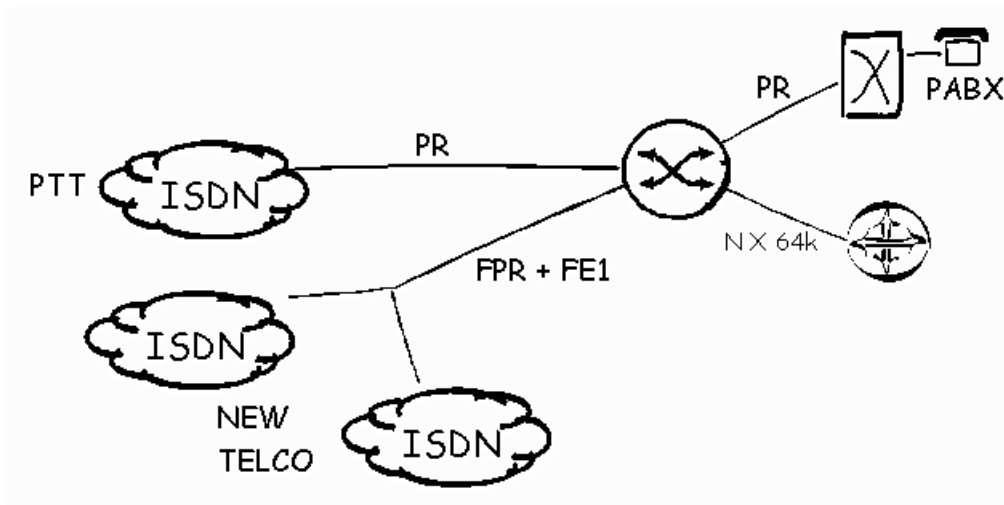
With this functionality, you can have IntelliShare's call in remotely to a central management system, notifying the management system about serious events.

To avoid the possibility of a flood of outcalls in case a serious problem generates a huge amount of traps, only one such an alarm call can happen per hour, i.e. after a successful alarm call is generated, a second alarm call will only be made after at least an hour. Remark that an alarm call won't be retried if it failed a first time.



**PR-COMBI: Fractional E1 and ISDN on a single PRI.**

**Application.**



Many companies are confronted with the need for leased lines along with the need for switched (dial up) lines.

The IntelliShare provides an attractive solution for this situation which can be exploited by operators who are able to combine nailed up circuits and ISDN controlled circuits on a single PRI line.

An example is the use of nailed up circuits for online Internet Access, combined with support for a classic PABX.

**Configuration.**

Start from a working factory default (optionally modified for LAN access) as described before.

The network operator will specify the channels that are used for nailed up circuits. Let us assume that channels B22 to B31 are all used for internet.

On the customer site, these 10 channels need to be split off from the provider's PRI line (L1), and will be routed to L3 which is connected with a Router using a G703 interface (example).

To achieve this, the Line and Port configurations are specified as follows

```

-Line-----0001--
N Type Name           Act Sgn  Tei  NT  Crc4
1 PR   TO NET1         On  Isdn 0   TE  CRC4
2 PR   TO PABX         On  Isdn 0   NT  CRC4
3 PR   TO ROUTER      On  Isdn 0   NT  CRC4
4 PR   L4              Off  Isdn 0   TE  NoCRC4
    
```

```

-FixN64-----0003--
N Act Name           NrTLineITSILineOTSOPContrl
1 On  F2             10 L1  22 L3  22 ---
2 Off F3             0  NONE 1  NONE 1  ---
    
```

Note that L3 has been defined as connected to a TE. The TE equipment is expected to retrieve the clock from the IntelliShare.



```

-Line-----0001--
N Sts  PH DL BConn                      AlmFrom
1 ACT  Up  Up  -----NNNNNNNNNN-----
2 ACT  Up  Up  -----NNNNNNNNNN-----
3 ACT  Up  Up  -----NNNNNNNNNN-----
4 IDLE Dn  Dn  -----NNNNNNNNNN-----

```

As a result of this configuration, 10 successive channels (B22,B23,..B31) from L1 will be routed to L3 starting at B1 (so L1.B23=L3.B1, L1B24=L3.B2, and so on).

For the PABX, nothing is changed. It is still allowed to assume that it has access to all channels. The IntelliShare will do whatever is needed (channel negotiation, checking of available channels) to ensure correct operation.

As a consequence, this operation can be combined with any of the applications described in prior chapters.

