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

Manual de Usuario

Doc. 266 Rev. 2.0
Abril, 2002

ÍNDICE

CAPÍTULO 1 INTRODUCCIÓN 1

1. INTRODUCCIÓN 2
2. FUNCIONALIDADES DEL SISTEMA DE GESTIÓN 3

CAPÍTULO 2 INSTALACIÓN DE LA GESTIÓN TMS 4

1. REQUISITOS PREVIOS A LA INSTALACIÓN 5
2. INSTALACIÓN DE ORACLE 7 WORKGROUP SERVER VERSIÓN 7.3.3.0.0 6
   - *2.1. Requisitos previos del sistema 6*
   - *2.2. Procedimiento de Instalación 7*
3. INSTALACIÓN DEL CENTRO DE GESTIÓN TMS 8
   - *3.1. Descarga del software TMS 8*
   - *3.2. Ajuste de la Base de Datos para la Gestión TMS 10*
     - a) Configuración del LISTENER y del traductor de nombres 10
     - b) Configuración de ORACLE (TABLESPACES, ROLLBACK …) 11
   - *3.3. Variables de entorno 12*
     - a) Variables generales 12
     - b) Variables para el funcionamiento de descubridor de IP 12
4. BASE DE DATOS 14

CAPÍTULO 3 GESTIÓN TMS 15

1. INTRODUCCIÓN 16
2. GESTIÓN DE EQUIPOS TMS 17
   - *2.1. Menú principal 18*
   - *2.2. Barra de herramientas 19*
   - *2.3. Lista de routers maestros 19*
   - *2.4. Lista de equipos en la BD 21*
   - *2.5. Lista de equipos en gestión 25*
   - *2.6. Indicador de lectura de BD y último comando ejecutado 27*
3. ÚLTIMOS EQUIPOS DISPONIBLES 29
4. AUDITORÍA DE INTERVENCIONES 30

CAPÍTULO 4 GESTIÓN DE EQUIPOS 31

1. CONFIGURACIÓN 32
   - *1.1. Parámetros de configuración 32*
     - a) General 33
     - b) Canal B1 (solo para equipos NOVACOM y NOVACOM-X25) 37
     - c) Rutas IP 40
     - d) Acceso IP 41
     - e) Entidades visibles 47
     - f) Configuración de puertos visibles en la LAN 50
     - g) Configuración de servidores de DNS 52
     - h) Configuración de Backup 54
     - i) Configuración de Callback 58
     - j) MPPP (Point to Point Protocol) 60
     - k) Configuración de NAT (Network Address Translation) estático 64
     - l) Configuración X.25 (sólo equipos NOVACOM-X25) 68
     - m) DHCP 78

n) Conexiones ATM ... 80
o) Conexiones IP ... 82
p) RDSI ... 86
q) Controles temporales ... 87
r) TCP ... 88
s) TRMTP ... 90
t) TPV ... 91
u) UART ... 92
v) RTC ... 93
w) WAN ... 94
x) IPSEC ... 95
1.2. Comandos de ficheros ... 99
a) Leer configuración de fichero ... 99
b) Escribir configuración en fichero ... 100
c) Visualizar fichero de log ... 100
1.3. Comandos de Base de Datos ... 101
a) Leer configuración de la base de datos ... 101
b) Guardar configuración de la base de datos ... 102
1.4. Comandos de comunicaciones ... 102
a) Pedir configuración al equipo ... 102
b) Enviar configuración al equipo ... 102
c) Sincronización del equipo con la estación de gestión ... 103
d) Salvar a memoria FLASH la configuración en el equipo ... 103
e) Reiniciar el equipo con su configuración en memoria FLASH ... 103
f) Telecargar software al equipo ... 103
2. MONITORIZACIÓN ... 105
2.1. Descripción de la ventana principal ... 105
a) Comandos de ficheros ... 105
b) Visualizar fichero de log ... 107
c) Comandos de Base de Datos ... 107
d) Comandos de comunicaciones ... 109
2.2. Monitorización Diaria ... 110
a) RDSI ... 110
b) ADSL ... 114
2.3. Monitorización Quincenal ... 118
a) RDSI ... 118
b) ADSL ... 120
2.4. Monitorización de TPV ... 123
a) Transacciones correctas ... 124
b) Transacciones erróneas ... 125

CAPÍTULO 5 RECOGIDA AUTOMÁTICA DE ESTADÍSTICOS ... 126

1. RECOGIDA AUTOMÁTICA DE ESTADÍSTICOS ... 127
1.1. Instalación ... 127
1.2. Arranque ... 127
1.3. Sincronización de los equipos ... 128
1.4. Progreso ... 128
1.5. Resultados ... 129

CAPÍTULO 6 OPERACIONES SOBRE GRUPOS ... 130

1. OPERACIONES SOBRE GRUPOS ... 131
1.1. Definición de operaciones sobre grupos ... 132
1.2. Gestión de grupos ... 135

1.3. Operaciones de configuración de grupos de equipos ... 137
a) Ejemplos de operaciones de configuración sobre grupos ... 138
1.4. Ejecución de operaciones sobre grupos ... 142
1.5. Monitorización de operaciones sobre grupos ... 144

CAPÍTULO 7 BASE DE DATOS ORACLE ... 149

1. TABLAS UTILIZADAS EN LA BASE DE DATOS ... 150
2. ACTUALIZACIÓN DE LA BASE DE DATOS ... 152
3. COPIAS DE SEGURIDAD ... 153
3.1. Backup físico off line de la base de datos ... 153
3.2. Exportación de la base de datos ... 154
3.3. Backup de todos los datos de la gestión TMS ... 154
3.4. Recuperación de los datos en caso de desastre ... 155

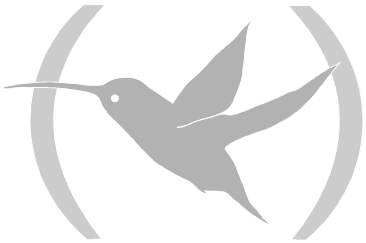
CAPÍTULO 8 REGISTRO DE SUCESOS ... 156

1. REGISTRO DE SUCESOS ... 157

CAPÍTULO 9 APÉNDICES ... 159

1. REVISIONES ... 160
1.1. Versión 1.0.0 ... 160
1.2. Versión 1.1.0 ... 160
1.3. Versión 1.2.0 ... 160
1.4. Versión 1.2.1 ... 160
1.5. Versión 1.3.0 ... 160
1.6. Versión 1.4.0 ... 160
1.7. Versión 1.5.0 ... 160
1.8. Versión 1.6.0 ... 160
1.9. Versión 1.7.0 ... 160
2. FORMATO DE LOS FICHEROS DE ESTADÍSTICOS QUINCENALES ... 161
2.1. Equipos NOVACOM, NOVACOM-X25, Teldat C2B, Teldat C3B y Teldat C4i (RDSI) ... 161
2.2. Equipos Teldat C2, Teldat C2-UP, Teldat C3 y Teldat C4i (ADSL) ... 163
3. FORMATO DE LOS FICHEROS DE TRANSACCIONES ... 166
4. CÓDIGOS Y MODELOS DE EQUIPO ... 168
5. CAUSAS DE LIBERACIÓN RDSI ... 169
6. ERRORES EN LAS TRANSACCIONES ... 171
7. BIBLIOGRAFÍA ... 172

Capítulo 1
Introducción



1. Introducción

La Figura 1 muestra el entorno genérico de gestión de las soluciones Teldat para acceso a Internet / Intranet de empresas.

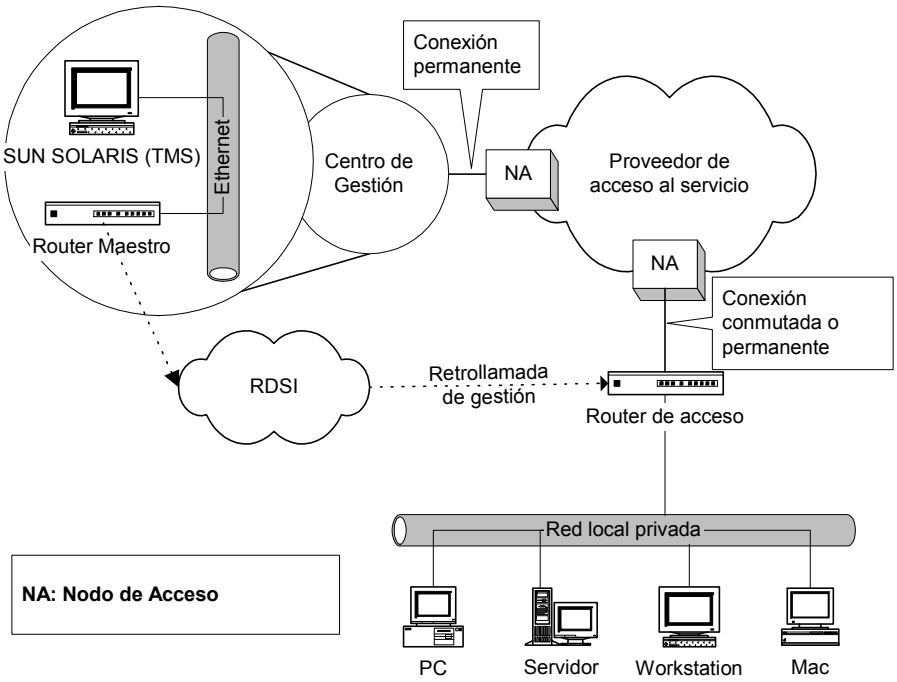


Figura 1 : Escenario genérico de gestión TMS

Dos elementos principales participan en el escenario: el centro de gestión y el router de acceso.

El **centro de gestión**, en las dependencias del proveedor del servicio, es el lugar (centralizado) desde el que se gestionan los routers de acceso de los clientes dados de alta en el servicio. Consta de la aplicación de gestión (TMS), la base de datos y un router "despertador" (a partir de ahora **router maestro**) de equipos remotos para puesta en gestión, para el caso de acceso RDSI.

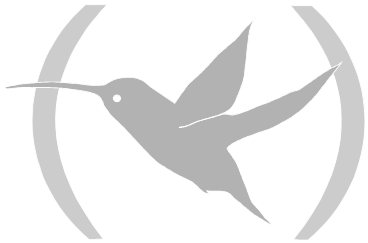
El **router de acceso** es el equipo Teldat que conecta la red local del cliente dado de alta en el servicio con los servicios contratados (Internet / Intranet). Puede ser un router de acceso RDSI / RTC (ó XOT) o un router de acceso ADSL.

Como puede apreciarse en la figura, en el caso de que el router de acceso sea RDSI, el sistema TMS incluye un procedimiento de puesta en gestión mediante llamada RDSI de gestión. De esta forma, se puede siempre gestionar los equipos de acceso RDSI, independientemente de que estén conectados o no a la red e independientemente también de que cada vez se conecten con un dirección IP diferente, ya que el sistema descubre con qué dirección se conecta cada equipo en cada momento.

2. Funcionalidades del sistema de gestión

- **Sistema homogéneo y a medida**. Como se ha indicado en el apartado de ventajas del sistema, éste ofrece una visión sencilla y homogénea al operador. La funcionalidad del sistema es semejante, independientemente de que el acceso del equipo remoto se realice desde una red conmutada. Sólo se pueden configurar las cosas que son realmente necesarias para la funcionalidad requerida, por lo que el sistema gana en sencillez y facilidad de manejo.
- **Aprendizaje dinámico de la dirección IP del router de acceso.** La aplicación de gestión TMS aprende dinámicamente con qué dirección se han conectado los routers de acceso cuando se les desea gestionar. De esta forma se puede acceder a gestionar un equipo aunque éste se conecte cada vez con una dirección IP diferente. Esta funcionalidad simplifica y flexibiliza enormemente el proceso de gestión a la vez que permite ahorrar direcciones IP.
- **Multi-display / Multi-operador**. El sistema de gestión permite el funcionamiento simultáneo con varios operadores del servicio en varios terminales de gestión. El sistema está protegido frente a colisiones de gestión, evitando que distintos operadores gestionen simultáneamente el mismo equipo.
- **Operaciones sobre grupos**. Se dispone de una versátil herramienta de operaciones sobre grupos. Con ella es posible planificar, operar y monitorizar operaciones comunes a realizar sobre grupos de la base instalada de clientes. Por ejemplo, se puede planificar una actualización remota del software de todos los routers de acceso de un determinado cliente.
- **Base de datos profesional**. Toda la plataforma de gestión está soportada sobre una potente base de datos. El resultado es una rápida, potente y flexible herramienta de gestión, que da la posibilidad de generar informes detallados de utilización e incidencias además de posibilitar una operación centralizada y controlada de todo el sistema, incluido el alta y baja de clientes (manejo de fichas), puesta en gestión, etc.
- **Recogida automática de estadísticos**. Los equipos remotos de acceso de Teldat soportan el almacenamiento en memoria no volátil de estadísticos de tráfico y operación. La aplicación de gestión recoge periódicamente dichos estadísticos almacenados, posibilitando la elaboración de informes de uso del servicio y tráfico al cliente final.
- **Siempre se garantiza la gestión**. Uno de los requisitos claves para poder ofrecer el servicio es que siempre que se solicite la gestión de un equipo, éste esté disponible para dicha gestión. Esto es, que si no está conectado, se conecte y si no hay canales físicos disponibles para realizar la conexión de gestión, se libere uno de los ocupados a favor de la conexión de gestión. De esta manera se puede reaccionar rápidamente ante el requerimiento por parte del cliente final de cambio de configuración, solución de averías, etc.
- **Registro de todas las acciones**. Para el control del servicio y utilizando este registro, se pueden, por ejemplo, realizar informes de actividad de los operadores, informes de incidencias (averías) de los equipos instalados, etc.

Capítulo 2
Instalación de la gestión TMS



1. Requisitos previos a la instalación

Requisitos Hardware

* Estación SUN Ultra 5 o superior.
* Lector de CD-ROM.
* Oracle 7.3 Workgroup Server o superior:
    * 32 Mbytes de RAM (128 recomendado).
    * Tres veces el tamaño de RAM de espacio de swap.
    * 700 Mbytes de espacio libre en disco.
* Gestión TMS:
    * 128 Mbytes de RAM.
    * 200 Mbytes de espacio libre en disco para la propia aplicación.

    Para gestionar hasta 4000 equipos:
        * 120 Mbyes de espacio libre para datos de las tablas de la base de datos.
        * 30 Mbytes de espacio para ficheros de configuración (en el caso de que se utilicen).
        * El espacio necesario para los ficheros de estadísticos depende de la regularidad con la que se procesen y del tráfico cursado en los equipos.

Requisitos Software

* Sistema Operativo SOLARIS 2.5.1 o 2.6 (instalación completa).
    * Paquete “Font Server Cluster”.
    * Parches necesarios para ORACLE 7.3 (fuente {ORACLE:2, 97}:
        * 103640-01 o superior.
    * Paquetes necesarios para ORACLE 7.3:
        * SUNWarc.
        * SUNWbtool.
        * SUNWhea.
        * SUNWlibm.
        * SUNWlibms.
        * SUNWsprot.
        * SUNWtoo.
        * SUNWmfrun.
        * Librerías Motif con los siguientes parches mínimos:
            103461-07
* ORACLE 7.3.
* Para documentación y ayuda es preciso tener instalado un navegador que visualice formato HTML

2. Instalación de Oracle 7 Workgroup Server Versión 7.3.3.0.0

2.1. Requisitos previos del sistema

La instalación de Oracle Workgroup server requiere al menos 32 MB de memoria RAM y 700 MB de disco duro.

En cuanto al sistema operativo, es necesario para la correcta instalación del gestor de bases de datos Oracle, que estén instalados los siguientes paquetes:

Sistema Operativo	Requerimientos software
Solaris 2.x	SUNWbtool
	SUNWtoo
	SUNWsprot
	SUNWarc
	SUNWlibm
	SUNWlibms
	SUNWhea
	SUNWmfrun

Para comprobar la existencia de dichos paquetes se puede ejecutar el siguiente comando:

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

La salida debe ser:

```
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
```

Si alguno de los anteriores paquetes no estuviera instalado se puede proceder a su instalación con ayuda del comando:

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

En Solaris 2.x además de los paquetes mencionados, es necesario establecer una serie de parámetros del sistema operativo. Para ello editar el fichero **`/etc/system`** como root y añadir o modificar los siguientes parámetros:

```
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
```

En el directorio **$TELDATMS/db/etc** se encuentra un fichero **system.teldat** que contiene estos parámetros y que puede copiarse sobre el **/etc/system** si este no tiene otra información relevante.

Tras modificar dicho fichero rearrancar la estación para que los nuevos parámetros tomen efecto.

2.2. Procedimiento de Instalación

La instalación de Oracle Workgroup Server consiste en la ejecución del script **wgstart** que se encuentra en el CD-ROM de Oracle en el directorio **/cdrom/oracle/wgstart** y se siguen los pasos que indica el fabricante. Se recomienda la siguiente asignación de usuarios y passwords inicial:

Usuario	Password
wguser	oracle7
oracle7	oracle7

Cuando aparece la ventana que solicita el directorio de instalación para ORACLE hay que poner en el campo SID la cadena **GEST**. Se recomienda idioma **spanish** y juego de caracteres **WE8DEC**. Posteriormente, en el entorno del usuario de gestión, la variable de entorno ORACLE_SID deberá contener esta misma cadena (GEST).

Una vez finalizada la instalación, hay que editar el fichero **/etc/rc2.d/S84tcplsnr** y verificar si el directorio donde se ha instalado ORACLE coincide con el que aparece dentro del fichero. Además hay que comentar (poniendo el carácter '**#**' al comienzo de las líneas) el segundo **"if**" del fichero. Si no se lleva a cabo esta operación al rearrancar la estación aparece un prompt como el siguiente:

```
LSNCTRL>
```

en el que habría que introducir los siguientes comandos:

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

lo que permitiría continuar el arranque de la estación.

Además, también hay que copiar la librería **libsunmath.so.1,** incluida en el CDROM de ORACLE, en el directorio **$ORACLE_HOME/lib**.

3. Instalación del Centro de Gestión TMS

Las principales aplicaciones del centro de gestión TMS son:

tmsdefgo	Definición de grupos y operaciones sobre grupos.
tmsgroupop	Operaciones sobre grupos (recogida de estadísticos, reconfiguración, etc.).
tmsmonauto	Monitorización de la recogida automática de estadísticos quincenales.
tmsmongo	Monitorización de operaciones sobre grupos.
tmsconfig	Lanza la aplicación de configuración de equipos NOVACOM y Teldat Cx.
tmsmanager	Lanza la aplicación de mantenimiento de la base de datos y comunicación con los routers maestros para gestionar los routers de acceso.
Tmsmon	Lanza la aplicación de monitorización diaria y quincenal de los equipos NOVACOM y Teldat Cx.

Para la óptima presentación de las ventanas se necesita que esté instalado el paquete "Font Server Cluster" que incluye el CDROM del sistema operativo SOLARIS 2.5.1. Para proceder a su instalación se puede utilizar la herramienta **admintool**.

Antes de proceder a la instalación de la gestión TMS se debe crear un usuario de gestión (o asignar uno existente, aunque se recomienda la primera opción).

La gestión TMS se suministra en un CD que se introduce en la unidad conectada a la estación de gestión.

A partir de este punto se seguirá el siguiente convenio: "En los comandos que deben ser ejecutados como root el prompt del sistema será el carácter '#', mientras que los que tienen que ser ejecutados como usuario de gestión tendrán el carácter '>'."

Para garantizar que el sistema monta el CD en el sistema de ficheros ejecutar (como root):

```
#volcheck
```

IMPORTANTE: Si se trata de una actualización de versión, se advierte que en el proceso de instalación **se perderán todos los datos** almacenados en la base de datos, por tanto es responsabilidad del usuario **hacer un backup** de dichos datos **antes** de comenzar todo el proceso.

3.1. Descarga del software TMS

Actualmente, en el CD que se distribuye como paquete software se muestra la versión mas una línea en la parte inferior similar a la siguiente:

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

Este es el comando que se debe ejecutar (como root) para comenzar la instalación.

NOTA: El punto que se muestra al final del comando forma parte del nombre del fichero, por tanto se debe escribir para poder ejecutar el comando

Aparece la siguiente pantalla:

```
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]:
```

Pulse '1' o return (opción por defecto).

Durante la instalación se hacen al instalador una serie de preguntas para la correcta instalación del software.

Se pregunta el directorio donde se deben copiar todo el sistema de ficheros descargados. Por defecto se ofrece una ruta pero el instalador puede cambiarla si lo estima conveniente. Si se desea la opción por defecto se pulsa retorno de carro.

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

El directorio raíz de ORACLE (que se instaló previamente). En este caso no existe valor por defecto y se hace totalmente necesario escribir la ruta donde se tiene instalado ORACLE.

```
ORACLE root directory:
```

Usuario creado para la gestión o asignado para este fin. Por defecto se ofrece la opción del usuario *gestion* de grupo *gestion* que debe existir antes de comenzar el proceso de instalación.

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

Para la correcta visualización de la ayuda es preciso que la estación tenga instalado un navegador.

Se pide la ruta completa del navegador que será asignada a la variable de entorno **TMSHELPBROWSER** en el proceso de instalación, pero esta variable puede cambiarse en cualquier instante.

```
Help browser:
```

Entre las opciones a configurar, estará la de instalar o no el demonio de descubrimiento de direcciones IP dinámicas **IPDiscover**. Si se tienen que gestionar equipos cuyas direcciones IP van a ser dinámicas, el demonio debería ser instalado, no siendo necesario en caso contrario. Independientemente de la respuesta, si en un futuro se necesitará el IPDiscover, se podrá acceder a él sin repetir la instalación.

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

Finalmente se presenta un resumen de los datos introducidos y la posibilidad de cambiarlos si alguno no es correcto.

```
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
```

A partir de este punto comienza la instalación pero si el directorio base no existe se muestra un mensaje y se pregunta si se crea de forma automática.

```
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
```

La descarga de ficheros se realiza durante unos minutos presentando un mensaje por cada elemento que se descarga.

Una vez instalado el paquete puede visualizarse sus propiedades con la herramienta "admintool" como root:

```
#admintool
```

Seleccionando "Browse->Software->Application Software" aparece la lista de aplicaciones instaladas.

El siguiente paso es establecer las variables de entorno para el usuario de gestión y ajustat la base de datos,

3.2. Ajuste de la Base de Datos para la Gestión TMS

a) Configuración del LISTENER y del traductor de nombres

Suponiendo que el camino del directorio base donde se instaló ORACLE está contenido en la variable de entorno ORACLE_HOME, e debe modificar dos ficheros:

1. el fichero $ORACLE_HOME/network/admin/tnsnames.ora donde se encontrará definida la cadena de conexión de las aplicaciones del Centro de Gestión que es **tms_tcp_GEST**. La variable de entorno **ORATMS** del usuario de gestión deberá contener esta misma cadena.

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

donde ***nom_maquina*** es el nombre de la máquina donde se instala la base de datos o en su defecto el número IP. Si la instalación es como cliente en este campo se debe poner el nombre (o número IP) de la máquina que contiene el servidor de la base de datos.

2. el fichero ORACLE_HOME/network/admin/listener.ora que debe tener un aspecto similar al siguiente

```
LISTENER =
  (ADDRESS_LIST =
        (ADDRESS= (PROTOCOL= IPC)(KEY= tms_tcp_GEST))
        (ADDRESS= (PROTOCOL= IPC)(KEY= PNPKEY))
        (ADDRESS= (PROTOCOL= TCP)(Host= nom_maquina)(Port= 1521))
  )
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME= nom_maquina.)
      (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
```

Después de estas acciones volver a arrancar la estación y prestar atención a los mensajes de arranque para detectar posibles errores en la instalación.

b) Configuración de ORACLE (TABLESPACES, ROLLBACK …)

Una vez descargado el software TMS y como usuario de gestión ejecutar el script siguiente:

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

donde TELDATMS es el directorio base de la gestión.

Si se trata de una actualización de versión se verá que el script presenta errores que no son significativos.

Para crear (o actualizar) la base de datos de la aplicación de gestión se ejecuta el siguiente script como usuario de gestión:

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

Si se trata de una actualización de versión se borrarán todas las tablas y se crearán de nuevo. Como se advirtió previamente, es responsabilidad del usuario hacer un backup de los datos al principio del proceso de instalación.

3.3. Variables de entorno

a) Variables generales

Para el correcto funcionamiento de las aplicaciones de gestión TMS es preciso configurar ciertas variables de entorno. Es tan simple como añadir una línea en el fichero de arranque del usuario de gestión, que dependiendo del tipo de shell es el fichero ***.cshrc*** o ***.profile***.

Para averiguar cual es la shell en uso se puede utilizar el siguiente comando (como usuario gestion):

```
>echo $SHELL
```

Si la shell es "csh" o "tcsh" editar el fichero ***.cshrc*** en el directorio home del usuario de gestión y añadir la línea:

```
source directorio_raiz/script/teldatms.csh
```

donde ***directorio_raiz*** es la ruta donde se descargó el software de la gestión.

Si la shell es "sh", "ksh" o "psh" entonces en el fichero **.profile** del directorio home del usuario de gestión añadir la línea siguiente:

```
. directorio_raiz/script/teldatms.env
```

Nota: Esta línea empieza con los caracteres punto y espacio.

Para la conexión con la base de datos ORACLE son de especial importancia las variables **ORACLE_HOME**, **ORACLE_SID** y **ORATMS**. **ORATMS** contiene la cadena de caracteres con la que las aplicaciones del Centro de Gestión se conectan a la base de datos.

Para el arranque automático del demonio **ipdiscover**, se deberá configurar la variable **IPDBOOT**, que podrá ser *"y"* (en caso de querer tal arranque), o *"n",* si se prefiere trabajar sin descubrimiento (se inicializa con la opción elegida en la instalación).

Todas las aplicaciones con interfaz gráfica de usuario han sido desarrolladas con la herramienta **ILOG Views versión 2.4.1**. Dicha herramienta guarda la información asociada a las ventanas en ficheros con extensión "ilv" que son leídos al iniciarse la aplicación. Para que ILOG localice estos ficheros es necesario establecer la variable de entorno **ILVPATH** con el valor **"$TELDATMS/ilv**".

b) Variables para el funcionamiento de descubridor de IP

Por último, para el correcto funcionamiento del programa IPDiscover, habrá que configurar los siguientes parámetros en el fichero **$TELDATMS/etc/ipdiscover/ipdiscover.ini:**

- DBServerName: nombre del servidor de base de datos.
- DBServerType: tipo del servidor de base de datos.

- DBUserName: usuario de la base de datos.
- DBPassword: password del usuario.
- Inactivity: tiempo máximo de inactividad de un equipo, en minutos. Cuando un equipo con dirección IP dinámica no envía información en un tiempo menor a inactivity, se considerará que no está disponible.

El resto de valores del fichero pueden dejarse con su valor por defecto.

Al instalar la gestión, este fichero se copia con unos valores por defecto que el usuario debe revisar.

Los valores por defecto son:

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

4. Base de Datos

La Gestión TMS utiliza una base de datos ORACLE versión 7.3 (o superior) en la que se definen las siguientes tablas:

acc<codigo_equipo>_<entidad>	Tablas de estadísticos quincenales.
Auto	Tabla de resultados de la última recolección automática de estadísticos quincenales.
conf<codigo_equipo>_<entidad>	Tablas de configuración de cada equipo.
device	Tabla con las fichas de los equipos que se gestionan.
go_log	Tabla de log de operaciones sobre grupos.
go_op	Tabla de operaciones sobre grupos.
Groups	Tabla de grupos de equipos.
infomanaged	Tabla que contiene los equipos gestionados por los maestros y por direcciones IP estáticas.
infodevice	Tabla de información del equipos: Número de serie, número de placa, versión de software, versión de BIOS.
managed	Tabla que indica que equipos está gestionando cada maestro.
mancalls	Tabla con un histórico de llamadas de gestión con la fecha y hora de comienzo y fin de la llamada.
master	Tabla de los routers maestros disponibles.
mon<codigo_equipo>_<entidad>	Tablas espejo de las listas de las aplicaciones de monitorización quincenal de cada equipo.

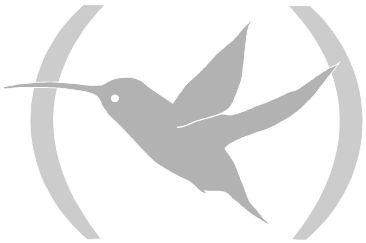
Dichas tablas están a disposición del usuario para ser exportadas a otros formatos o bases de datos, para hacer informes o construir cualquier otra aplicación sobre ellas.

Requerimientos de espacio:

Se estima que para gestionar 4000 equipos con código de equipo 37 con sus configuraciones almacenadas en la base de datos se precisa un fichero de datos de unos 80 Mbytes, aproximadamente .

Inicialmente, el fichero se dimensiona con un tamaño de 5Mbytes y a medida que se incorporen equipos a la base de datos el fichero se autoexpande.

Capítulo 3
Gestión TMS



1. Introducción

La gestión TMS de TELDAT es soportada por un conjunto de aplicaciones independientes que se comunican a través de la misma base de datos ORACLE, dos procesos ejecutándose permanentemente en segundo plano y una aplicación de operaciones sobre grupos:

tmsgroupop	Operaciones sobre grupos.
tmsconfig	Configuración de equipos.
tmsmanager	Mantenimiento de la base de datos de equipos y routers maestros.
tmsmon	Monitorización de estadísticos diarios y quincenales de los equipos.
tmssynchro	Actualización de la base de datos con información recogida periódicamente de los routers maestros.
IPDiscover	Actualización de la base de datos con información recogida de los equipos con dirección IP dinámica.

2. Gestión de equipos TMS

La aplicación **tmsmanager** utiliza una base de datos ORACLE (versión 7.3) para guardar los datos de los routers maestros y equipos TMS así como los estadísticos quincenales de los equipos. Esta base de datos es actualizada por dos procesos: el proceso **tmssynchro** , que consulta periódicamente la tabla de equipos gestionados de los routers maestros dados de alta en la base de datos, y el proceso **ipdiscover**, que actualiza la base de datos con las dirección IP de los equipos cuya dirección es dinámica. Periódicamente, la aplicación comprueba si está ejecutándose en el proceso **tmssynchro** y, si no es así, presenta el siguiente mensaje que permite que el usuario lo lance desde la aplicación:

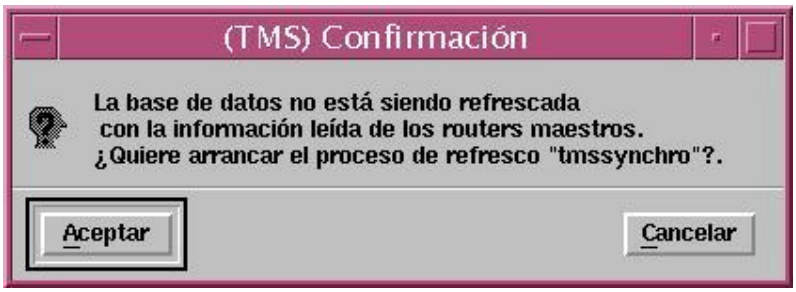


Figura 2 : Confirmación de arranque de proceso tmssynchro

Puede haber múltiples instancias de la aplicación **tmsmanager** ejecutándose simultáneamente sobre la misma estación, sobre la base de datos local, o incluso, sobre otra base de datos remota conectada con la estación.

En el caso de que la aplicación trabaje con una base de datos remota no se necesita ejecutar el proceso **tmssynchro** en la estación local porque la base de datos ya está siendo refrescada con el proceso **tmssynchro** de la estación remota. En este caso, para deshabilitar la comprobación de que el proceso **tmssynchro** está ejecutándose, basta ejecutar:

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

(ncs = no check tmssynchro)

Dependiendo de las opciones de instalación, si se eligió no instalar el demonio de descubrimiento, el arranque del **ipdiscover** se debe habilitar explícitamente mediante:

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

(ipd = ipdiscover)

Cuando arranca, la aplicación **tmsmanager** establece una conexión con la base de datos (local o remota) y, a partir de ahí, la consulta periódicamente para detectar cambios en los estados de los equipos en gestión u otros cambios provocados por otros posibles usuarios de gestión operando sobre otras instancias de la aplicación.

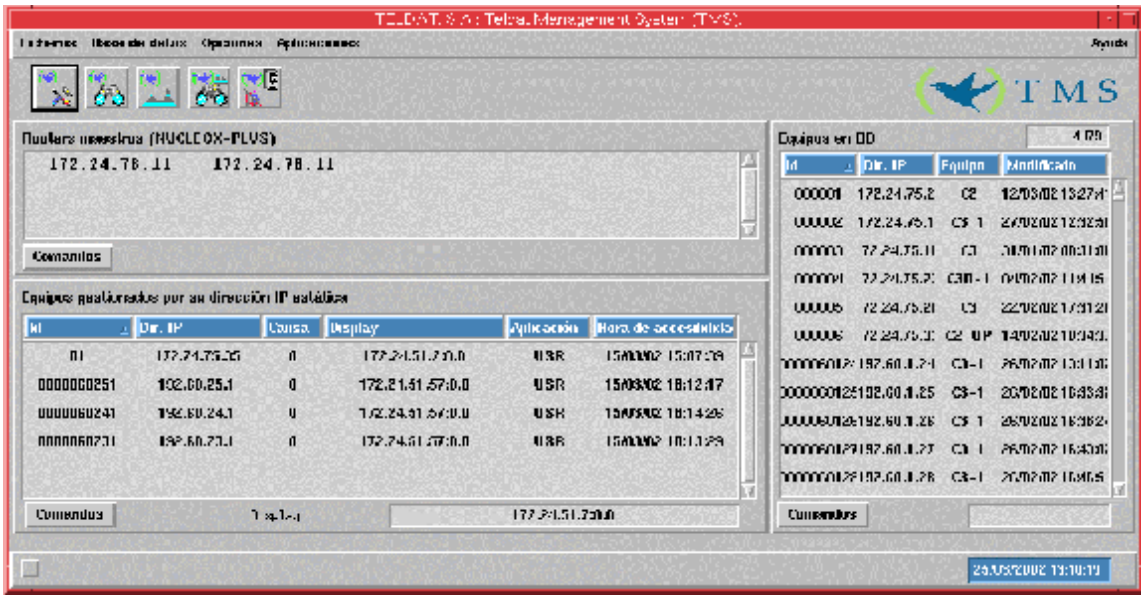


Figura 3 : Ventana principal de la aplicación de gestión

Esta ventana consta de varias partes, que se explican en los apartados siguientes.

2.1. Menú principal

I. Ficheros

A. Backup TMS

Consultar el apartado Backup de todos los datos de la gestión TMS.

B. Salir.

Salir de la aplicación.

II. Base de Datos

A. Exportar

Consultar el apartado Exportación de la base de datos.

III. Opciones

A. Opciones

IV. Aplicaciones

A. Configuración

B. Monitorización

C. Recogida automática

D. Monitorización de la recogida automática

E. Operaciones sobre grupos

V. Ayuda

Muestra el contenido de la ayuda de la aplicación.

2.2. Barra de herramientas


Lanza la aplicación de configuración de equipos.


Lanza la aplicación de monitorización de equipos.


Lanza la aplicación de recogida automática de estadísticos quincenales de los equipos.


Lanza la aplicación de monitorización de la recogida automática de estadísticos quincenales de los equipos.


Lanza el gestor de operaciones sobre grupos de equipos.

2.3. Lista de routers maestros

Muestra todos los routers maestros contenidos en la tabla **master** de la base de datos. Sobre esta lista es posible ejecutar las acciones contenidas en el menú **Comandos** situado bajo la lista. Un equipo no puede ser gestionado simultáneamente por más de un router maestro.

Para **añadir un router maestro** a la base de datos se selecciona **Comandos->Agregar** lo cual despliega la ventana de **Edición de router maestro** con los valores por defecto de los campos. Cuando se hayan rellenado convenientemente se pulsa el botón **Salvar** que guarda el equipo en la base de datos. Si no ha habido errores inmediatamente aparece un mensaje de confirmación en la parte inferior de la ventana principal. En el siguiente refresco de la ventana aparecerá el equipo en la lista.

Para **editar un router maestro** de la base de datos se selecciona en la lista y se ejecuta **Comandos->Editar** que también despliega la ventana de Edición de router maestro con el actual contenido de los campos. Tras realizar las modificaciones deseadas se pulsa **Salvar** para guardar los cambios.

Figura 4 : Ventana de edición de router maestro

Los campos configurables son los siguientes:

Nombre ("/etc/hosts") o dirección IP del router maestro:
Es la dirección IP del router maestro. También puede introducirse un nombre asociado a una dirección IP a través del fichero "/etc/hosts" de la estación. Se admiten un máximo de 15 caracteres.

Contraseña de acceso:
Se trata de la contraseña de acceso al equipo por TELNET y FTP. Las aplicaciones no la utilizan, simplemente es una forma de tenerla accesible como recordatorio para el operador. Se admiten 31 caracteres distintos del blanco.

En **Parámetros SNMP** podemos configurar los siguientes campos:

Comunidad de acceso:
Es la comunidad SNMP con la que el usuario pretende acceder al equipo. Sólo se puede acceder a un equipo si la comunidad de acceso SNMP de su configuración coincide con la de su ficha. Admite hasta 31 caracteres y no se admiten blancos.

Máximo número de intentos:
Es el máximo número de intentos que se realiza una petición SNMP al equipo en caso de que las anteriores hayan fracasado. El valor por defecto es 2 intentos.

Tiempo de espera de respuesta:
Es el plazo (en segundos) que espera la estación de gestión respuesta a una consulta SNMP antes de terminar con un mensaje de time-out. El valor por defecto es 10 segundos.

Si se desea borrar un router maestro de la base de datos, basta con seleccionarlo en la lista y escoger la opción **Comandos->Borrar**.

A cada maestro contenido en la lista, la aplicación **tmssynchro** le hace una petición periódica de la tabla de equipos que están siendo gestionados por él.

Cuantas más estaciones interaccionen con el mismo router maestro mayor será el tiempo de respuesta a dichas interacciones.

Colisión de peticiones SNMP

Cuando aparece este mensaje asociado a un router maestro indica que mientras se estaba solicitando la tabla de equipos en gestión al maestro se ha producido un SET SNMP que ha provocado la inserción o el borrado de un elemento de la tabla y ha desbaratado por tanto la tabla recibida en la estación.

En tal caso, el contenido de la tabla recibida se ignora y se vuelve a pedir.

2.4. Lista de equipos en la BD

Muestra todos los equipos que hay en la tabla **device** de la base de datos así como las direcciones IP que tienen asignadas. Que aparezcan equipos en esta área no significa que se estén gestionando, sólo implica que ese equipo existe en la base de datos. Si un equipo aparece en rojo, significa que se gestiona por dirección IP dinámica y que en ese momento no está disponible. Un equipo en rojo no puede ser gestionado.

Sobre la esquina superior derecha de la tabla aparece el cardinal de la tabla que muestra el número de equipos dados de alta en la BD.

Significado de los campos de la tabla:

Id	Identificador del equipo. En caso de equipos con IP dinámica, será el número de serie.
Dir: IP	Es la dirección IP estática (o dinámica en caso de tenerla) asignada al equipo que se utilizará para gestionarlo.
Equipo	Es el modelo del equipo. Para más información acerca de los códigos de equipo consultar el apartado Códigos y modelos de equipo.
Modificado	Indica el instante en que se modificó por última vez el registro de la tabla.

Esta área de la ventana tiene asociado, también, un menú de comandos. En el se pueden realizar cuatro acciones:

Comando	Descripción
Editar	Al seleccionar este comando, aparece la ventana de edición de equipos. Esta ventana se actualiza con el contenido del equipo cada vez se seleccione uno en la lista.

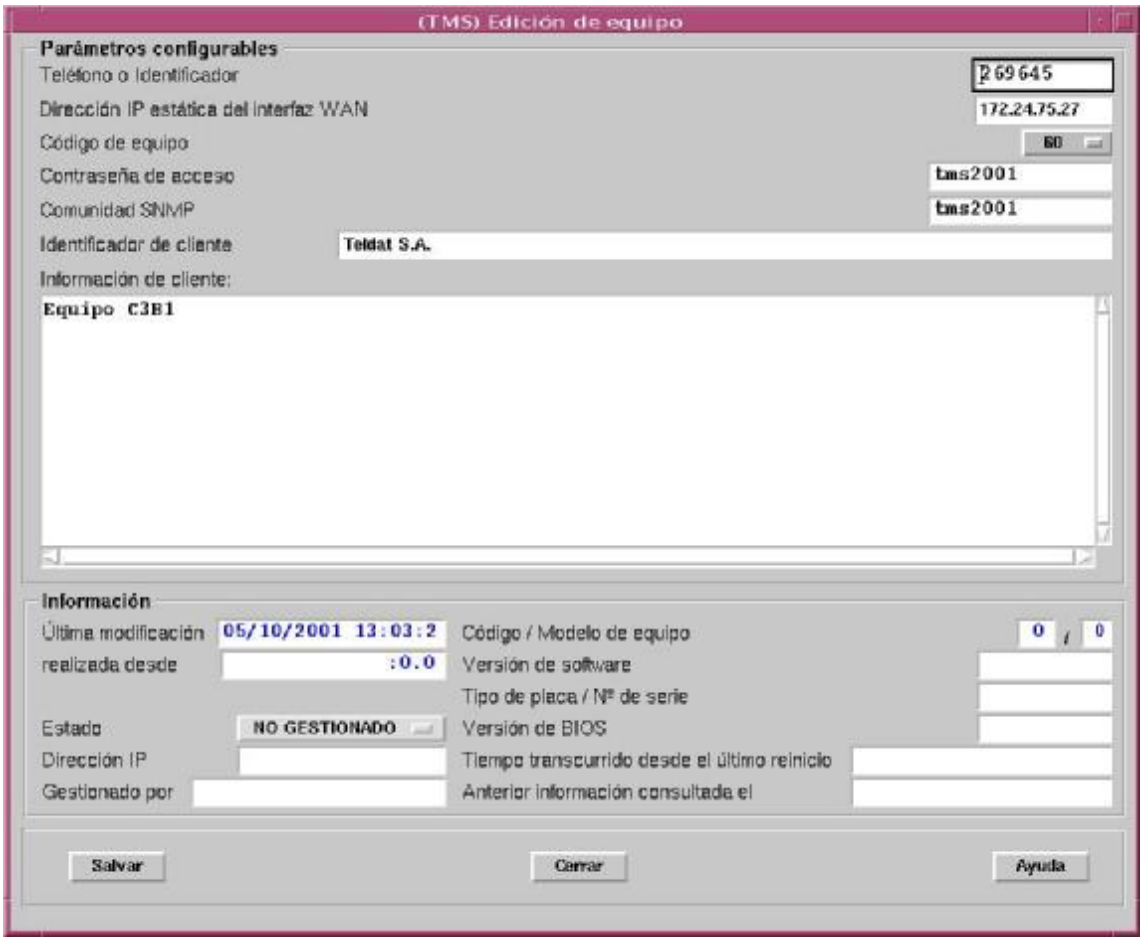


Figura 5 : Ventana de edición de equipo.

