TMS Management (TELDAT Management System) (V1.7.0)

User Manual

Doc. Dm266-I Rev. 2.0

April, 2002

INDEX

Chapter 1
Introduction

1. Introduction

Figure 1 displays the management generic environment of the Teldat solutions for access to company Internet/Intranets.

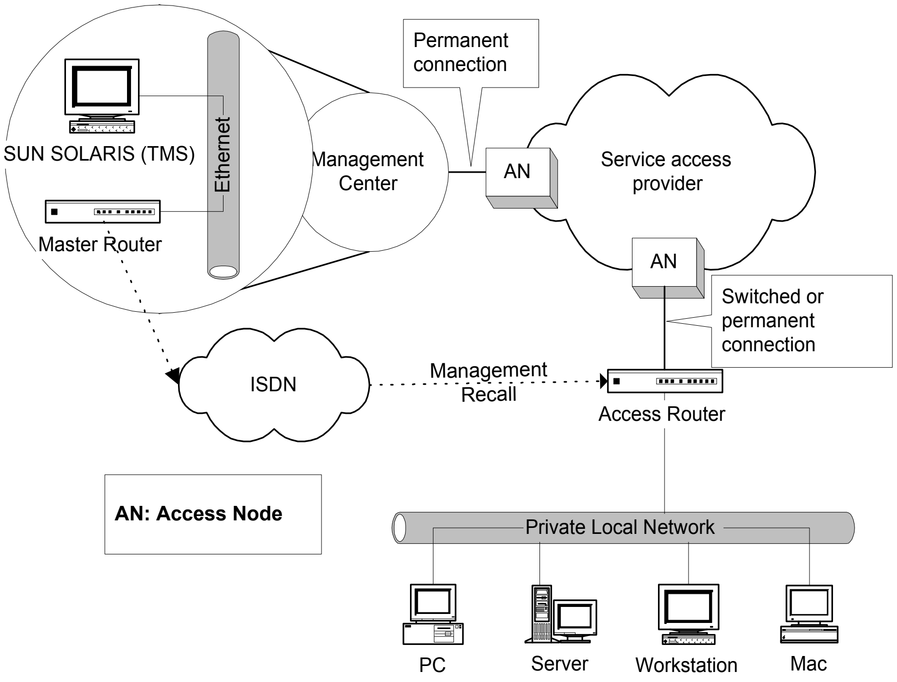


Figure 1 : TMS generic management scenario

Two principal elements participate in this scenario: the management center and the access router.

The **management center**, in the premises of the service providers, is the place (centralized) from which the registered clients access routers are managed. This consists of the management application (TMS), the database and a 'wake up' router (known as the **master router** from now on) for remote devices in order to execute management in cases of ISDN access.

The **access router** is a TELDAT device that connects the registered client's local network with the contracted services (Internet/Intranet). This can be an ISDN/PSTN (or XOT) access router or an ADSL access router.

As you can see in the figure, in cases where the access router is ISDN, the TMS systems includes a procedure for starting management through an ISDN management call. In this way, you can always manage the ISDN access devices, independently of whether they are connected to the network or not and independently of the fact that connection is carried out with a distinct IP address each time as the system automatically discovers what address is being used to connect each time.

2. Management System Functionalities

- **Homogeneous system and made to measure.** As indicated in the section on advantages of the system, this offers a simple and homogeneous vision for the operator. The function of the system is similar, independently of whether the device access is executed from a switched network. You only need to configure those things that are really necessary for the required operations, consequently the systems gains in simplicity and ease of handling.
- **Dynamic learning of the access router's IP address.** The TMS management application dynamically learns which IP address has been used to connect with the access routers when management is required. In this way, you can access the device for management purposes even though this connects through a different IP address each time. This functionality simplifies and makes the management process very flexible at the same time as saving IP addresses.
- **Multi-display / Multi-operator**. The management system permits simultaneous operation with various service operators in various management terminals. The system is protected against management collisions thus avoiding the situation where different operators simultaneously manage the same device.
- **Operations over groups.** A versatile tool for operations over groups is available. Through this it is possible to plan, operate and monitor common operations that have to be carried out over groups of the clients installed base. For example, you can plan remote software updating for all the access routers pertaining to a determined client.
- **Professional database.** The entire management platform is supported over a powerful database. The result is a rapid, powerful and flexible management tool that provides the possibility of generating detailed reports on use and incidents as well as enabling a centralized and controlled operation of all the system, including the registering and de-registering of clients (handling of files), start up of management etc.
- **Automatic accounts collection.** The Teldat remote access devices support the saving of traffic and operations statistics in non-volatile memory. The management application periodically collects the said stored statistics thus enabling the possibility of generating reports on service use and traffic for the end client.
- **Management is always guaranteed.** One of the key requirements in order to offer this service is that whenever management for a device is requested, this is available for the said management. I.e., if the device is not connected then it connects and if there are no physical channels available to carry out management connection, one of the busy channels is released in order to do this. In this way, swift reaction response can be carried out when the end client requires configuration changes, solutions for breakdowns etc.
- **Events Register.** For service control and use of this register, you can, for example, generate operator activity reports, events reports (breakdowns) for the installed devices etc.

Chapter 2
Installing the TMS management

1. Requirements prior to installation

Hardware Requirements

* SUN Ultra 5 station or higher.

* CD-ROM reader.

* Oracle 7.3 Workgroup Server or higher:

    * 32 RAM Mbytes (128 recommended).

    * Three times the swap space RAM size.

    * 700 Mbytes free space in disk.

* TMS Management:

    * 128 RAM Mbytes.

    * 200 Mbytes free space in disk for the application itself.

    In order to manage up to 4000 devices:

        * 120 Mbytes free space for database table data.

        * 30 Mbytes free space for configuration files (should these be used).

        * The space required for the statistic files depends on the regularity these are processed and the traffic present in the devices.

Software Requirements

* SOLARIS 2.5.1 or 2.6 Operative System (complete installation).

    * Packet "Font Server Cluster".

    * Patches required for ORACLE 7.3 (source {ORACLE:2, 97}:

        * 103640-01 or higher.

    * Packets required for ORACLE 7.3:

        * SUNWarc.

        * SUNWbtool.

        * SUNWhea.

        * SUNWlibm.

        * SUNWlibms.

        * SUNWsprot.

        * SUNWtoo.

        * SUNWmfrun.

        * Motif Libraries with the following minimum patches:

            103461-07

* ORACLE 7.3.

* For documentation and help, a browser that can display HTML format must be installed.

2. Instalation of Oracle 7 Workgroup Server Version 7.3.3.0.0

2.1. Prior System Requirements

Oracle Workgroup server installation requires a minimum of 32 RAM memory and 700 MB hard disk.

As regards the operating system, for correct installation of the Oracle database management, the following packets must also be installed:

Operating System	Software requirements
Solaris 2.x	SUNWbtool
	SUNWtoo
	SUNWsprot
	SUNWarc
	SUNWlibm
	SUNWlibms
	SUNWhea
	SUNWmfrun

In order to check the existence of these packets, you can execute the following command:

```
>pkginfo -i SUNWbtool SUNWtoo SUNWsprot SUNWarc SUNWlibm SUNWlibms SUNWhea SUNWmfrun
```

The result should be:

```
system              SUNWarc       Archive Libraries
system              SUNWbtool     CCS tools bundled with SunOS
system              SUNWhea       SunOS Header files
system              SUNWlibm      SPARCCompilers Bundled libm
system              SUNWlibms     SPARCCompilers Bundled shared libm
system              SUNWmfrun     Motif Runtime Kit
system              SUNWsprot     Solaris Bundled tools
system              SUNWtoo       Programming tools
```

If one of the above packets is not installed, you can install it with the help of the following command

```
#pkgadd -s /cdrom/cdrom0/s0 SUNWbtool SUNWtoo SUNWsprot SUNWarc SUNWlibm SUNWlibms
SUNWhea SUNWmfrun
```

For Solaris 2.x, in addition to the already mentioned parameters, it is also necessary to install a series of operating system parameters. In order to do this, edit the file **`/etc/system`** as root and add or modify the following parameters:

```
set shmsys: shminfo_shmmin    = 1
set shmsys: shminfo_shmmni    = 100
set shmsys: shminfo_shmmax    = 209715200
set shmsys: shminfo_shmseg    = 50
set semsys: seminfo_semmns    = 1750
set semsys: seminfo_semmni    = 70
```

In the **$TELDATMS/db/etc** directory, you will find a file **system.teldat,** this contains these parameters and they can be copied over the **/etc/system** if this does not contain any other relevant information.

Once you have modified the said file, restart the station so the new parameters take effect.

2.2. Installation Procedure

The Oracle Workgroup Server installation consists of executing the **wgstart** scrip found in the Oracle CD-ROM in the **/cdrom/oracle/wgstart** directory and then following the steps indicated by the manufacturer. We recommend the following initial assignment of users and passwords:

User	Password
wguser	oracle7
oracle7	oracle7

When the screen requesting the ORACLE installation directory appears, you need to put the **GEST** string in the SID field. We recommend using **Spanish** and the **WE8DEC** set of characters. Subsequently, in the management user environment, the ORACLE_SID environment variable should contain this same string (GEST).

Once the installation has been completed, you need to edit the **/etc/rc2.d/S84tcplsnr** file and verify if the directory where the ORACLE has been installed coincides with that that appears within the file. We also need to comment on (by placing the # character at the beginning of these lines) the second **'if'** in the file**.** If this operation is not executed, on restarting the station, a prompt such as the one shown below will appear:

```
LSNCTRL>
```

where you have to introduce the following commands:

```
LSNCTRL>start
LSNCTRL>quit
```

which permits you to continue restarting the station.

You also need to copy the **libsunmath.so.1** library, included in the ORACLE CDROM in the **$ORACLE_HOME/lib** directory.

3. Installing the TMS Management Center

The principal TMS management center applications are:

tmsdefgo Definition of groups and operations over groups.

tmsgroupop Operations over groups (accounts collection, reconfiguration etc.).

tmsmonauto Monitoring of automatic collection of fortnightly accounts.

tmsmongo Monitoring of the operations over groups.

tmsconfig Launches the NOVACOM and Teldat Cx devices configuration application.

tmsmanager Launches the database maintenance application and the communication with the master routers in order to manage the access devices.

tmsmon Launches the daily and fortnightly monitoring application for the NOVACOM and Teldat Cx devices.

For optimum screen presentation, you need the “Font Server Cluster” packet installed, this packet is included in the SOLARIS 2.5.1 operating system CDROM. You can use the **admintool** tool for the installation procedure.

Before proceeding with the TMS management installation, you must create a management user (or assign an existing one, although we recommend the first option).

The TMS management is supplied in a CD, which you introduce in the unit connected to the management station

From this point, follow the following agreement “For those commands that must be executed as root, the system prompt will be the ‘#’character, while for those commands that have to be executed as management user, the prompt character is ‘>’.”

In order to guarantee that the system incorporates the CD in the file system, execute (as root):

```
#volcheck
```

IMPORTANT: If this a version updating process, you are advised that in the installation process that **you will lose all the data** stored in the database. Therefore it is the responsibility of the user to **make a backup copy** of the said data **before** beginning the process.

3.1. TMS software Download

Currently, in the CD distributed as the software packet, there is the version displayed plus one line in the lower part similar to the following:

```
#pkgadd -d /cdrom/cdrom0/tms170.
```

This is the command that you need to execute (as root) in order to begin the installation.

NOTE: the period displayed at the end of the command forms part of the file name, therefore this must be included in order to execute the command.

The following screen will appear:

```
The following packages are available:
  1  TMS170     TELDAT Management System (V1.7.0).
                (sparc) 1.7.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Press ‘1’ or return (default option).

During installation, the installer is asked a series of questions in order to ensure the correct installation of the software.

The installer is asked which directory the whole of the downloaded files system should be installed in. A route is offered by default, however the installer may change this if he deems this to be appropriate. If the installer wishes to use the default option, simply press the carriage return key.

```
TMS root directory [/opt/TMS/V1.7.0]:
```

The ORACLE root directory (this was previously installed). In this case a default value does not exist and it is essential to enter the route where the ORACLE has to be installed.

```
ORACLE root directory:
```

User created for management or assigned to this end. By default the option of *management* group *management* user is offered, which must exist before beginning the installation process.

```
TMS user: [gestion]:
Group of gestion: [gestion]:
```

In order to correctly view the help, you must have a browser installed in the station.

You request the complete browser route which will be assigned to the **TMSHELPBROWSER** environment variable in the installation process, however this can be changed at any time.

```
Help browser:
```

Among the options requiring configuration, you will find the option to install (or not) the dynamic IP addresses discovery demon, **IPDiscover**. If you have to manage devices whose IP addresses are going to be dynamic, the demon must be installed; contrariwise this will not be necessary. Independently of this answer, if in the future you are going to need IPDiscovery, you can access this without needing to repeat the installation process.

```
Do you want to install Teldat IP Discover (See manual for further information)?
(y/n):
```

Finally, a summary of the introduced data is presented with the possibility of changing it should there be any errors.

```
TMS root directory:     /opt/TMS/V1.7.0
ORACLE root directory:  /opt/oracle
TMS user:               gestion
Group of gestion:          gestion
Help browser:           /opt/TMS/netscape/netscape
Teldat IP Discover:     y
Are you agree with this parameters?  (y/n): y
```

From this point on the installation process commences, however if the base directory does not exist a message is displayed asking if you wish this to be automatically created.

```
The selected base directory </opt/TMS/V1.7.0> must exist before
installation is attempted.

Do you want this directory created now [y,n,?,q] y
```

The downloading of the files takes a few minutes. A message is presented for each downloaded element.

Once the packet is installed, you can view the properties through the “admintool” tool as root:

```
#admintool
```

By selecting “Browse->Software->Application Software” the list of installed applications appears.

The following step consists of establishing the environment variables for the management user and adjusts the database.

3.2. Ajusting the Database for the TMS Management

a) *Configuring the LISTENER and the name translator*

Supposing the base directory path where the ORACLE was installed is contained in the ORACLE_HOME environment variable and two files need to be modified:

1. the $ORACLE_HOME/network/admin/tnsnames.ora file where the Management Center applications connection string is defined, which is **tms_tcp_GEST**. The management user **ORATMS** environment variable must contain this same string.

```
tms_tcp_GEST =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL= TCP)(Host= machine_name)(Port= 1521))
    (CONNECT_DATA = (SID = GEST))
  )
```

   where ***machine_name*** is the name of the machine where the database is installed or in its defect, the IP number. If the installation is as client you need to enter the name (or IP number) of the machine that contains the database server in this field.

2. the ORACLE_HOME/network/admin/listener.ora file should have an aspect similar to that shown below:

```
LISTENER =
  (ADDRESS_LIST =
        (ADDRESS= (PROTOCOL= IPC)(KEY= tms_tcp_GEST))
        (ADDRESS= (PROTOCOL= IPC)(KEY= PNPKEY))
        (ADDRESS= (PROTOCOL= TCP)(Host= machine_name)(Port= 1521))
  )
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME= machine_name.)
      (ORACLE_HOME= /opt/oracle)
      (SID_NAME = GEST)
    )
    (SID_DESC =
      (SID_NAME = extproc)
      (ORACLE_HOME = /opt/oracle)
      (PROGRAM = extproc)
    )
  )
STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10
TRACE_LEVEL_LISTENER = OFF
```

Once these actions have been carried out, restart the station once again and pay close attention to the start up messages in order to detect any possible errors in the installation.

b) Configuring the ORACLE (TABLESPACES, ROLLBACK, …)

Once the TMS software is downloaded and as a management user, execute the following script

```
>$TELDATMS/script/tmsdbini.sh
```

where TELDATMS is the management base directory.

If this a version updating process, you will see that the script presents errors that are not significant.

In order to create the management application database, execute the following scrip as management user:

```
>$TELDATMS/script/tmsdbcreate.sh
```

If this a version updating process, all the tables will be deleted and re-created. As previously mentioned, it is the sole responsibility of the user to make a backup copy of the data before beginning the installation process.

3.3. Environment Variables

a) General Variables

For the correct operation of the TMS management applications, it is necessary to configure certain environment variables. This is as simple as adding a lie in the management user start file, which depending on the type of shell is file ***.cshrc*** or ***.profile***.

In order to find out which shell is being used, you can use the following command: (as management user):

```
>echo $SHELL
```

If the shell is “csh” or “tcsh” edit the **`.cshrc`** file in the management user’s home directory and add the line:

```
source root_directory/script/teldatms.csh
```

where ***root_directory*** is the route where the management software is downloaded.

If the shell is "sh", “ksh” or “psh”, then in the management user’s home directory file **`.profile`** add the following line

```
. root_directory/script/teldatms.env
```

Note: This line begins with the dot and space characters.

For connection with the ORACLE database, the **ORACLE_HOME**, **ORACLE_SID** and **ORATMS** variables are particularly important. **ORATMS** contains the character string through which the Management Center applications connect to the database.

For automatic start up of the **ipdiscover** demon, you must configure the **IPDBOOT** variable, which can be “*y*” (should you wish for the said start up) or “*n*” if you wish to work without discovery (this is initialized with the option selected in the installation).

All the applications with user graphic interface have been developed with the **ILOG Views version 2.4.1**. tool. This tool stores the information associated to the screens in files with the extension “ilv” that are read on initializing the application. So that the ILOG can locate these files, you need to establish the environment variable **ILVPATH** with the value **`"$TELDATMS/ilv`** ".

b) Variables for the IP Discover functionality

Finally, in order to ensure correct functionality for the IPDiscover program, you need to configure the following parameters in the **`$TELDATMS/etc/ipdiscover/ipdiscover.ini`** file:

- DBServerName: database server name.
- DBServerType: type of database server.
- DBUserName: database user.
- DBPassword: user password.
- Inactivity: Maximum inactivity time for a device in minutes. When a device with a dynamic IP address does not send information within a period of time less than the inactivity time, it is considered unavailable.

The rest of the file values can be left with their default values.

On installing the management, this file copies some default values which the user must check.

The default values are:

```
DBServerName = tms_tcp_GEST
DBServerType = ORACLE
DBUserName = tms
DBPassword = tms
DBName =
DBRole =
Inactivity = 1
```

4. Database

The TMS Management uses an ORACLE database version 7.3 (or higher) where the following tables are defined:

`acc<device_code>_<entity>`	Fortnightly accounts tables.
`Auto`	Results table of the last automatic collection of the fortnightly accounts
`conf<device_code>_<entity>`	Configuration tables for each device.
`Device`	Table containing the files for the devices that are managed.
`go_log`	Log table of the operation over groups.
`go_op`	Operations over groups of devices.
`Groups`	Table of the groups of devices.
`Infomanaged`	Table containing the devices managed by the masters and by static IP addresses.
`Infodevice`	Device information table: Serial number, board number, software version, and BIOS version.
`Managed`	Table indicating which devices each master manages.
`Mancalls`	Table containing the management calls history with the start and end call date and time.
`Master`	Table of available master routers.
`mon<device_code>_<entity>`	Mirror tables of the fortnightly monitoring applications lists of each device.

These tables are available to the user to be exported to other formats or databases, to generate reports or construct any other application over them.

Space requirements:

We estimate that in order to manage 4000 devices with device code 37 with their configurations stored in the database, you need a data file of approximately 80 Mbytes .

Initially, the file is sized at 5 Mbytes and as the devices are incorporated in the database, the data file automatically expands.

Chapter 3
TMS Management

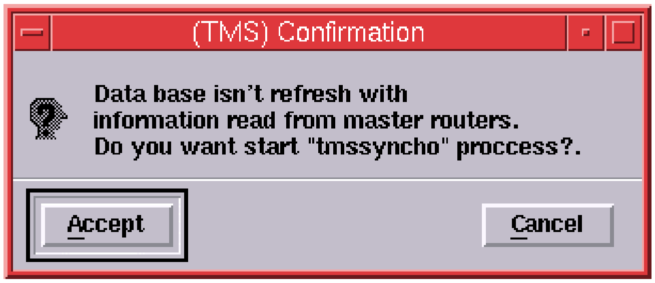
1. Introduction

The TELDAT TMS management is supported by a set of independent applications that communicate through the same ORACLE database, two permanently executing background processes and an operations over groups application:

tmsgroupop	Operations over groups.
tmsconfig	Configuration of devices.
tmsmanager	Maintenance of devices and master routers database.
tmsmon	Monitoring of the devices daily and fortnightly accounts.
tmssynchro	Updating of the database with information periodically collected from the master routers.
IPDiscover	Updating of the database with information periodically collected from the devices with dynamic IP addresses.

2. Management of TMS Devices

The **tmsmanager** application uses an ORACLE (version 7.3) database to store the master router and TMS device data as well as the devices' fortnightly accounts. This database is updated through two processes: the **tmssynchro** process, which periodically queries the devices table managed by the master routers registered in the database and the **ipdiscover** process that updates the database with the IP addresses of the devices whose address is dynamic. Periodically the application checks that the **tmssynchro** process is being executed. If this is not happening, the following message appears permitting the user to launch this from the application


(TMS) Confirmation

Data base isn't refresh with
information read from master routers.
Do you want start "tmssyncho" proccess?.

Figure 2 : tmssynchro process start up confirmation

There can be multiple instances where the **tmsmanager** application simultaneously executes over the same station, the local database or even over another remote database connected to the station.

In cases where the application works with a remote database, it is not necessary to execute the **tmssynchro** process in the local station. This is because the database is already being refreshed with the **tmssynchro** process from the remote station. In this case, in order to disable the check on whether the said process is being executed or not, simply execute the following:

```
$TELDATMS/bin/tmsmanager -ncs
```

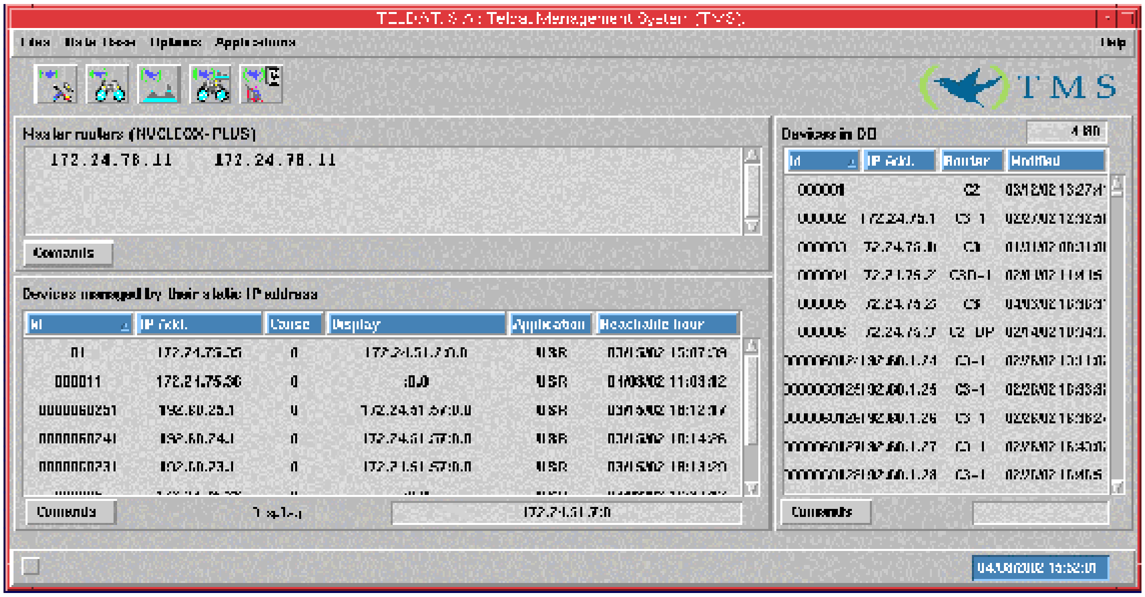
(ncs = no check tmssynchro)

Depending on the installation options, if you have elected not to install the discovery demon, the **ipdiscover** start up must be explicitly enabled through:

```
$TELDATMS/bin/tmsmanager -ipd
```

(ipd = ipdiscover)

On start up, the **tmsmanager** application establishes a connection with the database (local or remote) and from there, the periodic query in order to detect changes in the status of the managed devices or other changes provoked by other possible management users operating over other diverse application instances.



Master routers (NUCLEOX-PLUS)

172.24.78.11 172.24.78.11

Devices managed by their static IP address

Id	IP Add.	Cause	Display	Application	Reachable hour
01	172.24.75.25	0	172.24.51.7:0.0	USR	03/15/02 15:07:29
000011	172.24.75.30	0	:0.0	USR	01/03/02 11:03:12
0000060251	192.60.25.1	0	172.24.51.57:0.0	USR	03/15/02 18:12:17
0000060741	192.60.74.1	0	172.24.51.57:0.0	USR	03/15/02 18:14:26
0000060731	192.60.73.1	0	172.24.51.57:0.0	USR	03/15/02 18:13:20

172.24.51.7:0

Devices in DB 4 80

Id	IP Add.	Router	Modified
000001		C2	03/12/02 13:27:4
000002	172.24.75.1	C3-1	02/27/02 12:32:3
000003	172.24.75.11	C3	01/31/02 09:31:0
000004	172.24.75.7	C3D-1	02/11/02 11:41:5
000005	172.24.75.25	C3	04/03/02 16:36:3
000006	172.24.75.3	C2 UP	02/14/02 10:34:3
0000060124	192.60.1.24	C3-1	02/25/02 13:11:5
0000060125	192.60.1.25	C3-1	02/20/02 10:35:4
0000060126	192.60.1.26	C3-1	02/26/02 16:36:2
0000060127	192.60.1.27	C3-1	02/26/02 16:40:0
0000060128	192.60.1.28	C3-1	02/27/02 16:46:5

04/03/2002 15:52:07

Figure 3 : Main screen for the management application

This screen is made up of various sections that are further explained in the following paragraphs.

2.1. Main menu

I. Files

A. TMS Backup

See the chapter on Backup of all the TMS management data.

B. Exit.

Exits the application.

II. Database

A. Export

Consult the section on Exporting from the database.

III. Options

A. Options

IV. Applications

A. Configuration

B. Monitoring

C. Automatic accounts collect

D. Monitoring of automatic accounts collect

E. Operations over Groups

V. Help

Displays the content of the application help.

2.2. Tool Bar

Launches the devices configuration application.

Launches the devices monitoring application.

Launches the automatic collection application for fortnightly accounts of the devices.

Launches the automatic collection monitoring application for fortnightly accounts of the devices.

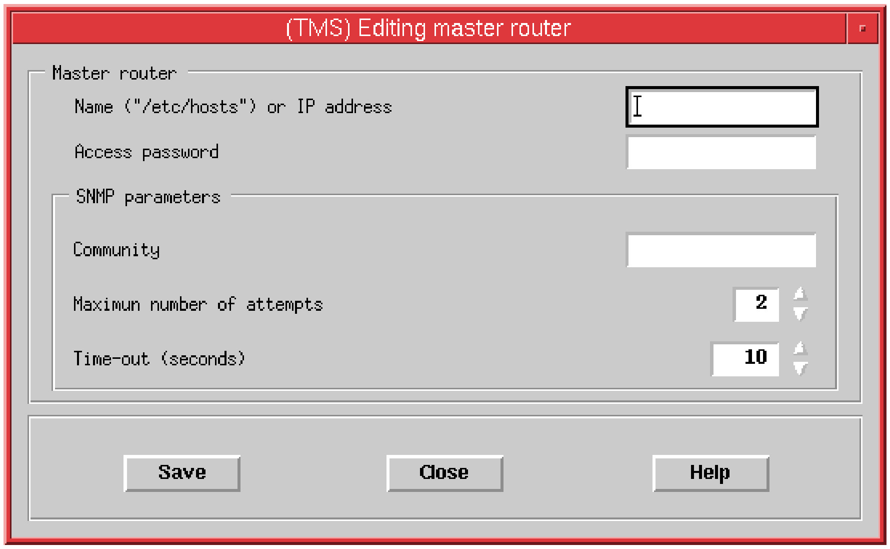
Launches the manager for the devices operations over groups.

2.3. List of master routers

This displays all the master routers contained in the database **master** table. Over this list, you can execute the following actions contained in the **Commands** menu located under the list. A device cannot be simultaneously managed by more than one master router.

In order to **add a master router** to the database you need to select **Commands->Add**. A **master router Edit** screen will then appear containing all the default values in the fields. When these have been adequately filled out, press the **Save** button which then saves the device in the database. If no errors have occurred, then a confirmation message will immediately appear below the main screen. The device will appear in the list on the subsequent screen refresh.

In order to **edit a master router** in the database, you need to select it from the list and execute **Commands->Edit**. This will also open the master router Edit screen with the current field contents. Once you have carried out the modifications required, press **Save** in order to reserve the changes.



(TMS) Editing master router

Master router

Name ("/etc/hosts") or IP address

Access password

SNMP parameters

Community

Maximun number of attempts 2

Time-out (seconds) 10

Figure 4 Master router edit screen

The configurable fields are as follows:

Master router name ("/etc/hosts") or IP address:
This is the master router's IP address. You can also introduce a name associated to an IP address through the station's **"/etc/hosts"** file. A maximum of 15 characters is permitted.

Access password:
This is the access password for the device through TELNET and FTP. The applications do not use this; simply, this is a way to have this accessible as a reminder to the operator. 31 characters are admitted distinct to blank spaces.

The following fields can be configured in the **SNMP Parameters:**

Access community:
This is the SNMP community through which the user tries to access the device. The device can only be accessed if the SNMP access community in his/her configuration coincides with that in the file. This admits up to 31 characters and does not permit blank spaces.

Maximum number of Attempts:
This is the maximum number of attempts carried out by an SNMP petition to the device in cases where the previous attempts have failed. The default value is three.

Response wait time (Time-out):
This is the period of time (in seconds) needed for the management station to respond to an SNMP request before terminating with a time-out message. The default value is 10 seconds.

If you wish to delete a master router from the database, simply select it in the list and choose the **Commands**->**Delete** option.

For each master contained in the list, the **tmssynchro** application makes a periodic petition from the devices table being managed by it.

> ***The greater the number of stations interacting with the same master router, the greater the response time will be to the said interactions.***

> *SNMP petition collisions*
>
> ***When this message appears associated to a master router this indicates that while the table of devices being managed was being requested from the master, a SET SNMP has been produced. This has provoked the insertion or deletion of an element in the table and consequently disordered the table received in the station.***
>
> ***In these cases, the content of the received table is ignored and is re-requested.***

2.4. List of devices in the BD

This displays all the devices contained in the **device** table in the database such as the assigned IP addresses. The fact that devices appear in this area does not mean that they are managing; it simply indicates that these devices exist in the database. If a device appears in red, this means that it is managed by its dynamic IP address and is unavailable at this given moment. A device displayed in red cannot be managed.

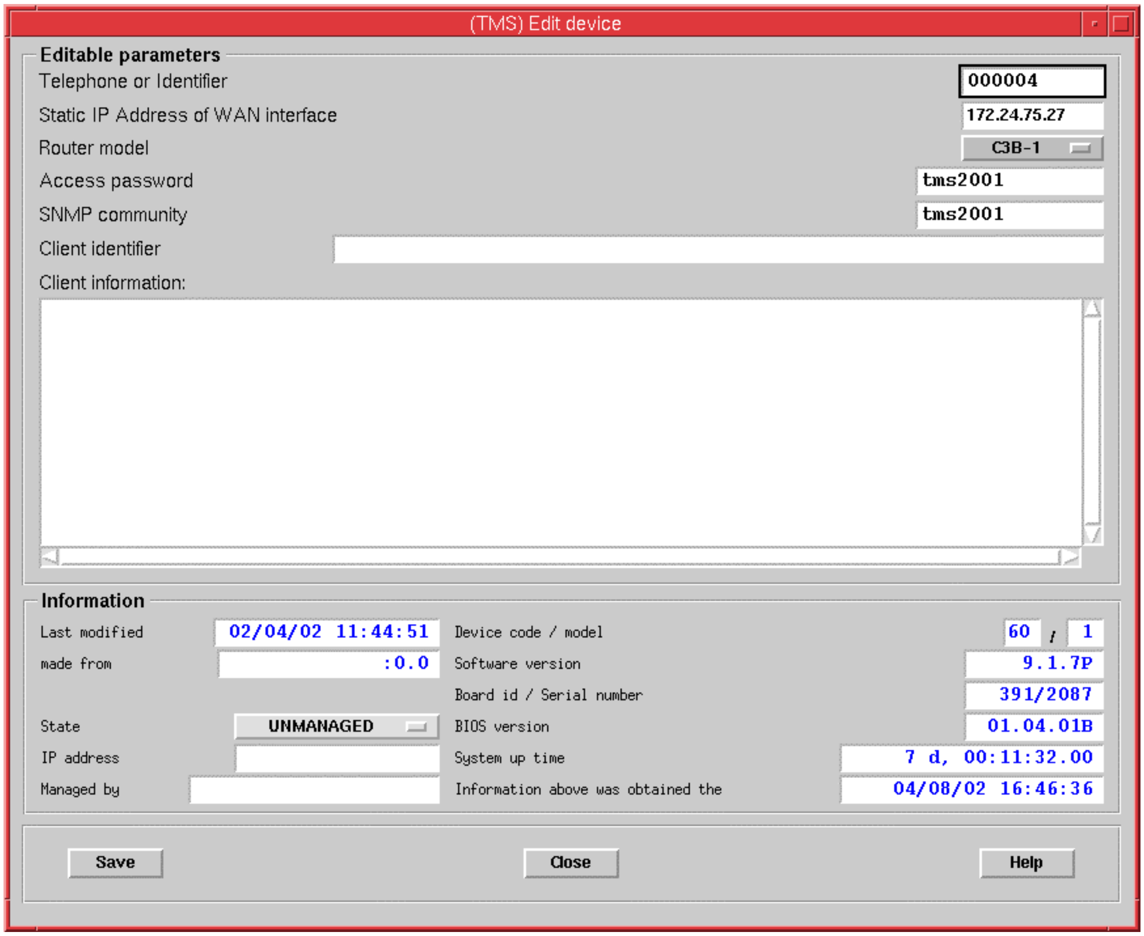
Over the upper right hand corner of the table, the table cardinal appears displaying the number of devices registered in the database.

The significance of the fields in the table is as follows:

Id	Device identifier. In cases of devices with dynamic IP, this is the serial number.
Add: IP	This is the static IP address (or dynamic should there be one) assigned to the device and is used to manage it.
Code	This is a number of two digits that identifies the type of device. For further information on device codes, please consult the section on Devices Codes and Models.
Modified	Indicates the moment when the table register was last modified.

This screen area also has a commands menu associated. Four actions can be carried out from here:

Command	Description
Edit	On selecting this command, the device edit screen appears. This screen is updated with the device content each time one is selected from the list.



Editable parameters

Telephone or Identifier	000004
Static IP Address of WAN interface	172.24.75.27
Router model	C3B-1
Access password	tms2001
SNMP community	tms2001
Client identifier	
Client information:	

Information

Last modified	02/04/02 11:44:51	Device code / model	60 / 1
made from	:0.0	Software version	9.1.7P
		Board id / Serial number	391/2087
State	UNMANAGED	BIOS version	01.04.01B
IP address		System up time	7 d, 00:11:32.00
Managed by		Information above was obtained the	04/08/02 16:46:36

Figure 5: Device edit screen.

In cases where on selecting **Edit** from the commands menu, you have a device selected, the parameters for the said device are edited. If on the other hand a device has not been selected, a new one is created and added to the database. The configurable fields in the register associated to a device in the database are:

In **Editable Parameters:**

Telephone or identifier:

This is the device identifier; in cases of ISDN routers this corresponds with its telephone number. For devices with dynamic IP addresses this corresponds to its serial number.

Static IP Address of WAN interface:

This is the IP address assigned to the devices having permanent or almost permanent connection. When this address exists, the operator can try and manage the device through this without using either a master device or the management call.

Router model:

Identifies the type of device being dealt with.

Access password:

This is the password requested by the device when accessing this through TELNET or FTP. Admits up to 31 letters and digits.

SNMP community:

This is the SNMP community through which the user tries to access the device. The device can only be accessed if the SNMP access community in his/her configuration coincides with that in the file. This admits up to 31 characters and does not permit blank spaces.

Client Identifier:

This is a string of up to 80 characters, which serve to carry out queries to the database for report grouping or groups of devices for clients.

Client information:

This is a field used for saving information on the client the device pertains to. The typical content of this field can be: contact person, telephone number, address, software version etc.

In **Information:**

Last modified:

Indicates the moment of the latest modification of the **infomanaged** table register where the information is taken from.

made from:

Indicates which station executed the updating of the said register.

State:

This represents the state of the device. This can be NOT MANAGED, REACHABLE or TESTING. In cases where this is REACHABLE, the device's IP address appears on the screen. This appears in the information block and cannot be modified.

IP address:

Represents the IP address in numeric format.

Managed by:

This is the identifier of the master router managing the device when its state is REACHABLE. This is located in the information block in the master device edit screen and cannot be modified by the user. If the device is REACHABLE and this field is empty, this is due to the fact it is being managed through the static IP address. This information is not displayed for the Teldat Cx routers.

Device code and model

These values have been read directly from the device. A case may arise where these do not coincide with the device code configured by the user (e.g. when the device has been physically exchanged for another one with a distinct code since the last information gathering) and in this case, the user must put this under management and request configuration in order to find out what type of device this is and to modify it in the database should this be necessary. This information is not displayed for the Teldat Cx routers.

Software version:

This is a string of characters identifying the device software version.

Board id/Serial number:

This indicates the serial number and the type of hardware motherboard in the device.

BIOS version:

This is the version of the start program that is in the device's EPROM memory.

System up time:

This field contains the MIB variable value known as "**sysuptime**" or time lapsed since the last restart. In the device and in the database this is stored in hundredths of seconds, however this is displayed to the user in days, hours, minutes and seconds.

Information above was obtained the:

Moment when the above information was read from the device.

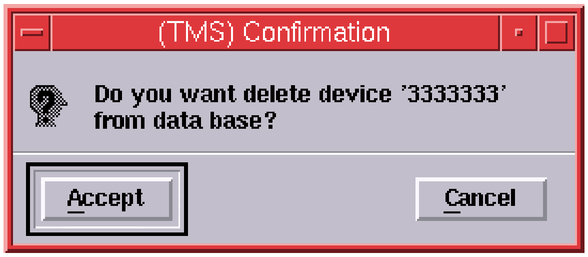
Management When you have selected a master router from the list, this command sends an order to the master to add the selected device to its list of the devices being managed. Where no master has been selected, the device is managed by its static IP address. In the status line on the screen, a message appears indicating whether the operation has been successful or not. The **tmssyncro** process updates the database and in the next reading that the application executes in the database, it refreshes the list of devices being managed with the new device.

When the master establishes contact with the device, its IP address appears indicating that it is accessible. If a device is being managed through its static IP address and does not respond, you will need to try and manage it through a master with conventional management methods.

If you try and manage a device that is already being managed, an error message appears.

If you try to manage a Cx device through a master router, an error message appears.

Delete This deletes the device from the database. Before continuing with the delete, the following conformation screen appears:


(TMS) Confirmation

Do you want delete device '3333333' from data base?

Figure 6: Delete device confirmation screen

If you press **Accept**, the device is deleted from the database. If you press **Cancel**, the operation is abandoned.

Search Beneath the database device list, you will see a text box that is used to search for a specific device through its identifier. Each time you modify the content of the text box, the program searches for the first device in the list whose identifier begins with the string entered in this box.

2.5. List of devices being managed

This area corresponds to the state of the devices that are being managed by the master selected in the master routers list, through its static IP address when no master has been selected or through its dynamic IP address if one has been assigned.

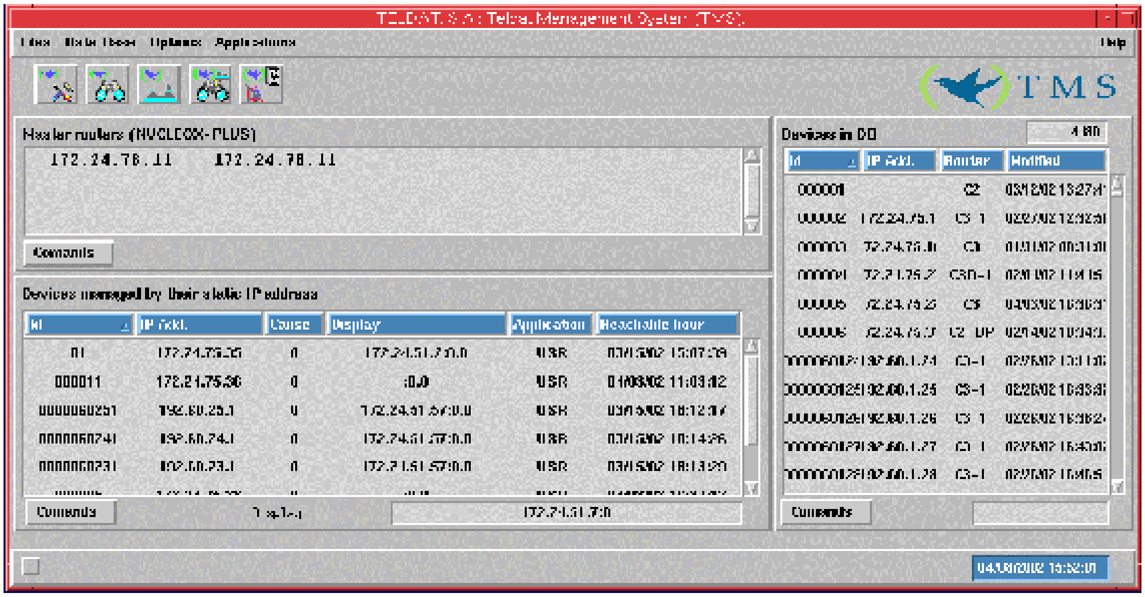
In order to view those devices being managed through their static or dynamic IP addresses, simply do not select any master router from the above list. You need to bear in mind that if a device with dynamic IP address disconnects; this after a while automatically stops managing.

The list header indicates the master router through which they are being managed. If no master router has been selected, the devices are displayed.

This list is refreshed with the results obtained from the periodic petition of the state from list of devices under management to the master executing the "**tmssynchro**" process and the database **infomanaged** table query.

In the same way as the other two areas, this has a commands menu associated. The only command that can be executed here is **De-manage**. What this command does is provoke the master router selected in the above list to delete the selected device from its list of devices being managed (this is not deleted from the database). Subsequently the master ceases to send its periodic "echo" and the managed device releases its ISDN call as soon as the **Release Time without data** timeout for the management calls lapses. From **version 5.0**, release time without data for the management calls is established at one minute. Prior to this version, the time used for the release time without data was the one configured in the corresponding ISDN channel device. If the device is being managed through its static IP address when it is de-managed, it is deleted from the "**informanaged**" table so another user can manage it.

The refresh period is only visible for those devices managed by the selected master router (or for those devices managed by their static IP address when no master has been selected) although this refresh is carried out for all the devices managed by all the master routers.



Master routers (NUCLEOX-PLUS)

172.24.78.11   172.24.78.11

Devices managed by their static IP address

Id	IP Add.	Cause	Display	Application	Reachable hour
01	172.24.75.25	0	172.24.51.7:0.0	USR	03/15/02 15:07:29
000011	172.24.75.30	0	:0.0	USR	01/08/02 11:03:12
0000060251	192.60.25.1	0	172.24.51.57:0.0	USR	03/15/02 18:12:17
0000060241	192.60.24.1	0	172.24.51.57:0.0	USR	03/15/02 18:14:26
0000060231	192.60.23.1	0	172.24.51.57:0.0	USR	03/15/02 18:13:20

172.24.51.7:0

Devices in DB   4 80

Id	IP Add.	Router	Modified
000001		C2	03/12/02 13:27:[illegible]
000002	172.24.75.1	C3-1	02/27/02 12:32:[illegible]
000003	172.24.75.11	C3	01/31/02 08:31:[illegible]
000004	172.24.75.2	C3D-1	02/11/02 11:34:15
000005	172.24.75.25	C3	04/03/02 16:36:[illegible]
000006	172.24.75.[illegible]	C2-DP	02/14/02 10:34:[illegible]
000006012[illegible]	192.60.1.24	C3-1	02/26/02 13:[illegible]
000006012[illegible]	192.60.1.25	C3-1	02/26/02 10:33:[illegible]
000006012[illegible]	192.60.1.26	C3-1	02/26/02 16:36:[illegible]
000006012[illegible]	192.60.1.27	C3-1	02/26/02 16:40:[illegible]
000006012[illegible]	192.60.1.28	C3-1	02/26/02 16:40:[illegible]

04/18/2002 15:52:07

Figure 7: Devices managed through their static IP address

Id:

Identifier of the device being managed.

IP Add.:

This is the IP address assigned to the device in its WAN interface. If this is being managed through a master router, it is dynamically assigned by the ISP. If it is being managed through its static IP address, this is the one assigned by contract through the service provider.

Cause:

This is the indication of the causes through which the latest call provided by the ISDN network complying with the ISO Q931 norms is released. This data has no meaning in the case of a Teldat Cx router.

> ***From version 1.4.1 in the master router, the ISDN release cause is only significant when the number of managed devices in TESTING state in the master router is less or equal to two.***

For further information on ISDN release causes, please consult ISDN release causes.

Display:

Here the IP address for the station that placed the device under management is displayed. This is the **DISPLAY** environment variable content that identifies the display from the station placing the device under management (see the reference to multidisplay management further on in the manual).

Application:

Indicates if the device has been placed under management by a manual management application (user). In this case the **USR** string will appear. If however it has been placed under management by an operation over groups, the string is **AUTO**.

Reachable Hour:

This is when the device obtained its IP address and thus established a management call. This enables the operator to be aware of the duration of the management call.

2.6. DB reader indicator and the last executed command

On the extreme lower left hand side of the screen, you will find a small box whose function is to monitor the periodic reading of the database and the updating of the screen. During the reading interval and updating this lights up in green. If the number of devices in the database is low, then it is possible that the change in color is almost imperceptible.

To the right of the indicator, a confirmation of the result of the most recent command executed is presented. There do exist some commands whose results are not immediately shown where you have to wait for a response from the device or until the next screen refresh. In these cases, a text will appear on the lower edge of the screen confirming that the action has been dealt with.

> ***ATTENTION***
>
> ***Call Release:***
>
> ***The fact that a device is being managed by a master router means that the latter is sending periodic "echo" commands to the former to maintain the link through the ISDN thus avoiding the situation where the device releases the call due to absence of traffic. Should the application be uncontrollably interrupted or is abandoned without de-managing the devices, these will maintain the ISDN management call active for a period of one hour (in master router versions prior to 1.3.0, the call is indefinitely maintained).***

> ***Maximum interval permitted for a device in TESTING state.***
>
> ***From master router version 1.3.0 onwards, the maximum interval a master permits a device to be in a TESTING state is 5 minutes (as opposed to 10 minutes for previous versions).***

> ***Deceleration in the change of state of the managed devices.***
>
> ***If there are inaccessible router masters in the database or ones that do not respond, this slows down the updating of the managed devices state depending on the number of attempts and time-out associated to the said masters. For this reason, we recommend that only those master routers that are being currently used should be in the database.***

3. Last Available Devices

Thanks to the dynamic IP address discovery capacity, all the devices that send their address to TMS when **ipdiscover** is in execution will be registered in the **last_devices** table. You can obtain a report by executing the **`$TELDATMS/script/showlastdevices.sh`** script. This script also cleans up the table, therefore it is convenient to periodically generate a report. With this report, you will know which devices have connected at some point since the last time you generated this report.

The appearance of the report is similar to the one shown below:

```
18/10/2001                                                       page    1
                                                TELDAT, S.A: Last available devices:

Serial number        Code Date
-------------------- ---- -------------------
068/1234                  10/10/2001 17:27:11
015/1234                  10/10/2001 17:27:48
024/1234                  10/10/2001 17:27:57
067/1234                  10/10/2001 17:28:22
033/1234                  10/10/2001 17:30:14
026/1234                  10/10/2001 17:31:04
049/1234                  10/10/2001 17:33:12
031/1234                  10/10/2001 17:33:13
038/1234                  10/10/2001 17:33:32
039/1234                  10/10/2001 17:34:15
069/1234                  10/10/2001 17:34:43
035/1234                  10/10/2001 17:34:54
065/1234                  10/10/2001 17:37:01
066/1234                  10/10/2001 17:37:26
017/1234                  10/10/2001 17:37:51
040/1234                  10/10/2001 17:37:55
032/1234                  10/10/2001 17:38:04
072/1234                  10/10/2001 17:39:01
025/1234                  10/10/2001 17:39:25
016/1234                  10/10/2001 17:39:26
070/1234                  10/10/2001 17:39:39
046/1234                  10/10/2001 17:40:03
028/1234                  10/10/2001 17:40:03
060/1234                  10/10/2001 17:40:24
022/1234                  10/10/2001 17:40:26
003/1234                  18/10/2001 13:03:16

26 rows selected.
```

4. Intervention Auditory

The date, time, duration and the station carrying out the call for all the management calls are saved in the database. This is saved in the **mancalls** table and reports can be generated with the **`$TELDATMS/etc/db/$TMSLANG/showmancalls.sql`** script.

The aspect of the report is similar to the one shown below:

```
17/01/2000                                                           página    1
         Informe de duracion de llamadas de gestion de equipos.

Equipo              Estacion        Accesible            t. accesible
------------------- --------------- -------------------- ------------
918060405           daisy:0         13/01/2000 16:08:00  00:01:24
918060405           daisy:0         13/01/2000 16:22:11  00:06:33
918060405           jpalacios:0     13/01/2000 16:32:36  00:07:40
911234567           jpalacios:0     13/01/2000 16:41:26  00:01:46
918060405           daisy:0         13/01/2000 16:42:01  00:01:23
918060405           burgos:0        13/01/2000 16:45:28  00:06:55
911234567           burgos:0        13/01/2000 16:45:40  00:02:51
918060405           daisy:0         17/01/2000 10:13:41  00:29:23
918060405           daisy:0         17/01/2000 12:57:28  00:01:50
918060405           daisy:0         17/01/2000 15:01:37  00:01:31
918060405           daisy:0         17/01/2000 16:54:44  00:08:00

11 filas seleccionadas.

17/01/2000                                                           página    1
   Duracion minima, media y máxima de las llamadas de gestion en cada equipo

Equipo              Intervenciones Minima (min.) Media (min.) Maxima (min.)
------------------- -------------- ------------- ------------ -------------
911234567                        2             1            2             2
918060405                        9             1            7            29

2 filas seleccionadas.

17/01/2000                                                           página    1
  Duracion minima media y maxima de las llamadas de gestion por cada estacion

Estacion        Intervenciones Minima (min.) Media (min.) Maxima (min.)
--------------- -------------- ------------- ------------ -------------
burgos:0                     2             2            4             6
jpalacios:0                  2             1            4             7
daisy:0                      7             1            7            29

3 filas seleccionadas.