## VXI Module: Fractional E1 on a V35, V36 or X21.

### The application

The COMBI application describes how a fractional E1 leased line circuit can be extracted from a fractional PRI and routed to one of the G704 interfaces. In many cases, this will prove to be a perfect solution. However, your end equipment may be equipped with a serial interface instead. If this is the case, then the VXI module is for you. Since the data is delivered as a serial stream, it is important that the sequence of timeslots can be treated as a single "big" slot: the time consistency must be maintained within this sequence of slots. Check this with the provider in case of uncertainty.

The VXI module is an optional extension card that can be placed in the same housing as the main card, and that provides up to 4 V35, V36 or X21 compliant interfaces. The selection between V35, V36 and X21 is made through the use of the correct cable.

### Enabling the VX ports.

First of all, you should ensure that the IntelliShare firmware is enabled for operation with the VXI module. Boot the IntelliShare and look carefully at the boot messages. Expect to see something like this:

```
> [other boot messages]
> VXI 1--- .. Enabled
```

This indicates that the IntelliShare firmware is enabled for port P1 on the IntelliShare. This is the normal case if you ordered the VXI module together with the IntelliShare. If more than 1 port is enabled, you will see them as shown below (ports 1,2,3,4 enabled).

```
> [other boot messages]
> VXI 1234 .. Enabled
```

If the VX ports are not enabled, then you will see

```
> VXI ..... Disabled
```

To enable ports on the VXI module, you need to install the SoftKey options. Please contact the manufacturer for more details.



## V35, V36 and X21 cables

The VX interface is generic. The choice between a V35, V36 or X21 interface is made by ordering the correct type of cable.

- DX\_C2\_VX\_V35\_T :V35 Cable
- DX\_C2\_VX\_V36\_T :V36 Cable
- DX\_C2\_VX\_X21\_T :X21 Cable

In the human interface screens, the control signals are indicated as follows:

On Screen	V35/V36 meaning	X21 meaning
S	DSR	does not exist
C	DCD	I
T	DTR	T
M	TMI	does not exist
L	LL	does not exist
D	DL	does not exist

## Configuration.

### Example

As an example, assume that your provider delivers a fractional PRI on line L1 with a fractional E1 in slots 24 till 31 (512 Kb/s), and with ISDN in slots 1 to 23 (16 used for ISDN signaling). The ISDN channels are routed to the PABX as shown in several previous examples. The fractional E1 stream is routed to VX port P1 using the FixN64 menu.

```

-FixN64-----0001--
N Act Name                NrTLineITSILineOTSOPContrl
1 On Fract-E1             8 L1 24 P1 1 ----
2 Off F2                  0 NONE 1 NONE 1 ----
3 Off F3                  0 NONE 1 NONE 1 ----
4 Off F4                  0 NONE 1 NONE 1 ----
5 Off F5                  0 NONE 1 NONE 1 ----
6 Off F6                  0 NONE 1 NONE 1 ----
7 Off F7                  0 NONE 1 NONE 1 ----
8 Off F8                  0 NONE 1 NONE 1 ----
9 Off F9                  0 NONE 1 NONE 1 ----
10 Off F10                0 NONE 1 NONE 1 ----

```

```

-FixN64-----0001--
N      1
Act    On
Name   Fract-E1          --
NrTS   8                 -- number of subsequent timeslots
LineIn L1                -- L1 (operator PRI)
TSIn   24                -- start at B24
LineOut P1               -- VX interface P1
TSOut  1                 -- use 1 for VX interface
PContrl ---             -- normal behaviour for control lines

```

Note that "Lineout" is now not really the G704 line interface, but the VX port interface instead. Since the VX datastream is serial, there is no need to specify a starting timeslot on P1, so use 1.

The field PControl specifies how the VX control signals should be used. Note that the VX port will only act on these settings when the port is active (i.e. when the port is specified in an active FixN64 configuration line).

The default settings ("----") specify that:

- The clock will be delivered by the VX port to the end equipment (typical DCE behaviour). The VX uses RxClk (CT115) as well as TxClk (CT114) to deliver the clocks.
- Te DSR (and CTS) control signals will be asserted by the VX port as a reaction on the DTR of the end equipment.
- The DCD signal will be asserted when the corresponding PRI line interface is physically active. When maintenance conditions are active, then the behaviour of DCD differs as described below.