En el caso de que al seleccionar **Editar** en el menú de comandos se tenga seleccionado un equipo, se editan los parámetros de dicho equipo. Si por el contrario, no se ha seleccionado ninguno, se crea uno nuevo y se añade a la base de datos. Los campos configurables del registro asociado a un equipo en la base de datos son:

En **Parámetros configurables:**

Teléfono:

Es el identificador del equipo, que para el caso de los routers RDSI se corresponde con su número de teléfono, y para equipos con dirección IP dinámica, con su número de serie.

Dirección IP estática del interfaz WAN:

Es la dirección IP asignada a los equipos que tienen conexión permanente o casi permanente. Cuando existe esta dirección el operador puede intentar gestionar el equipo a su través sin utilizar un router maestro ni llamada de gestión.

Modelo de equipo:

Indica el tipo de equipo del que se trata.

Contraseña de acceso:

Es la contraseña que solicita el equipo cuando se trata de acceder a él por TELNET o por FTP. Se admiten hasta 31 letras y dígitos.

Comunidad SNMP:

Es la comunidad SNMP con la que el usuario pretende acceder al equipo. Sólo se puede acceder a un equipo si la comunidad de acceso SNMP de su configuración coincide con la de su ficha. Admite hasta 31 caracteres y no se admiten blancos.

Identificador de cliente:

Se trata de una cadena de hasta 80 caracteres que sirva para realizar consultas a la base de datos para agrupaciones de informes o grupos de equipos por clientes.

Información de cliente:

Es un campo para guardar información del cliente al que pertenece el equipo. Un contenido típico de este campo puede ser: persona de contacto, teléfono, dirección, versión de software, etc.

En **Información:**

Última modificación:

Indica el instante de la última modificación del registro de la tabla **infomanaged** de donde se toma la información.

realizada desde:

Indica la estación que realizó la actualización de dicho registro.

Estado:

Representa el estado del equipo y puede ser NO GESTIONADO, ACCESIBLE o CONSULTANDO. En el caso de estar ACCESIBLE aparecerá la Dirección IP del equipo en la ventana. Aparece en el bloque de información y no puede ser modificado.

Dirección IP:

Representa la dirección IP, en formato numérico.

Gestionado por:

Identificador del router maestro que está gestionando al equipo cuando su estado es ACCESIBLE. Esta situada en el bloque de información de la ventana de edición de

router maestro y no puede ser modificada por el usuario. Si el equipo está ACCESIBLE y este campo está vacío es porque se está gestionando por su dirección IP estática. Este dato no se muestra para los routers Teldat Cx.

Código y modelo de equipo:

Estos valores se han leído directamente del equipo. Pudiera darse el caso de que no coincidieran con el código de equipo configurado por el usuario (por ejemplo cuando se ha cambiado físicamente el equipo por otro con código distinto desde la última recogida de información) y, en este caso, el usuario debería ponerlo en gestión y pedirle la configuración para cerciorarse de tipo de equipo que es y modificarlo en la base de datos si fuera pertinente. Estos datos no se muestran para los routers Teldat Cx.

Versión de software:

Es una cadena de caracteres que identifica la versión de software del equipo.

Tipo de placa/Nº de serie:

Indica el número de serie y el tipo de placa hardware del equipo.

Versión de BIOS:

Versión del programa de arranque que está en la memoria EPROM del equipo.

Tiempo transcurrido desde el último reinicio:

Este campo contiene el valor de la variable de la MIB denominada "sysuptime" o tiempo desde el último reinicio. En el equipo y en la base de datos se almacena en centésimas de segundo, pero al usuario se le muestra en días horas minutos y segundos.

Anterior información consultada el:

Instante en que se leyó la anterior información del equipo.

Gestionar Cuando hay seleccionado un router maestro en la lista este comando envía una orden al maestro para añadir el equipo seleccionado a su lista de equipos en gestión. Cuando no hay ningún maestro seleccionado el equipo se intenta gestionar por su dirección IP estática. En la línea de estado de la ventana aparece un mensaje indicando si la operación ha tenido éxito. El proceso **tmssynchro** actualizará la base de datos y en la siguiente lectura que la aplicación realice de la base de datos se refrescará la lista de equipos en gestión con el nuevo equipo.

Cuando el maestro establezca contacto con el equipo aparecerá su dirección IP indicando que está accesible. Si un equipo está siendo gestionado por su dirección IP estática y no responde habrá que intentar su gestión a través de un maestro de forma convencional.

Si se intenta gestionar un equipo que ya está siendo gestionado se presenta un mensaje de error.

Si se intenta gestionar un equipo Cx a través de un router maestro se presenta un mensaje de error.

Borrar Borra el equipo de la base de datos. Antes de proceder al borrado se presenta la siguiente ventana de confirmación:

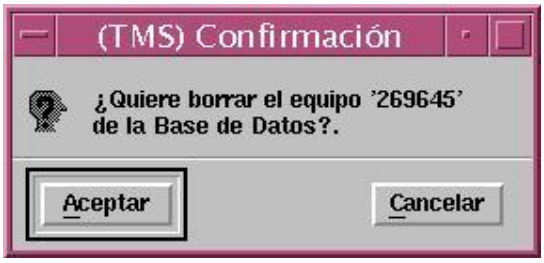


Figura 6 : Confirmación de borrado de equipo

Si se pulsa **Aceptar** se borra el equipo de la base de datos, si se pulsa **Cancelar** se abandona la operación.

Buscar Bajo la lista de equipos de la base de datos se encuentra un recuadro de texto que sirve para buscar un equipo concreto a partir de su identificador. Cada vez que se modifica el contenido del recuadro de texto el programa busca el primer equipo de la lista cuyo identificador comienza por la cadena introducida en el recuadro.

2.5. Lista de equipos en gestión

Esta área se corresponde con el estado de los equipos que están siendo gestionados por el maestro seleccionado en la lista de routers maestros, por su dirección IP estática cuando no hay ningún maestro seleccionado o bien por su dirección IP dinámica si tienen una asignada.

Para ver los equipos gestionados por su dirección IP estática o dinámica basta con no seleccionar ningún router maestro en la lista superior. Hay que tener en cuenta que si un equipo con dirección IP dinámica se desconecta, se deja de gestionar automáticamente pasado un tiempo.

La cabecera de la lista indica el router maestro a través del que están siendo gestionados. Si no hay seleccionado ningún router maestro se muestran los equipos.

Esta lista se refresca con los resultados obtenidos de la petición periódica de estado de la lista de equipos en gestión al maestro que realiza el proceso "tmssynchro" y de la consulta a la tabla **infomanaged** de la base de datos.

Al igual que en las otras dos áreas, ésta tiene asociada un menú de comandos. El único comando que se puede ejecutar es **Desgestionar**. Este comando provoca que el router maestro seleccionado en la lista superior borre de su tabla de equipos en gestión al equipo seleccionado (no se borra de la base de datos). Tras esta operación el maestro cesa su envío periódico de "echo" y el equipo gestionado liberará la llamada RDSI tan pronto como venza su **Tiempo de liberación sin datos** para las llamadas de gestión. A partir de la **versión 5.0** el tiempo de liberación sin datos de las llamadas de gestión se establece en 1 minuto. Antes de esta versión se utilizaba el tiempo de liberación sin datos configurado

en el equipo canal RDSI correspondiente). Si el equipo está siendo gestionado por su dirección IP estática cuando se desgestiona se borra de la tabla **infomanaged** para que otro usuario pueda gestionarlo.

El refresco periódico sólo es visible para los equipos gestionados por el router maestro que esta seleccionado (o para los equipos gestionados por su dirección IP estática si no hay ningún maestro seleccionado) aunque este refresco se realiza para todos los equipos gestionados por todos los routers maestros.

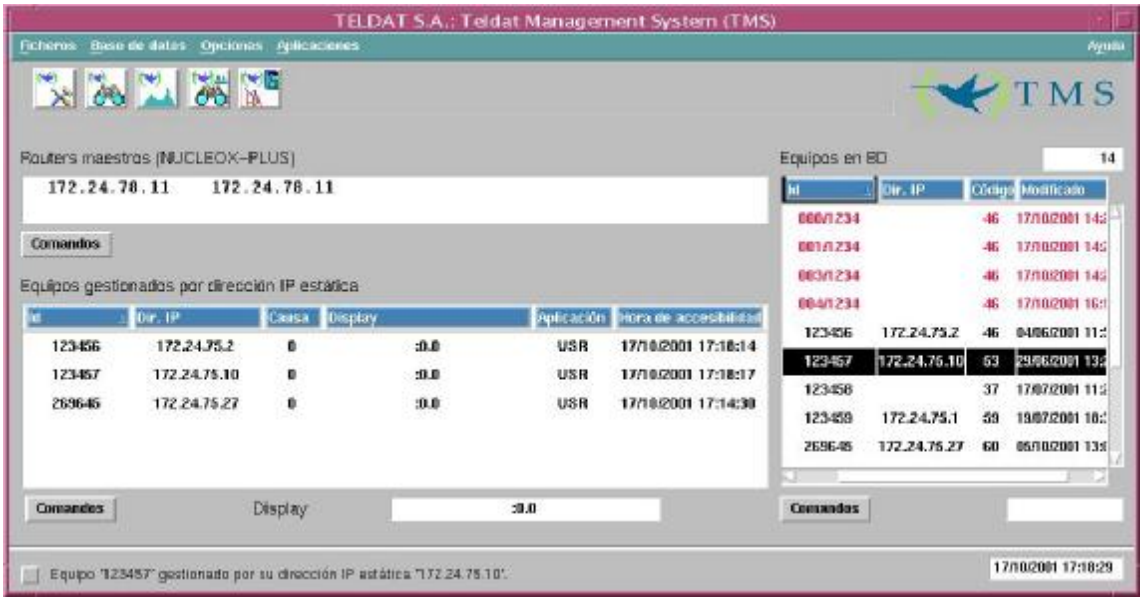


Figura 7 : Equipos gestionados por su dirección IP estática

Id:
Identificador del equipo en gestión.

Dir. IP:
Dirección IP asignada al equipo en su interfaz WAN. Si está siendo gestionado a través de un router maestro es asignada dinámicamente por el CPI. Si se está gestionando por su dirección IP estática es la asignada contractualmente por el proveedor del servicio.

Causa:
Es una indicación de la causa por la que se liberó la última llamada proporcionada por la red RDSI según la norma Q931 de ISO. Este dato no tiene sentido para el caso del router Teldat Cx.

> ***A partir de la versión 1.4.1 del router maestro la causa de liberación RDSI sólo es significativa cuando el número de equipos gestionados en estado CONSULTANDO en el router maestro es menor o igual a dos.***

Para más información acerca de las causas de liberación RDSI consultar Causas de liberación RDSI.

Display:
En este campo entre se indica la dirección IP de la estación que puso el equipo en gestión. Es el contenido de la variable de entorno **DISPLAY** que identifica el display desde el que se puso en gestión al equipo (ver referencia a gestión multidisplay mas adelante).

Aplicación:
Indica si el equipo ha sido puesto en gestión por una aplicación de gestión manual (de usuario), en cuyo caso aparece la cadena **USR**, o si, por el contrario, ha sido puesto en gestión por una operación sobre grupos en cuyo caso la cadena es **AUTO**.

Hora de accesibilidad:
Es el instante en que el equipo obtuvo su dirección IP y por tanto se estableció la llamada de gestión. Sirve para que el operador tenga constancia de la duración de la llamada de gestión.

2.6. Indicador de lectura de BD y último comando ejecutado

En el extremo inferior izquierdo de la ventana se encuentra un pequeño cuadrado cuya función es monitorizar la lectura periódica de la base de datos y la actualización de la ventana. Durante el intervalo de lectura y actualización se pone en color verde. Si el número de equipos en la base de datos es pequeño, es posible que el cambio de color apenas se aprecie.

A la derecha del indicador se presenta a modo de confirmación el resultado del último comando ejecutado por el usuario. Hay comandos cuyo resultado no se muestra instantáneamente, sino que hay que esperar hasta recibir respuesta del equipo o hasta el próximo refresco de la ventana. En tales casos, el texto que aparece en el borde inferior de la ventana confirma al usuario que su acción ha sido cursada.

ATENCIÓN

Liberación de llamada:

El hecho de que un equipo esté siendo gestionado por un router maestro supone que el segundo está enviando periódicamente comandos "echo" al primero para mantener el enlace a través de RDSI evitando de esta forma que el equipo gestionado libere la llamada por ausencia de tráfico. Si la aplicación se interrumpe de forma incontrolada o si se abandona sin desgestionar los equipos, estos mantendrán activa la llamada RDSI de gestión durante 1 hora (en versiones del router maestro anteriores a la 1.3.0 se mantenía indefinidamente).

Máximo intervalo permitido para un equipo en estado CONSULTANDO.

A partir de la versión 1.3.0 del router maestro, el máximo intervalo que el maestro permite que un equipo esté en estado CONSULTANDO es de 5 minutos (frente a los 10 minutos de versiones anteriores).

Ralentización en el cambio de estado de los equipos gestionados:

Si en la base de datos hay routers maestros inaccesibles o que no responden, esto retardará el refresco del estado de los equipos gestionado en función del número de intentos y time-out asociados a dichos maestros. Por ello, se recomienda tener en la base de datos únicamente los routers maestros que se estén utilizando en cada instante.

3. Últimos equipos disponibles

Gracias a la capacidad de descubrimiento de dirección IP dinámicas, todos los equipos que envían su dirección a TMS cuando **ipdiscover** está en ejecución, serán registrados en la tabla **last_devices**. Se puede obtener un informe mediante la ejecución del script **`$TELDATMS/script/showlastdevices.sh`**. Este script se encarga además de limpiar la tabla, por lo que es conveniente generar un informe periódicamente. Con este informe se podrá saber que equipos se han conectado alguna vez desde la última vez que generamos el informe.

La apariencia del informe es similar a:

```
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.
```

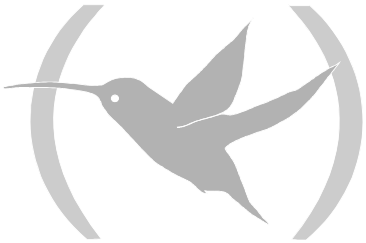
4. Auditoría de intervenciones

En la base de datos se guarda la fecha, la hora, la duración y la estación que realizó la llamada para todas las llamadas de gestión. Se guardan en la tabla **mancalls** y se pueden generar informes con el script **`$TELDATMS/etc/db/$TMSLANG/showmancalls.sql`**.

La apariencia del informe es similar a:

```
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.
```

Capítulo 4
Gestión de equipos



1. Configuración

La configuración de los equipos NOVACOM y Teldat C se lleva a cabo con la aplicación **tmsconfig** que puede lanzarse desde cualquiera de las otras aplicaciones o desde la línea de comando con las siguientes opciones:

```
>tmsconfig [-h] [-t <tiempo de refresco en segundos>] [-i <direccion IP> -c <comunidad
SNMP> -id <Id. equipo>]
```

El tiempo de refresco indica el período con el cual la aplicación lee de la base de datos el estado de los equipos para seleccionar aquellos que están accesibles.

El resto de parámetros permiten el acceso a un equipo que no se encuentre en la base de datos con la condición de poner un tiempo de refresco suficientemente alto para que la aplicación no refresque la ventana con el estado de los equipos.

La opción -h presenta las opciones de uso.

La ventana de **edición de configuración**, se utiliza para lanzar los comandos de comunicación con el equipo relativos a configuración. Desde esta ventana se pueden realizar las siguientes tareas sobre el equipo accesible seleccionado en la ventana principal:

* Pedir la configuración.
* Enviar la configuración.
* Guardar la configuración del equipo en la memoria FLASH.
* Rearrancar el equipo con la configuración de su memoria FLASH.
* Enviar un nuevo software al equipo.
* Sincronizar la hora del equipo con la estación de gestión.
* Telecarga.

También se pueden realizar operaciones con ficheros:

* Modificar la configuración leída.
* Leer la configuración de fichero.
* Guardar la configuración en fichero.
* Visualizar el fichero de log.

Operaciones con la base de datos:

* Leer una configuración de la base de datos.
* Escribir una configuración en la base de datos.

1.1. Parámetros de configuración

Dependiendo del tipo de equipo, los parámetros de configuración que se usan, van a ser diferentes, por lo que seguidamente se analizan los mismos de forma separada.

a) ***General***

- ***Equipos NOVACOM y NOVACOM-X25***

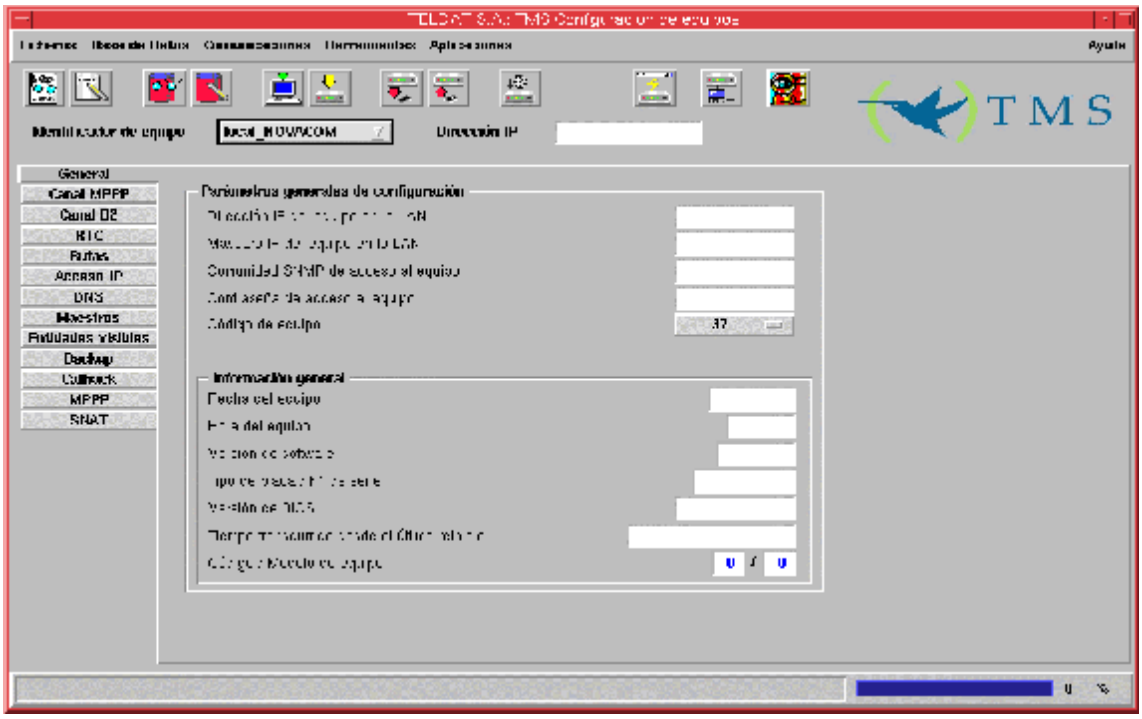


Figura 8 : Configuración general

Parámetros generales que se pueden modificar:

- **Dirección IP del equipo en la LAN:** Es la dirección IP del interfaz LAN del equipo.

- **Máscara IP del equipo en la LAN:** Es la máscara de la dirección IP del interfaz LAN del equipo.

- **Comunidad SNMP de acceso al equipo:** Es la comunidad SNMP que el equipo autoriza que le gestione. Sólo se puede acceder a un equipo si la comunidad de acceso SNMP de su configuración coincide con la de su ficha. Admite hasta 31 caracteres y no se permiten blancos.

- **Contraseña de acceso al equipo:** Es la palabra de paso al equipo para la conexión a través de TELNET y FTP. Si se omite, no se pedirá clave de acceso cuando se realice TELNET o FTP. No admite blancos y el número máximo de caracteres es 31.

- **Código de equipo:** Permite definir para qué tipo de equipo es la configuración que se muestra en la ventana. En función de la selección pueden habilitarse o inhabilitarse el acceso a ciertas entidades. En el caso normal, este código deberá coincidir con el leído por SNMP del propio equipo y que se muestra en la parte informativa de la solapa. Si no coincidiesen, el operador

deberá investigar la causa. Simplemente, puede haberse cambiado el equipo remoto y, en tal caso, habrá que actualizar su ficha en la base de datos. La aplicación no permite enviar una configuración a un equipo si no coinciden el código de equipo configurado con el que realmente tiene.

- **Interfaz del equipo:** Permite definir que tipo de interfaz utiliza el equipo, identificando si utiliza X.25 o tiene alojada una impresora a su línea serie (ASDP).

Parámetros de información que NO se pueden modificar:

- **Fecha y hora del equipo:** Indica la fecha y hora del equipo en el momento en el que se le pidió la configuración.

- **Versión de software:** Es una cadena de caracteres que identifica la versión de software con la que arrancó el equipo al que se pidió la configuración.

- **Tipo de placa/Nº de serie:** Indica el número de serie y el tipo de placa hardware del equipo al que se le pidió la configuración.

- **Versión de BIOS:** Versión del programa de arranque que está en la memoria EPROM del equipo.

- **Tiempo transcurrido desde el último reinicio:** Contiene el valor de la variable de la MIB denominada "sysuptime" o tiempo desde el último reinicio. En el equipo y en la base de datos se almacena en centésimas de segundo, pero al usuario se le muestra en días, horas, minutos y segundos.

Estos parámetros de información se guardan en la tabla **infodevice** de la base de datos cada vez que se pide la configuración al equipo.

Cuando se lee una configuración de la base de datos, las etiquetas de fecha y hora del equipo cambian para expresar que las nuevas fecha y hora son las que tenía la estación de gestión cuando se obtuvieron los parámetros informativos. Dicha fecha no tiene por que coincidir con la fecha en la que se pidió la configuración.

- ***Equipos Cx***

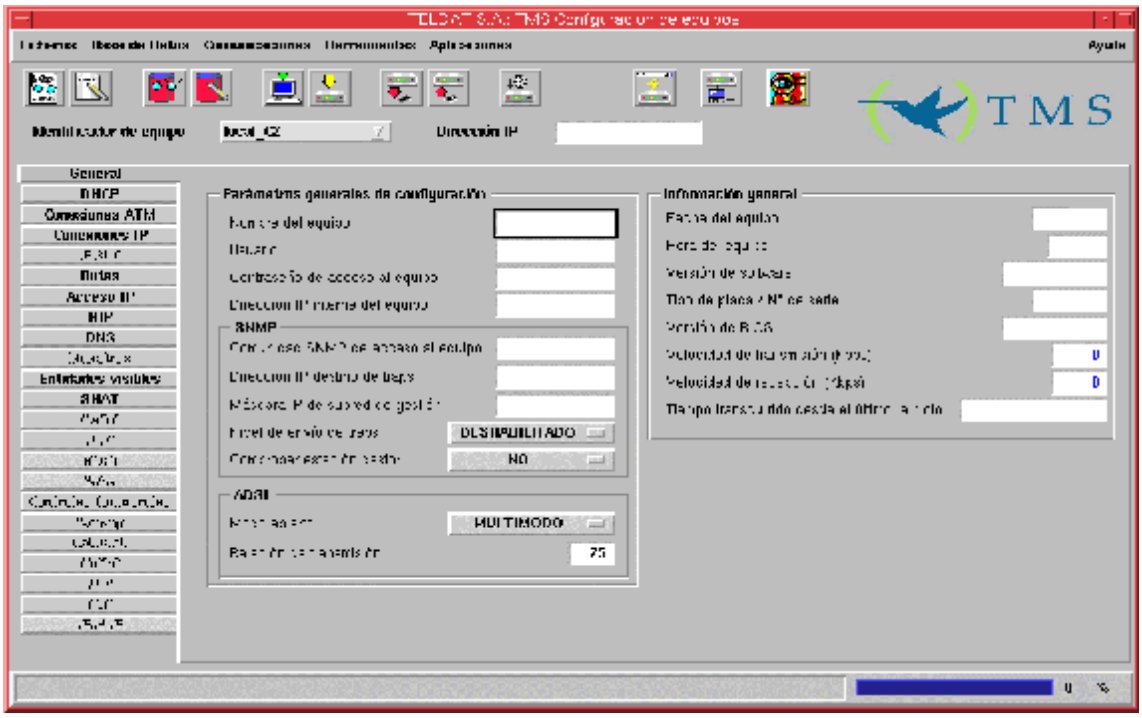


Figura 9 : Configuración general

Parámetros que se pueden modificar :

- **Nombre del equipo:** Nombre con el que se desea identificar al router.
- **Usuario:** Nombre del usuario con permisos para acceder al equipo.
- **Contraseña de acceso al equipo:** Es la palabra de paso al equipo para la conexión a través de TELNET y FTP. Si se omite, no se pedirá clave de acceso cuando se realice TELNET o FTP. No admite blancos y el número máximo de caracteres es 31.
- **Dirección IP interna del equipo:** Dirección IP de uso interno del equipo.
- **Comunidad SNMP de acceso al equipo:** Es la comunidad SNMP que el equipo autoriza que le gestione. Sólo se puede acceder a un equipo si la comunidad de acceso SNMP de su configuración coincide con la de su ficha. Admite hasta 31 caracteres y no se permiten blancos.
- **Dirección IP destino de traps:** Es la dirección IP a la que el router enviará las traps SNMP que tenga habilitadas. El puerto al que el equipo envía las traps es el 162.
- **Máscara IP de subred de gestión:** Se trata de una máscara IP que junto a la dirección IP anterior define la subred a la que el equipo contestará peticiones SNMP. El valor "0.0.0.0" (o vacío) indica que el router responderá a cualquier dirección IP y el valor "255.255.255.255" indica que sólo la estación destinataria de traps puede hacerle peticiones SNMP.

- **Nivel de envío de traps:** Hay cuatro niveles de traps: NINGUNO, BAJO, MEDIO y ALTO. Excepto en NINGUNO, en la que no se envía ninguna trap, en todas las demás se mandan todas las traps genéricas así como las "enterprise" que se habiliten. El nivel de trap determina las traps "enterprise" que se van a mandar:

  * BAJO: las traps definidas como ERROR.
  * MEDIO: las traps anteriores más las traps de información de eventos inesperados.
  * ALTO: las traps definidas como error o como información.

- **Comprobar estación gestor:** Indica si el equipo debe comprobar que su estación gestora es alcanzable a través de la red.

- **Modo abierto:** Modo de transmisión en ADSL.

- **Relación de transmisión:** Relación entre el tráfico recibido y el enviado.

- **Velocidad de transmisión [Kbps]:** Velocidad de transmisión para el interfaz ADSL en Kbps.

- **Velocidad de recepción [Kbps]:** Velocidad de recepción para el interfaz ADSL en Kbps.

Parámetros de información que NO se pueden modificar:

- **Fecha y hora del equipo:** Indica la fecha y hora del router en el momento en el que se le pidieron los parámetros informativos.

- **Versión de software:** Es una cadena de caracteres que identifica la versión de software con la que arrancó el router.

- **Tipo de placa/Nº de serie:** Indica el número de serie y el tipo de placa hardware del router C2.

- **Versión de BIOS:** Versión del programa de arranque que está en la memoria EPROM del router.

- **Tiempo transcurrido desde el último reinicio:** Se obtiene a partir de la variable de la MIB que contiene el denominado "sysuptime" o tiempo que lleva el router encendido. En el equipo y en la base de datos (tabla **inforouters**) se guarda en centésimas de segundo pero al usuario se le muestra en días, horas, minutos, segundos y centésimas de segundo. Hay que tener en cuenta que a dicho tiempo hay que sumarle el intervalo que va desde la hora en que se pidió el valor al router hasta el instante actual.

Cada vez que se pide la configuración al router o se leen sus estadísticos quincenales con la aplicación de recogida automática de estadísticos se piden también los parámetros informativos y se guardan en la tabla **inforouters**.

Cuando se lee una configuración de la base de datos, las etiquetas de fecha y hora del router cambian para expresar que las nuevas fecha y hora son las que tenía la estación de gestión cuando se obtuvieron los parámetros informativos. Dicha fecha no tiene por que coincidir con la fecha en la que se pidió la configuración.

b) Canal B1 (solo para equipos NOVACOM y NOVACOM-X25)

Hay una ventana de configuración por cada uno de los dos canales B RDSI de los que dispone el equipo y otra para el canal RTC (con el mismo aspecto). En cada una de ellas se configura el destino y las propiedades de la conexión que el equipo establecerá por cada canal.

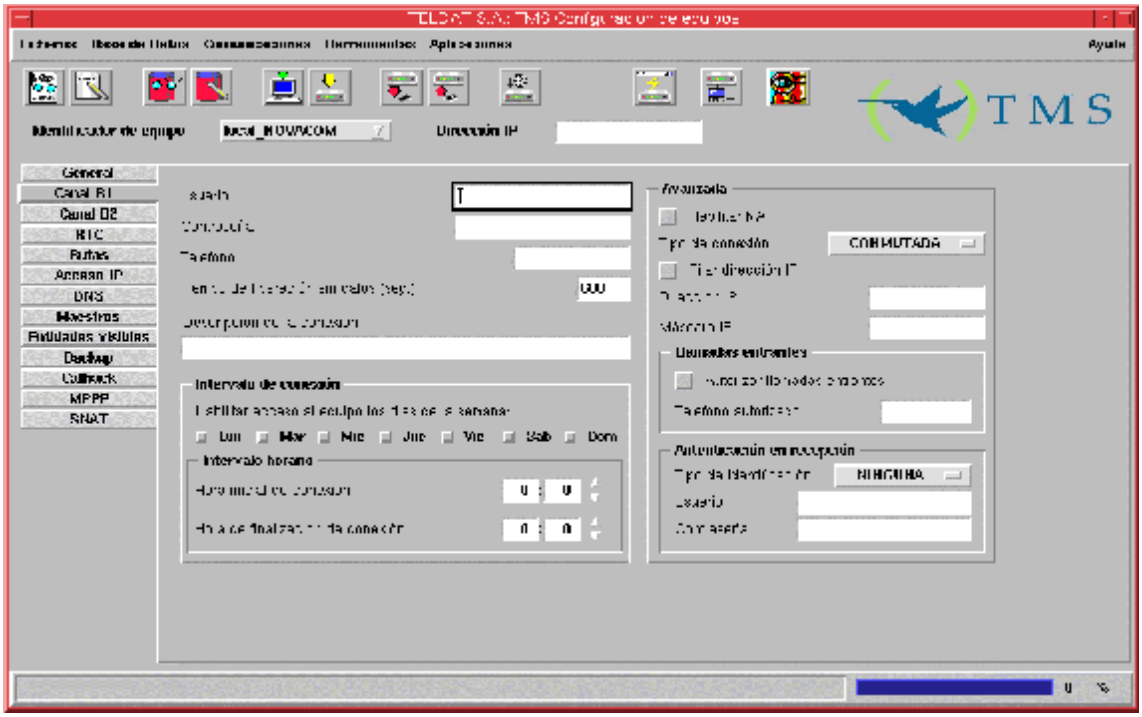


Figura 10 : Configuración del canal B1 RDSI

- **Usuario:** Usuario a través del que se accede al servicio. Lo suministra el proveedor y lleva asociados una dirección IP de conexión y ciertos privilegios. Se admiten hasta 31 caracteres.

- **Contraseña:** Contraseña de acceso asociada al usuario anterior (suministrada por el proveedor del servicio). Su máxima longitud es de 31 caracteres.

- **Teléfono:** Es el teléfono al que el equipo demanda la conexión. Para minimizar el coste de las llamadas es conveniente utilizar el teléfono del Nodo de Acceso más próximo al equipo. Se admiten un máximo de 19 dígitos.

- **Tiempo de liberación sin datos (seg):** Las conexiones se terminarán normalmente por ausencia de datos en la línea un tiempo igual o superior al tiempo de liberación sin datos. El valor por defecto es de 600 segundos. No es recomendable usar tiempos demasiado bajos. La

precisión del temporizador es de T/10 siendo T el tiempo de liberación sin datos. Se permiten valores en el rango [0, 60 .. 65535] siendo 600 segundos el valor por defecto. El valor 0 es un caso especial que equivale a una conexión permanente. Este valor se utiliza, por ejemplo, como medio para unir subredes. Si hay establecido un control horario y el tiempo de liberación sin datos es 0, entonces, el equipo establece conexión con en el instante en que comienza el período horario de accesibilidad. De esta forma, en dicho período, el cliente puede comunicar sus subredes. Si no hay restricciones horarias y se asigna el valor 0, el equipo establece una conexión permanente tras el arranque.

- **Descripción de la conexión:** Cadena de hasta 79 caracteres cualesquiera de información del tipo de conexión que se establecerá por el canal.

- **Intervalo de conexión:** Sirve para restringir el tráfico a través del equipo a un intervalo temporal ciertos días de la semana o para forzar la conexión del equipo en dicho intervalo. El intervalo de conexión especifica el período en que el equipo estará operativo. Fuera de este intervalo el interfaz está bloqueado, excepto para conexiones de gestión, que siempre están garantizadas.

    - Seleccionar los días de la semana en los cuales el equipo funcionará normalmente.

    - Introducir el instante de comienzo del intervalo y el instante final del intervalo en formato **hh:mm**. Para la hora se admiten valores dentro del intervalo [0..23] y para los minutos [0..59]. Si la hora final es menor que la inicial se considera que pertenece al día siguiente. Si el día siguiente no está permitida la conexión tiene prioridad el día sobre la hora y la conexión estará deshabilitada para dicho día.

    - Cuando el tiempo de liberación sin datos es 0, el equipo se conecta automáticamente al comenzar el intervalo temporal establecido en la configuración horaria.

Configuración avanzada:

- **Habilitar NAT:** Por defecto, el equipo realiza **Network Address Translation (NAT)** extendido en las conexiones definidas. De esta forma usa sólo una dirección IP para conectar a un número indefinido de puestos locales a redes externas como INTERNET. Si no se desea este funcionamiento, sino que se quiere que las estaciones de la LAN a la que está conectado el equipo salgan como tales al exterior se puede deshabilitar NAT. Para más información acerca de NAT puede consultarse la referencia {Teldat: NAT, 99}.

- **Tipo de conexión:** Indica el tipo de conexión que se establece en el canal. Si el usuario tiene contratado con el proveedor de RDSI un canal B RDSI permanente, debe indicarlo con este parámetro. Un canal B permanente es un canal B RDSI especial que no utiliza la señalización porque su destino está fijado en la contratación del servicio. Dicho canal B no hace llamadas RDSI y siempre está conectado. Si habilita un canal B como **PERMANENTE**, los parámetros de teléfono destino de la conexión, tiempo de liberación por ausencia de datos e intervalo de conexión permitido son ocultados. En la contratación del canal B permanente se especifica qué canal B (B1, B2 o ambos) responde a este perfil. No se permite que los dos canales tengan conexión permanente porque, en tal caso, el equipo dejaría de ser gestionable. El valor por defecto es **CONMUTADA**.

- **Fijar dirección IP:** En un escenario normal de acceso a una red externa como INTERNET, el equipo se conecta contra un servidor de terminales. Dicho servidor de terminales asigna al equipo una dirección IP cada vez que se conecta. La política de asignación de direcciones IP en función del usuario llamante suele corresponder al proveedor de acceso a la red externa y, en general, no garantiza que llamadas consecutivas del mismo usuario reciban la misma dirección IP. Sin embargo, es posible trabajar en entornos en donde el direccionamiento WAN debe ser fijo y conocido a priori. Por ejemplo, para interconectar dos redes remotas a través de dos equipos. Mediante los parámetros de dirección IP y máscara se define el direccionamiento WAN de la conexión. El equipo, por defecto, solicita al extremo remoto la asignación de dirección IP. Si se habilita esta opción aparecen debajo dos campos en los que se puede indicar la dirección IP y máscara asociadas a la conexión de este canal. Si dichos campos se dejan en blanco es equivalente a deshabilitar la opción.

- **Dirección IP:** Si se habilita la opción anterior, establece la dirección IP de la conexión a través del canal.

- **Máscara IP:** Es la máscara IP que se aplica a la dirección anterior.

- **Autorizar llamadas entrantes:** Como equipo de acceso, es el propio equipo el que realiza la llamada al proveedor de la red externa a la que se quiere conectar. Sin embargo, en escenarios de conexión entre dos equipos, uno realiza la llamada y el otro la recibe. Si se desea que un equipo pueda recibir llamadas entrantes, debe habilitarse este parámetro. El comportamiento por defecto del equipo es no permitir las llamadas entrantes.

- **Teléfono autorizado:** Si las llamadas entrantes están habilitadas, este parámetro indica el número RDSI que está autorizado para conectarse. Si no se configura ningún valor, cualquier llamante estará autorizado para conectarse, aunque deberá autenticarse vía PAP o CHAP si así se le indica.
- El valor por defecto (vacío) de este parámetro autoriza a cualquier número llamante.

- **Tipo de autenticación en recepción:** Lo habitual al acceder a una red externa es que sea la propia red externa la que solicite al equipo de acceso que se autentique como paso previo a poder usar la red. Sin embargo, en escenarios punto a punto, donde no se accede a una red externa, sino a una red remota conocida, a través de un equipo remoto también conocido, es posible indicar al extremo remoto que necesita autenticarse. El equipo soporta los protocolos de autenticación PPP **Password Authentication Protocol (PAP)** y **Challenge Handshake Authentication Protocol (CHAP)**.

- **Usuario remoto:** Si se exige autenticación al extremo remoto, este parámetro indica el login de usuario remoto permitido para esta conexión. El equipo validará el login remoto recibido vía PAP o CHAP con el configurado en este parámetro. Es una cadena de hasta 31 caracteres.

- **Contraseña de usuario remoto:** Si se exige autenticación al extremo remoto, este parámetro indica la contraseña de usuario remoto permitido para esta conexión. El equipo validará la contraseña remota recibida vía PAP o CHAP con la configurada en este parámetro. Se admiten hasta 31 caracteres.

c) ***Rutas IP***

• *Equipos NOVACOM y NOVACOM-X25*

En esta ventana se indica al equipo hacia donde tiene que encaminar los paquetes para llegar a su destino.

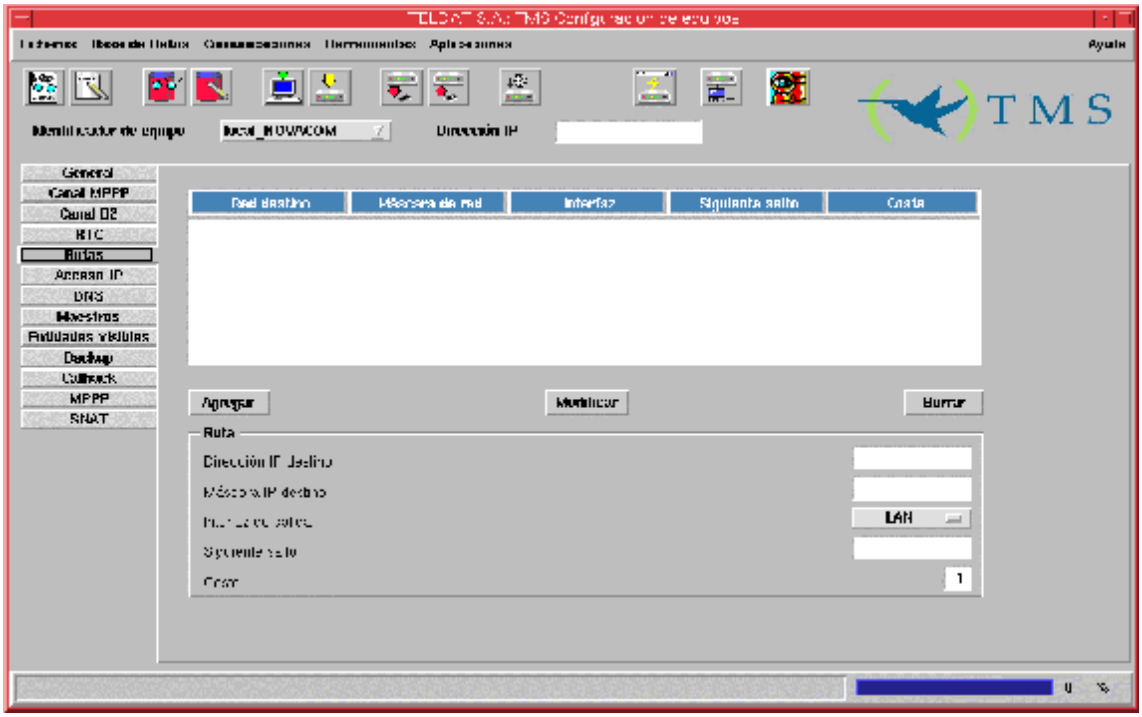


Figura 11 : Configuración de rutas IP

- **Dirección IP destino:** Dirección IP de la estación o la subred a la que va dirigido el tráfico. La dirección 0.0.0.0 junto a la máscara 0.0.0.0 indica que es la ruta por defecto del equipo.

- **Máscara IP destino:** Máscara IP de la subred destino.

- **Interfaz de salida:** Interfaz asociado a la ruta.

- **Siguiente salto:** Dirección IP del siguiente equipo que se encargará de encaminar el paquete. Sólo tiene sentido cuando la interfaz seleccionado anteriormente es el LAN, sino se oculta este campo.

- **Coste:** Coste asociado a la ruta. Se permiten valores en el rango [0 .. 16].

- ***Equipos Cx***

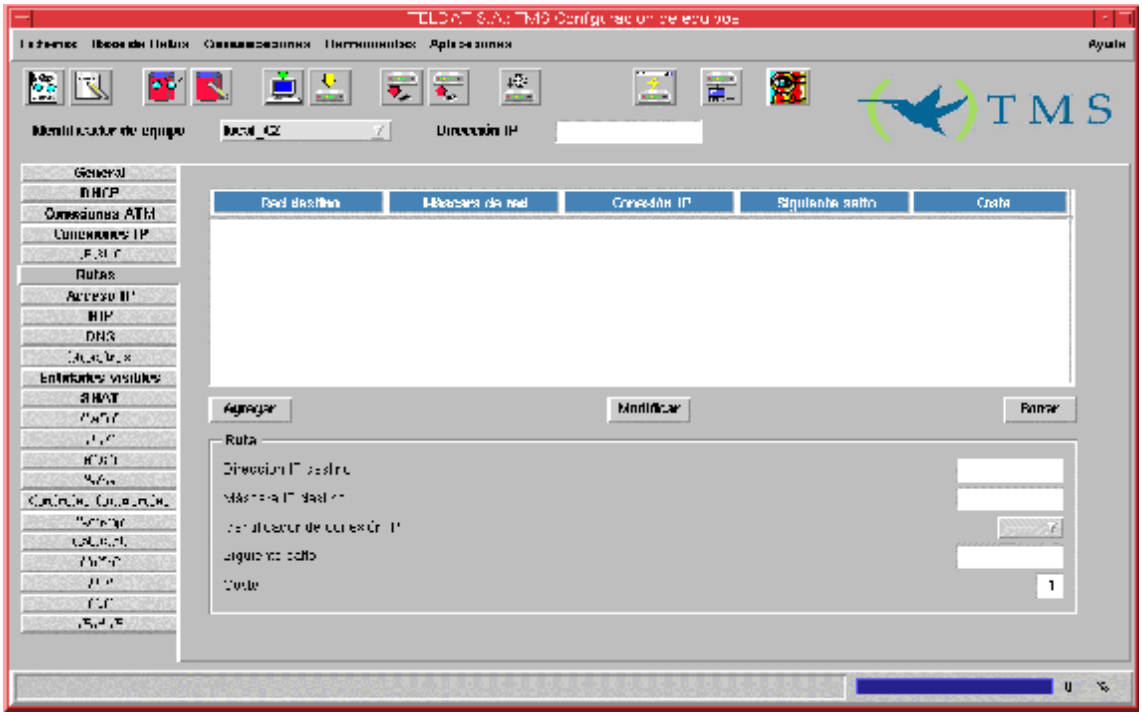


Figura 12 : Configuración de rutas IP

Dirección IP destino: Dirección IP de la estación o la subred a la que va dirigido el tráfico. La dirección 0.0.0.0 junto a la máscara 0.0.0.0 indica que es la ruta por defecto del router.