17/01/2000                                                           página    1
 Numero de intervenciones y duracion minima, media y maxima para todo el parque

Mes                  Intervenciones Minima (min.) Media (min.) Maxima (min.)
-------------------- -------------- ------------- ------------ -------------
Enero                            11             1            6            29

1 fila seleccionada.
```

Chapter 4
Management of Devices

1. Configuration

Configuration of NOVACOM and Teldat C devices is carried out with the **tmsconfig** application. This can be launched from any of the other applications or from the command line with the following options:

```
>tmsconfig [-h] [-t <refresh time in seconds>] [-i <IP address> -c <SNMP community> -
id <device Id.>]
```

The refresh time indicates the period where the application reads the status of the devices from the database in order to select those that are accessible.

The rest of the parameters permit access to a device not found in the database with the condition that the refresh time is sufficiently high so the application does not refresh the screen showing the device status.

Option –h presents the use options.

The **edit configuration** screen is used to launch the communication commands with the relative device for configuration. From this screen you can carry out the following tasks over the accessible device selected from the principal screen:

* Request the configuration.
* Send the configuration.
* Save the device configuration in FLASH memory.
* Restart the device with the configuration from the FLASH memory.
* Send new software to the device.
* Synchronize the device time with the management station.
* Connect with the device through TELNET.

You can also carry out the following operations with files:

* Modify the read configuration.
* Read the file configuration.
* Save the configuration in a file.
* View the log file.

Operations with the database:

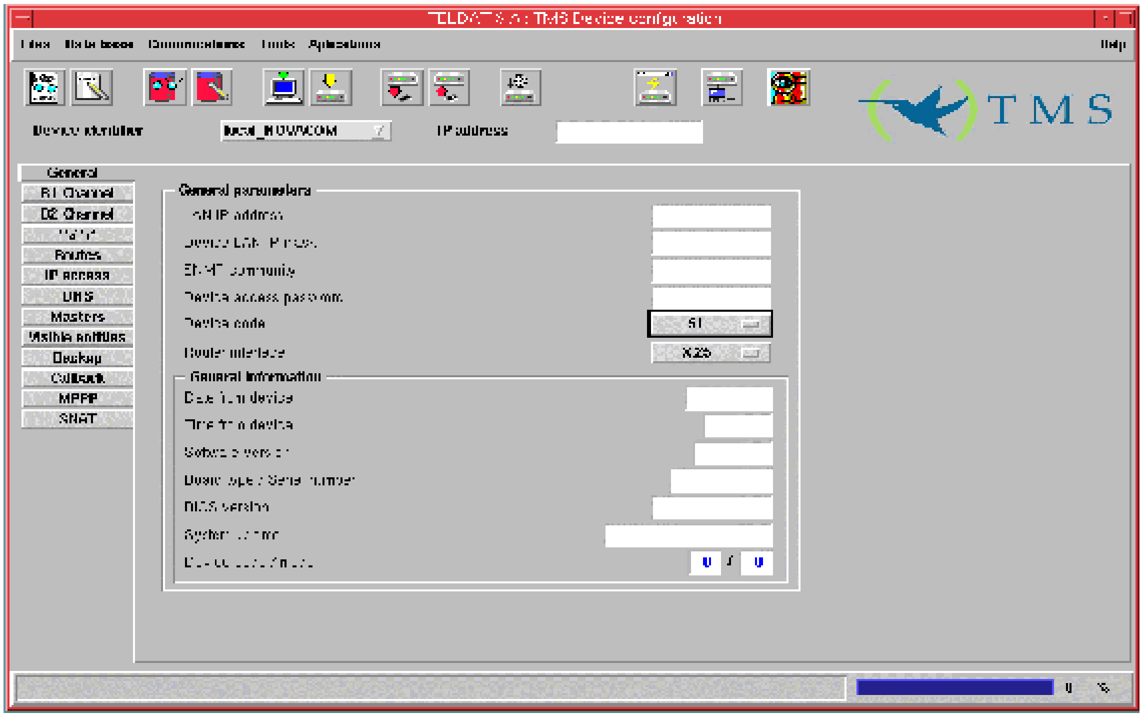
* Read a configuration from the database.
* Write a configuration in the database.

1.1. Configuration Parameters

Depending on the type of device, the configuration parameters used will be different. Below, you will find the devices explained separately.

a) General

• NOVACOM and NOVACOM-X25 Devices



Device identifier: local_NOVACOM
IP address:

General parameters
LAN IP address:
Device LAN IP mask:
SNMP community:
Device access password:
Device code: 51
Router interface: X25

General information
Date from device:
Time from device:
Software version:
Device type / Serial number:
BIOS version:
System uptime:
[illegible]: 0 / 0

Figure 8: General configuration

General parameters that may be modified:

- **LAN IP address:** This is the device LAN interface IP address.

- **Device LAN IP mask:** This is the device LAN interface IP mask.

- **SNMP community:** This is the SNMP community authorized to manage the device. The device can only be accessed if the SNMP access community in the device's configuration coincides with that in its file. This admits up to 31 characters and does not permit blank spaces.

- **Device access password:** This is the password for the device for connection through TELNET and FTP. If this is omitted, the access password is not requested when carrying out TELNET or FTP. No blanks are admitted and the maximum number of characters is 31.

- **Device Code:** Permits you to define what type of device the configuration displayed on the screen is for. Depending on the selection, access to certain entities are enabled or disabled. For normal cases, this code must coincide with that read by the SNMP from the device itself and this is displayed in the information part of the tab. If this does not coincide, the operator should investigate the cause. What could have happened is quite simply the remote devices have been changed, in which case you must update the file in the database. The application does not permit you to send a configuration to a device if the configured device code does not coincide with the one it actually has.

- **Router interface:** This permits you to define the type of interface used by the device, identifying if it uses X.25 or if it has a printer housed to its serial line (ASDP).

Information parameters that CANNOT be modified:

- **Date and time from device:** Indicates the device date and time at the moment the configuration was requested.

- **Software version:** This is a character string identifying the software version the device started up with and which the configuration was requested from.

- **Board type/ Serial number:** Indicates the serial number and the type of hardware motherboard of the device where the configuration was requested.

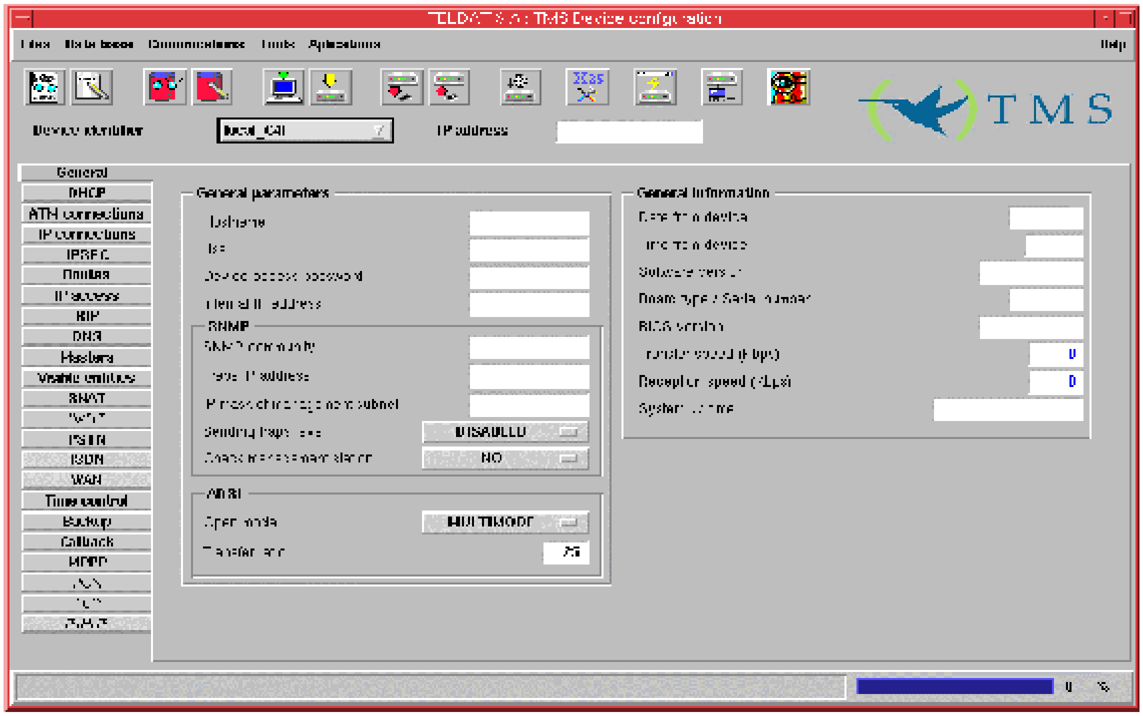
- **BIOS version:** This is the version of the start up program that is in the device's EPROM memory.

- **System up time:** This contains the MIB variable value known as "sysuptime" or time lapsed since the last restart. In the device and in the database this is stored in hundredths of seconds, however this is displayed to the user in days, hours, minutes and seconds.

These information parameters are saved in the **infodevice** table in the database each time the configuration is requested from the device.

When a configuration is read from the database, the device's date and time tabs change in order to express that the new dates and times are those possessed by the management station when the informative parameters were obtained. This date does not have to coincide with the date the configuration was requested.

• *Cx Devices*



Device identifier: local_C4I
IP address:

General parameters
Hostname:
User:
Device access password:
Internal IP address:

SNMP
SNMP community:
Traps IP address:
IP mask of management subnet:
Sending traps: DISABLED
Check management station: NO

ADSL
Oper mode: MULTIMODE
Transfer rate: 75

General information
Date in device:
Time in device:
Software version:
Board type / Serial number:
BIOS version:
Transfer speed (Kbps): 0
Reception speed (Kbps): 0
System uptime:

Figure 9: General configuration

Parameters that may be modified:

- **Hostname:** Name used to identify the router.

- **User:** User name with permisions to access the router.

- **Device access password:** This is the password for the device for connection through TELNET and FTP. If this is omitted, the access password is not requested when carrying out TELNET or FTP. No blanks are admitted and the maximum number of characters is 31.

- **Internal IP address:** IP address for internal use for the device.

- **SNMP community:** This is the SNMP community authorized to manage the device. The device can only be accessed if the SNMP access community in the device's configuration coincides with that in its file. This admits up to 31 characters and does not permit blank spaces.

- **Traps IP address:** IP address that the router will send the enabled SNMP traps. The port the device sends the traps to is 162.

- **IP mask of management subnet:** This deals with an IP mask that together with the previous IP address defines the subnet to which the device will respond to SNMP petitions. Value "0.0.0.0" (or empty) indicates that the router will respond to any IP address. Value

"255.255.255.255" indicates that only the traps destination station can carry out SNMP petitions.

- **Sending traps level:** There are four traps levels: NONE, LOW, MEDIUM AND HIGH. With the exception of NONE where no traps are sent, all the rest send all the generic traps as well as the "enterprise" traps that are enabled. The trap level determines which "enterprise" traps are going to be sent:

  * LOW: Traps defined as ERROR.
  * MEDIUM: The previous traps as well as unexpected events information traps.
  * HIGH: Traps defined as error or as information.

- **Check management station:** Indicates if the device should check that its manager station can be reached through the network.

- **Open mode:** Transmission mode in ADSL.

- **Transfer ratio:** Relation between traffic received and sent.

- **Transfer speed [Kbps]:** Transmission speed for the ADSL interface in Kbps.

- **Reception speed [Kbps]:** Reception speed for the ADSL interface in Kbps.

Information parameters that CANNOT be modified:

- **Date and time from device:** Indicates the device date and time at the moment the configuration was requested.

- **Software version:** This is a character string identifying the software version the device started up with.

- **Board type / Serial number:** Indicates the serial number and the type of hardware motherboard of the C2 router.

- **BIOS version:** This is the version of the start up program that is in the device's EPROM memory.

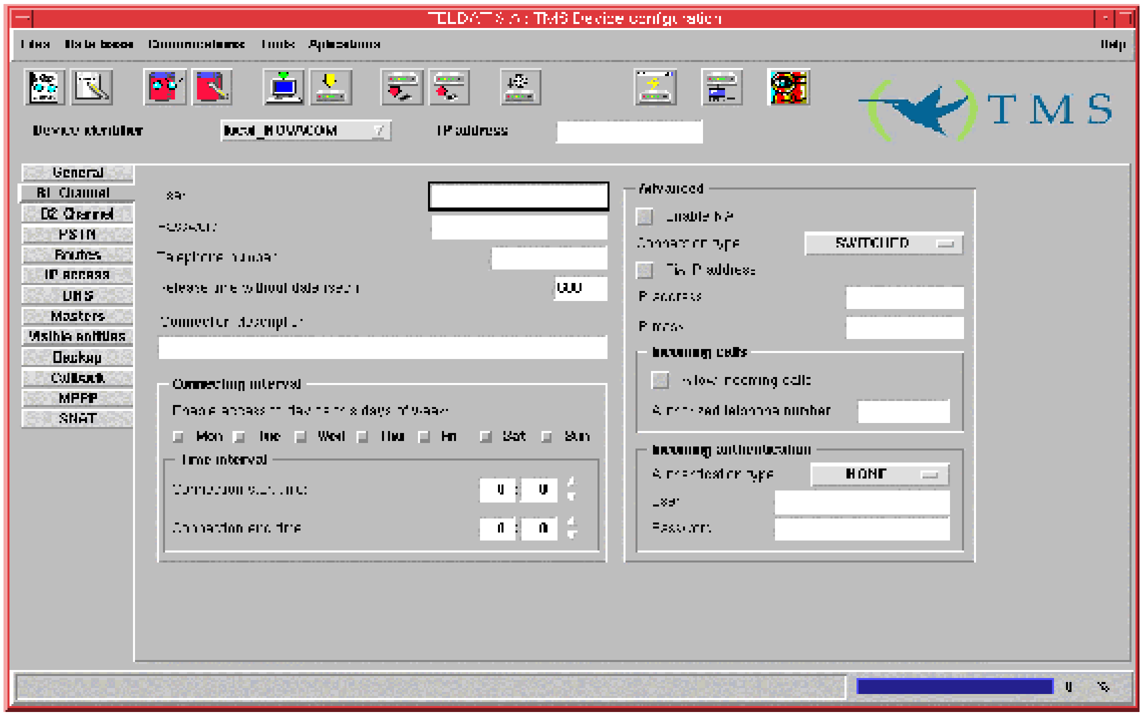
- **System up time:** This contains the MIB variable value known as "sysuptime" or time lapsed since the last restart. In the device and in the database (**inforouters** table) this is stored in hundredths of seconds, however this is displayed to the user in days, hours, minutes and seconds. You must take into account that at the said time, you must add the interval from the time value was requested from the router up till the current moment.

Each time you request the configuration from the router or read its fortnightly statistics with the statistics automatic gathering application, you also request the informative parameters and these are saved in the **inforouters** table.

When a configuration is read from the database, the device's date and time tabs change in order to express that the new dates and times are those possessed by the management station when the informative parameters were obtained. This date does not have to coincide with the date the configuration was requested.

b) B1 Channel (NOVACOM and NOVACOM-X25 devices only)

There is a configuration screen for each of the two ISDN B channels available in the device and another one for the PSTN channel (with the same aspect). In each of these, the destination and the connection properties are configured that the device will establish for each channel



Device identifier: local_NOVACOM
IP address:
User:
Password:
Telephone number:
Release time without data reception: 000
Connection description:
Connecting interval
Enable access on the following days of week:
□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time interval
Connection start time: 0 : 0
Connection end time: 0 : 0
Advanced
□ Enable NAT
Connection type: SWITCHED
□ Fix IP address
IP address:
IP mask:
Incoming calls
□ Allow incoming calls
Authorized telephone number:
Incoming authentication
Authentication type: NONE
User:
Password:

Figure 10: Configuring ISDN B1 Channel

- **User:** User, through which the service is accessed. This is provided by the supplier and has a connection IP address and certain privileges associated. Up to 31 characters are admitted.

- **Password:** Access password associated to the above user (provided by the service supplier). A maximum of 31 characters are permitted.

- **Telephone number:** This is the telephone number the device demands connection through. In order to minimize the cost of the calls, use the telephone number of the Access Node nearest to the device. A maximum of 19 digits is admitted.

- **Release time without data (sec):** The connections normally terminate due to absence of data on the line in a time equal or superior to the release time without data. The default value is 600 seconds. We do not recommend that you use a very low time period. The timer precision is T/10 where T is the release time without data. Values within the range [0, 60 .. 65535] are admitted, 600 seconds being the default value. The value 0 is a special case and is equivalent to a permanent connection. This value is used for example as a means of uniting subnets. If a timetable control has been established and the release time without data is 0, then the device establishes a connection as soon as the access period commences. In this way and during this period, the client can communicate his subnets. If there are no timetable restrictions and a 0 value is assigned, the device establishes a permanent connection after start up.

- **Connection description:** This is a string of up to any 79 characters of information on the connection type that will be established through the channel

- **Connecting interval:** This serves to restrict traffic though the device to a temporary interval certain days of the week or to force the device connection in the said interval. The connection interval specifies the period where the device is operative. Outside of this interval the interface is blocked except for management connections, which are always guaranteed.

    - Selects the days of the week where the device operates normally.

    - Introduce the start and the end of the interval in an **hh:mm** format. For the hour, admitted values within the interval are [0 to 23] and for the minutes [0 to 59]. If the end time is inferior to the start then this is considered as pertaining to the next day. If connection is not permitted the following day, the day takes priority over the time and the connection is disabled for that day.

    - When the release time without data is 0, the device automatically connects when the temporary interval established in the timetable configuration begins.

Advanced:

- **Enable NAT:** By default, the device executes extended **Network Address Translation** (NAT) in the defined connections. In this way only one IP address is used to connect an indefinite number of local workstations to external networks such as INTERNET. Should you not require this operation and wish the LAN stations the device is connected to communicate with the exterior as they are, you can disable NAT. For further information on NAT please consult {Teldat: NAT, 99}.

- **Connection type:** This indicates the type of connection established in the channel. If the user has a permanent ISDN B channel contracted from the supplier, this should be indicated through this parameter. A permanent B channel is a special ISDN B channel that does not use signaling as its destination is set in the service contract. This B channel does not carry out ISDN calls and is always connected. If you enable a B channel as **PERMANENT**, the connection destination telephone parameters, release time due to absence of data and the permitted connection interval are hidden. The permanent B channel contract specifies which B channel (B1, B2 or both) responds to this profile. Both channels cannot have permanent connection, as the device in this case cannot be managed. The default value is **SWITCHED**.

- **Fix IP address:** In a normal access scenario to an external network such as INTERNET, the device connects through a terminal server. This terminal server assigns an IP address to the device each time it connectsThe policy of assigning IP addresses according to caller user usually corresponds to the access server for the external network and in general does not guarantee that consecutive calls from the same user will receive the same IP address. However it is possible to work in environments where the WAN addressing is fixed and known a priori, for example, in order to interconnect two remote networks through two devices. Here the WAN connection addressing is defined through the IP address and mask parameters. The device by default, requests IP assignment from the remote end. If this option is enabled, two fields appear below where you can indicate the IP address and mask associated to the connection for this channel. If these two fields are left empty, this is equivalent to disabling the option.

- **IP address:** If the previous option has been enabled, this establishes the connection IP address through the channel.

- **IP mask:** This is the IP mask applied to the previous address.

Incoming calls:

- **Allow incoming calls:** As an access device, it is the device itself that carries out the call to the external network supplier to which you wish to connect. However in connection scenarios between two devices, one makes the call while the other receives it. If you wish the device to be able to receive incoming calls, you have to enable this parameter. By default, the device does not permit incoming calls.

- **Authorized telephone number:** If the incoming calls are enabled, this parameter indicates the ISDN number authorized for connection. If there is no value configured here then any caller is authorized to connect although it must be authenticated through PAP or CHAP if this is indicated. The default value (empty) for this parameter is to authorize any calling number.

Incoming authentication:

- **Authentication type:** Normally on accessing an external network, it is the external network itself that requests the access device to authenticate prior to being able to use the network. However, in point-to-point scenarios, where it is not an external network being accessed but a known remote network through an also known remote device, it is possible to indicate to the remote end that it needs to authenticate itself. The device supports the PPP authentication protocols: **Password Authentication Protocol (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**.

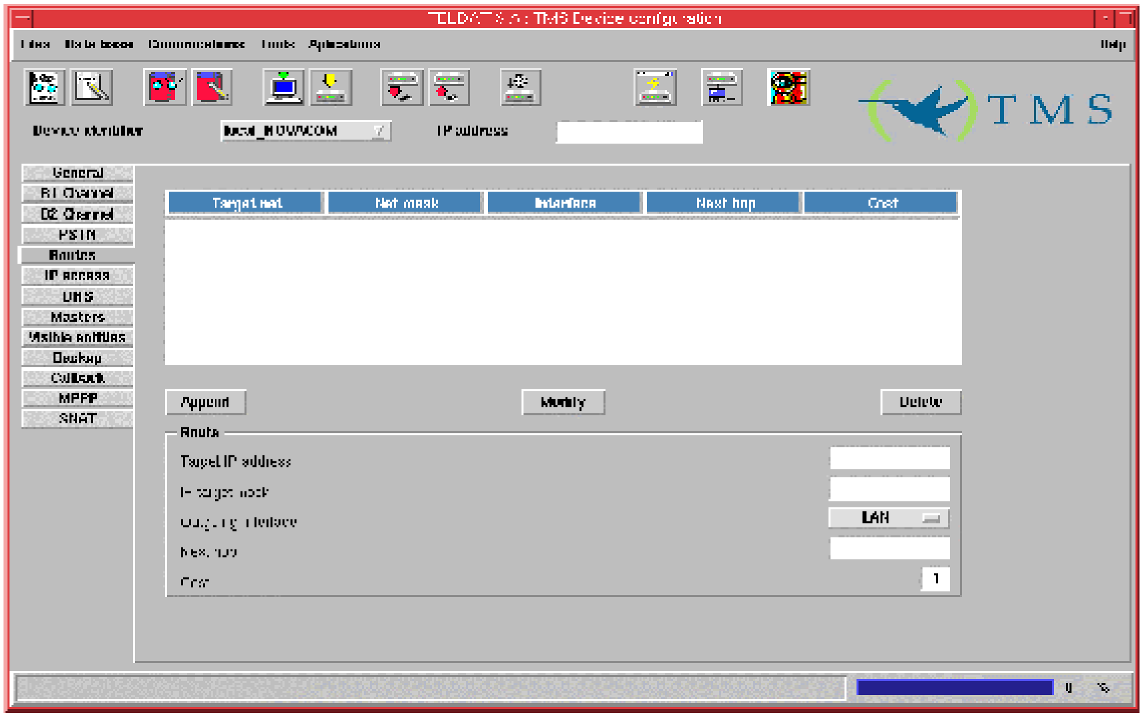
- **User:** If you demand authentication from the remote end, this parameter indicates the remote user login permitted for this connection. The device validates the remote login received via PAP or CHAP with the login configured in this parameter. This is a string of up to 31 characters.

- **Password:** If you demand authentication from the remote end, this parameter indicates the remote user password permitted for this connection. The device validates the remote password received via PAP or CHAP with the password configured in this parameter. Up to 31 characters are admitted.

c) IP routes

• NOVACOM and NOVACOM-X25 devices

This screen is used to indicate to the device where it has to route the packets to in order to reach their destination.



Device identifier: local_NOVACOM
IP address:

Target IP address:
IP target mask:
Outgoing interface: LAN
Next hop:
Cost: 1

Figure 11: Configuring IP routes

- **Target IP address:** This is the IP address of the station or subnet where the traffic is directed. Address 0.0.0.0 together with mask 0.0.0.0. indicates that this is the device’s default route.

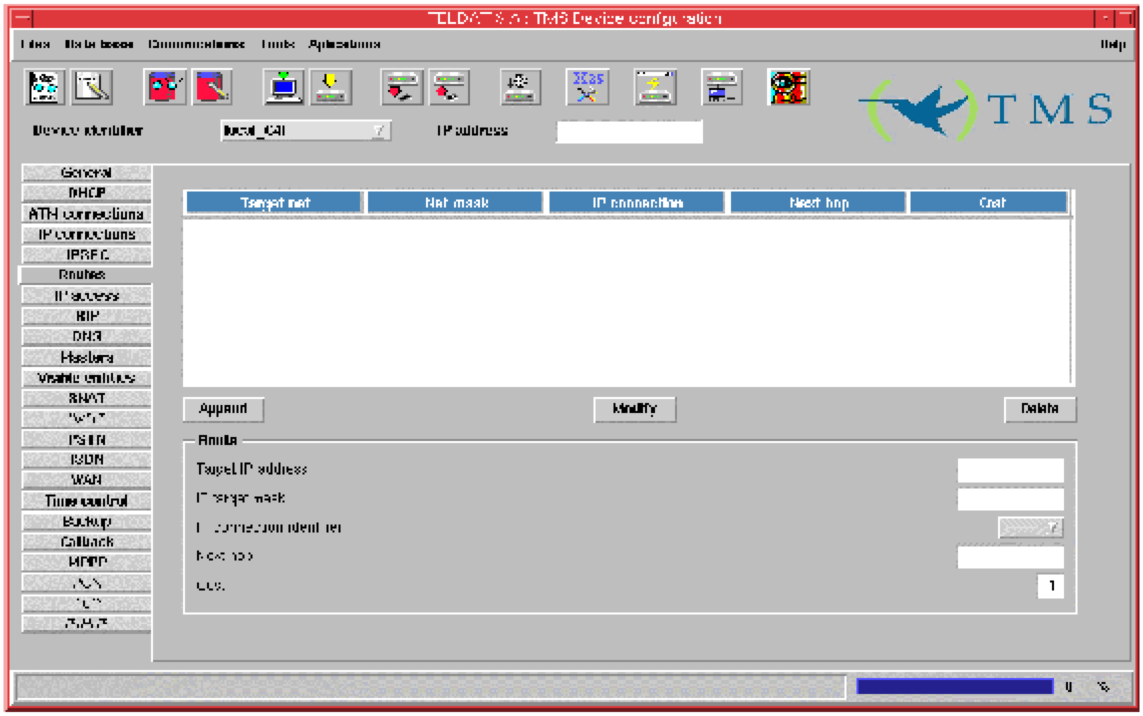
- **IP target mask:** This is the IP mask for the destination subnet.

- **Outgoing interface:** Interface associated to the route.

- **Next hop:** This is the IP address of the next device in charge of routing the packet. This is only significant when the previously selected interface is LAN, if not this field is hidden.

- **Cost:** This is the cost associated to the route. Values within the range [0 to 16] are permitted.

- ***Cx Devices***



Device identifier: local_C4I
IP address:

Target net	Net mask	IP connection	Next hop	Cost

Target IP address:
IP target mask:
IP connection identifier:
Next hop:
Cost: 1

Figure 12: Configuring IP routes

Target IP address: This is the IP address of the station or subnet where the traffic is directed. Address 0.0.0.0 together with mask 0.0.0.0. indicates that this is the device's default route.

IP target mask: This is the IP mask for the destination subnet.

IP connection identifier: Reference to the IP address through which the route packets are sent. If this value is 0, this indicates the packets are sent trough the LAN interface.

Next hop: This is the IP address of the next device in charge of routing the packet. This is only significant when the previously selected interface is LAN, if not this field is hidden.

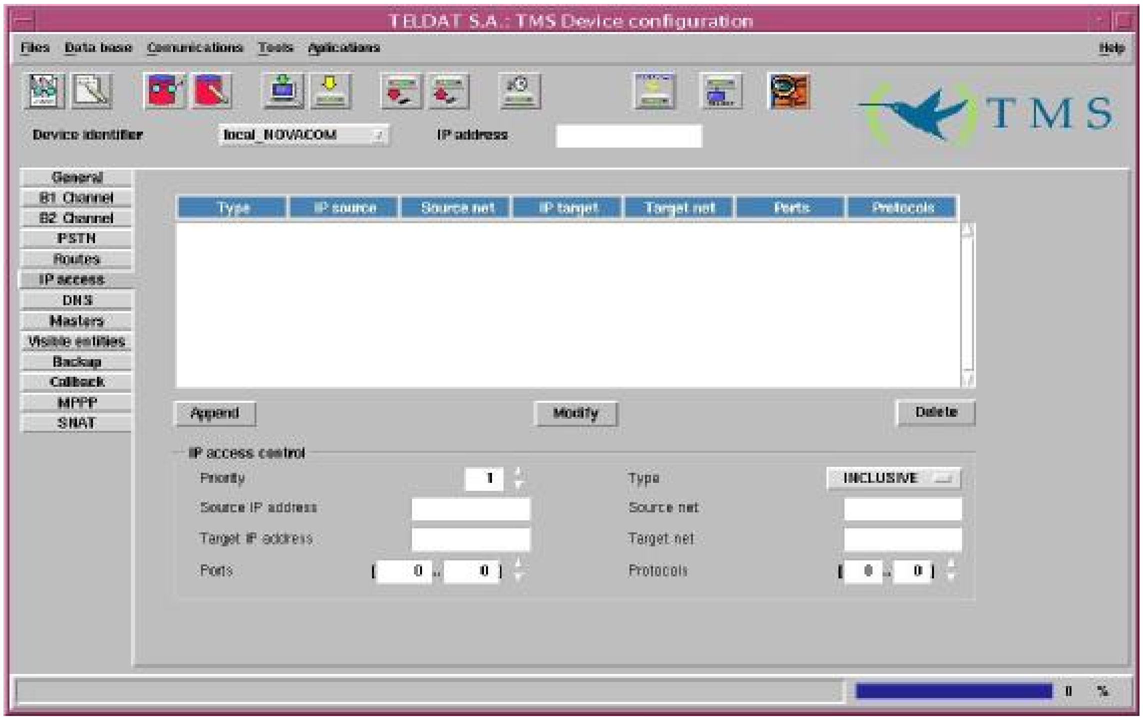
Cost: This is the cost associated to the route. Values within the range [0 to 16] are permitted.

> ***A maximum of 200 routes is admitted.***

d) *IP access*

- ***NOVACOM and NOVACOM-X25 devices***

Each time an IP address is received, the device chronologically checks the access controls list. Each of these is made up of the following fields: Type, IP Source, Source net, IP target, Target net, Ports, Protocols.



Device identifier: local_NOVACOM
IP address:

Priority: 1
Type: INCLUSIVE
Source IP address:
Source net:
Target IP address:
Target net:
Ports: [0 .. 0]
Protocols: [0 .. 0]

0 %

Figure 13: Configuring IP access controls

- **Type: INCLUSIVE** implies accepting the packet and **EXCLUSIVE** rejects the packet if this matches the profile.

- **IP source:** IP address of the source station or subnet.

- **Source net:** Source subnet IP Mask. This has to be consistent with the previous address. For this reason, the binary AND operation between the address the binary negation of the mask must result in 0. The combination of the address and mask 0.0.0.0 implies “any source”.

- **IP target:** This is the IP address of the packet’s destination station or subnet.

- **Target net:** Destination subnet IP mask. This has to be consistent with the previous address. For this reason, the binary AND operation between the address the binary negation of the mask must result in 0. The combination of the address and mask 0.0.0.0 implies “any destination”.

- **Ports :** Range of ports that the packet can be destined for. Values admitted in the range are [0 .. 65535].

- **Protocols:** Range of protocols that the packet can be associated to. Values admitted in the range are [0 .. 255].

The algorithm is as follows:

1. The binary AND is carried out between the **source IP** address and the **source Network**. Then a check is carried out to make sure that this coincides with the result of the same operation between the IP address of the packet received by the device and the **source Network**.
2. The same check as above is repeated but this time with the **target IP** address and the **target Network**.
3. A check is also carried out to see if the **Protocol** the packet is directed to, is within the range of access control protocols.
4. A check is also made to see if the **Port** the packet is directed to, is within the range of access control ports.
5. If all the above points are satisfactorily fulfilled, then the operation indicated for Type is executed. The possible actions here are ***accept packet*** in cases where the Type is **INCLUSIVE** or ***reject packet*** where the Type is **EXCLUSIVE**.
6. If one of the above conditions is not fulfilled, then you return to point 1 and execute the same operations with the next one registered in the access controls list.
7. If there are no further access controls, then the packet is accepted.
8. The order the access controls are found in is very important as this determines the priority.

In order to ***add*** a new access control, you need to fill out all the fields below the list and press the **Append** button.

In order to ***modify*** an element in the list, select it, modify the corresponding fields and press **Modify**.

In order to ***delete*** an access control, select it and press **Delete**.

In cases of **Protocols** and **Ports**, a range of operational values is established. E.g. if you wish to only accept SNMP packets, select as the Protocol Range [11..11], as 11 corresponds to the UDP protocol; and for the Ports Range [161..162], as these are used by SNMP.

The TMS management uses the following ports for its communications with the device:

Protocol	**Port**
FTP	21
TELNET	23
Private echo master - device	2006
SNMP	161

Warning!

If you introduce a totally exclusive access control and the device analyses it because the previous ones have failed, then the device will infallibly discard the packet. In this case it is essential to guarantee that at least a master router and a management station verify one of the inclusive higher priority access controls. If this condition is not respected then the device will be inaccessible for management

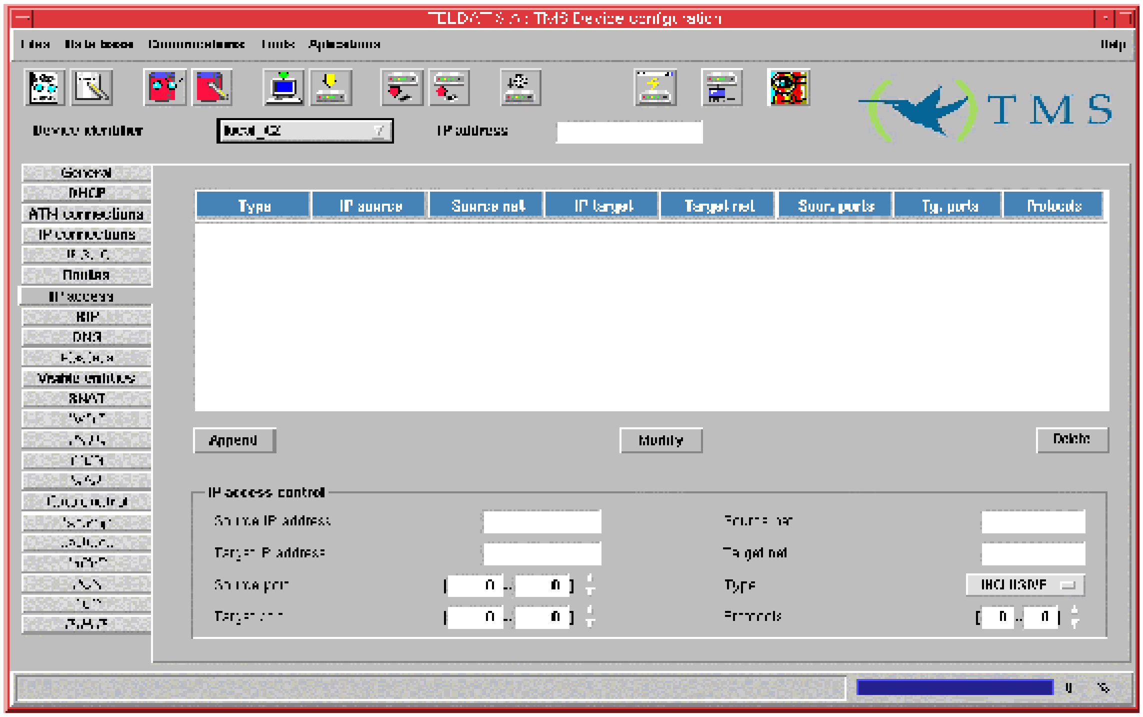
Guaranteeing the bi-directional communication with any device through an inclusive control requires two access control registers: one as source and the other as destination.

NOTE:

In the access controls, address 0.0.0.0 together with mask 0.0.0.0 is equivalent to "any IP address".

In order to know the port numbers and the protocols assigned in INTERNET, you can consult the RFC 1700 "INTERNET ASSIGNED NUMBERS" as help to define the IP access controls in the device. This information is available at the following Internet address: ftp://ds.internic.net

- ***Cx Devices***



Source port [0 .. 0]

Target port [0 .. 0]

Type INCLUSIVE

Protocols [0 .. 0]

Figure 14: Configuring IP access controls

Each time an IP address is received, the router chronologically checks the access controls list. Each of these is made up of the following fields:

- **Type: INCLUSIVE** implies accepting the packet and **EXCLUSIVE** rejects the packet if this matches the profile.

- **IP source:** IP address of the source station or subnet.

- **Source net:** Source subnet IP Mask. This has to be consistent with the previous address. For this reason, the binary AND operation between the address the binary negation of the mask must result in 0. The combination of the address and mask 0.0.0.0 implies "any source".

- **IP target:** This is the IP address of the packet's destination station or subnet.

- **Target net:** Destination subnet IP mask. This has to be consistent with the previous address. For this reason, the binary AND operation between the address the binary negation of the mask must result in 0. The combination of the address and mask 0.0.0.0 implies "any destination".

- **Sour. ports:** Range of ports that the packet can come from. Values admitted in the range are [0 .. 65535].

- **Tg. ports:** Range of ports that the packet can be destined for. Values admitted in the range are [0 .. 65535].

- **Protocols:** Range of protocols that the packet can be associated to. Values admitted in the range are [0 .. 255].

The algorithm is as follows:

- The binary AND is carried out between the **source IP** address and the **source Network**. Then a check is carried out to make sure that this coincides with the result of the same operation between the IP address of the packet received by the device and the **source Network**.
- The same check as above is repeated but this time with the **target IP** address and the **target Network**.
- A check is also carried out to see if the **Protocol** the packet is directed to, is within the range of access control protocols.
- A check is also made to see if the **Port** the packet is directed to, is within the range of access control ports.
- If all the above points are satisfactorily fulfilled, then the operation indicated for Type is executed. The possible actions here are ***accept packet*** in cases where the Type is **INCLUSIVE** or ***reject packet*** where the Type is **EXCLUSIVE**
- If one of the above conditions is not fulfilled, then you return to point 1 and execute the same operations with the next one registered in the access controls list.
- If there are no further access controls, then the packet is accepted.

The order the access controls are found in is very important as this determines the priority.

In order to ***add*** a new access control, you need to fill out all the fields below the list and press the **Append** button.

In order to ***modify*** an element in the list, select it, modify the corresponding fields and press **Modify**.

In order to ***delete*** an access control, select it and press **Delete**.

In cases of **Protocols** and **Ports**, a range of operational values is established. E.g. if you wish to only accept SNMP packets, select as the Protocol Range [11..11], as 11 corresponds to the UDP protocol; and for the Ports Range [161..162], as these are used by SNMP.

The following ports are used for management:

Service	Port
FTP	21
TELNET	23
Web Server	80
SNMP	161

A maximum of 40 IP access controls are admitted.

Warning!

If you introduce a totally exclusive access control and the device analyses it because the previous ones have failed, then the device will infallibly discard the packet. In this case it is essential to guarantee that at least a master router and a management station verify one of the inclusive higher priority access controls. If this condition is not respected then the device will be inaccessible for management. (Guaranteeing the bi-directional communication with any device through an inclusive control requires two access control registers: one as source and the other as destination).

In the access controls, address 0.0.0.0 together with mask 0.0.0.0 is equivalent to "any IP address".

In order to know the port numbers and the protocols assigned in INTERNET, you can consult the RFC 1700 "INTERNET ASSIGNED NUMBERS" as help to define the IP access controls in the device.

e) Visible entities

• NOVACOM and NOVACOM-X25 devices

The device may be connected to a LAN with subnets that require being accessed from the exterior. Under normal conditions, given that the device carries out NAT, the LAN stations cannot be accessed from the exterior

So a subnet can be visible from the outside you need to add it to the list of visible subnets. The device behaves in the following way with the subnets from this list:

1. It is possible to configure a visible subnet for each ISDN B channel and another one for the PSTN interface. The number of visible stations can be very high depending on the subnet mask.

2. A subnet that is visible in a network is visible to all effects and for all types of IP traffic i.e. the device does not carry out extended NAT over the packets whose source or destination is included in the subnet.

3. The subnets visible in an external network are not visible in the other possible external networks that the device connects to through other channels where the device continues to carry out extended NAT.

4. The stations in a visible subnet can communicate with the normal stations in the LAN or with the stations of another subnet visible in the same LAN through the device itself. These do not generate either calls or traffic to the external networks.

So that the visible stations can respond to external petitions, it is necessary that a route to the external network be configured in all of them through the IP address of the so-called **virtual router**. This is due to the fact that the stations will have IP addresses pertaining to a distinct network than the one connected to the device's LAN interface. As the device only has one LAN interface, another "virtual" one is needed in order to connect to the servers.

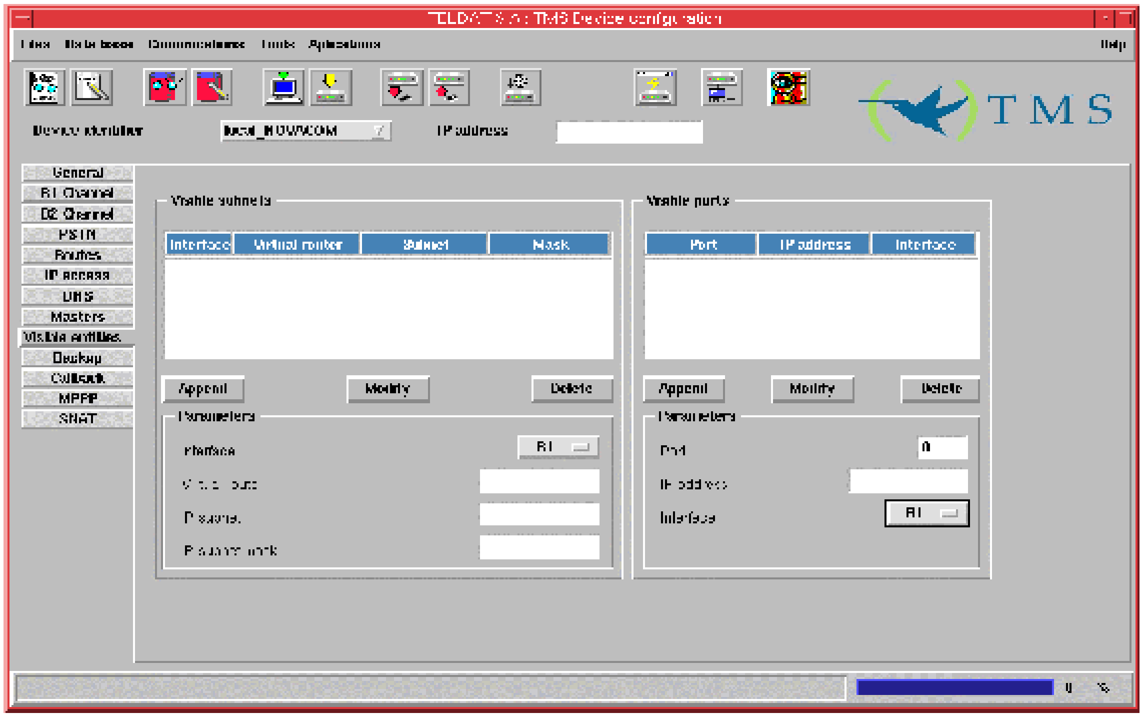


Figure 15: Configuring visible entities

- **Interface:** This is the interface through which the subnet is visible.

- **Virtual router:** This is the IP address through which the visible subnet traffic is routed to the outside. This must pertain to the same visible subnet.

- **IP subnet:** This is the subnet IP address over which the router does not carry out NAT.

- **IP subnet mask:** Visible subnet IP mask.

In order to ***add*** a subnet to the list, introduce the appropriate values in the fields below the list and press the **Append** button.

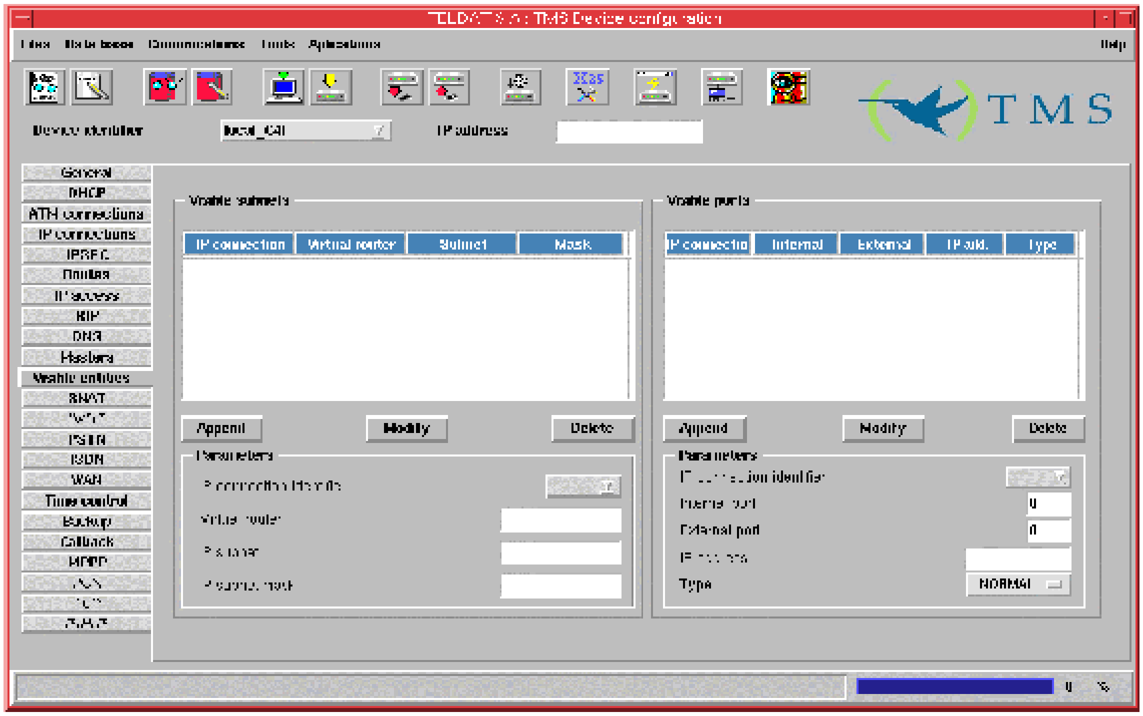
In order to ***modify*** a subnet in the list, select it and once modified through the corresponding fields, press the **Modify** button.

In order to ***delete*** a visible subnet from the list, select it and press **Delete**.

• *Cx devices*

As the Cx routers carry out extended address translation, the internal devices always access a unique registered address that the router conveniently transforms when the IP packet enters the LAN.

In order to permit certain LAN subnets to be visible to the outside with their own IP addresses (registered) you need to disable the address translation in the router for the said subnets. In this screen, the user specifies those subnets where the router does not carry out NAT and therefore are accessible from the exterior.



Device identifier local_C41

IP address

Internal port 0

External port 0

Type NORMAL

Figure 16: Configuring visible entities

The following parameters are configured for each visible subnet:

- **IP connection identifier:** This is the IP connection identifier through which the subnet is visible.

- **Virtual router:** IP address assigned to the router so that the device itself knows that it must not carry out NAT over the packets it receives. This must pertain to the same visible subnet.

- **IP subnet:** This is the subnet IP address over which the router does not carry out NAT.

- **IP subnet mask:** Visible subnet IP mask.

The router behaves in the following way with the subnets from this list:

1. It is possible to configure a visible subnet for each IP connection. The number of visible stations can be very high depending on the subnet mask.

2. A subnet that is visible in a network is visible to all effects and for all types of IP traffic i.e. the device does not carry out extended NAT over the packets whose source or destination is included in the subnet.

3. The subnets visible in an external network are not visible in the other possible external networks that the device connects to through other channels where the device continues to carry out extended NAT.

4. The stations in a visible subnet can communicate with the normal stations in the LAN or with the stations of another subnet visible in the same LAN through the device itself. These do not generate either calls or traffic to the external networks.