When toggled ON, non-default behaviour is selected:

'X'	Use of 'External Clocking'. The VX port delivers the RxClk (CT115) for the RX data. It is assumed that the DTE will synchronize on this signal for received data, and will produce its own clock for the data that it transmits to the DCE. This clock is transmitted on Tx'Clk (CT113). The VX port then uses Tx'Clk to receive the Tx data.
'S'	The DSR signal is always asserted (when the VX port is enabled and active)
'C'	The DCD signal is always asserted (when the VX port is enabled and active)

*Status indications and LED behaviour.*

Basic status indication is available from the slot status screen (WIN STS SLOT). The second line shows information on the VXI hardware (serial number) and firmware version. Also, the current state of the LEDs can be seen (in this case, port P1 shows a red led).

```

- Slot -----0001--
N Sts SW HW LED
1 ACT PRTA5314 4.0 09700630 g--RR-----
2 ACT PRTA5333 1.0 09800301 b R-----
    
```

```

-FixN64 -----0001--
N Sts PortSts
1 ACT -----
2 IDLE -----
3 IDLE -----
4 IDLE -----
    
```

The port specific information (status of the control signals) can be seen in the FixN64 status screen (WIN STS FIXN64). The PControl field shows the status of the signals "XSCMTLD".

X	<b>Off</b> indicates (normal) internal clocking. <b>On</b> indicates external clocking (CT 113 clock from DTE).
S	<b>Off/On</b> indicates that DSR and CTS to the DTE are <b>Off/On</b> .
C	<b>Off/On</b> indicates that DCD to the DTE is <b>Off/On</b> .
M	<b>Off</b> indicates that there are no maintenance conditions. <b>On</b> indicates that either local loop (LL) or digital loop (DL) are active.
T	<b>Off/On</b> indicates the status of the DTR signal delivered by the DTE.
L	<b>Off/On</b> indicates that the internal Local Loop has been activated
D	<b>Off/On</b> indicates that the internal Digital Loop has been activated.

The LEDs also provide status information. **Note** however that the Heartbeat and Alarm LEDs are not active on the VXI module. The LEDs for the ports P1, P2, P3 and P4 will act as follows:

Off	Port is not enabled (Softkey) or not active (No config line in FixN64).
Green	Data is being routed from an active G704 interface to the VX port.
Red	Corresponding G704 interface is not activated or not working.
Yellow	Maintenance condition exists.



*Maintenance conditions*

It is possible to set the VX port in a local or digital loop using the maintenance commands. When a loop is active the port LED will turn yellow and the TMI signal will be asserted.

To set a local loop for P1, use the command **SET LOOP LL P1**  
 To set a digital loop, use **SET LOOP DL P1**  
 To turn off the loops, use **SET LOOP OFF P1**

Note that the VX Port will not act on the maintenance signals that can be delivered over the V35/V36 interface.

**SW Upgrade on the VXI module.**

Since the SW on the VXI module resides in FLASH EPROM, a SW upgrade is as simple as a file transfer. In general the following upgrade procedure may be applied:

1. Connect ANSI terminal to the control port of the VXI module by using appropriate conversion cable : insert jack plug into jack receptacle on front of the VXI module.  
 Note that the serial speed of the control port is now set to 9600 bit/s. Change the speed setting on your ANSI terminal if necessary.
2. Enter the '**BOOT**' command from the Human Interface.  
 Note that the VXI LED's turn yellow.
3. Once in the maintenance menu, the following commands are available:  
**ID**: shows the identification of the product.  
**UPGRADE**: starts the upgrade procedure.
4. Enter the '**UPGRADE**' command to start an X-modem file receive session (character 'C' will appear).  
 After entering this command, the operator should send the 'vxi.bin' file which can be found on the 'SW' directory of the SW upgrade floppy.

```
? ID UPGRADE
UPGRADE
Erasing and waiting for <update>.BIN upload
C
```

5. As soon as the VXI confirms receipt of the complete file, the new SW type and revision is displayed. At this point the operator may power down the IntelliShare.

```
? ID UPGRADE
UPGRADE
Erasing and waiting for <update>.BIN upload
C..2668 Pkts.
OK
PRTA5333 1.0
```

6. Power on the IntelliShare again. After a successful selftest the VXI module will start up with the factory default settings for the configuration.

**REMARK!**

If some fault occurs during the X-modem file transfer, you must repeat the upgrade procedure as described above, with the following differences :

2. Instead of logging-in and entering the '**BOOT**' command, power down the system and place jumper JP65 on the VXI module (located behind the LEDs).  
 Power on the system again.
6. In addition to powering down the system remove jumper JP65 on the VXI module.

## **Other applications.**

The IntelliShare is a versatile platform and we are often surprised of the applications that are considered by our customers. Let us know about yours, and maybe we can do something to make things even better.