Máscara IP destino: Máscara IP de la subred destino.

Identificador de conexión IP: Referencia la conexión IP por la que se encaminan los paquetes de la ruta. Si su valor es 0 indica que se encaminan por el interfaz LAN.

Siguiente salto: Dirección IP del siguiente router que se encargará de encaminar el paquete. Sólo tiene sentido cuando el interfaz seleccionado anteriormente es el LAN, sino se oculta este campo.

Coste: Coste asociado a la ruta. Se permiten valores en el rango **[0 .. 16]**.

Se admiten hasta un máximo de 200 rutas.

d) Acceso IP

- ***Equipos NOVACOM y NOVACOM-X25***

Cada vez que recibe una dirección IP, el equipo consulta ordenadamente la lista de controles de acceso. Cada uno de ellos se compone de los siguientes campos: Tipo, IP origen, Red origen, IP destino, Red destino, Protocolos, Puertos.

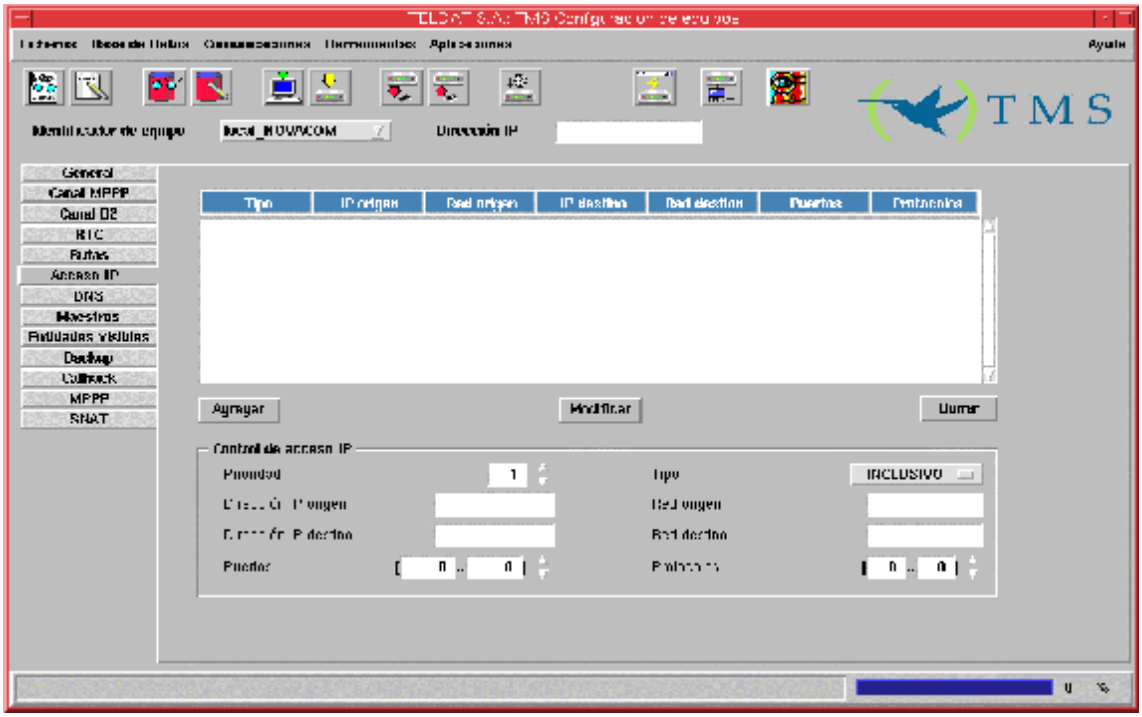


Figura 13 : Configuración de controles de acceso IP

- **Tipo: INCLUSIVO** implica aceptar el paquete y **EXCLUSIVO** rechazar el paquete si encaja en el perfil.

- **IP origen:** Dirección IP de la estación o de la subred origen.

- **Red origen:** Máscara IP de la subred origen. Tiene que ser coherente con la dirección anterior. Para ello la operación AND binario entre la dirección y la negación binaria de la máscara ha de resultar 0. La combinación de dirección y máscara 0.0.0.0 implica "cualquier origen".

- **IP destino:** Dirección IP de la estación o de la subred destino del paquete.

- **Red destino:** Máscara IP de la subred destino. Tiene que ser coherente con la dirección anterior. Para ello la operación AND binario entre la dirección y la negación binaria de la máscara ha de resultar 0. La combinación de dirección y máscara 0.0.0.0 implica "cualquier destino".
- **Puertos :** Rango de puertos a los que puede ir destinado el paquete. Se admiten valores en el rango [0 .. 65535].

- **Protocolos:** Rango de protocolos a los que se puede asociar el paquete. Se admiten valores en el rango [0 .. 255].

El algoritmo es el siguiente:

1. Se realiza el AND binario entre la dirección **IP origen** y la **Red origen** y se comprueba si coincide con el resultado de la misma operación entre la dirección IP del paquete que ha recibido el equipo y la **Red origen**.
2. Se realiza la misma comprobación que en el punto anterior pero ahora con la dirección **IP destino** y la **Red destino**.
3. Se comprueba si el **Protocolo** al que va dirigido el paquete está dentro del rango de protocolos del control de acceso.
4. Se comprueba si el **Puerto** al que va dirigido el paquete está dentro del rango de puertos del control de acceso.
5. Si todos los puntos anteriores se han cumplimentado satisfactoriamente para un paquete, entonces se realiza la operación indicada por Tipo. Las acciones posibles son ***aceptar el paquete*** en el caso de que Tipo sea **INCLUSIVO** o ***rechazar el paquete*** en el caso de que Tipo sea **EXCLUSIVO**.
6. Si no se cumple alguna de las anteriores condiciones se vuelve al punto 1 y se realizan las mismas operaciones con el siguiente registro de la lista de controles de acceso.
7. Si no existen más controles de acceso se acepta el paquete.
8. Es importante el orden en el que se encuentran los controles de acceso pues este orden determina la prioridad.

Para ***agregar*** un nuevo control de acceso se rellenan todos los campos bajo la lista y se pulsa el botón **Agregar**.

Para ***modificar*** un elemento de la lista se selecciona, se modifican los campos correspondientes y se pulsa **Modificar**.

Para ***borrar*** un control de acceso, se selecciona y se pulsa **Borrar**.

En el caso de los **Protocolos** y de los **Puertos**, se establece un rango de valores de funcionamiento. Por ejemplo, si sólo se desean aceptar paquetes SNMP, se seleccionará como Rango de Protocolos [11..11], pues el 11 corresponde al protocolo UDP; y como Rango de Puertos [161..162], que son los que utiliza SNMP.

La gestión TMS utiliza los siguientes puertos en sus comunicaciones con el equipo:

Protocolo	Puerto
FTP	21
TELNET	23
echo privado maestro - equipo	2006
SNMP	161

¡Atención!

Si se introduce un control de acceso totalmente exclusivo y el equipo llega a analizarlo porque los anteriores han fallado, entonces, el equipo desechará indefectiblemente el paquete. En tal caso, es imprescindible garantizar que, al menos, un router maestro y una estación de gestión verifiquen alguno de los controles de acceso inclusivo de mayor prioridad. Si esta condición no se respeta el equipo quedará inaccesible para la gestión

Garantizar la comunicación bidireccional con cualquier equipo mediante un control de acceso inclusivo precisa de dos registros de controles de acceso: uno como origen y otro como destino.

NOTA:

En los controles de acceso, la dirección "0.0.0.0" junto con la máscara "0.0.0.0" equivale a "cualquier dirección IP".

Para conocer los números de los puertos y protocolos asignados en INTERNET se puede consultar la RFC 1700 "INTERNET ASSIGNED NUMBERS" como ayuda para la definición de controles de acceso IP en el equipo. Esta información está disponible en la dirección de Internet ftp://ds.internic.net

- ***Equipos Cx***

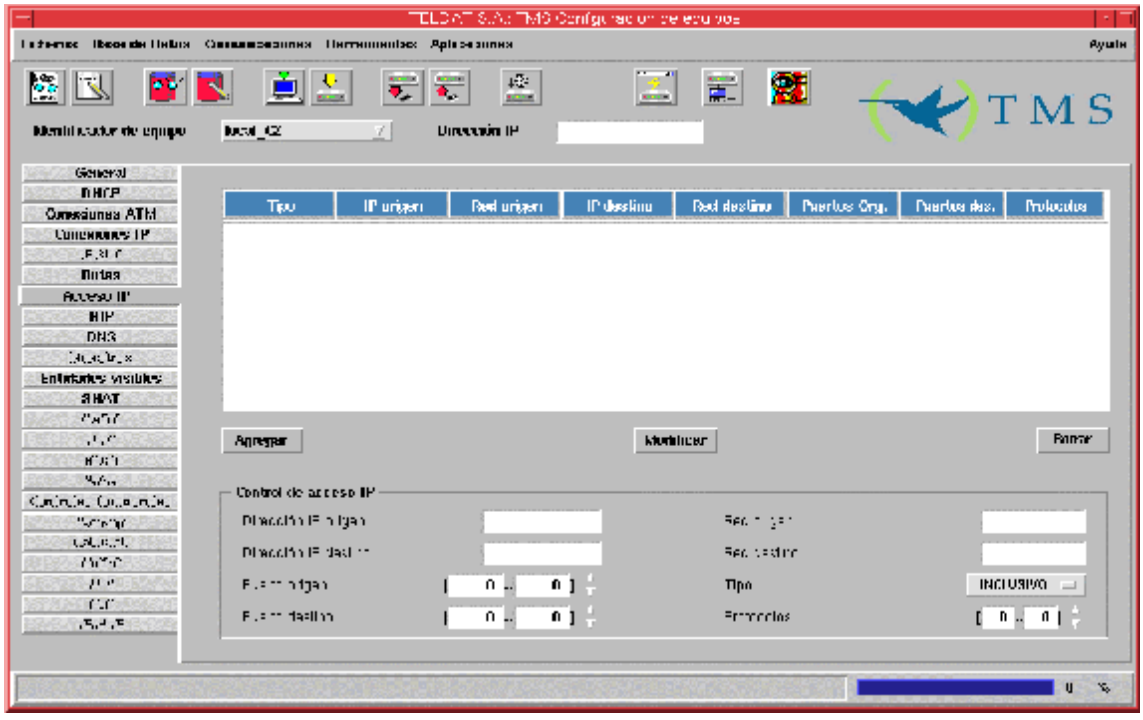


Figura 14 : Configuración de controles de acceso IP

Cada vez que recibe una dirección IP, el router consulta ordenadamente la lista de controles de acceso. Cada uno de ellos se compone de los siguientes campos:

- **Tipo: INCLUSIVO** implica aceptar el paquete y **EXCLUSIVO** rechazar el paquete si encaja en el perfil.

- **IP origen:** Dirección IP de la estación o de la subred origen.

- **Red origen:** Máscara IP de la subred origen. Tiene que ser coherente con la dirección anterior. Para ello la operación AND binario entre la dirección y la negación binaria de la máscara ha de resultar 0. La combinación de dirección y máscara 0.0.0.0 implica "cualquier origen".

- **IP destino:** Dirección IP de la estación o de la subred destino del paquete.

- **Red destino:** Máscara IP de la subred destino. Tiene que ser coherente con la dirección anterior. Para ello la operación AND binario entre la dirección y la negación binaria de la máscara ha de resultar 0. La combinación de dirección y máscara 0.0.0.0 implica "cualquier destino".

- **Puertos origen:** Rango de puertos de los que puede provenir el paquete. Se admiten valores en el rango [0 .. 65535].

- **Puertos destino:** Rango de puertos a los que puede ir destinado el paquete. Se admiten valores en el rango [0 .. 65535].

- **Protocolos:** Rango de protocolos a los que se puede asociar el paquete. Se admiten valores en el rango [0 .. 255].

El algoritmo es el siguiente:

1. Se realiza el AND binario entre la **dirección IP origen y la Red origen** y se comprueba si coincide con el resultado de la misma operación entre la dirección IP del paquete que ha recibido el router y la Red origen.

2. Se realiza la misma comprobación que en el punto anterior pero ahora con la **dirección IP destino y la Red destino**.

3. Se comprueba si el **protocolo** al que va dirigido el paquete está dentro del rango de protocolos del control de acceso.

4. Se comprueba si el puerto del que proviene el paquete está en el rango de **puertos origen**.

5. Se comprueba si el **puerto** al que va dirigido el paquete está dentro del rango de **puertos destino**.

6. Si todos los puntos anteriores se han realizado satisfactoriamente para un paquete, entonces se realiza la operación indicada por **Tipo**. Las acciones posibles son **aceptar el paquete** en el caso de que Tipo sea **INCLUSIVO** o **rechazar el paquete** en el caso de que Tipo sea **EXCLUSIVO**.

7. Si no se cumple alguna de las anteriores condiciones se vuelve al punto 1 y se realizan las mismas operaciones con el siguiente registro de la lista de controles de acceso.

8. Si no existen más controles de acceso **se acepta el paquete**.

Es importante el orden en el que se encuentran los controles de acceso pues este orden determina la prioridad.

Para agregar un nuevo control de acceso, se rellenan todos los campos que hay bajo la lista y se pulsa el botón **Agregar**.

Para modificar un elemento de la lista, se selecciona, se modifican los campos correspondientes y se pulsa **Modificar**.

Para borrar un control de acceso, se selecciona y se pulsa **Borrar**.

En el caso de los Protocolos y de los Puertos, se establece un rango. Por ejemplo, si sólo se desean aceptar paquetes SNMP se seleccionaría como Rango de Protocolos [17..17] pues el 17 hace referencia al protocolo UDP y Rango de Puertos [161 .. 162] que son los que utiliza SNMP.

Los siguientes puertos son utilizados por la gestión:

Servicio	Puerto
FTP	21
TELNET	23
Servidor web	80
SNMP	161

Se admite un máximo de 40 controles de acceso IP.

¡Atención!

Si se introduce un control de acceso totalmente exclusivo y el router llega a analizarlo porque los anteriores han fallado, entonces, el router desechará indefectiblemente el paquete. En tal caso, es imprescindible garantizar que, al menos, una estación de gestión verifique alguno de los controles de acceso inclusivo de mayor prioridad. Si esta condición no se respeta el router quedará inaccesible para la gestión. (Garantizar la comunicación bidireccional con cualquier equipo mediante un control de acceso inclusivo precisa de dos registros de controles de acceso: uno como origen y otro como destino).

En los controles de acceso, la dirección "0.0.0.0" junto con la máscara "0.0.0.0" equivale a "cualquier dirección IP".

Para conocer los números de los puertos y protocolos asignados en INTERNET se puede consultar la RFC 1700 "INTERNET ASSIGNED NUMBERS" como ayuda para la definición de controles de acceso IP en el router C2.

e) ***Entidades visibles***

• ***Equipos NOVACOM y NOVACOM-X25***

El equipo puede estar conectado a una LAN que contenga subredes que quieran ser accedidas desde el exterior. En condiciones normales, dado que el equipo realiza conversión de direcciones (NAT), las estaciones de la LAN no pueden ser accedidas desde el exterior.

Para que una subred sea visible desde el exterior se tiene que añadir a la lista de subredes visibles. Con las subredes de esta lista el equipo se comporta de la siguiente forma:

1. Es posible configurar una subred visible por cada canal B RDSI y otra por el interfaz RTC. El número de estaciones visibles puede ser muy alto en función de la máscara de la subred.

2. La subred visible en una red lo es a todos los efectos y para todo tipo de tráfico IP, esto es, el equipo no realiza NAT extendido a los paquetes con origen o destino incluido en la subred.

3. Las subredes visibles en una red externa no lo son en otras posibles redes externas a las que el equipo se conecte por otros canales en los que el equipo sigue realizando NAT extendido.

4. Las estaciones de una subred visible pueden comunicarse con las estaciones normales de la LAN o con estaciones de otra subred visible de la misma LAN a través del propio equipo y sin generar llamadas ni tráfico a las redes externas.

Para que las estaciones visibles puedan responder las peticiones externas es preciso que en todas ellas se configure la ruta a la red externa a través de la dirección IP del denominado **router virtual**. Esto es debido a que las estaciones tendrán direcciones IP pertenecientes a una red distinta de la que está conectada al interfaz LAN del equipo. Como el equipo tiene un sólo interfaz LAN necesita de otro "virtual" al que conectar a los servidores.

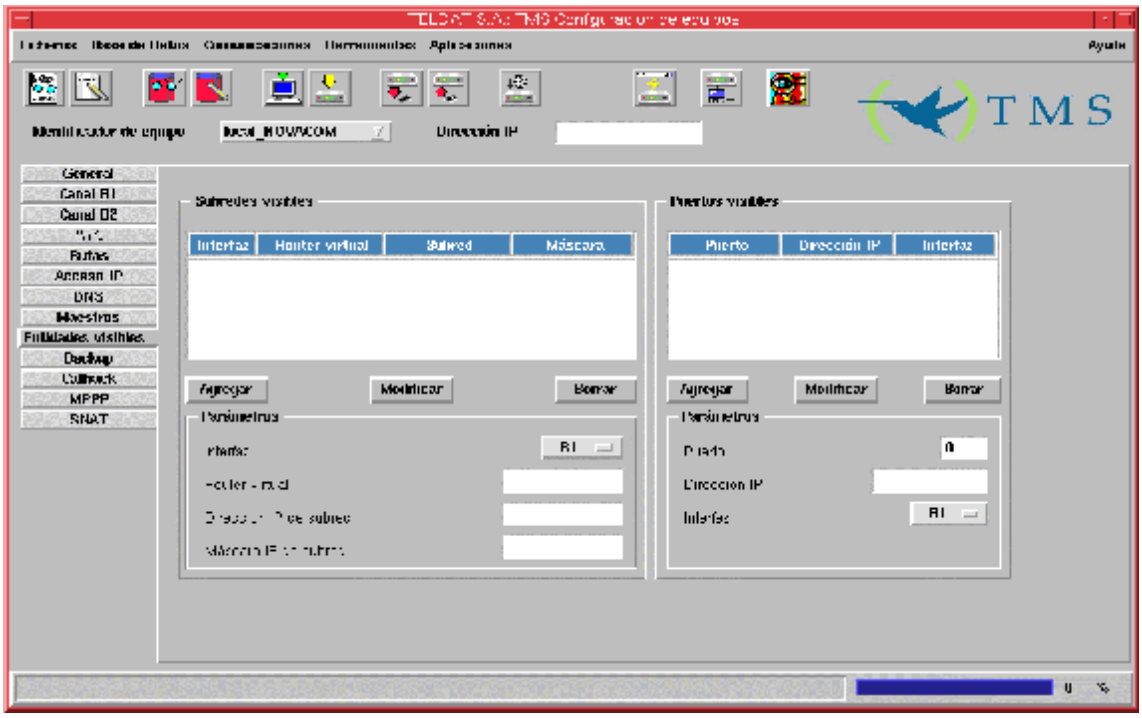


Figura 15 : Configuración de entidades visibles

- **Interfaz:** Es la interfaz a través del cual la subred es visible.

- **Router virtual:** Dirección IP que se asigna al router para que el propio equipo sepa que con los paquetes que recibe no debe hacer NAT. Tiene que ser una dirección perteneciente a la propia subred visible.

- **Dirección IP de la subred:** Es la dirección IP de la subred sobre la que el router no hace NAT.

- **Máscara IP de la subred:** Máscara IP de la subred visible.

Para ***agregar*** una subred a la lista se introducen los valores apropiados en los campos que hay bajo la lista y se pulsa el botón **Agregar**.

Para ***modificar*** una subred de la lista se selecciona y, tras modificarla en los campos correspondientes, se pulsa el botón **Modificar**.

Para ***borrar*** una subred visible de la lista se selecciona y se pulsa **Borrar**.

• *Equipos Cx*

Debido a que los routers Cx realizan conversión de direcciones extendida los equipos externos siempre acceden a una única dirección registrada que el router transforma convenientemente cuando el paquete IP entra en la LAN.

Para permitir que ciertas subredes de la LAN sean visibles al exterior con sus propias direcciones IP (registradas) es necesario deshabilitar la conversión de direcciones en el router para dichas subredes. En esta ventana el usuario especifica aquellas subredes para las que el router no hace NAT y, por tanto, son accesibles desde el exterior.

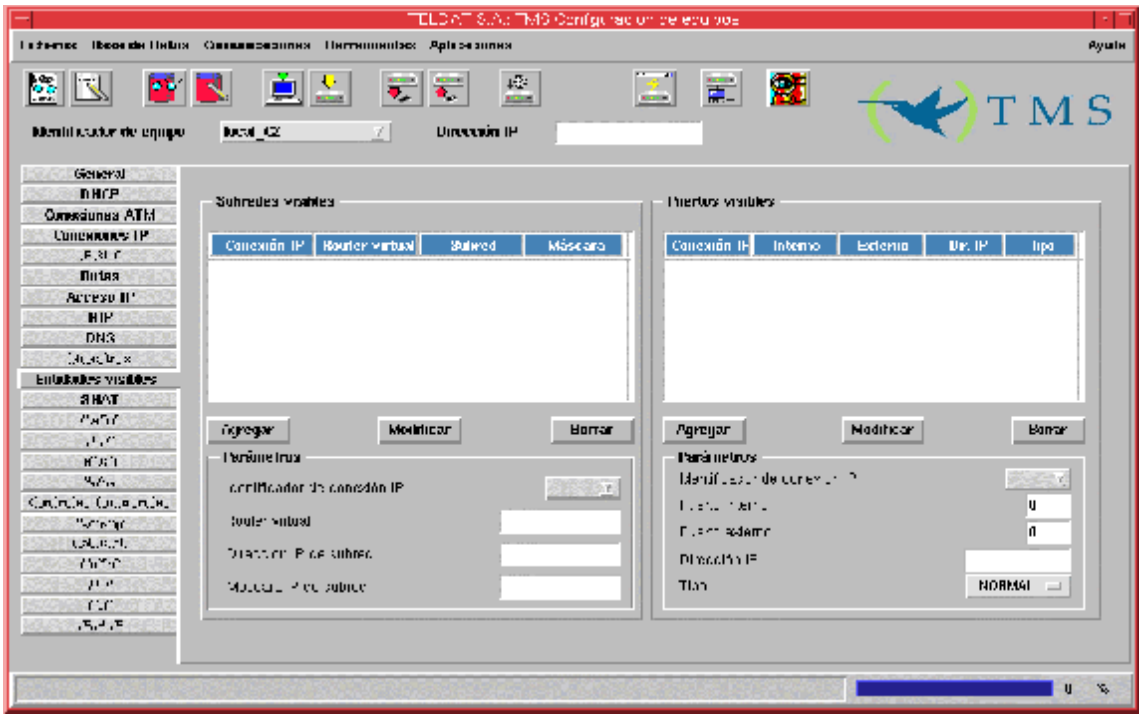


Figura 16 : Configuración de entidades visibles

Para cada subred visible se configuran los siguientes parámetros:

- **Identificador de conexión IP:** Identificador de conexión IP a través de la cual es visible la subred.
- **Router virtual:** Dirección IP que se asigna al router para que el propio equipo sepa que con los paquetes que recibe no debe hacer NAT. Tiene que ser una dirección perteneciente a la propia subred visible.
- **Dirección IP de la subred:** Es la dirección IP de la subred sobre la que el router no hace NAT.
- **Máscara IP de la subred:** Máscara IP de la subred visible.

Con las subredes de esta lista el router se comporta de la siguiente forma:

1. Es posible configurar una subred visible por cada conexión IP. El número de estaciones visibles puede ser grande en función de la máscara de la subred.

2. La subred visible en una red lo es a todos los efectos y para todo tipo de tráfico IP, esto es, el router no realiza NAT extendido a los paquetes con origen o destino incluido en la subred.

3. Las subredes visibles en una red externa no lo son en otras posibles redes externas a las que el equipo se conecte por otros canales en los que el router sigue realizando NAT extendido.

4. Las estaciones de una subred visible pueden comunicarse con las estaciones normales de la LAN o con estaciones de otra subred visible de la misma LAN a través del propio router y sin generar llamadas ni tráfico a las redes externas.

Para que las estaciones visibles puedan responder las peticiones externas es preciso que en todas ellas se configure la ruta a la red externa a través de la dirección IP del denominado **router virtual**. Esto es debido a que las estaciones tendrán direcciones IP pertenecientes a una red distinta de la que está conectada al interfaz LAN del router. Como el router tiene un sólo interfaz LAN necesita de otro "virtual" al que conectar a los servidores.

Para agregar una subred a la lista, rellenar los campos y pulsar **Agregar**.

Para modificar una subred se selecciona en la lista y, tras modificar los campos correspondientes, se pulsa **Modificar**.

En el caso de la opción **Borrar**, se elimina la subred seleccionada.

Se admiten hasta 10 subredes visibles.

Entidades visibles y controles de acceso IP:

Los controles de acceso IP tienen preponderancia sobre las entidades visibles. Esto quiere decir que con un control de acceso exclusivo se pueden hacer inaccesibles puertos o subredes visibles.

f) Configuración de puertos visibles en la LAN

En la misma ventana de entidades visibles se permite configurar los puertos (normalmente asociados a protocolos) que son visibles desde el exterior. La idea es similar a la de las estaciones visibles pero con la diferencia de que, en este caso, es más restrictivo (sólo ciertos puertos) y, además, las direcciones IP asociadas a los puertos pueden ser privadas y así no se desperdician direcciones IP registradas.

Se admite un máximo de 5 puertos. Los puertos no deben estar repetidos. Si así fuese, el equipo encaminaría todo el tráfico al primero de la lista.

Ciertos puertos están prohibidos en esta ventana. Son los puertos que necesita el equipo para su propio tráfico.

Puertos prohibidos:

Nº Puerto	Protocolo
21	FTP
23	TELNET
53	DNS
80	Servidor web
161	SNMP

También están reservados para el NAT de puertos los comprendidos en el rango **[32768 .. 33791].**

Los campos configurables son los siguientes:

- **Identificador de conexión IP:** Conexión IP a través de la que el puerto es visible.
- **Puerto interno:** Número de puerto que quiere hacerse visible.
- **Puerto externo:** Puerto por el que es accesible el puerto interno desde el exterior.
- **Dirección IP:** Dirección IP local de la estación a la que pertenece el puerto y que estará visible al exterior de la LAN. Tiene que ser una dirección IP de la LAN a la que pertenece el router.
- **Tipo:** Tipo de puerto **NORMAL** o **FTP**. Si el tipo es **FTP** el router realiza NAT sobre las direcciones contenidas dentro de los paquetes. Si el tipo es **NORMAL** el router sólo hace NAT sobre las direcciones de las cabeceras de los paquetes.

Se admite un máximo de 5 puertos visibles.

Para agregar un nuevo puerto a la lista, rellenar los campos y pulsar **Agregar**.

Para modificar un puerto se selecciona en la lista y, tras modificar los campos correspondientes, se pulsa **Modificar**.

En el caso de la opción **Borrar**, se elimina el elemento seleccionado.

Entidades visibles y controles de acceso IP:

Los controles de acceso IP tienen preponderancia sobre las entidades visibles. Esto quiere decir que con un control de acceso exclusivo se pueden hacer inaccesibles puertos o subredes visibles.

g) Configuración de servidores de DNS

El equipo permite manejar una lista de hasta 3 servidores de **DNS (Domain Name Server)** que traduzcan nombres a direcciones IP.

La idea es centralizar la gestión DNS en el equipo de forma que las estaciones de la LAN tengan como servidor de DNS predeterminado a la dirección IP del propio equipo en la LAN y que sea este el que se encargue de encaminar el tráfico de DNS a los verdaderos servidores. El orden de los servidores en la lista indica la prioridad que utiliza el equipo para enviar las peticiones.

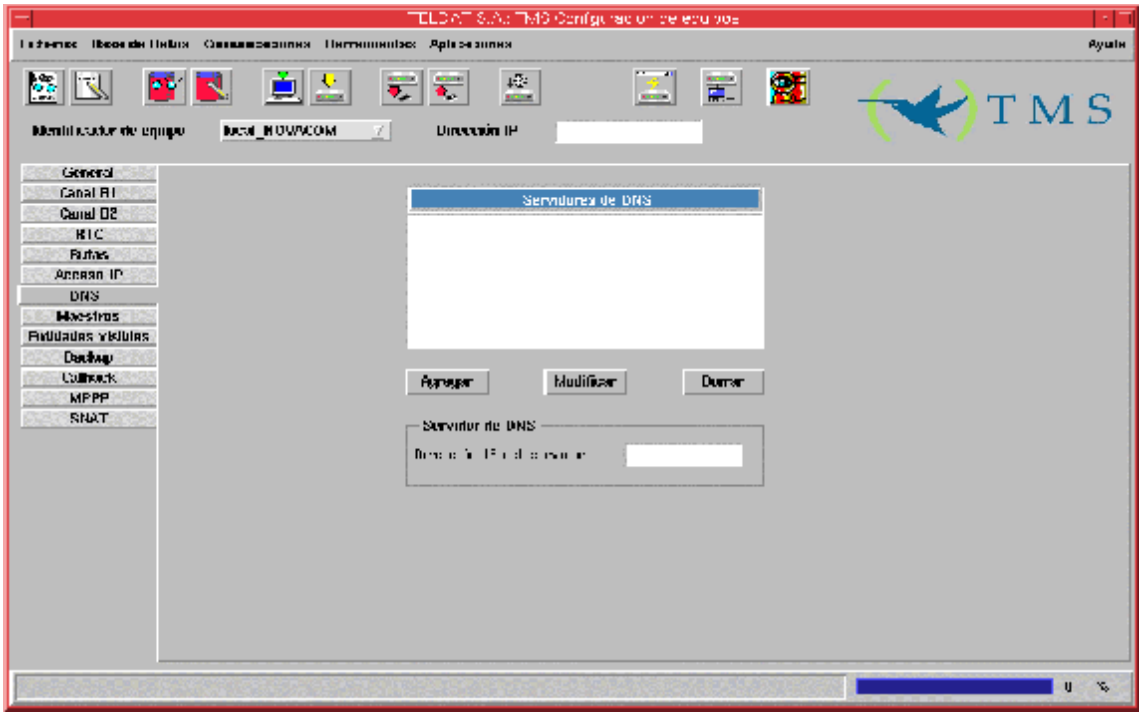


Figura 17 : Configuración de servidores de DNS

Para ***agregar*** un servidor de DNS se deben introducir su dirección IP y, a continuación, pulsar el botón **Agregar**.

Para ***modificar*** un servidor de DNS, se selecciona en la lista, se altera su dirección IP y se pulsa el botón **Modificar**.

Para ***borrar*** un servidor de DNS, se selecciona en la lista y se pulsa **Borrar**.

- ***Configuración de routers maestros autorizados***

En esta ventana se deben introducir los parámetros de los routers maestros autorizados a gestionar el equipo.

Se define el teléfono, la dirección IP y los parámetros de la conexión que establecerá el equipo cuando se requiera su gestión.

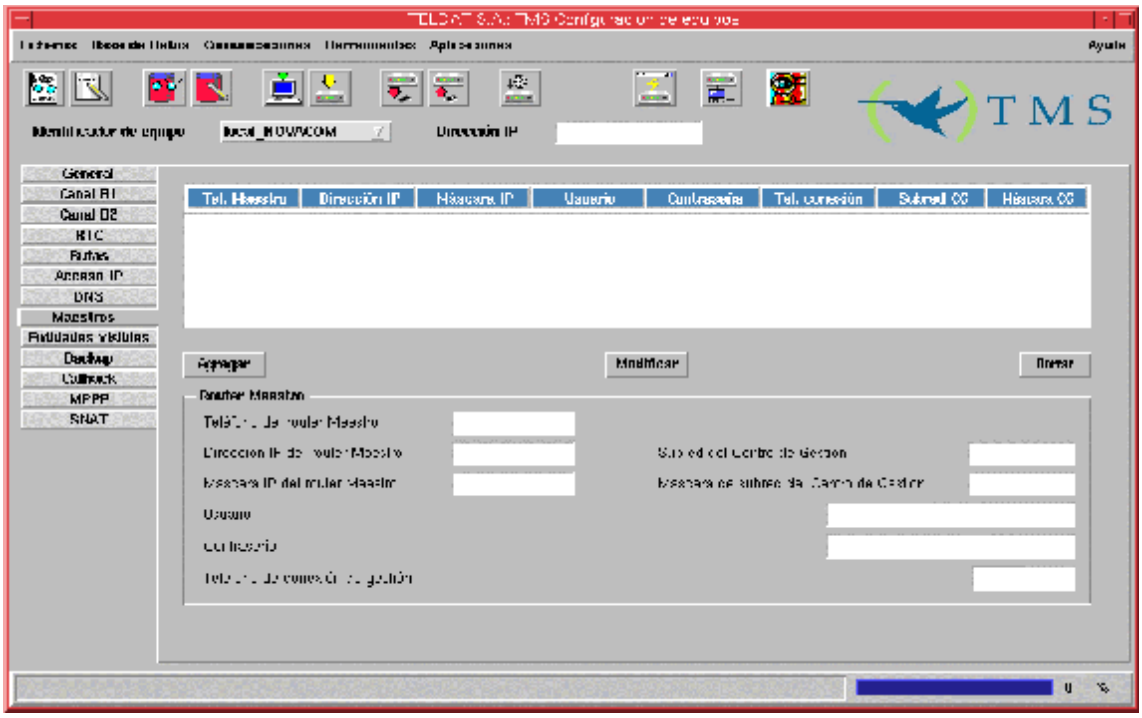


Figura 18 : Configuración de maestros autorizados

- **Teléfono del router Maestro:** Número de teléfono del router maestro autorizado a gestionar el equipo. Cuando el equipo recibe una llamada de este número no la acepta, pero comienza el proceso de establecimiento de una conexión de gestión llamando al número de teléfono que se configura a continuación. Se admiten hasta 19 dígitos.

- **Dirección IP del router Maestro:** Dirección IP del router maestro autorizado. Una vez establecida la conexión de gestión el equipo comunica al maestro su dirección IP.

- **Máscara IP del router Maestro:** Este campo se usa para restringir la red a la que pertenece el router maestro. Su valor por defecto es vacío o "0.0.0.0" que significa lo mismo.

- **Usuario:** Identificador de usuario de la conexión de gestión. Se admiten hasta 31 caracteres.

- **Contraseña:** Contraseña asociada al usuario anterior. Se admiten hasta 31 caracteres.

- **Teléfono de conexión de gestión:**

- Número de teléfono al que tiene que llamar el equipo para establecer la conexión de gestión.

- **Subred del Centro de Gestión:** Este campo y el siguiente permiten especificar una subred IP asociada al Centro de Gestión para un mejor aprovechamiento de las direcciones.
- El valor por defecto es vacío o "0.0.0.0".

- **Máscara de subred del Centro de Gestión:** El valor por defecto es vacío o "0.0.0.0".

Para ***agregar*** un router maestro se rellenan ambos campos y se pulsa el botón **Agregar**.

Para ***modificar*** un router maestro, se selecciona, se modifica en los campos de edición y se pulsa **Modificar**.

Para ***borrar*** un router maestro se selecciona en la lista y se pulsa **Borrar**.

Se admite un máximo de 15 routers maestros autorizados.

El mínimo número de maestros autorizados desde la aplicación de configuración es 4.

h) Configuración de Backup

• *Equipos NOVACOM y NOVACOM-X25*

La configuración de backup que permite que el equipo intente una vía alternativa de conexión en caso de que la preestablecida falle. Se configura de manera independiente para cada uno de los dos canales B RDSI.

El interfaz de backup puede ser el mismo canal B, el otro canal B o la línea RTC (a través de módem). Puede ocurrir, por ejemplo, que un usuario no pueda conectarse a con su proveedor con un determinado usuario y password y, en tal caso, entrar en backup llamando al mismo teléfono pero con otro usuario y password.

Hay dos posibles causas de entrada en backup:

1. Por vencimiento de plazo de conexión.
2. Por superación del número de intentos de conexión.

La primera que se cumpla lanza el proceso de entrada en backup.

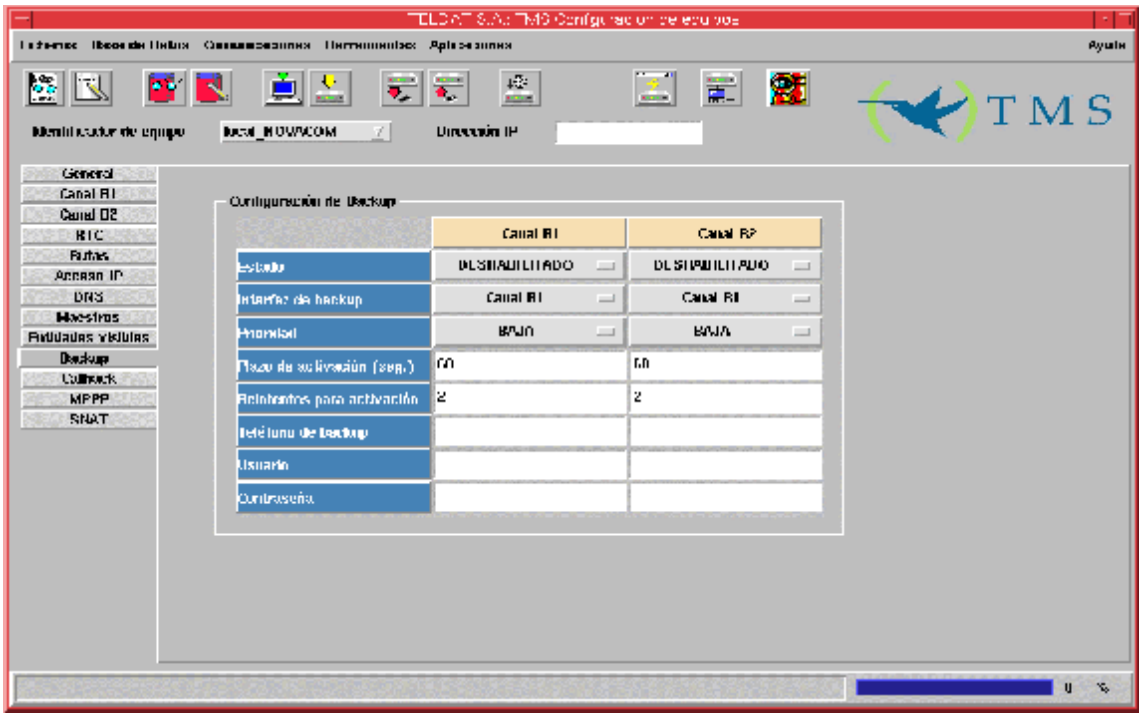


Figura 19 : Configuración de backup

Los parámetros configurables son los siguientes:

- **Estado de backup:** Indica, para cada canal B RDSI, si el backup esta habilitado o no. Si no está habilitado la aplicación no comprueba los restantes parámetros de backup del canal.

- **Interfaz de backup:** Es la interfaz por el que se intentará la conexión de backup. Puede ser cualquiera de los dos canales B RDSI o el RTC.

Con multienlace PPP habilitado cada canal RDSI únicamente puede hacer backup a través de sí mismo o a través del canal RTC.

- **Prioridad de backup:** Sirve para decidir que canal B RDSI tiene mayor prioridad en el caso de que ambos entren en backup por la misma interfaz. Si esto ocurre, prevalecerá el backup cuya prioridad es mayor interrumpiendo, si fuera preciso, al otro. Si ambas son iguales, prevalecerá el primero que entró en backup.

- **Plazo de activación de backup:** Es el tiempo en segundos que el equipo espera para establecer la conexión desde el instante de demanda. Si, transcurrido este tiempo, no consigue establecer la conexión, entonces, intenta la conexión de backup. Cuando se establece la conexión se borra el contador de tiempo transcurrido. Se admiten valores en el rango **[20 .. 120]** segundos.

- **Reintentos para activación de backup:** El equipo cada vez que recibe un paquete IP intenta establecer una llamada RDSI si no está establecida. Si no consigue establecerla y el backup

esta deshabilitado, descarta el paquete. Sin embargo, si está habilitado el backup, incrementa el contador de intentos fallidos de conexión y, cuando alcanza el valor almacenado en este parámetro, intenta la conexión de backup. Una vez establecida la llamada se pone a cero el contador de intentos. Se admiten valores en el rango **[0 .. 4].** El valor 0 indica que debe intentarse establecer la llamada de backup la primera vez que se demande un envío.

- **Teléfono de backup:** Es el número de teléfono al que llama el equipo para intentar establecer la llamada de backup. Este parámetro es obligatorio si el backup está habilitado. Se admiten hasta 31 caracteres numéricos.

- **Usuario de backup:** Es el identificador de usuario con el que se intenta establecer la conexión de backup.

- **Password de usuario de backup:** Es la contraseña del usuario de backup. Se admiten hasta 31 caracteres distintos del carácter blanco.

• *Equipos Cx*

La configuración de backup que permite que el equipo intente una vía alternativa de conexión en caso de que la preestablecida falle. Se configura de manera independiente para cada conexión IP asociada a una línea RDSI.

La conexión IP de backup puede ser la misma que la principal u otra asignada a una línea RDSI.

Hay dos posibles causas de entrada en backup:

1. Por vencimiento de plazo de conexión.
2. Por superación del número de intentos de conexión.

La primera que se cumpla lanza el proceso de entrada en backup.