So that the visible stations can respond to external petitions, it is necessary that a route to the external network be configured in all of them through the IP address of the so-called **virtual router**. This is due to the fact that the stations will have IP addresses pertaining to a distinct network than the one connected to the router's LAN interface. As the router only has one LAN interface, another "virtual" one is needed in order to connect to the servers

In order to ***add*** a subnet to the list, introduce the appropriate values in the fields and press the **Append** button.

In order to ***modify*** a subnet in the list, select it and once modified through the corresponding fields, press the **Modify** button.

In order to ***delete*** a visible subnet from the list, select it and press **Delete**.

Up to 10 visible subnets are admited.

Visible entities and IP access controls:

The IP access controls have preference over the visible entities. This means that an exclusive access control can make ports or visible subnets inaccessible.

f) Configuring visible ports in the LAN

In the same screen as the visible entities, you can configure the ports (normally associated to protocols), which are visible from the outside. The idea is similar to the visible stations but the difference in this case is that it is more restrictive (only certain ports) and that the IP addresses associate to the ports can be private: In this way registered IP addresses are not squandered.

Up to a maximum of 5 ports are admitted. The ports cannot be repeated. Should this occur, the device would route all the traffic to the first one on the list.

Certain ports are prohibited in this screen. These are the ports the device needs for its own traffic.

Prohibited ports:

Port #	Protocol
21	FTP

23	TELNET
53	DNS
80	Web Server
161	SNMP

Also reserved for the NAT ports are those ports within the range **[32768 .. 33791]**.

The configurable fields are as follows:

- **IP connection identifier:** IP connection through which the port is visible.

- **Internal port:** Number of the port you wish to make visible.

- **External port:** Port through which the internal port is accessible from the outside.

- **IP address:** This is the local station IP address to which the port pertains to and will be visible to the outside from the LAN. There must be a LAN IP address that the router pertains to.

- **Type:** This is the port type, **NORMAL** or **FTP**. If it is **FTP**, the router carries out NAT over the addresses contained in the packets. If it is **NORMAL**, the router only carries out NAT over the packet header addresses.

> ***Up to 5 visible ports are admitted.***

To add a new port to the list, fill out the fields and press **Append**.

In order to modify a port in the list, select it, modify the corresponding fields and press **Modify**.

In the case of the **Delete** option, the selected element is deleted.

> ***Visible entities and IP access controls:***
>
> ***The IP access controls have preference over the visible entities. I.e. with exclusive access control you can make ports or visible subnets inaccessible.***

g) Configuring DNS servers

The device permits you to handle a list of up to 3 **DNS (Domain Name Server)** servers who translate names to IP addresses.

The idea is to centralize the DNS management in the device in such a way that the LAN stations have a predetermined DNS server to the IP address of the device itself in the LAN and that this is in charge of routing the DNS traffic to the true servers. The order of the servers in the list indicates the priority used by the device to send petitions.

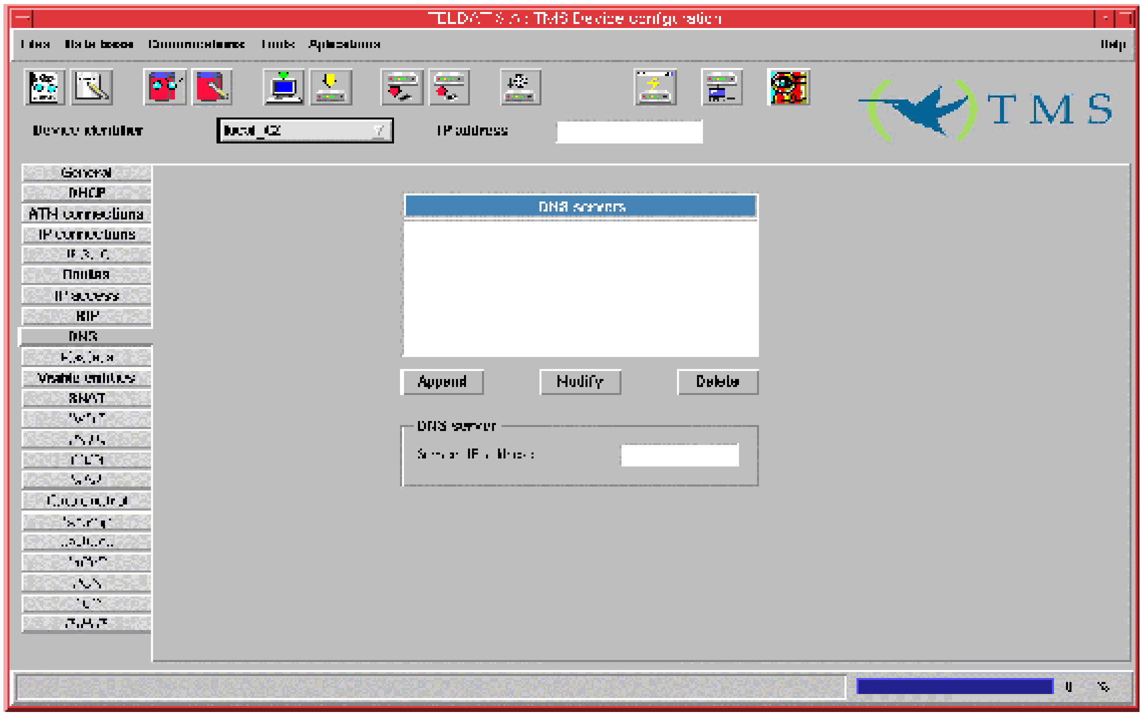


Figure 17: Configuring DNS server

To ***add*** a DNS server, introduce its IP address and subsequently press the **Append** button.

To ***modify*** a DNS server, select it from the list, alter its IP address and press the **Modify** button.

To ***delete*** a DNS server, select it from the list and press **Delete**.

- ***Configuring authorized master routers***

The parameters for the master routers authorized to manage the device must be introduced in this screen.

You need to define the telephone number, the IP address and the connection parameters, which the device establishes when management is needed.

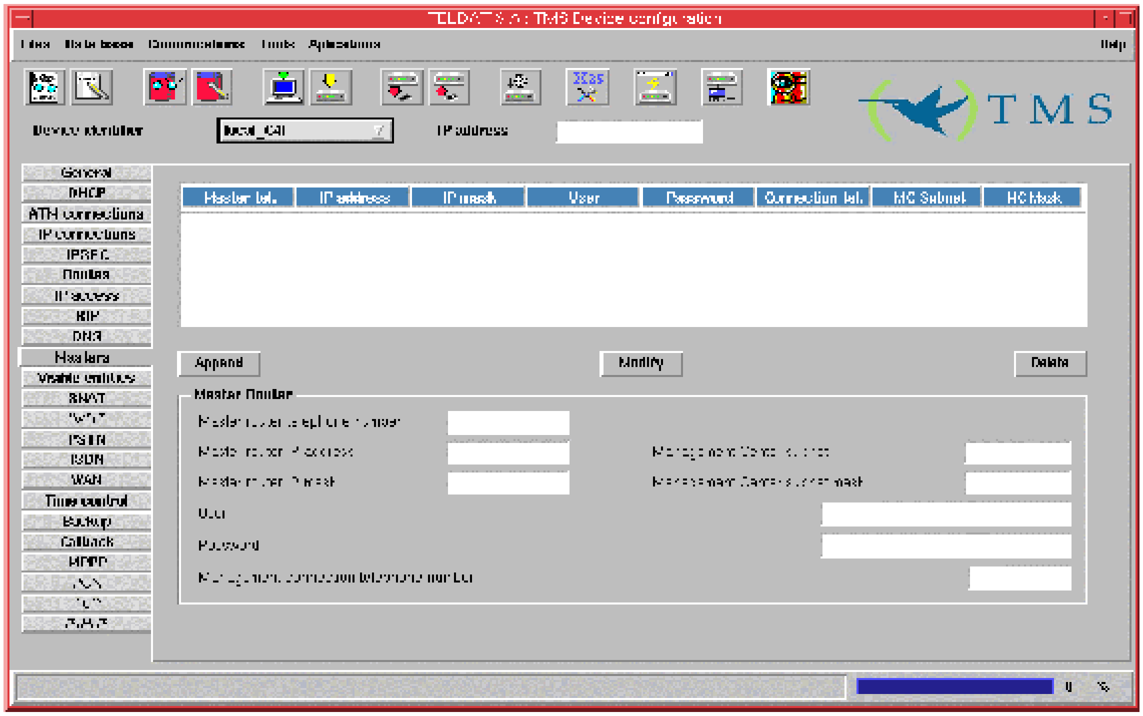


Figure 18: Configuring authorized masters

- **Master router telephone number:** The telephone number of the master router authorized to manage the device. When the device receives a call from this number, it does not accept it but begins the establishment process for a management connection calling the telephone number that will be configured below. Up to 19 digits are admitted.

- **Master router IP address:** IP address of the authorized master router. Once the management connection has been established, the device communications its IP address to the master.

- **Master router IP mask:** This field is used to restrict the network the Master router pertains to. The default value is empty or 0.0.0.0 which means the same.

- **User:** Management connection user identifier. Up to 31 characters are admitted.

- **Password:** Password associated to the above user. Up to 31 characters are admitted.

- **Management connection telephone number:** This is the telephone number the device must call in order to establish the management connection.

- **Management Center subnet:** This field and the following field permit you to specify an IP subnet associated to the Management Center in order to take better advantage of the addresses. The default value is empty or “0.0.0.0”.

- **Management Center subnet mask:** The default value is empty or “0.0.0.0”.

In order to ***add*** a master router, fill out both fields and press the **Append** button.

To ***modify*** a master router, select it, modify it in the edit fields and then press **Modify**.

To ***delete*** a master router, select it from the list and press **Delete**.

A maximum of 15 authorized masters are admitted.

The minimum number of masters authorized from the configuration application is 4

h) Configuring Backup

• NOVACOM and NOVACOM-X25 devices

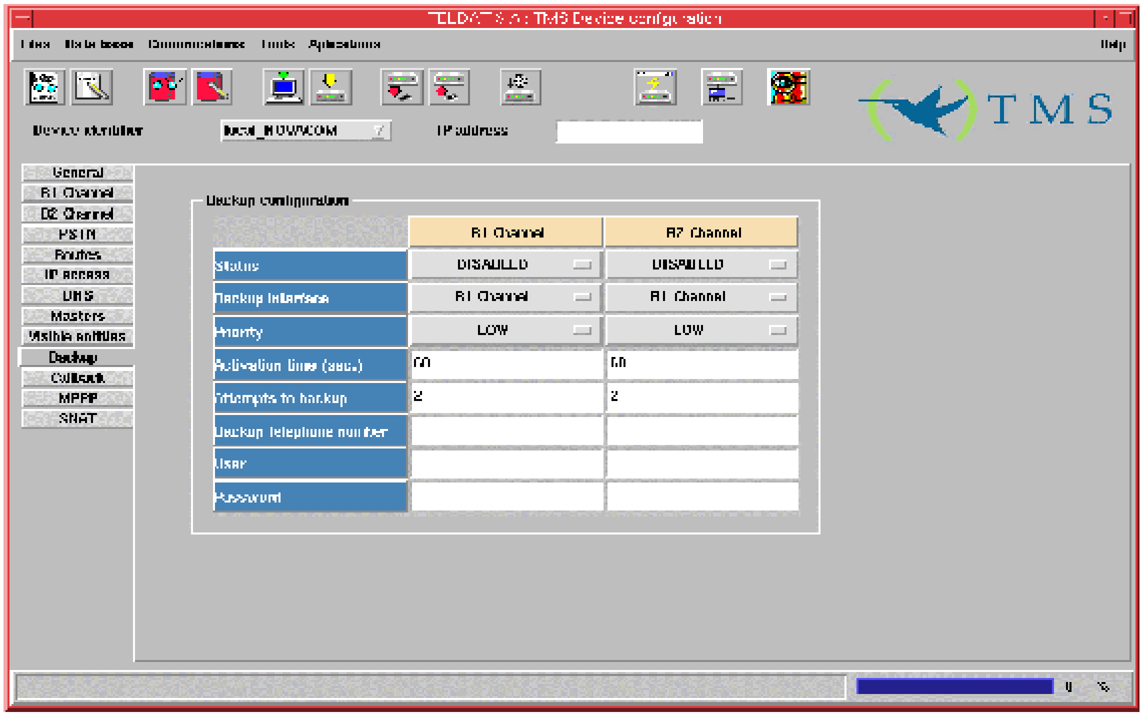
Backup configuration permits the device to try an alternative connection route in cases where the pre-established connection fails. This is independently configured for each of the two ISDN B channels.

The backup interface can be the same B channel, the other B channel or the PSTN line (through a modem). The following could occur for example, the user cannot connect to his supplier with a determined user and password, in this case switch to backup commences calling the same telephone number but with an alternative user and password.

There are two possible causes to switch to backup:

1. When the connection times out.
2. When the number of connection retries is exceeded.

When one of these conditions is met, the switch to backup process begins.



Device identifier: local_NOVACOM
IP address:

Backup configuration

	B1 Channel	B2 Channel
Status	DISABLED	DISABLED
Backup interface	B1 Channel	B1 Channel
Priority	LOW	LOW
Activation time (sec.)	60	60
Attempts to backup	2	2
Backup telephone number		
User		
Password		

Figure 19: Configuring backup

The following parameters are configurable:

- **Status:** This indicates for each ISDN B channel whether backup is enabled or not. If it is not enabled, the application will not check the rest of the channel backup parameters.

- **Backup interface:** This is the interface through which backup connection is carried out. This can be either of the two ISDN B channels or PSTN.

> ***With PPP multilink enabled in each ISDN channel, backup can only be carried out through this or through the PSTN channel.***

- **Priority:** This serves to decide which ISDN B channel has greater priority in cases where both enter into backup through the same interface. Should this happen, the backup channel with higher priority prevails, interrupting the other if necessary. If both have the same priority, then the one that enters backup first prevails.

- **Activation time (sec.):** This is the period of time in seconds that the device waits in order to establish the connection demanded. If the connection cannot be established within this period then the device will try the backup connection. Once this connection has been established, the timer returns to zero. Values within the range of **[20 .. 120]** seconds are admitted.

- **Attempts to backup:** Each time the device receives an IP packet; it tries to establish an ISDN call if this is not already established. If a connection cannot be established and the backup is disabled, the packet is discarded. However, if the backup is enabled, the counter for failed connection attempts increases. When the maximum number of attempts in this parameter has been reached, the device tries the backup connection. Once the call has been established, the attempts counter returns to zero. Values within the range **[0 .. 4]** are admitted. The value 0 indicates that the backup call will be tried the first time a transmission is demanded.

- **Backup telephone number:** This is the telephone number the device calls in order to establish the backup call. This parameter is compulsory if backup is enabled. A maximum of 31 numerical characters are admitted.

- **User:** This is the user identifier that is used to try and establish the backup connection.

- **Password:** This is the backup user password. Up to 31 characters distinct to blank are admitted.

• *Cx devices*

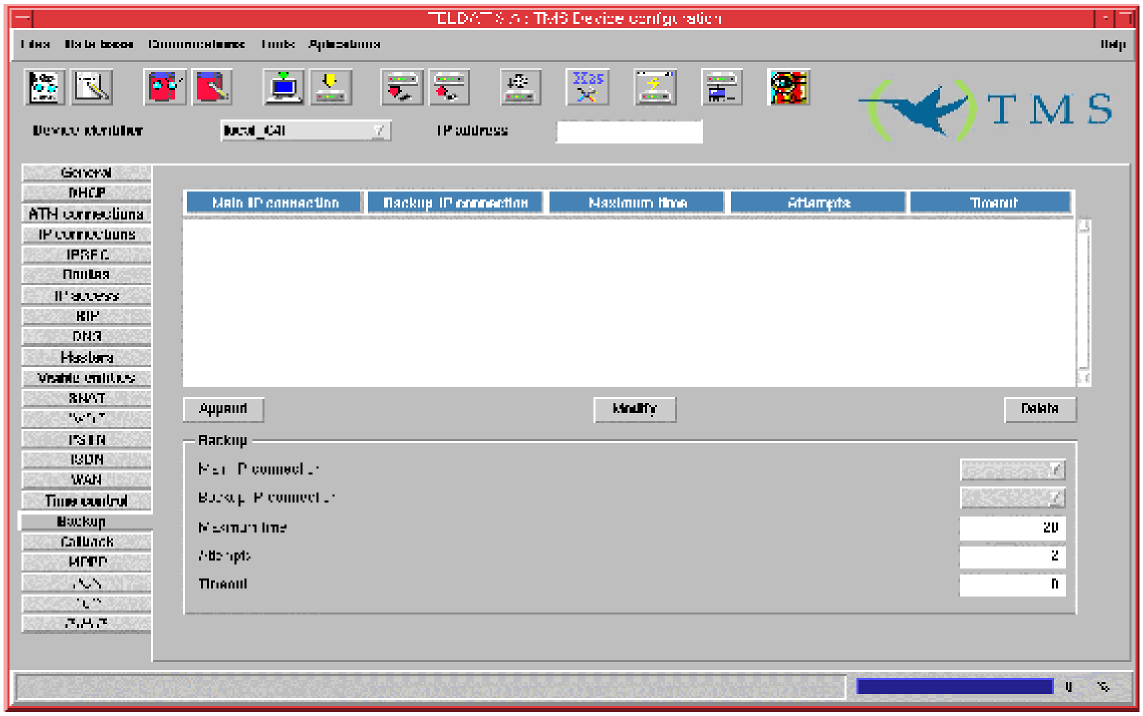
Backup configuration permits the device to try an alternative connection route in cases where the pre-established connection fails. This is independently configured for each IP connection associated to an ISDN line.

The backup IP connection can be the same as the main one or a different one assigned to an ISDN line.

There are two possible causes to switch to backup:

3. When the connection times out.
4. When the number of connection retries is exceeded.

When one of these conditions is met, the switch to backup process begins.



Device identifier: local_C4I
IP address:

Main IP connection:
Backup IP connection:
Maximum time: 20
Attempts: 2
Timeout: 0

Figure 20: Configuring backup

The following parameters are configurable:

- **Main IP connection:** Indicates the IP connection through which backup has been configured.

- **Backup IP connection:** This is the IP connection through which the backup connection is attemped.

> ***With multilink PPP enable, the IP connection associated to an ISDN line can only carry out backup through itself.***

- **Maximum time:** Maximum wait time for backup.

- **Attempts:** Each time the device receives an IP packet; it tries to establish an ISDN call if this is not already established. If a connection cannot be established and the backup is disabled, the packet is discarded. However, if the backup is enabled, the counter for failed connection attempts increases. When the maximum number of attempts in this parameter has been reached, the device tries the backup connection. Once the call has been established, the attempts counter returns to zero. Values within the range **[0 .. 4]** are admitted. The value 0 indicates that the backup call will be tried the first time a transmission is demanded

- **Time out:** This is the period of time in seconds that the device waits in order to establish the connection demanded. If the connection cannot be established within this period then the device will try the backup connection. Once this connection has been established, the timer returns to zero. Values within the range of **[20 .. 120]** seconds are admitted.

In order to ***add*** a new backup to the list, introduce the appropriate values in the fields and press the **Append** button.

In order to ***modify*** a backup, select it in the list and once modified through the corresponding fields, press the **Modify** button.

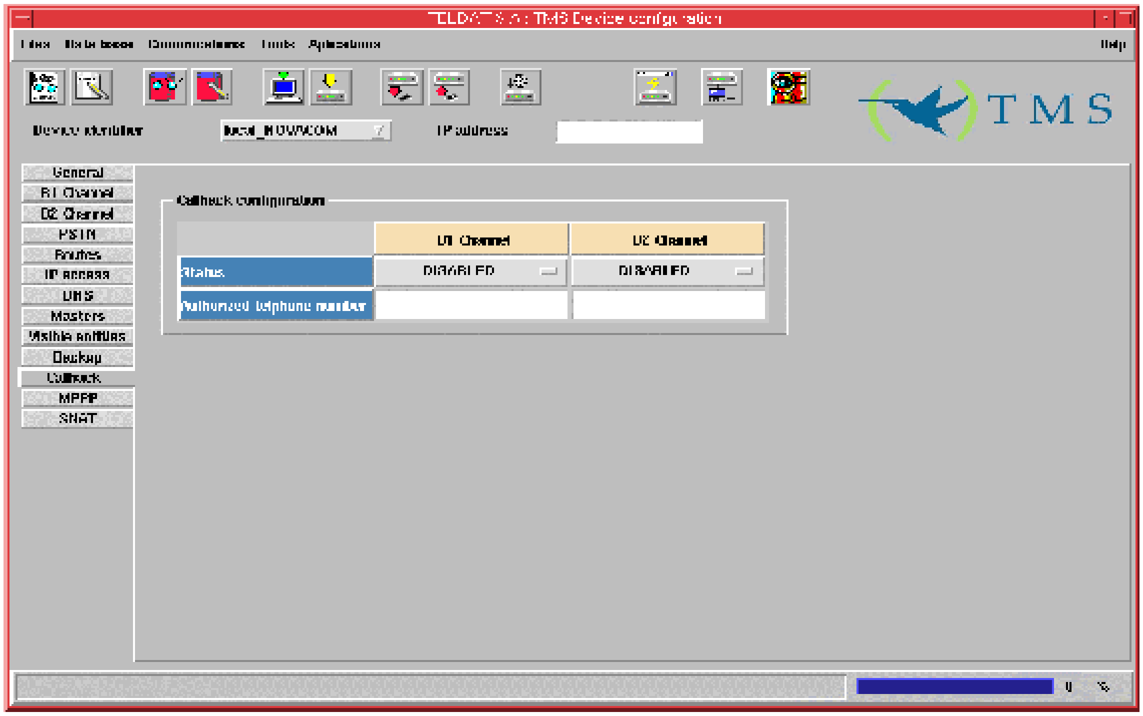
In order to ***delete*** a backup from the list, select it and press **Delete**.

A maximum of 10 backups are admitted

i) Configuring Callback

• *NOVACOM and NOVACOM-X25 devices*

The so-called "Callback Facility" permits the device to connect through one of the two ISDN B channels and obtain an IP address when a call is received from an authorized telephone number. The aim is to permit connection on demand from outside the LAN connected to the device.



Device identifier: local_NOVACOM
IP address:

Callback configuration

	B1 Channel	B2 Channel
Status	DISABLED	DISABLED
Authorized telephone number		

Figure 21: Configuring callback

The configurable parameters are as follows:

- **Status:** If this is configured as ENABLED, when the device receives a call from the authorized telephone number, it connects through the connection configured for the associated ISDN B channel. In all cases, the call is always rejected by the device (cost free for the caller).

- **Authorized telephone number:** This is the telephone number authorized to “wake” the callback connection process. If this field is empty, this is interpreted as any ISDN call received by the device provokes the callback connection process (all telephone numbers are authorized). Up to 19 digits are admitted.

> ***Compatibility with versions prior to 5.4.0.***
>
> ***Device versions prior to 5.4.0 do not support independent callback configuration for each channel. In order to maintain compatibility follow the below criteria:***
>
> ***“If callback is disabled for the B1 channel and enabled for B2, the B2 channel configuration is sent to the device. In any other case, the B1 channel callback configuration is sent”.***

• Cx devices

The so-called “Callback Facility” permits the device to connect through one IP connection associated to an ISDN line and obtain an IP address when a call is received from an authorized telephone number. The aim is to permit connection on demand from outside the LAN connected to the device.

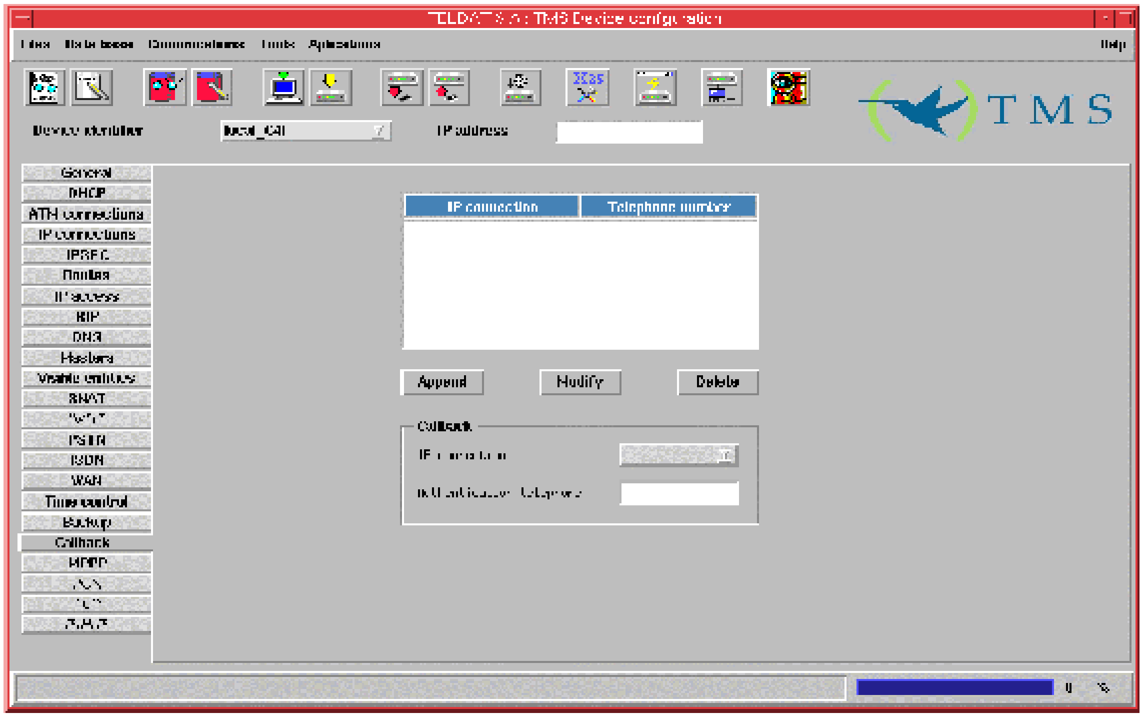


Figure 22: Configuring callback

The configurable parameters are as follows:

- **IP connection:** IP connection identifier.

- **Authentication telephone**: This is the authorized telephone number to wake the callback connection process. If this field is empty, any ISDN called received by the device will lunch the callback connection process (all telephone numbers are autorized). Up to 19 digits are admitted.

In order to ***add*** a new callback to the list, introduce the appropriate values in the fields and press the **Append** button.

In order to ***modify*** a callback, select it in the list and once modified through the corresponding fields, press the **Modify** button.

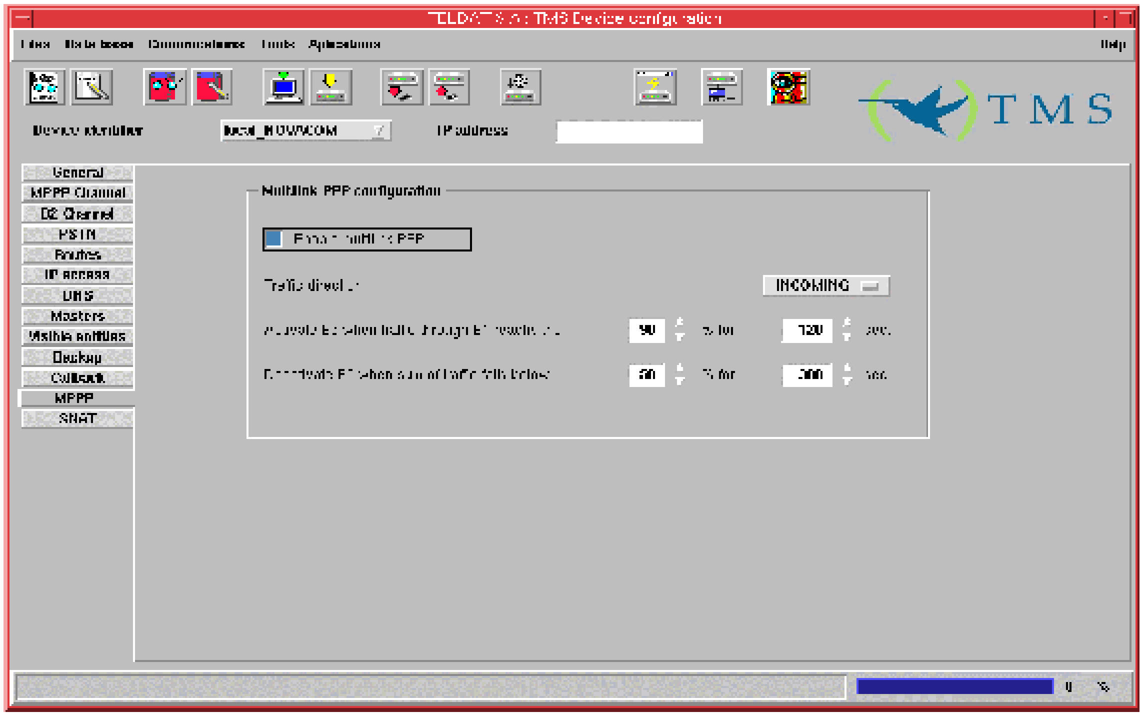
In order to ***delete*** a callback from the list, select it and press **Delete**.

A maximum of 10 callbacks are admitted

j) MPPP (Point to Point Protocol)

• NOVACOM and NOVACOM-X25 devices

From device **version 5.2.0** onwards, you can configure the device in such a way that when traffic sent through the ISDN B1 channel surpasses a determined threshold, a connection through the B2 channel is established and the traffic divided between them.



Device identifier: local_NOVACOM

IP address:

☑ Enable multilink PPP

Traffic direction: INCOMING

Activate B2 when traffic through B1 reaches 90 % for 120 sec.

Deactivate B2 when sum of traffic falls below 60 % for 300 sec.

Figure 23: Configuring multilink PPP

The following parameters can be configured:

- **Enable PPP multilink:** This permits you to enable or disable multilink PPP. If this is enabled, it prevents the user from altering the ISDN B2 channel configuration as this obligatorily takes the same configuration as the B1 channel and is reserved for cases of heavy traffic in B1. Also, all the configuration entities referring to the B2 channel are ignored (e.g. routes).

- **Traffic direction:** This indicates the direction of the traffic to consider whether to activate or deactivate the multilink. This can be **INCOMING** traffic in the LAN, **OUTGOING** or **BOTH**. If you are considering a single direction, the line capacity is 64 Kbps while in both directions it is 128 Kbps. The default value only considers **INCOMING** traffic in the LAN.

- **Activation threshold:** Percentage of traffic sent through the B1 channel, if this is exceeded during the whole of the activation interval, the multilink connection is launched through the B2 channel. Values in the interval of [**0 .. 100]%** are admitted for the line capacity. The default value is **90%**.

- **Activation interval:** Temporary interval where the traffic being sent is compared with the activation threshold. Values within the range [**28 .. 18000]** seconds are admitted. The default value is **120** seconds.

- **Deactivation threshold:** Percentage of active traffic which if this falls below the deactivation threshold during the whole of the deactivation interval, the multilink connection through the B2 channel is deactivated. In order to deactivate, the total volume of the traffic is shown (for both the channels together). Values within the range of [**0 .. 100]% are** admitted. The default value is **50%**.

- **Deactivation interval:** Temporary interval where the traffic being sent is compared with the deactivation threshold. Values within the range [**28 .. 18000]** seconds are admitted. The default value is **300** seconds.

Below you can see a typical PPP multilink activation sequence with default configuration values.

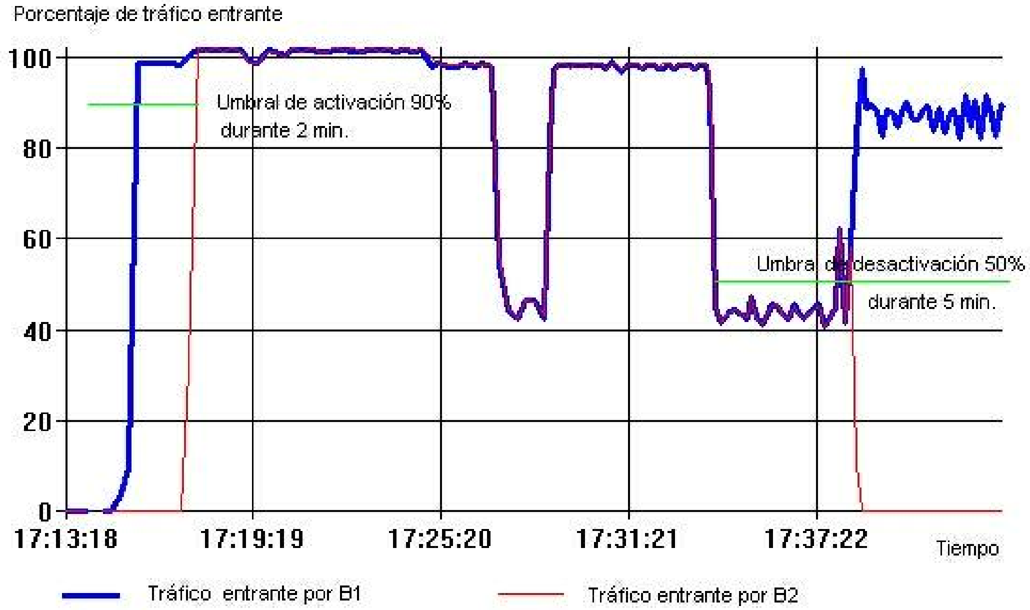


Figure 24: multilink PPP activation sequence

The situation is as follows. We have a device with the multilink PPP activated with the default configuration. This consists of an activation threshold of a 90% load, taking into consideration only incoming traffic in the LAN, during 2 minutes and a deactivation threshold of 50% during 5 minutes.

At approximately 17.15, reception begins of a large file through FTP via channel B1 and the load for the said channel rapidly reaches 100% of its capacity. However, the B2 channel does not activate until an approximate period of 2 minutes has lapsed from the time the traffic through the B1 channel exceeds the activation threshold of 90%. Once the connection has been established through the B2 channel you can see the device uses the capacity of both the channels at 100%.

At 17:27, a drop in the B1 channel load is produced falling below the deactivation threshold (50%) but lasts for a period of time less than the deactivation period (5 minutes), therefore the B2 connection is maintained.

Finally at 17:38, the traffic through the B1 channel drops below the deactivation threshold during a period of time greater than the deactivation interval and therefore the device releases the B2 channel call.

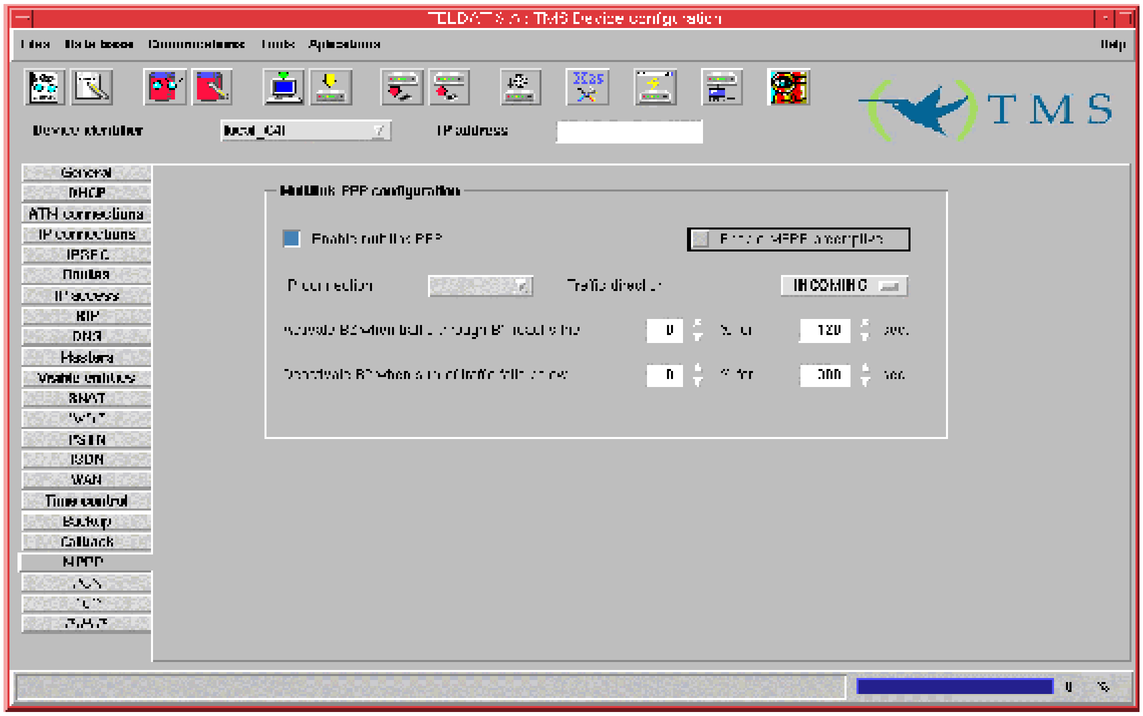
Multilink PPP and ISDN B2 channel:

From version 5.2.0 to versions 5.3.0, enabling the multilink PPP meant the deactivation of the connection profile established in the B2 channel as well as the entities used such as the routes for example.

> ***From version 5.3.0 onwards, the B2 connection profile has priority over the second multilink PPP channel, if this is enabled. I.e. if both channels are being used by the multilink and a connection is requested through B2, then the multilink will release its second channel and establish the requested connection. Vice versa, if the B2 connection is established, then the multilink cannot use its second channel.***

- ***Cx devices***

Trought the TMS you can configure the device in such a way that when traffic sent through the ISDN B1 channel surpasses a determined threshold, a connection through the B2 channel is established and the traffic divided between them



Device identifier local_C4I
IP address

Multilink PPP configuration

■ Enable multilink PPP
□ Enable MPPP preemptive

IP connection
Traffic direction INCOMING

Activate B2 when traffic through B1 exceeds the 0 % for 120 sec.

Deactivate B2 when amount of traffic falls under 0 % for 300 sec.

Figure 25: Configuring multilink PPP

The following parameters can be configured:

- **IP connection:** IP connection identifier.

- **Enable multilink PPP:** This permits you to enable or disable multilink PPP. If this is enabled, it prevents the user from altering the ISDN B2 channel configuration as this obligatorily takes the same configuration as the B1 channel and is reserved for cases of heavy traffic in B1. Also, all the configuration entities referring to the B2 channel are ignored (e.g. routes).

- **Enable MPPP preemptive:** Permits enable or disable the MPPP preemptive.

- **Traffic direction:** This indicates the direction of the traffic to consider whether to activate or deactivate the multilink. This can be **INCOMING** traffic in the LAN, **OUTGOING** or

BOTH. If you are considering a single direction, the line capacity is 64 Kbps while in both directions it is 128 Kbps. The default value only considers **INCOMING** traffic in the LAN.

- **Activation threshold:** Percentage of traffic sent through the B1 channel, if this is exceeded during the whole of the activation interval, the multilink connection is launched through the B2 channel. Values in the interval of [**0 .. 100]%** are admitted for the line capacity. The default value is **90%**.

- **Activation interval:** Temporary interval where the traffic being sent is compared with the activation threshold. Values within the range [**28 .. 18000]** seconds are admitted. The default value is **120** seconds.

- **Deactivation threshold:** Percentage of active traffic which if this falls below the deactivation threshold during the whole of the deactivation interval, the multilink connection through the B2 channel is deactivated. In order to deactivate, the total volume of the traffic is shown (for both the channels together). Values within the range of [**0 .. 100]% are** admitted. The default value is **50%**.

- **Deactivation interval:** Temporary interval where the traffic being sent is compared with the deactivation threshold. Values within the range [**28 .. 18000]** seconds are admitted. The default value is **300** seconds.

k) Configuring static NAT (Network Address Translation)

A **NAT (Network Address Translation)** incoming register table can be configured in the router. This deals with the conversion of local address ranges to global address ranges taking into consideration the outgoing interface as well.

NAT may be necessary in the following cases:

1. When you wish to have connectivity with INTERNET, but not all the devices have global IP addresses (permitted). In this case you configure a NAT device as the link between the private domain (local network) and the public domain (public network: in this case Internet). The NAT device translates the local addresses into global addresses before sending the packet to the exterior.

2. A company requires IP connectivity between remote branches. These remote branches possess internal IP networks which do not comply with an addressing plan meaning that the routing tables in order to achieve connectivity between them are too big or impossible. In this case, it is sufficient to configure NAT in the boundary devices for each branch and thus carry out the transformation between the internal branch networks to the global networks that now comply with the addressing plan.

3. In cases where you need to change the internal addresses for many devices, instead of carrying out this change, which would be very time consuming, you can execute NAT.

The term "local" represents those networks that pertain to a company and that need to be translated. Within in the local domain, a determined device will possess a local address, while to the exterior; it appears to possess an address from another group of addresses. I.e. the first space of addresses is **local** and the second is **global**.

Types of NAT

Address translation can be:

Static NAT The correspondence of local and global addresses is unique. This is the type configured in this screen.

Dynamic NAT Correspondence of local addresses is established in a global address pool. I.e. the correspondence between global and local addresses is not unique and depends on the execution conditions.

NAPT (Address Port Translation) Correspondence is established between local addresses and a single global address. In this case a translation of the transport protocol ports (UDP, TCP) is carried out.

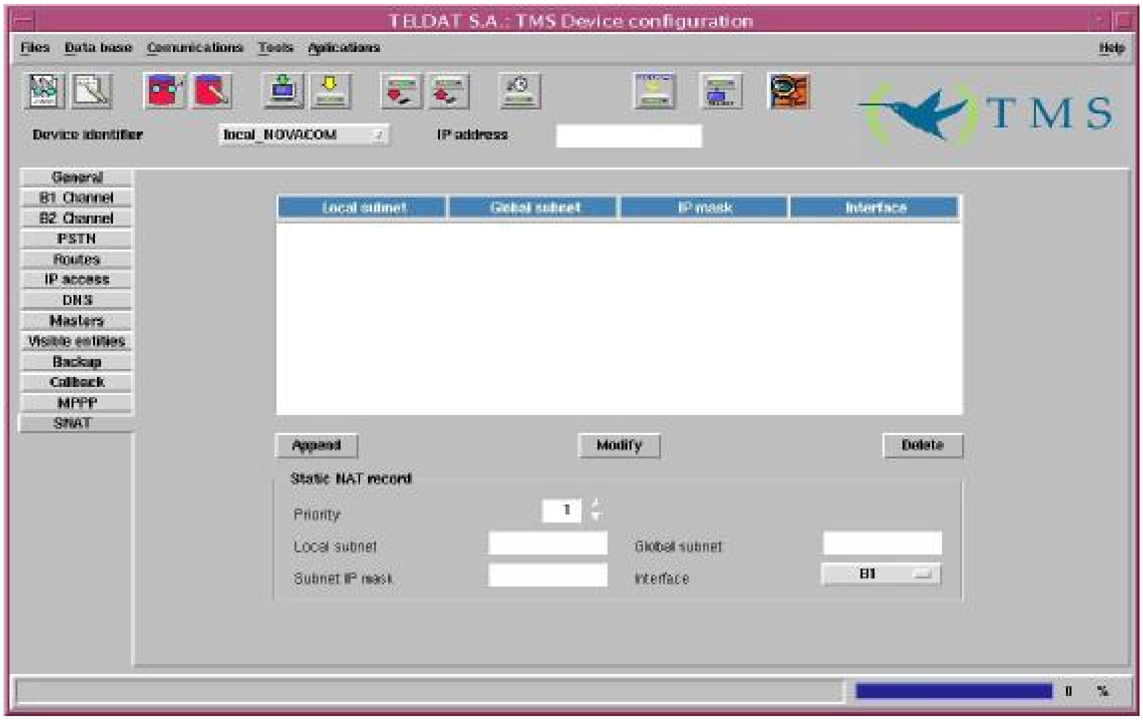
Address conversion is bi-directional i.e. any address pertaining to the local subnet that is in a register from this table converts to a range of global addresses if these exit through the assigned interface and vice versa, any address that enters through the interface from the exterior and pertains to the global subnet is converted to the local range.

For each packet the interface and IP address is compared with that of the local subnet (if the packet exits through the LAN) or with the global (if the packet enters the LAN) with the table registers, in order, until one matches. From here the order of the registers in the table is important, as this is equivalent to the priority of some conversion rules versus others.

Should you require further information on NAT, please consult the manual {Teldat: NAT, 99}.

• *NOVACOM and NOVACOM-X25 devices*

From device **version 5.6.0** onwards, you can configure a new register table of **NAT** entries **(Network Address Translation)**.



Device identifier: local_NOVACOM
IP address:

Local subnet	Global subnet	IP mask	Interface

Priority: 1
Local subnet:
Global subnet:
Subnet IP mask:
Interface: B1

Figure 26: Configuring static NAT

The fields making up each static NAT register are as follows:

- **Priority :** This specifies the order in which the NAT regulations are checked. This will be applied to the first one that complies with this.

- **Local subnet:** Host IP address or address of the subnet pertaining to the LAN that the device is connected to.

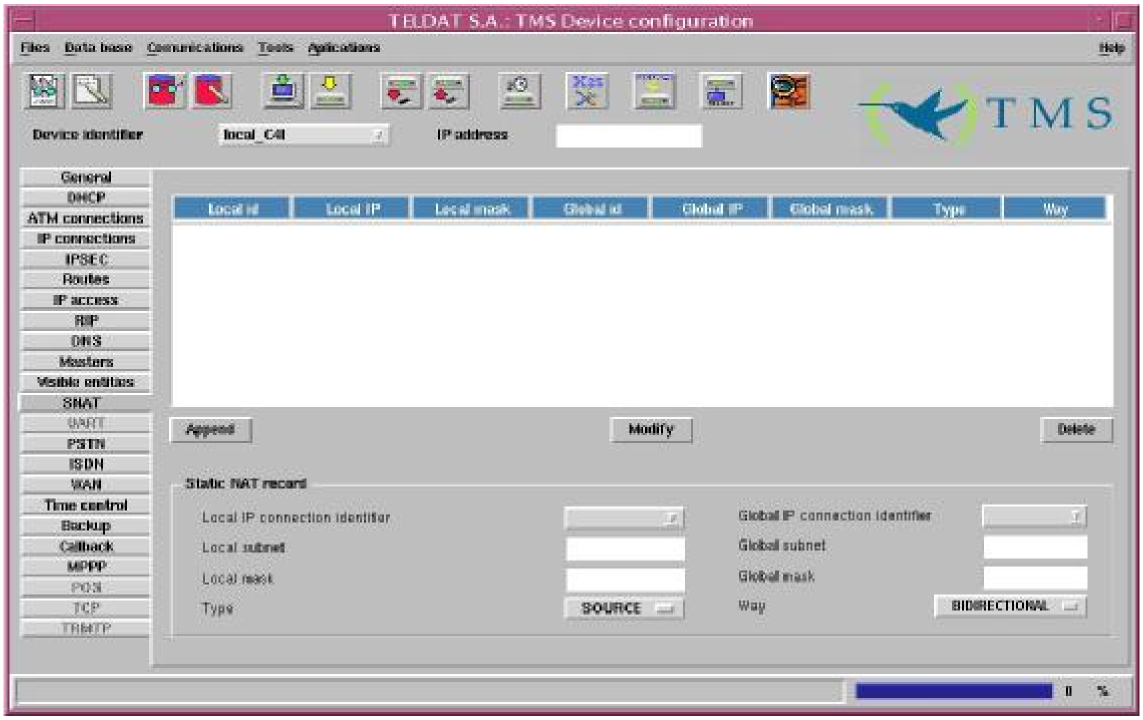
- **Global subnet:** IP address for the host or subnet assigned in the WAN where the device is connected through the interface indicated in the register.

- **Subnet IP mask:** IP mask for the subnet or the host, which is applied over the above two addresses to delimit the subnets. This must comply so the binary AND between each subnet and the negated mask is equal to 0.

- **Interface:** This is the interface through which the device connects to the WAN.

Up to a maximum of 10 registers are permitted in the table.

- ***Cx devices***



Device identifier: local_C4I

IP address:

Local id	Local IP	Local mask	Global id	Global IP	Global mask	Type	Way

Static NAT record

Local IP connection identifier:

Local subnet:

Local mask:

Type: SOURCE

Global IP connection identifier:

Global subnet:

Global mask:

Way: BIDIRECTIONAL

Figure 27: Configuring static NAT

The field components for each static NAT register are as follows:

- **Local IP connection identifier:** Specifies the IP connection through which you access the local subnet. If this value is zero, this refers to the LAN interface.
- **Global IP connection identifier:** Specifies the IP connection through which you access the global subnet. If this value is zero, this refers to the LAN interface.
- **Local subnet:** Host IP address or address of the subnet pertaining to the LAN that the router is connected to.
- **Global subnet:** IP address for the host or subnet assigned in the WAN where the router is connected through the interface indicated in the register.
- **Máscara IP:** IP mask for the subnet or the host, which is applied over the above two addresses to delimit the subnets. This must comply so the binary AND between each subnet and the negated mask is equal to 0.
- **Type:** There are two types of transformation:

  1. **SOURCE**

- For all the packets that pass from the local domain to the global (always complying with the required regulations), the local source address will be changed for the corresponding global address. Also all the packets that pass from the global domain to the local (always complying with the required regulations) will have their global destination address changed for the corresponding local on.

2. DESTINATION

- For all the packets that pass from the local domain to the global (always complying with the required regulations), the local destination address will be changed for the corresponding global address. Also all the packets that pass from the global domain to the local (always complying with the required regulations) will have their global source address changed for the corresponding local one.

- **Direction:** There are 5 transformation directions

1. **LOCAL TO GLOBAL:** If the packet enters through the local interface and exits by the global interface and its address (source or destination) belongs to the local network, then the local address (source or destination) changes to the corresponding global address.

2. **GLOBAL TO LOCAL:** If the packet enters through the global interface and its address (source or destination) belongs to the global network, then the global address (source or destination) changes to the corresponding local address.

3. **BI-DIRECTIONAL:** The two above points apply to this.

4. **DISABLE LOCAL:** If the packet enters through the local interface and exits by the global interface and its address (source or destination) belongs to the local network, then no change is carried out.

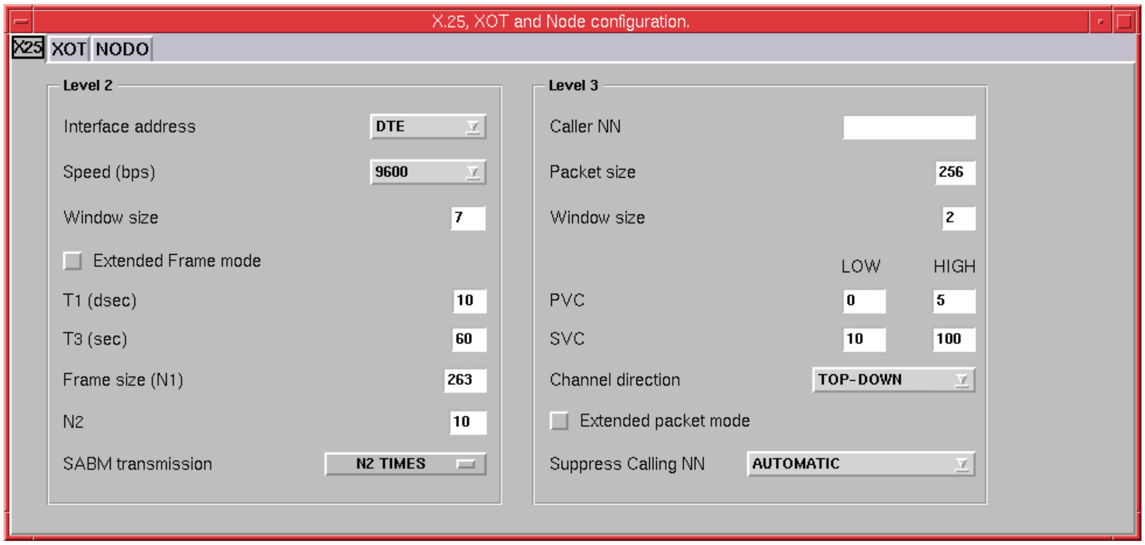
5. **DISABLE GLOBAL:** If the packet enters through the global interface and its address (source or destination) belongs to the local network, then no change is carried out.

Up to a maximum of 10 registers are permitted in the table.

I) Configuring X.25 (NOVACOM-X25 devices only)

The X.25, Node and XOT configuration screens open on pressing the X25 button on the tool bar.

In the below figure, the configurable parameters for an X.25 line are shown, grouped according to the levels.



Level 2

Interface address: DTE

Speed (bps): 9600

Window size: 7

□ Extended Frame mode

T1 (dsec): 10

T3 (sec): 60

Frame size (N1): 263

N2: 10

SABM transmission: N2 TIMES

Level 3

Caller NN:

Packet size: 256

Window size: 2

	LOW	HIGH
PVC	0	5
SVC	10	100

Channel direction: TOP-DOWN

□ Extended packet mode

Suppress Calling NN: AUTOMATIC

Figure 28: Configuring X.25

Level 2 (LAPB protocol)

- **Interface address:** Specific for the level 2 X.25 LAPB protocol, this behaves as terminal (**DTE**) or modem (**DCE**).
- **Speed (bps):** Through this parameter, the binary regime at which the X.25 interface operates is configured. The possible values are the range of synchronous speeds from **1.200** to **2.048.000** bits per second (bps).
- **Window size:** Maximum number of I frames consecutively numbered that DTE or the DCE may have pending (i.e. without reception acknowledgement) at a given moment. The value of this parameter (parameter *k*) is within the range **[2 .. 7]** if the extended frame mode is not activated and **[2 .. 127]** if this is activated. The default value is **7**.
- **Extended Frame mode:** Specifies the NS field module (Sequence Number) for the X.25 link level. I.e. the module used to consecutively number the sent LAPB frames. If this is not activated this is module 8 and if it is, 128.
- **T1 (dsec):** T1 is the maximum time in tenths of seconds that frame acknowledgement is waited. Once this is lapsed, if there has been no exchange of frames, the device retransmits the frame pending acknowledgement. Values in the range of **[1 .. 100]** are admitted with **10** tenths of a second being the default value.
- **T3 (sec):** This is the maximum time in seconds that a frame acknowledgement is awaited. Once this time has lapsed, the device sends an RR with poll bit. This must be sufficiently long enough so the DCE T1 timer period (i.e. T3>T1) on the expiry of T3, has sufficient time to ensure that the data link channel is found in an non-active or non-operational state and it is necessary to establish a data link to resume normal operation. Values in the range of **[1 .. 100]** are admitted with **60** seconds being the default value.
- **Tamaño de Trama (N1):** Maximum number of bytes in a frame (excluding flags; 0 bits or the control escape octets inserted so there is transparency in the synchronous or start stop transmission respectively; and the bits inserted for the transmission timer in the start stop transmission) which the DCE or the DTE are able to accept from the DTE or the DCE respectively. Values in the range of **[1 .. 4103]** are admitted with **263** bytes being the default value.
- **N2:** This is the maximum number of retransmissions for a non-acknowledged frame. Values in the range of **[1 .. 100]** are admitted with **10** being the default value.

- **SABM transmission:** Determines if the X.25 level 2 entity will constantly try and establish the link transmitting SABM. SABM (*Set Asynchronous Balanced Mode*) ensures that all the order/response control fields have a length of one octet.
  - **N2 TIMES**: (Default value) transmits the SABM frame N2 tim.
  - **CONTINUOUS**: Continuously sent.
  - **DISABLED**: Waits for the remote entity to establish the link.

> ***If at a physical layer (a non logical value is configured with the "interface Address" parameter) the device is operating as DTE, the value CONTINUOUS is not admitted and when the configuration is sent, an SNMP error is returned.***

In order to see how the device is configured at a physical level, you need to enter the device console through TELNET and enter the following commands (in **bold**):