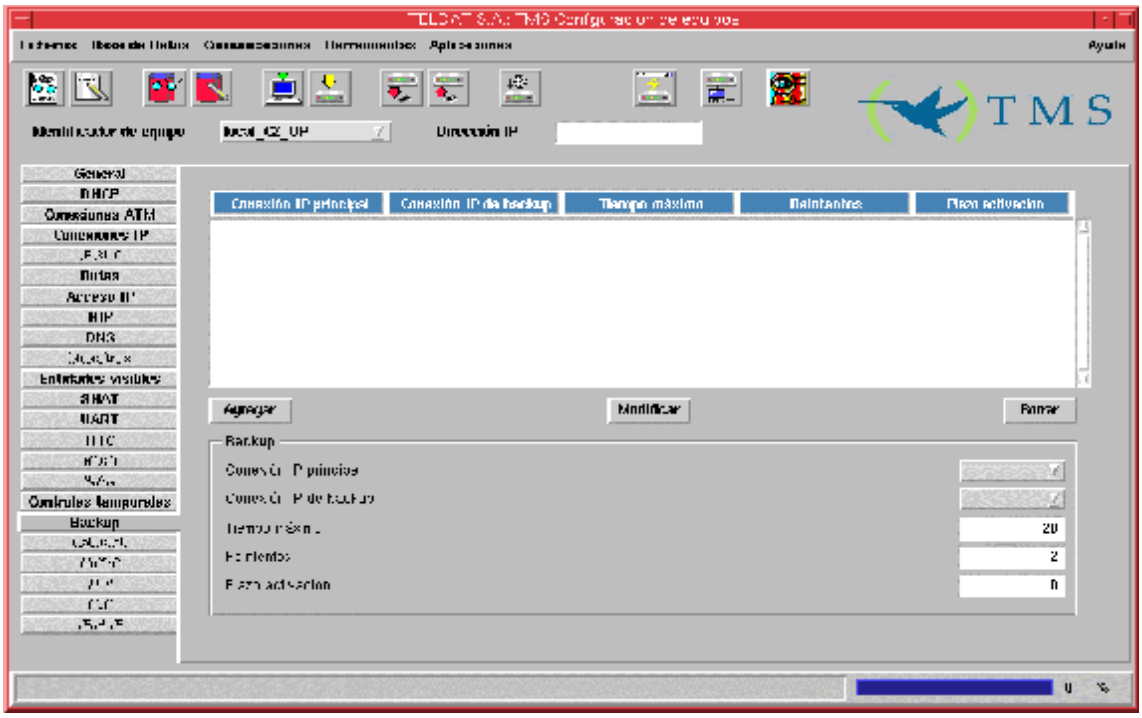


Figura 20 : Configuración de backup

Los parámetros configurables son los siguientes:

- **Conexión IP principal:** Indica la conexión IP para la que se ha configurado el backup.

- **Conexión IP de backup:** Es la conexión IP por el que se intentará la conexión de backup.

> ***Con multienlace PPP habilitado la conexión IP asociada a una línea RDSI únicamente puede hacer backup a través de sí misma***

- **Tiempo máximo:** Tiempo máximo de espera del backup.

- **Reintentos:** El equipo cada vez que recibe un paquete IP intenta establecer una llamada RDSI si no está establecida. Si no consigue establecerla y el backup esta deshabilitado, descarta el paquete. Sin embargo, si está habilitado el backup, incrementa el contador de intentos fallidos de conexión y, cuando alcanza el valor almacenado en este parámetro, intenta la conexión de backup. Una vez establecida la llamada se pone a cero el contador de intentos. Se admiten valores en el rango **[0 .. 4].** El valor 0 indica que debe intentarse establecer la llamada de backup la primera vez que se demande un envío.

- **Plazo de activación:** Es el tiempo en segundos que el equipo espera para establecer la conexión desde el instante de demanda. Si, transcurrido este tiempo, no consigue establecer la conexión, entonces, intenta la conexión de backup. Cuando se establece la conexión se borra el contador de tiempo transcurrido. Se admiten valores en el rango **[20 .. 120]** segundos.

Para agregar un nuevo backup a la lista, rellenar los campos y pulsar **Agregar**.

Para modificar un backup se selecciona en la lista y, tras modificar los campos correspondientes, se pulsa **Modificar**.

En el caso de la opción **Borrar**, se elimina el elemento seleccionado.

Se admite un máximo de 10 backups

i) Configuración de Callback

- ***Equipos NOVACOM y NOVACOM-X25***

La denominada "Facilidad de Callback" permite que el equipo se conecte a través de uno de los canales B RDSI y obtenga una dirección IP cuando recibe una llamada desde un teléfono autorizado. El objetivo es permitir la conexión por demanda exterior a la LAN que está conectado el equipo.

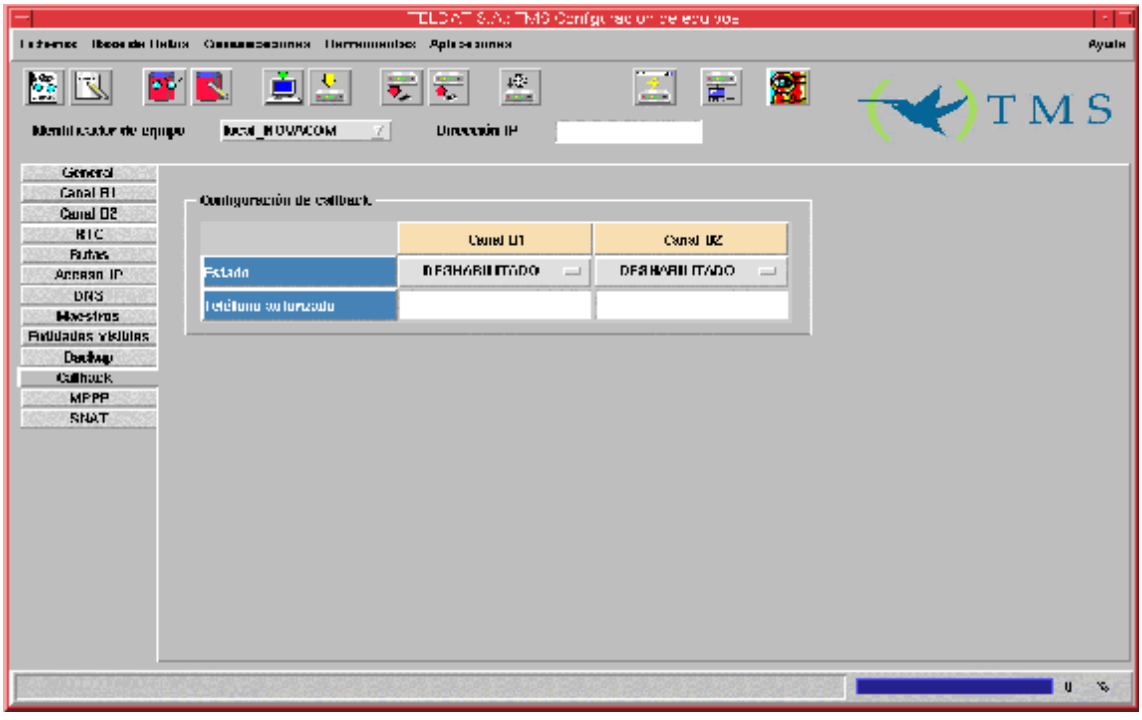


Figura 21 : Configuración de callback

Los parámetros configurables son los siguientes:

- **Estado:** Si se configura como HABILITADO, cuando el equipo reciba una llamada desde el teléfono autorizado, se conectará por la conexión configurada para el canal B RDSI asociado. En cualquier caso, la llamada siempre es rechazada por el equipo (sin coste para el llamante).

- **Teléfono autorizado:** Es el número de teléfono autorizado para despertar el proceso de conexión de callback. Si este campo está vacío se interpreta como que cualquier llamada RDSI recibida en el equipo desencadenará el proceso de conexión de callback (todos los teléfonos estarían autorizados). Se admiten hasta 19 dígitos.

> ***Compatibilidad con versiones anteriores a la 5.4.0.***
>
> ***Las versiones de equipo anteriores a la 5.4.0 no soportan configuración de callback independiente para cada canal por lo que para mantener la compatibilidad se seguirá el siguiente criterio:***
>
> ***"Si está deshabilitado el callback por el canal B1 y habilitado por el canal B2 se envía la configuración del canal B2 al equipo. En cualquier otro caso se envía la configuración de callback del canal B1"***

• *Equipos Cx*

La denominada "Facilidad de Callback" permite que el equipo se conecte a través de una conexión IP asociada a una línea RDSI y obtenga una dirección IP cuando recibe una llamada desde un teléfono autorizado. El objetivo es permitir la conexión por demanda exterior a la LAN que está conectado el equipo.

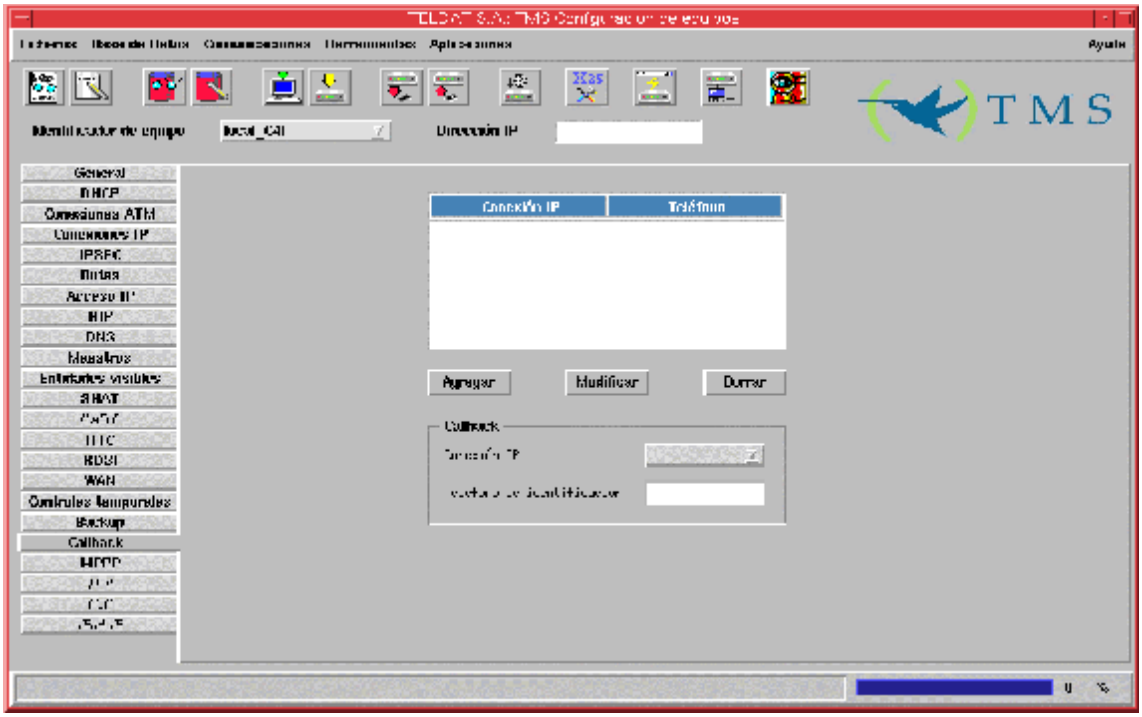


Figura 22 : Configuración de callback

Los parámetros configurables son los siguientes:

- **Conexión IP:** Identificador de la conexión IP.

- **Teléfono de identificación:** Es el número de teléfono autorizado para despertar el proceso de conexión de callback. Si este campo está vacío se interpreta como que cualquier llamada RDSI recibida en el equipo desencadenará el proceso de conexión de callback (todos los teléfonos estarían autorizados). Se admiten hasta 19 dígitos.

Para agregar un nuevo callback a la lista, rellenar los campos y pulsar **Agregar**.

Para modificar un callback se selecciona en la lista y, tras modificar los campos correspondientes, se pulsa **Modificar**.

En el caso de la opción **Borrar**, se elimina el elemento seleccionado.

Se admite un máximo de 10 callbacks

j) MPPP (Point to Point Protocol)

• *Equipos NOVACOM y NOVACOM-X25*

A partir de la **versión 5.2.0** del equipo, se puede configurar el equipo de manera que, cuando el tráfico cursado a través del canal RDSI B1 supere un determinado umbral, se establezca una conexión a través del canal B2 y se reparta el tráfico entre ambos.

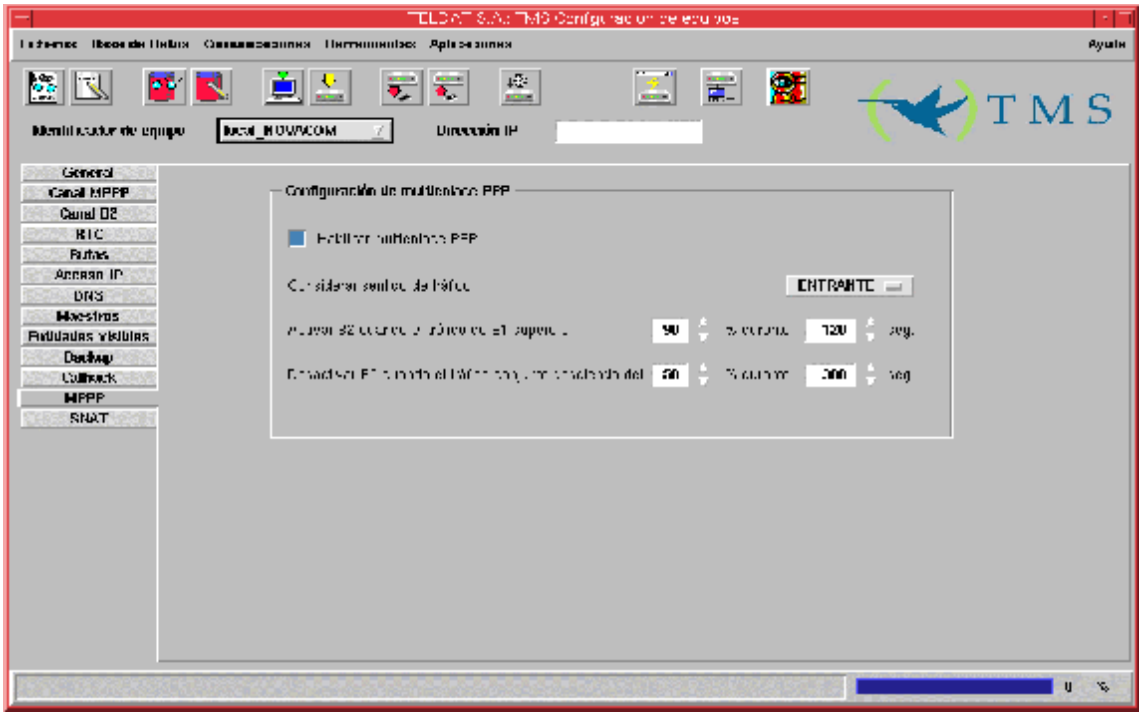


Figura 23 : Configuración de multienlace PPP

Se pueden configurar los siguientes parámetros:

- **Habilitar multienlace PPP :** Permite habilitar o deshabilitar el multienlace PPP. Si está habilitado, se impide que el usuario pueda alterar la configuración del canal RDSI B2 porque este toma obligatoriamente la misma configuración que el canal B1 y se reserva para ser activado en caso de alta carga en B1. Además, todas las entidades de la configuración que hagan referencia al canal B2 se ignoran (por ejemplo, las rutas).

- **Sentido del tráfico :** Indica el sentido del tráfico a considerar para activar o desactivar el multienlace.
- Puede ser tráfico **ENTRANTE** en la LAN, **SALIENTE** o **AMBOS**. Si se considera un sólo sentido, la capacidad de la línea es de 64 Kbps mientras que, en ambos sentidos, es 128 Kbps. El valor por defecto es considerar sólo tráfico **ENTRANTE** en la LAN.

- **Umbral de activación :** Porcentaje de tráfico cursado por el canal B1 que, si se supera durante todo el intervalo de activación, lanza la conexión del multienlace por el canal B2. Se permiten valores en el intervalo [**0 .. 100]%** de la capacidad de la línea. El valor por defecto es **90%**.

- **Intervalo de activación :** Intervalo temporal en el que se compara el tráfico cursado con el umbral de activación. Se permiten valores en el rango **[28 .. 18000]** segundos. El valor por defecto es **120** segundos.

- **Umbral de desactivación :** Porcentaje de tráfico cursado que, si desciende por debajo del umbral de desactivación durante todo el intervalo de desactivación, desconecta la conexión del multienlace por el canal B2. Para desactivar se muestrea el tráfico total (por los dos canales conjuntamente). Se admiten valores dentro del rango **[0 .. 100] %**. El valor por defecto es **50%**.

- **Intervalo de desactivación :** Intervalo temporal en el que se compara el tráfico cursado con el umbral de desactivación. Se permiten valores en el rango **[28 .. 18000]** segundos. El valor por defecto es **300** segundos.

A continuación, se muestra una típica secuencia de activación del multienlace PPP con los valores de configuración por defecto.

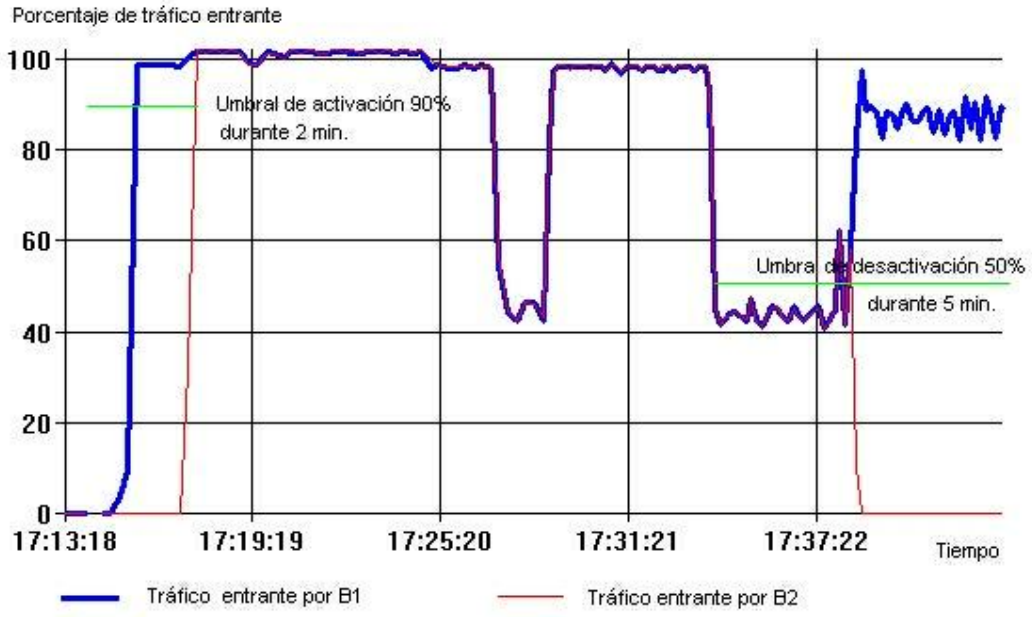


Figura 24 :. Secuencia de activación del multienlace PPP

La situación es la siguiente. Tenemos un equipo con el multienlace PPP activado con la configuración por defecto que consiste en un umbral de activación del 90 % de carga, considerando sólo tráfico entrante en la LAN, durante 2 minutos y un umbral de desactivación del 50 % durante 5 minutos.

Aproximadamente a las 17:15, comienza la recepción de un fichero de gran tamaño a través de un FTP por el canal B1 y la carga de dicho canal alcanza rápidamente el 100 % de su capacidad. Sin embargo, el canal B2 no se activa hasta que transcurren alrededor de 2 minutos desde que el tráfico por B1 superó el umbral de activación del 90 %. Una vez establecida la conexión por el canal B2, vemos que el equipo utiliza la capacidad de los dos canales al 100 %.

A las 17:27 se produce un descenso de la carga del canal B1 por debajo del umbral de desactivación (50 %) pero durante un intervalo de tiempo menor que el intervalo de desactivación, que es de 5 minutos. Por está razón, se mantiene la conexión del canal B2.

Finalmente, a las 17:38, desciende el tráfico por el canal B1 por debajo del umbral de desactivación durante un tiempo superior al intervalo de desactivación y el equipo libera la llamada del canal B2.

Multienlace PPP y canal B2 RDSI:

Desde la versión 5.2.0 hasta la 5.3.0 la habilitación del multienlace PPP suponía la desactivación del perfil de conexión establecido en el canal B2 así como la de las entidades que lo utilizaban como, por ejemplo, las rutas.

A partir de la versión 5.3.0, el perfil de conexión de B2 tiene prioridad sobre el segundo canal del multienlace PPP si este está habilitado. Es decir, si los dos canales están siendo utilizados por el multienlace y se solicita una conexión por B2, entonces, el multienlace libera su segundo canal y se establece la conexión solicitada. A la inversa, si está establecida la conexión por B2 entonces el multienlace no podrá disponer de su segundo canal.

- ***Equipos Cx***

A través de TMS se puede configurar el equipo de manera que, cuando el tráfico cursado a través de un canal RDSI B1 supere un determinado umbral, se establezca una conexión a través del canal B2 y se reparta el tráfico entre ambos.

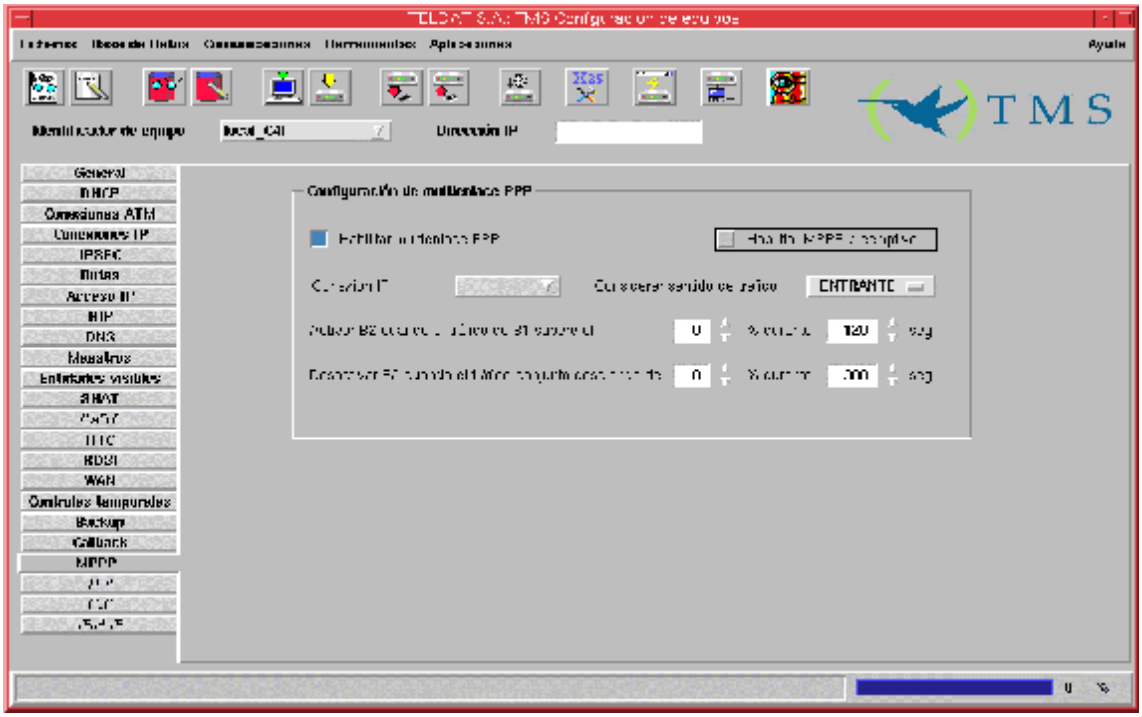


Figura 25 : Configuración de multienlace PPP

Se pueden configurar los siguientes parámetros:

- **Conexión IP:** Identificador de la conexión IP.

- **Habilitar multienlace PPP:** Permite habilitar o deshabilitar el multienlace PPP. Si está habilitado, se impide que el usuario pueda alterar la configuración del canal RDSI B2 porque este toma obligatoriamente la misma configuración que el canal B1 y se reserva para ser activado en caso de alta carga en B1. Además, todas las entidades de la configuración que hagan referencia al canal B2 se ignoran (por ejemplo, las rutas).

- **Habilitar MPPP preemptivo:** Permite habilitar o deshabilitar el MPPP preemptivo.

- **Sentido del tráfico:** Indica el sentido del tráfico a considerar para activar o desactivar el multienlace. Puede ser tráfico **ENTRANTE** en la LAN, **SALIENTE** o **AMBOS**. Si se considera un sólo sentido, la capacidad de la línea es de 64 Kbps mientras que, en ambos sentidos, es 128 Kbps. El valor por defecto es considerar sólo tráfico **ENTRANTE** en la LAN.

- **Umbral de activación:** Porcentaje de tráfico cursado por el canal B1 que, si se supera durante todo el intervalo de activación, lanza la conexión del multienlace por el canal B2. Se permiten valores en el intervalo [**0 .. 100]%** de la capacidad de la línea. El valor por defecto es **90%**.

- **Intervalo de activación:** Intervalo temporal en el que se compara el tráfico cursado con el umbral de activación. Se permiten valores en el rango **[28 .. 18000]** segundos. El valor por defecto es **120** segundos.

- **Umbral de desactivación:** Porcentaje de tráfico cursado que, si desciende por debajo del umbral de desactivación durante todo el intervalo de desactivación, desconecta la conexión del multienlace por el canal B2. Para desactivar se muestrea el tráfico total (por los dos canales conjuntamente). Se admiten valores dentro del rango **[0 .. 100] %**. El valor por defecto es **50%**.

- **Intervalo de desactivación:** Intervalo temporal en el que se compara el tráfico cursado con el umbral de desactivación. Se permiten valores en el rango **[28 .. 18000]** segundos. El valor por defecto es **300** segundos.

k) Configuración de NAT (Network Address Translation) estático

En el router se puede configurar una tabla de registros de entradas **NAT (Network Address Translation)**. Se trata de convertir rangos de direcciones locales a rangos de direcciones globales teniendo en consideración también el interfaz de salida.

NAT puede ser necesario en los siguientes casos:

1. Se quiere tener conectividad con Internet, pero no todos los equipos poseen direcciones IP globales (permitidas). En este caso se configura un router NAT como enlace entre el dominio privado (red local) y el dominio público (red pública: en este caso Internet). El router NAT traduce las direcciones locales en direcciones globales antes de enviar los paquetes al exterior.

2. Una empresa requiere conectividad IP entre oficinas remotas. Dichas oficinas remotas posee redes IP internas que no cumplen con un plan de direccionamiento con lo que las tablas de rutas para lograr conectividad entre ellas es grande o imposible. En este caso sería suficiente con configurar NAT en los routers frontera de cada oficina, realizar así la transformación entre

las redes internas de las oficinas a redes globales, que ahora si cumplen con el plan de direccionamiento.

3. Se necesitan cambiar la direcciones internas de muchos equipos. En lugar de realizar dicho cambio que sería muy costoso en tiempo se podría realizar NAT.

El termino "local" representa a aquellas redes que pertenecen a una empresa y que deben ser traducidas. Dentro del dominio local un determinado equipo poseerá una dirección local, mientras que en el exterior aparentará que posee una dirección de otro espacio de direcciones. Por tanto, al primer espacio de direcciones es el **local** y el segundo espacio de direcciones es el **global**.

Tipos de NAT

La traducción de direcciones puede ser:

NAT estático	La correspondencia de direcciones locales y globales es unívoca. Este tipo es el que se configura en esta ventana.
NAT dinámico	Se establece una correspondencia de direcciones locales en un pool de direcciones globales. Por tanto la correspondencia entre direcciones globales y locales no es unívoca y depende de condiciones de ejecución.
NAPT (Network Address Port Translation)	Se establece una correspondencia entre direcciones locales y una única dirección global. En este caso lo que se realiza es una traslación de los puertos de protocolos de transporte (UDP, TCP).

La conversión de direcciones es bidireccional, es decir, cualquier dirección perteneciente a la subred local que esté en un registro de esta tabla se convierte al rango de direcciones global si sale por el interfaz asignado y viceversa, cualquier dirección que entre por el interfaz desde el exterior y pertenezca a la subred global se convierte al rango local.

Para cada paquete se examina el interfaz y su dirección IP se compara con la de la subred local (si el paquete sale de la LAN) o con la global (si el paquete entra en la LAN) con los registros de la tabla, por orden, hasta que se encuentra uno en el que encaje. De aquí que sea importante el orden de los registros en la tabla puesto que equivale a la prioridad de unas reglas de conversión frente a otras.

Si se desea más información acerca de NAT consúltese la referencia {Teldat: NAT, 99}.

• *Equipos NOVACOM y NOVACOM-X25*

A partir de la **versión 5.6.0** del equipo se puede configurar una nueva tabla de registros de entradas **NAT (Network Address Translation)**.

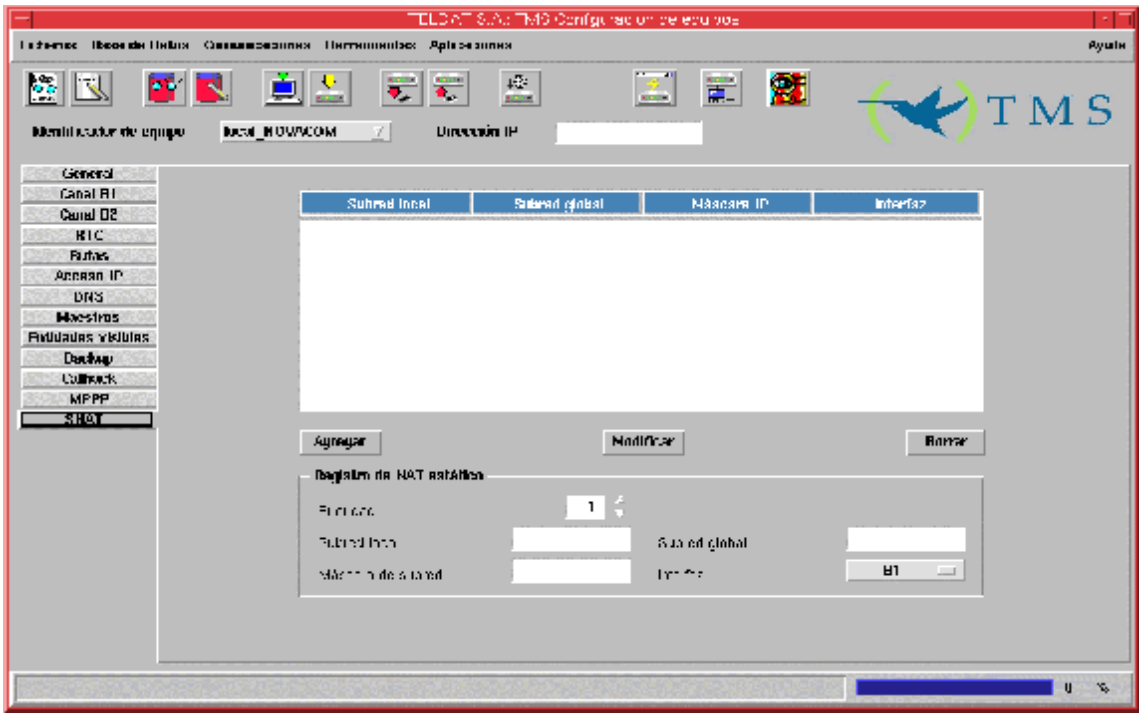


Figura 26 : Configuración de NAT estático

Los campos componentes de cada registro NAT estático son los siguientes:

- **Prioridad :** Especifica el orden en que se comprobarán las reglas NAT. Se aplicará la primera que se cumpla.
- **Subred local :** Dirección IP de host o de subred perteneciente a la LAN a la que está conectado el equipo.
- **Subred global:** Dirección IP de host o de subred asignada en la WAN a la que está conectado el equipo por la interfaz indicada en el registro.
- **Máscara IP:** Mascara IP de subred o de host que se aplica sobre las dos direcciones anteriores para delimitar las subredes. Se tiene que cumplir que el AND binario entre cada subred y la máscara negada sea igual a 0**.**
- **Interfaz:** Interfaz por el que el equipo se conecta con la WAN.

Se admiten un máximo de 10 registros en la tabla.

- ***Equipos Cx***

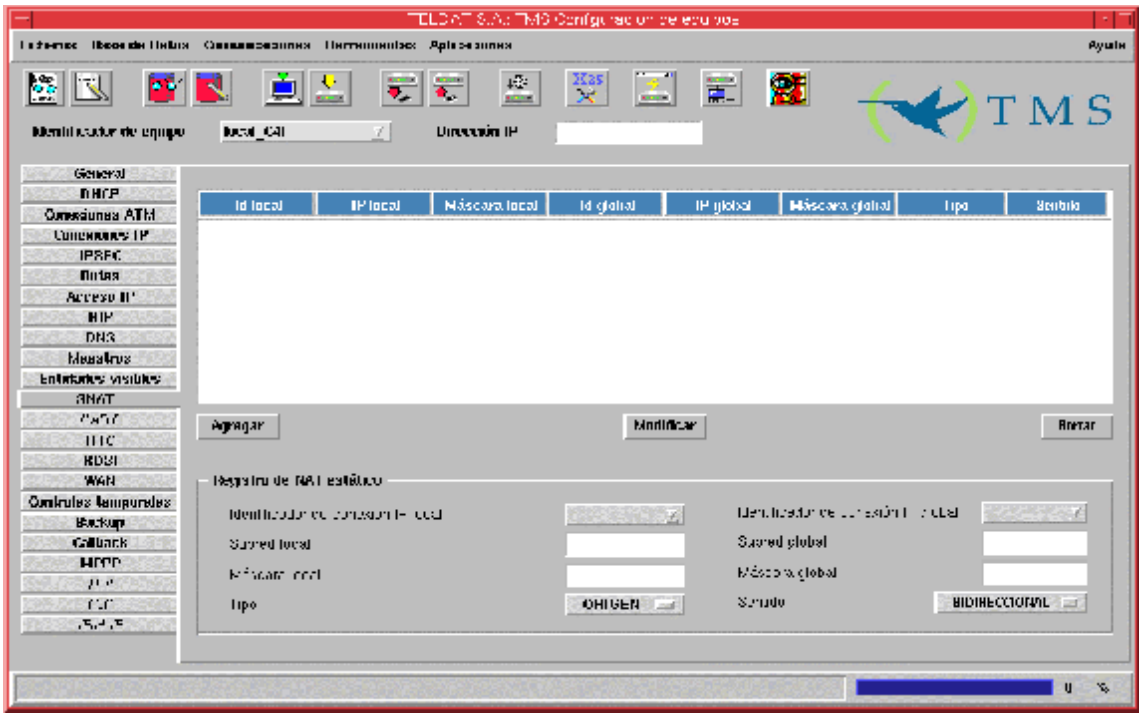


Figura 27 : Configuración de NAT estático

Los campos componentes de cada registro NAT estático son los siguientes:

- **Identificador de conexión IP local:** Especifica la conexión IP por la que se accede a la subred local. Si su valor es cero se refiere a la interfaz LAN.

- **Identificador de conexión IP global:** Especifica la conexión IP por la que se accede a la subred global. Si su valor es cero se refiere a la interfaz LAN.

- **Subred local:** Dirección IP de host o de subred perteneciente a la LAN a la que está conectado el router.

- **Subred global:** Dirección IP de host o de subred asignada en la WAN a la que está conectado el router por la interfaz indicada en el registro.

- **Máscara IP:** Mascara IP de subred o de host que se aplica sobre las dos direcciones anteriores para delimitar las subredes. Se tiene que cumplir que el AND binario entre cada subred y la máscara negada sea igual a 0**.**

- **Tipo:** Hay 2 tipos de transformación :

1. **ORIGEN**

- A todo paquete que pase del dominio local al global (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección origen local por la correspondiente global. Y a todo paquete que pase del dominio global al local (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección destino global por su correspondiente local.

2. DESTINO

- A todo paquete que pase del dominio local al global (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección destino local por la correspondiente global. Y a todo paquete que pase del dominio global al local (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección origen global por su correspondiente local.

- **Sentido:** Hay 5 sentidos de transformaciones

1. **LOCAL A GLOBAL:** Si el paquete entra por el interfaz local y sale por el interfaz global y su dirección (origen o destino) pertenece a la red local entonces cambiar dirección (origen o destino) local por su correspondiente dirección global.

2. **GLOBAL A LOCAL:** Si el paquete entra por el interfaz global y su dirección (origen o destino) pertenece a la red global entonces cambiar dirección (origen o destino) global por su correspondiente dirección local.

3. **BIDIRECCIONAL:** Se aplican las dos anteriores.

4. **INHIBIR LOCAL:** Si el paquete entra por el interfaz local y sale por el interfaz global y su dirección (origen o destino) pertenece a la red local entonces no realizar cambio alguno.

5. **INHIBIR GLOBAL:** Si el paquete entra por el interfaz global y su dirección (origen o destino) pertenece a la red global entonces no realizar cambio alguno.

Se admiten un máximo de 10 registros en la tabla.

I) Configuración X.25 (sólo equipos NOVACOM-X25)

Las ventanas de configuración de X.25, Nodo y XOT se despliegan al pulsar el botón 

de la barra de herramientas.

En la figura se muestran los parámetros configurables de para una línea X.25 agrupados según los niveles.

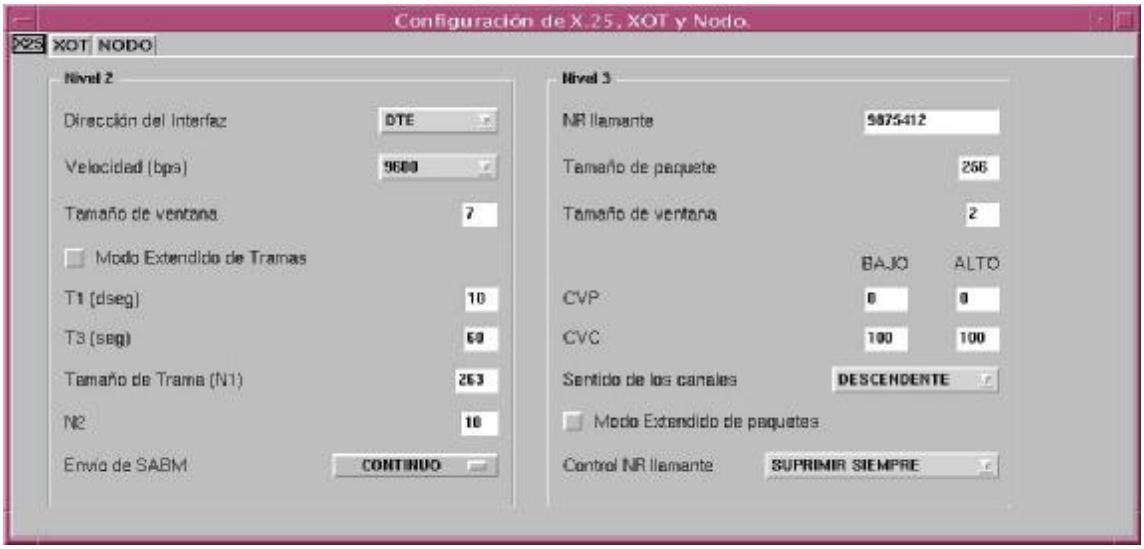


Figura 28 : Configuración X.25

Nivel 2 (protocolo LAPB)

- **Dirección del interfaz:** Especifica para el protocolo LAPB del nivel 2 X.25, el comportamiento como terminal (**DTE**) o como módem (**DCE**).
- **Velocidad (bps):** Mediante este parámetro se configura el régimen binario al que funcionará el interfaz X.25. Los posibles valores son el rango de velocidades síncronas desde **1.200** a **2.048.000** bits por segundo (bps).
- **Tamaño de Ventana:** Número máximo de tramas I numeradas secuencialmente que el DTE o el DCE pueden tener pendientes (es decir, sin acuse de recibo) en un momento dado. El valor de este parámetro (parámetro *k*) estará en el rango **[2 .. 7]** si no está activado el modo extendido de tramas y **[2 .. 127]** si está activado. El valor por defecto es **7**.
- **Modo extendido de tramas:** Especifica el módulo del campo NS (Número de Secuencia) del nivel de enlace X.25, esto es, el módulo utilizado para numerar consecutivamente las tramas LAPB enviadas. Si no está activado es módulo 8, sino 128.
- **T1 (dseg):** T1 es el tiempo máximo en décimas de segundo que se espera un asentimiento de trama, pasado el cual, si no ha habido intercambio de tramas, el equipo retransmite la trama pendiente de asentimiento. Se admiten valores en el rango **[1 .. 100]** siendo **10** décimas de segundo el valor por defecto.
- **T3 (seg):** Es el tiempo máximo en segundos que se espera un asentimiento de trama. Transcurrido este tiempo el equipo envía un RR con bit de poll. Será suficientemente mayor que el período del temporizador T1 del DCE (es decir, T3 > T1) para que al expirar T3 se tenga suficiente seguridad de que el canal del enlace de datos se encuentra en un estado no activo y no operacional, y que es necesario establecer el enlace de datos para reanudar su funcionamiento normal. Se admiten valores en el rango **[1 .. 100]** siendo **60** seg. el valor por defecto.
- **Tamaño de Trama (N1):** Número máximo de bytes en una trama I (excluyendo las banderas; los bits 0 o los octetos de escape de control insertados para que haya transparencia en la transmisión síncrona o arrítmica, respectivamente; y los bits insertados para la temporización de transmisión en la transmisión arrítmica) que el DCE o el DTE esté dispuesto a aceptar del DTE o del DCE, respectivamente. Se admiten valores en el rango **[1 .. 4103]**, siendo **263** bytes el valor por defecto.

- **N2:** Es el número máximo de retransmisiones de una trama no asentida. Se admiten valores en el rango **[1 .. 100],** siendo **10** el valor por defecto.
- **Envío de SABM:** Determina si la entidad de nivel 2 de X.25 intentará establecer continuamente el enlace transmitiendo SABM. SABM (*Set Asynchronous Balanced Mode*) o Paso a Modo Equilibrado Asíncrono hace que todos los campos de control de instrucción / respuesta tengan la longitud de un octeto.
  - **N2 VECES**: (Valor por defecto) se envía N2 veces la trama SABM.
  - **CONTINUO**: Se envía constantemente.
  - **DESHABILITADO**: Esperará a que sea la entidad remota la que establezca el enlace.

Si a nivel físico (no lógico que es el valor que se configura con el parámetro "Dirección del interfaz") el equipo está funcionando como DTE, no admitirá el valor CONTINUO y cuando se envíe la configuración devolverá un error SNMP.

Para ver como está configurado el equipo a nivel físico hay que entrar por TELNET a la consola del equipo e introducir los siguientes comandos (en negrita):

```
*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>
```

Nivel 3

- **NR llamante:** El NR (Número de Red) es la dirección X.25 llamante de los paquetes de solicitud de llamada que salgan por el puerto, independientemente del NR con que hayan sido recibidos en el equipo. Se admiten hasta 15 dígitos.
- **Tamaño de ventana:** Configura la ventana de nivel 3, es decir, el máximo número de paquetes X.25 que puede haber pendientes de asentimiento. Si está activado el modo extendido de paquetes el rango es **[2 .. 127],** si no está activado, es **[2 .. 7].** El valor por defecto es **2** paquetes.
- **Tamaño de paquete:** Tamaño máximo del paquete X.25 en bytes. Paquetes mayores provocan un error en la llamada establecida. Se admiten valores en el rango **[128 .. 1024]** siendo **256** bytes el valor por defecto.

- **CVP mas bajo:** Indica el número más bajo de Canal Virtual Permanente que podrá ser utilizado en comunicaciones X.25. El rango de CVP que utilice su equipo estará negociado con la PTT. Se admiten valores en el rango **[0 .. 4096]** siendo **0** el valor por defecto.
- **CVP mas alto:** Indica el número más alto de Canal Virtual Permanente que podrá ser utilizado en comunicaciones X.25. El rango de CVP que utilice su equipo estará negociado con la PTT. El rango de CVP siempre estará por debajo del rango de CVC. Se admiten valores en el rango **[0 .. 4096]** siendo **0** el valor por defecto.
- **CVC mas bajo:** Indica el número más bajo de Circuito virtual Conmutado que podrá ser utilizado en comunicaciones X.25. El rango de CVC que utilice su equipo estará negociado con la PTT. Se admiten valores en el rango **[0 .. 4096]** siendo **100** el valor por defecto.
- **CVC mas alto:** Indica el número más alto de Circuito virtual Conmutado que podrá ser utilizado en comunicaciones X.25. El rango de CVC que utilice su equipo estará negociado con la PTT. Se admiten valores en el rango **[0 .. 4096]** siendo **100** el valor por defecto.
- **Sentido de los canales:** Especifica si los números de canal lógico se utilizarán por orden desde el inferior hasta el superior (**ASCENDENTE**) o viceversa (**DESCENDENTE**).
- **Suprimir NR llamante:** Hace que no aparezca el número de red del llamante en el destino.
- **Modo extendido de paquetes:** Módulo utilizado para numerar consecutivamente los paquetes X.25 enviados. Desactivado es módulo 8, activado es módulo 128.

• *Configuración del nodo (sólo equipos NOVACOM-X25)*

La configuración de nodo se presenta agrupada en cuatro bloques de información.

Configuración global del nodo

Esta ventana muestra los parámetros globales de la configuración.

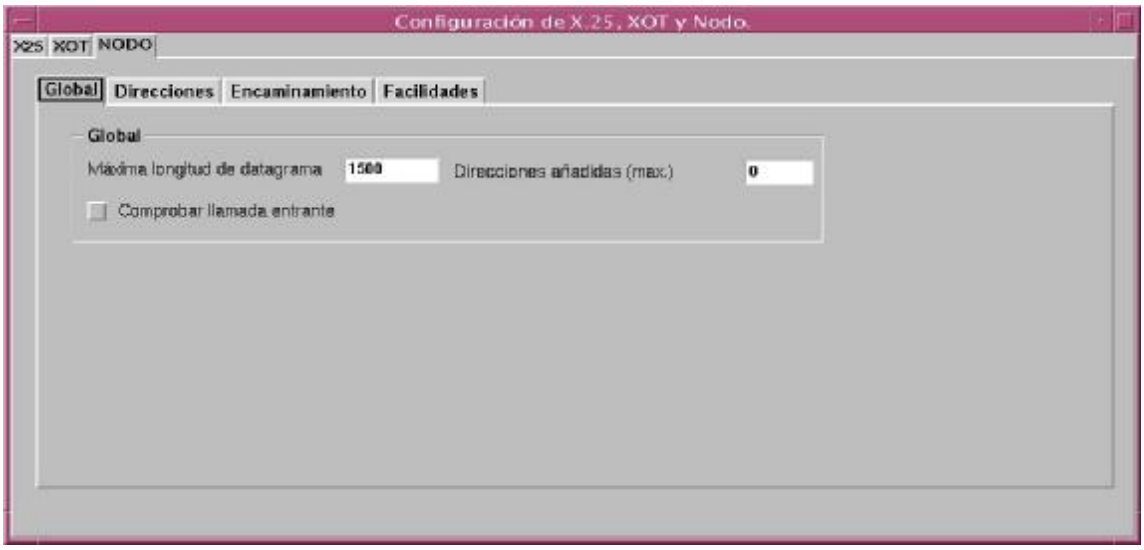


Figura 29 : Configuración global del nodo

Como se muestra en la figura, la configuración global permite configurar los campos :

- **Máxima longitud de datagrama:** Tamaño máximo en bytes de un paquete. Se admiten valores en el rango **[256 .. 18000]** siendo **1500** bytes el valor por defecto.

- **Comprobar NR llamante:** Hace que el equipo verifique que un determinado número de red llamante está en sus tablas. Este parámetro debe estar siempre activado si se va a encaminar IP por X.25.
- **Direcciones añadidas (máx.):** Permite configurar cuantas direcciones IP se pueden añadir de forma dinámica, es decir sin necesidad de reiniciar el equipo para que se activen. Se admiten valores en el rango **[0 .. 500]** siendo **10** el valor por defecto.

Configuración de direcciones del nodo

Esta ventana permite relacionar una dirección IP con una dirección X.25 y asociarles determinadas características para la transmisión de datos. La figura muestra como se permite crear, borrar y modificar estas relaciones.

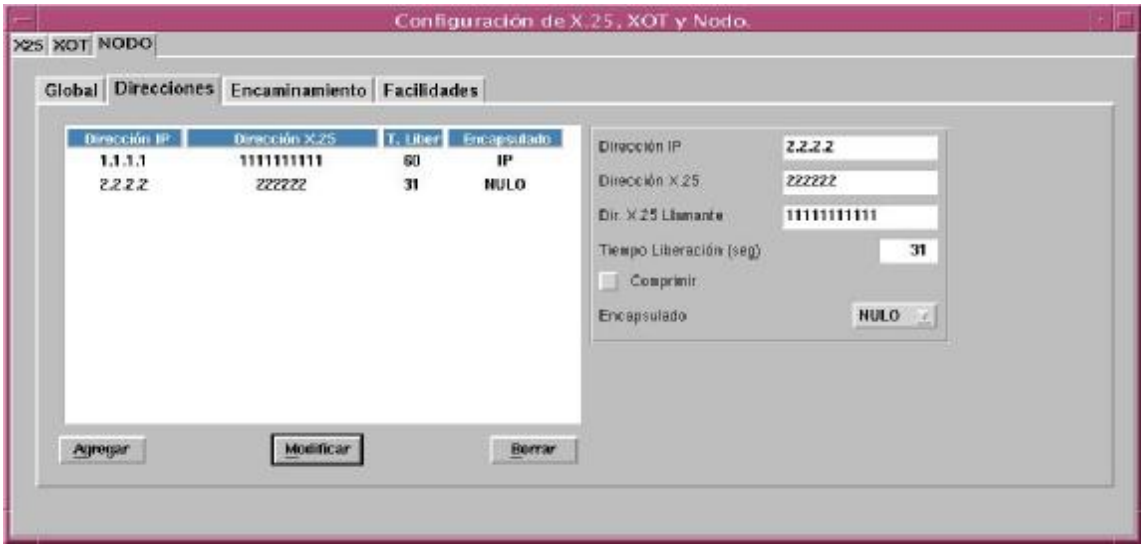


Figura 30 : Configuración de direcciones del nodo

- **Dirección IP:** Dirección IP de host.
- **Dirección X.25:** Número de red destino de la llamada. Se admiten hasta 15 dígitos.
- **Dirección X.25 llamante:** Número de red llamante. Se admiten hasta 15 dígitos.
- **Tiempo de liberación (seg):** Transcurrido este tiempo se libera la llamada por ausencia de tráfico. Se admiten valores en el rango **[0 .. 65000]** siendo **60** el valor por defecto.
- **Comprimir:** Se aplica compresión a los datos.
- **Encapsulado:** Hay dos formas de encapsular IP en X.25:
  - **IP:** que consiste en poner los datos de usuario a CC en el paquete de llamada. Es el utilizado por defecto.
  - **NULO:** que consiste en poner datos de usuario a 0x00 y la cabecera 0xCC en cada paquete de datos.

El número de entradas posibles en la tabla está limitado por la memoria del equipo.

Configuración de encaminamiento del nodo

El encaminamiento consiste básicamente en relacionar un interfaz con una o varias direcciones X.25 para que el nodo pueda realizar la conmutación (recibir la información por una puerta y transmitirla por otra).

Este grupo presenta la tabla de encaminamiento del nodo y la posibilidad de añadir, modificar o borrar sus elementos. La figura muestra el aspecto de esta ventana.

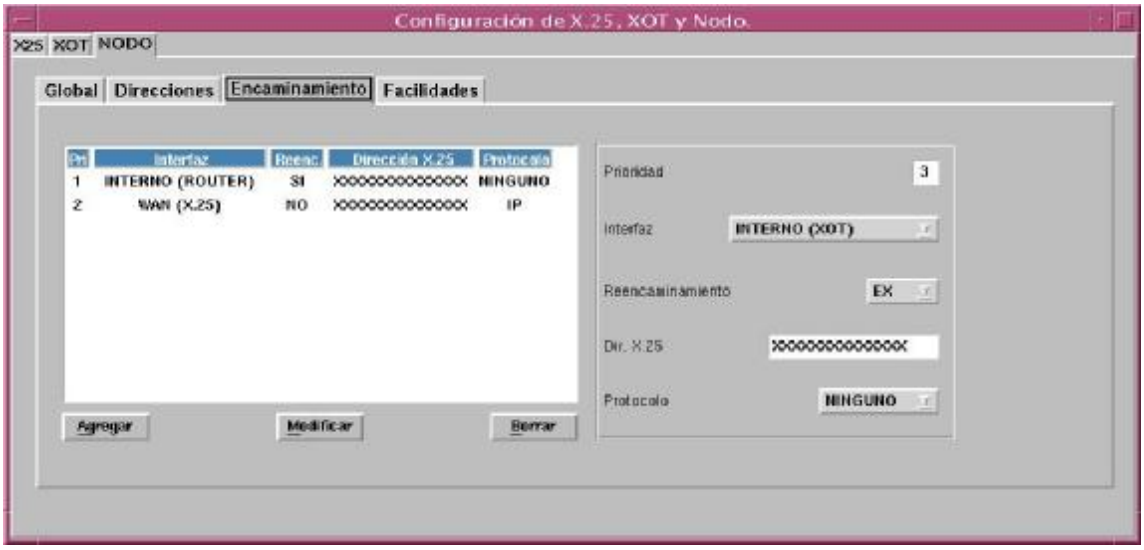


Figura 31 : Configuración de encaminamiento del nodo

- **Prioridad:** Es el indicador de prioridad de la asignación. Siendo: 0 Mayor prioridad y 9 Menor prioridad. Se admiten valores en dicho rango [0 .. 9], siendo 9 el valor por defecto (máxima prioridad). Las prioridades pueden repetirse.
- **Interfaz:** interfaz al que se le asigna la dirección X.25 (o grupo de estas).
- **Reencaminamiento:** Cuando en una solicitud de llamada el equipo detecta que la línea destino está caída o está ocupada (no tiene canales lógicos libres), tiene tres opciones:
  - **NO:** Liberar la llamada.
  - **EX:** Esta opción impide encaminar una llamada X25 hacia el mismo puerto por el que entra la llamada, es decir, si el encaminamiento con más prioridad ruta la llamada hacia un CVC del mismo puerto por el está entrando, entonces se busca si hay otros encaminamientos hacia otros puertos.
  - **SI:** reencaminar la llamada hacia otra línea con *Número de Red* (NR) válido.
- **Dirección X.25:** Es el número de red que se asigna al puerto. Para establecer un circuito con este puerto, el NR del paquete de llamada (origen) debe coincidir con el programado en este campo (destino). Se admiten hasta 15 dígitos o caracteres comodín 'X'.
- **Protocolo:** Identificador de protocolo: permite realizar encaminamientos en función del primer octeto del campo de datos de usuario, que identifica al protocolo. Si no se programa no se mira este campo**. [0..255]**. El valor 0 corresponde a encapsulado NULO y el valor 204 (0xCC) al protocolo IP.

Configuración de facilidades del nodo

En esta ventana se permite configurar las facilidades X.25 para una puerta determinada.

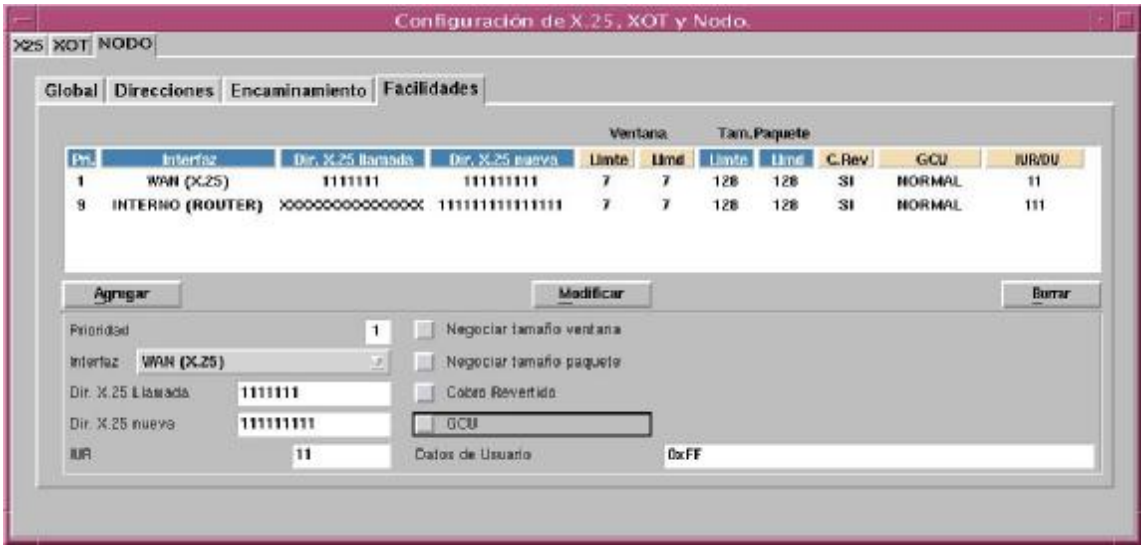


Figura 32 : Configuración de facilidades del nodo

- **Prioridad :** Es el orden en el que se verifican las facilidades a aplicar.
- **Interfaz :** Identifica el interfaz del equipo sobre el que se aplica.
- **Dirección X.25 llamada:** Es la dirección X.25 o NRI a la que se le van a aplicar las facilidades. Admite como entrada 15 dígitos o caracteres comodín '**X**'.
- **Dirección X.25 nueva:** Es la dirección X.25 o NRI nuevo que va a tener el paquete de salida. Admite como entradas dígitos, caracteres '**S',** que suprime el dígito que figure en esa posición, y caracteres '**X**' que no lo cambia.
- **Negociar tamaño ventana:** Si no se activa no hay negociación de ventana y se usa la que esté configurada.
- **Negociar tamaño paquete:** Si no se activa no hay negociación y se utiliza el configurado.
- **Cobro revertido:** Permite solicitar al DTE llamadas a cobro revertido.
- **GCU:** Grupo Cerrado de Usuarios. Permite al usuario formar grupos de DTE con acceso restringido de entrada y/o salida. Permite a los DTE pertenecientes a este grupo comunicarse entre sí, pero excluye la comunicación con todos los demás DTE.
  - **Tipo:** Indica el tipo de GCU:
    - **NORMAL** (o entrante): Permite a un DTE perteneciente al grupo recibir llamadas de DTE situados en la parte abierta de la red (es decir, DTE no pertenecientes a ningún CGU) y d DTE pertenecientes a otros GCU con tipo SALIENTE.
    - **BILATERAL:** Permite a un par de DTE comunicarse entre sí mediante acuerdo bilateral, pero excluye la comunicación con todos los demás DTE.
    - **SALIENTE:** Permite al DTE pertenecer a uno o más GCU y originar llamadas virtuales a destinadas a DTE situados en la parte abierta de la red (es decir, DTE no pertenecientes a ningún CGU) y a DTE pertenecientes a otros GCU con tipo NORMAL (o entrante).
  - **Número:** Identificador del GCU.
- **IUR:** Identificador de Usuario de Red. Se usa en servicio X.32 de ETD identificado, y se compone de 10 caracteres (dígitos y letras). Sirve para facilidades de facturación, seguridad, gestión de red o solicitud de las facilidades a las que se está abonado.

- **Datos de usuario:** Este campo se codifica en hexadecimal. Es el nuevo valor que se envía en el paquete de llamada para los NR indicados en *Dirección X.25 llamada*. Admite hasta 4 bytes.

El tamaño máximo de la tabla viene determinado por la memoria del equipo.

• *Configuración XOT (sólo equipos NOVACOM-X25)*

Para configurar el protocolo XOT, se proporcionan dos ventanas, una con parámetros globales y otra para definir direcciones.

Configuración XOT Global

Los parámetros globales engloban la información del nivel 3 de X.25.

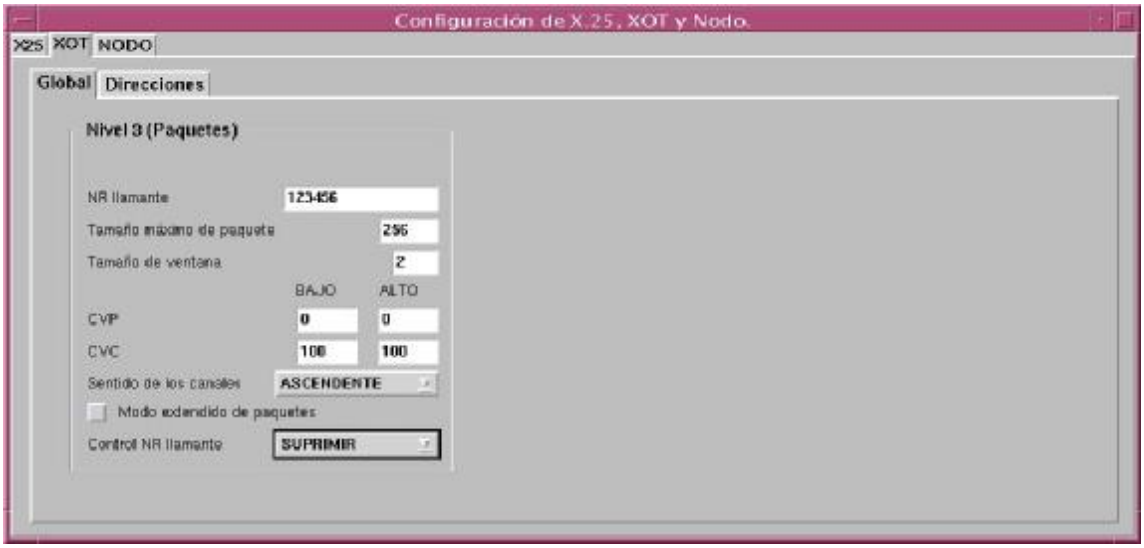


Figura 33 : Configuración XOT global

Habilitar XOT: Activa la configuración XOT en el equipo.

NIVEL 3 (Paquetes)

- **NR llamante :** Indica la dirección X.25 que debe colocarse como dirección llamante en las tramas de salida o como dirección llamada en las de entrada. Se admiten hasta 15 dígitos.
- **Tamaño máximo de paquete:** Es la longitud máxima en octetos del paquete transmitido. Se admiten valores en el rango **[128 .. 1024]** siendo **256** el valor por defecto.
- **Tamaño de ventana:** Indica el número de tramas enviadas pendientes de verificar. Si está activado el modo extendido de paquetes el rango es **[2 .. 127]** y sino **[2 .. 7]**.
- **CVP más bajo:** Número de Circuito Virtual Permanente más bajo utilizable. Se admiten valores en el rango **[0 .. 4096]** siendo **0** el valor por defecto.
- **CVP más alto:** Número de Circuito Virtual Permanente más alto utilizable. El CVP alto debe ser mayor o igual que el CVP bajo. El rango de CVP está siempre por debajo del rango de CVC. Se admiten valores en el rango **[0 .. 4096]** siendo **0** el valor por defecto.
- **CVC más bajo:** Número de Circuito Virtual Conmutado más bajo utilizable. El CVP alto debe ser menor que el CVC bajo. Se admiten valores en el rango **[0 .. 4096]** siendo **100** el valor por defecto.

- **CVC más alto:** Número de Circuito Virtual Conmutado más alto utilizable. El CVC alto debe ser mayor o igual que el CVC bajo utilizable. Se admiten valores en el rango **[0 .. 4096]** siendo **100** el valor por defecto.
- **Sentido de los canales:** Orden de asignación de los canales lógicos en las llamadas salientes.
- **Modo extendido de paquetes:** Módulo utilizado para numerar consecutivamente los paquetes X.25 enviados. Si está habilitado se utiliza módulo 128 y si no módulo 8.
- **Control NR llamante :** Indica si se modifica el NR llamante o se mantiene el que venga en la llamada. Puede tomar los siguientes valores:
  - **AGREGAR**: Añade el NR en todas las llamadas.
  - **SUPRIMIR**: Suprime el NR de todas las llamadas que pasen por el puerto.
  - **SALIENTES**: Añade el NR en las llamadas salientes.
  - **ENTRANTES**: Añade el NR en las llamadas entrantes.
  - **DTE-DCE**: Según interfaz, si es un DCE añade el NR en las llamadas que entran por el puerto, si es un DTE añade el NR en las llamadas que salen.

Configuración de direcciones XOT

La ventana de direcciones relaciona una dirección X.25 con una dirección IP. Se presenta un listado con las relaciones ya creadas y la posibilidad de crear otras nuevas, así como modificar las existentes o borrarlas.

- **Dirección X.25:** Dirección X.25 asignada a una determinada dirección IP. Se admiten hasta 15 dígitos o el carácter "X" (comodín).
- **Dirección IP:** Dirección IP (de host) asignada a una determinada dirección X.25.
- **Dirección IP alternativa:** Dirección IP de host alternativa de backup. Si no se consigue establecer la llamada con la primera en el tiempo establecido en el parámetro siguiente se intenta con esta.
- **Timeout:** Tiempo de espera, en segundos, de establecimiento de la conexión con la primera dirección IP. Si se supera, se pasa a intentar la conexión con la dirección IP alternativa. Se admiten valores en el rango **[0 .. 1000]** siendo **30** el valor por defecto que significa que no está activado el backup.

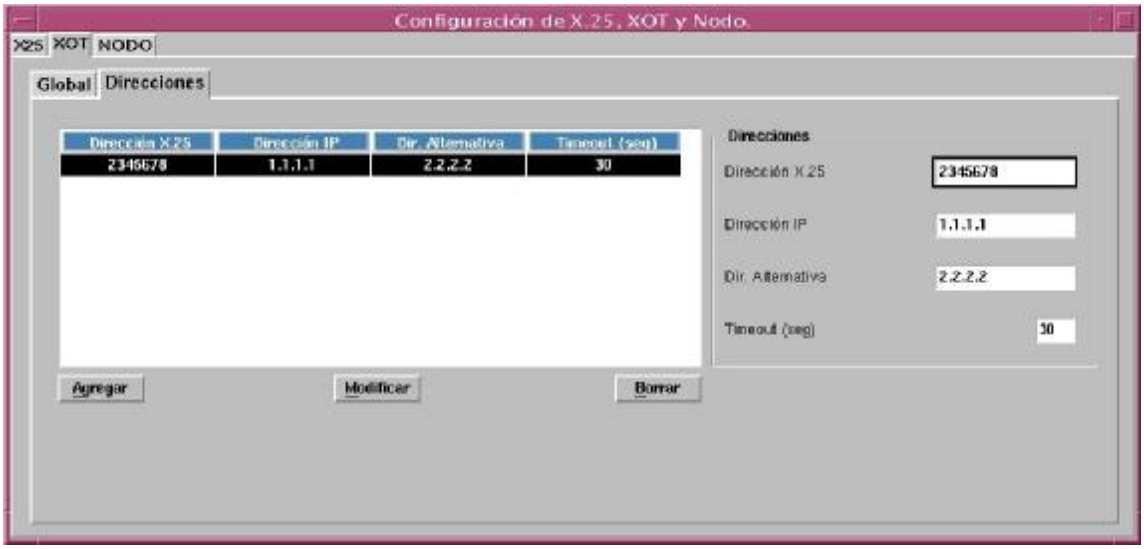


Figura 34 : Configuración de direcciones XOT

- ***Configuración ASDP (sólo equipos C4I)***

Las ventana de configuración de ASDP (Asynchronous Serial Device Proxy) se activa pulsar el botón  de la barra de herramientas.

En la figura se muestran los parámetros configurables de este interfaz.

Figura 35 : Configuración ASDP

- **Velocidad de la línea serie (bps):** Especifica la velocidad en bits por segundo con la que se comunican el router y la impresora conectada a esa línea. El rango de valores de este campo se encuentra comprendido entre **300** y **57600** bits por segundo
- **Puerto TCP:** Puerto de la comunicación TCP que se establece entre el router y el equipo remoto.
- **Control de flujo:** En muchos casos el router es capaz de enviar datos al dispositivo serie a un ritmo mayor que éste es capaz de soportar. Por ello, con este parámetro establecemos un mecanismo para regular el ritmo del flujo de datos entre ambos.

m) DHCP

El router C2 tiene tres modos de funcionamiento respecto del protocolo DHCP (Dynamic Host Configuration Protocol):

DESHABILITADO	El router no ofrece servicio DHCP.
REPETIDOR	El router retransmite los paquetes del protocolo DHCP de los clientes a un servidor DHCP principal y, opcionalmente, a otro secundario.
SERVIDOR	El router se comporta como servidor DHCP respondiendo a las peticiones de los clientes.

• *Configuración como repetidor DHCP*

Como repetidor DHCP el router reenvía los paquetes de los cliente DHCP al servidor(es) que tiene configurados.

Es obligatorio introducir la dirección IP de un servidor primario y opcional la del secundario. Si hay dos configurados el router les reenvía a ambos los paquetes.

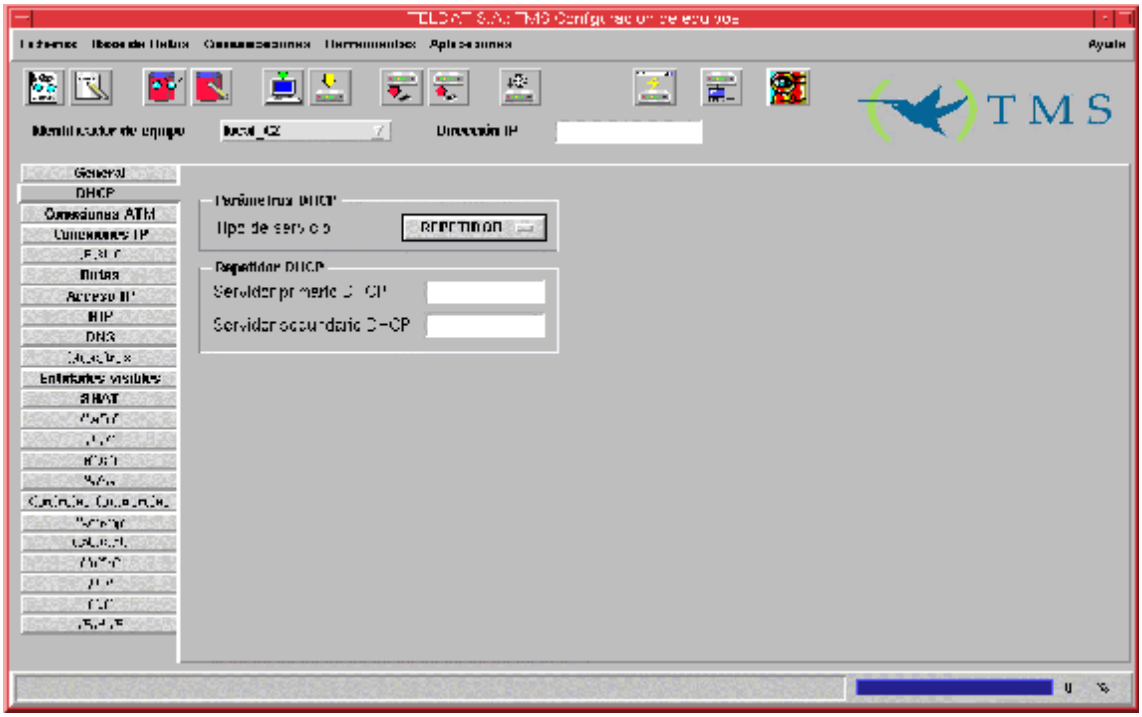


Figura 36 : Configuración de repetidor DHCP

• *Configuración como servidor DHCP*

Como servidor el router atiende las peticiones DHCP de los clientes.

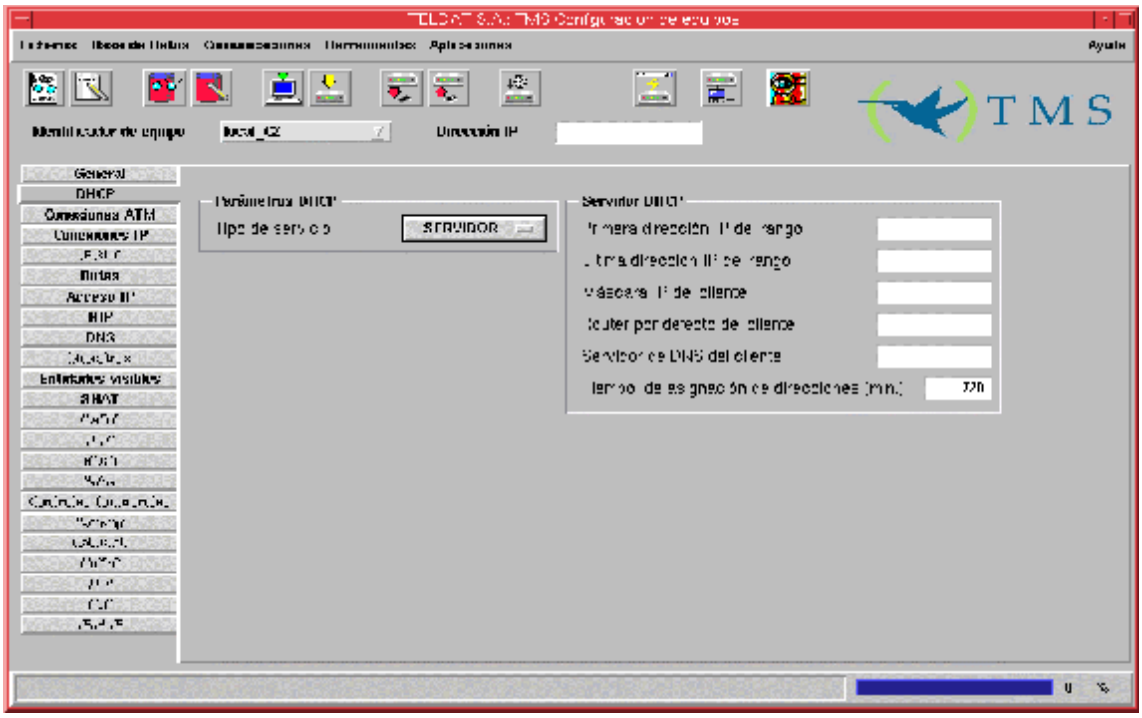


Figura 37 : Configuración como servidor DHCP

Los parámetros configurables son los siguientes:

Primera dirección IP del rango: El router dispone de un rango de direcciones IP para asignar a los clientes. Esta es la primera dirección IP del rango. Dentro de este rango el equipo discrimina su propia dirección IP, y la del router por defecto y servidor de DNS para que no sean asignadas.

Última dirección IP del rango: Límite superior del rango de direcciones asignables por el router. Es preciso que la primera dirección IP no sea superior a la última del rango, por eso la aplicación convierte a binario y verifica que esto no ocurra.

Máscara IP del cliente: Es la máscara IP que se le asigna al cliente DHCP junto con la dirección.

Router por defecto del cliente: Es el router por defecto que se le configurará al cliente DHCP.

Servidor de DNS del cliente: Es el servidor de DNS que se le configurará al cliente DHCP.

Tiempo de asignación de direcciones [min.]: Es el tiempo en minutos que el servidor mantendrá asignada una dirección si el cliente no solicita su renovación. Transcurrido este tiempo la dirección podrá ser reasignada a otro cliente que la solicite. Se admiten valores en el rango [1 .. 525600] minutos. El valor por defecto es 720.

Se espera que el funcionamiento más extendido sea el de configuración más simple, es decir, aquel en el que el router se instala en una pequeña LAN que necesita acceso a INTERNET y se configura como

servidor DHCP configurándose él mismo como router por defecto y servidor de DNS, de forma que, cuando arranca cualquier estación de la LAN le solicita una dirección IP y su configuración y, una vez recibida, la estación estaría en condiciones de navegar por INTERNET.

n) Conexiones ATM

Las conexiones ATM (Asynchronous Transfer Mode) son la entidad de más bajo nivel que se configura desde la gestión . Sobre ellas se definen las conexiones IP y a partir de estas el resto de entidades de la configuración del router.

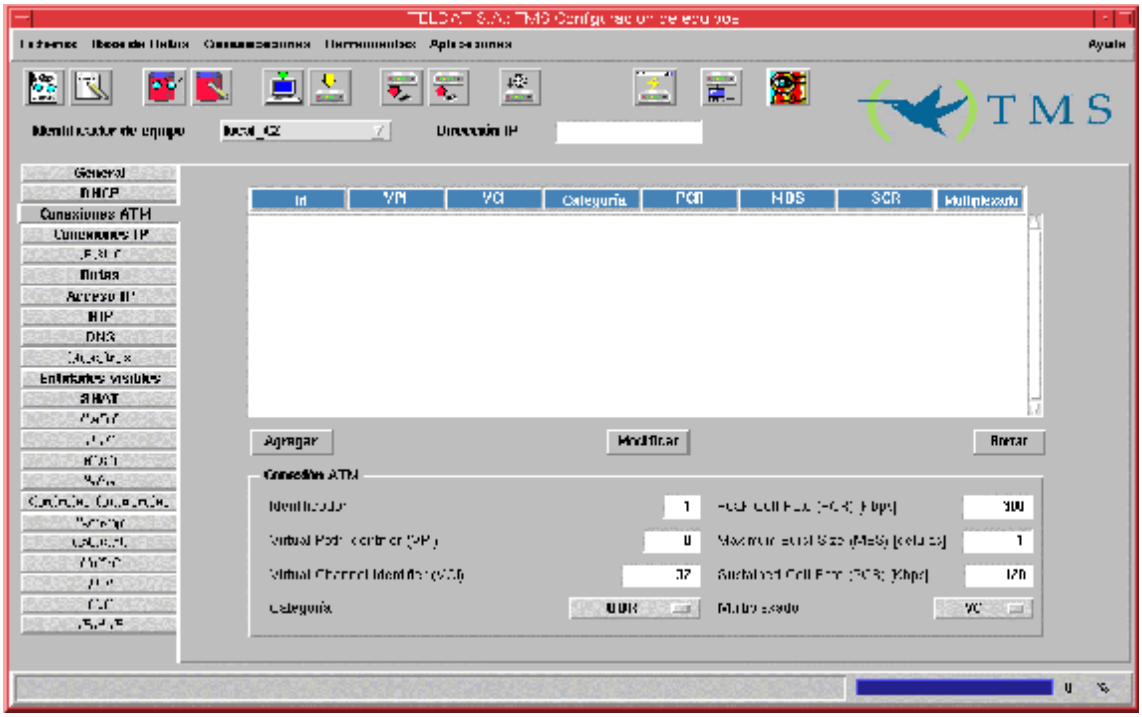


Figura 38 : Configuración de conexiones ATM

Los parámetros configurables son los siguientes:

- **Identificador:** Identificador de conexión ATM. Se trata de un entero perteneciente al rango **[1 .. 99]** que no puede repetirse.

- **Virtual Path Identifier (VPI):** Identificación de ruta virtual ATM. Este identificador junto con el VCI, proporciona la información de encaminamiento. Se trata de un entero en el rango **[0 .. 255]**. No se puede repetir el binomio VPI/VCI.

- **Virtual Channel Identifier (VCI):** Identificador de canal virtual ATM. La ITU-T (International Telecommunications Union) define un "virtual channel" como el transporte unidireccional de celdas entre dos nodos asociadas a un VCI común; es decir, cada VCI identifica una conexión distinta entre dos extremos. Se trata de un entero en el rango **[32 .. 65535].** No se puede repetir el binomio VPI/VCI.

- **Categoría:** Este apartado describe las diferentes categorías de servicio ATM (denominación ATM Forum) o capacidades de transferencia ATM (denominación ITU-T).
- Puede tomar los valores **CBR**, **VBR_RT**, **VBR_NRT** o **UBR**. El valor por defecto es **UBR**.

  1. Variable Bit Rate (VBR): También llamado Statistical Bit Rate (SBR). El servicio VBR se caracteriza por ofrecer dos velocidades, siendo adecuado para tráficos cuyos requisitos de velocidad tienen variaciones en el tiempo. Se definen dos tipos, uno para aplicaciones de tiempo real (VBR_RT) (con restricciones en el retardo y su variación), como voz con supresión de silencios y el vídeo comprimido, y otro (VBR_NRT) para aplicaciones con transmisión a ráfagas pero sin restricciones de retardo. Los parámetros configurables son la velocidad de pico (PCR o Peak Cell Rate), la velocidad sostenida (SCR o Sustained Cell Rate) y el tamaño máximo de la ráfaga (MBS o Maximum Burst Size) que determinan que, después de un periodo largo de silencio, el equipo puede transmitir un determinado tiempo a PCR (este tiempo viene determinado por el PCR, el SCR y el MBS), para después pasar a transmitir a SCR; durante los periodos de silencio, el equipo gana "crédito" para, cuando tenga necesidad de transmitir, pueda transmitir un determinado tiempo de nuevo a PCR.

  2. Constant Bit Rate (CBR): También llamado Deterministic Bit Rate (DBR). El servicio CBR se caracteriza por ofrecer una velocidad constante de valor configurado, sean cuales sean las condiciones de congestión de la red ATM, es decir, ofrece una tasa garantizada, de modo que, utiliza recursos de la red aun cuando no haya información disponible para transmitir. Se puede entender como un circuito convencional, en el que se toma una porción de la capacidad del medio físico y que queda permanentemente asignada a dicha comunicación. Como parámetro configurable está la velocidad del circuito, representada por el PCR o Peak Cell Rate. Este tipo de servicio se enfoca hacia aplicaciones de tiempo real, es decir, aquellas que requieren retardos y variaciones en dicho retardo bajos, como voz, vídeo y emulación de circuitos.

  3. Unspecified Bit Rate (UBR): El servicio UBR es un servicio denominado "best effort", orientado a aplicaciones que no tienen restricciones de retardo o variación del mismo, ni requieren unos parámetros de calidad de servicio determinados, lo que abarata su contratación. Está enfocado a aplicaciones que generan un tráfico a ráfagas no continuo, lo cual permite un alto grado de multiplexación estadística. El servicio UBR suele tener un único parámetro configurable, el PCR, que determina la velocidad que nunca debe superar el circuito que hace uso de este servicio. Aplicaciones típicas son la transferencia de datos, la mensajería, etc.

- **Peak Cell Rate (PCR):** Determina la tasa binaria máxima a la que se permite transmitir a la conexión. Se permiten valores en el rango **[1 .. 8192]** Kbps. El valor por defecto es de **300** Kbps.

- **Maximum Burst Size (MBS):** Determina el tamaño máximo (en células) de la ráfaga (MBS) permitida a PCR antes de pasar a transmitir a SCR. Este parámetro solo se solicita si la categoría de tráfico es VBR_RT o VBR_NRT. Se admiten valores mayores que 0. El valor por defecto es **1** célula.

- **Sustained Cell Rate (SCR):** Determina la tasa binaria a la que se permite realizar una transmisión sostenida. Este parámetro solo se solicita si la categoría de tráfico es VBR_RT o

VBR_NRT. Se admiten valores en el rango **[1 .. 8192]** Kbps pero además nunca debe de ser mayor que el valor del parámetro PCR. El valor por defecto es **128** Kbps.

- **Multiplexado:** Hay dos tipos de multiplexado

  1. Virtual Circuit (VC): Cada tipo de tráfico de nivel superior se transporta en una conexión diferente, sin añadir ningún tipo de cabecera.

  2. Logic Link Control (LLC): Diversos tipos de tráfico de nivel superior comparten la misma conexión para transportar sus datos, insertando una cabecera LLC para indicar el tipo de tráfico contenido en dicha trama.

El máximo número de conexiones ATM que se pueden definir es 5.

Para añadir un conexión rellenar los campos y pulsar **Agregar**.

Para modificar una conexión, seleccionarla en la lista, modificar los campos correspondientes y pulsar **Modificar**.

Para borrar una conexión ATM seleccionarla en la lista y pulsar **Borrar**.

Borrado de conexiones ATM.
No se puede borrar una conexión ATM de la que dependa una conexión IP. Para borrarla antes hay que borrar las conexiones IP que dependan de ella.

o) Conexiones IP

Las conexiones IP se sustentan sobre las conexiones ATM y a su vez sustentan al resto de entidades de configuración.

Según el tipo de conexión, el encapsulado y el modelo de equipo habilitan los distintos parámetros de configuración.

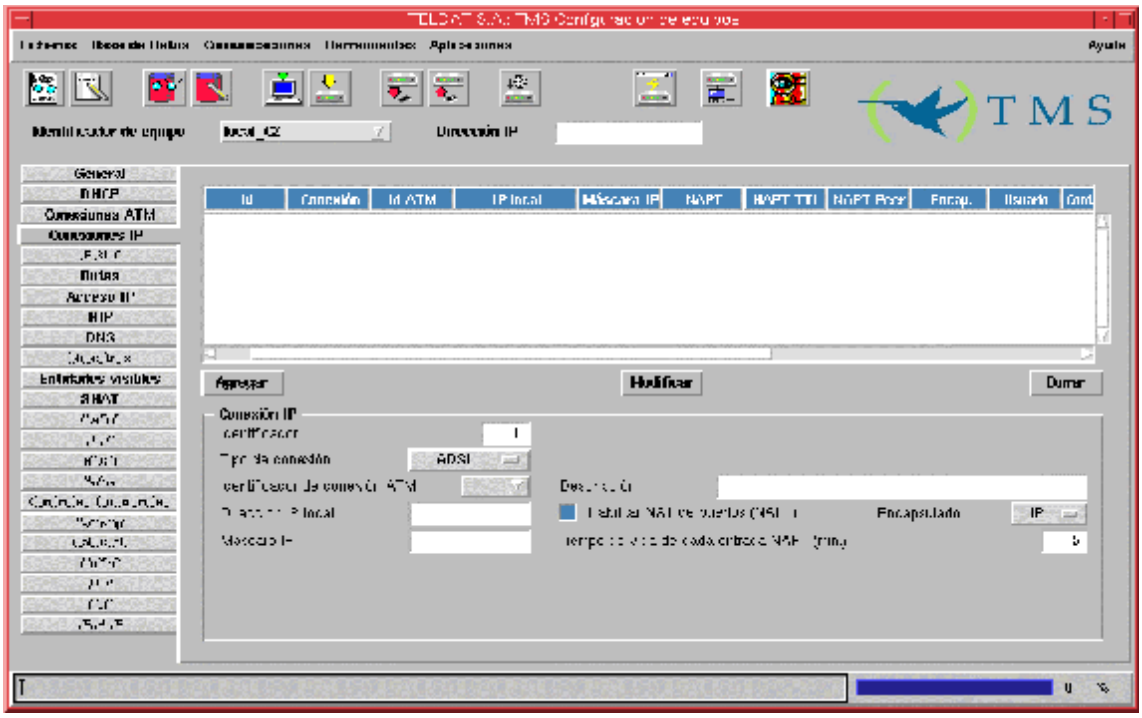


Figura 39 : Conexiones IP con tipo ADSL

Están compuestas de los siguientes parámetros:

- **Identificador:** Identificador de conexión IP. Es un entero en el rango **[1 .. 99]** que no puede repetirse.
- **Identificador de conexión ATM:** Identificador de la conexión ATM sobre la que se sustenta. Sólo se pueden seleccionar los que están definidos en la ventana de conexiones ATM.
- **Dirección IP local:** Se trata de una dirección de subred o de host. Todos los paquetes dirigidos a cualquier dirección IP de este rango se encaminan por esta conexión IP a no ser que exista una ruta más restrictiva en la tabla de rutas en cuyo caso se encaminan de acuerdo a dicha ruta.
- **Máscara IP:** Junto con la dirección IP anterior definen el rango de direcciones asociado a la conexión IP.
- **Encapsulado:** Con la opción PPP se muestran las entradas para usuario y contraseña.
- **Usuario:** Identificador de usuario en conexiones con encapsulado PPP.
- **Contraseña:** Contraseña del usuario anterior en conexiones con encapsulado PPP.
- **NAT de puertos:** Habilita o deshabilita el NAT de puertos en la conexión.