```
*p 3

+node x25

-- X25 Monitor --
X25>display port
Port number(7-11): 7
Line: 1

Interface type: DTE

   Circuit:      105 108 106 107 109
   RS232-C:      RTS DTR CTS DSR DCD
   Status:        ON  ON  ON  ON  ON

Restart Status: Ready (R1)

LCN    WINDOW   N(s)  N(r)  N(ack)      STATE
   1      2       0     0      0    P1 Ready
   2      2       0     0      0    P1 Ready

X25>
```

Level 3

- **Caller NA:** The NA (Network Number) is the caller X.25 address for the call request packets that exit through the port, independently of the NA with which they have been received in the device. Up to 15 digits are admitted.
- **Window size:** Configures the level 3 screen i.e. the maximum number of X.25 packets that can be pending acknowledgement. If the extended packet mode is activated, the range is **[2 .. 127],** if it is not activated, it is **[2 .. 7].** The default value is **2** packets.
- **Packet size:** Maximum size of the X.25 packet in bytes. Larger packets provoke an error in the established call. Admit values in the range **[128 .. 1024]** with **256** being the default value.
- **Lowest PVC:** Indicates the lowest Permanent Virtual Channel number that can be used in X.25 communications. The PVC range used by your device is negotiated with the PTT. Values in the range **[0 .. 4096]** are admitted with **0** being the default value.

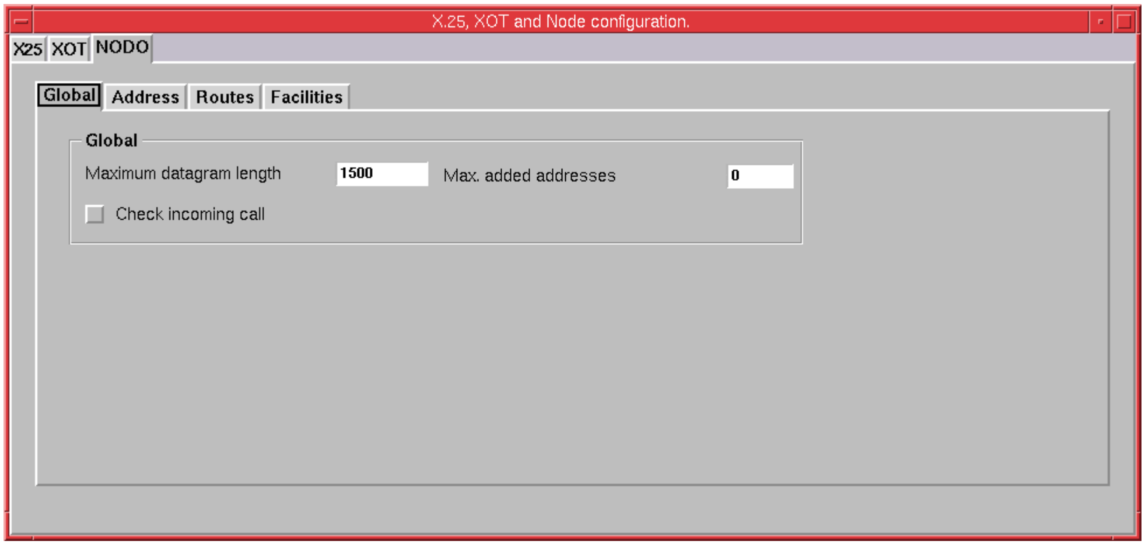
- **Highest PVC:** Indicates the highest Permanent Virtual Channel number that can be used in X.25 communications. The PVC range used by your device is negotiated with the PTT. The PVC range must always be below the SVC range. Values in the range **[0 .. 4096]** are admitted with **0** being the default value.
- **Lowest SVC:** Indicates the lowest Switched Virtual Circuit number that can be used in X.25 communications. The SVC range used by your device is negotiated with the PTT. Values in the range **[0 .. 4096]** are admitted with **100** being the default value.
- **Highest SVC:** Indicates the highest Switched Virtual Circuit number that can be used in X.25 communications. The SVC range used by your device is negotiated with the PTT. Values in the range **[0 .. 4096]** are admitted with **100** being the default value.
- **Channel direction:** Specifies if the logical channel numbers are used in order from the lowest to the highest (**ASCENDING**) or vice versa (**DESCENDING**).
- **Suppress calling NA:** This ensures that the calling network number does not appear at the destination.
- **Extended packet mode:** Module used to consecutively number the sent X.25 packets. Module 8 is deactivated and module 128 is activated.

• *Configuring the node (NOVACOM-X25 and C4i devices only)*

The node configuration is presented grouped in four information blocks.

Global configuration of the node

This screen shows the global configuration parameters.



Maximum datagram length: 1500
Max. added addresses: 0
□ Check incoming call

Figure 29: Global configuration of the node

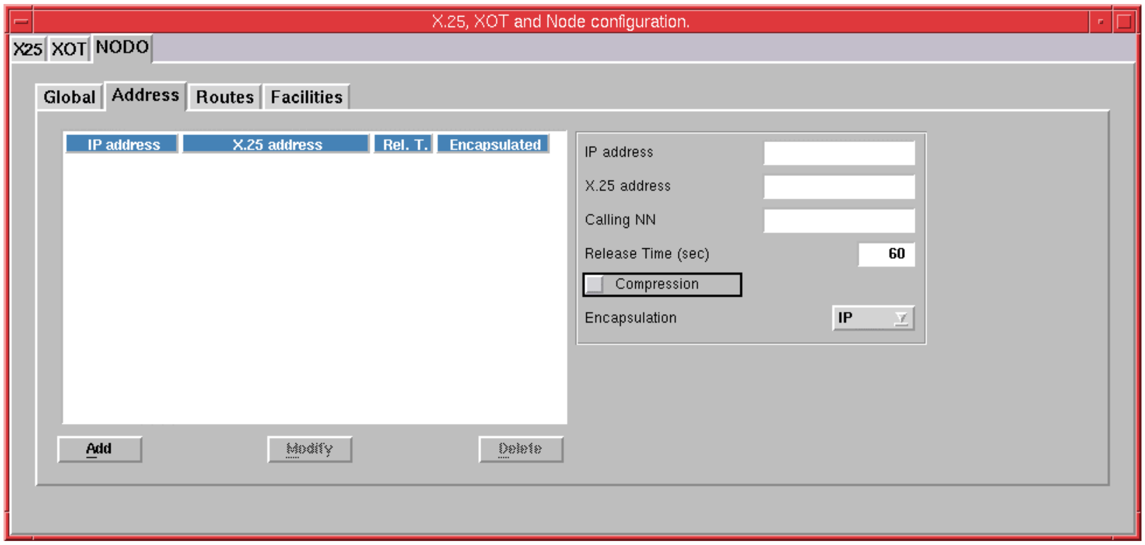
As shown in the figure, global configuration permits you to configure the following fields:

- **Maximum datagram length:** This is the maximum size in bytes for a packet. Values in the range **[256 .. 18000]** are admitted with **1500** bytes being the default value.
- **Check incoming call:** Ensures the device verifies that a determined network caller number is in its tables. This parameter must always be active if you are going to route IP over X.25.

- **Max. added addresses:** This permits you to configure how many IP addresses you can dynamically add, i.e. without needing to restart the device so these activate. Values in the range **[0 .. 500]** are admitted with **10** being the default value.

Configuring node addresses

This screen permits you to relate an IP address with an X.25 address and associate determined characteristics to them in order to transmit data. The figure below shows how to create, delete and modify these relations.



IP address

X.25 address

Calling NN

Release Time (sec) 60

□ Compression

Encapsulation IP

Figure 30: Configuring node addresses

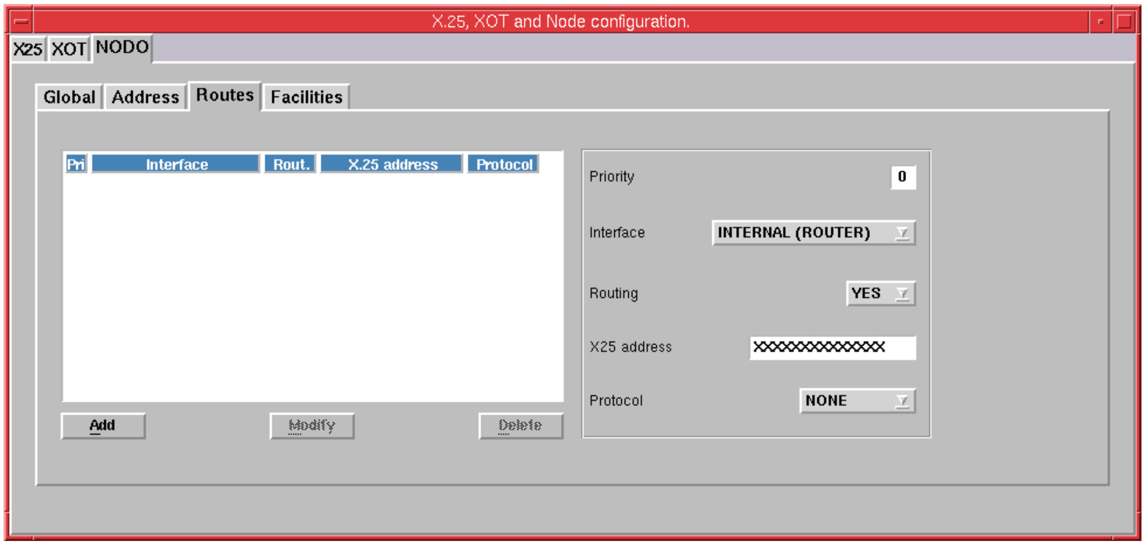
- **IP address:** This is the host IP address.
- **X.25 address:** Destination network number for the call. Up to 15 digits are admitted.
- **Calling NN:** Calling network number. Up to 15 digits are admitted.
- **Release Time (sec):** Once this time has timed out, the call is released due to absence of traffic. Values in the range of **[0 .. 65000]** are admitted with **60** being the default value.
- **Compression:** Compression is applied to the data.
- **Encapsulation:** There are two methods to encapsulate IP in X.25:
  - **IP:** this consists of putting the user data to CC in the call packet. This is used by default.
  - **VOID:** this consists of putting the user data to 0x00 and the header 0xCC in each data packet.

The number of possible entries in the table is limited by the device memory.

Configuring the node route

The routing basically consists of associating an interface with one or various X.25 addresses so the node can carry out the switch (receive information via one port and transmit it through another).

This group presents the node routing table and the possibility of adding, modifying or deleting the elements. The appearance of this screen is shown below.



Priority 0

Interface INTERNAL (ROUTER)

Routing YES

X25 address XXXXXXXXXXXXXX

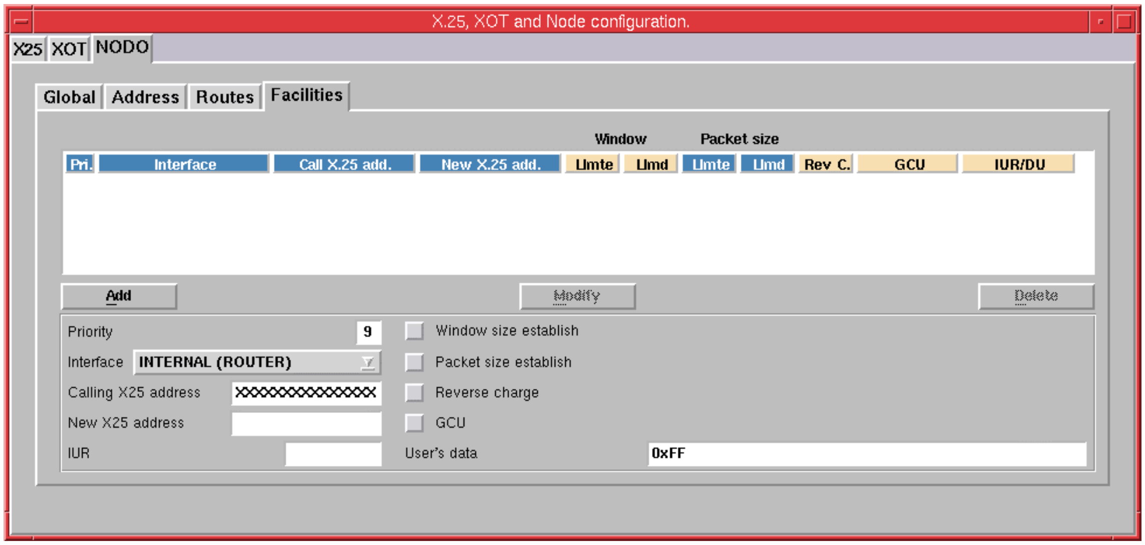
Protocol NONE

Figure 31: Configuring the node route

- **Priority:** This is the assignment priority indicator. 0 is considered as the highest priority with 9 as the lowest. Values are admitted within the said range [0 .. 9], with 9 being the default value (minimum priority). The priorities can be repeated.
- **Interface:** this is the interface the X.25 address is assigned to (or group of these).
- **Re-routing:** When dealing with a call request, the device detects that the destination line is down or busy (there are no free logical channels), it has three options:
  - **NO:** Release the call.
  - **EX:** This option prevents an X.25 call from being routed towards the same port it entered by i.e. if the highest priority routing routes the call towards an SVC from the same port that the call entered through, then the device will search to see if there are other routes towards other ports.
  - **YES:** reroutes the call towards another line with a valid *Network Number* (NA).
- **X.25 address:** This is the network number assigned to the port. In order to establish a circuit with this port, the call packet NA (source) must coincide with that programmed in this field (destination). Up to 15 digits are admitted or 'X' wildcards.
- **Protocol:** Protocol identifier: this permits you to carry out rerouting depending on the first octet in the user data field that identifies the protocol. If this is not programmed, this field is not checked**. [0..255]**. Value 0 corresponds to VOID encapsulation and 204 (0xCC) to the IP protocol.

Configuring the node facilities

This screen permits you to configure the X.25 facilities for a determined port.



X.25, XOT and Node configuration.

X25 | XOT | NODO

Global | Address | Routes | Facilities

				Window		Packet size				
Pri.	Interface	Call X.25 add.	New X.25 add.	Llmte	Llmd	Llmte	Llmd	Rev C.	GCU	IUR/DU

Priority: 9

Interface: INTERNAL (ROUTER)

Calling X25 address: XXXXXXXXXXXXXXX

New X25 address:

IUR:

□ Window size establish

□ Packet size establish

□ Reverse charge

□ GCU

User's data: 0xFF

Figure 32: Configuring the node facilities

- **Priority:** This is the order the facilities to be applied are verified.
- **Interface:** This identifies the device interface where this is applied.
- **Calling X.25 address:** This is the X.25 address or the NAI where the facilities are going to be applied. Admits 15 digits or '**X**' wildcards to be entered.
- **New X.25 address:** This is the new X.25 address or NAI that the outgoing packet will have. Admits as entry digits, '**S**' characters that suppress the digit figured in this position and **'X'** characters that do not change.
- **Window size establish:** If this is not activated then there is no screen size negotiation and that already configured is used.
- **Packet size establish:** If this is not activated, there is no negotiation and that already configured is used.
- **Reverse charge:** Permits you to request the DTE calls to be reverse charged.
- **GCU:** Closed User Group. Permits the user to form DTE groups with restricted incoming and/or outgoing access. Permits the DTEs pertaining to this group to communicate but excludes communication with the rest of the DTEs.
  - **Type:** Indicates the type of CUG:
    - **NORMAL** (or incoming): Permits a DTE pertaining to a group to receive calls from DTEs located in the open part of the network (i.e. DTEs that do not pertain to any CUG) and from DTEs pertaining to other CUGs with OUTGOING type.
    - **BILATERAL:** Permits a pair of DTEs to communicate through a bilateral agreement, but excludes communication with all other DTEs.
    - **OUTGOING:** Permits a DTE to pertain to one or more CUGs and originate virtual calls destined to a DTE located in the open part of the network (i.e. DTEs that do not pertain to other CUGs) and to DTEs pertaining to other CUGs with NORMAL type (or incoming).
  - **Number:** CUG identifier.
- **NUI:** Network User Identifier. This is used in the identified DTE X.32 service and is composed of 10 characters (digits and letters). This is used for invoicing facilities, network management or facility requests to those that are subscribed.

- **User's data:** This field is encoded in hexadecimal. This is the new value sent in the call packet for the NA indicated in the *X.25 address call*. Admits up to 4 bytes.

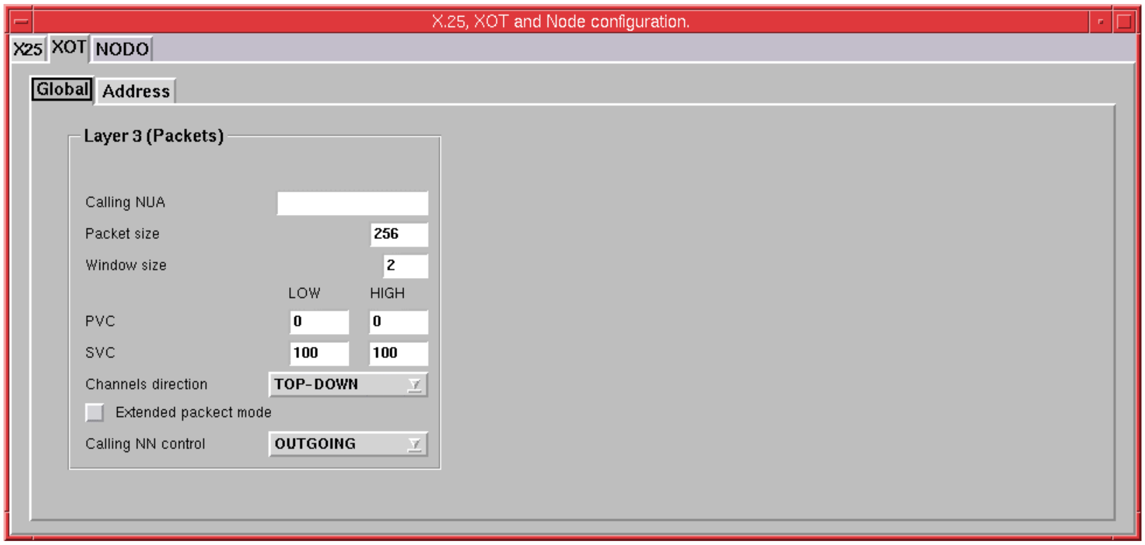
The maximum size of the table is determined by the device memory.

• *Configuring XOT (NOVACOM-X25 and C4i devices only)*

In order to configure the XOT protocol there are two screens, one with the global parameters and the other to define addresses.

Configuring Global XOT

The global parameters encompass the X.25 level 3 information.



Layer 3 (Packets)

	LOW	HIGH
Calling NUA		
Packet size		256
Window size		2
PVC	0	0
SVC	100	100
Channels direction	TOP-DOWN	
□ Extended packect mode		
Calling NN control	OUTGOING	

Figure 33: Configuring global XOT

Enable XOT: Activates the XOT configuration in the device.

LEVEL 3 (Packets)

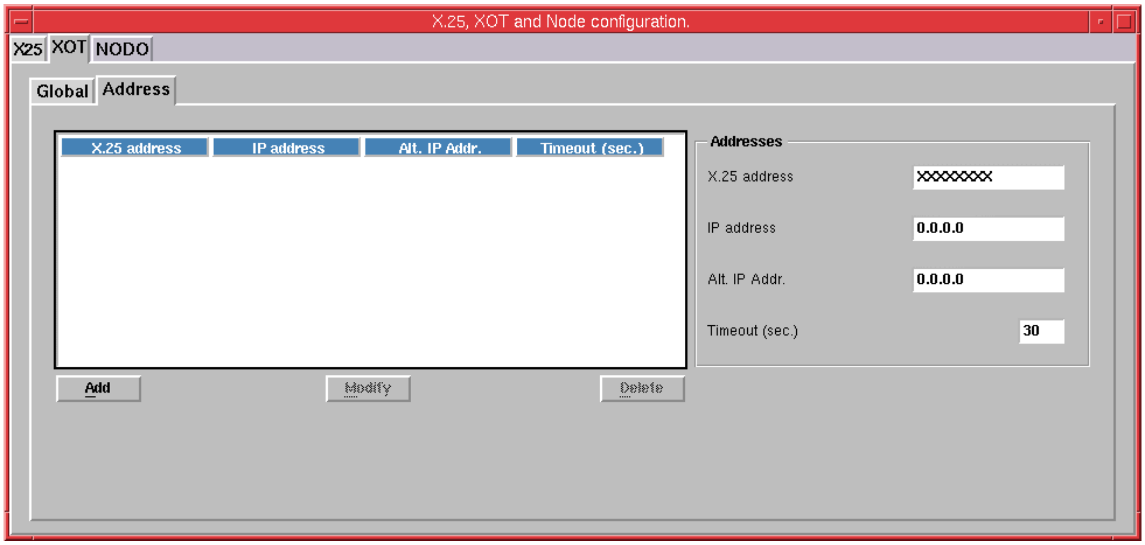
- **Calling NUA:** Indicates the X.25 address that must be used as calling address in the outgoing frames or as the called address in the incoming frames. Up to 15 digits are admitted.
- **Packet size:** This is the maximum length of the transmitted packet in octets. Values in the range **[128 .. 1024]** are admitted with **256** being the default value.
- **Windows size:** This indicates the number of sent frames pending verification. If extended packet mode is activated, the range is **[2 .. 127]** and if not **[2 .. 7]**.
- **Lowest PVC:** Number of the lowest Permanent Virtual Circuit that can be used. Values in the range **[0 .. 4096]** are admitted with **0** being the default value.
- **Highest PVC:** Number of the highest Permanent Virtual Circuit that can be used. The high PVC must be greater or equal to the low PVC. The PVC range must always be lower than the SVC range. Values in the range **[0 .. 4096]** are admitted with **0** being the default value.
- **Lowest SVC:** Number of the lowest Switched Virtual Circuit that can be used. The high PVC must be less than the low SVC. Values in the range **[0 .. 4096]** are admitted with **100** being the default value.

- **Highest SVC:** Number of the highest Switched Virtual Circuit that can be used. The highest SVC must be greater or equal to the lowest SVC that can be used. Values in the range **[0 .. 4096]** are admitted with **100** being the default value.
- **Channels direction:** Assignment order of the logical channels in the outgoing calls.
- **Extended packet mode:** This module is used to consecutively number the sent X.25 packets. If this is enabled, module 128 is used, if not, module 8.
- **Calling NN control :** Indicates if you must modify the calling NA or maintain the one that comes in the call. The following values can be taken:
  - **ADD**: Adds the NA to all the calls.
  - **SUPPRESS**: Suppresses the NA in all the calls passing through the port.
  - **OUTGOING**: Adds the NA in all the outgoing calls.
  - **INCOMING:** Adds the NA to all the incoming calls.
  - **DTE-DCE**: This depends on the interface. If it is a DCE this adds the NA to all the calls passing through the port. If it is DTE, this adds the NA to all the outgoing calls.

Configuring the XOT addresses

The address screen associates an X.25 address to an IP address. A list is presented with the associations already created and the possibility of creating new ones as well as modifying the current ones or deleting them.

- **X.25 address:** X.25 address assigned to a determined IP address. Up to 15 digits are admitted or the character “X” (wildcard).
- **IP address:** IP address (host) assigned to a determined X.25 address.
- **Alternative IP address:** Alternative host IP address for backup. If the call cannot be established with the first address within the time established in following parameter, the second is tried.
- **Timeout (sec.):** Wait time in seconds in order to establish a connection though the first IP address. If this is exceeded, the connection is tried through the alternative IP address. Values in the range **[0 .. 1000]** are admitted with **30** being the default value, which means that the backup is not activated.



X.25 address	IP address	Alt. IP Addr.	Timeout (sec.)

Addresses

X.25 address: XXXXXXXX

IP address: 0.0.0.0

Alt. IP Addr.: 0.0.0.0

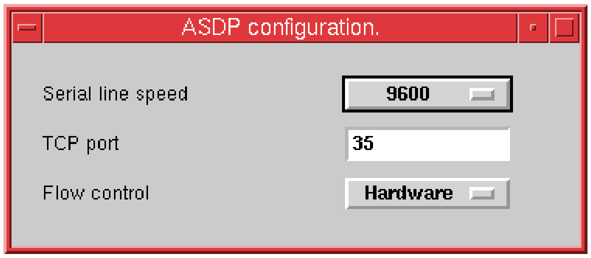
Timeout (sec.): 30

Figure 34: Configuring XOT addresses

• *Configuring ASDP (C4I devices only)*

The ASDP (Asynchronous Serial Device Proxy) configuration screen is activated by pressing the button on the tool bar.

The following figure presents the configurable parameters for this interface.



Serial line speed: 9600

TCP port: 35

Flow control: Hardware

Figure 35: Configuring ASDP

- **Serial line speed:** This specifies the speed in bits per second, which communicates the router and the printer connected to this line. The value range of this field is between **300** and **57600** bits per second.
- **TCP port:** TCP communication port established between the router and the remote device.
- **Flow control:** In many cases the router is able to send data to the serial device at a higher rhythm than this is able to support. For this reason, with this parameter you establish a mechanism in order to regulate the rhythm of the data flow between both.

m) DHCP

The C2 router has three operation modes with respect to the DHCP protocol (Dynamic Host Configuration Protocol):

DISABLED The router does not provide DHCP service.

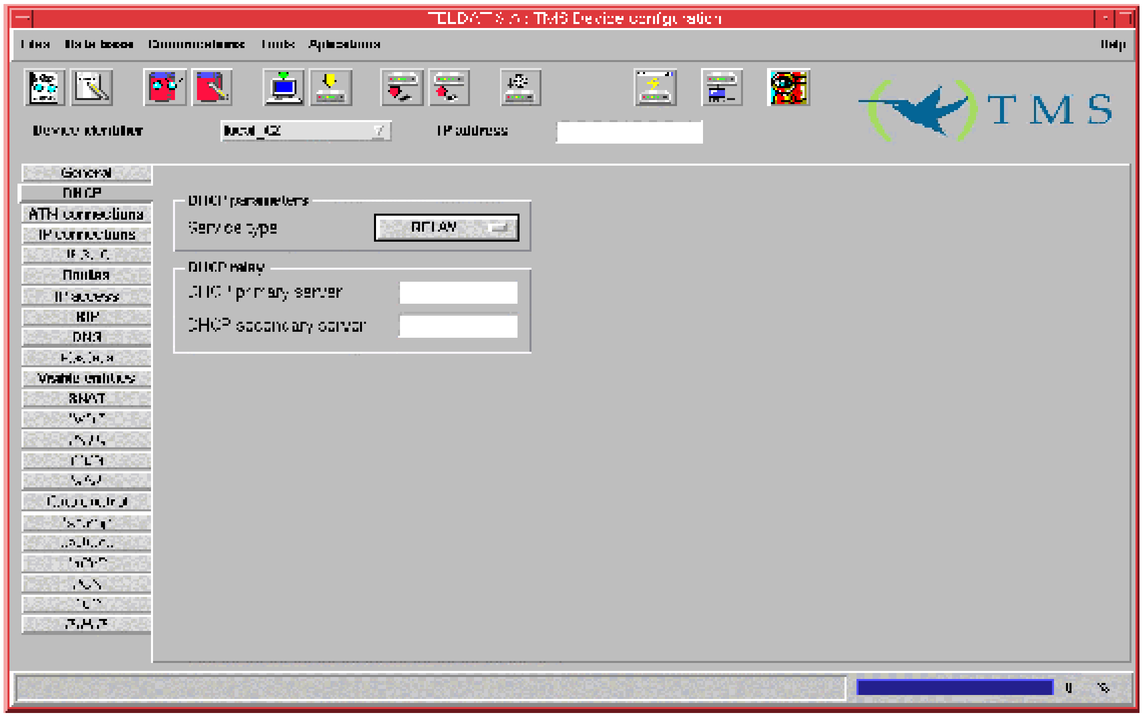
REPEATER The Router re-transmits the client DHCP protocol packets to a main DHCP server and, optionally, to a secondary server.

SERVER The router behaves as a DHCP server responding to the client petitions.

• Configuring DHCPas a repeater

As a DHCP repeater, the router resends the client DHCP packets to the server(s) that you have configured.

You must introduce the primary server IP address and optionally a secondary server. If there are two configured, the router will resend the packets to both.



DHCP parameters

Service type: RELAY

DHCP relay

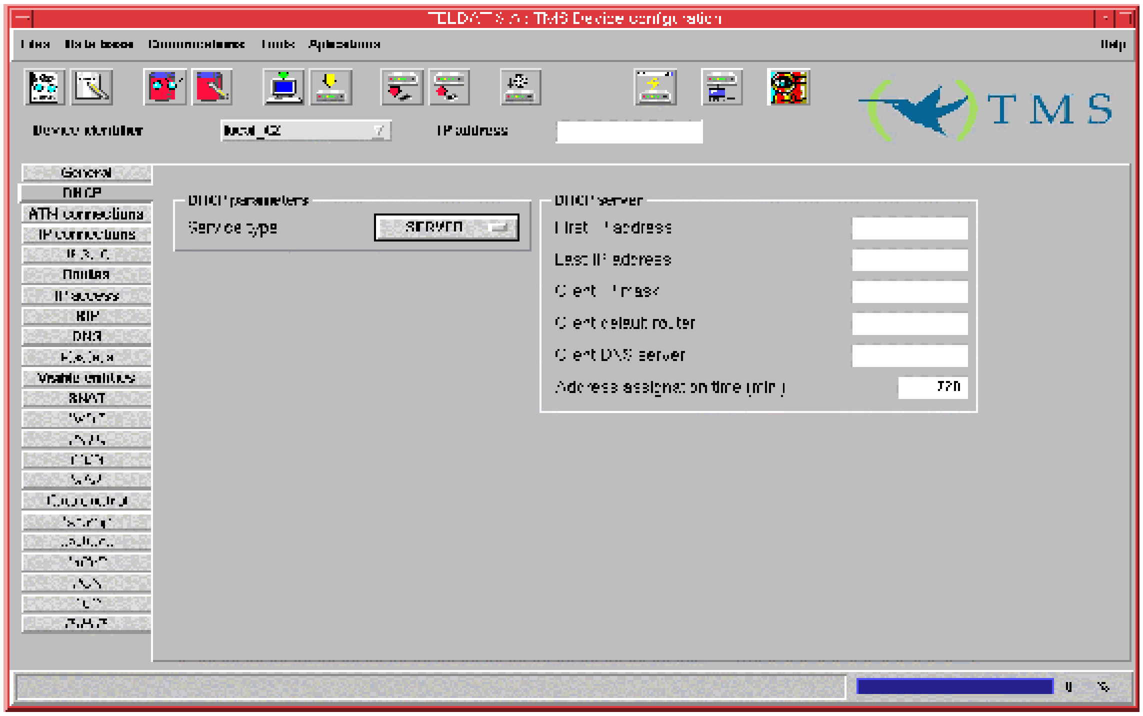
DHCP primary server

DHCP secondary server

Figure 36: Configuring the DHCP repeater

• Configuring DHCP as a server

As a server, the router attends the client DHCP requests.



Device identifier: local_42
IP address:

DHCP parameters
Service type: SERVER

DHCP server
First IP address:
Last IP address:
Client IP mask:
Client default router:
Client DNS server:
Address assignation time (min.): 720

Figure 37: Configuring as DHCP server

The configurable parameters are as follows:

First IP address: The router has a range of IP addresses available to assign to the customers. This is the first IP address in the range. Within this range, the device can differentiate its own IP address, the router's address by default and that of the DNS server so these are not assigned.

Last IP address: This is the highest limit of the range of address that can be assigned by the router. It is very important that the first IP address is not higher than the last address in the range; the application will convert to binary and verify that this does not occur.

Client IP mask: This is the IP mask assigned to the DHCP customer, together with the address.

Client default router: This is the default router that will be configured to the DHCP customer.

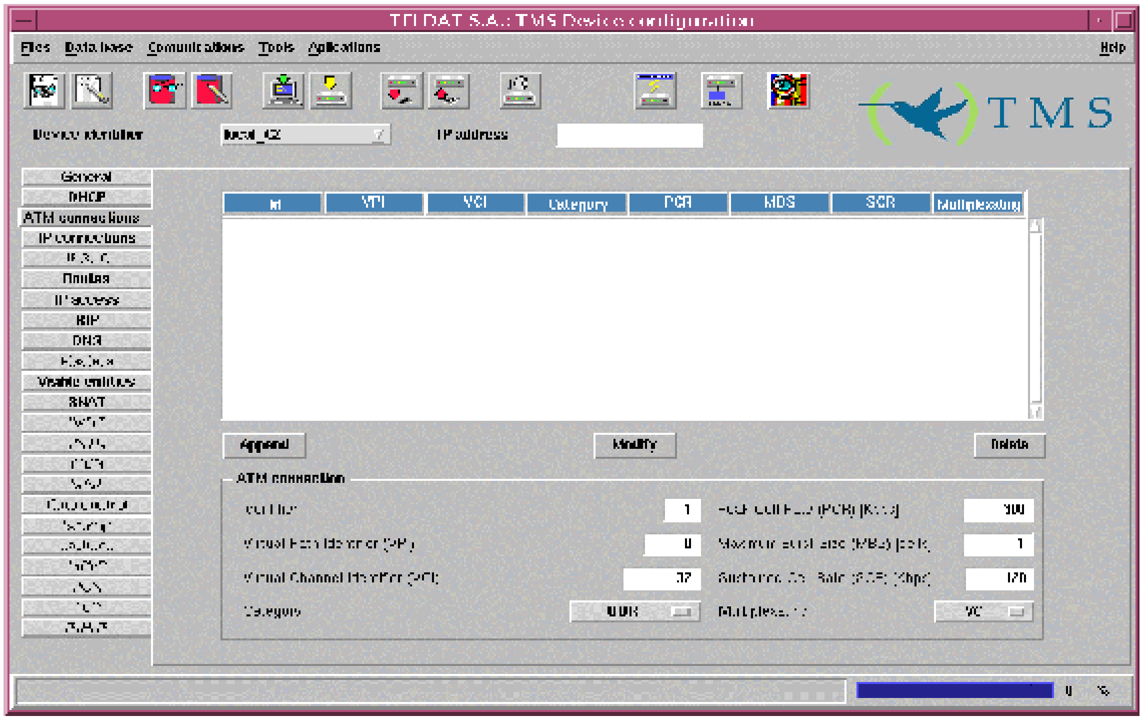
Client DNS server: This is the DNS server that will be configured to the DHCP customer.

Address assignation time [min.]: This is the time, in minutes that the server will maintain an address assigned if the customer does not request its renewal. After this time has lapsed, the address can be reassigned to another customer who requests it. The admitted values in this range are [1 .. 525600] minutes. The default value is 720.

Optionally the most extended operation is the simplest configuration, i.e. that where the router is installed in a small LAN needing access to INTERNET and is configured as a DHCP server, configuring this as a default router and DNS server. In this way when any LAN station is started up, it requests an IP address and its configuration. Once this is received the station will be ready to browse through INTERNET.

n) ATM connections

The ATM (Asynchronous Transfer Mode) connections are the lowest level entity configured from the management. Over these you define the IP connections and from this the rest of the router configuration entities.



ATM connection

Identifier	1	Peak Cell Rate (PCR) [Kbps]	300
Virtual Path Identifier (VPI)	0	Maximum burst size (MBS) [cells]	1
Virtual Channel Identifier (VCI)	32	Sustained Cell Rate (SCR) [Kbps]	170
Category	UBR	Multiplexing	VC

Figure 38: Configuring ATM connections

The configurable parameters are as follows:

- **Identifier:** This is the ATM connection identifier. This is an integer pertaining to the **[1 .. 99]** range and cannot be repeated.

- **Virtual Path Identifier (VPI):** ATM virtual route identifier. This identifier together with the VCI provides the path information. This is an integer within the range **[0 .. 255]**. The binomial VPI/VCI cannot be repeated.

- **Virtual Channel Identifier (VCI):** This is the ATM's virtual channel identifier. The ITU-T (International Telecommunication Union) defines a "virtual channel" as a unidirectional transport of cells between two nodes associated to a common VCI; i.e. each VCI identifies a distinct connection between two ends. This is an integer within the range **[32 .. 65535].** The binomial VPI/VCI cannot be repeated.

- **Category:** This section describes the different ATM service categories (known as ATM Forum) or the ATM transference capacities (known as ITU-T).

  These can take the values **CBR, VBR_RT, VBR_NRT** or **UBR**. The default value is **UBR**.

  1. Variable Bit Rate (VBR): Also known as Statistical Bit Rate (SBR). The VBR service is characterized by providing two speeds, being adequate for traffic whose speed requirements have variations in time. There are two defined types, one for real time applications (VBR_RT) (with restrictions in the delay and its variation), such as voice with silence suppression and compressed video, and the other is (VBR_NRT) for applications with burst transmission but without delay restrictions. The configurable parameters are the peak speed (PCR or Peak Cell Rate), the sustained speed (SCR or Sustained Cell Rate) and the maximum burst size (MBS or Maximum Burst Size). These determine that after a long period of silence, the device can transmit a determined time to PCR (this time is determined by the PCR, the SCR and the MBS), in order to subsequently transmit to SCR; during the periods of silence, the device earns "credit", so when it is required to transmit, it can once more transmit a determined time to PCR.

  2. Constant Bit Rate (CBR): Also known as Deterministic Bit Rate (DBR). The CBR service is characterized by providing a constant configured speed value, whatever the ATM network congestion conditions are, i.e. a guaranteed rate is offered, in such a way that the network resources are used even when there is no information available to transmit. A conventional circuit can be understood as where a portion of the physical medium capacity is taken and this remains permanently assigned to the said communication. As a configurable parameter there is the circuit speed, represented by the PCR or Peak Cell Rate. This type of service is aimed towards real time applications i.e. those requiring delays and variations in the said low delay, such as voice, video and circuit emulations.

  3. Unspecified Bit Rate (UBR): The UBR service is a service known as "best effort", aimed at applications that do not have delay restrictions or variations of this. Nor do they require determined quality of service parameters, which reduces the contract costs. This is focused on applications that generate non-continuous traffic bursts thus permitting a high grade of static multiplexing. The UBR service normally has a single configurable parameter, the PCR, which determines that the speed should never surpass the circuit using this service. Typical applications are data transference, message services, etc.

- **Peak Cell Rate (PCR):** This determines the maximum binary rate at which transmission to the connection is permitted. The permitted values in the range are **[1 .. 8192]** Kbps. The default value is **300** Kbps.

- **Maximum Burst Size (MBS):** This determines the maximum burst (MBS) size (in cells) permitted for PCR before passing to transmit to SCR. This parameter is only requested if the traffic category is VBR_RT or VBR_NRT. Values higher than 0 are admitted. The default value is **1** cell.

- **Sustained Cell Rate (SCR):** This determines the binary rate that permits carrying out continuous transmission. This parameter is only requested if the traffic category is VBR_RT or VBR_NRT. The admitted values in the range are **[1 .. 8192]** Kbps, however the value must never be higher than the PCR parameter. The default value is **128** kbps.

- **Multiplexating:** There are two types of multiplexing:

  1. Virtual Circuit (VC): Each higher-level traffic type is transported in a different connection without adding any type of header.

  2. Logic Link Control (LLC): Diverse types of high-level traffic share the same connection to transport their data, inserting an LLC header to indicate the type of traffic contained in the said frame.

> ***The maximum number of ATM connections that can be defined is 5.***

To add a connection, fill out the fields and press **Add**.

In order to modify a connection, select it from the list, modify the corresponding fields and press **Modify**.

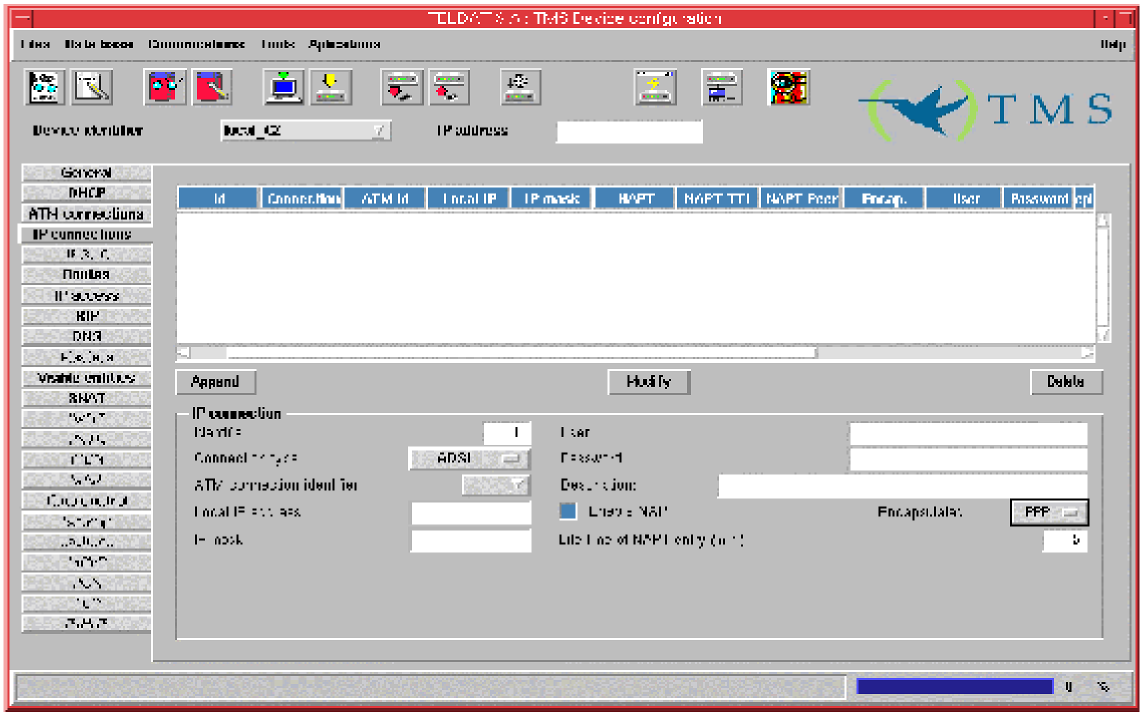
To delete an ATM connection, select it from the list and press **Delete**.

> ***Deleting ATM connections.***
>
> ***You cannot delete an ATM connection that an IP connection depends on. In order to delete the connection you must first delete the IP connection depending on this.***

o) IP connections

IP connections are supported over ATM connections, which in turn supports the rest of the configuration entities.

Depending on the type of connection, encapsulation and the device model enable distinct configuration parameters.



Identifier: 1

Connection type: ADSL

ATM connection identifier

☑ Enable NAPT

Encapsulation: PPP

Life time of NAPT entry: 5

Figure 39: IP connections with ADSL type

These are composed of the following parameters:

- **Identifier:** IP connection identifier. This is an integer in the **[1 .. 99]** range that cannot be repeated.

- **ATM connection identifier:** This is the ATM connection identifier over which it is maintained. You can only select the identifiers defined in the ATM connections screen.

- **Local IP address:** This deals with a subnet or host address. All of the packets directed to any IP address in this range are routed through this IP connection as long as there does not exist a more restrictive route in the route table, in which case the packets are sent in agreement with this route.

- **IP mask:** Together with the previous IP address, this defines the range of addresses associated to the IP connection.

- **Encapsulation:** With the PPP option, the entries for the user and password are shown.

- **User:** User identifier in connections with encapsulated PPP.

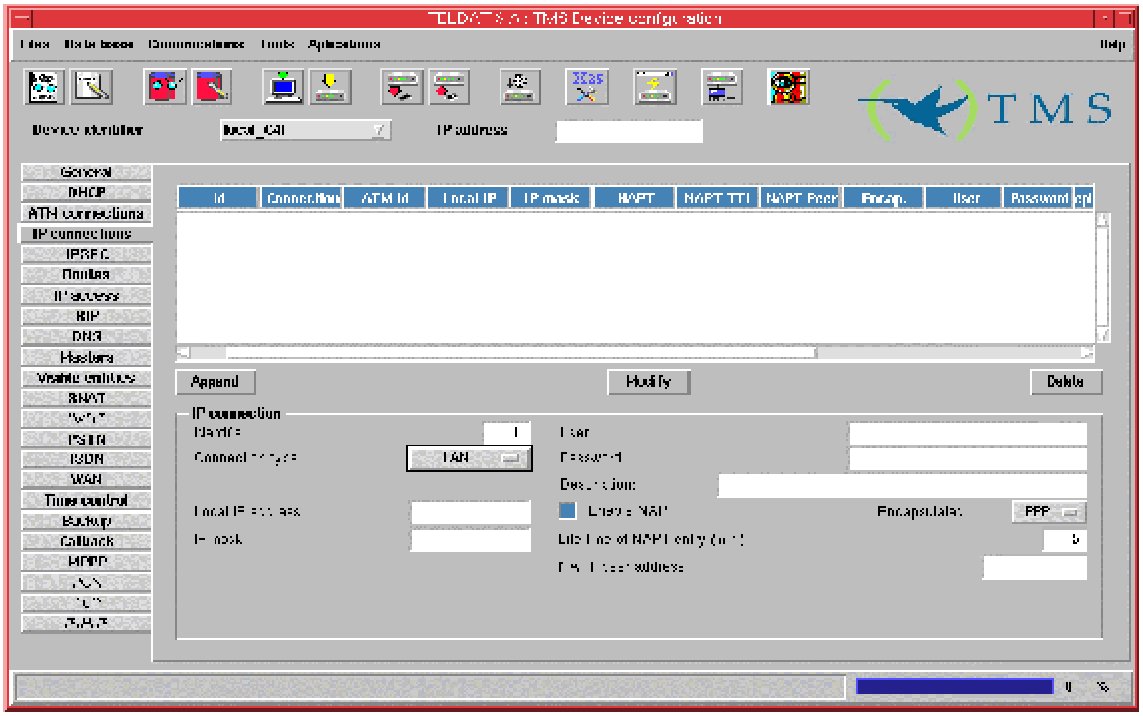
- **Password:** Previous user password in connections with encapsulated PPP.

- **Enable NAPT:** Enables or disables the NAT in the connection ports.

- **Life time NAPT entry:** When the NAT is enabled the time that each entry is maintained is indicated in minutes before discarding it. The values admitted in the range are **[1 .. 240]** minutes. The default value is **5**.

- **Description:** Information string up to 79 characters.

A LAN connection and encapsulated PPP have been selected in the following screen .



Device identifier: local_C4I

IP address

Id	Connection	ATM Id	Local IP	IP mask	NAPT	NAPT TTL	NAPT Peer	Encap.	User	Password

IP connection

Identifier: 1

Connection type: LAN

Local IP address:

IP mask:

User:

Password:

Description:

□ Enable NAT

Encapsulation: PPP

Life time of NAPT entry (min): 5

NAPT peer address:

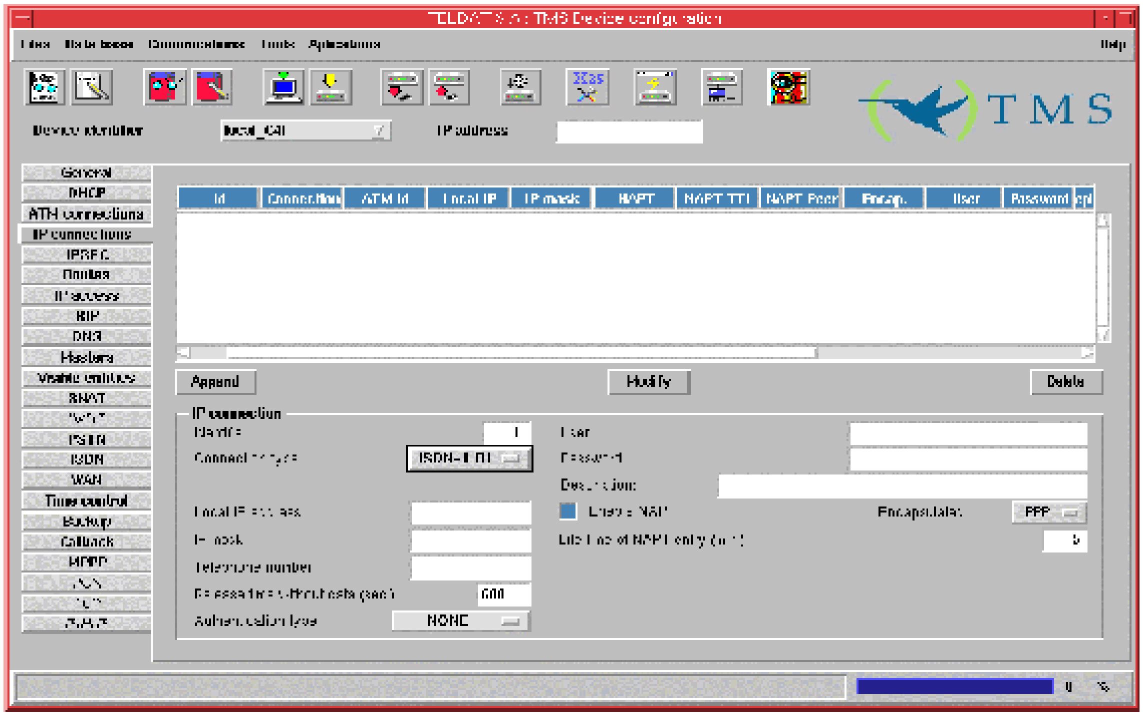
Figure 40: IP connections with LAN type and PPP

- **User:** User identifier in connections.

- **Pasword:** Previous user password in connections.

- **NAPT peer address:** Device public address for external users when NAT is enabled.

When a C3 with PSTN or ISDN connection is selected, the aspect of the screen is as follows:



Identifier: 1
Connection type: ISDN-[illegible]
Local IP address:
IP mask:
Telephone number:
Release time without data (sec.): 600
Authentication type: NONE
User:
Password:
Description:
■ Enable NAPT
Encapsulation: PPP
Life time of NAPT entry (min): 5

Figure 41: IP Connections with PSTN type and PPP

Telephone number: This is the telephone number through which the device demands the connection via ISDN. In order to minimize the costs of the calls, you should use the telephone number of the Access Node nearest the device. A maximum of 19 digits is admitted.

Release time without data (sec.): Connections through ISDN normally terminate due to absence of data on the line at a time equal or superior to release time without data. The default value is 600 seconds. We do not recommend that you use very low times. The timer is configured at T/10, T being the release time without data. Values within the range [0, 60 .. 65535] are admitted. The value 0 is a special case which is equivalent to a permanent connection. This value is used for example as a means of uniting subnets. If there is a timetable control established and the release time without data is 0, the device establishes connection as soon as the access period commences. In this way, during the said period, the client can communicate with his subnets. If there are no timetable restrictions and the value 0 is assigned, a permanent connection is established after startup.

Authentication type: Normally on accessing an external network, it is the network itself that requests the access device to authenticate before the latter can use the network. However, in point-to-point scenarios where it is not an external network being accessed but a known remote network through an also known remote device, it is possible to indicate to the remote end that it must authenticate itself. The device supports the PPP authentication protocols **Password Authentication Protocol (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**.

A maximum of 10 IP connections are admitted.

To add a connection, fill out the fields and press **Add**.

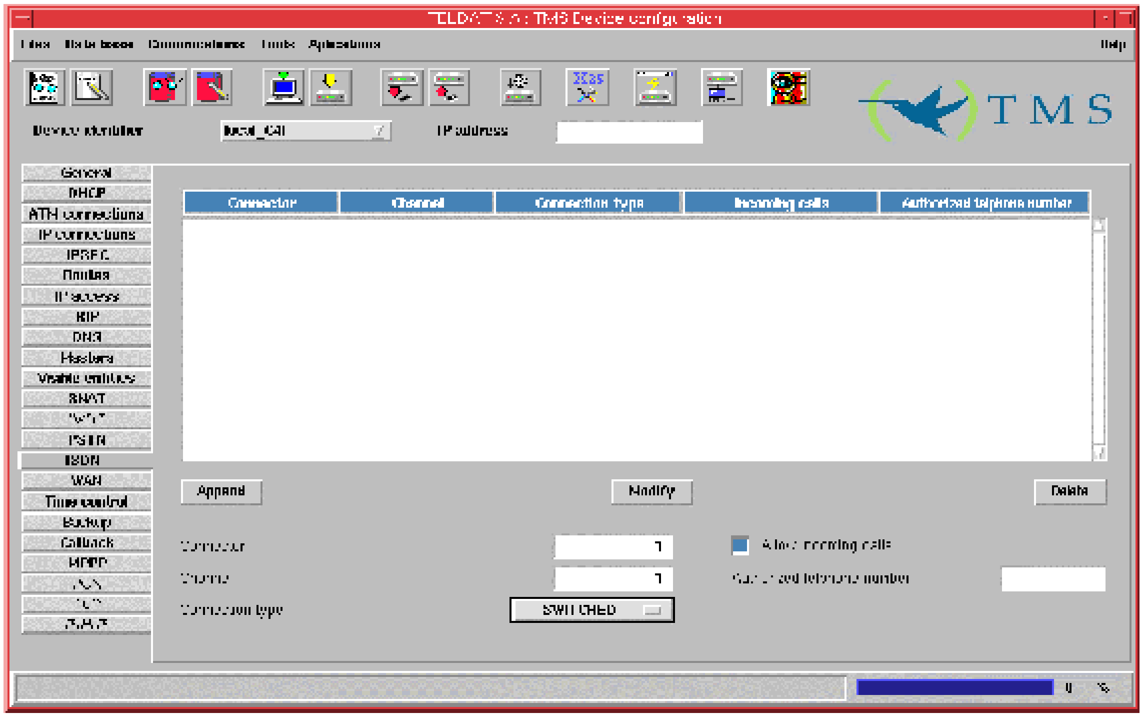
To modify a connection, select it from the list, modify the corresponding fields and press **Modify**.

To delete an IP connection, select it from the list and press **Delete**.

> ***Deleting IP connections.***
>
> ***You cannot delete an IP connection that is being used by any other entity, such as a route, visible port, visible subnet, etc. You must first delete all the associated entities.***

p) ISDN

There is a configuration screen for the ISDN B channels that the device has available:



Connector	Channel	Connection type	Incoming calls	Authorized telephone number

Device identifier: local_C41

Connector: 1

Channel: 1