- **Tiempo de vida de entrada NAT:** Cuando está habilitado NAT indica el tiempo en minutos que se mantiene cada entrada antes de desecharla. Se admiten valores en el rango **[1 .. 240]** minutos siendo **5** minutos el valor por defecto.

- **Descripción:** Cadena explicativa de hasta 79 caracteres.

En la siguiente ventana se ha seleccionado una conexión LAN y encapsulado PPP.

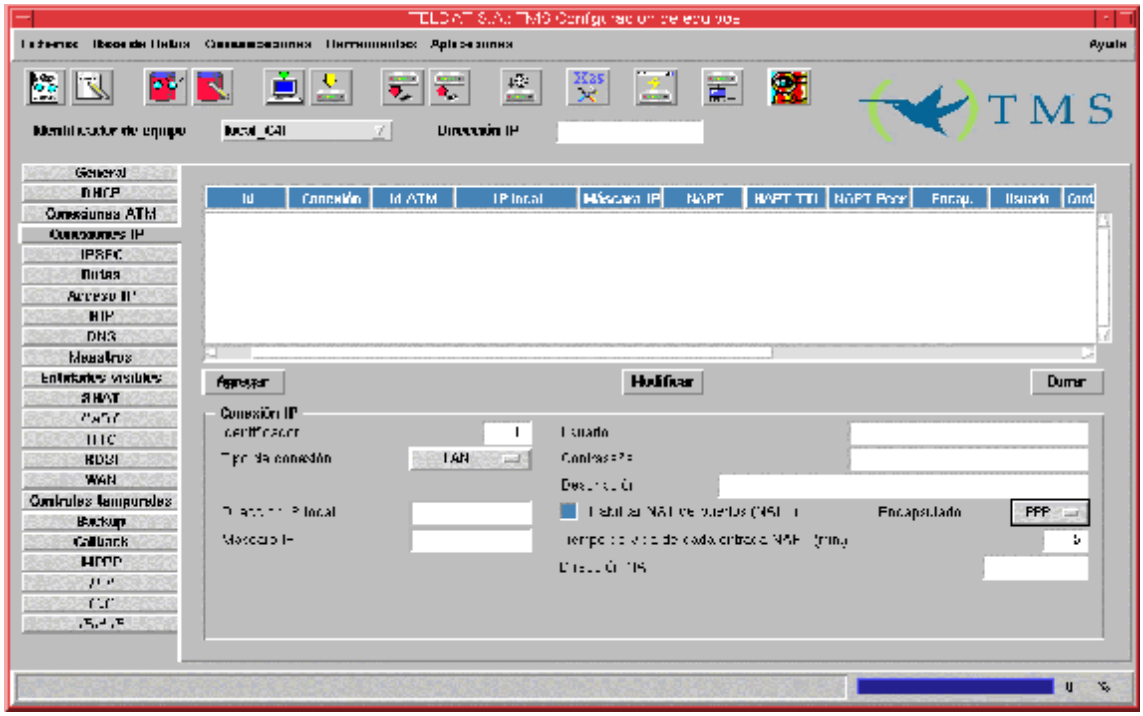


Figura 40 : Conexiones IP con tipo LAN y PPP

- **Usuario:** Identificador de usuario en conexiones

- **Contraseña:** Contraseña del usuario anterior en conexiones

- **Dirección NATP:** Dirección pública del equipo para usuarios externos cuando se habilita el NAT.

Cuando se selecciona un C3 con conexión RTC o RDSI la ventana presenta un aspecto como sigue:

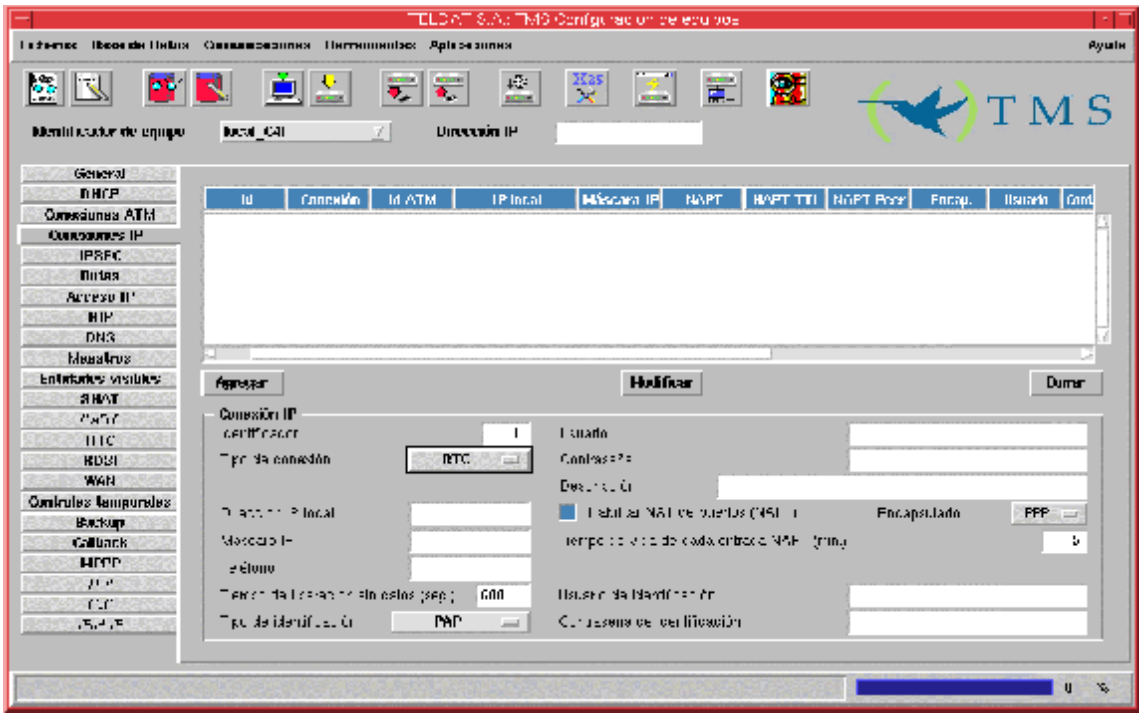


Figura 41 : Conexiones IP con tipo RTC y PPP

Teléfono: Es el teléfono al que el equipo demanda la conexión a través de la RDSI. Para minimizar el coste de las llamadas es conveniente utilizar el teléfono del Nodo de Acceso más próximo al equipo. Se admiten un máximo de 19 dígitos.

Tiempo de liberación sin datos (seg): Las conexiones a través de RDSI se terminarán normalmente por ausencia de datos en la línea durante un tiempo igual o superior al tiempo de liberación sin datos. El valor por defecto es de 600 segundos. No es recomendable usar tiempos demasiado bajos. La precisión del temporizador es de T/10 siendo T el tiempo de liberación sin datos. Se permiten valores en el rango [0, 60 .. 65535]. El valor 0 es un caso especial que equivale a una conexión permanente. Este valor se utiliza, por ejemplo, como medio para unir subredes. Si hay establecido un control horario y el tiempo de liberación sin datos es 0, entonces, el equipo establece conexión con en el instante en que comienza el período horario de accesibilidad. De esta forma, en dicho período, el cliente puede comunicar sus subredes. Si no hay restricciones horarias y se asigna el valor 0, el equipo establece una conexión permanente tras el arranque.

Tipo de identificación: Lo habitual al acceder a una red externa es que sea la propia red externa la que solicite al equipo de acceso que se autentique como paso previo a poder usar la red. Sin embargo, en escenarios punto a punto, donde no se accede a una red externa, sino a una red remota conocida, a través de un equipo remoto también conocido, es posible indicar al extremo remoto que necesita autenticarse. El equipo soporta los protocolos de autenticación PPP **Password Authentication Protocol (PAP)** y **Challenge Handshake Authentication Protocol (CHAP)**.

Se admite un máximo de 10 conexiones IP.

Para añadir un conexión rellenar los campos y pulsar **Agregar**.

Para modificar una conexión, seleccionarla en la lista, modificar los campos correspondientes y pulsar **Modificar**.

Para borrar una conexión IP seleccionarla en la lista y pulsar **Borrar**.

> ***Borrado de conexiones IP.***
>
> ***No se puede borrar una conexión IP que esté siendo utilizada por alguna otra entidad como pueda ser una ruta, un puerto visible, una subred visible, etc. Es necesario borrar antes todas las entidades asociadas.***

p) RDSI

Hay una ventana de configuración de los canales B de la RDSI de los que dispone el equipo:

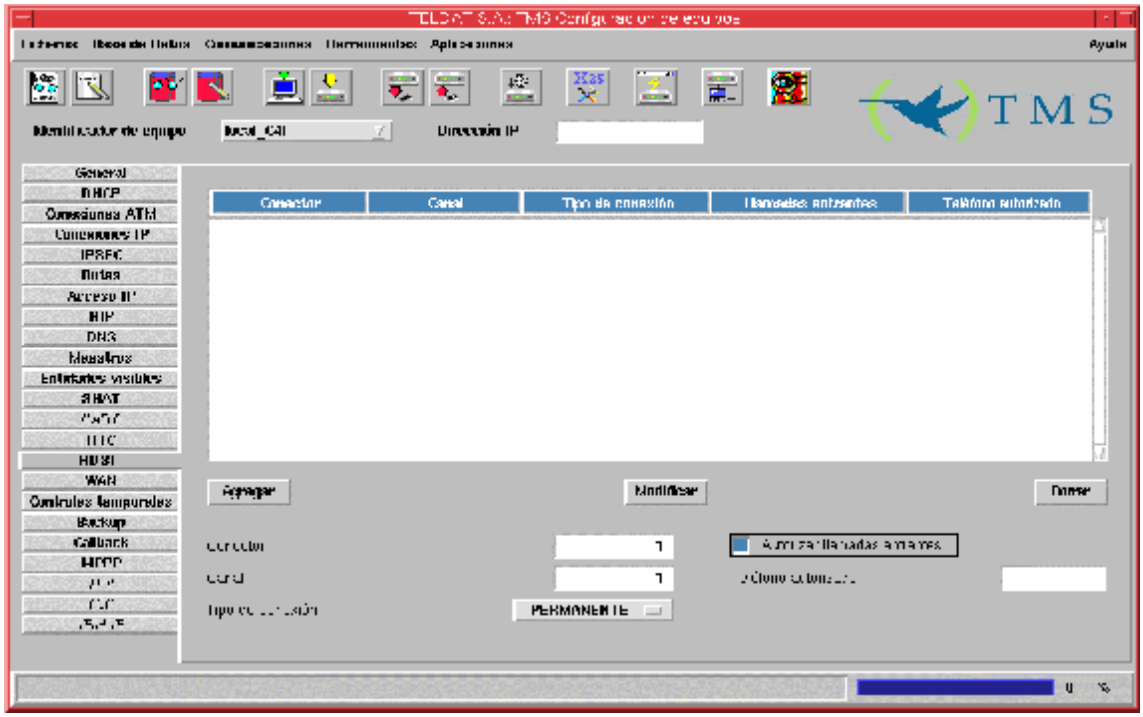


Figura 42 : Configuración de los canales RDSI

- **Conector:** Línea RDSI a la cual esta asociada el canal B correspondiente.
- **Canal:** Canal B asociado a una determinada línea RDSI.

- **Tipo de conexión:** Indica el tipo de conexión que se establece en el canal. Si el usuario tiene contratado con el proveedor de RDSI un canal B RDSI permanente, debe indicarlo con este parámetro. Un canal B permanente es un canal B RDSI especial que no utiliza la señalización porque su destino está fijado en la contratación del servicio. Dicho canal B no hace llamadas RDSI y siempre está conectado. Si habilita un canal B como **PERMANENTE**, los parámetros de teléfono destino de la conexión, tiempo de liberación por ausencia de datos e intervalo de conexión permitido son ocultados. En la contratación del canal B permanente se especifica qué canal B (B1, B2 o ambos) responde a este perfil. No se permite que los dos canales tengan conexión permanente porque, en tal caso, el equipo dejaría de ser gestionable. El valor por defecto es **CONMUTADA**.

- **Autorizar llamadas entrantes:** Como equipo de acceso, es el propio equipo el que realiza la llamada al proveedor de la red externa a la que se quiere conectar. Sin embargo, en escenarios de conexión entre dos equipos, uno realiza la llamada y el otro la recibe. Si se desea que un equipo pueda recibir llamadas entrantes, debe habilitarse este parámetro. El comportamiento por defecto del equipo es no permitir las llamadas entrantes.

- **Teléfono autorizado:** Si las llamadas entrantes están habilitadas, este parámetro indica el número RDSI que está autorizado para conectarse. Si no se configura ningún valor, cualquier llamante estará autorizado para conectarse, aunque deberá autenticarse vía PAP o CHAP si así se le indica. El valor por defecto (vacío) de este parámetro autoriza a cualquier número llamante.

Para agregar un nuevo canal a la lista, rellenar los campos y pulsar **Agregar**.

Para modificar un canal se selecciona en la lista y, tras modificar los campos correspondientes, se pulsa **Modificar**.

En el caso de la opción **Borrar**, se elimina el elemento seleccionado.

Se admiten un máximo de dos líneas RDSI con dos canales B cada una de ellas

q) Controles temporales

Sirve para restringir el tráfico a través cada conexión IP a un intervalo temporal ciertos días de la semana o para forzar la conexión del equipo en dicho intervalo.

El intervalo de conexión especifica el período en que la conexión IP elegida estará operativa. Fuera de este intervalo la conexión está bloqueado, excepto para conexiones de gestión, que siempre están garantizadas.

Seleccionar la conexión IP.

Seleccionar los días de la semana en los cuales el equipo funcionará normalmente.

Introducir el instante de comienzo del intervalo y el instante final del intervalo en formato **hh:mm**. Para la hora se admiten valores dentro del intervalo [0..23] y para los minutos [0..59]. Si la hora final

es menor que la inicial se considera que pertenece al día siguiente. Si el día siguiente no está permitida la conexión tiene prioridad el día sobre la hora y la conexión estará deshabilitada para dicho día.

Cuando el tiempo de liberación sin datos es 0, el equipo se conecta automáticamente al comenzar el intervalo temporal establecido en la configuración horaria.

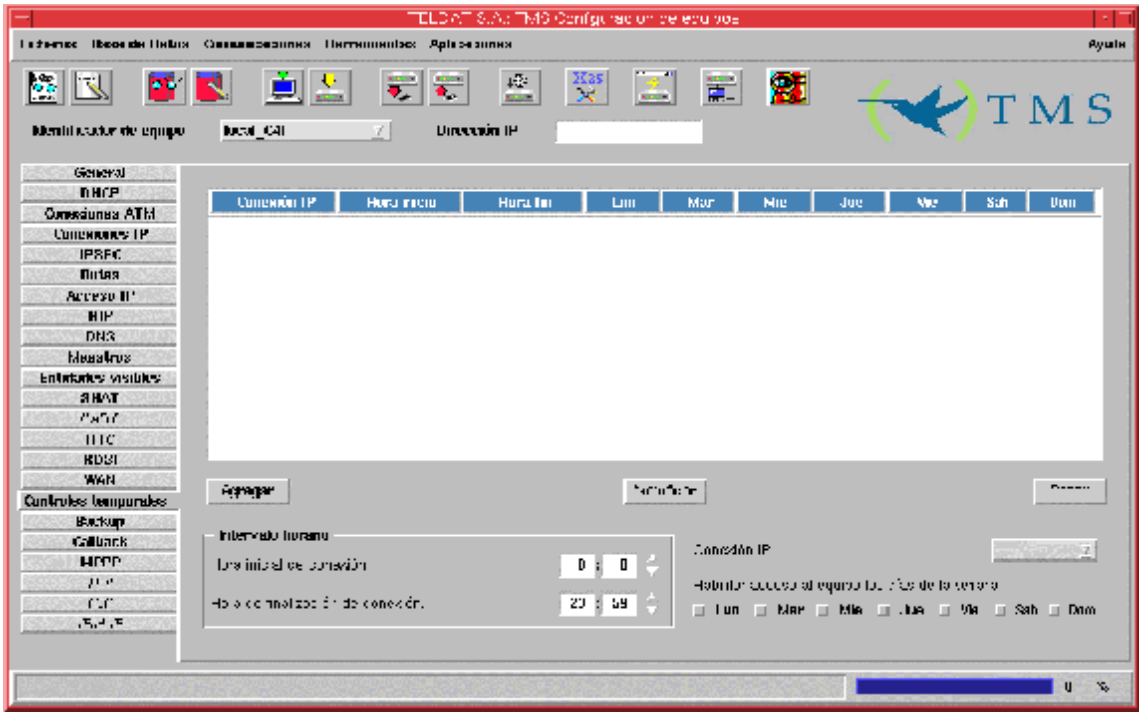


Figura 43 : Configuración de los intervalos de conexión

Para agregar un nuevo intervalo a la lista, rellenar los campos y pulsar **Agregar**.

Para modificar un intervalo se selecciona en la lista y, tras modificar los campos correspondientes, se pulsa **Modificar**.

En el caso de la opción **Borrar**, se elimina el elemento seleccionado.

Se admite un máximo de 10 intervalos de conexión

r) TCP

En esta ventana se configuran las distintas conexiones TCP de las que dispondrá el router.

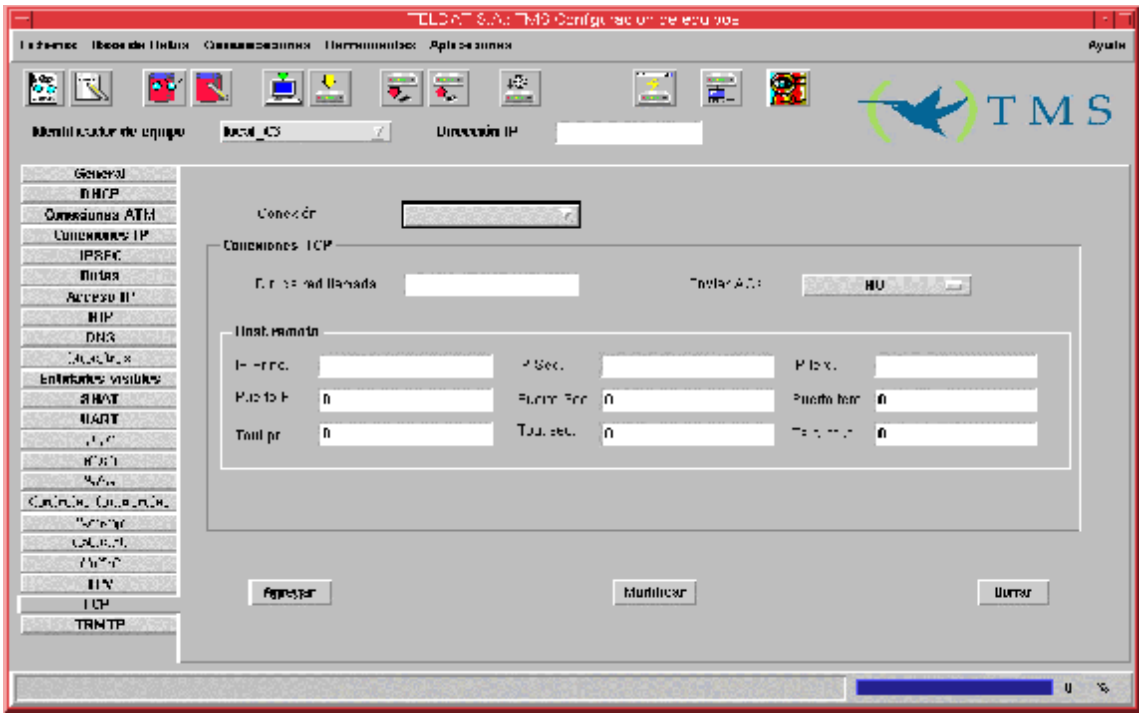


Figura 44 :. Configuración de conexiones TCP.

Los distintos parámetros que se pueden configurar desde esta ventana son:

- **Dirección de red llamada:** Este parámetro permite configurar la dirección IP a la que llamará el router. Se considerará válida cualquier dirección de hasta 15 caracteres, permitiendo introducir también el carácter X. La dirección por defecto, y por tanto la nula, es la XXXXXXXXXXXXXXX.

El resto de los parámetros servirán para configurar las direcciones, puertos y temporizadores de los hosts remotos:

- **Dirección IP:** Representa la dirección IP de cada uno de los tres hosts remotos que se pueden configurar.

- **Puerto remoto:** Representa el puerto de cada uno de los tres hosts remotos que se pueden configurar.

- **Time out de respuesta:** Representa el tiempo que se puede esperar hasta obtener respuesta de cada uno de los hosts remotos que se pueden configurar. La unidad de medida será segundos, permitiéndose valores entre 0 y 100.

Para añadir una conexión, rellenar los campos y pulsar **Agregar**.

Para modificar una conexión, seleccionarla en la lista desplegable, modificar los campos correspondientes y pulsar **Modificar**.

Para borrar una conexión TCP, seleccionarla en la lista y pulsar **Borrar**.

s) TRMTP

Mediante esta ventana se podrán configurar todos los parámetros de las conexiones TRMTP del router. Para facilitar la configuración de cada conexión, cada uno de los tres host que se podrán configurar podrán ser seleccionados en una lista desplegable y configurados separadamente.

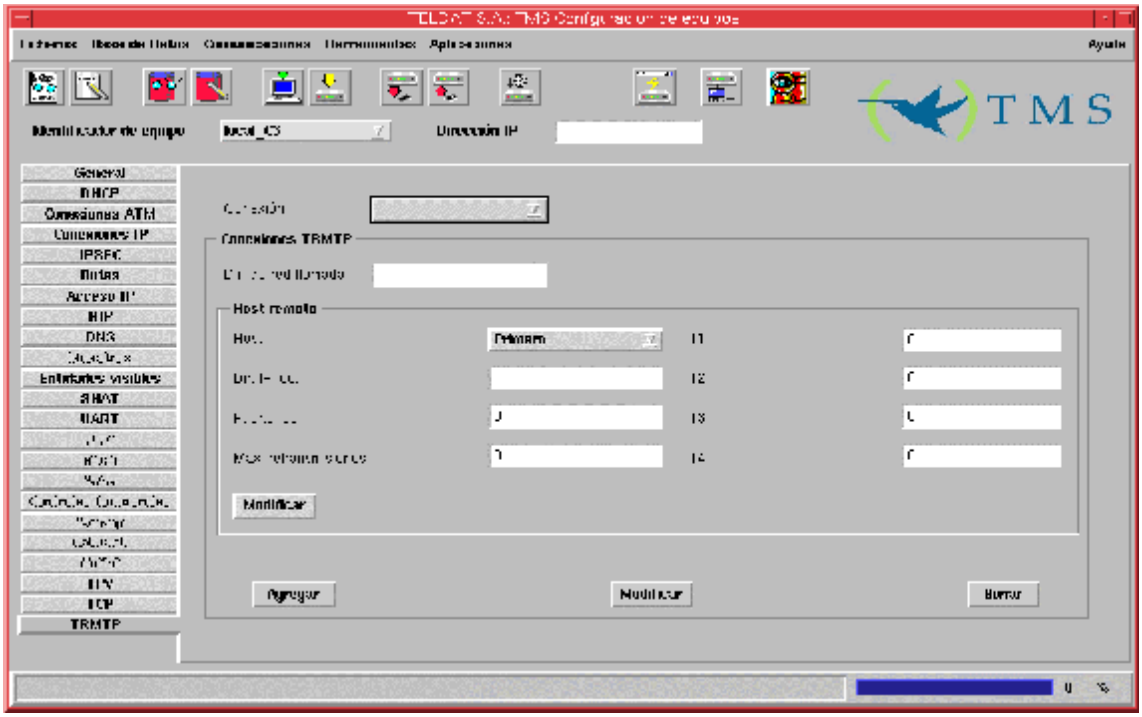


Figura 45 :. Configuración de conexiones TRMTP

Los parámetros que se pueden configurar desde esta ventana son:

- **Dirección de red llamada**: Dirección IP a la que el router llamará.

Para cada uno de los tres hosts configurables:

- **Dirección IP**: Dirección IP del host que está siendo configurado.
- **Puerto:** Puerto de cada uno de los hosts a configurar.
- **Máximo número de retransmisiones:** Máximo número de veces que se desea que retransmite el host remoto. Su valor estára comprendido entre cero y 65535 retransmisiones, siendo 3 su valor por defecto.

- **Temporizador T1:** Tiempo de espera de una confirmación antes de retransmitir. Su valor estará comprendido entre 1 segundo y 65535, siendo su valor por defecto 10.

- **Temporizador T2**: Tiempo de espera antes de salir de un estado de error en el transmisor. Su valor estará comprendido entre 1 segundo y 65535, siendo su valor por defecto 40.

- **Temporizador T3:** Tiempo de inactividad antes de salir del estado de datos en el transmisor. Su valor estará comprendido entre 1 segundo y 65535, siendo su valor por defecto 30.

- **Temporizador T4:** Tiempo de inactividad antes de volver al estado de OFF. Su valor estará comprendido entre 1 segundo y 65535, estando su valor por defecto establecido en 100 segundos.

Para añadir una conexión, rellenar los campos y pulsar **Agregar**.

Para modificar una conexión, seleccionarla en la lista desplegable, modificar los campos correspondientes y pulsar **Modificar** general.

Para borrar una conexión TRMPT, seleccionarla en la lista y pulsar **Borrar**.

Para modificar un host, seleccionarlo en su lista desplegable, rellenar los campos y pulsar el botón **Modificar** del host remoto.

t) TPV

En esta ventana se configurarán los parámetros generales para los TPV. El máximo número de terminales será cuatro en el caso de equipos C3 y tan sólo uno para los equipos C3G.

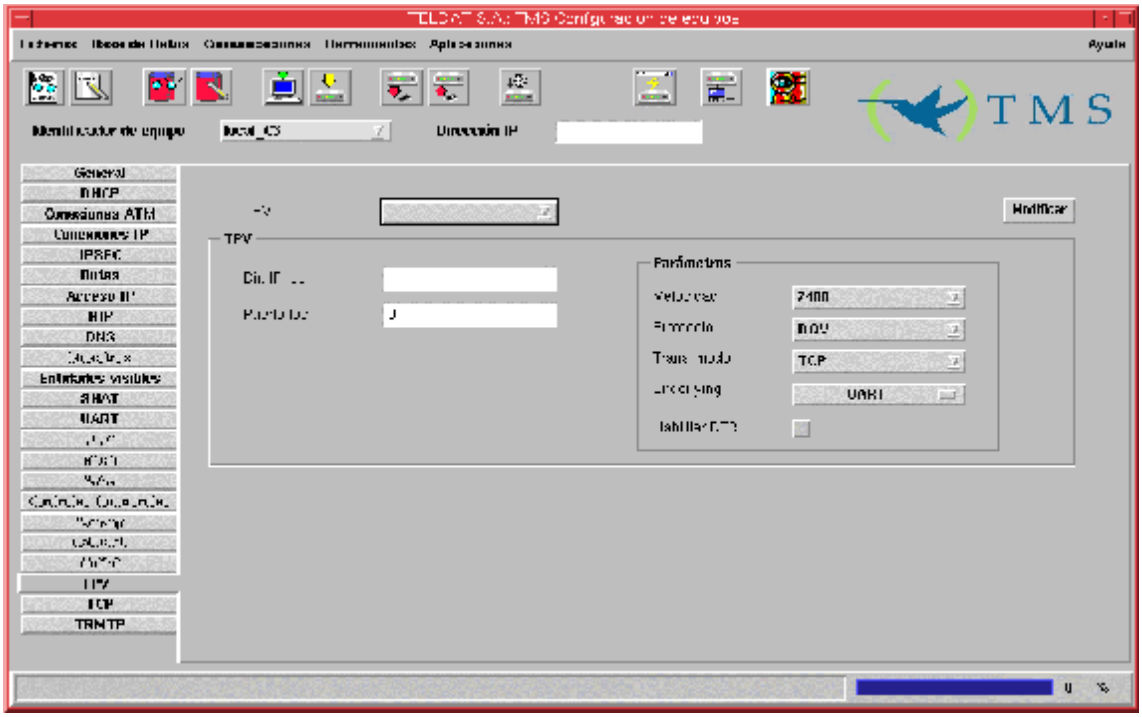


Figura 46 :. Configuración de los TPV

Los diferentes parámetros que se pueden configurar para cada TPV desde esta ventana son los siguientes:

- **Dirección IP:** La dirección IP del terminal sólo tiene significado si se escoge como protocolo TCP. En otro caso, su valor se ignorará.

- **Puerto loc.:** El puerto local sólo tiene significado si el protocolo seleccionado es TRMTP. En otro caso, su valor se ignora.

- **Velocidad de transmisión:** Indica la velocidad del terminal medido en bits por segundo. Debe estar comprendida entre 300 y 64000. Su valor por defecto será 2400.

- **Protocolo usado para la transmisión:** El protocolo que se use para la transmisión podrá elegirse para que sea DOV, DAT o VISANET.

- **Modo de transmisión:** El modo de transmisión podrá elegirse para que sea TCP o TRMTP.

u) UART

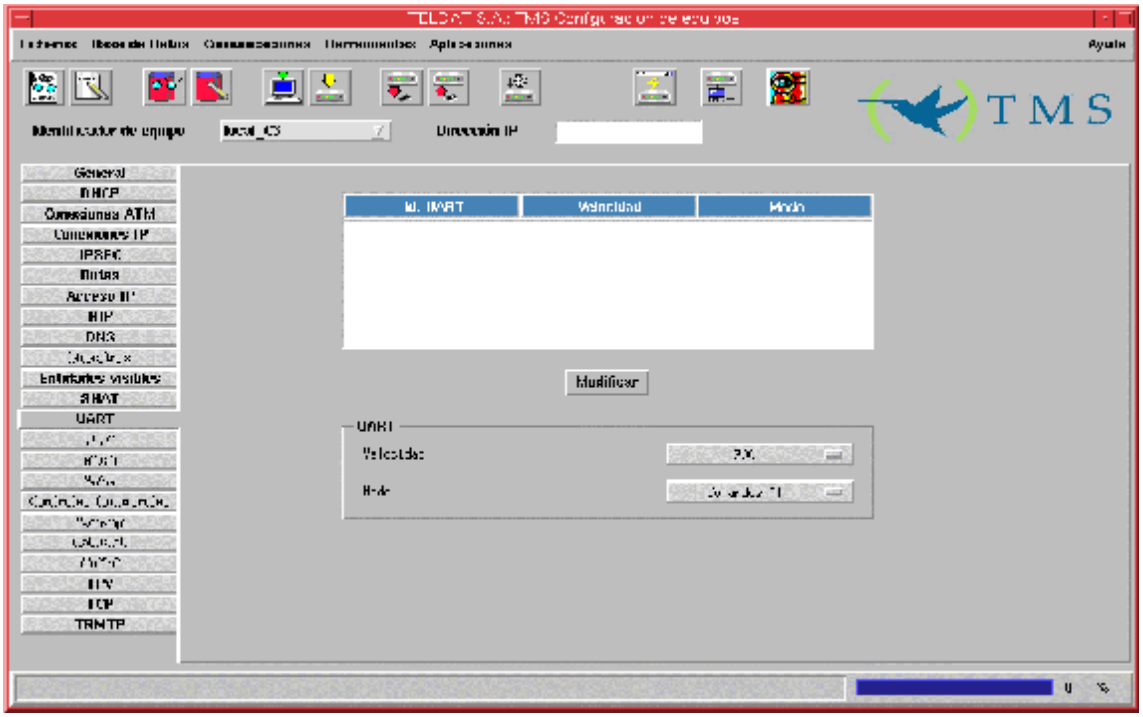


Figura 47 :. Configuración UART.

- **Velocidad:** Indica que velocidad posee la línea del puerto UART
- **Modo:** Especifica el uso que se le da al puerto UART.

v) RTC

- ***Equipos NOVACOM Y NOVACOM-X25***

Ver el punto Canal B1 (solo para equipos NOVACOM y NOVACOM-X25) para mas detalles.

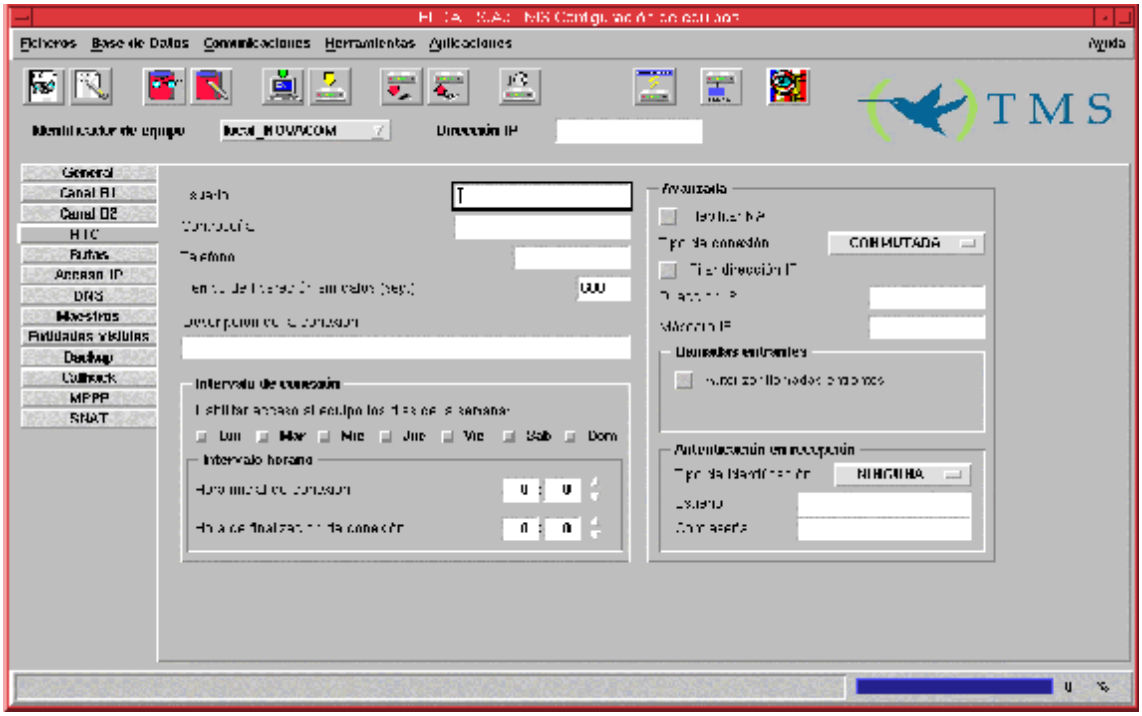


Figura 48 :. Configuración RTC para equipos NOVACOM.

- ***Equipos Cx***
  - **Habilitar patrón de llamadas:** Permite la activación de una determinada secuencia para efectuar una llamada a través de RTC.
  - **Número de tonos:** Número de tonos que tiene el patrón de llamadas.
  - **Número de silencios:** Número de silencios que tiene el patrón de llamadas
  - **Autorizar llamadas entrantes:** Permite recibir llamadas a través de la RTC.
  - **Teléfono del patrón:** Número al que se envía el patrón de llamadas

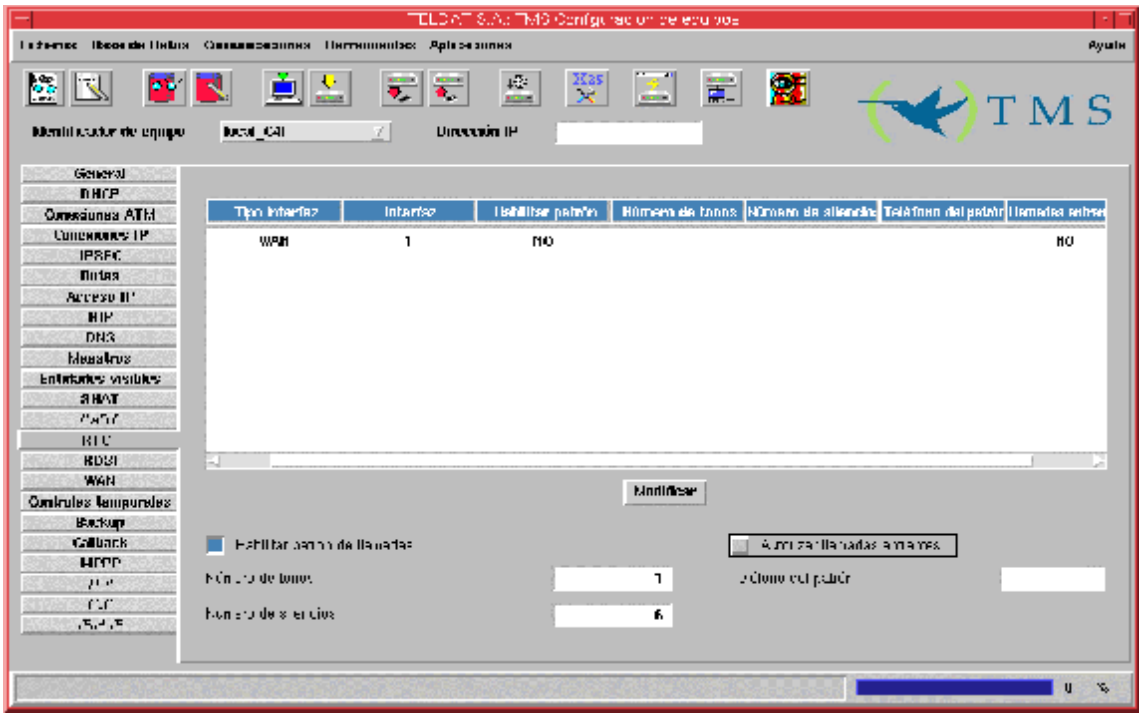


Figura 49 :. Configuración RTC para equipos Cx.

w) WAN

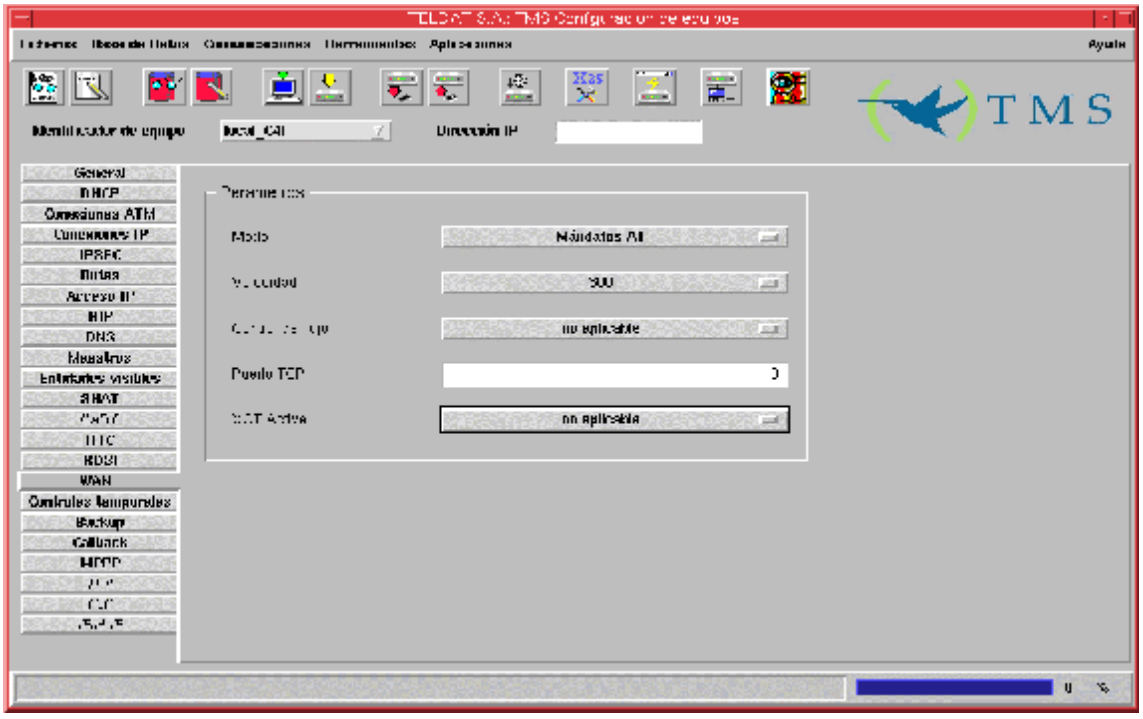


Figura 50 :. Configuración WAN.

- **Modo:** Tipo de funcionamiento de la línea WAN.

- **Velocidad:** Velocidad de la línea.
- **Control de flujo:** En el caso de que la línea funcione en modo ASDP indica el tipo de control de flujo hardware que posee
- **Puerto TCP:** En el caso de que la línea funcione en modo ASDP indica por que puerto TCP existe comunicación.
- **XOT active:** Indica si se encuentra activo XOT cuando la línea WAN está funcionando en modo X.25

x) IPSEC

IPSec es una plataforma de seguridad a nivel de *red* que permite acomodar nuevos algoritmos de encriptación y autenticación de forma flexible y robusta.

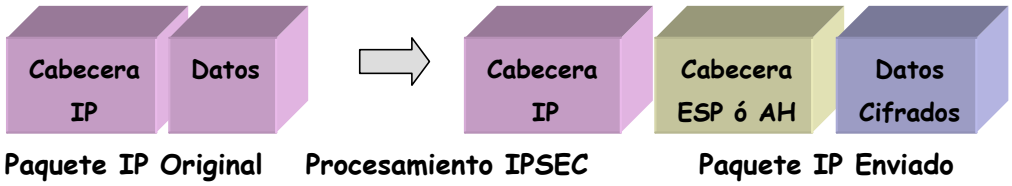
IPSec define dos servicios distintos de seguridad:

- **ESP:** *Encapsulating Security Payload*: Proporciona confidencialidad, autenticación de dirección origen en cada paquete IP, integridad, y protección ante réplicas.
- **AH:** *Authentication Header*: Proporciona autenticación de dirección origen en cada paquete IP, integridad y protección ante réplicas, pero no ofrece confidencialidad de los datos. Este servicio es apropiado en aquellos casos en que tan sólo se necesita asegurar el origen de los datos.

• *Túneles*

La plataforma IPSec permite dos modos de funcionamiento, pudiendo emplear en cada uno de ellos cualquiera de los dos servicios de seguridad ESP o AH:

- **Modo Transporte:** permite una comunicación segura, normalmente establecida entre dos hosts (por ejemplo, la comunicación entre una estación de trabajo y un servidor, o entre dos servidores) pero en ningún caso enmascara la dirección origen y destino del paquete a enviar. En el modo transporte, IPSec sólo actúa sobre los datos internos del paquete IP, sin modificar la cabecera de éste. Por ejemplo, sobre un segmento TCP o UDP, o un paquete ICMP.



- **Modo Túnel:** se encapsula el paquete IP original entero en un nuevo paquete IP, ocultando así todo el contenido original. De esta forma, la información viaja a través de un 'túnel' desde un punto de la red a otro, sin que pueda ser examinado su contenido. Este modo es el más apropiado para utilizarlo en las comunicaciones entre un router y un host externo, o entre dos routers.

Los Router Teldat permiten realizar el **Modo Túnel IPSec**.

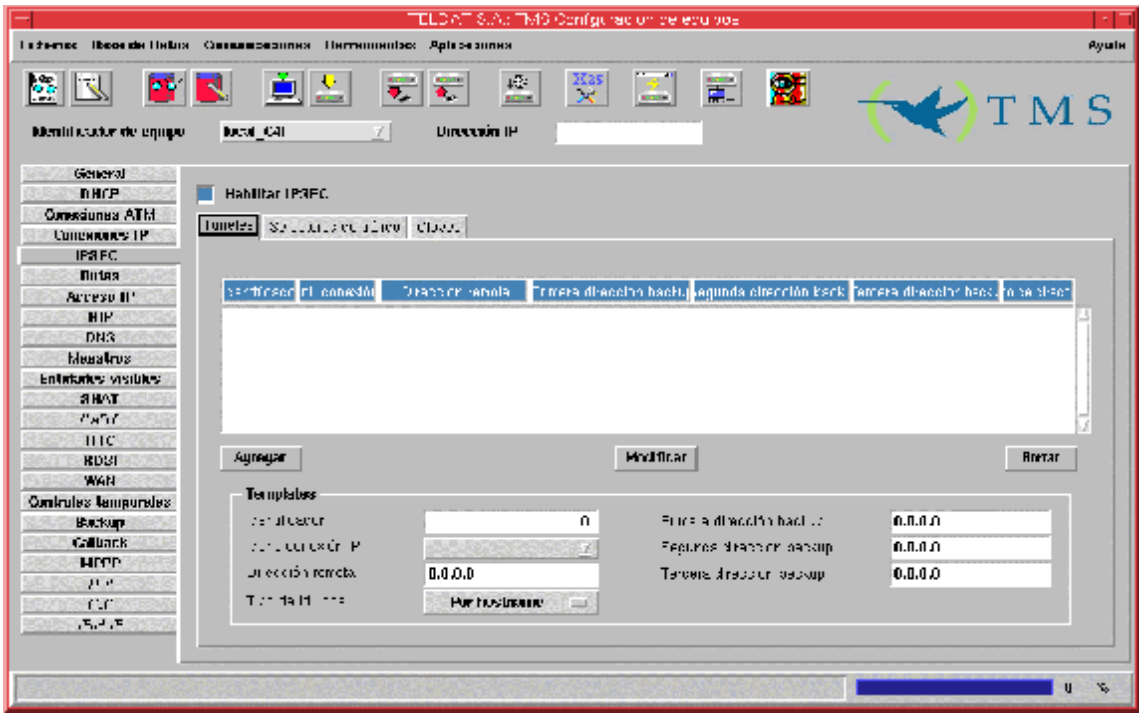


Figura 51 :. Configuración IPSEC Túneles.

- **Identificador:** Identificador del túnel.
- **Identificador conexión IP:** Si se pone a 0 no se define conexión IP.
- **Dirección remota:** dirección IP del equipo remoto con el que se establece el túnel.
- **Tipo de la id. local:** Modo en el que se van a identificar los equipos de los extremos del túnel. Puede ser por el nombre de los equipos o por las direcciones IP de estos.
- **Primera dirección backup:** dirección de otro equipo remoto por si el intento de establecer el túnel con la *Dirección remota* falla.
- **Segunda dirección backup:** dirección de otro equipo remoto por si el intento de establecer el tunel con la *Dirección remota* falla.
- **Tercera dirección backup:** dirección de otro equipo remoto por si el intento de establecer el túnel con la *Dirección remota* falla.

• *Selectores de Tráfico*

La plataforma IPSec necesita saber que *política de seguridad* aplicar al paquete IP, en función de los campos de cabecera, también llamados *selectores*. Las políticas de seguridad deciden qué algoritmos de cifrado y autenticación se han de usar en la conexión segura.

La base de datos de políticas de seguridad o ***Security Policy Database*** (**SPD**) almacena las entradas que contienen selectores de control, y sus políticas de seguridad asociadas.

Tras mirar en la base de datos de políticas de seguridad, dentro de las acciones aplicables a un paquete IP existen 3 posibilidades:

- Descartar el paquete.
- Enrutar el paquete de forma normal.

- Aplicar Seguridad IPSec con unos determinados algoritmos de encriptación o autenticación, que dependerán del compromiso de seguridad-rendimiento que adoptemos. Por ejemplo, si consideramos más importante la velocidad de procesado que la seguridad, elegiremos una política con encriptación DES en lugar de Triple DES.

Un selector es un filtro de paquetes de entrada y salida que se introduce en la lista de control de acceso.

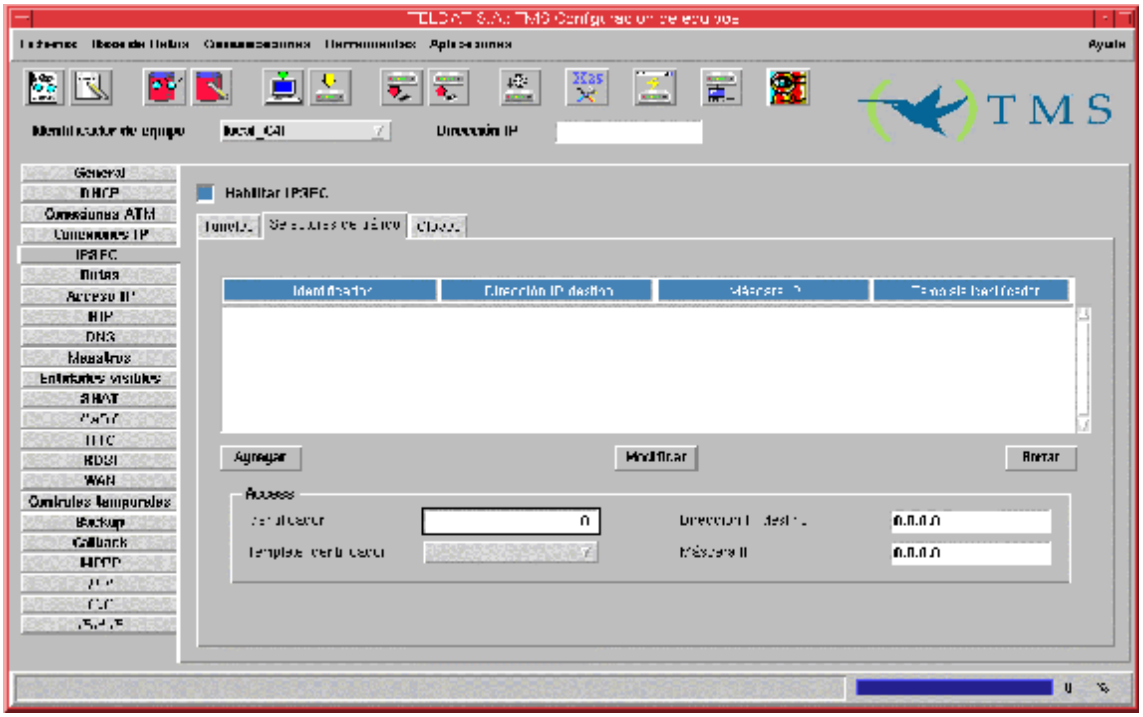


Figura 52 : Configuración IPSEC Selectores de Tráfico

- **Identificador:** Identificador del selector que se está definiendo.
- **Template Identificador:** Identificador del túnel por el que se van a enviar los paquetes.
- **Dirección IP destino:** Identifica la dirección o subred a la que va dirigido el paquete.
- **Máscara IP:** Máscara de la dirección o subred a la que va dirigido el paquete.

Un paquete cuyos selectores coincidan con una de las entradas de la ***SPD*** se procesará de acuerdo con la política asociada a esa entrada. Una *Security Association* es la conexión de seguridad que se crea una vez consultada la ***SPD*** y contiene la información de seguridad (claves de autenticación y encriptación) necesaria para procesar el paquete.

• *Claves*

Toda plataforma de seguridad basada en claves secretas deja de ser segura si las claves no se renuevan cada cierto tiempo.

Cuanto menor sea el periodo de refresco, mayor será la seguridad de nuestro sistema frente a herramientas de Criptoanálisis.

Para la gestión de las claves y parámetros de seguridad en IPSec existen dos modos generales de trabajo posibles: manual (IPSec manual) y automático o dinámico (IPSec IKE). Estos modos hacen referencia a la forma en que se acuerda entre extremos los parámetros de seguridad del túnel a establecer.

La plataforma IPSec permite automatizar este proceso gracias al protocolo *IKE, Internet Key Exchange* (basado en el protocolo de intercambio de claves OAKLEY y la plataforma ISAKMP). Los dos extremos del Túnel negocian automáticamente los parámetros de la comunicación segura (claves, algoritmos de cifrado y autenticación). Para efectuar esta negociación, los extremos antes han de llevar a cabo una **primera fase**, en la que se ponen de acuerdo en los parámetros de seguridad que protegerán la negociación. En esta primera fase además, se lleva a cabo una autenticación de los extremos del túnel, utilizando una clave común (*Pre-shared Key*) introducida manualmente en ambos extremos, utilizando firmas digitales o con un algoritmo de clave pública.

Gracias a este automatismo se pueden renegociar periódicamente los parámetros de seguridad. Para ello, se configura un tiempo de vida a cada SA. Cuando este tiempo expira, una nueva SA se crea con claves de autenticación y encriptación nuevas.

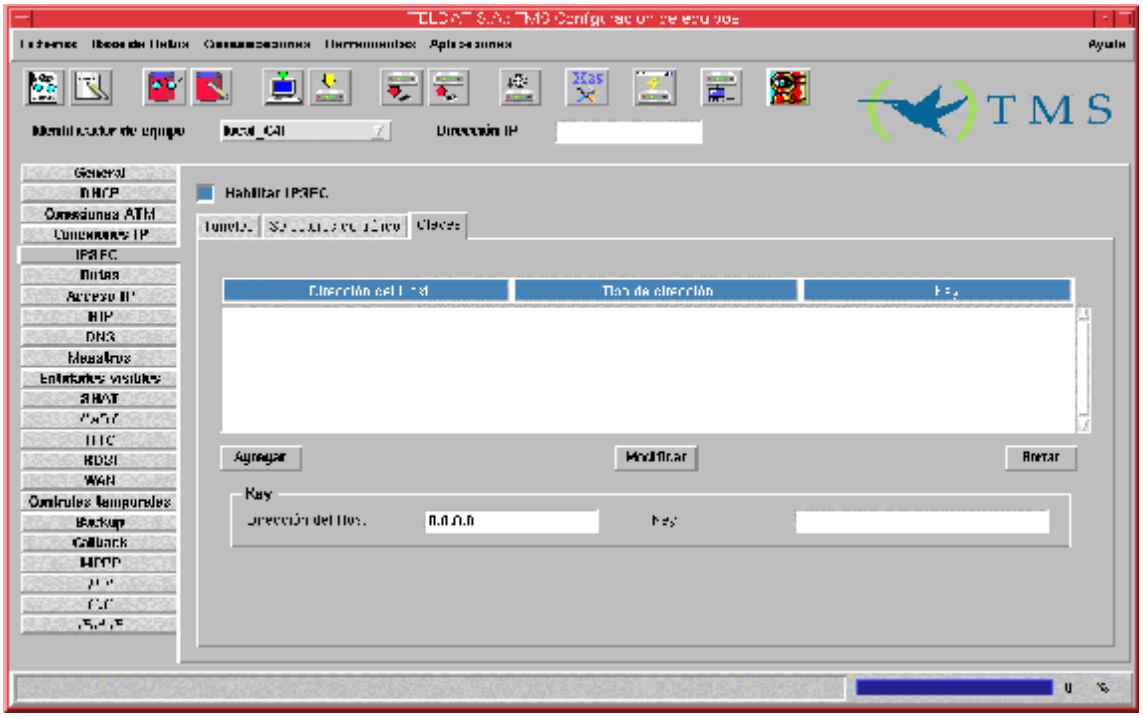


Figura 53 : Configuración IPSEC Claves

- **Dirección del Host:** Dirección IP del Host. Interviene en la autenticación para establecer el túnel.
- **Tipo de dirección:** El tipo de dirección es meramente informativo.
- **Key:** clave para la autenticación al establecer el túnel. Debe ser igual en los equipos extremos del túnel.

1.2. Comandos de ficheros

El conjunto de acciones sobre ficheros que se pueden ejecutar y sus correspondientes significados son los siguientes:

a) Leer configuración de fichero

 El comando de **lectura de configuración** se utiliza para la lectura de la configuración de un equipo desde un fichero. La configuración se lee de un fichero de texto ASCII en el que se encuentran todas las variables que aparecen en la ventana. El fichero deberá tener un formato específico para poder ser interpretado con posterioridad, si bien, la generación de dicho formato la realiza la propia aplicación.

Una vez que se ha seleccionado esta opción, aparece una ventana en la que se puede establecer el nombre del fichero que se desea leer como nueva configuración del equipo que se está editando. La ventana que aparece es la que se muestra a continuación:

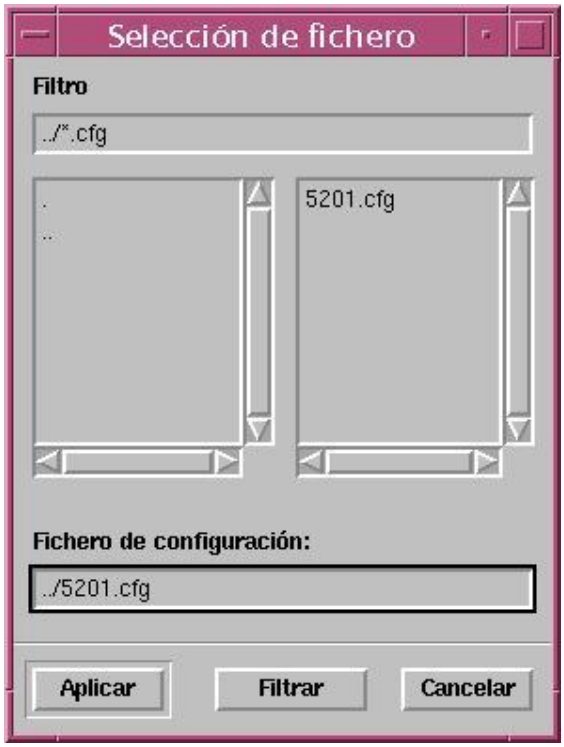


Figura 54 : Ventana de selección de fichero

Elemento	Descripción
Filtro	Es el filtro del tipo de fichero que se desea observar. Por defecto está seleccionado para ver todos los ficheros de configuración del tipo de equipo actualmente seleccionado. Los ficheros de configuración se encuentran situados en el directorio **$TELDATMS/cfgs/$TMSLANG**.

Directorios Se trata de dos listas. La lista de la izquierda contiene los directorios que cuelgan del directorio **$TELDATMS/cfgs/$TMSLANG**. La lista de la derecha contiene todos los ficheros existentes en el directorio para el filtro indicado. Para que sea efectivo el cambio de directorio tras modificar el texto hay que pulsar **Aplicar**.

Fichero de configuración En esta área de texto se escribe o aparece el nombre del fichero desde el cual se desea leer la configuración. Se deben seleccionar ficheros con extensión **cfg** para el caso de los equipos con código 37 y 51, con extensión **C2cfg** para los equipos con código 46, con extensión **C3cfg** para los equipos con código 53 y 59 y con extensión **C3Bcfg** para los equipos con código 60. Si se trata de un equipo con código 51, después de leer correctamente el fichero se interpreta que se trata de un equipo 51, entonces, se lee (de forma transparente al usuario de otro fichero con el mismo nombre y extensión **x25cfg**) la parte específica de XOT, X.25 y Nodo.

Botones Pulsar el botón **Aplicar** para leer la configuración del fichero seleccionado.

Pulsar **Filtrar** para actualizar las listas aplicando el filtro.

Pulsar **Cancelar** para abortar la lectura de configuración.

Los ficheros de configuración sólo se interpretarán correctamente si se leen desde una aplicación que está funcionando con el mismo idioma en que se guardó el fichero.

b) Escribir configuración en fichero

 El comando de **escritura de configuración** se utiliza para guardar la configuración que se muestra en la ventana en un fichero. El fichero quedará almacenado con un formato ASCII.

Al hacer clic sobre el icono, aparecerá una ventana de selección similar a la anterior en la que al rellenar los campos se está estableciendo el nombre del fichero a generar y el directorio en el que se desea almacenarlo.

En los equipos con código 51 la parte específica de configuración XOT, X.25 y Nodo se guarda en otro fichero con el mismo nombre y extensión "x25cfg".

c) Visualizar fichero de log

 Si se lanza este comando aparece una ventana de terminal que permite visualizar en tiempo real el fichero por defecto sobre el que se guarda un histórico de las acciones, avisos y errores de la gestión.

El fichero por defecto es **`$TELDATMS/log/tms.log`**.

1.3. Comandos de Base de Datos

a) *Leer configuración de la base de datos*

 Presenta una ventana de selección de las configuraciones almacenadas en la base de datos para que el usuario escoja la que quiere presentar en las ventanas. Únicamente se presentan las configuraciones almacenadas que se correspondan con el código del equipo actualmente seleccionado. El campo "Identificador de configuración" no permite su modificación más que a través de la selección en la lista.

Las configuraciones se almacenan en una serie de tablas asociadas a las distintas entidades que la componen.

Para más información consultar Tablas utilizadas en la base de datos

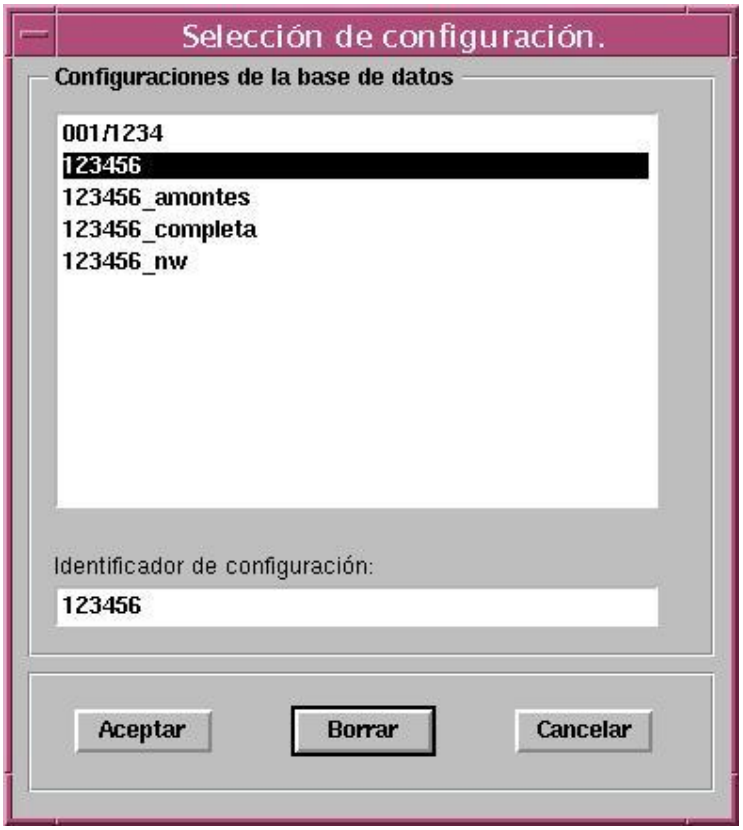


Figura 55 :. Selección de configuración de BD

A medida que se introducen dígitos en la entrada del identificador de configuración la aplicación busca en la lista el equipo que más se aproxima.

b) Guardar configuración de la base de datos

El comando **guardar configuración en la base de datos** se utiliza para escribir configuraciones en la base de datos en las distintas tablas asociadas a las entidades que la componen (véase Tablas utilizadas en la base de datos).

Como en el caso anterior, se presenta la ventana de selección de identificador de configuración. Se puede guardar con uno de los identificadores asociados a alguna de las configuraciones existentes en la base de datos o añadir uno nuevo en el campo de edición.

1.4. Comandos de comunicaciones

Los siguientes comandos establecen comunicación SNMP con el equipo.

a) Pedir configuración al equipo

El comando de **petición de configuración**, pide la configuración al equipo accesible seleccionado en la ventana. Es decir, obtiene los datos relativos a todos los parámetros comentados anteriormente. Para indicar que se está en proceso de comunicación con el equipo, la aplicación presenta como puntero un reloj para indicar que se está trabajando a la vez que se actualiza el indicador de progreso que hay en la parte inferior de la ventana.

La configuración que se obtiene es la de la memoria DRAM del equipo que puede ser distinta de la activa en ese instante (la del arranque almacenada en la memoria FLASH) si el usuario la ha modificado.

Tras recibir la configuración completa se guardan los parámetros de información (número de serie, número de placa, versión de software y versión de BIOS en la base de datos en la tabla **infodevice**.

En el pie de la ventana se muestra información del tiempo que ha tardado la aplicación en traerse la configuración del equipo.

b) Enviar configuración al equipo

El comando de **envío de configuración** toma la configuración de la ventana y la envía a la memoria DRAM del equipo accesible seleccionado en la ventana.

Tras enviar la configuración al equipo se limpia la ventana y se realiza una petición de configuración que sirva de confirmación de entrega.

Durante la operación la aplicación indica que está ocupada mostrando un reloj como puntero y actualizando el indicador de progreso de la parte inferior de la ventana.

Se muestra al pie de la ventana el tiempo invertido en enviar y, a continuación, pedir la configuración al equipo.

c) Sincronización del equipo con la estación de gestión

El comando de **puesta en hora** sirve para sincronizar la fecha y hora del equipo con la estación de gestión. Tras activar el icono aparece una ventana de confirmación:

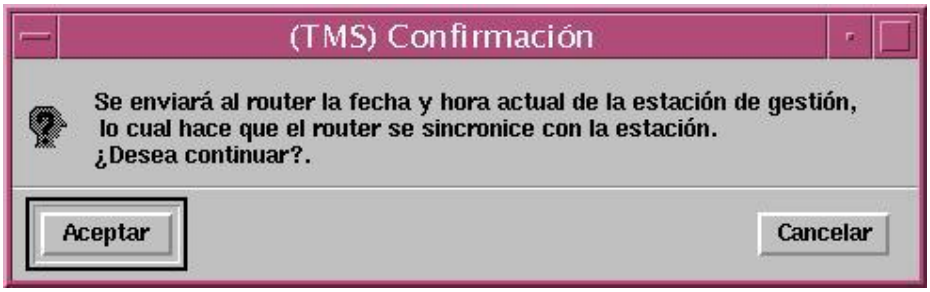


Figura 56 :. Confirmación de sincronización

Seleccione **Aceptar** para confirmar la acción y **Cancelar** si desea abortarla.

d) Salvar a memoria FLASH la configuración en el equipo

El comando **guardar configuración** almacena la configuración almacenada en la memoria DRAM (volátil) del equipo en su memoria FLASH (permanente). Tras este comando la configuración está almacenada de forma permanente pero aún no es la activa en el equipo. Pasará a activarse en el momento que el equipo se rearranque o se reconfigure con el comando que se describe a continuación.

e) Reiniciar el equipo con su configuración en memoria FLASH

El comando **reconfigurar** hace que el equipo lea la configuración de su memoria FLASH (permanente) y la deposite en su memoria DRAM (volátil) convirtiéndola en activa.

> ***Nota: La reconfiguración supone la pérdida de conexión con el equipo hasta que el maestro vuelva a contactar con él tras su reactivación.***

f) Telecargar software al equipo

El comando **telecarga de software** se utiliza para enviar el programa que se ejecuta en el equipo. El Centro de Gestión puede actualizar así el software del equipo con nuevas versiones. Cuando se selecciona el comando de telecarga, se abre la ventana que aparece a continuación:

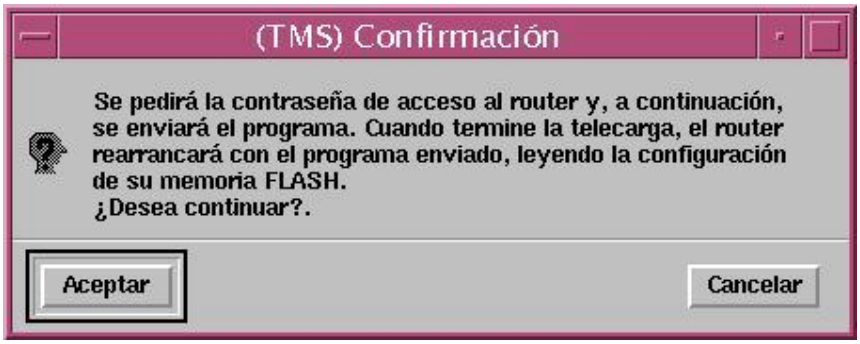


Figura 57 :. Confirmación de telecarga de software

Se trata de una ventana de confirmación en la que se explican las consecuencias del comando. Una vez confirmada, aparecerá la ventana de **selección de fichero** para escoger el programa que se desea telecargar.

El fichero por defecto que se utiliza para los equipos con código 37 y 51 suele ser **cbra<version>.x** aunque puede ser cualquiera que contenga el código necesario para el funcionamiento correcto del equipo. En los equipos con código 46 el fichero por defecto que se utiliza suele ser **teldatc.bin**.

Una vez finalizada la telecarga, se rearranca el equipo con el nuevo software y la configuración de su memoria FLASH, por eso, hasta que el router maestro no vuelve a gestionar el equipo que se ha telecargado, éste aparecerá como inaccesible.

La operación de telecarga deja información de su progreso en el fichero **`$TELDATMS/log/telecarga_usr_<id_equipo>.log`**.

Cuando se llama desde operaciones sobre grupos la telecarga de cada equipo deja su progreso en el fichero **`$TELDATMS/log/telecarga_<id_equipo>.log`** (en ambos casos <id_equipo> es el identificador del equipo, actualmente su número de teléfono, en la base de datos).

¡ATENCIÓN!

Es muy importante no interrumpir la telecarga durante su ejecución pues dejaría el equipo totalmente inaccesible de forma remota. En el caso en el que se produzca esta situación, se deberá entrar al equipo por consola (localmente).

¡EVITE PULSAR CTRL-C DURANTE LA TELECARGA!

Así mismo, es responsabilidad del operador el enviar un fichero válido, puesto que la aplicación no realiza comprobaciones relativas al contenido del fichero.

Los equipos TMS está protegidos frente a telecargas simultáneas impidiendo nuevas conexiones FTP cuando hay una establecida.

2. Monitorización

Los equipos TMS dispone de la capacidad de almacenar dos tipos principales de estadísticos que a partir de ahora denominaremos quincenales y diarios. Además los router Teldat C3 y Teldat C3B almacenan estadísticos relacionados con las transacciones de los TPV que se ha realizado ha través de él.

Los **estadísticos quincenales** son valores que el equipo almacena en memoria RAM con baterías y que, por tanto, permanecen aunque el equipo se apague o se reconfigure. Están orientados a proporcionar al cliente datos históricos de sus conexiones.

Los **estadísticos diarios**, por el contrario, son valores almacenados desde el último arranque del equipo y se almacenan en memoria RAM volátil por lo que se pierden cuando se resetea el equipo. Su propósito es ayudar a resolver problemas de configuración del equipo.

La aplicación **tmsmon** solicita, vía SNMP, los estadísticos diarios y quincenales almacenados en los equipos NOVACOM y Teldat C. Consulta periódicamente la base de datos para comprobar el estado de los equipos y permite seleccionar como destino de las peticiones cualquiera de los que están accesibles. Para poner un equipo en gestión y que obtenga el estado ACCESIBLE se utiliza la aplicación **tmsmanager** que puede lanzarse desde la opción **Aplicaciones->Gestión** del menú principal.

No obstante, también es posible la obtención de los estadísticos diarios y quincenales asociados a un equipo sin necesidad de acceder a través de la aplicación **tmsmanager**. Para ello se debe invocar monitorización de la siguiente manera:

```
>tmsmon [-h] [-i <ipadd>]  [-c <comunidad>] [-id <id_equipo>] [-t <período de refresco
en segundos>]
```

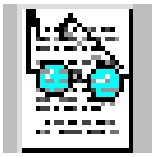
El parámetro -h presenta el formato de invocación de la aplicación.

2.1. Descripción de la ventana principal

La barra de herramientas que hay en la parte superior de la ventana contiene los siguientes botones:

a) Comandos de ficheros

- ***Leer estadísticos de ficheros***



Este comando se utiliza para leer los estadísticos almacenados en tres ficheros de texto (estadísticos quincenales del interfaz WAN, direcciones más visitadas y tráfico por estación) con un determinado formato. Para más información del formato de los ficheros consultar Formato de los ficheros de estadísticos quincenales

Además en los router C3 y C3B se utiliza para leer los estadísticos almacenados sobre las transacciones realizadas por los TPV. Para más información del formato de los ficheros consultar Formato de los ficheros de transacciones

Una vez que se ha seleccionado esta opción, aparece una ventana en la que se puede establecer el nombre del fichero que se desea leer como nueva configuración del equipo que se está editando. La ventana que aparece es la que se muestra a continuación:

Figura 58 :. Ventana de selección de fichero

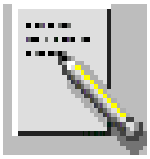
Elemento	Descripción
Filtro	Es el filtro del tipo de fichero que se desea observar. Por defecto está seleccionado para ver todos los ficheros de estadísticos quincenales del interfaz WAN (*.wan). Los ficheros de estadísticos quincenales (y de transacciones en el caso de los Teldat C3 y Teldat C3B) se encuentran situados en el directorio **$TELDATMS/accounts/$TMSLANG**.
Directorios	Se trata de dos listas. La lista de la izquierda contiene los directorios que cuelgan del directorio **$TELDATMS/accounts/$TMSLANG**. La lista de la derecha contiene todos los ficheros existentes en el directorio para el filtro indicado. Para que sea efectivo el cambio de directorio tras modificar el texto hay que pulsar **Aplicar**.
Fichero de estadísticos	En esta área de texto se escribe o aparece el nombre del fichero desde el cual se desea leer los estadísticos. Se deben seleccionar ficheros con extensión **wan**.
Botones	Pulsar el botón **Aplicar** para leer la configuración del fichero seleccionado.

Pulsar **Filtrar** para actualizar las listas aplicando el filtro.

Pulsar **Cancelar** para abortar la lectura de configuración.

Los ficheros de estadísticos sólo se interpretarán correctamente si se leen desde una aplicación que está funcionando con el mismo idioma en que se guardó el fichero.

- ***Escribir estadísticos en fichero***

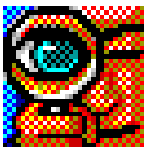


Se utiliza para guardar los estadísticos quincenales (y transacciones en el caso de los router Teldat C3x) que se muestran en la ventana en ficheros.

Para más información acerca del formato de los ficheros consultar Formato de los ficheros de estadísticos quincenales y/o Formato de los ficheros de transacciones

Al hacer clic sobre el icono, aparecerá una ventana de selección similar a la anterior en la que al rellenar los campos se está estableciendo el nombre del fichero a generar y el directorio en el que se desea almacenarlo.

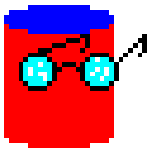
b) Visualizar fichero de log



Si se lanza este comando aparece una ventana de terminal que permite visualizar en tiempo real el fichero por defecto sobre el que se guarda un histórico de las acciones, avisos y errores de la gestión. El fichero por defecto es **`$TELDATMS/log/tms.log`**.

c) Comandos de Base de Datos

- ***Leer estadísticos de la base de datos***



Presenta una ventana de selección de los estadísticos almacenados en la base de datos para que el usuario escoja la que quiere presentar en las ventanas. El campo "Identificador de estadísticos" no permite su modificación más que a través de la selección en la lista.

Los estadísticos se almacenan en una serie de tablas asociadas a las distintas entidades que la componen.

Para más información consultar Tablas utilizadas en la base de datos

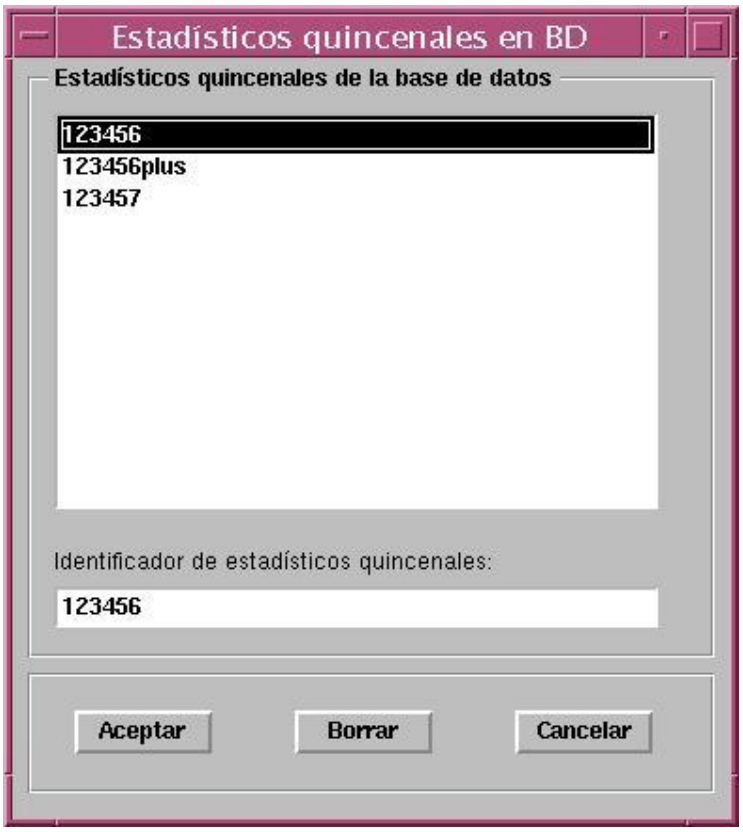


Figura 59 : Selección de estadísticos quincenales en BD

A medida que se introducen caracteres en la entrada del identificador de estadísticos la aplicación busca el identificador que más se aproxima.

- ***Guardar estadísticos en la base de datos***

Se utiliza para escribir los estadísticos quincenales (y transacciones en el caso de los router Teldat C3x) de la ventana en la base de datos en las distintas tablas asociadas a las entidades que la componen (véase Tablas utilizadas en la base de datos).

Como en el caso anterior, se presenta la ventana de selección de identificador de estadísticos. Se puede guardar con uno de los identificadores asociados a alguna de las configuraciones existentes en la base de datos o añadir uno nuevo en el campo de edición.

d) Comandos de comunicaciones

• *Pedir estadísticos al equipo*

 Se piden al equipo los estadísticos de la solapa actualmente seleccionada y se presentan en la ventana.

• *Borrar los estadísticos del equipo.*

 Si se pulsa este botón aparecerá un mensaje de confirmación que si el usuario acepta provocará el envío al equipo de una orden para que borre definitivamente sus estadísticos quincenales (o transacciones en el caso de los router Teldat C3 y Teldat C3B) almacenados.

Si en la petición de estadísticos al equipo aparecen valores inconsistentes se recomienda borrar los estadísticos y volver a pedir.

Pudiera darse el caso que tras una actualización del software del equipo los estadísticos comenzarán a guardarse de forma errónea, aunque son situaciones aisladas.

Los **Botones** que aparecen en la parte inferior de la ventana son tres:

Cerrar: Este botón se utiliza para cerrar la aplicación de monitorización.

Actualizar: Al pulsar este botón se monitorizan los parámetros de la solapa seleccionada. Esta acción es equivalente a pulsar sobre el icono que se encuentra en la esquina superior derecha de la ventana 

Ayuda: Tal y como su nombre indica, el botón de ayuda permite acceder a la ayuda desde la ventana de Monitorización.

Además de los botones comentados, en la parte superior de la ventana existe una barra de menú desde la que se pueden realizar todas las acciones referentes a los botones así como otras que se comentan a continuación:

Fichero: Desde este menú se pueden realizar las siguientes opciones:

Leer Fichero:

Lee los estadísticos de ficheros como se explicó más arriba.

Salvar a fichero:

Guarda los estadísticos a fichero como se comentó más arriba.

Salir:

Esta opción del menú equivale a la selección del botón de Cerrar descrito anteriormente.

Base de Datos:

Leer de base de datos:

Lee los estadísticos de la base de datos como se explicó en el apartado anterior.

Guardar en base de datos:

Guarda los estadísticos en la base de datos.

Aplicaciones: **Gestión:**

Lanza la aplicación de gestión.

Configuración:

Lanza la aplicación de configuración.

Estado de la recogida automática:

Lanza la aplicación de monitorización de la recogida automática de estadísticos quincenales.

Operaciones sobre grupos:

Lanza la aplicación de gestión de operaciones sobre grupos.

Comunicaciones:

Desde este menú se pueden pedir los estadísticos al router y borrar sus estadísticos quincenales (o transacciones en caso de los router Teldat C3x) como se explicó en los botones de la barra de herramientas.

2.2. Monitorización Diaria

La monitorización diaria permite la visualización de los estadísticos que el equipo ha almacenado desde su última reconfiguración. Dependiendo del tipo de equipo, los datos a presentar son diferentes.

a) RDSI

- ***Parámetros globales***

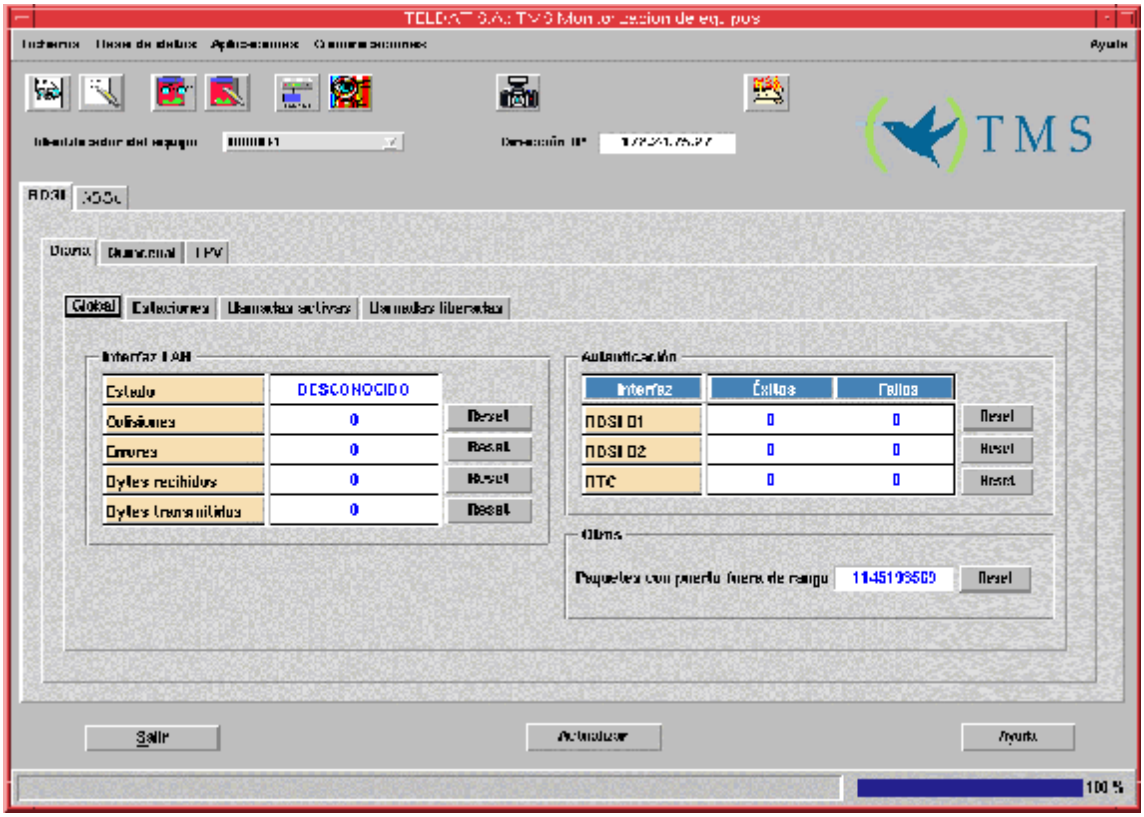


Figura 60 : Monitorización diaria de parámetros globales RDSI

En esta ventana se pueden monitorizar los siguientes parámetros:

- **Interfaz LAN**
  - **Estado:** Puede tomar uno de estos valores: ACTIVO, CAIDO o EN TEST.
  - **Colisiones:** Número de tramas no transmitidas por excesivas colisiones.
  - **Errores:** Número de errores en el interfaz LAN.
  - **Bytes transmitidos:** Número de octetos provenientes de las conexiones de los canales B1 y B2 y transmitidos a la LAN.
  - **Bytes recibidos:** Número de octetos provenientes de la LAN con destino el propio equipo o las conexiones de los canales B1 o B2.
- **Autenticación para cada canal B RDSI (equipos 37 , 51 y 60) y RTC (sólo equipos 37).**
  - **Éxitos:** Número de veces que se estableció con éxito la fase de autenticación a nivel del protocolo PPP.
  - **Fallos:** Número de veces que se falló la fase de autenticación PPP.
- **Otros**
  - **Paquetes con puerto fuera de rango:** Número de paquetes no procesados por tener un puerto fuera de rango. Son paquetes recibidos de la WAN con un puerto destino que no se corresponde con ninguna entrada NAT. Son paquetes entrantes que, bien no tuvieron paquete saliente asociado, bien lo tuvieron pero la entrada NAT correspondiente caducó.

Los contadores que tienen a su derecha el botón **Reset** pueden ponerse a 0 con sólo pulsarlo.

Reset de Errores:

Si se pone a 0 el contador de errores también se pone a 0 el de colisiones.

Reset de contador de autenticación:

Cuando se pulsa se ponen a cero los éxitos y los fallos.

• Estaciones que provocaron llamada

Además, la monitorización diaria permite visualizar las 20 últimas estaciones que provocaron una llamada mostrándose para cada una de ellas tanto su **Dirección IP** como la **Fecha y la Hora** en la que se realizó la llamada. La presentación de la fecha sólo ocurre cuando el equipo tiene una versión de software 5.1 o superior, en caso contrario sólo se presenta la hora de inicio de la conexión.