Connection type: SWITCHED

■ Allow incoming calls

Authorized telephone number:

Figure 42: Configuring ISDN channels

- **Connector:** ISDN line to which the corresponding B channel is associated.

- **Channel:** B channel associated to a determined ISDN line.

- **Connection type:** This indicates the type of connection established in the channel. If the user has a permanent ISDN B channel contracted from the supplier, this should be indicated through this parameter. A permanent B channel is a special ISDN B channel that does not use signaling as its destination is set in the service contract. This B channel does not carry out ISDN calls and is always connected. If you enable a B channel as **PERMANENT**, the connection destination telephone parameters, release time due to absence of data and the permitted connection interval are hidden. The permanent B channel contract specifies which B channel (B1, B2 or both) responds to this profile. Both channels cannot have permanent connection, as the device in this case cannot be managed. The default value is **SWITCHED**.

- **Allow incoming calls:** As an access device, it is the device itself that carries out the call to the external network supplier to which you wish to connect. However in connection scenarios between two devices, one makes the call while the other receives it. If you wish the device to be able to receive incoming calls, you have to enable this parameter. By default, the device does not permit incoming calls.

- **Authorized telephone number:** If the incoming calls are enabled, this parameter indicates the ISDN number authorized for connection. If there is no value configured here then any caller is authorized to connect although it must be authenticated through PAP or CHAP if this is indicated. The default value (empty) for this parameter is to authorize any calling number.

To add a new channel to the list, fill out the fields and press **Append**.

In order to modify a channel in the list, select it, modify the corresponding fields and press **Modify**.

In the case of the **Delete** option, the selected element is deleted.

A maximum of two ISDN lines with two B channels for each is admitted.

q) Connection intervals

This serves to restrict traffic though each IP connection to a temporary interval certain days of the week or to force the device connection in the said interval.

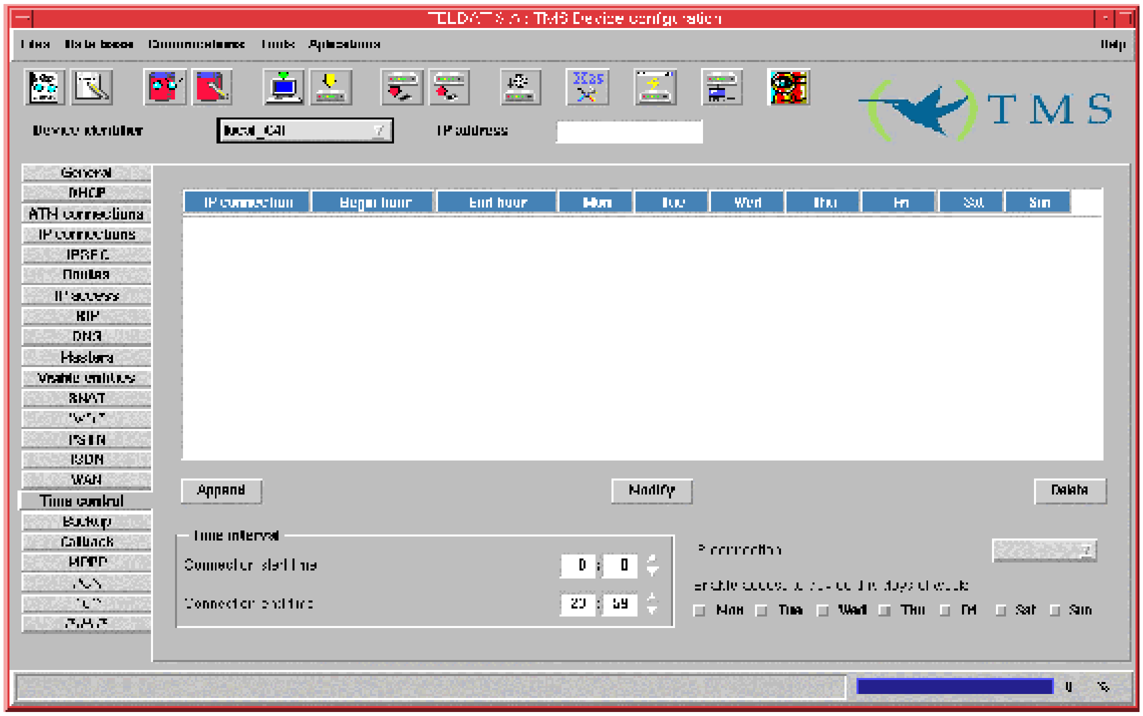
The connection interval specifies the period where the chosen IP connection is operative. Outside of this interval the connection is blocked except for management connections, which are always guaranteed.

Select the IP connection.

Select the days of the week where the device operates normally.

Introduce the start and the end instant for the interval in an **hh:mm** format. For the hour, admitted values within the interval are [0 to 23] and for the minutes [0 to 59]. If the end time is inferior to the start then this is considered as pertaining to the next day. If connection is not permitted the following day, the day takes priority over the time and the connection is disabled for that day.

When the release time without data is 0, the device automatically connects when the temporary interval established in the timetable configuration begins.



Connection start time 0 : 0

Connection end time 23 : 59

Figure 43: Configuring the connection intervals

To add a new interval to the list, fill out the fields and press **Append**.

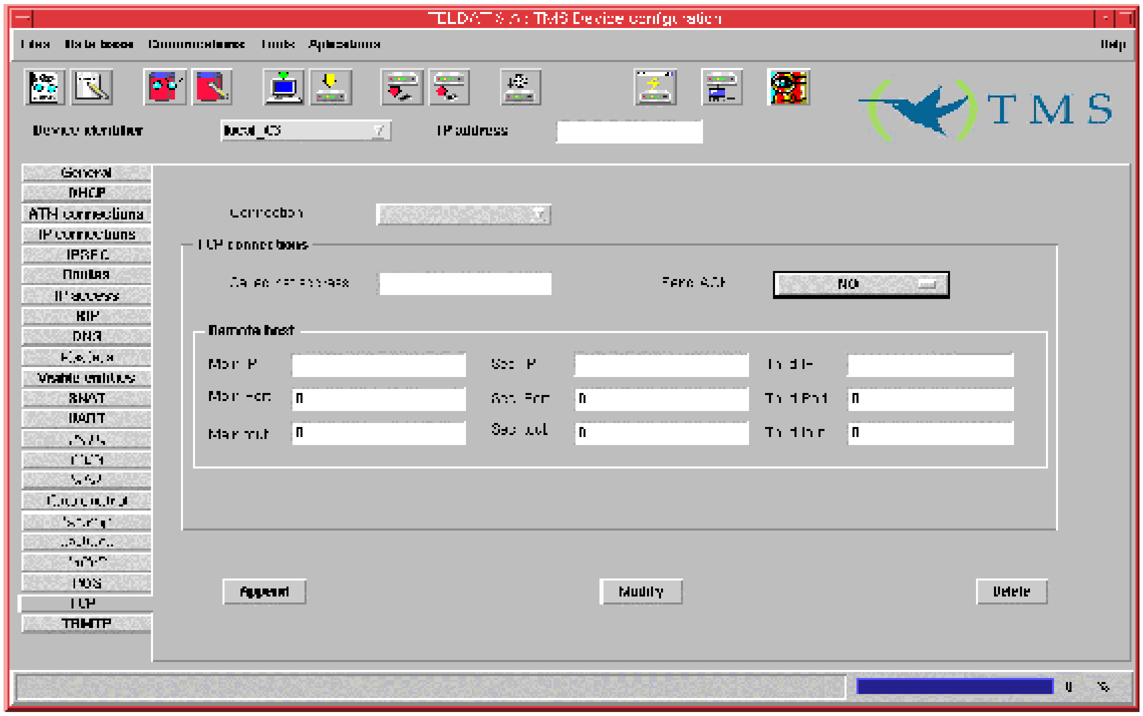
In order to modify an interval in the list, select it, modify the corresponding fields and press **Modify**.

In the case of the **Delete** option, the selected element is deleted.

Up to a maximum of 10 connection intervals are admitted.

r) TCP

In this screen you configure the different TCP connections the router will have available.



Device identifier: local_C3
IP address:
Connection:
TCP connections
Called net address:
Send ACK: NO
Remote host
Main IP: | Sec. IP: | Third IP:
Main Port: 0 | Sec. Port: 0 | Third Port: 0
Main tout: 0 | Sec. tout: 0 | Third tout: 0

Figure 44: Configuring the TCP connections.

The different parameters that can be configured from this screen are:

- **Called net address:** This parameter permits you to configure the IP address that the router calls. Any address is considered valid up to 15 characters, permitting you to also introduce the X character. The default address, therefore the void address, is XXXXXXXXXXXXXXX.

The remaining parameters are used to configure remote hosts addresses, ports and the timers:

- **IP address:** This represents the IP address of each of the three remote hosts that can be configured.

- **Remote port:** This represents the port of each of the three remote hosts that can be configured.

- **Response Time out:** This represents the wait time until a response from each of the remote hosts that can be configured is obtained. This is measured in seconds. The permitted values are between 0 and 100.

To add a connection, fill out the fields and press **Append.**

In order to modify a connection in the list, select it from the pull down list, modify the corresponding fields and press the **Modify** button.

To delete a TCP connection, select it from the list and press the **Delete** button.

s) TRMTP

Through this screen you can configure all the TRMTP connection parameters from the router. In order to simplify the configuration for each connection, each of the three hosts that can be configured may be selected in a pull up list and configured separately.

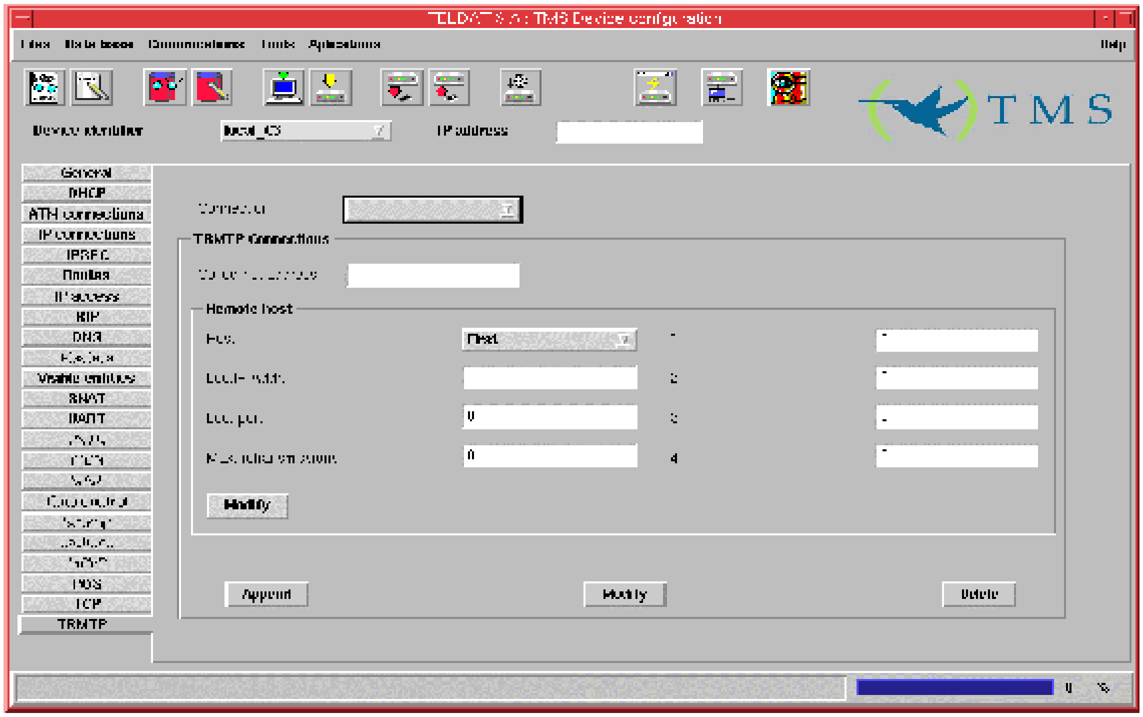


Figure 45: Configuring TRMTP connections

The parameters that can be configured from this screen are:

- **Called net address**: This is the IP address the router will call.

For each of the three configurable hosts:

- **Loc. IP Addr.**: This is the IP address of the host that is being configured.

- **Loc. Port**: This is the port of each of the hosts to be configured.

- **Max. retransmissions**: This is the number of times you wish the remote host to retransmit. Its value is between zero and 65535 retransmissions, 3 being the default value.

- **T1 timer**: This is the wait time for a confirmation before retransmission. Its value is between 1 second and 65535, 10 being the default value.

- **T2 timer**: This is the wait time before exiting an error state in the transmitter. Its value is between 1 second and 65535, 40 being the default value.

- **T3 timer**: This is the inactivity time before exiting the data state in the transmitter. Its value is between 1 second and 65535, 30 being the default value.

- **T4 timer**: This is the inactivity time before returning to the OFF state. Its value is between 1 second and 65535, 100 seconds being the established default value.

To add a connection, fill out the fields and press **Append**.

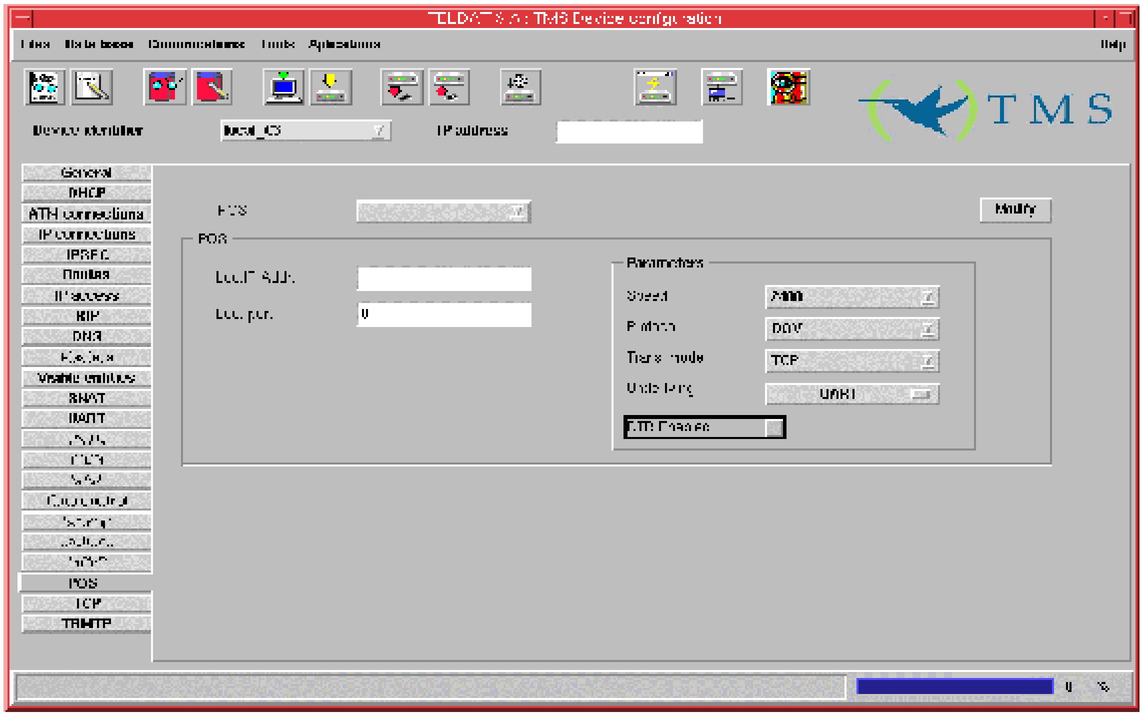
To modify a connection, select it from the pull up list, modify the corresponding fields and press general **Modification**.

To delete a TRMPT connection, select it from the list and press **Delete**.

To modify a host, select it from the pull up list, fill out the fields and press the remote host **Modify** button.

t) ***POS***

In this screen you configure the general POS parameters. The maximum number of terminals will be four in the case of C3 devices and only one for the C3G devices.



Device identifier: local_C3
IP address:
POS:
Local IP Addr.:
Local port: 0
Speed: 2400
Parity: ODD
Trans mode: TCP
Underlying: UART

Figure 46: Configuring POS

The different parameters that can be configured for each of the POSs from this screen are as follows:

- **Loc. IP Addr.**: The terminal IP address is only significant if you choose the TCP protocol. In any other case, this value is ignored.

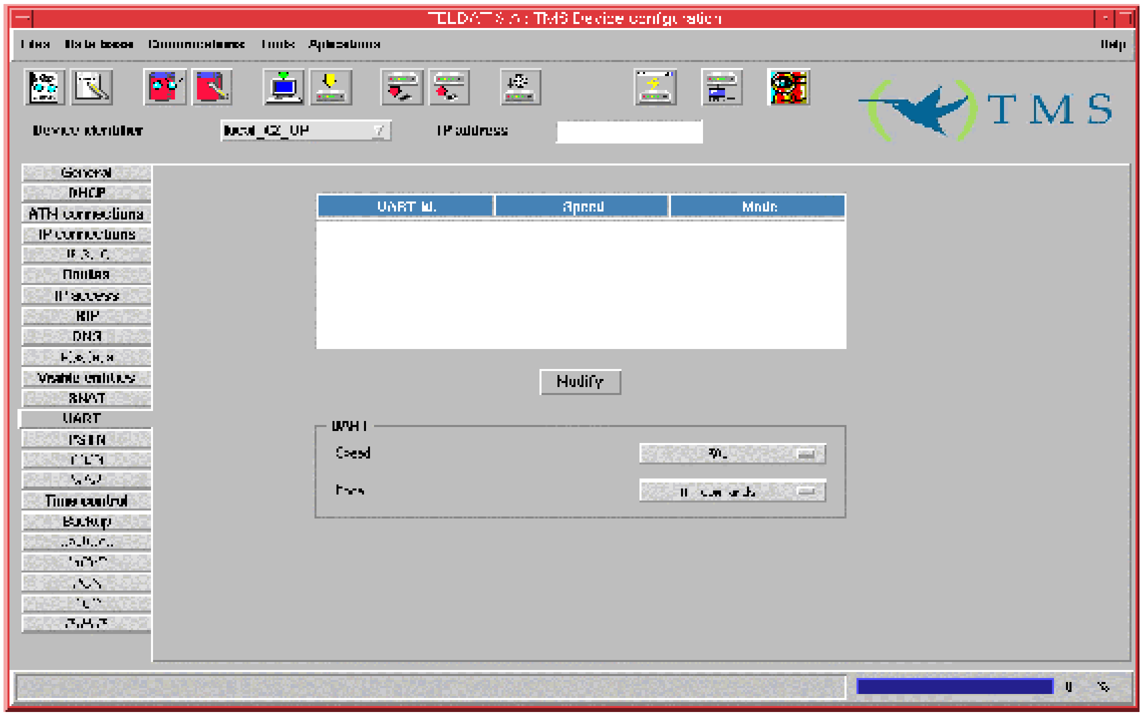
- **Loc. port**: The Local port is only significant if you choose the TRMTP protocol. In any other case, this value is ignored.

- **Speed:** This indicates the terminal speed measured in bits per second. It should be between 300 and 64000. The default value will be 2400.

- **Protocol:** The protocol used for the transmission can be chosen so that it will be DOV, DAT or VISANET.

- **Trans. mode:** The transmission mode can be chosen so that is will be TCP or TRMTP.

u) ***UART***



Device identifier: local_42_UP

IP address

UART Id.	Speed	Mode

UART

Speed

Mode

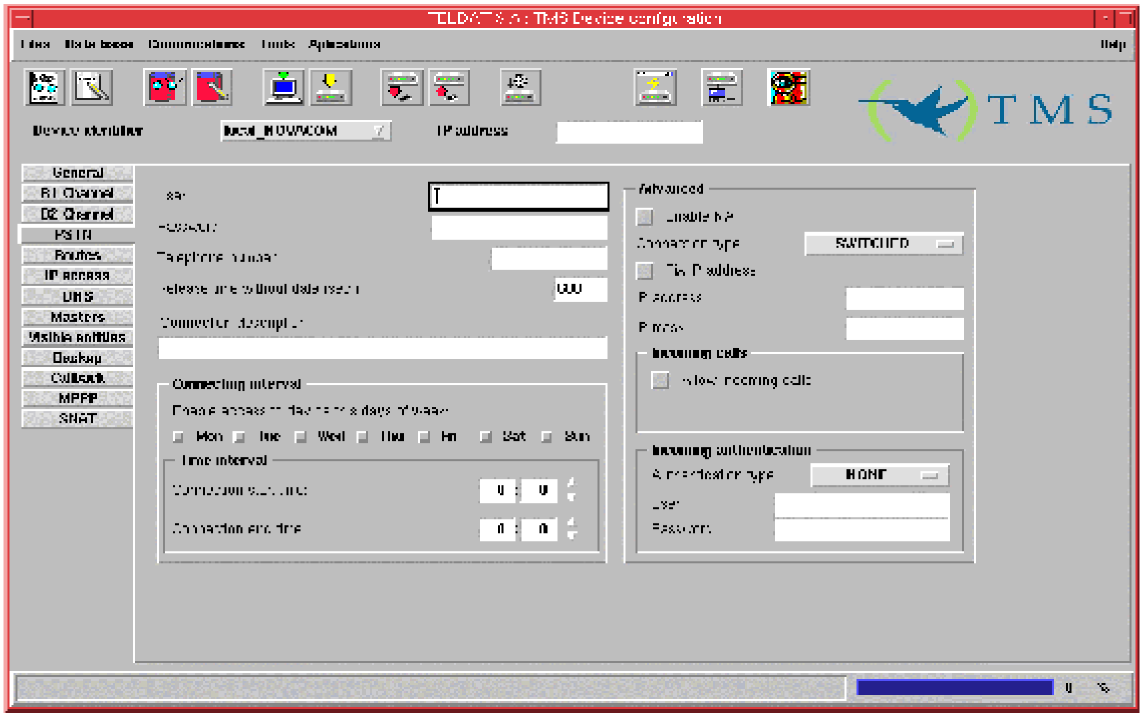
Figure 47: Configuring UART

- **Speed:** Indicates the UART port line speed.
- **Mode:** Specifies what the UART port will be used for.

v) PSTN

• NOVACOM and NOVACOM-X25 devices

Please see point B1 Channel (NOVACOM and NOVACOM-X25 devices only) for further details.



Device identifier: local_NOVACOM

IP address:

User: T

Password:

Telephone number:

Release time without data (sec.): 600

Connection description:

Connecting interval

Enable access on the following days of week

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time interval

Connection start time: 0 : 0

Connection end time: 0 : 0

Advanced

□ Enable NAT

Connection type: SWITCHED

□ Fix IP address

IP address:

IP mask:

Incoming calls

□ Allow incoming calls

Incoming authentication

Authentication type: NONE

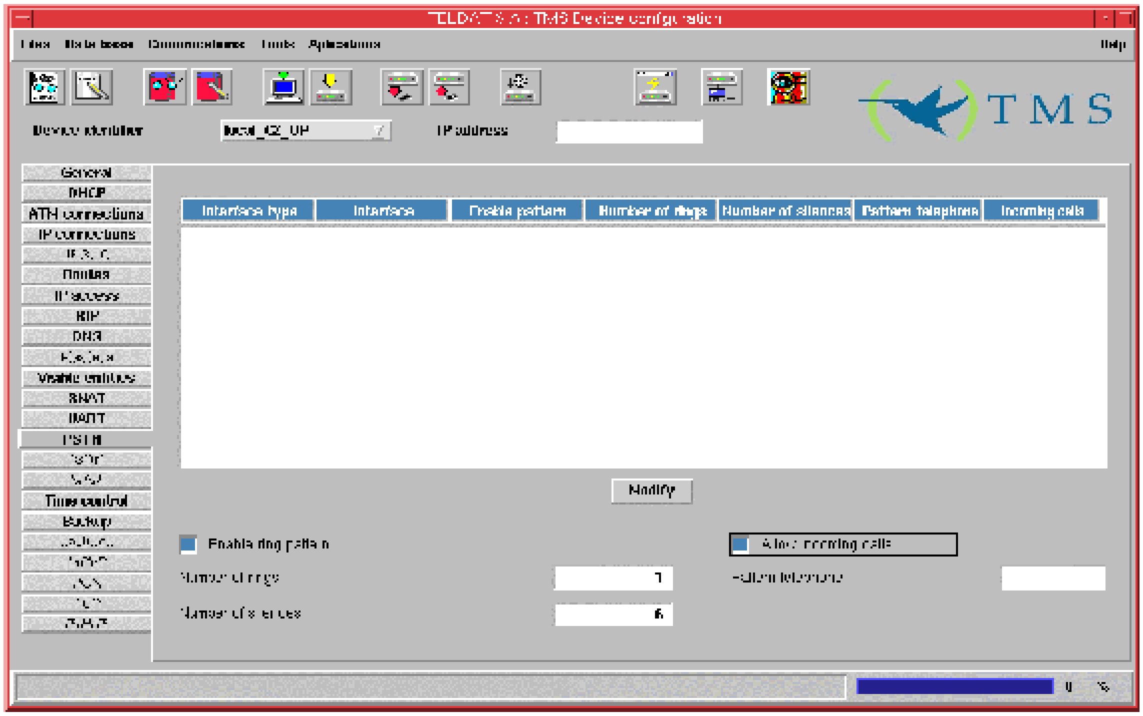
User:

Password:

Figure 48: Configuring PSTN for NOVACOM devices

• Cx devices

- **Enable ring pattern:** Permits the activation of a determined sequence in order to carry out a call via PSTN.
- **Number of rings:** Number of rings the calls pattern has configured.
- **Number of silences:** Number of silences the calls pattern has configured.
- **Allowing incoming calls:** Permits calls to be received via PSTN.
- **Pattern telephone:** Telephone number that the calls pattern is sent to.



Device identifier: local_C2_UP

IP address:

Interface type	Interface	Enable pattern	Number of rings	Number of silences	Pattern telephone	Incoming calls

■ Enable ring pattern

■ Allow incoming calls

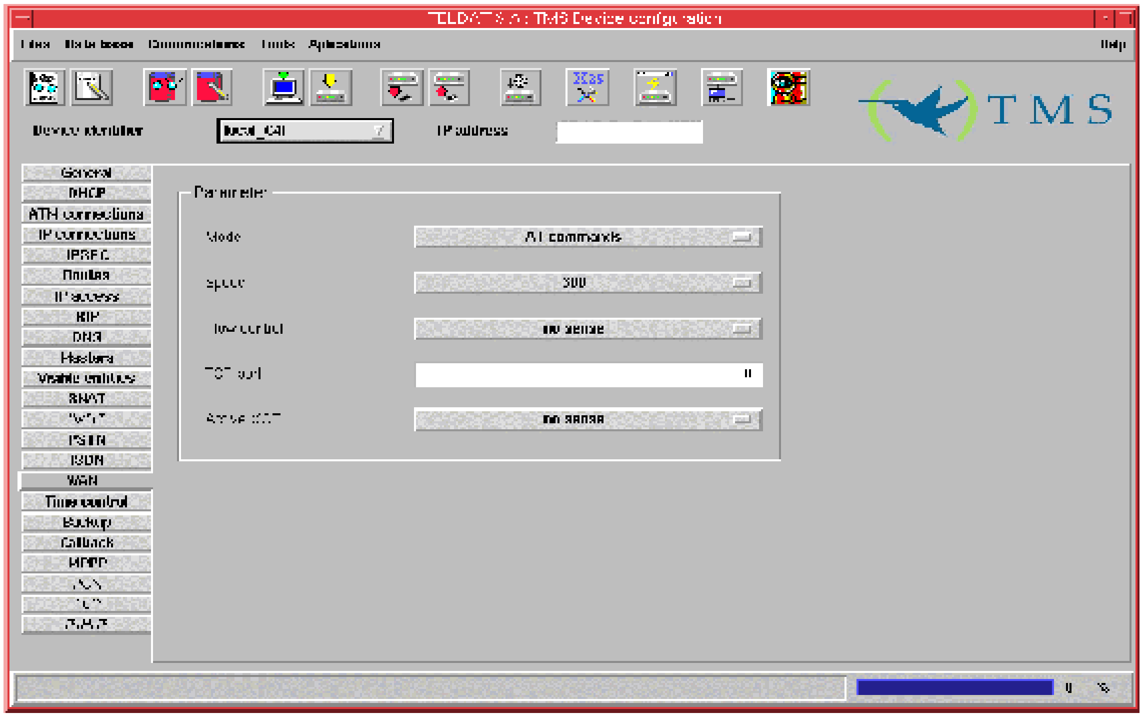
Number of rings: 1

Pattern telephone:

Number of silences: 6

Figure 49: Configurin PSTN for Cx devices

w) WAN



Device identifier: local_C4I

IP address:

Parameter

Mode: AT commands

Speed: 300

Flow control: no sense

TCP port: 0

Active DCT: no sense

Figure 50: Configuring WAN

- **Mode:** Type of WAN line operating mode.

- **Speed:** Line speed.
- **Flow control:** In cases where the line operates in ASDP mode, this indicates the type of hardware flow control.
- **TCP port:** In cases where the line operates in ASDP mode, this indicates which TCP port has communication.
- **Active XOT:** Indicates if the XOT is active when the WAN line is operating in X.25 mode.

x) IPSEC

IPSec is a security platform at the *network* level. This provides the ability to accommodate new encryption and authentication algorithms in a flexible and robust way.

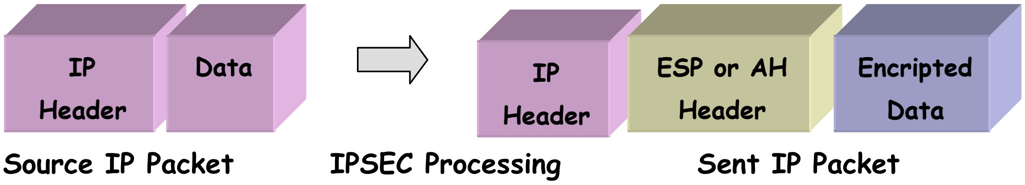
IPSec defines two distinct security services:

- **ESP:** *Encapsulating Security Payload*: provides confidentiality, address source authentication in each IP packet, integrity and protection from copies being made.
- **AH:** *Authentication Header*: provides address source authentication in each IP packet, integrity and protection against copies being made, however this does not offer data confidentiality. This service is appropriate in cases where you only need to affirm the origin of the data.

• *Tunnels*

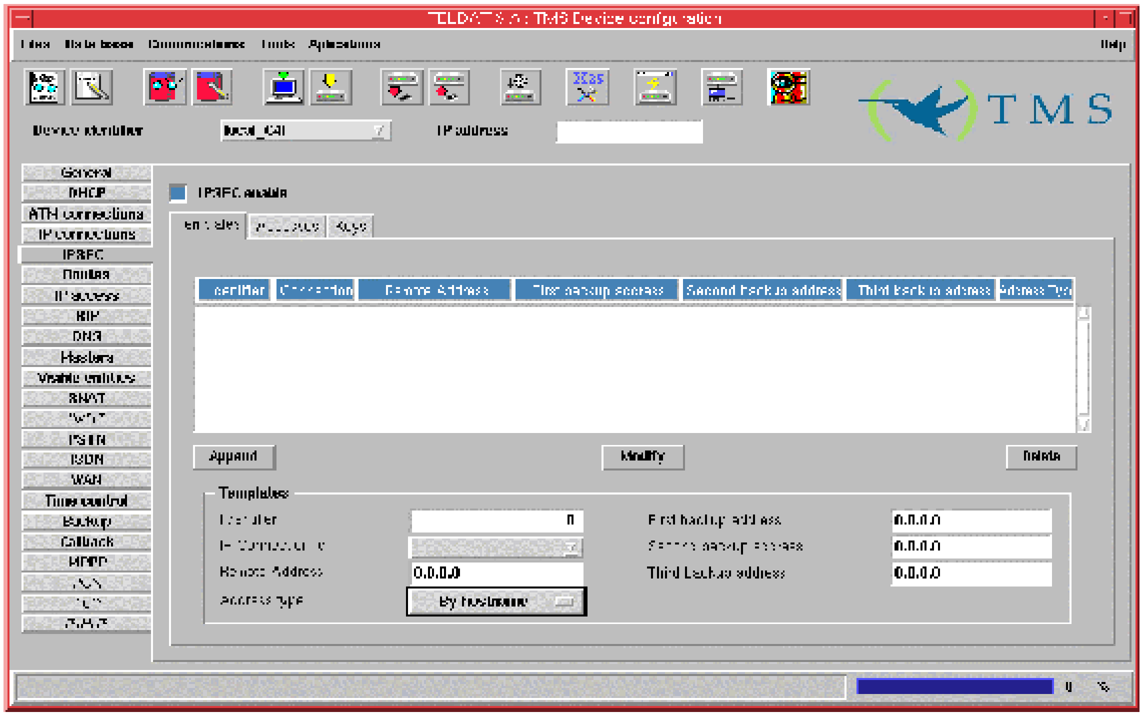
The IPSec platform permits two operation modes. You can use either of the two security services, ESP or AH, in each of them:

- The ***Transport Mode*** permits secure communications, normally established between the two hosts (e.g. communication between a workstation and a server or between two servers). However, in neither case does this mask the source or destination address of the packet to be sent. In transport mode, IPSec only acts over the IP packet internal data, without modifying the packet header. E.g. over a TCP or UDP segment or an ICMP packet.



- The IPSec ***Tunnel Mode*** encapsulates the whole of the original IP packet in a new IP packet, thus hiding all the original content. In this way the information is routed through a 'tunnel' from one point in the network to another without anyone being able to examine the content. This mode is the most appropriate one to be used in communications between a router and an external host or between two routers.

The Teldat Routers permits **IPSEC Tunnel mode** to be carried out.



Device identifier: local_C4I

IP address:

Templates

Identifier: 0

IP Connection id:

Remote Address: 0.0.0.0

Address type: By hostname

First backup address: 0.0.0.0

Second backup address: 0.0.0.0

Third backup address: 0.0.0.0

Figure 51: Configuring IPSEC Templates

- **Identifier:** Tunnel identifier.
- **IP connection identifier:** If this is set to 0, the IP connection is not defined.
- **Remote address:** remote device IP address through which the tunnel is established.
- **Address type:** Mode in which the devices at the tunnel ends are going to be identified. This can be the name of the devices or their IP addresses.
- **First backup address:** address of another remote device should the attempt to establish the tunnel through the *Remote Address* fail.
- **Second backup address:** address of another remote device should the attempt to establish the tunnel through the *Remote Address* fail.
- **Third backup address:** address of another remote device should the attempt to establish the tunnel through the *Remote Address* fail.

• *Accesses*

The IPSec platform must know which *security policies* to apply to the IP packet, depending on the header fields, also known as *selectors*. The security policies decide which encryption and authentication algorithms should be used in the secure connection.

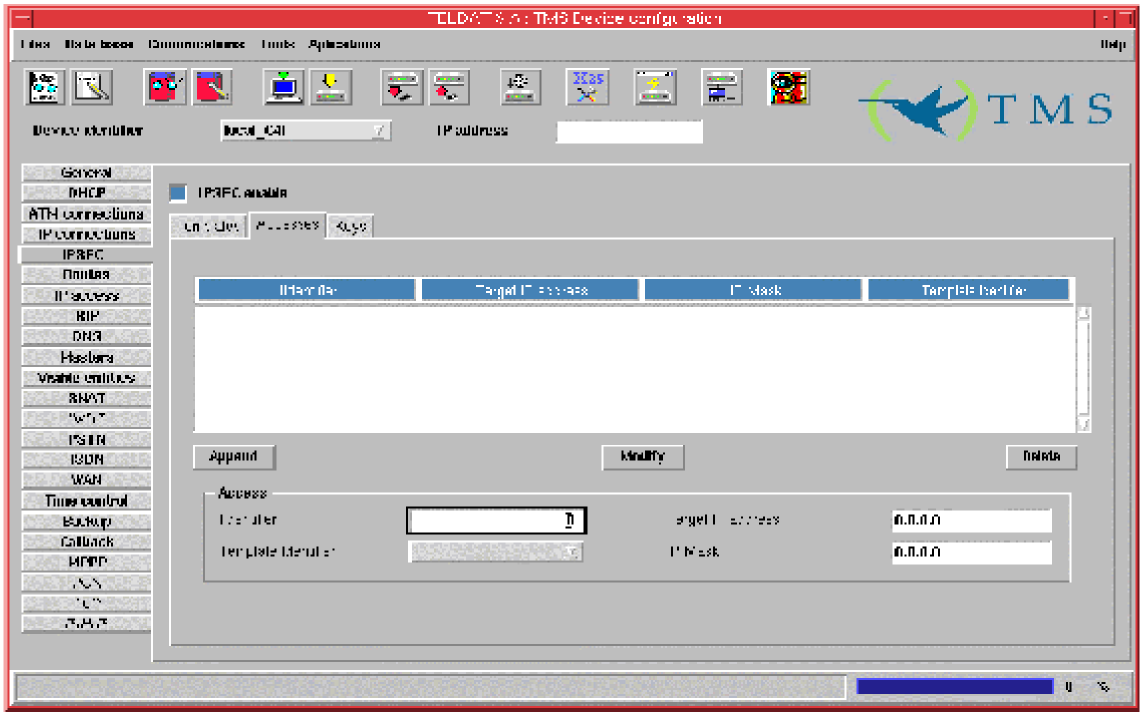
The ***Security Policy Database*** (**SPD**) stores the entries that contain the selectors and the associated security policies.

After checking the security policies database, within the policies applicable to an IP packet, three possibilities exist:

- Discard the packet
- Route the packet normally.

- Apply the IPSec Security with some determined encryption or authentication algorithms that depend on the obligations of the security-efficiency adopted. For example, if you consider the processing speed as being more important than security, choose the DES encryption policy instead of the Triple DES.

An access is an incoming and outgoing packet filter that is introduced in the access control list.



Device identifier: local_C41
IP address:

☑ IPSEC enable

Identifier	Target IP address	IP Mask	Template Identifier

Identifier: 1
Target IP address: 0.0.0.0
Template Identifier:
IP Mask: 0.0.0.0

Figure 52: Configuring IPSEC Accesses

- **Identifier: :** Identifier of the selector being defined.
- **Template Identifier:** Identifier of the tunnel through which the packets are going to be sent.
- **Target IP address:** Identifies the address or subnet that the packet is being sent to.
- **IP Mask:** Mask of the address or subnet that the packet is being sent to.

A packet whose selector coincides with one of the ***SPD*** entrances will be processed in accordance to the policy associated to this selector. A *Security Association* is the security connection that is created after the ***SPD*** has been consulted and contains the security information (authentication keys and encryption) required to process the packet.

• *Keys*

The entire security platform based on secret keys stops being secure if the keys are not periodically renewed.

The shorter the refresh time, the greater security of our system against Cryptanalysis tools.

There are two possible general work modes for the management of the security parameters and passwords in IPSec: manual (IPSec manual) and automatic or dynamic (IPSec IKE). These modes refer to the way in which an agreement is reached between peers on security parameters established for the tunnel.

The IPSec platform permits this process to be automated, thanks to the *IKE Internet Key Exchange* protocol (based on the OAKLEY key exchange protocol and the ISAKMP platform). The two ends of the Tunnel automatically negotiate the secure communication parameters (keys, encryption and authentication algorithms). In order to generate this negotiation, the ends must first carry out a **first phase** where they agree on the security parameters that will protect the negotiation. Additionally in this first phase, authentication of the tunnel ends is carried out, using a common key (*Pre-Shared Key*) manually introduced at both ends, digital signatures or with a public key algorithm.

Thanks to this atomization, you can periodically re-negotiate the security parameters. For this, a limited life span is configured for each SA: when this times out, a new SA is created with new authentication and encryption keys.

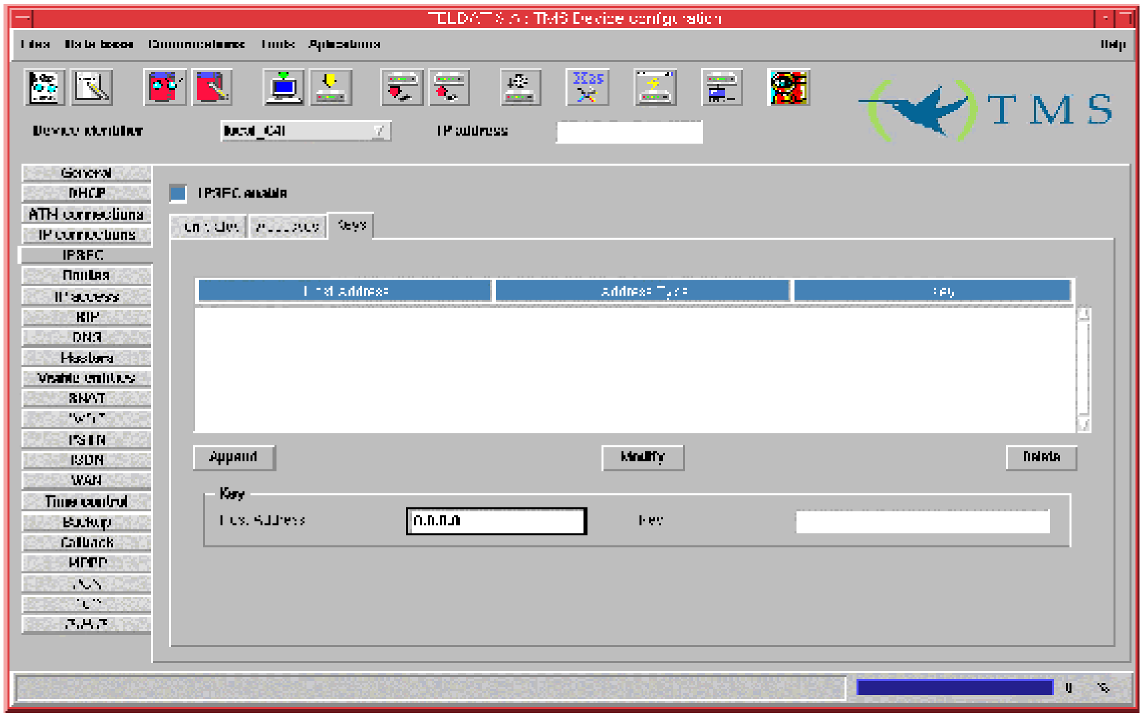


Figure 53: Configuring IPSEC Keys

- **Host Address:** Host IP address. This intervenes in the authentication in order to establish the tunnel.
- **Address Type:** Address type is simply for information purposes.
- **Key:** key for authentication on establishing the tunnel. This must be the same in the tunnel end devices.

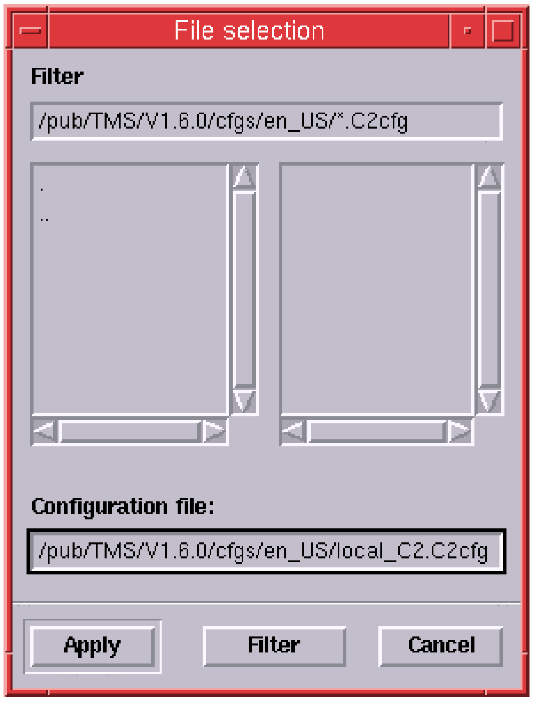
1.2. File commands

This is the group of actions that can be executed over the files. The corresponding meanings are as follows:

a) Read file configuration

The command **read configuration** is used in order to read the configuration of a device from a file. The configuration is read from an ASCII text file where all the variables that appear on the screen are found. The file must have a specific format for subsequent interpretation although this format is generated by the application itself.

Once you have selected this option, a screen appears where you can establish the name of the file you wish to read as the new device configuration which is being edited. The screen is shown below:



Filter: /pub/TMS/V1.6.0/cfgs/en_US/*.C2cfg

Configuration file: /pub/TMS/V1.6.0/cfgs/en_US/local_C2.C2cfg

Figure 54: File selection screen

Element	Description
Filter	This is the filter for the type of file you wish to view. By default this is selected in order to see all the configuration files for the type of device currently selected. The configuration files are found located in the **$TELDATMS/cfgs/$TMSLANG** directory.
Directories	This deals with two lists. The list on the left contains the directories that are attached to the **$TELDATMS/cfgs/$TMSLANG** directory. This right hand list contains all the files currently in the directory for the indicated filter. In order for the directory change to take effect, once the text is modified, press **Apply**.
Configuration File	In this text area you need to write the file name (or this will appear) you wish to read the configuration from. You need to select the files with a **cfg**

extension in cases of devices with the code 37 and 51, with a **C2cfg** extension for devices with code 46, with **C3cfg** extension for devices with codes 53 and 59 and **C3Bcfg** extension for devices with code 60. If we are dealing with a device with code 51, once the file has been read correctly this interprets if you are dealing with a device 51, then the specific part for the XOT, X.25 and Node (transparent to the user of another file with the same name and extension **x25cfg**) is read.

Buttons Press the **Apply** button in order to read the configuration file selected.

Press the **Filter** button in order to update the lists applying the filter.

Press **Cancel** to abort the configuration reading.

The configuration files can only be interpreted correctly if they are read from an application operating in the same language the file was saved in.

b) Writing the configuration in file

The command **write configuration** is used to save the configuration displayed on the screen in a file. This file will remain stored in an ASCII format.

On clicking over the icon, a selection screen similar to the one above appears where on filling out the fields, the file name to be generated and the directory where you wish this to be saved is established.

In devices with code 51, the specific part of the XOT, X.25 and Node configuration is saved in another file with the same name and extension "*x25cfg*".

c) Viewing the log file

If you execute this command, a terminal screen appears that permits you to view in real time the default file where the history on the actions, warnings and management errors are saved.

The default file is **`$TELDATMS/log/tms.log`**.

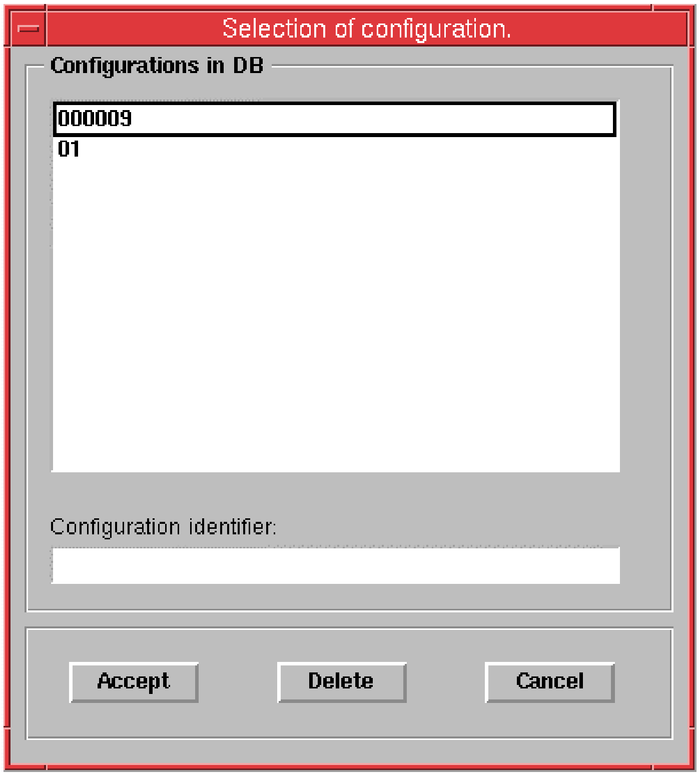
1.3. Database Commands

a) Reading the configuration from the database

This presents a selection screen for the configurations saved in the database so the user can chose the one he wishes to be presented on the screens. Only the saved configurations that correspond with the code of the currently selected device are displayed. The "configuration identifier" field can only be modified by selecting it from the list.

The configurations are saved in a series of tables associated to the distinct entities that make this up.

For further information, please consult Tables used in the database



000009
01

Figure 55: Selecting the database configuration

As you introduce digits in the configuration identifier entry, the application searches through the list for the device that comes the closest to matching this.

b) Saving the database configuration

The command **save configuration to database** is used to write configurations in the database in the distinct tables associated to the entities making this up (see Tables used in the database).

As in the above case, a configuration identifier selection screen is presented. You can save with one of the identifiers associated to one of the configurations already existing in the database or add a new one in the edition field.

1.4. Communications Commands

The following commands establish SNMP communication with the device.

a) Requesting configuration from the device

The command **configuration petition** requests the configuration from the accessible device selected in the screen. I.e. obtains the data relative to all the parameters previously commented on. In order to indicate if communication with the device is in process, the application presents a curser in the shape of a clock indicating this operation and at the same time the progress bar on the lower right hand side of the screen updates.

The configuration obtained is the one from the device DRAM memory and can be different from the one currently active (the start up configuration saved in the FLASH memory) if the user has modified it.

Once the whole configuration has been received, the information parameters are saved (serial number, motherboard number, software version and BIOS version) in the database in the **infodevice** table.

Information on the time the application takes to bring the device configuration is displayed at the foot of the screen.

b) Sending the configuration to the device

The command **send configuration** takes the configuration from the screen and sends it to the accessible device DRAM memory by selecting from the screen.

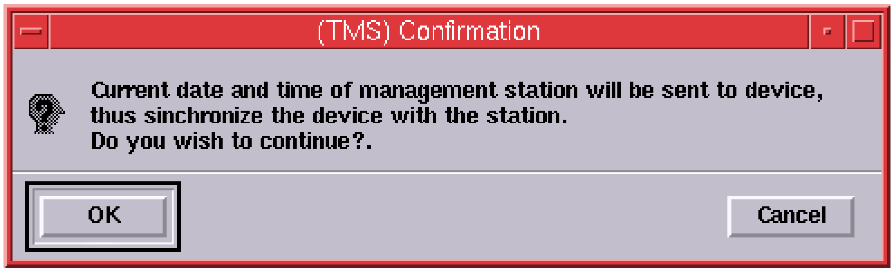
Once the configuration has been sent to the device, the screen clears and a configuration petition is executed. This serves to confirm delivery.

During this operation, the application indicates that it is occupied by showing the cursor as a clock and at the same time the progress bar found on the lower part of the screen updates.

The time spent on the sending and subsequently requesting the configuration from the device is displayed at the bottom of the screen.

c) Synchronizing the device with the management station

The command **set time** serves to synchronize the device date and time with the management station. Once the icon is activated, the following confirmation screen appears:


(TMS) Confirmation

Current date and time of management station will be sent to device,
thus sinchronize the device with the station.
Do you wish to continue?.

Figure 56: Synchronization confirmation

Select **OK** to confirm the action or **Cancel** if you wish to abort.

d) Saving the device configuration to FLASH memory

The command **save configuration** stores the configuration saved in the device's DRAM memory (volatile) to the FLASH memory (permanent). Once the command is executed, the configuration is permanently saved, however it is not the currently active configuration in the device. In order to activate the new configuration, you need to restart the device or reconfigure it through the command described in the next section.

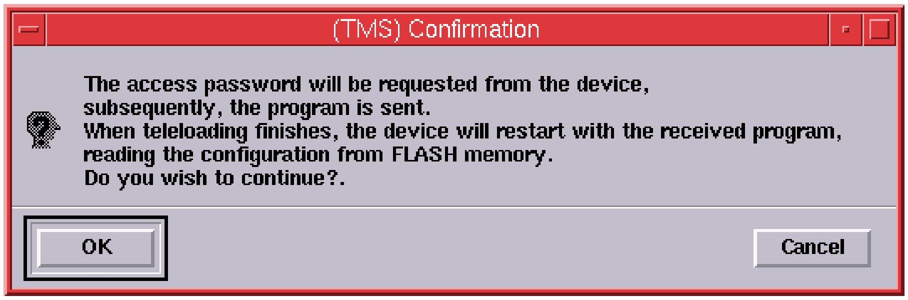
e) Restart the device with the configuration in the FLASH memory

The command **reconfigure** ensures that the device reads the configuration from its FLASH memory (permanent) and deposits it in the device's DRAM memory (volatile) thus converting it into the active configuration..

> ***Note: Reconfiguration assumes the loss of the connection with the device until the master makes contact again once the device has been restarted.***

f) Teleloading software to the device

The command **teleload software** is used to send the program executed in the device. The Management Center can then update the device software with the new versions. When you select the teleload command, a screen appears as shown below:



The access password will be requested from the device,
subsequently, the program is sent.
When teleloading finishes, the device will restart with the received program,
reading the configuration from FLASH memory.
Do you wish to continue?.

Figure 57: Confirmation of Software teleload

This deals with a confirmation screen where the consequences of the command are explained. Once confirmed, a **file selection** screen appears in order to choose the program you wish to teleload.

The default file that is used for the devices with codes 37 and 51 is usually **cbra<version>.x** although it can be any file that contains the necessary code for correct device operation. In devices with code 46 the default file used is usually **teldatc.bin**.

Once the teleloading has completed, the device is restarted with the new software and the configuration in the FLASH memory. For this reason, until the master router begins to manage the said device once more, this will appear inaccessible.

The teleloading operation provides information on its progress in the **`$TELDATMS/log/telecarga_usr_<device_id>.log`** file.

When you call from the operations over groups, the teleloading for each device leaves the information on its progress in the **`$TELDATMS/log/telecarga_<device_id>.log`** file (in both cases <device_id> is the device identifier, currently its telephone number in the database).

WARNING

It is essential that you do not interrupt the teleloading operation while it is being executed, as this will leave the device completely inaccessible from a remote point of view. In cases where this situation arises, you must enter the device via the console (i.e. locally).

AVOID PRESSING CTRL-C DURING TELELOADING!

In the same way, it is the responsibility of the operator to send a valid file, as the application does not carry out any checks on the file content.

The TMS devices are protected against simultaneous teleloading preventing new FTP connections when one is already established.

2. Monitoring

The TMS devices are capable of storing two main types of statistics, which from here on will be known as fortnightly and daily accounts. Also the Teldat routers C3 and C3B store statistics related to the POS transactions that are carried out through them.

The **fortnightly accounts** are values the device stores in the RAM memory with batteries. This memory therefore remains even if the device is switched off or reconfigured. This is used in order to provide connection history data for the client.

The **daily accounts** on the other hand are values stored since the last start up of the device and are saved in the volatile RAM memory. This means this data will be lost when the device is reset. The aim of these accounts is to help resolve device configuration problems.

The **tmsmon** application requests the daily and fortnightly accounts stored in the CBRA and Teldat C devices through SNMP. This periodically consults the database in order to check the state of the devices and permits you to select any of those accessible as destination for the petitions. In order to place a device under management and obtain an ACCESSIBLE state, the **tmsmanager** application is used, which can be launched from the **Applications**->**Management** option from the main menu.

However, you can also obtain the daily and fortnightly accounts associated to a device without needing to access through the **tmsmanager** application. For this you need to invoke monitoring in the following way:

```
>tmsmon [-h] [-i <ipadd>]  [-c < community>] [-id <device_id>] [-t <refresh period in
seconds>]
```

The –h parameter presents the application invocation format.

2.1. Description of the main screen

The tool bar located on the upper part of the screen contains the following buttons:

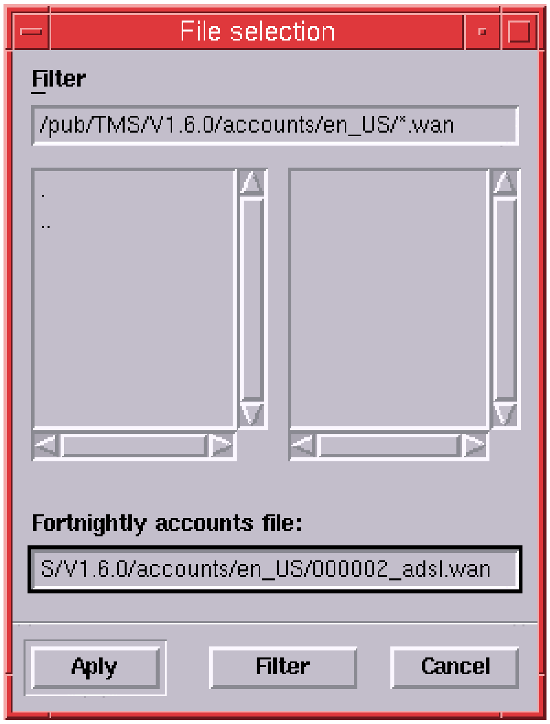
a) *File Commands*

- ***Read file accounts***

This command is used to read the accounts saved in three text files (fortnightly accounts from the WAN interface, addresses most visited and traffic per station) with a determined format. For further information on the files, consult Format of the fortnightly account files

In addition the C3 and C3B routers are used to read the accounts saved on the transactions that have been carried out by the POSs. For further information on the files, consult Format of the transaction files

Once you have selected this option, a screen will appear where you can establish the name of the file you wish to read as new device configuration being edited. The screen that appears is shown in the below figure:



Filter

/pub/TMS/V1.6.0/accounts/en_US/*.wan

.
..

Fortnightly accounts file:

S/V1.6.0/accounts/en_US/000002_adsl.wan

Figure 58: File selection screen

Element	Description
Filter	This is the filter for the type of file you wish to view. By default this is selected in order to see all the fortnightly accounts files from the WAN interface (*.wan). The fortnightly accounts files (and transactions in cases of Teldat C3 and Teldat C3B) are found located in the **$TELDATMS/accounts/$TMSLANG** directory.
Directories	This deals with two lists. The list on the left contains the directories that are attached to the **$TELDATMS/accounts/$TMSLANG** directory. The right hand list contains all the files currently in the directory for the indicated filter. In order for the directory change to take effect, once the text is modified, press **Apply**.
Accounts File	In this text area you need to write the file name (or this will appear) you wish to read the accounts from. You need to select the files with a **wan** extension.
Buttons	Press the **Apply** button in order to read the configuration file selected. Press the **Filter** button in order to update the lists applying the filter. Press **Cancel** to abort the configuration reading.

The accounts files can only be interpreted correctly if they are read from an application operating in the same language the file was saved in.

- ***Writing the account file***

This is used to save the fortnightly accounts (and transactions in cases of the Teldat C3x router), which are displayed on the screen in files. For further information on the file format, please consult Format of the fortnightly files and/or Format of the transaction files

On clicking over the icon, a selection screen similar to the one above appears where on filling out the fields, the file name to be generated and the directory where you wish this to be saved is established.

b) Viewing a log file

If you execute this command, a terminal screen appears that permits you to view in real time the default file where the history on the actions, warnings and management errors are saved. The default file is **`$TELDATMS/log/tms.log`**.

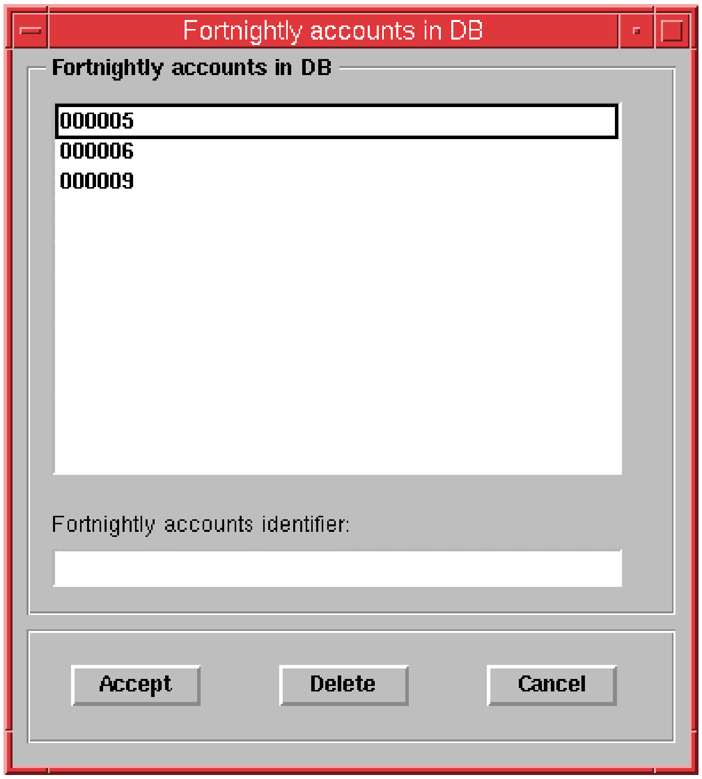
c) Database Commands

- ***Reading the accounts from the database***

This presents a selection screen for the accounts saved in the database so the user can chose the one he wishes to be presented in the screens. The "accounts identifier" field can only be modified through selection from the list.

The accounts are saved in a series of tables associated to the distinct entities that make this up.

For further information, please consult Tables used in the database


Fortnightly accounts in DB
Fortnightly accounts in DB
Fortnightly accounts identifier:
Accept
Delete
Cancel

000005
000006
000009

Figure 59: Selecting the database fortnightly accounts

As you introduce characters in the accounts identifier entry, the application searches through the list for the identifier that comes the closest to matching this.

- ***Saving the accounts in the database***

This is used to write the fortnightly accounts (and transactions in cases of the Teldat C3x router) from the screen in the various tables associated with the entities making up the database. (See Tables used in the database).

As in the above case, an accounts identifier selection screen is presented. You can save with one of the identifiers associated to one of the configurations already existing in the database or add a new one in the editing field.

d) Communications Commands

- ***Requesting accounts from the device***

The accounts in the currently selected tab are requested from the device and presented on the screen.

• *Deleting the accounts from the device*

If you press this button, a confirmation message will appear that, if accepted by the user, will provoke the sending of an order to the device to permanently delete the stored fortnightly accounts (or transactions in cases of the Teldat C3 and Teldat C3B routers).

If various inconsistent values appear in the accounts petition to the device, we recommend deleting all the accounts and requesting them again.

A case may arise where after an updating of the device software has been carried out, the accounts begin to be saved in an erroneous form although these tend to be isolated situations.

The three **Buttons** appearing on the lower part of the screen are as follows:

Close: This button is used to close the monitoring application.

Update: On pressing this button, the selected tab parameters are monitored. This action is equivalent to pressing the icon found on the upper right hand corner of the screen.

Help: As the name indicates, the help button permits you to access the help from the Monitoring screen.

In addition to the buttons already mentioned, on the upper part of the screen there is a menu bar. From this bar you can execute all the actions associated to the buttons as well as other actions that are explained below:

File: You can carry out the following options from this menu:

Read File:

Read the file accounts as described above.

Save the file:

Saves the accounts to file as described above.

Exit:

This menu option is the equivalent to selecting the Close button previously described.

DataBase:

Read Database:

This reads the accounts from the database as described in the previous section.

Save Database:

Saves the accounts in the database.

Applications: **Management**:

Launches the management application.

Configuración:

Launches the configuration application.

Automatic collection status:

Launches the monitoring application for the automatic collection of the fortnightly accounts.

Operations over groups:

Launches the operations over groups management application.

Communications:

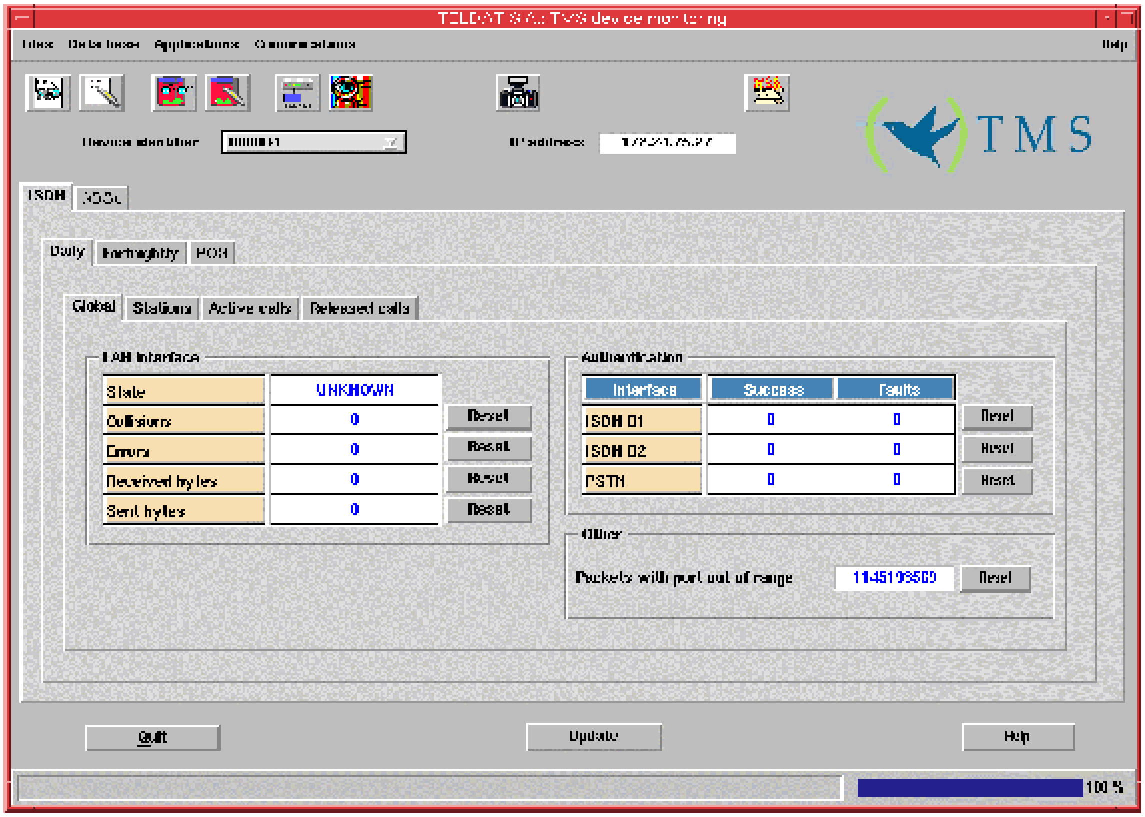
From this menu, you can request the daily and fortnightly accounts from the router (or transactions in cases of the Teldat C3x routers) and delete them as described in the section on the tool bar buttons.

2.2. Daily Monitoring

Daily monitoring permits you to view the accounts the device has stored since its last reconfiguration. The data presented is different depending on the type of the device.

a) ISDN

• Global parameters



LAN Interface

State	UNKNOWN	
Collisions	0	Reset
Errors	0	Reset
Received bytes	0	Reset
Sent bytes	0	Reset

Authentication

Interface	Success	Faults	
ISDN 01	0	0	Reset
ISDN 02	0	0	Reset
PSTN	0	0	Reset

Other

Packets with port out of range 1145193509 Reset

Figure 60: Daily monitoring of ISDN global parameters

The following parameters can be monitored from this screen:

- **LAN Interface**

  - **State:** This can take one of the following values: UP, DOWN or UNDER TEST.
  - **Collisions:** Number of frames not transmitted due to excessive collisions.
  - **Errors:** Number of errors in the LAN interface.
  - **Sent bytes:** Number of octets arriving from the B1 or B2 channel connections and transmitted to the LAN.
  - **Received bytes:** Number of octets arriving from the LAN with the device itself or the B1 or B2 channels connection as the destination.
- **Authentication for each ISDN B channel (devices 37 , 51 and 60) and PSTN (only devices 37).**
  - **Success:** Number of times that the authentication phase has been successfully established at the PPP protocol level.
  - **Faults:** Number of times that the PPP authentication phase has failed.
- **Others**
  - **Packets with port out of range:** Number of packets that have not been processed as the port is out of range. These are packets received from the WAN with a destination port that does not correspond to any NAT entry. These are incoming packets that either, did not have an associated outgoing packet or, the corresponding NAT entry for the outgoing packet has timed out.

The counters located to the right of the **Reset** button can be returned to zero (0) with a simple click.

> ***Error Reset:***
>
> ***If the error counter is set to 0, then the collisions counter will also return to 0.***

> ***Authentication counter reset:***
>
> ***When pressed, this zeroizes the successes and failures counter.***

• *Stations provoking calls*

Furthermore, the daily monitoring permits you to view the last 20 stations that have provoked a call displaying for each of them both the **IP address** and the **Date** and **Time** when the call was carried out. The date is only shown when the device has software **version 5.1** and above, otherwise only the time the connection was initiated will be given.

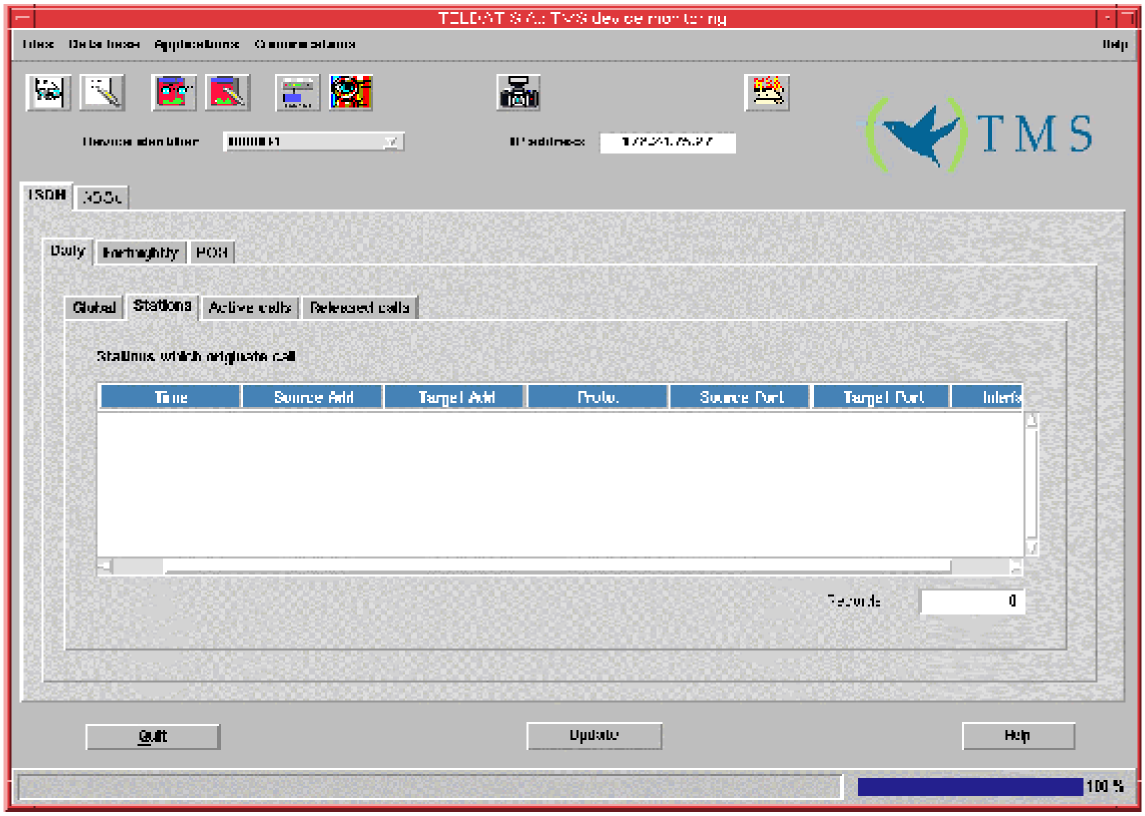
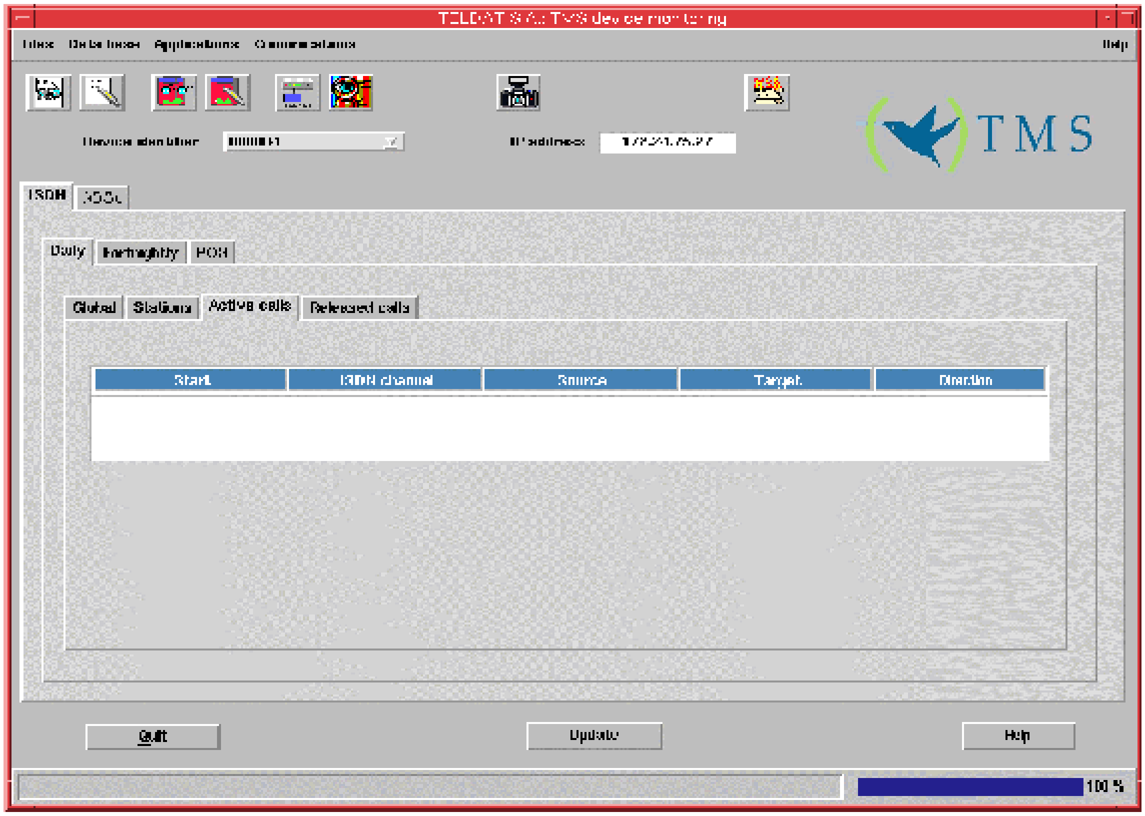


Figure 61: Daily monitoring of the stations provoking calls

> ***DNS Traffic:***
>
> ***In device software version prior to 5.1, the DNS traffic generated by the stations are assigned to the IP address of the device itself. From version 5.1 onwards, this is assigned to the source station.***

- ***Active calls***

The system's active ISDN calls have a set of variables to provide specific information on the call.



Device identifier 000001

IP address 172.24.75.27

Start	ISDN channel	Source	Target	Direction

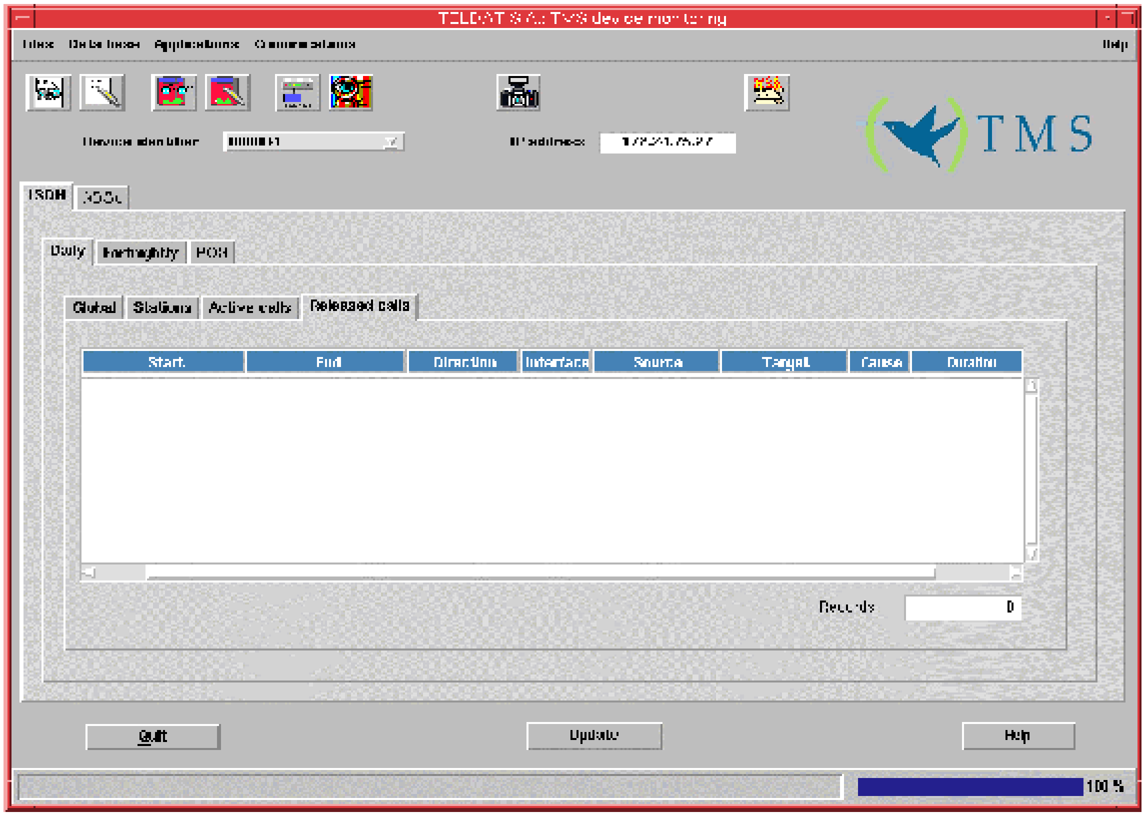
Figure 62: Daily monitoring of the active calls

The set of parameters that can be seen are as follows:

- **Start:** The moment when the call is established.
- **ISDN Channel:** In cases of active ISDN calls, this indicates which channel (B1 or B2) the call was established through.
- **Source:** Calling number.
- **Target:** When the call is **Outgoing**, this indicates the number of the interlocutor.
- **Direction:** This can take two values: **Outgoing**, indicating which device executed the call, or **Incoming**, indicating which device responded to the call.

• *Released calls*

In this screen, you can view the attempted calls and those established in the device from the last time this was reconfigured.



Start	End	Direction	Interface	Source	Target	Cause	Duration

Records 0

Figure 63: Daily monitoring of the released calls

You can consult the following fields:

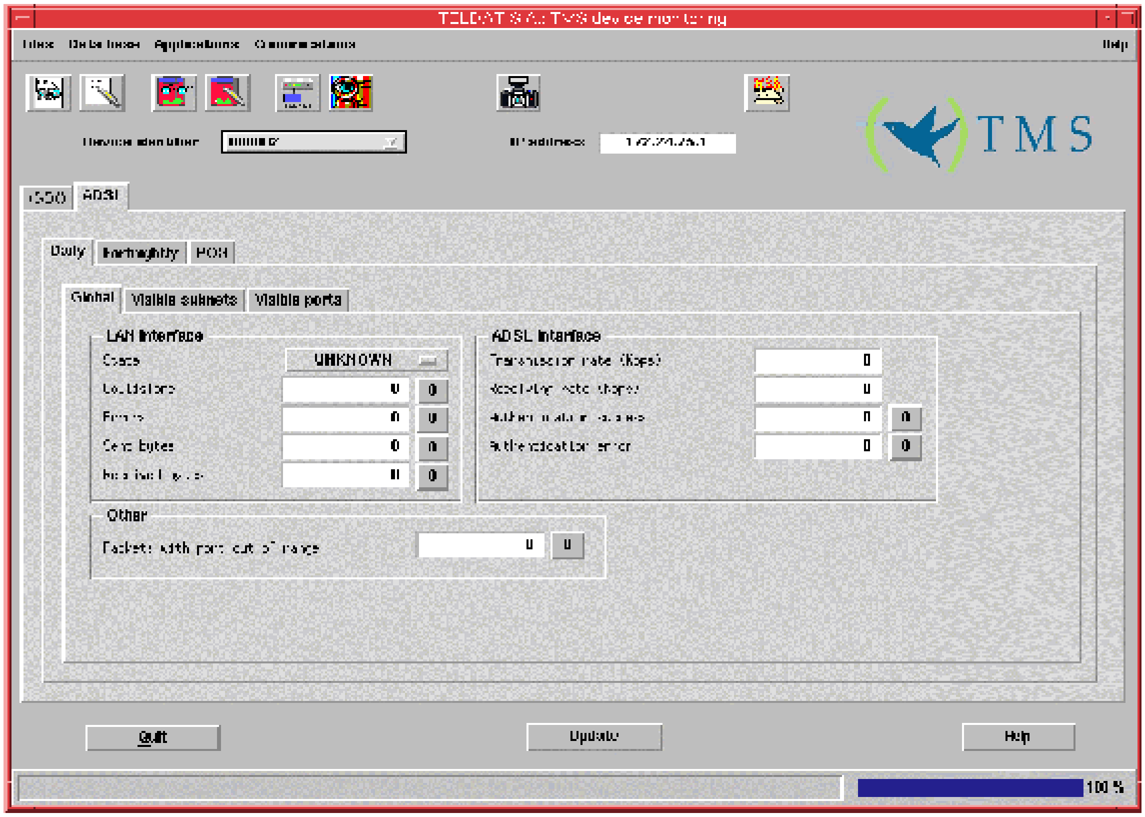
- **Start:** Call start date and time.
- **End:** Call release date and time.
- **Direction:** This can take two values: **Outgoing**, indicating which device executed the call, or **Incoming**, indicating which device responded to the call.
- **Interface:** ISDN B channel the call is established through.
- **Source:** Calling number.
- **Target:** Interlocutor ISDN number of the device.
- **Cause:** This is an indication of the cause through which the last call proportioned by the ISDN network complying with the ISO Q931 standard was released. There is a list of causes in the section on ISDN release causes.
- **Duration:** Call duration in hours, minutes and seconds.

b) ADSL

• Global Parameters

The following screen presents the daily monitoring of the global parameters.

The counters have a “0” button. By clicking this button you return to zero.



Device identifier: [illegible]
IP address: [illegible]

LAN interface

State	UNKNOWN
Collisions	0
Errors	0
Sent bytes	0
Received bytes	0

ADSL interface

Transmission rate (Kbps)	0
[illegible]	0
Authentication failures	0
Authentication error	0

Other

Packets with port out of range	0

Figure 64: Daily monitoring of the ADSL global parameters

The SNMP MIB list of variables that are monitored are as follows:

LAN interface

- **State:** This can take one of the following values: **UNKNOWN**, **ACTIVE**, **DOWN** or **UNDER TEST**.
- **Collisions:** Number of frames not transmitted due to excessive collisions. When set to zero and if there are no other errors in the LAN interface, the error counters are also reset.
- **Errores:** Number of errors in the LAN interface. This includes the collisions, for this reason when set to 0, the collisions counter also resets.
- **Received Bytes:** Number of bytes received in the router that comes from the LAN.
- **Sent Bytes:** Number of bytes transmitted by the router towards the LAN.

Others

- **Packets with port out of range:** Number of packets that have not been processed as the port is out of range. These are packets received from the WAN with a destination port that does not correspond to any NAT entry. These are incoming packets that either, did not have an associated outgoing packet or, the corresponding NAT entry for the outgoing packet has timed out.

ADSL Interface

- **Transmission rate [Kbps]:** This is the real speed at which the ADSL interface is transmitting. This may not coincide with the speed configured in the router.

- **Receiving rate [Kbps]:** This is the real speed at which the router ADSL interface is receiving. This may not coincide with the configured speed.
- **Authentication success:** This is the number of times that the PPP protocol authentication phase is established in the ADSL interface.
- **Authentication error:** This is the number of times that the PPP protocol authentication phase has failed to establish in the ADSL interface.

• *Visible Subnets*

This screen displays the access statistics for the visible subnets configured in the router.

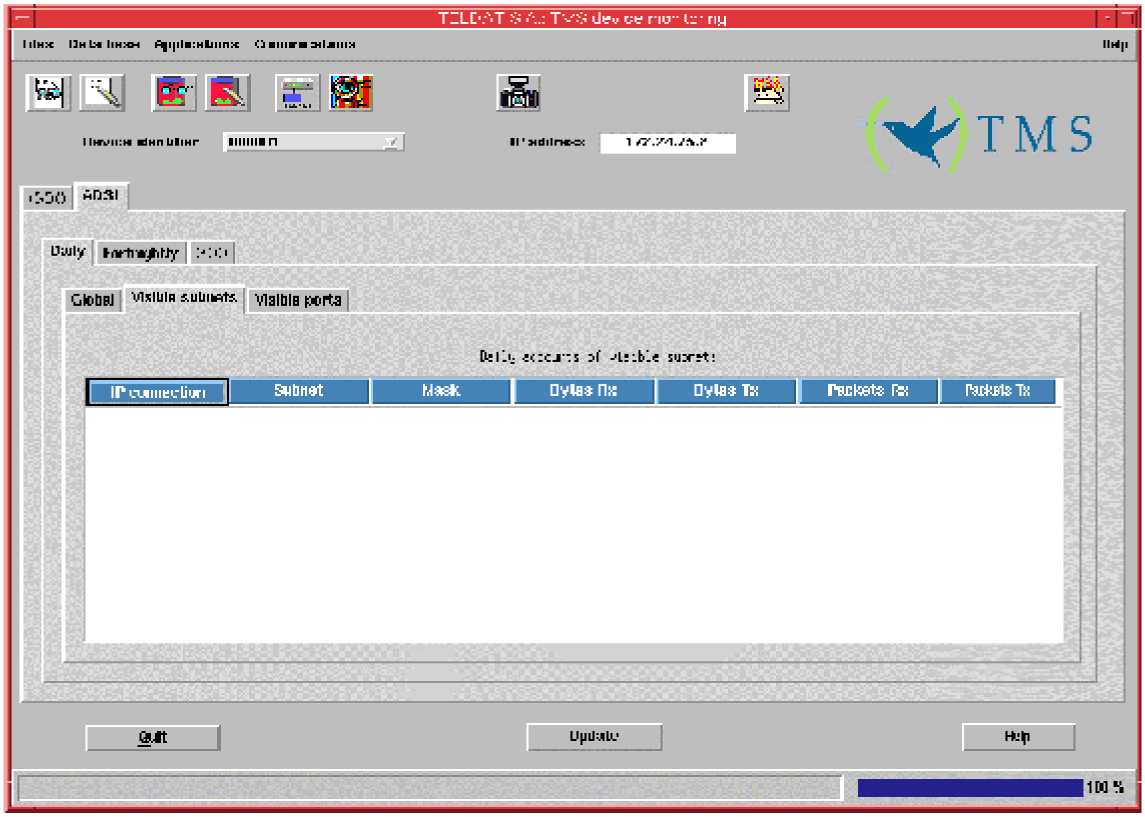
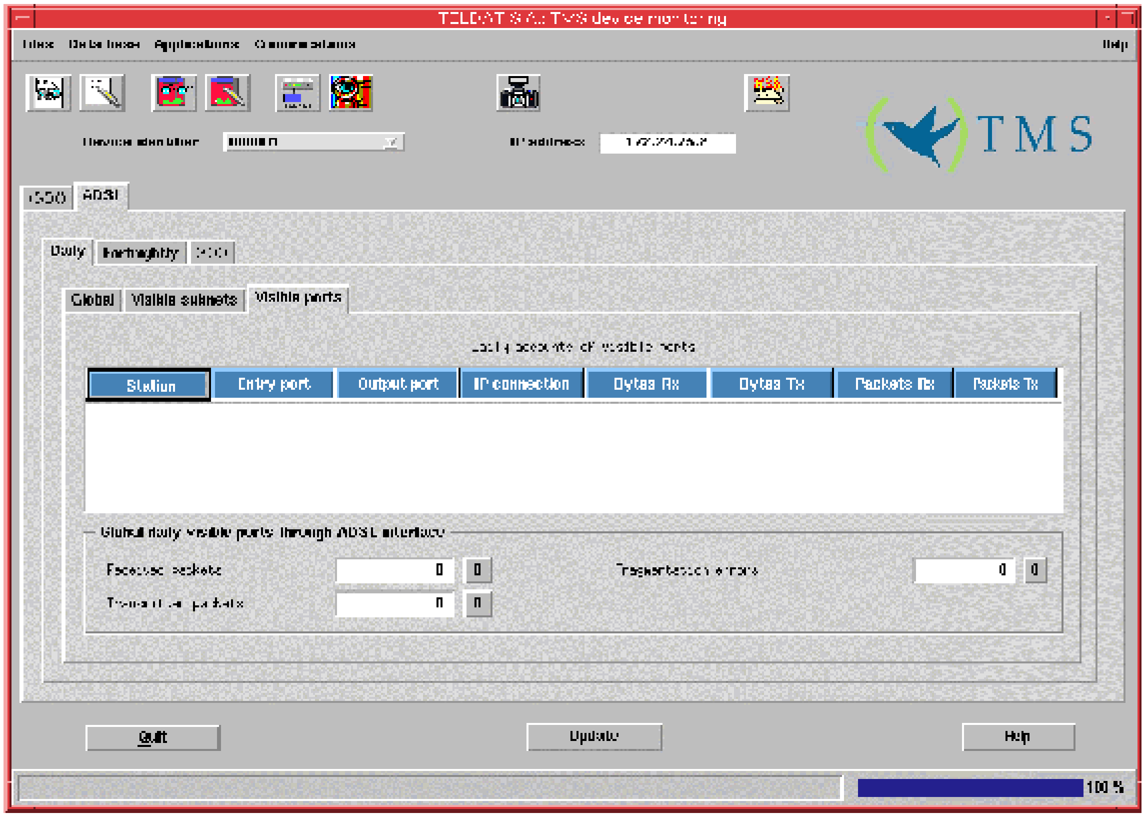


Figure 65: Daily monitoring of the visible subnets

- **IP connection:** IP connection identifier through which the subnet is made visible to the outside.
- **Subnet:** Visible subnet IP address.
- **Mask:** Visible subnet IP mask.
- **Bytes Rx:** Bytes that have crossed the router towards the visible subnet.
- **Bytes Tx:** Bytes that have crossed the router sent by the visible subnet.
- **Packets Rx:** Packets that have crossed the router towards the visible subnet.
- **Packets Tx:** Packets that have crossed the router, sent by a visible port.

- ***Visible Ports***

The access statistics to visible ports are displayed in this list.



Daily accounts of visible ports

Station	Entry port	Output port	IP connection	Bytes Rx	Bytes Tx	Packets Rx	Packets Tx

Global daily visible ports through ADSL interface

Received packets 0 0

Transmitted packets 0 0

Fragmentation errors 0 0

Figure 66: Daily monitoring of visible ports

In the lower part of the screen, the global access parameters to the set of visible ports is displayed:

- **Received packets:** The total number of packets received from the visible ports.
- **Transmitted packets:** The total number of packets sent from the visible ports.
- **Fragmentation errors:** Total number of packets received in the router indicating that the packet that has been sent requires fragmentation and does not have the fragmentation bit activated. The packet that produces this error is discarded.

The fields making up the individual monitoring list of visible ports are as follows:

- **Station:** LAN station that holds the visible port.
- **Entry port:** Station port that is visible.
- **Output port:** The previous port is substituted for this one when ports NAT is carried out (NAPT).
- **IP connection:** IP connection through which the port is visible.
- **Bytes Rx:** Bytes that have crossed the router with a visible port as the destination.
- **Bytes Tx:** Bytes that have crossed the router, sent by a visible port.
- **Packets Rx:** Packets that have crossed the router towards to one of the visible ports.

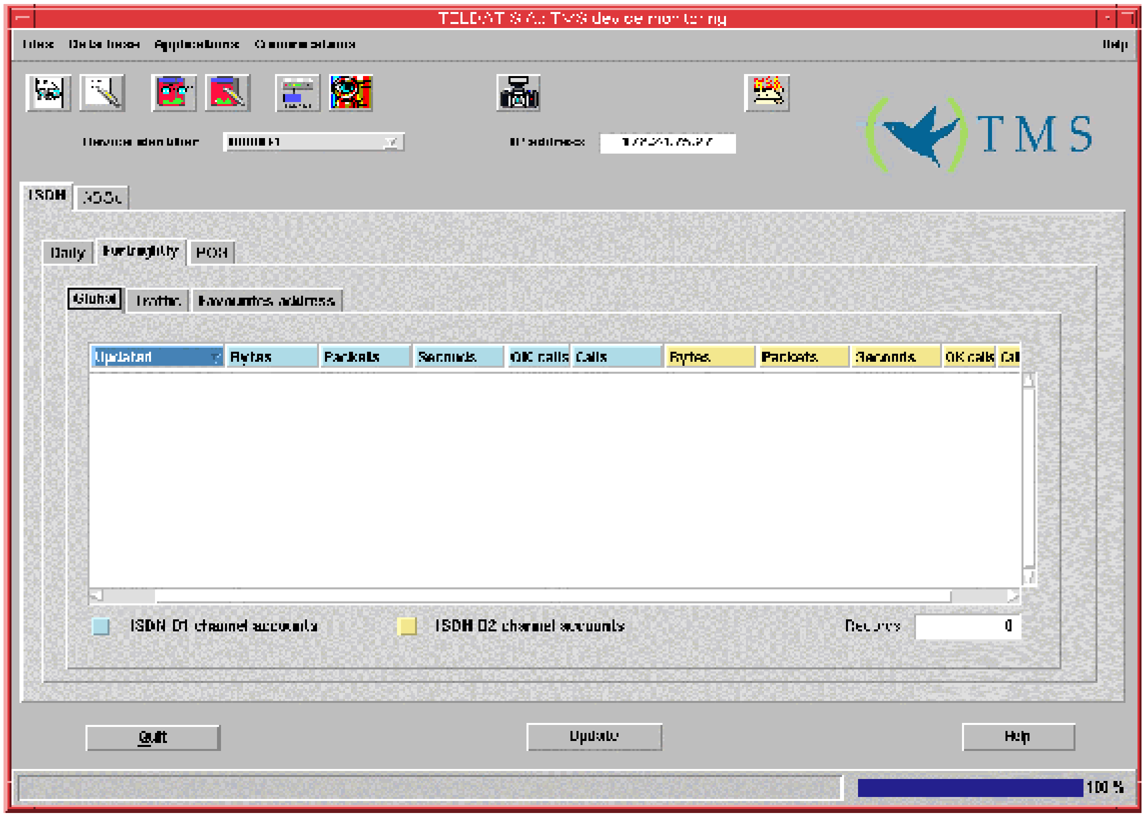
- **Packets Tx:** Packets that have crossed the router, sent by a visible port.

2.3. Fortnightly Monitoring

In the fortnightly monitoring, the accounts stored in the device for the last 15 days are displayed. In order to refresh the screen, you need to enter the fortnightly monitoring folder and press **Update** or the icon located in the upper right hand corner of the screen. Each time the fortnightly accounts are requested from the device, they are automatically saved in the accounts files in the **`$TELDATMS/acounts/$TMSLANG`** directory. Depending on the type of device, the data presented is different.

a) ISDN

• Global accounts for the 15 days



Device identifier

IP address

Updated	Bytes	Packets	Seconds	OK calls	Calls	Bytes	Packets	Seconds	OK calls	Cal

ISDN B1 channel accounts

ISDN B2 channel accounts

Records: 0

Figure 67: Fortnightly monitoring of the ISDN global parameters

Each line displays the data for one day. The values correspond to the lapsed interval from the previous line date and time to the date and time of the current line.

The following fields are displayed for each ISDN B channel:

- **Updated:** The date and time the data was stored in the device.
- **Bytes:** Octets sent and received through the device.

- **Packets:** Packets sent and received through the device.
- **Seconds:** Total connection time.
- **OK calls:** Total number of calls that have successfully managed to establish connection at the PPP protocol level over ISDN.
- **Total calls:** Total number of calls generated in a given day. The ISDN connection was established for all of them but it is possible that the communication did not progress. Some of the calls may have been rejected due to an error in authentication or through an error in the PPP protocol parameters negotiation over ISDN. If the ISDN connection does not establish, the counter does not increase.

> ***None of the previous parameters includes the management call accounts so that the client is not charged.***

• *Traffic per station*

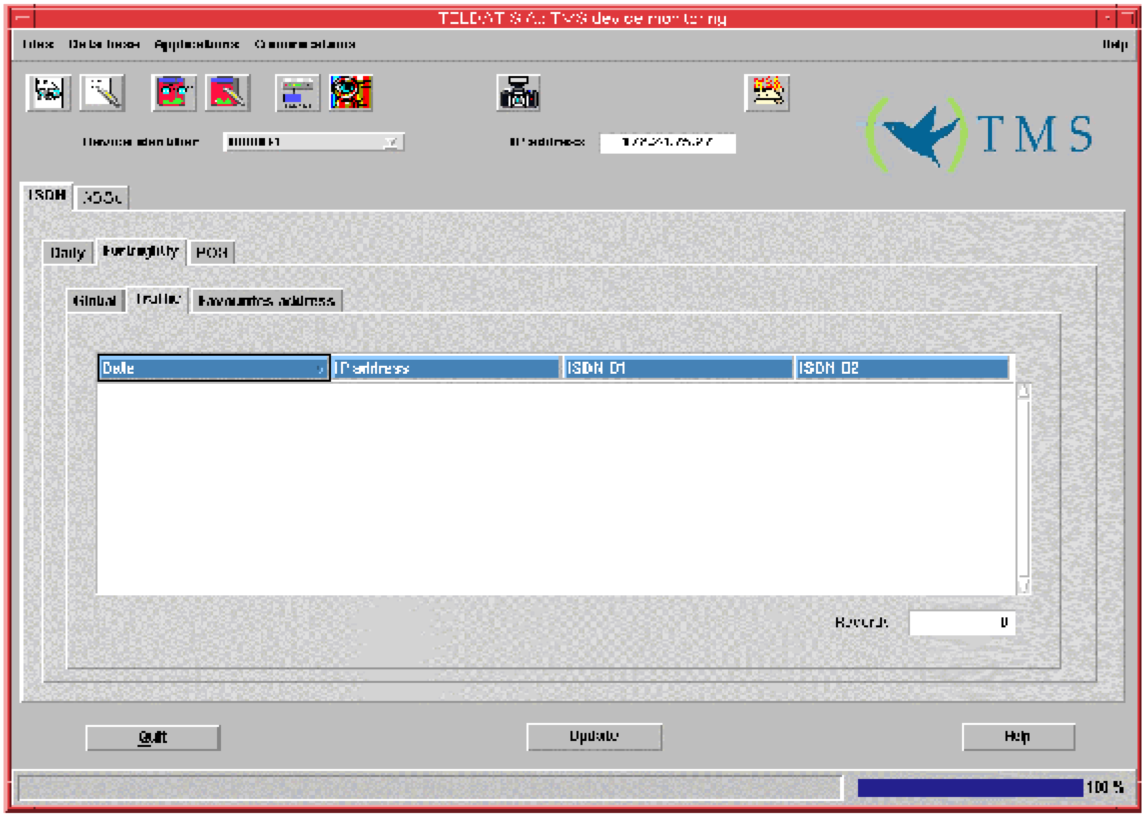


Figure 68: Fortnightly monitoring for traffic per ISDN station

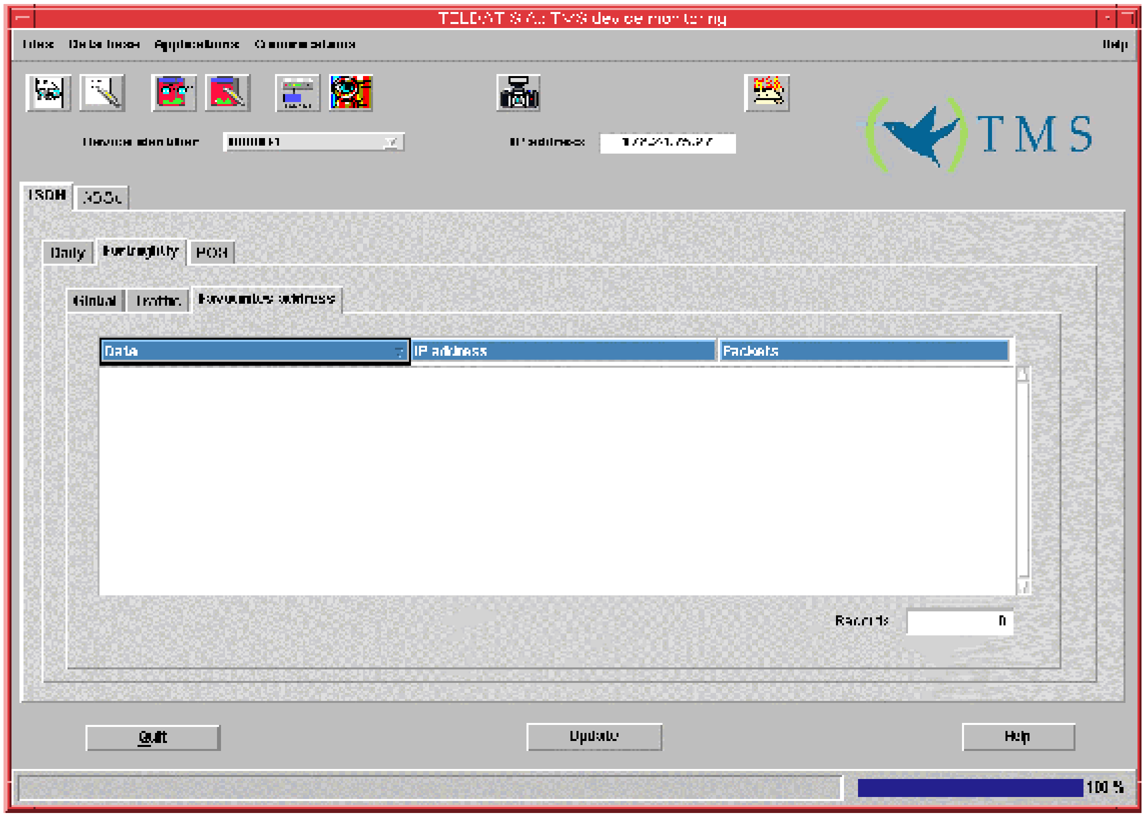
The second area, traffic per station, is represented by a set of values providing information on connections executed by a determined station. The parameters used to represent traffic are as follows:

- **Date:** The date the station connected.
- **IP address:** Station IP Address.
- **ISDN B1:** Packets running through the ISDN B1 channel.

- **ISDN B2:** Packets running through the ISDN B2 channel.

• Favorite address

This list contains the addresses visited in the last 15 days, for the first 256 addresses visited, both for B1 and B2. The management calls traffic is not included.



Device identifier: [illegible]
IP address: [illegible]

Date	IP address	Packets

Records: 0

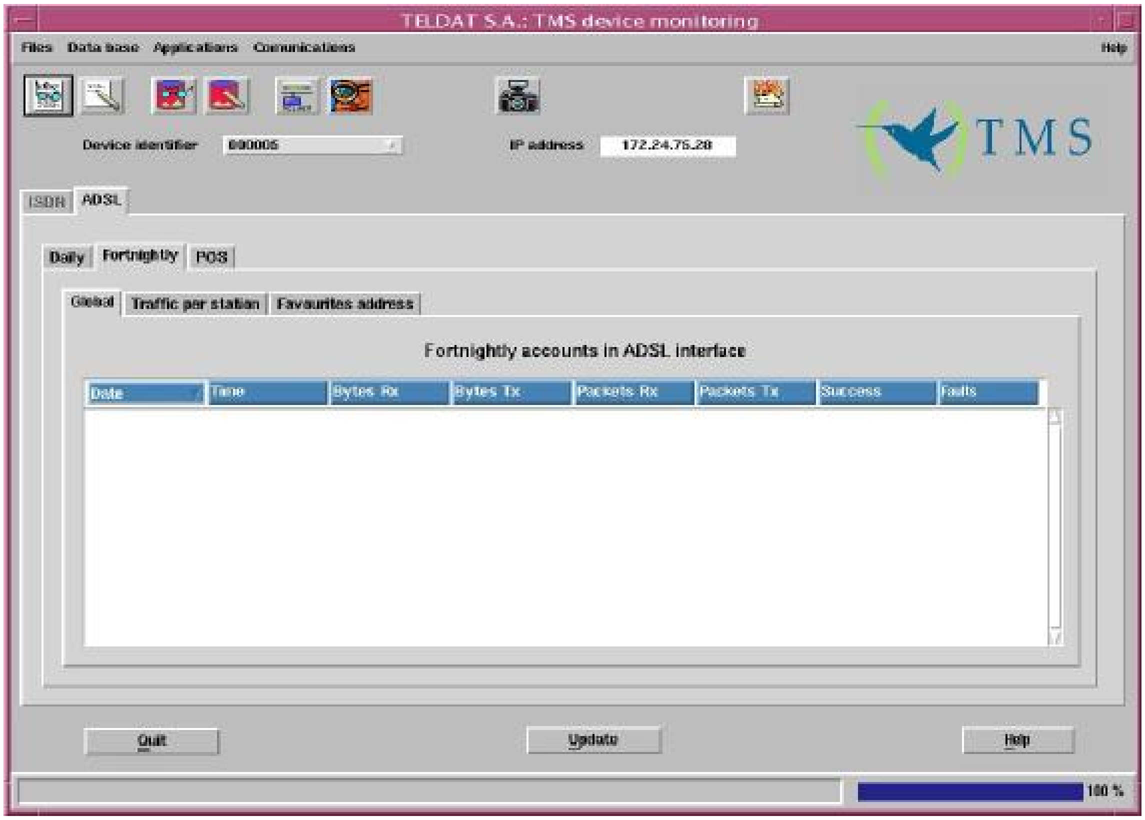
Figure 69: Fortnightly monitoring of the most visited ISDN addresses

- **Date:** Represents the day the connection was carried out.
- **IP address:** IP Address the connection was established through.
- **Packets:** Total traffic (packets) in transmission.

b) ADSL

• Global accounts for the last 15 days

This screen displays the global traffic parameters that the device has transmitted in the last fifteen days.



TELDAT S.A.: TMS device monitoring

Device identifier: 000005

IP address: 172.24.75.28

Fortnightly accounts in ADSL interface

Date	Time	Bytes Rx	Bytes Tx	Packets Rx	Packets Tx	Success	Faults

Figure 70: Fortnightly monitoring of the ADSL interface

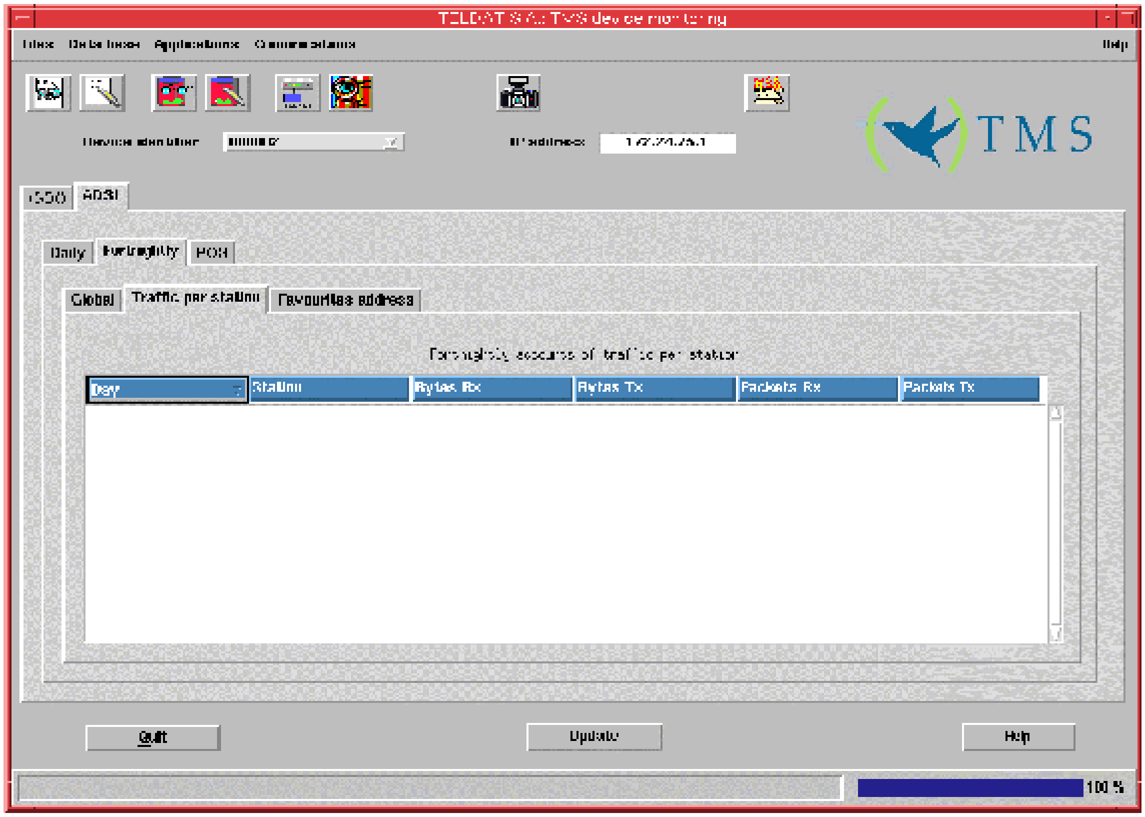
Each line displays the data for one day. The values correspond to the interval starting from the date and time from the previous line up to the date and time of the line in progress.

The following fields are displayed:

- **Date:** Date the router stored the data from this line.
- **Time:** Time the Router stored the data from this line.
- **Bytes Rx:** Bytes received in the router ADSL interface.
- **Bytes Tx:** Bytes transmitted by the router ADSL interface.
- **Packets Rx:** Packets received in the router ADSL interface.
- **Packets Tx:** Packets transmitted by the router ADSL interface.
- **Success:** Total number of times that the connections have been successfully established at the PPP protocol level over the ADSL interface.
- **Faults:** Total number of connections rejected due to authentication failure or due to a failure in the PPP protocol parameters negotiation over ADSL. If a connection is not established this counter increases.

- ***Traffic per station***

In this screen, the traffic transmitted through the first 50 stations that generate traffic each day through the router is displayed.



Fortnightly accounts of traffic per station

Day	Station	Bytes Rx	Bytes Tx	Packets Rx	Packets Tx

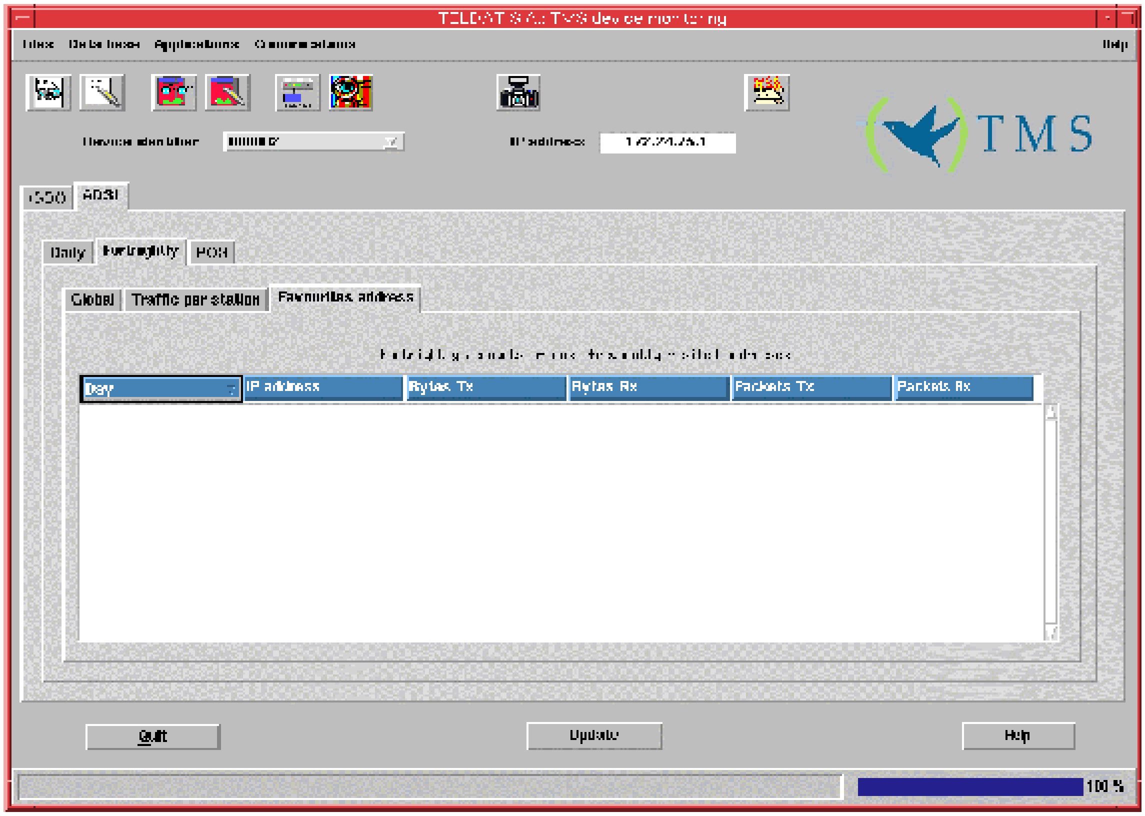
Figure 71: Fortnightly monitoring for traffic per ADSL station

The variables to be monitored are as follows:

- **Day:** The date the station connected.
- **Station:** Station IP Address that transmitted the traffic.
- **Bytes Rx:** Bytes received in the router ADSL interface.
- **Bytes Tx:** Bytes transmitted by the router ADSL interface.
- **Packets Rx:** Packets received in the router ADSL interface.
- **Packets Tx:** Packets transmitted by the router ADSL interface.

- ***Most visited addresses***

This table contains the addresses visited in the last 15 days, for the first 256 visited addresses.



Day	IP address	Bytes Tx	Bytes Rx	Packets Tx	Packets Rx

Figure 72: Fortnightly monitoring of the most visited addresses

The data is as follows:

- **Day:** Represents the day the connection was carried out.
- **IP address:** IP Address the connection was established through.
- **Bytes Tx:** Bytes transmitted through the ADSL interface with the previous IP address as destination.
- **Bytes Rx:** Bytes received in the router ADSL interface sent by the previous address.
- **Packets Tx:** Packets transmitted through the ADSL interface with the previous IP address as destination.
- **Packets Rx:** Packets received in the router ADSL interface sent by the previous address.

2.4. POS Monitoring

In the POS tabs, the information (for those devices that save this) on executed transactions (whether correct or not) is monitored. In the monitoring of transactions, the statistics saved in the device are presented. In order to refresh the screen, you must enter the transaction monitoring folder and press **Update** or click on the icon located on the upper right hand corner of the screen. Each time the accounts are requested from the device, they are automatically saved in the accounts files in the **`$TELDATMS/acounts/$TMSLANG`** directory.

The displayed information is identical for ISDN and ADSL devices.

a) Correct Transactions

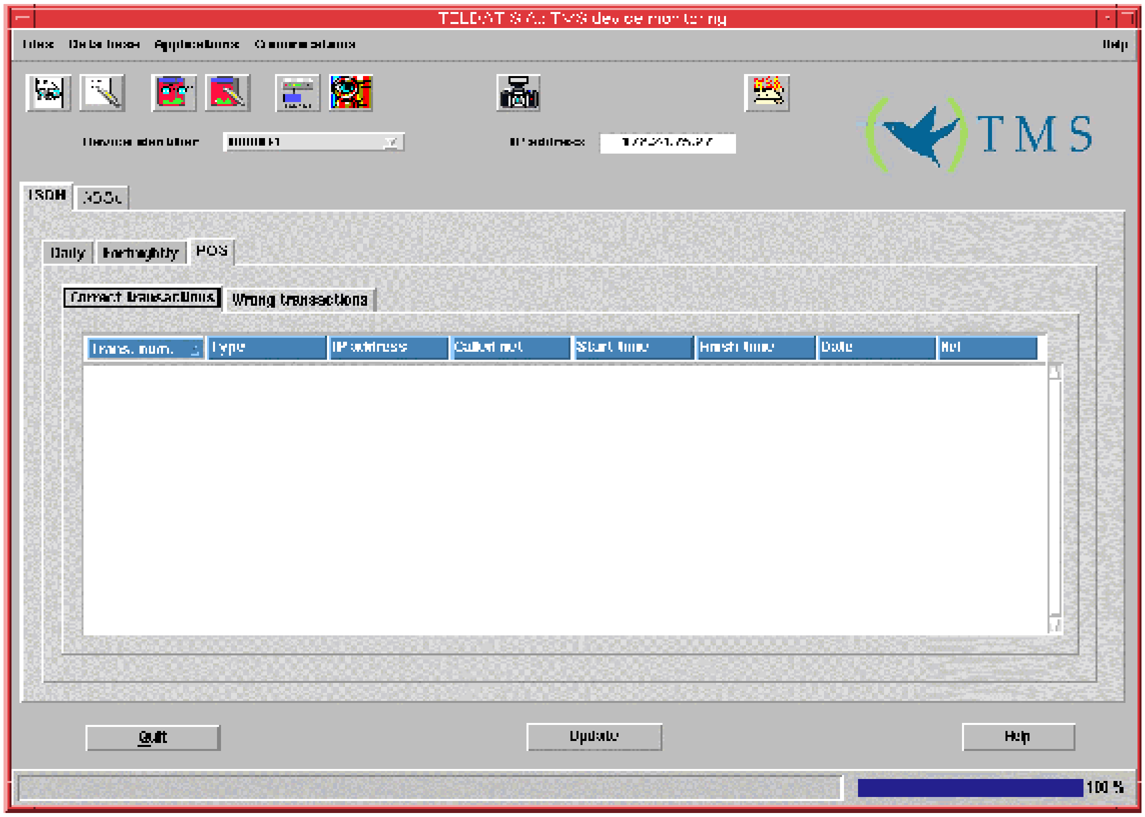


Figure 73: Correct transactions monitoring

Each line displays the data of a transaction correctly carried out by a point of sales terminal.

The fields for each transaction are as follows:

- **Trans. Num.:** Number of the transaction carried out.
- **Type:** The type the transaction pertains to.
- **IP address:** IP address of the transaction authorizing entity.
- **Called net:** Network called in order to carry out the transaction.
- **Start time:** The start time of the transaction.
- **Finish time:** The end time of the transaction.
- **Date:** Date the transaction was carried out.
- **Net:** Entity through which the transaction is carried out.

b) *Erroneous Transactions*

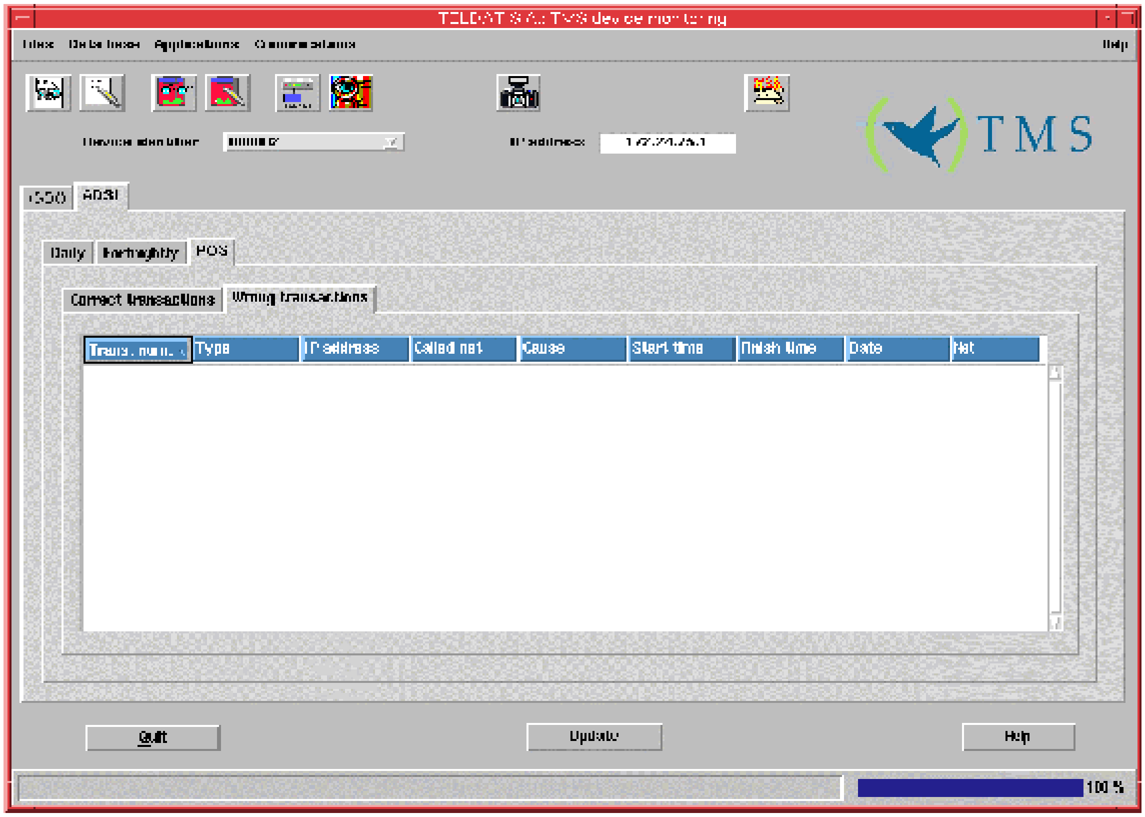


Figure 74: Monitoring erroneous transactions

Each line displays the data of a transaction incorrectly carried out by a point of sales terminal.

The fields for each transaction are as follows

- **Trans. num.:** Number of the transaction carried out.
- **Type:** Type the transaction pertains to.
- **IP address:** IP Address of the transaction authorizing entity.
- **Called net:** The network called in order to carry out the transaction.
- **Cause:** This is the reason the transaction was not carried out correctly. The significance of these values is found in Errors in the transactions.
- **Start time:** Start time the transaction was carried out.
- **Finish time:** Time the transaction ended.
- **DateFecha:** Date the transaction was carried out.
- **Net:** Entity through which the transaction is carried out.

Chapter 5
Automatic Accounts Collection

1. Automatic Accounts Collection

The automatic accounts collection immerges from the need to periodically collect the fortnightly accounts from all the TMS devices in the database; this is integrated within the concept of operations over groups.

This is launched every night at 0:00 and first collects from those devices that have never had their accounts collected and secondly from those devices whose data has not been collected in more than 7 days. The application also tries to finish before 7 in the morning. The devices are collected in parallel and the parallel can be graded so that the communication channel is not saturated.

1.1. Installation

Internally, this is linked to the user CRON table in such a way that in order to check that automatic collection is installed, the management user must execute the following command:

```
>crontab -l
```

If the following line appears on the screen:

```
0 0 * * * $TELDATMS/scripts/autocron.sh
```

it is installed.

In order to install the automatic collection, execute the **`$TELDATMS/scripts/install_autocron.sh`** script as management user. This script adds the above line to the user CRON table that starts the automatic collection.

1.2. Start Up

In order to launch the automatic accounts collection, you need to execute the operations over groups manager **tmsgroupop** with the **sincrogetaccounts** operation (NOVACOM, NOVACOM-X25 and Teldat C3B) **sincrogetaccounts46** (Teldat C2 and Teldat C3) (or **getaccounts** if you do not wish to synchronize the devices).

```
$TELDATMS/bin/tmsgroupop -acc [-auto] -o [sincro]getaccounts[46] -f <file> -m
<master> [-hour <HH:MM>]
```

-acc Indicates to the operations over groups manager to update the automatic accounts collection auto table.

-auto The registers in the auto table update as pertaining to the automatic application.

-f <file> File with the group of devices to collect.

-m <master> Master Router where the devices are managed.

sincrogetaccounts Synchronizes the devices before collection.
sincrogetaccounts46
getaccounts Does not synchronize the devices.
getaccounts46

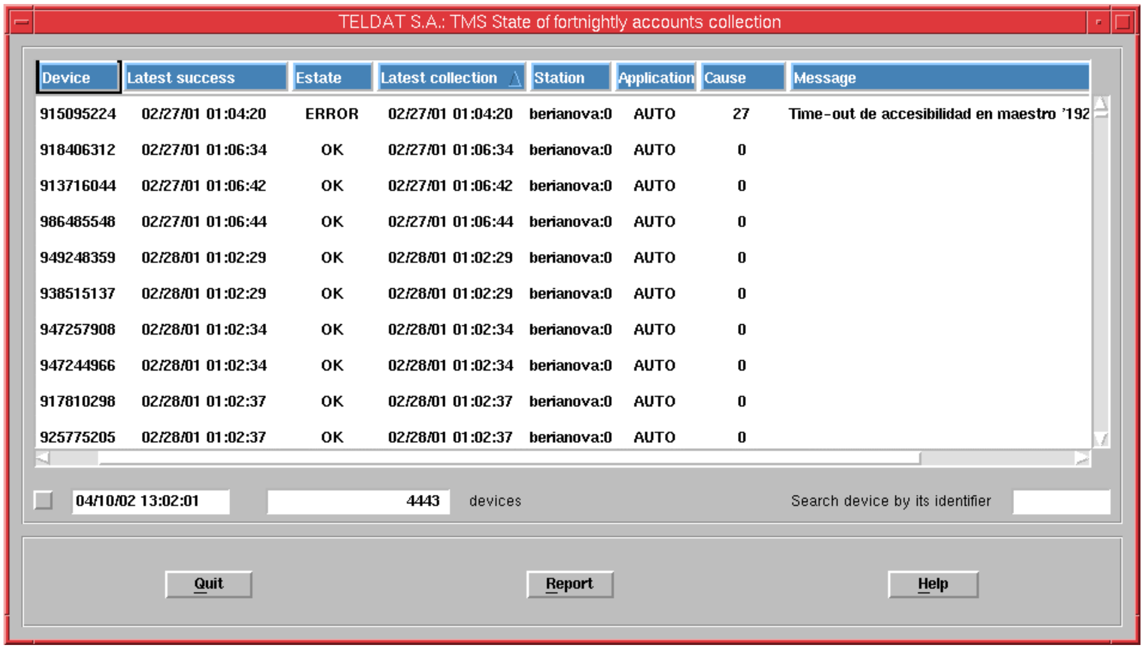
There also exist options pertaining to the collection itself and are configured in the register parameters field from the **getaccounts/getaccounts46** operation in the **go_op** table where the operations over groups are defined.

1.3. Synchronizing the devices

As seen in the previous paragraph, in order to synchronize you need to use the **sincrogetaccounts/sincrogetaccounts46** operation.

1.4. Progress

In order to monitor the collection status for all the devices in the database, use the **tmsmonauto** application whose main screen is shown below:



TELDAT S.A.: TMS State of fortnightly accounts collection

Device	Latest success	Estate	Latest collection	Station	Application	Cause	Message
915095224	02/27/01 01:04:20	ERROR	02/27/01 01:04:20	berianova:0	AUTO	27	Time-out de accesibilidad en maestro '192
918406312	02/27/01 01:06:34	OK	02/27/01 01:06:34	berianova:0	AUTO	0	
913716044	02/27/01 01:06:42	OK	02/27/01 01:06:42	berianova:0	AUTO	0	
986485548	02/27/01 01:06:44	OK	02/27/01 01:06:44	berianova:0	AUTO	0	
949248359	02/28/01 01:02:29	OK	02/28/01 01:02:29	berianova:0	AUTO	0	
938515137	02/28/01 01:02:29	OK	02/28/01 01:02:29	berianova:0	AUTO	0	
947257908	02/28/01 01:02:34	OK	02/28/01 01:02:34	berianova:0	AUTO	0	
947244966	02/28/01 01:02:34	OK	02/28/01 01:02:34	berianova:0	AUTO	0	
917810298	02/28/01 01:02:37	OK	02/28/01 01:02:37	berianova:0	AUTO	0	
925775205	02/28/01 01:02:37	OK	02/28/01 01:02:37	berianova:0	AUTO	0	

□ 04/10/02 13:02:01 | 4443 devices | Search device by its identifier

Figure 75: Monitoring of the automatic accounts collection

The application periodically tests (every 10 seconds by default) the **auto** table content that is updated by the operations over groups manager, the monitoring application (when the fortnightly accounts are read) and the automatic accounts collection application.

If the user clicks over any of the column headers, the application reads all the registers in the table and orders them according to the content of the selected column. If you click again over the same header, the data is reread and the order is inversed.

In the absence of user interactions, the application will only update the registers that have changed since the last reading was carried out and with the said registers, ordering is not carried out when these are modified in the screen.

The user can modify the width of the table columns in order to improve viewing. In order to do this, place the cursor between the two column headers until it's appearance changes to '⬅' and subsequently resize it. When the application starts up again, the sizes of the last execution are maintained.

The significance of the table columns is as follows:

Device Device identifier associated to the register.

Latest success Date and time of the last accounts collection successfully carried out over the device.

Estate Result state of the last collection.

Latest collection Date and time of the last collection carried out over the device.

Station Station identifier where the last collection was carried out (environment variable DISPLAY).

Application Application from where the last collection was carried out. If this is automatic collection, its content will be AUTO, if it is the monitoring application, it will be USR.

Cause ISDN release cause or pseudocause (see "ISDN release causes") associated to the last gathering.

Message Information on the state and causes.

From master router version 1.4.1 onwards, the ISDN release cause is only significant when the number of devices managed in TESTING status in the master router is less or equal to two.

Under the lower left hand corner of the table, an indicator is found for database reading and the current date and time in order to contrast these with those in the table.

Next to the lower right hand corner there is an entry where the user can enter the telephone number of the device he wishes to supervise and the application is selected from the list.

1.5. Results

The execution of the automatic accounts collection is confirmed by consulting the management user mail.

The application sends debugging, information and error messages through the **syslogd** demon from the log system with the facility **local7** and priorities **debug**, **err** and **info**. The user can configure this demon so the messages generated by the application appear on the console, are saved in a file or resent to another station. For further information please consult the Events Logging System.

Also, the final results are saved in the database auto table and can be viewed through the **tmsmonauto** application as previously explained.

Chapter 6
Operations over groups

1. Operations over groups

Operations over groups were conceived as a very powerful tool in order to facilitate the management of the devices, but potentially dangerous if used without extreme care (imagine for example, executing a software teleloading over the whole of the group of devices in the database passing as a parameter an invalid program file). Additionally, the group configuration operations require in-depth knowledge of SQL in order to be able to alter the configurations to be sent in the database. For this reason, sufficiently capable management personnel should always carry out these operations and we recommend that the number of authorized administrators be reduced.

The user wishing to carry out an operation over a subgroup of devices in the database should comply with the following steps:

1. Define the operation.
2. Define the group of devices over which this is applied.
   2.1. Through a file with a device telephone number identifier per line.
   2.2. In the **groups** table in the database with SQL queries.

> ***The operations over groups are always launched with a group file.***

3. If this is a configuration operation …
   3.1. Generate the temporary configuration tables.
   3.2. Modify the configurations to send.
4. Execute the operation over groups.
5. Monitor the progress of the operation.

> ***Simultaneous operations over groups.***
>
> ***The application does support the execution of various simultaneous operations over groups although this is not recommended. However, in configuration operations, it is essential that the groups are separate i.e. a device cannot pertain to more than one group where an operation is being executed. If this requirement is not complied with the temporary configurations of the said devices will be altered depending on the needs of each operation with the last modifications made remaining.***

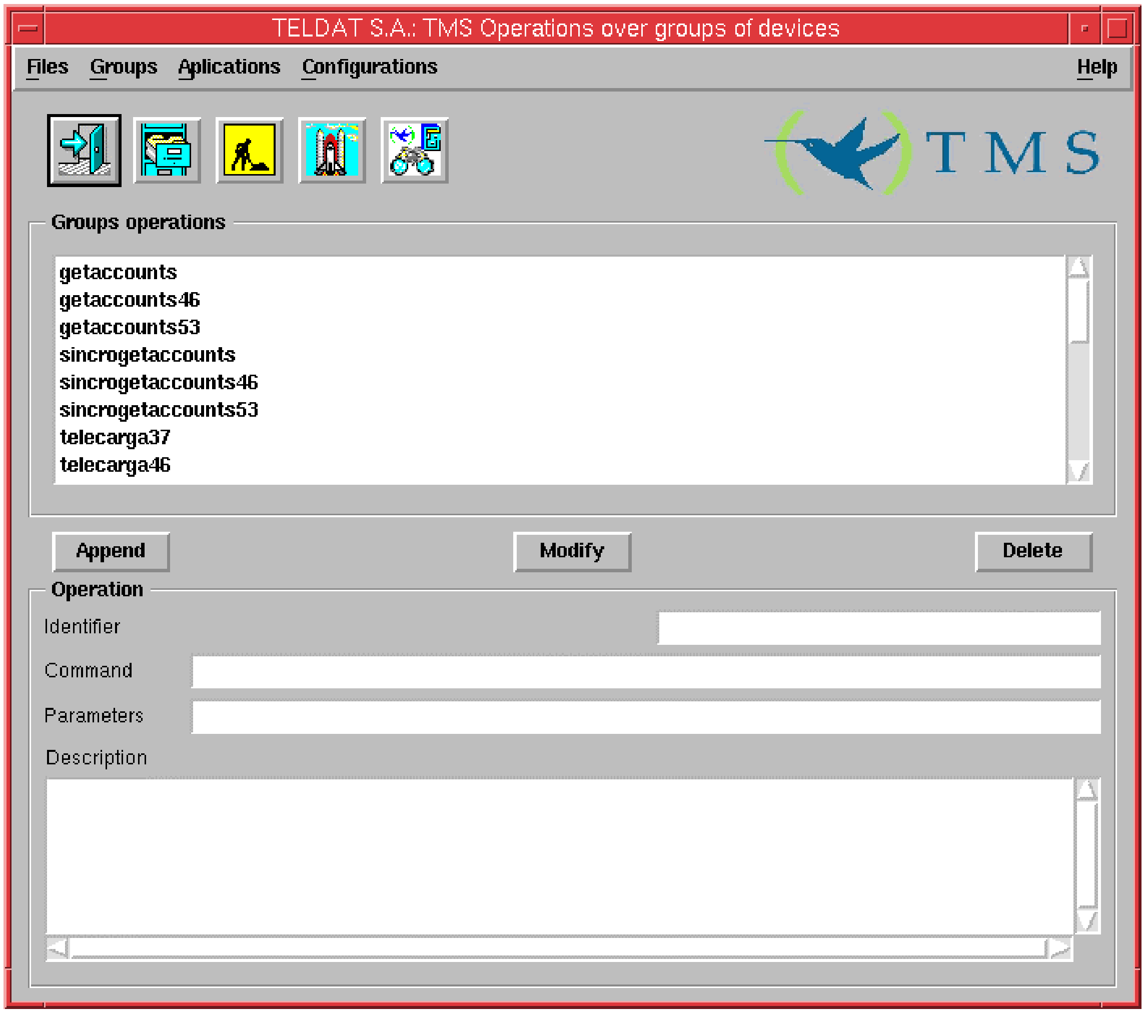
1.1. Definitión of operations over groups

The most common operations are defined In the **go_op** table in the database:

Operation	**Description**
Getaccounts	Collecting of the device's fortnightly accounts and device information parameters for NOVACOM, Teldat C2B and Teldat C3B devices and the ISDN parameters for the Teldat C4I devices.
sincrogetaccounts	Synchronization and collection of fortnightly accounts and device information parameters for NOVACOM, Teldat C2B and Teldat C3B devices and Teldat C3B devices and the ISDN parameters for the Teldat C4I devices.
getaccounts46	Collecting the device's fortnightly accounts and device information parameters for Teldat C2, Teldat C2-UP and Teldat C3 devices.
sincrogetaccounts46	Synchronization and collection of fortnightly accounts and device information parameters for Teldat C2, Teldat C2-UP and Teldat C3 devices.
getaccounts53	Collection of transactions accounts from the Teldat C3 and Teldat C3B devices.
telecarga37	Teleloading of the last version for the NOVACOM devices.
telecarga46	Teleloading of the last version for the Teldat Cx devices.
tmsgetconf51	Configuration request from NOVACOM devices and saving to the database.
tmsgetconf46	Configuration request from Teldat C2 devices and saving to the database.
tmsgetconf53	Configuration request from the Teldat C3 devices and saving to the database.
tmsgetconf57	Configuration request from the Teldat C2B devices and saving to the database.
tmsgetconf60	Configuration request from the Teldat C3B devices and saving to the database.
tmsgetconf68	Configuration request from the Teldat C4I devices and saving to the database.
tmsgetconf72	Configuration request from the Teldat C2-UP devices and saving to the database.
Tmsgetinfo	Obtaining informative parameters from the device.
Tmsreset	Reset the device.
tmssetconf51	Reconfiguration of the NOVACOM devices. Sends the temporary configuration, re-requests this from the device, it is saved in the database, saved to FLASH memory and resets.
tmssetconf46	Reconfiguration of the Teldat C2 devices. Sends the temporary configuration, re-requests this from the device, it is saved in the database, saved to FLASH memory and resets.
tmssetconf53	Reconfiguration of the Teldat C3 devices. Sends the temporary configuration, re-requests this from the device, it is saved in the database, saved to FLASH memory and resets.

tmssetconf57	Reconfiguration of the Teldat C2B devices. Sends the temporary configuration, re-requests this from the devices, it is saved in the database, saved to FLASH memory and resets.
tmssetconf60	Reconfiguration of the Teldat C3B devices. Sends the temporary configuration, re-requests this from the devices, it is saved in the database, saved to FLASH memory and resets.
tmssetconf68	Reconfiguration of the Teldat C4I devices. Sends the temporary configuration, re-requests this from the device, it is saved in the database, saved to FLASH memory and resets.
tmssetconf72	Reconfiguration of the Teldat C2-UP devices. Sends the temporary configuration, re-requests this from the devices, it is saved in the database, saved to FLASH memory and resets.
Tmssettime	NOVACOM, Teldat C2B and Teldat C3B device time set.
tmssettime46	Teldat C2, Teldat C2-UP and Teldat C3 device time set.

Management of groups and operations over groups is executed from the **tmsdefgo** application.



getaccounts
getaccounts46
getaccounts53
sincrogetaccounts
sincrogetaccounts46
sincrogetaccounts53
telecarga37
telecarga46

Figure 76:. Definition of operations over groups

Each operation is characterized by the following fields:

Identifier:
This is a string of characters assigned to the operation.
Admits up to 30 characters.
There cannot be two operations with the same name.

Command:
This is a UNIX command that can correspond to an executable or a shell script. In both cases the call sequence must be:

```
<application> -i <IP address> [-id <device id. >] [-ppid
<ppid>] [-c <SNMP community>] [...]
```

<IP address>	Device IP address.
<device id>	Device identifier (telephone number).
<SNMP community>	Device SNMP community.

The parameters shown in brackets are optional but if they do not indicate the device identifier and the process identifier, the operation status cannot be updated. This admits up to a maximum of 255 characters.

Parameters:
Additional parameters for the above command. Admits up to 255 characters.

Description
Information so the user is aware of the aims of the operation. There are 255 characters available.

In order to **add** a new operation to the list, fill out the fields and press the **Append** button.

In order to **modify** an operation on the list, select it and once the corresponding fields have been altered, press the **Modify** button.

In order to **delete** an operation from the list, select it and press the **Delete** button.

In order to exit the application, press .

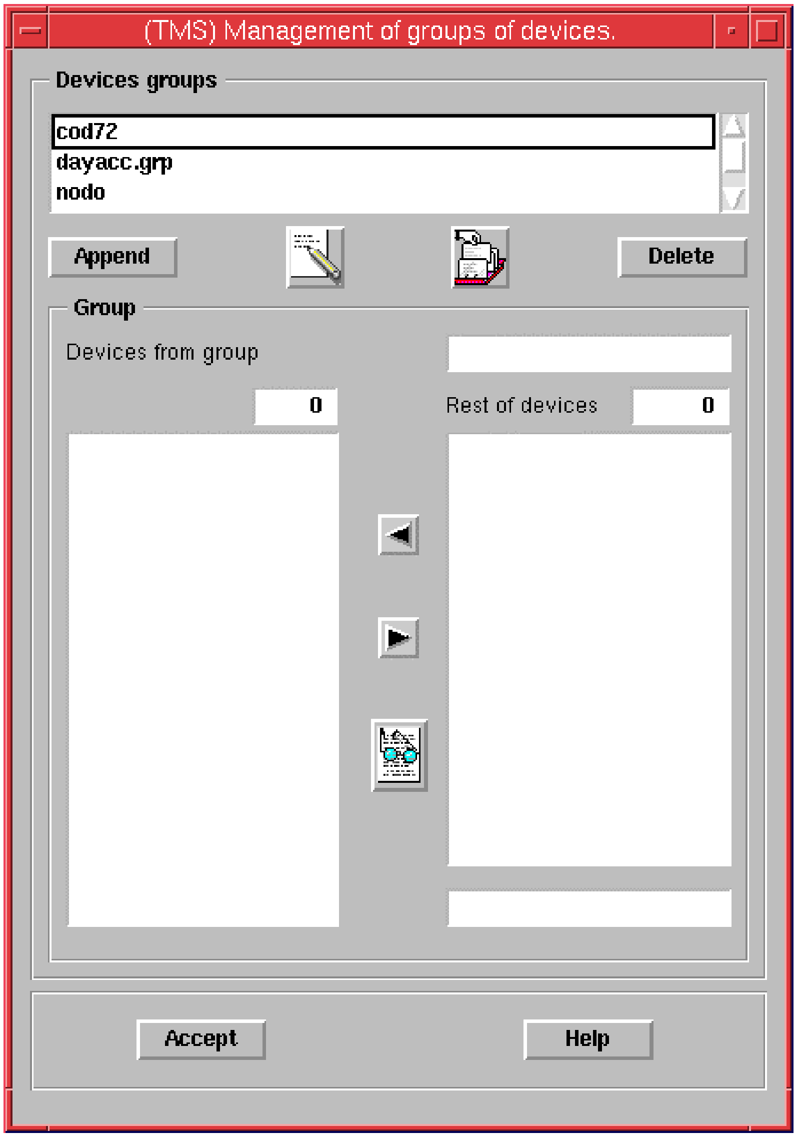
Group management is accessed through the button.

When you wish to modify the temporary configurations sent to the devices, use the button.

In order to launch an operation over groups, press the button.

1.2. Groups Management

Group management is carried out through the following screen that opens from the **tmsdefgo** application through the button:



cod72
dayacc.grp
nodo

Figure 77: Definition of groups

In the above list, the groups defined in the **groups** table in the database appear. When you select a group from this list, its components appear in the lower left hand list and the rest of the devices in the database appear in the lower right hand list, under the cardinals of both lists.

> ***If there are no groups defined then the lists appear empty.***
>
> ***When you add the first group, the devices from the database appear in the lower right hand list.***

In order to ***add*** a new group, enter the name in the identifier field and press the **Append** button.

In order to ***delete*** a group, select it and press the **Delete** button. A confirmation screen will subsequently appear.

In order to ***generate a group file*** from a group in the database, press .

In order to ***add*** the devices from a group file to a group in the database press .

It is essential that all the devices in a file are registered in the **device** table in the devices database.

> ***Si se genera el fichero en un PC o compatible hay que tener en cuenta la diferencia de codificación del retorno de carro en UNIX y DOS (o WINDOWS). Para convertir los ficheros de grupo editados en PC a ficheros UNIX existe el comando UNIX "dos2unix" (consulte las páginas del manual UNIX al respecto).***

In order to ***generate the temporary configurations*** associated to a group and that the user can alter these so they can be sent to the devices, use the button.

Devices can be added or deleted through the arrow buttons that are found among the lists. A multiple selection can be carried out in both lists. In order to select multiple devices, press the <Control> key and without releasing it select the devices with the mouse. In order to select a consecutive group of devices, select the first one with the mouse, press the upper case key and without releasing it, select the last one.

In order to **search** for a device, you can enter the device telephone number in the text box located blow the right hand list and the device closest to this will be shown at the top of the list.

You can also generate groups from the SQL queries in the SQL*Plus® application that can be launched from the operations over groups definition screen through the button.

Let's take a look at some examples:

1. Group of all the Madrid devices:

```
(tmsgrp)SQL>insert into groups
  2  select 'madrid', id from device
  3  where id like '91%';
```

2. Group containing all the devices that have been operating for more than one day (8640000 hundredths of seconds):

```
 (tmsgrp)SQL>insert into groups
  2  select 'mas_de_un_dia', id from infodevice
  3  where sysuptime > 8640000;
```

3. Devices whose accounts have not been collected in more than 7 days:

```
 (tmsgrp)SQL>insert into groups
  2  select 'acc_mas_7', id from auto
  3  where datetime < (sysdate - 7);
```

> ***Warning!***
>
> ***The operation always works with a group file, therefore the group must be dumped in a file before executing it. For this reason, it is worthwhile maintaining the group files and the groups in the database up to date and that both contain the same devices.***

1.3. Configuration Operations for device groups

Before initiating the operation, you need to define the group as indicated in the previous section. Subsequently, the temporary configurations are generated. These are copies of the originals and the user may alter them if he so wishes. In order to generate these, press the button.

When you wish to modify the temporary configurations which are sent to the database, use the button.

A screen with the ORACLE SQL*Plus® prompt will appear. This is an SQL interpreter from where you can alter the tables. The connection to the database is carried out as a **tmsgrp** user of group management. This user can consult the **tms** user tables, this is the main TMS management user, but this user can only alter the temporary configuration tables. Before modifying the temporary configurations, it is essential that these be generated from the group management screen from the **tmsdefgo** application.

All the actions executed from the SQL*Plus® screen are saved in the **`$TELDATMS/log/tmsgrp.log`** file.

In order to facilitate the task of the operations over groups administrator (**tmsgrp** user), SQL scripts have been created in the **`$TELDATMS/etc`** directory.

a) Example of configuration operations over groups

Below you can see some typical examples of temporary configuration modifications. For these examples, we will work with the **maqueta_teldat** group made up of a single device with telephone number **918060405**. This group is created by following the indications given in section "Group Management" and this must also be saved in the file with the same name.

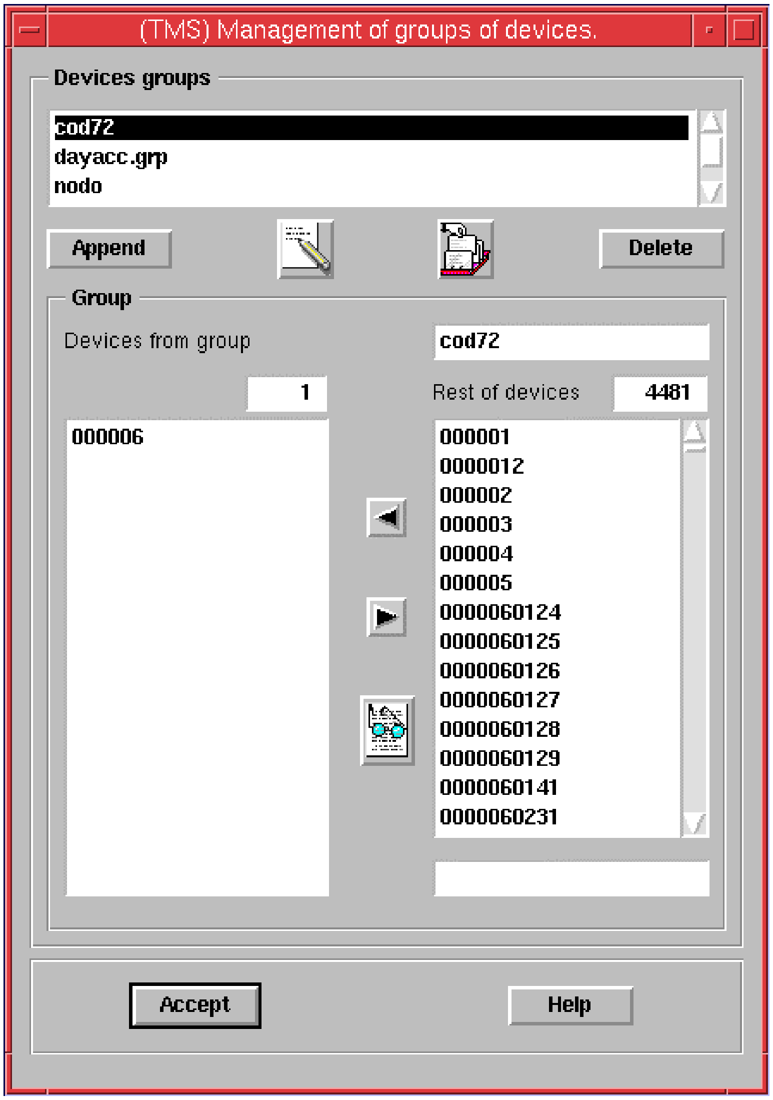
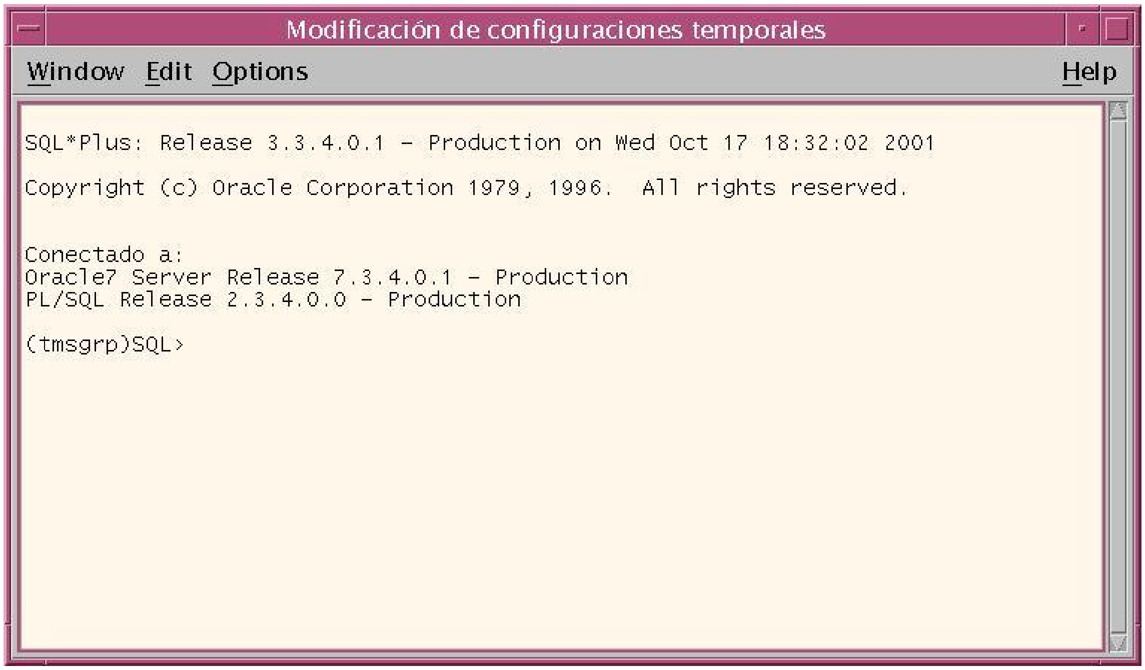


Figure 78: 'cod72' example group

In order to generate the group's temporary configurations, select it and press 🖨.

In order to modify the temporary configurations press the button and the following screen will appear:



```
SQL*Plus: Release 3.3.4.0.1 - Production on Wed Oct 17 18:32:02 2001

Copyright (c) Oracle Corporation 1979, 1996.  All rights reserved.


Conectado a:
Oracle7 Server Release 7.3.4.0.1 - Production
PL/SQL Release 2.3.4.0.0 - Production

(tmsgrp)SQL>
```

Figure 79: ORACLE-SQL *PLUS. Modification of temporary configurations

Let’s take a look at some typical cases (the text written in bold represents the commands that the user must introduce).

The description of the authorized masters temporary table **conf37_masters** is as follows:

```
(tmsgrp)SQL>desc conf37_masters
Nombre                          ¿Nulo?   Tipo
------------------------------- -------- ----
NAME                                     VARCHAR2(80)
TEL                                      VARCHAR2(19)
IPADD                                    VARCHAR2(15)
USR                                      VARCHAR2(31)
PASSWD                                   VARCHAR2(31)
CONTEL                                   VARCHAR2(19)
IPMASK                                   VARCHAR2(15)
CGIPADD                                  VARCHAR2(15)
CGIPMASK                                 VARCHAR2(15)
```

- ***Insertion of a new master router authorized for all the devices in a group***

```
 (tmsgrp)SQL>@../db37/es/showconf 918060405

                                                      Configuración "918060405"
Maestros autorizados
Teléfono   Dirección IP    Máscara IP      Usuario         Contraseña Tel. Conex Subred CG       Máscara CG
---------- --------------- --------------- --------------- ---------- ---------- --------------- ---------------
936578457  195.53.0.189                    tmsman@teldat   devpasswd   915792000
911234568  195.235.254.36                  tmsman@operlab  devpasswd   915792000
917004310  10.130.130.5                    tmsman@cgtms    devpasswd   915792000
917004311  10.130.130.5    255.255.255.0   tmsman@cgtms    devpasswd   915792000 193.5.6.0       255.255.255.0
916080105  195.53.0.189                    tmsman@teldat   devpasswd   915792000

(tmsgrp)SQL>@../db37/es/insert_master
Grupo al que se añade el maestro autorizado: maqueta_teldat
Telefono del router maestro: 916080105
Direccion IP del router maestro: 193.53.0.189
Mascara IP del router maestro: 255.255.0.0
Usuario: tmsman@teldat
Contraseña: devpasswd
Telefono de conexion de gestion: 915792000
Subred de gestion: 192.6.34.0
Mascara IP de subred de gestion: 255.255.255.0

Procedimiento PL/SQL terminado con éxito.

(tmsgrp)SQL>@../db37/es/showconf 918060405
                                                      Configuración "918060405"
Maestros autorizados
Teléfono   Dirección IP    Máscara IP      Usuario         Contraseña Tel. Conex Subred CG       Máscara CG
---------- --------------- --------------- --------------- ---------- ---------- --------------- --------------
936578457  195.53.0.189                    tmsman@teldat   devpasswd   915792000
911234568  195.235.254.36                  tmsman@operlab  devpasswd   915792000
917004310  10.130.130.5                    tmsman@cgtms    devpasswd   915792000
917004311  10.130.130.5    255.255.255.0   tmsman@cgtms    devpasswd   915792000 193.5.6.0       255.255.255.0
916080105  195.53.0.189                    tmsman@teldat   devpasswd   915792000
916080105  193.53.0.189                    tmsman@teldat   devpasswd   915792000 192.6.34.0      255.255.255.0
```

- ***Modification of an authorized master router for all the devices in a group***

```
 (tmsgrp)SQL>@../db37/es/showconf 918060405



                                                     Configuración "918060405"
Maestros autorizados
Teléfono  Dirección IP   Máscara IP      Usuario            Contraseña Tel. Conex Subred CG      Máscara CG
--------- -------------- --------------- ------------------ ---------- ---------- -------------- ---------------
911234568 195.235.254.36 255.255.255.224 tmsman@operlab     devpasswd  915792000  195.235.254.32 255.255.255.224
917004310 10.130.130.5   255.255.255.224 tmsman@cgtms       devpasswd  915792000  195.235.254.0  255.255.255.224
917460127 192.168.30.4   255.255.255.0   tmsman@cgtms       devpasswd  915792000  192.168.30.0   255.255.255.0
917460228 192.168.30.5   255.255.255.0   tmsman@cgtms       devpasswd  915792000  192.168.30.0   255.255.255.0
916080105 195.53.0.189   255.255.255.255 tmsman@teldat      devpasswd  915792000  195.53.0.105   255.255.255.255


(tmsgrp)SQL>update conf37_masters
  2  set usr = 'gestion@newusr',
  3  passwd = 'newpasswd'
  4  where tel = '916080105' and name in (select rdsi from groups where name = 'maqueta_teldat');

1 fila actualizada.

(tmsgrp)SQL>commit;
(tmsgrp)SQL>@../db37/es/showconf 916080105

                                                     Configuración "918060405"
Maestros autorizados
Teléfono  Dirección IP   Máscara IP      Usuario            Contraseña Tel. Conex Subred CG     Máscara CG
--------- -------------- --------------- ------------------ ---------- ---------- ------------- ---------------
911234568 195.235.254.36 255.255.255.224 tmsman@operlab     devpasswd  915792000  195.235.254.32 255.255.255.224
917004310 10.130.130.5   255.255.255.224 tmsman@cgtms       devpasswd  915792000  195.235.254.0  255.255.255.224
917460127 192.168.30.4   255.255.255.0   tmsman@cgtms       devpasswd  915792000  192.168.30.0   255.255.255.0
917460228 192.168.30.5   255.255.255.0   tmsman@cgtms       devpasswd  915792000  192.168.30.0   255.255.255.0
916080105 195.53.0.189   255.255.255.255 gestion@newusr     newpasswd  915792000  195.53.0.105   255.255.255.255


(tmsgrp)SQL>quit
```

- ***Delete an authorized master router for all the devices in a group***

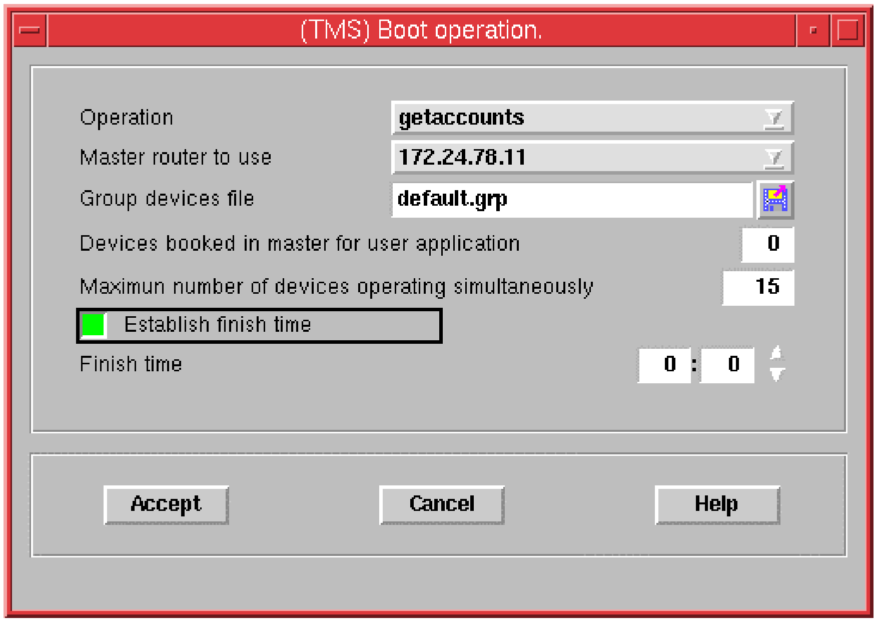
```
(tmsgrp)SQL>@../db37/es/showconf 918060405
                                                      Configuración "918060405"

Maestros autorizados
Teléfono  Dirección IP   Máscara IP      Usuario            Contraseña Tel. Conex Subred CG      Máscara CG
--------- -------------- --------------- ------------------ ---------- ---------- -------------- ---------------
911234568 195.235.254.36 255.255.255.224 tmsman@operlab     devpasswd  915792000  195.235.254.32 255.255.255.224
917004310 10.130.130.5   255.255.255.224 tmsman@cgtms       devpasswd  915792000  195.235.254.0  255.255.255.224
917460127 192.168.30.4   255.255.255.0   tmsman@cgtms       devpasswd  915792000  192.168.30.0   255.255.255.0
917460228 192.168.30.5   255.255.255.0   tmsman@cgtms       devpasswd  915792000  192.168.30.0   255.255.255.0
916080105 195.53.0.189   255.255.255.255 gestion@newusr     newpasswd  915792000  195.53.0.105   255.255.255.255


(tmsgrp)SQL>delete from conf37_masters
  2  where tel = '916080105' and name in (select id from groups where name = 'maqueta_teldat');

1 fila borrada.

(tmsgrp)SQL>commit;

(tmsgrp)SQL>@../db37/es/showconf

                                                      Configuración "918060405"
Maestros autorizados Teléfono Dirección IP Máscara IP Usuario Contraseña Tel. Conex Subred CG Máscara CG
-------------------- -------- ------------ ---------- ------- ---------- -------------------- ---------------
911234568 195.235.254.36 255.255.255.224 tmsman@operlab  devpasswd 915792000  195.235.254.32  255.255.255.224
917004310 10.130.130.5   255.255.255.224 tmsman@cgtms    devpasswd 915792000  195.235.254.0   255.255.255.224
917460127 192.168.30.4   255.255.255.0   tmsman@cgtms    devpasswd 915792000  192.168.30.0    255.255.255.0
917460228 192.168.30.5   255.255.255.0   tmsman@cgtms    devpasswd 915792000  192.168.30.0    255.255.255.0

(tmsgrp)SQL>quit
```

When you wish to send configurations saved in the database to a group of devices, use the **tmssetconf37** operation from the database.

> ***Confirmation of SQL sentences.***
>
> ***All sentences that modify table registers must be confirmed with the order "commit" (or be rectified with the order "rollback") before launching the operation.***
>
> ***When you exit SQL*Plus® with the "quit" order, a "commit" is produced implicating all sentences in the session.***

1.4. Executing operations over groups

In order to launch an operation over groups, press the 🚀 button in the main **tmsdefgo** application screen.



(TMS) Boot operation.

Operation	getaccounts
Master router to use	172.24.78.11
Group devices file	default.grp
Devices booked in master for user application	0
Maximun number of devices operating simultaneously	15
☑ Establish finish time	
Finish time	0 : 0

Figure 80: Executing operations over groups

Operation:

Identifier of the operation over groups to launch.

All the operations contained in the **go_op** table in the database are displayed..

Master Router to use:

This is the master router where all the devices in the group are managed in order to apply the operation.

Group devices file:

Complete file name where the group of devices over which the operation is applied is defined. The format is one identifier per line.

If you press the 💾 button, a group file selection screen appears.

Devices booked in master for user application:

By default, the operations over groups manager uses the maximum capacity of the master router to manage the devices. Currently, the master router can simultaneously manage up to 50 devices. If a device has not been reserved for user application (default value), the manager of the operations over groups will monopolize the master router for himself and will not leave any “space” so the user can manage any device. If, for example, the value is 10, then the manager will try to always leave 10 "spaces" so the user can manage devices. Values within the range [0 .. 50] are admitted.

Maximum number of devices operating simultaneously:

This parameter is introduced to prevent the saturation of the communications channel in the management station. The number of devices in the states TESTING, REACHABLE or OPERATING pertaining to this application can never exceed this value.

The default value is 100, which practically implies no limit.

Establish finish time:

If an end time is established, the operation over groups will not manage any device after the said time and will end when it has finished processing those that are already under management. If the end time is previous to start up then it is supposed that this pertains to the following day.

When the operation is launched, the application sends all the management orders possible to the master router guaranteeing that a number of "spaces" are left free equal to the "devices booked for manual application" parameter and not exceeding at any moment the "Maximum number of devices simultaneously operating". If the devices have a static IP address, management will first be attempted through this and if this fails then through the master.

The application waits for some four minutes so that each device being managed enters a REACHABLE state. If this does not occur then this is abandoned due to timeout.

When the device enters a REACHABLE state, the operations manager launches the operation and sends the de-management order to the master router, as the traffic generated by the operation itself should maintain the connection. This then permits another device to be put under management thus optimizing the speed of the operations over groups.

The operation over groups management finishes when it has applied the operation to all the devices in the group that have achieved a REACHABLE state or when an error has been produced in the communication or the user has interrupted consequently preventing the management to continue working.

The buttons on the screen provoke the following actions:

Accept Presents a screen requesting the security password. Only those users who know the password can execute an operation over groups. If you wish to change the password execute the **$TELDATMS/bin/tmsgrpwd** application.

Cancel Closes the screen canceling the operation.

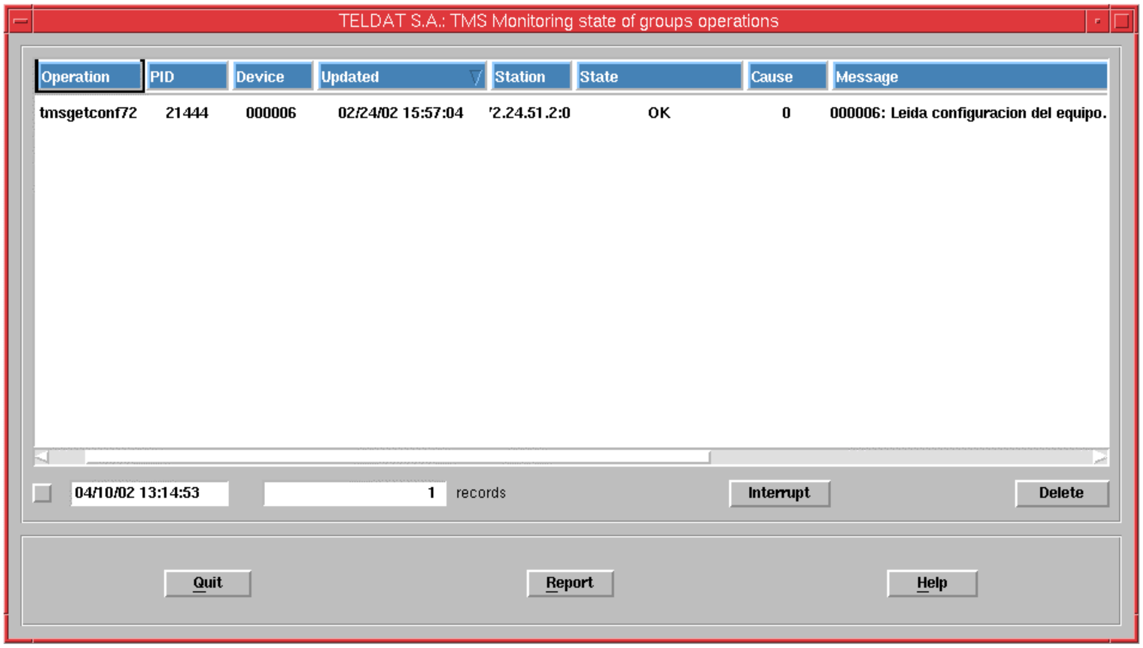
Help Presents the help screen.

> ***If a user enters the password screen and then decides not to continue and wishes to cancel the operation, simply press Accept with either an incorrect password or leave the field blank.***

1.5. Monitoring operations over groups

In the same way as the rest of the TMS management applications, the operations over groups send messages to the system log demon (syslogd) so this transmits them depending on the configuration file.

The **tmsmongo** application is used to monitor the state of the operations over groups.



TELDAT S.A.: TMS Monitoring state of groups operations

Operation	PID	Device	Updated	Station	State	Cause	Message
tmsgetconf72	21444	000006	02/24/02 15:57:04	'2.24.51.2:0	OK	0	000006: Leida configuracion del equipo.

04/10/02 13:14:53

1 records

Figure 81: Monitoring operations over groups

The application periodically queries (every 10 seconds by default) the content of the **go_log** table, which is updated by the operations over groups manager and by the operations themselves when they end or establish error conditions.

If the user clicks over any column header, the application reads all the registers in the table and orders them according to the content of the selected column. If the column header is clicked again, the application re-reads the data and inverses the order.

In the absence of user interactions, the application will only update the registers that have changed since the last reading was carried out and with the said registers, ordering is not carried out when these are modified on the screen.

The user can modify the width of the table columns in order to improve viewing. In order to do this, locate the cursor between the two column headers until it's appearance changes to '⇦' and subsequently resize it. When the application starts up again, the sizes of the last execution are maintained.

The meanings of the table columns are as follows:

Operation This is the operation identifier associated to that registered in the table.

PID (Process Identifier) UNIX process identifier assigned to the **groupop** application for operations over groups.

Device Device ISDN telephone associated to the register.

Updated Date and time of the last register update.

Station Station identifier from where the operation over groups was launched.

State Current state of the operation as regards the device associated to the register (see table).

Cause ISDN release cause or pseudocause (see "ISDN release causes") associated to the register. If the status is error, this can help determine the cause.

Message Information on the status and causes.

Suboperation Contains the name of the application that leaves the message in cases where the main operation launches new applications.

States of the registers in the operations over groups table:

Numeric value	State	Meaning
-8	**DE-MANAGED**	The device has been unexpectedly de-managed (e.g. if the user enters through TELNET or the console in the master router and de-manages it).
-7	**OP ERROR**	The operation launched over the device has terminated with an error. The **go_op** table "message" field provides the user with information on the cause. These can also be consulted through the log files.
-6	**INACCESSIBLE**	The accessibility time period has timed out (approximately 4 minutes) without the device obtaining an IP address.
-5	**BUSY**	The device is being managed by another application.
-4	**SNMP TIME-OUT**	An SNMP petition has been sent to the device and the wait period has timed out.
-3	**SNMP ERROR**	An error in an SNMP petition to the router has occurred.
-2	**MASTER TIME-OUT**	The master does not respond to petitions from the table of the devices being managed. This state is reached when 3 cycles of attempt/wait configured for the master router have been produced. Example: the master router has 2 attempts of 5 seconds configured in its SNMP petitions; therefore this state is reached after 30 seconds and 6 attempts. This state provokes the termination of the operation over groups.
-1	**MASTER ERROR**	An error has been produced in obtaining the managed devices table under management from the master. This state provokes the termination of the operation over groups.
0	**WAITING**	The device is waiting for a free "space" in the master in order to be managed.

1	**MANAGING**	The management order has been sent to the master but is still not in the table for the devices under management read from the master.
2	**TESTING**	The device has been managed over the master and is now in its devices under management table.
3	**REACHABLE**	The device is in an accessible state and the operation over group manager immediately executes an operation over it.
4	**OPERATING**	An operation has been launched over the device and has been de-managed in the master. The operation over groups manager has finished its task with the device.
5	**OK**	Operation over the device has successfully concluded.
6	**PAUSED**	The end time has timed out before processing this device.
7	**INT USR**	The user has interrupted the operation over groups before the operation over this device has been executed. This state provokes a termination of the operation over groups.

From master router version 1.4.1 onwards, the ISDN release cause is only significant when the number of managed routers in the TESTING state in the master router is less or equal to two.

Below the lower left hand corner of the table you can find the database read progress bar and the current date and time in order to contrast these with those in the table. To the right, the number of registers contained in the table is displayed. The higher the number of registers means slower times for queries and more traffic in the network. We recommend that the contents of the table be frequently deleted. If you wish to save the histories, you can generate reports or insert the registers in another auxiliary table that is not habitually consulted.

You can also generate a report from a text file by pressing the **Report** button. Subsequently, the user will be asked to indicate the destination file for the report and afterwards a format such as the one shown below is generated:

```
TELDAT, S.A.: Estado de operaciones sobre grupos de equipos TMS.

                             Fecha
Operacion  PID    Equipo     y hora      Estacion  Estado      Causa  Mensaje
---------  -----  ---------- ----------  --------  ----------  -----  -------
getinfo    11687  944352129  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944352195  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944396488  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944535085  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944544224  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944535225  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944535060  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944483315  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944483364  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944483369  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944483367  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944598032  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701961  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701973  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701969  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944723426  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701978  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701885  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944598638  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701273  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06

getinfo    11687  944701851  23/06/1999  daisy:0   ESPERANDO   0
                             18:01:06
```

In order to interrupt an operation over groups that is being executed, select any of its registers and press the **Interrupt** button. The application will execute the call to the system **`kill -QUIT <PID>`** where the PID is the process identifier associated with the operation.

The table registers are selected with the left hand mouse button and de-selected with the center button. In order to select a range of registers, select the first one required, hold down the upper case key and select the last register required. If you wish to remove some of these, use the center mouse button.

In order to **delete** registers from the table, select them and press the **Delete** button.

Chapter 7
ORACLE Database

1. Tables used in the database

The TMS Management uses an ORACLE database where the following tables are defined:

acc<device_code>_<entity>	Tables with the fortnightly accounts that the operator has saved from the devices in the database. In the C3 and C3B routers, these are used to save the transactions from the point of sales terminals.
conf<device_code>_<entity>	Tables that save the configurations of the devices with device code <device_code>.
infomanaged	Table containing the **managed** table as well as all the devices that are being managed through their static IP addresses.
infodevice	Device information table: series number, motherboard number, software version, and BIOS version.
managed	Table indicating which devices are being managed by each master.
mancalls	Table containing the duration of all the management calls.
master	Table of the available master routers.
device	Table of the available devices.

These tables are available for the user in order to be exported to other formats or databases in order to generate reports or construct any other application over them.

The management connects to the database as **tms** user as soon as it is identified by the **ORATMS** environment variable.

You can also create a user, **tmsmon,** for monitoring the database tables however this does not provide authorization to modify objects.

All the tables are the property of the **tms** user. For this reason, if the group administrator i.e. the **tmsgrp** user wishes to refer to them, he must be placed ahead of the proprieter. However in order to simplify the administer's task, synomyns have been defined for the **tmsgrp** user. All the **tms.tmp_conf<device_code>_<entity>** tables can be refered to from the said user as **conf<device_code>_<entity>.**

For example,

```
(tmsgrp)SQL>select * from conf37_masters;
```

is the same as

```
(tmsgrp)SQL>select * from tms.tmp_conf37_masters;
```

When the user wishes to execute a configuration operation over the groups, he alters the temporary configuration tables. The operations manager puts the device under management and sends the temporary configuration, this is saved in the FLASH memory and then this is requested once more so this is saved again this time in the main tables in the database. Finally the device is reset in order to start up with the new configuration.

2. Updating the Database

The **tmssynchro** process is executed in the background and carries out the SNMP petitions to the master routers defined in the database **master** table. From the responses received, the state of the devices under management is obtained and the database updated with these values.

When the **tmsmanager** application is initiated, it checks if this process is being executed or not. If it is not being executed there exists the option to initiate it from the application itself.

It is only necessary to execute one **tmssynchro** process in each management station. If you execute this in more than once this involves considerable prejudice in the station features but does not cause any damage.

> ***NOTE: "tmssynchro" Process.***
>
> ***If this process is not executed, the database does not update and the rest of the applications querying this do not operate correctly.***

Further to this process, the automatic updating of some of the tables is carried out through a series of triggers (operations that are executed when certain events are produced in the database):

UPDATE_AUTO
UPDATE_GO_LOG
UPDATE_INFOMANAGED
UPDATE_MANCALLS
UPDATE_MANINFOMANAGED
UPDATE_MASTER
UPDATE_DEVICE

In order to verify that all these are installed and operating, you can execute the **`$TELDATMS/etc/db/showtriggers.sql`** script

3. Backup Copies

In order to restore the database contents in cases of hardware or software failure where damage has been caused, it is a good idea to carry out periodic backups.

The strategy for maintaining backups strongly depends on the type of database you wish to conserve, the characteristics of the station being managed and the use made of it.

Taking into consideration the typical TMS management operations, with reference to the database, in the reference {Velpuri, 95} we recommend that you follow the following rules:

1. Carry out a physical backup off line each time a management application updating occurs.
2. Carry out daily exporting at times when it is little used (at night for example).
3. Verify the said exports, at least once a week, imported in the local database of another station.
4. Depending on the database activity, compact the tables by carrying out an export, deleting and importing once a month or each few months.

3.1. Database physical backup off line

An off line physical backup consists in copying all the files with the database shut down. Carry out the following steps for this.

First, you need to identify the files that require conserving. For this purpose, execute the **$TELDATMS/script/tmsfiles.sh** script which produces the **$TELDATMS/etc/db/OFFLINEBACKUP.FILES** file as a result. Edit the said file in order to eliminate a couple of lines that do not contain the file names at the beginning and at the end. Subsequently add the following to the said files:

```
$ORACLE_HOME/initGEST.ora
$ORACLE_HOME/configGEST.ora
listener.ora
tnsnames.ora
```

Following that and before shutting down the database, it is advisable to inform the users who have a session open in the database and stop all the management applications (including the **tmssynchro**).

In order to detain the database, execute the following commands:

```
>svrmgrl
svrmgrl>connect internal
svrmgrl>shutdown immediate
```

If everything has gone smoothly, a message is returned indicating that the database is shutdown.

Enter as proprietary user of the ORACLE software and make copies of the files to tape through the command:

```
>tar cvf /dev/rmt/0m -I $TELDATMS/etc/db/OFFLINEBACKUP.FILES
```

In order to restart the database again:

```
svrmgrl>startup
```

3.2. Exporting the database

The **$TELDATMS/script/tmsexportdb.sh** script exports the TMS database tables to the **$TELDATMS/accounts/expdat.dmp** file. This script can be launched from a terminal or from the configuration application with the **Database->Export** option.

There are various types of possible exports: complete, by user or by tables. The decision here has been taken to use user export as this is considered the most appropriate in this case.

Import recommended in cases of total disaster consists in executing, as management user, the command:

```
> $TELDATMS/script/tmsimportdb.sh -drop
```

which destroys the current tables in the database (thus losing the data in use) which are created again and compacted in the import data process from the **$TELDATMS/accounts/expdat.dmp** file.

If you do not wish to lose the data in use nor destroy the tables, you can use this without the **-drop** option.

If critical files in the database have been damaged, these need to be recovered from the physical backup off line. In this case, the database is shutdown and the files restored. Subsequently importing is carried out for the data as previously indicated.

3.3. Backup of all the TMS management data

The **$TELDATMS/script/tmsbackup.sh** script exports all the database information pertaining to the management user over the **$TELDATMS/accounts/expdat.dmp** file. Subsequently the **$TELDATMS/accounts** directory (where the fortnightly accounts files are found and the destination file for the database export) and the **$TELDATMS/cfgs** (where the device configurations are found which can also be duplicated in the database) are saved in a **tar** file. These directories are not saved with the complete route but with the relative one so they can be restored in any directory. This operation can be launched from a terminal or from the configuration application with the **Files->Backup TMS** option.

The previous script is prepared so that, with small modifications, after saving all the important data in a **tar** file, it can be sent to the designated station.

Once the **tar** file has been generated, you can save this in the magnetic band with the following root command:

```
#cp $TELDATMS/accounts/tmsbackup.tar /dev/rmt/0m
```

3.4. Recovering data in case of disaster

In order to recover data in cases of disaster, proceed in the following way:

1. Depending on the restoration source:

   1.1 From the magnetic band:

```
>cd $TELDATMS
>tar xvf /dev/rmt/0m
```

   1.2 From file:
   Supposing that the file in question is the tmsbackup.tar:

```
>cp tmsbackup.tar $TELDATMS
>cd $TELDATMS
>tar xvf tmsbackup.tar
```

2. Importing the data from the database:

```
>cd $TELDATMS/script
>tmsimportdb.sh -drop
```

Chapter 8
Events Logging System

1. Events Logging System

The various applications making up the TMS Management Center send debugging, information and error messages through the system's **syslogd** demon with the **local7** feature and priorities **debug**, **err** and **info**. The user can configure this demon so it is presented on screen, it is saved in file or resent to another station the messages generated by the application. For example, the following lines in the file "/etc/syslog.conf"...

```
# Para log de TMS.
local7.debug   /dev/console
local7.info    /$TELDATMS/log/tms.log
local7.err     @sharon
```

... ensure that all the messages are shown on the console. The information and error messages are saved in the "/$TELDATMS/log/tms.log " file and the error messages are resent to the station "sharon".

The applications head their messages with the following structure:
TELDAT:<application>(<display>)[<PID>] where <display> is the station identifier where the application is being executed.

For example, the following lines have been taken from the "cantabria" station log file:

```
May 22 18:06:00 cantabria TELDAT:tmssynchro(daisy:0)[6807]: Termina tmssynchro.
May 22 18:06:05 cantabria TELDAT:tmssynchro(daisy:0)[9363]: Comienza tmssynchro.
May 22 18:06:05 cantabria TELDAT:tmssynchro(daisy:0)[9363]: Modo charlatan.
May 22 18:06:27 cantabria TELDAT:tmsconfig51(goliat:0)[9373]: Leida configuracion
del equipo 918060666.
May 22 18:08:18 cantabria TELDAT:tmsconfig51(goliat:0)[9373]: Leida configuracion
del equipo 918060466.
May 22 18:08:18 cantabria TELDAT:tmsconfig51(goliat:0)[9373]: Enviada configuracion
 al equipo 918060466.
May 22 18:14:22 cantabria TELDAT:tmsconfig51(goliat:0)[9615]: Leida configuracion
del equipo 918060466.
May 22 18:15:13 cantabria TELDAT:tmsconfig51(goliat:0)[9615]: Leida configuracion
del equipo 918060466.
May 22 18:15:13 cantabria TELDAT:tmsconfig51(goliat:0)[9615]: Enviada configuracion
al equipo 918060466.
May 22 18:15:33 cantabria TELDAT:tmsconfig51(goliat:0)[9615]: Leida configuracion
del equipo 918060466.
May 22 18:15:33 cantabria TELDAT:tmsconfig51(goliat:0)[9615]: Enviada configuracion
al equipo 918060466.
May 22 18:35:24 cantabria TELDAT:tmsconfig51(goliat:0)[10187]: Leida configuracion
del equipo 918060466.
May 25 18:23:05 cantabria TELDAT:tmsconfig51(goliat:0)[11486]: Leida configuracion
del fichero ../cfgs/918060705.cfg.
May 25 18:35:13 cantabria TELDAT:tmsconfig51(goliat:0)[12341]: Leida configuracion
del fichero ../cfgs/918060705.cfg.
May 27 09:44:08 cantabria TELDAT:tmsconfig51(goliat:0)[6532]: Leida configuracion
del equipo 942876789.
May 27 09:47:00 cantabria last message repeated 3 times
May 27 09:49:09 cantabria TELDAT:tmsconfig51(goliat:0)[6662]: Leida configuracion
del equipo 937896788.
```

```
May 27 10:07:01 cantabria TELDAT:tmsconfig51(goliat:0)[6662]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 11:16:59 cantabria TELDAT:tmsconfig51(goliat:0)[9231]: Leida configuracion
del equipo 942873456.
May 27 11:48:46 cantabria TELDAT:tmsconfig51(goliat:0)[9829]: Leida configuracion
del equipo 942873456.
May 27 11:49:02 cantabria TELDAT:tmsconfig51(goliat:0)[9829]: Guardada configuracion
en el fichero ../cfgs/1234.cfg.
May 27 11:49:08 cantabria TELDAT:tmsconfig51(goliat:0)[9829]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 11:56:52 cantabria TELDAT:tmsconfig51(goliat:0)[10230]: Leida configuracion
del equipo 942873456.
May 27 11:57:06 cantabria TELDAT:tmsconfig51(goliat:0)[10230]: Guardada
configuracion en el fichero ../cfgs/1234.cfg.
May 27 11:57:12 cantabria TELDAT:tmsconfig51(goliat:0)[10230]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 12:00:16 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Leida configuracion
del equipo 942873456.
May 27 12:00:28 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Guardada
configuracion en el fichero ../cfgs/1234.cfg.
May 27 12:00:34 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 12:00:43 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Guardada
configuracion en el fichero ../cfgs/1234.cfg.
May 27 12:00:49 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 12:00:58 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Guardada
configuracion en el fichero ../cfgs/1234.cfg.
May 27 12:01:07 cantabria TELDAT:tmsconfig51(goliat:0)[10434]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 12:05:49 cantabria TELDAT:tmsconfig51(goliat:0)[10649]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 12:05:59 cantabria TELDAT:tmsconfig51(goliat:0)[10649]: Guardada
configuracion en el fichero ../cfgs/1234.cfg.
May 27 12:06:05 cantabria TELDAT:tmsconfig51(goliat:0)[10649]: Leida configuracion
del fichero ../cfgs/1234.cfg.
May 27 13:23:49 cantabria TELDAT:tmsconfig51(goliat:0)[10667]: Leida configuracion
del equipo 942873456.
```

The name that comes after “TELDAT” is the application generating the messages and the number between brackets is its process identifier (PID).

Chapter 9
Appendix

1. Revisions

1.1. Version 1.0.0

First TMS management revision that manages the NOVACOM and NOVACOM-X25 devices.

1.2. Version 1.1.0

Introduces the possibility of managing Teldat C2 routers in the TMS management.

1.3. Version 1.2.0

Introduces the possibility of managing Teldat C3 routers in the TMS management.

1.4. Version 1.2.1

Introduces the possibility of managing the ASDP interface in the NOVACOM-X25 devices in the TMS management.

1.5. Version 1.3.0

Introduces the possibility of managing Teldat C3B routers in the TMS management.

1.6. Version 1.4.0

Introduces the dynamic discovery of IP addresses in the TMS management.

1.7. Version 1.5.0

Introduces the possibility of managing Teldat C2-UP routers in the TMS management.

1.8. Version 1.6.0

Introduces the possibility of managing Teldat C4I routers in the TMS management.

1.9. Version 1.7.0

Introduces the possibility of managing Teldat C2B routers in the TMS management.

2. Format of the fortnightly account files

2.1. NOVACOM, NOVACOM-X25, Teldat C2B, Teldat C3B and Teldat C4i (ISDN) Devices

The most visited addresses table is saved in files with extension **fav** in fields with the following format:

Field	**Type**	**Length**	**Description**
Device	char19	19	Telephone number associated to the router.
Date	char10	10	The date that the accounts correspond to with the format “dd/mm/yyyy” in Spanish and "mm/dd/yyyy" for the other languages.
IPAdd	char16	16	Visited IP address.
Packets	int4	4	Total traffic (packets) related to the above address.

The traffic table per station is saved in files with extension **tra** with the following format:

Field	**Type**	**Length**	**Description**
Device	char19	19	Telephone number associated to the router.
Date	char10	10	The date that the accounts correspond to with the format “dd/mm/yyyy” in Spanish and "mm/dd/yyyy" for the other languages.
IPAdd	char16	16	Station IP address.
RDSIB1_packets	int4	4	Total traffic (packets) through the ISDN B1 channel.
RDSIB2_packets	int4	4	Total traffic (packets) through the ISDN B2 channel.

The global accounts table is saved in files with extension **wan** with the following format:

Field	**Type**	**Length**	**Description**
Device	char19	19	Telephone number associated to the router.
Date	char10	10	The date that the accounts correspond to with the format "dd/mm/yyyy" in Spanish and "mm/dd/yyyy" for the other languages.
Time	char8	8	The time of the last accounts recording with format "hh:mm:ss".
RDSIB1_bytes	int4	4	Total traffic through the ISDN B1 channel (bytes).
RDSIB1_packets	int4	4	Total traffic through the ISDN B1 channel (packets).
RDSIB1_calls	int4	4	Total number of calls through the ISDN B1 channel.
RDSIB1_calls_ok	int4	4	Total number of successful calls through the ISDN B1 channel.
RDSIB1_time	int4	4	Total connection time through the ISDN B1 channel (seconds).
RDSIB2_bytes	int4	4	Total traffic through the ISDN B2 channel (bytes).
RDSIB2_paquetes	int4	4	Total traffic through the ISDN B2 channel (packets).
RDSIB2_calls	int4	4	Total number of calls through the ISDN B2 channel.
RDSIB2_calls_ok	int4	4	Total number of successful calls through the ISDN B2 channel.
RDSIB2_time	int4	4	Total connection time through the ISDN B2 channel (seconds).

In the first two tables, the registers can be repeated with the same date (changing the "IPAdd"), however in the third table, each register corresponds to a day.

There will be an ASCII sequence file associated to each tale that fulfills the following conditions:

1) Within each sequence file register, the fields must be separated with the character '|' (ASCII 124 vertical bar).
2) The register divider must be a line jump.
3) The fields within each register must be in the same order as found in the previous tables.
4) The length of each field must be equal or less than the result of the conversion to ASCII of the highest value in each field specified in the previous tables.
5) A blank CHAR field must be represented in the ASCII file by zero or more blanks.

An example of two daily accounts registers from router 911234567 for each of the tables in Spanish:

Favorite addresses:

911234567|22/05/1997|192.6.1.102|34567
911234567|22/05/1997|192.6.1.32|23

Traffic per station:

911234567|22/05/1997|192.6.1.123|2345|4566
911234567|22/05/1997|192.6.1.1|265645|45

Global accounts:

911234567|22/05/1997|12:00:23|13123|235|32|4566|12345|345|15|567
911234567|23/05/1997|08:00:20|1123|35|20|456|12344|305|10|57

2.2. Teldat C2, Teldat C2-UP, Teldat C3 and Teldat C4i (ADSL) Devices

The most visited addresses table is saved in files with extension **fav** in fields with the following format:

Field	**Type**	**Length**	**Description**
Date	char10	10	The date that the accounts correspond to with the format "dd/mm/yyyy" in Spanish and "mm/dd/yyyy" for the other languages.
IPAdd	char16	16	Visited IP address.
Bytes transmitted	int10	10	Number of bytes transmitted.
Bytes received	int10	10	Number of bytes received.
Packets transmitted	int10	10	Number of packets transmitted.
Packets received	int10	10	Number of packets received.

The traffic table per station is saved in files with extension **tra** with the following format:

Field	**Type**	**Length**	**Description**
Date	char10	10	The date that the accounts correspond to with the format "dd/mm/yyyy" in Spanish and "mm/dd/yyyy" for the other languages.
IPAdd	char16	16	Visited IP address.
Bytes received	int10	10	Number of bytes received.
Bytes transmitted	int10	10	Number of bytes transmitted.
Packets received	int10	10	Number of packets received.
Packets transmitted	int10	10	Number of packets transmitted.

The global accounts table is saved in files with extension **wan** with the following format:

Field	**Type**	**Length**	**Description**
Date	char10	10	The date that the accounts correspond to with the format "dd/mm/yyyy" in Spanish and "mm/dd/yyyy" for the other languages.
Time	char8	8	The time of the last accounts recording with format "hh:mm:ss".
Bytes received	int10	10	Number of bytes received.
Bytes transmitted	int10	10	Number of bytes transmitted.
Packets received	int10	10	Number of packets received.
Packets transmitted	int10	10	Number of packets transmitted.
Successes	int10	10	Number of connections successfully established.
Failures	int10	10	Number of failed connections.

In the first two tables, the registers can be repeated with the same date (changing the "IPAdd"), however in the third table, each register corresponds to a day.

There will be an ASCII sequence file associated to each tale that fulfills the following conditions:

1) Within each sequence file register, the fields must be separated with blank characters.
2) The register must be a line jump.
3) The fields within each register must be in the same order as found in the previous tables.
4) The length of each field must be equal or less than the result of the conversion to ASCII of the highest value in each field specified in the previous tables.
5) A blank CHAR field must be represented in the ASCII file by zero or more blanks.

An example of two daily accounts registers from device 172.24.75.2 for each of the tables in Spanish:

Favorite addresses:

```
30/06/2000 192.6.1.5        222820       0     1301       0
30/06/2000 192.6.1.51        11500       0       44       0
```

Traffic per station:

```
04/07/2000 192.7.1.0        1682344        0      3889       0
04/07/2000 192.7.1.108        44292    44806       497     491
```

```
Global accounts:

03/07/2000 17:57:08   28547906    2369435     118811      4811        0        0
03/07/2000 23:59:59   13239216     251863      48967       745        0        0
```

3. Format of the transaction files

The correct transactions tables are saved in files with extension **".tok"** in fields with the following format:

Field	Type	Length	Description
Trans Num.	int10	10	Transaction number.
Type	char64	64	Type of transaction carried out.
IP Address	char16	16	IP address called
Network called	char16	16	Network Address called.
Start time	char8	08	Transaction start time.
End time	char8	08	Transaction end time.
Date	char10	10	Date of Transaction.
Network	int10	10	Transaction authorization entity.
Packets received	int10	10	Number of packets received.

The errors transactions table is saved in files with extension **".twg"** in fields with the following format:

Field	Type	Length	Description
Trans. Num.	int10	10	Transaction number.
Type	char64	64	Type of transaction carried out.
IP Address	char16	16	IP address called.
Network called	char16	16	Network Address called.
Cause	int10	10	Cause provoking the transaction error.
Start time	char8	08	Transaction start time.
End time	char8	08	Transaction end time.
Date	char10	10	Date of Transaction.
Network	int10	10	Transaction authorization entity.
Packets received	int10	10	Number of packets received.

An example of two transaction registers from device 172.24.75.1 for each of the tables in Spanish:

Correct transactions:

```
|0|195.76.9.196|217090529260999|16:38:03|16:38:07|02/07/01|2
2|0|195.76.9.196|217090529260999|16:37:08|16:37:12|02/07/01|2
3|0|195.76.9.196|217090529260999|16:36:42|16:37:08|02/07/01|2
4|0|195.76.9.196|217090529260999|08:50:39|08:50:43|02/07/01|2
5|0|195.76.9.196|217090529260999|08:50:05|08:50:39|02/07/01|2
```

```
6|0|195.76.9.196|217090529260999|17:26:45|17:27:09|29/06/01|2
7|0|195.76.9.196|217090529260999|17:22:27|17:22:31|29/06/01|2
8|0|195.76.9.196|217090529260999|17:04:10|17:04:14|29/06/01|2
9|0|195.76.9.196|217090529260999|17:01:47|17:01:50|29/06/01|2
10|0|195.76.9.196|217090529260999|17:01:25|17:01:29|29/06/01|2
11|0|195.76.9.196|217090529260999|17:00:55|17:01:25|29/06/01|2
12|0|195.76.9.196|217090529260999|15:56:10|15:56:12|29/06/01|2
13|0|195.76.9.196|217090529260999|15:52:13|15:52:58|29/06/01|2
```

Transaction errors:

```
1|U|0.0.0.0|217090529260999|1|16:33:50|16:33:50|02/07/01|2
2|U|0.0.0.0|217090529260999|1|16:33:21|16:33:21|02/07/01|2
3|0|195.76.9.196|217090529260999|5|17:27:09|17:27:58|29/06/01|2
4|0|195.76.9.196|217090529260999|5|17:22:48|17:23:34|29/06/01|2
5|U|195.76.9.196|30012111|2|17:22:12|17:22:13|29/06/01|2
6|0|195.76.9.196|217090529260999|5|17:20:37|17:21:24|29/06/01|2
7|0|195.76.9.196|217090529260999|5|17:18:54|17:19:41|29/06/01|2
8|0|195.76.9.196|217090529260999|5|17:05:02|17:05:49|29/06/01|2
9|0|195.76.9.196|217090529260999|5|16:35:27|16:36:18|29/06/01|2
10|0|195.76.9.196|217090529260999|5|16:04:36|16:05:23|29/06/01|2
11|0|195.76.9.196|217090529260999|5|16:02:45|16:03:33|29/06/01|2
12|0|195.76.9.196|217090529260999|5|16:01:20|16:02:06|29/06/01|2
13|0|195.76.9.196|217090529260999|5|15:59:19|16:00:05|29/06/01|2
14|0|195.76.9.196|217090529260999|5|15:56:49|15:57:35|29/06/01|2
15|0|195.76.9.196|217090529260999|5|15:54:12|15:54:58|29/06/01|2
16|U|195.76.9.196|333|2|15:39:06|15:39:06|29/06/01|2
17|U|195.76.9.196|333|4|15:37:32|15:37:47|29/06/01|2
18|U|0.0.0.0|333|1|15:34:49|15:34:49|29/06/01|2
19|U|0.0.0.0|333|1|15:33:11|15:33:11|29/06/01|2
20|U|0.0.0.0|333|1|15:30:27|15:30:27|29/06/01|2
21|U|0.0.0.0|333|1|15:21:09|15:21:09|29/06/01|2
22|U|0.0.0.0|333|1|15:20:12|15:20:12|29/06/01|3
23|U|0.0.0.0|333|1|15:08:30|15:08:30|29/06/01|3
24|U|0.0.0.0|30012111|1|13:18:16|13:18:16|29/06/01|3
```

4. Devices Codes and Models

The TMS management manages the following types of devices:

Code	Funcionality	Management version
37	Conventional NOVACOM Device	1.0.0 and subsequent
46	Teldat C2 Device	1.1.0 and subsequent
51	NOVACOM device with X.25 instead of PSTN. This device has the same configuration as the 37, with the exception of the PSTN part, and incorporates three new configuration entities: XOT, X.25 and Node. The accounts are currently the same as in the 37.	1.0.0 and subsequent
53	Teldat C3 Device	1.2.0 and subsequent
57	Teldat C2B Device	1.7.0 and subsequent
59	Teldat C3-1 Device	1.2.0 and subsequent
60	Teldat C3B Device	1.3.0 and subsequent
68	Teldat C4I Device	1.6.0 and subsequent
72	Teldat C2-UP Device	1.5.0 and subsequent

5. ISDN Release Causes

This is an indication of the causes why the last call provided by the ISDN network was released complying with the ISO Q931 standard. The possible values that can appear are:

0	Undefined. Indicates that the call has not been released yet.
1	Non-attributed number.
3	There is no existing route to the destination.
6	Unacceptable channel.
16	Normal call release.
17	User busy.
18	User does not respond.
19	The user has been advised but a response has not yet been received.
21	The call has been rejected. From **version 5.4.0** onwards for the device 37 and all the 51 versions, when this receives a management call, it is rejected and this cause is established.
22	The number has been changed.
27	The destination number is out of order.
28	The dialed number format is invalid.
31	Normal release.
34	There is no available circuit or channel.
38	The network is down.
41	A temporary failure has been produced.
42	The switch device is congested.
44	The requested circuit or channel is not available.
47	The resources are not currently available.
49	The quality of service is not available.
57	The carrier capacity is not authorized.
58	The carrier capacity is not currently available.
63	The service class or another option is not available.
65	The carrier capacity has not been carried out.
66	The requested channel type has not been carried out.
79	The service or another operation has not been carried out..
81	The call reference value is invalid.
82	The identified channel does not exist.
88	The destination is incompatible with the source.
95	Invalid message.
96	Mandatory information element is absent.
97	Message type is non-existent or not carried out.
98	Non-existent message or not implanted.

99	Non-existent information element or not carried out.
100	Invalid information element content.
101	Message incompatible with call status.
102	Recovery on the timer timeout.
111	A protocol error has been produced.
127	Interoperation.

In order to identify errors in the automatic accounts collection, you also use this field in the database. In this case, the following values can be taken.

500	Router managed by another application.
501	None of the masters is accessible.
502	Time-out in the SNMP petition to the device after this has been accessible.
503	Software version is not supported.
504	Unexpected interruption of the accounts collection.
505	Error in accounts collection (corrupt data blocks).
506	Operation interrupted by the user.
507	Device unexpectedly decongested.
508	Operation paused (end time exceeded).

6. Errors in the transactions

This indicates the reason the transaction did not execute correctly. The possible values that can appear are as follows:

1	The NRI sent by the dataphone does not coincide with any of those configured.
2	Disconnection received by the DEP.
3	Invalid operation from the dataphone.
4	An IP connection with the host cannot be established.
5	TRMP connection has ended.
6	TCP connection has ended.

7. Bibliography

Code	Reference
{Loney, 97}	“ORACLE. Manual del administrador” Kevin Loney McGraw-Hill, 1997.
{ORACLE:1, 96}	“Oracle7 Server Administrator’s Guide” Release 7.3 ORACLE, 1996.
{ORACLE:2, 97}	“Oracle7 Instalation Guide” Release 7.3.4 ORACLE, 1997.
{Teldat:NAT, 99}	“Equipo Teldat: Facilidad NAT” Doc. DM520 Rev. 8.00 Julio, 1999
{Velpuri, 95}	“ORACLE Backup & Recovery Handbook” Rama Velpuri Osborne McGraw-Hill. 1995.