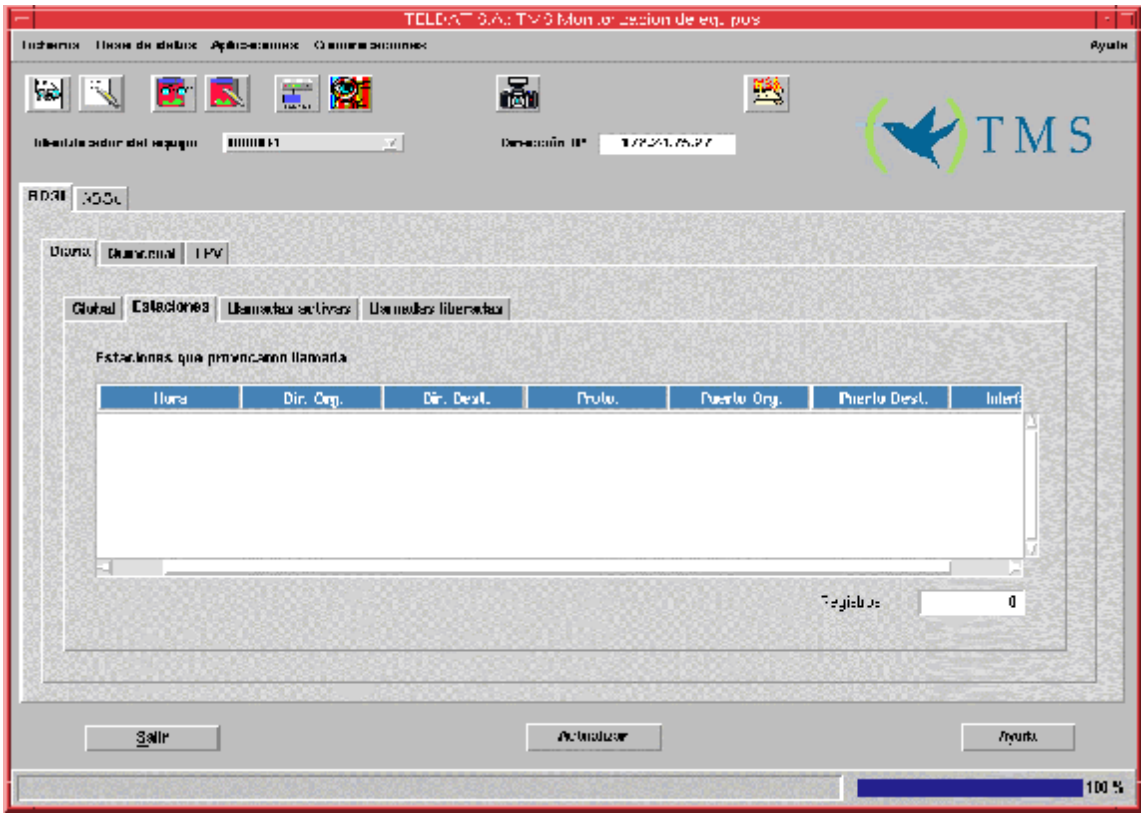


Figura 61 : Monitorización diaria de estaciones que provocaron llamada

> ***Tráfico DNS:***
>
> ***En versiones de software del equipo anteriores a la 5.1 el tráfico DNS generado por las estaciones se asignaba a la dirección IP del propio equipo. A partir de dicha versión se asigna a la estación que lo originó.***

- ***Llamadas activas***

Las llamadas RDSI activas del sistema disponen de un conjunto de variables para aportar información concreta de la llamada.

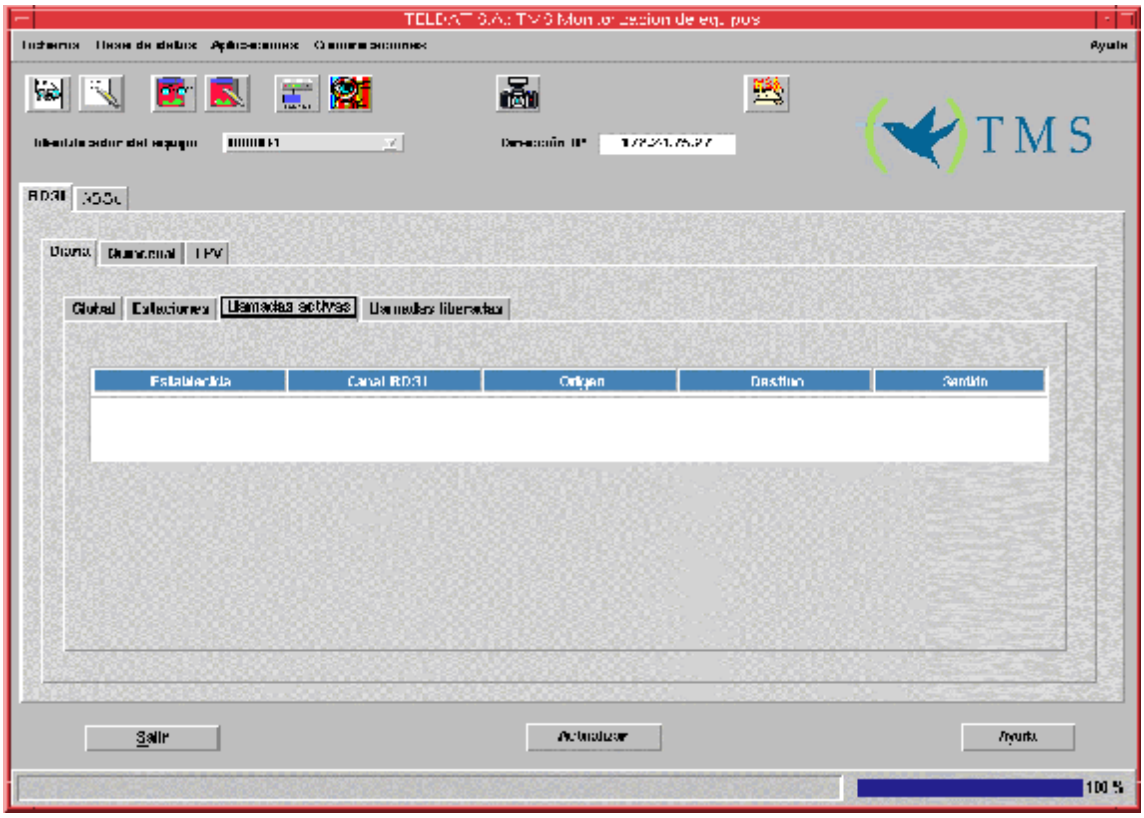


Figura 62 : Monitorización diaria de llamadas activas

El conjunto de parámetros que se observan son los siguientes:

- **Establecida:** Instante en el que se estableció la llamada.
- **Canal RDSI:** En el caso de las llamadas RDSI activas, indica el canal (B1ó B2) a través del cual está establecida la llamada.
- **Origen:** Número llamante.
- **Destino:** Cuando la llamada es **Saliente**, indica el número del interlocutor.
- **Sentido:** Puede tomar dos valores: **Saliente**, que indica que fue el equipo el que hizo la llamada, o **Entrante**, que indica que el equipo respondió a la llamada.

• *Llamadas liberadas*

En esta ventana se visualizan las tentativas de llamadas y las establecidas en el equipo desde que se reconfiguró por última vez.

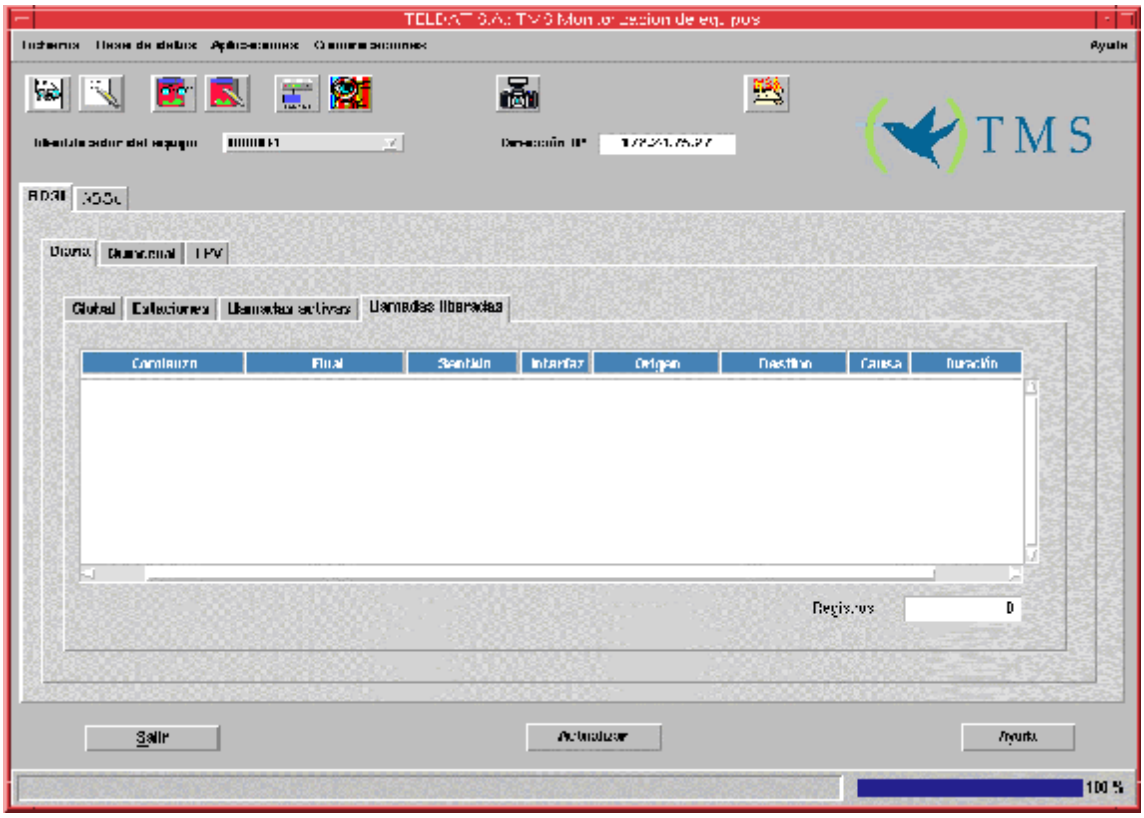


Figura 63 : Monitorización diaria de llamadas liberadas

Se pueden consultar los siguientes campos:

- **Comienzo:** Fecha y hora de inicio de la llamada.
- **Final:** Fecha y hora de liberación de la llamada.
- **Sentido:** Puede tomar dos valores: **Saliente**, que indica que fue el equipo el que hizo la llamada, o **Entrante**, que indica que el equipo respondió a la llamada.
- **Interfaz:** Canal B RDSI por el que se estableció la llamada.
- **Origen:** Numero llamante.
- **Destino:** Número RDSI interlocutor del equipo.
- **Causa:** Es una indicación de la causa por la que se liberó la última llamada proporcionada por la red RDSI según la norma Q931 de ISO. Hay una lista de las causas en el apartado Causas de liberación RDSI.
- **Duración:** Duración en horas minutos y segundos de la llamada.

b) ADSL

• *Parámetros globales*

La siguiente ventana muestra los parámetros globales de monitorización diaria.

Los contadores que tienen un botón "0" pueden ponerse a 0 cuando se pulsa dicho botón.

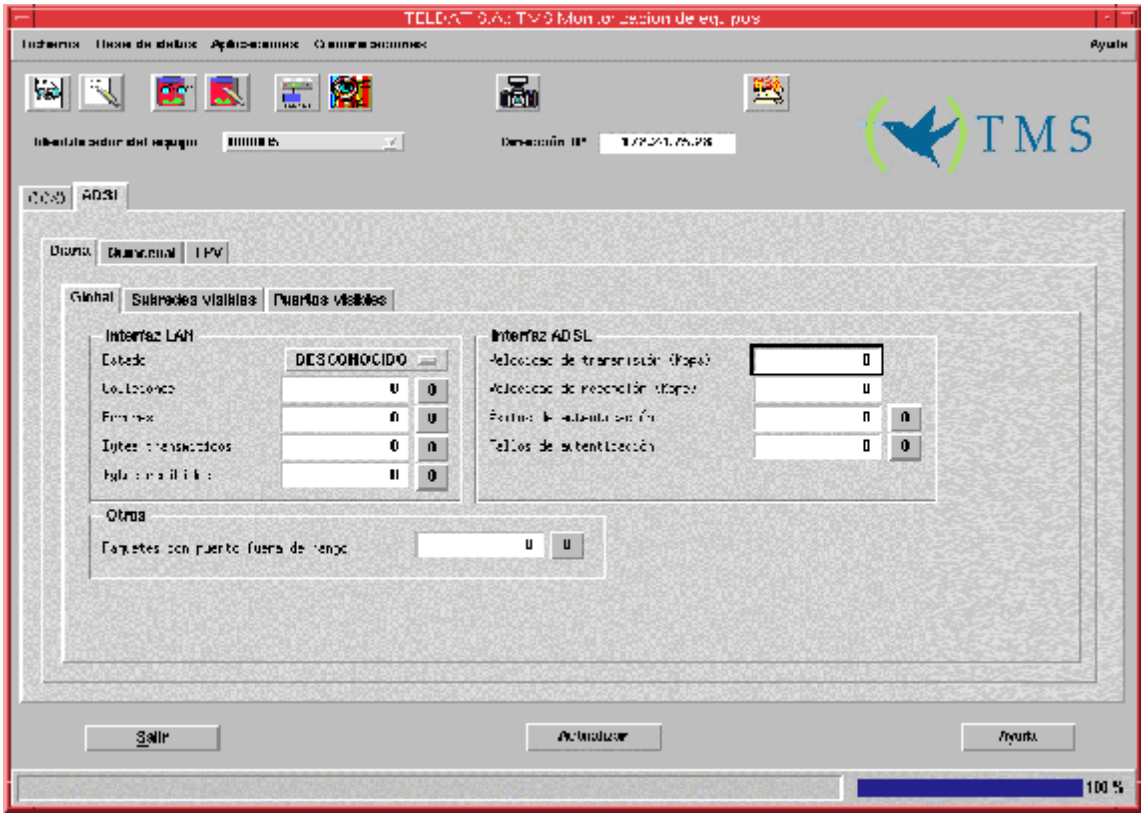


Figura 64 : Monitorización diaria de parámetros globales ADSL

La lista de variables de la MIB SNMP que se monitorizan es la siguiente:

Interfaz LAN

- **Estado:** Puede tomar los siguientes valores: **DESCONOCIDO**, **ACTIVO**, **CAIDO** o **EN TEST**.
- **Colisiones:** Número de tramas no transmitidas por excesivas colisiones. Cuando se pone a cero si no hay otros errores en el interfaz LAN también se resetea el contador de errores.
- **Errores:** Número de errores en el interfaz LAN. Se incluyen las colisiones por ello, cuando se pone a 0, también se resetea el contador de colisiones.
- **Bytes recibidos:** Número de bytes recibidos en el router provenientes de la LAN.
- **Bytes transmitidos:** Número de bytes transmitidos por el router hacia la LAN.

Otros

- **Paquetes con puerto fuera de rango:** Número de paquetes no procesados por tener un puerto fuera de rango. Son paquetes recibidos de la WAN con un puerto destino que no corresponde con ninguna entrada NAT. Son paquetes entrantes que, bien no tuvieron paquete saliente asociado o bien lo tuvieron pero la entrada NAT correspondiente caducó.

Interfaz ADSL

- **Velocidad de transmisión [Kbps]:** Es la velocidad real a la que está transmitiendo el interfaz ADSL. Puede no coincidir con la configurada en el router.
- **Velocidad de recepción [Kbps]:** Es la velocidad real a la que está recibiendo el interfaz ADSL del router. Puede no coincidir con la configurada.

- **Éxitos de autenticación:** Número de veces que se establece la fase de autenticación del protocolo PPP en el interfaz ADSL.
- **Fallos de autenticación:** Número de veces que no se establece la fase de autenticación del protocolo PPP en el interfaz ADSL.

• *Subredes visibles*

Se muestran las estadísticas de acceso a las subredes visibles configuradas en el router.

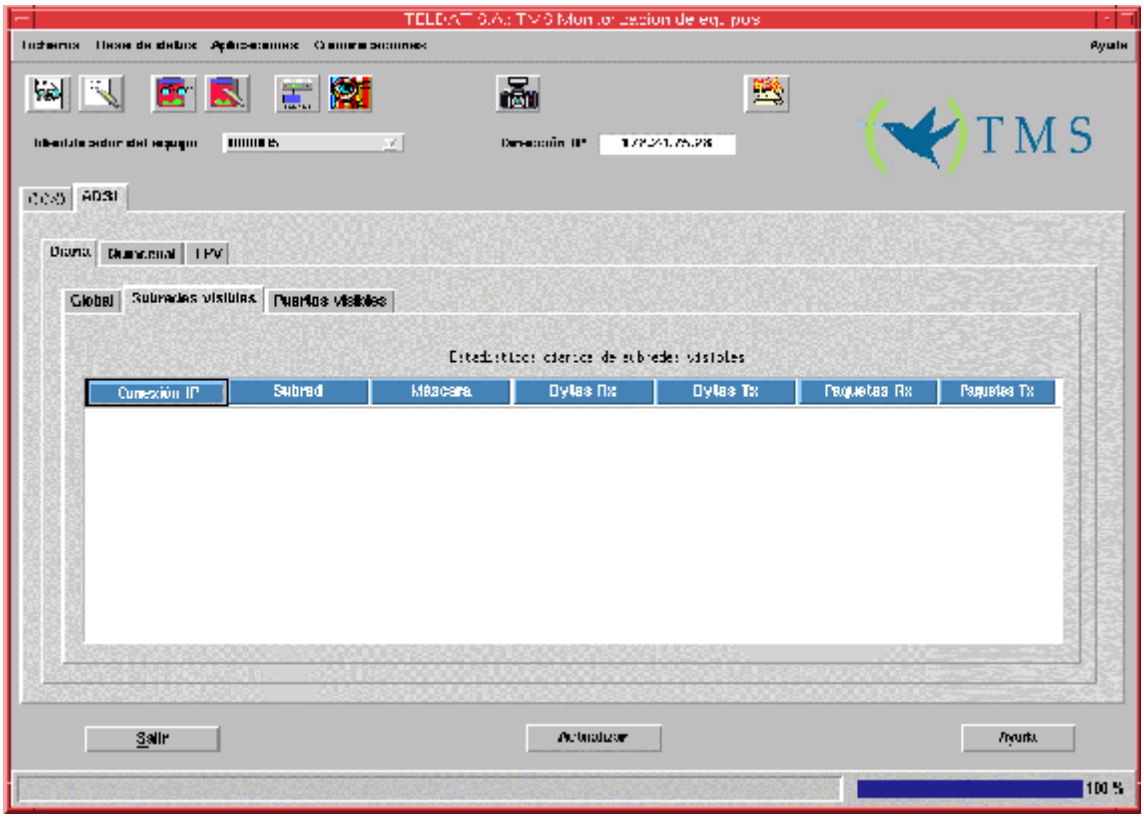


Figura 65 : Monitorización diaria de subredes visibles

- **Conexión IP:** Identificador de conexión IP a través del que la subred se hace visible al exterior.
- **Subred:** Dirección IP de la subred visible.
- **Máscara:** Máscara IP de la subred visible.
- **Bytes Rx:** Bytes que han atravesado el router en dirección a la subred visible.
- **Bytes Tx:** Bytes que han atravesado el router remitidos por la subred visible.
- **Paquetes Rx:** Paquetes que han atravesado el router en dirección a la subred visible.
- **Paquetes Tx:** Paquetes que han atravesado el router remitidos por la subred visible.

• *Puertos visibles*

En esta lista se muestran estadísticos de acceso a puertos visibles.

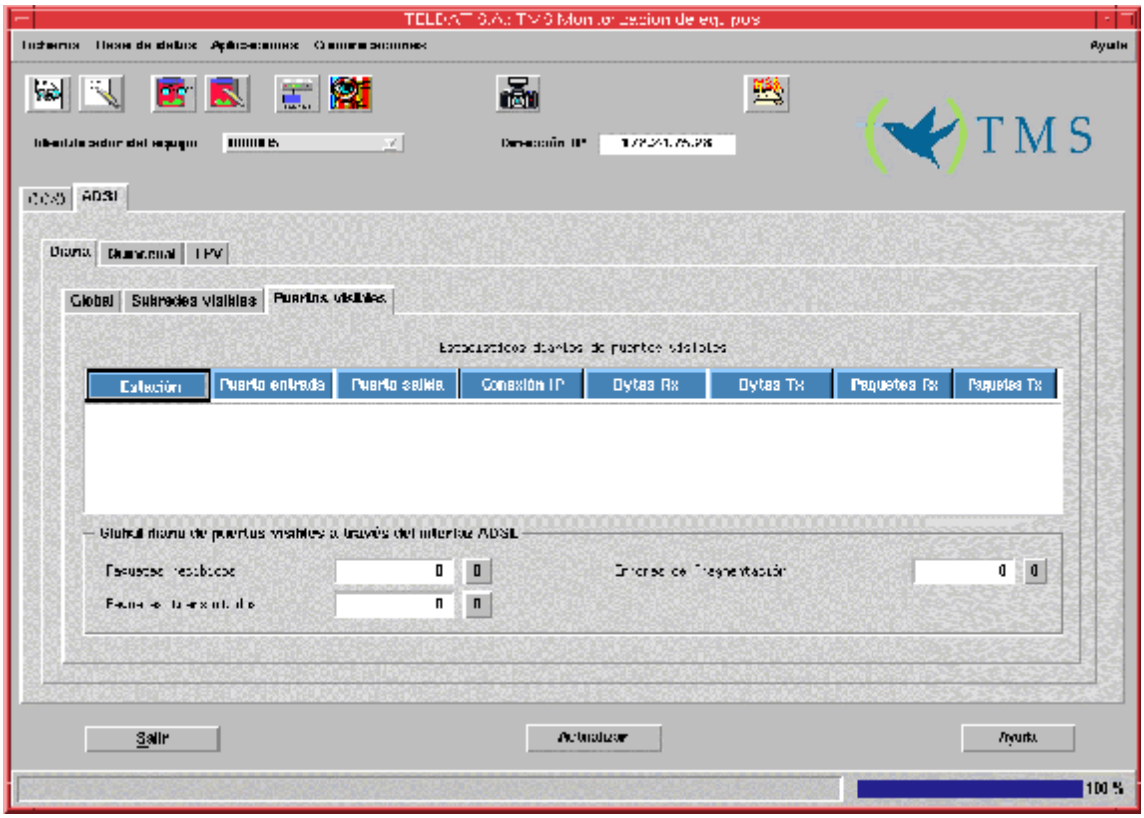


Figura 66 : Monitorización diaria de puertos visibles

En la parte inferior de la ventana se muestran parámetros de acceso globales al conjunto de puertos visibles:

- **Paquetes recibidos:** Total de paquetes enviados desde los puertos visibles.
- **Paquetes transmitidos:** Total de paquetes enviados desde los puertos visibles.
- **Errores de fragmentación:** Número total de paquetes recibidos en el router indicándole que el paquete que ha enviado necesita fragmentación y no tiene activado el bit de fragmentación. El paquete que produce este error se descarta.

Los campos de la lista de monitorización individual de puertos visibles son:

- **Estación:** Estación de la LAN que posee el puerto visible.
- **Puerto interno:** Puerto de la estación que es visible.
- **Puerto externo:** El puerto anterior se sustituye por este cuando se realiza NAT de puertos NAPT).
- **Conexión IP:** Conexión IP a través de la que el puerto es visible.
- **Bytes Rx:** Bytes que han atravesado el router con destino algún puerto visible.
- **Bytes Tx:** Bytes que han atravesado el router remitidos por un puerto visible.
- **Paquetes Rx:** Paquetes que han atravesado el router en dirección a uno de los puertos visibles.
- **Paquetes Tx:** Paquetes que han atravesado el router remitidos por un puerto visible.

2.3. Monitorización Quincenal

En la monitorización quincenal se presentan los estadísticos almacenados en el equipo en los últimos 15 días. Para refrescar la ventana es necesario situarse en la carpeta de monitorización quincenal y pulsar **Actualizar** o el icono de la esquina superior derecha de la ventana. Cada vez que se solicitan los estadísticos quincenales al equipo se almacenan automáticamente en los ficheros de estadísticos del directorio **`$TELDATMS/acounts/$TMSLANG`**. Dependiendo del tipo de equipo, los datos a presentar son diferentes.

a) RDSI

- ***Estadísticos globales de los últimos 15 días***

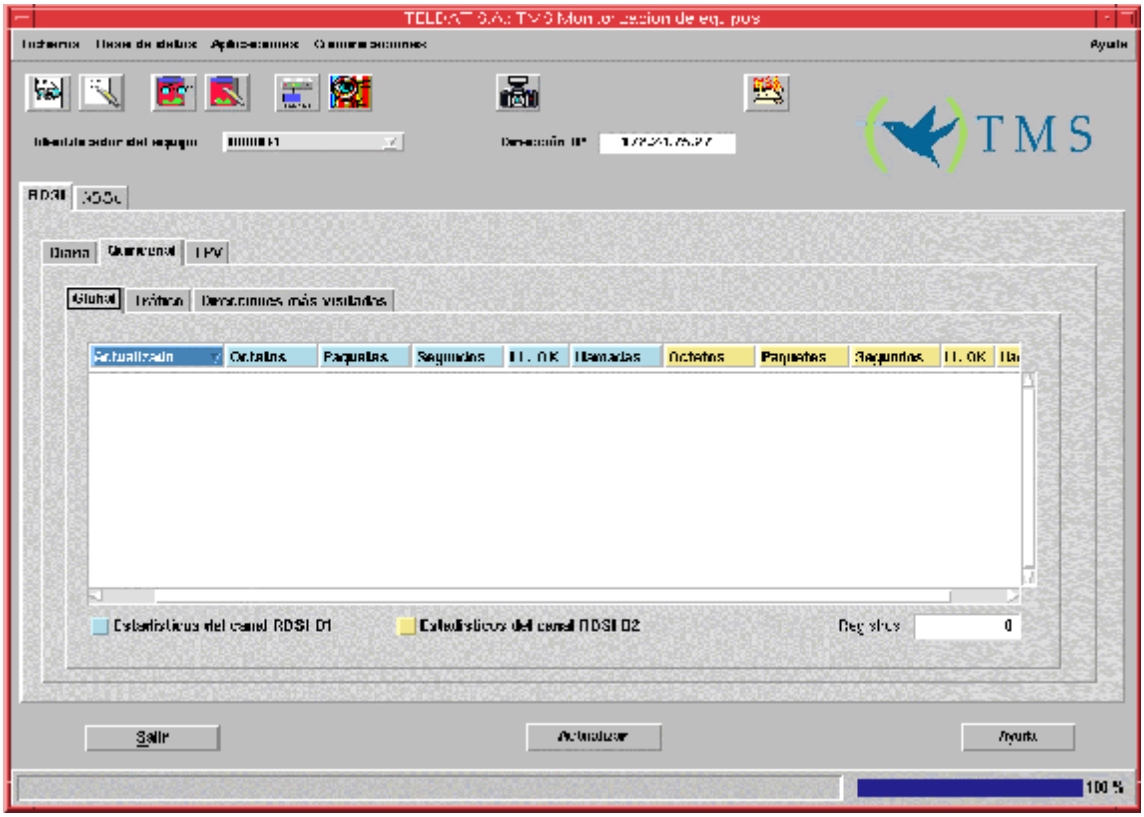


Figura 67 : Monitorización quincenal de parámetros globales RDSI

Cada línea muestra los datos de un día. Los valores corresponden al intervalo transcurrido desde la fecha y hora de la línea anterior hasta la fecha y hora de la línea en curso.

Se muestran los siguientes campos para cada canal B RDSI:

- **Actualizado:** Fecha y hora en la que se almacenaron en el equipo.
- **Octetos:** Octetos enviados y recibidos a través del equipo.
- **Paquetes:** Paquetes enviados y recibidos a través del equipo.
- **Segundos:** Tiempo total de conexión.

- **Llamadas OK:** Número total de llamadas que lograron establecer conexión a nivel del protocolo PPP sobre RDSI con éxito.
- **Llamadas totales:** Número total de llamadas generadas en un día dado. La conexión RDSI se establece en todas pero es posible que la comunicación no progrese. Algunas pueden haber sido rechazadas por un fallo de autenticación o por un fallo en la negociación de parámetros del protocolo PPP sobre RDSI. Si no llega a establecerse la conexión RDSI no se incrementa este contador.

En ninguno de los parámetros anteriores se incluyen los estadísticos de las llamadas de gestión para que no se le tarifiquen al cliente.

- ***Tráfico por estación***

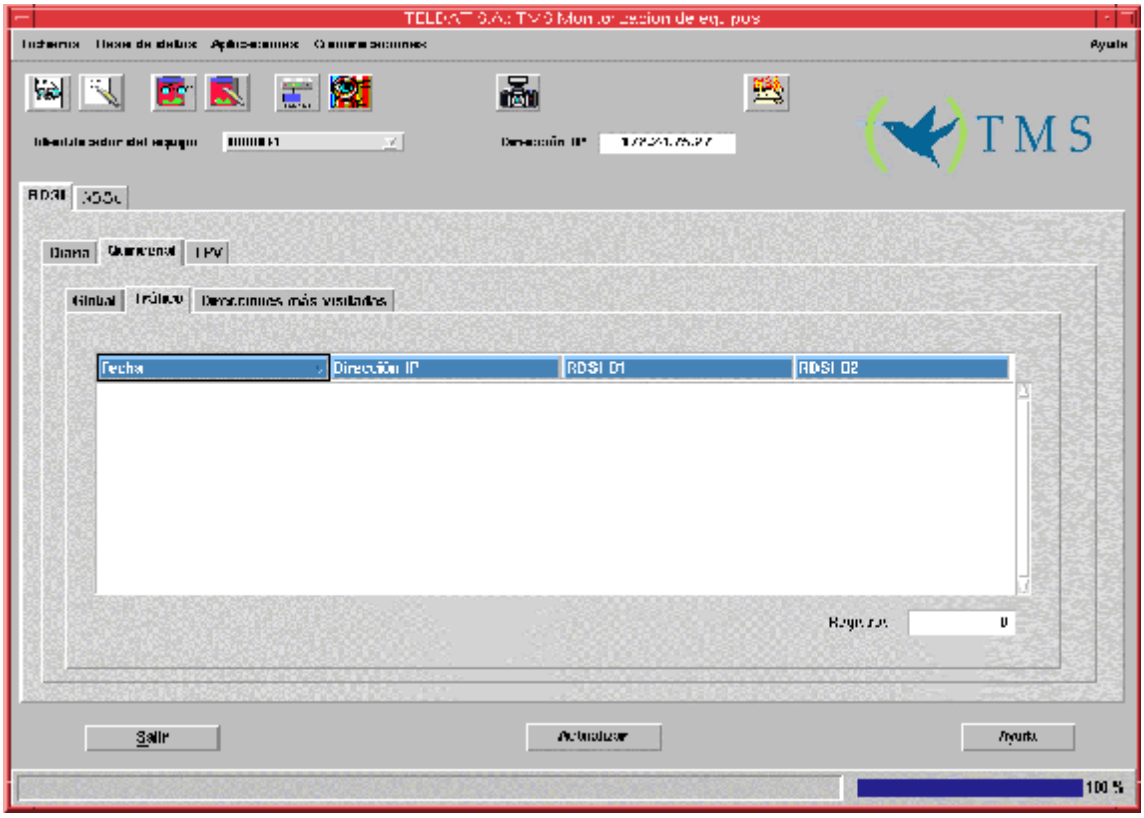


Figura 68 : Monitorización quincenal de tráfico por estación RDSI

La segunda área, tráfico por estación, viene representado por un conjunto de valores que nos dan información acerca de las conexiones realizadas por una determinada estación. Así, los parámetros utilizados para representar el tráfico son los siguientes:

- **Fecha:** Fecha en la que la estación se conectó.
- **Dirección IP:** Dirección IP de la estación.
- **RDSI B1:** Paquetes cursados a través del canal B1 RDSI.
- **RDSI B2:** Paquetes cursados a través del canal B2 RDSI.

- ***Direcciones más visitadas***

Esta lista contiene las direcciones visitadas en los últimos 15 días, para las 256 primeras direcciones visitadas, tanto por B1 como por B2. El tráfico de las llamadas de gestión no se anota.

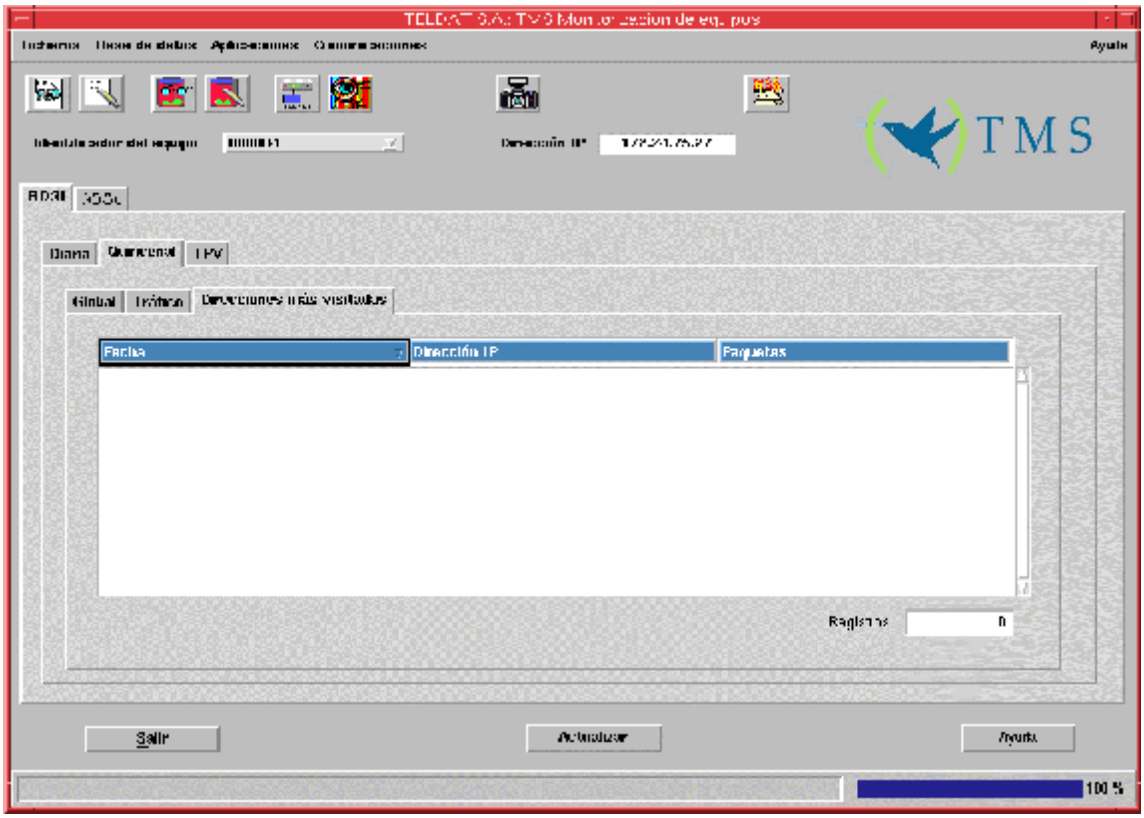


Figura 69 : Monitorización quincenal de direcciones más visitadas RDSI

- **Fecha:** Representa el día en el que se realizó una conexión.
- **Dirección IP:** Dirección IP con la que se estableció la conexión.
- **Paquetes:** Tráfico total (paquetes) cursado.

b) ADSL

- ***Estadísticos globales de los últimos 15 días***

En esta ventana se muestran los parámetros globales de tráfico que el equipo a cursado en los últimos quince días.

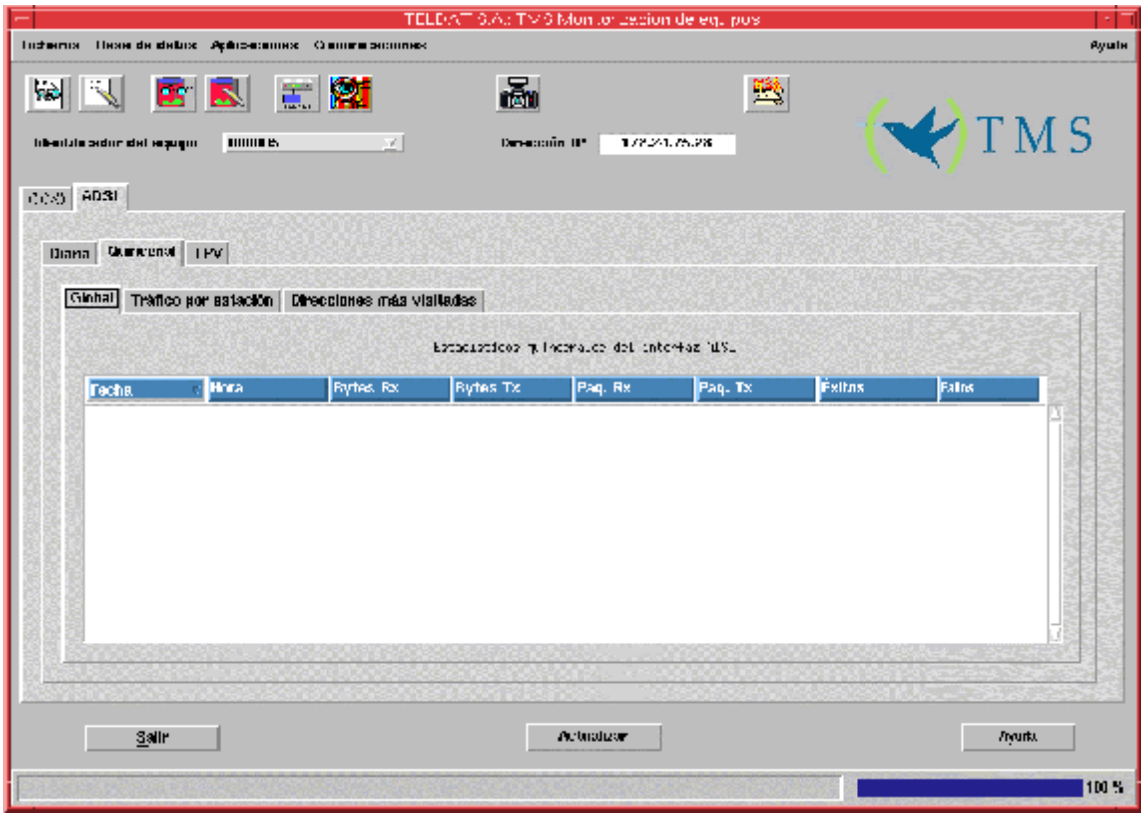


Figura 70 : Monitorización quincenal global ADSL

Cada línea muestra los datos de un día. Los valores corresponden al intervalo transcurrido desde la fecha y hora de la línea anterior hasta la fecha y hora de la línea en curso.

Se muestran los siguientes campos:

- **Fecha:** Fecha en la que el router almacenó los datos de esta línea.
- **Hora:** Hora en la que el router almacenó los datos de esta línea.
- **Bytes Rx:** Bytes recibidos en el interfaz ADSL del router.
- **Bytes Tx:** Bytes transmitidos por el interfaz ADSL del router.
- **Paquetes Rx:** Paquetes recibidos en el interfaz ADSL del router.
- **Paquetes Tx:** Paquetes transmitidos por el interfaz ADSL del router.
- **Exitos:** Número total de conexiones establecidas con éxito a nivel del protocolo PPP sobre el interfaz ADSL.
- **Fallos:** Número total de conexiones rechazadas por un fallo de autenticación o por un fallo en la negociación de parámetros del protocolo PPP sobre ADSL. Si no llega a establecerse la conexión se incrementa este contador.

- ***Tráfico por estación***

En esta ventana se presenta el tráfico cursado por las primeras 50 estaciones que cada día generaron tráfico a través del router.

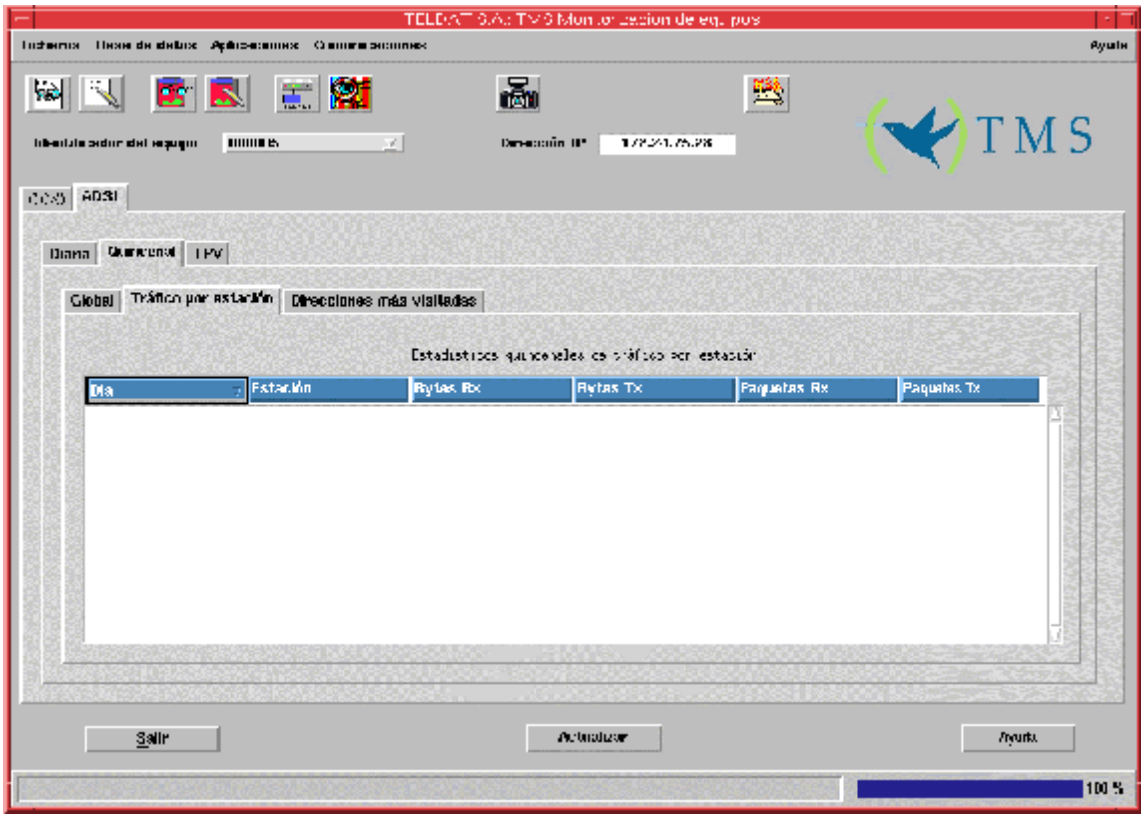


Figura 71 : Monitorización quincenal de tráfico por estación ADSL

Las variables a monitorizar son las siguientes:

- **Día:** Fecha en la que la estación se conectó.
- **Estación:** Dirección IP de la estación que cursó el tráfico.
- **Bytes Rx:** Bytes recibidos en el interfaz ADSL del router.
- **Bytes Tx:** Bytes transmitidos por el interfaz ADSL del router.
- **Paquetes Rx:** Paquetes recibidos en el interfaz ADSL del router.
- **Paquetes Tx:** Paquetes transmitidos por el interfaz ADSL del router.

- ***Direcciones más visitadas***

Esta tabla contiene las direcciones visitadas en los últimos 15 días, para las 256 primeras direcciones visitadas.

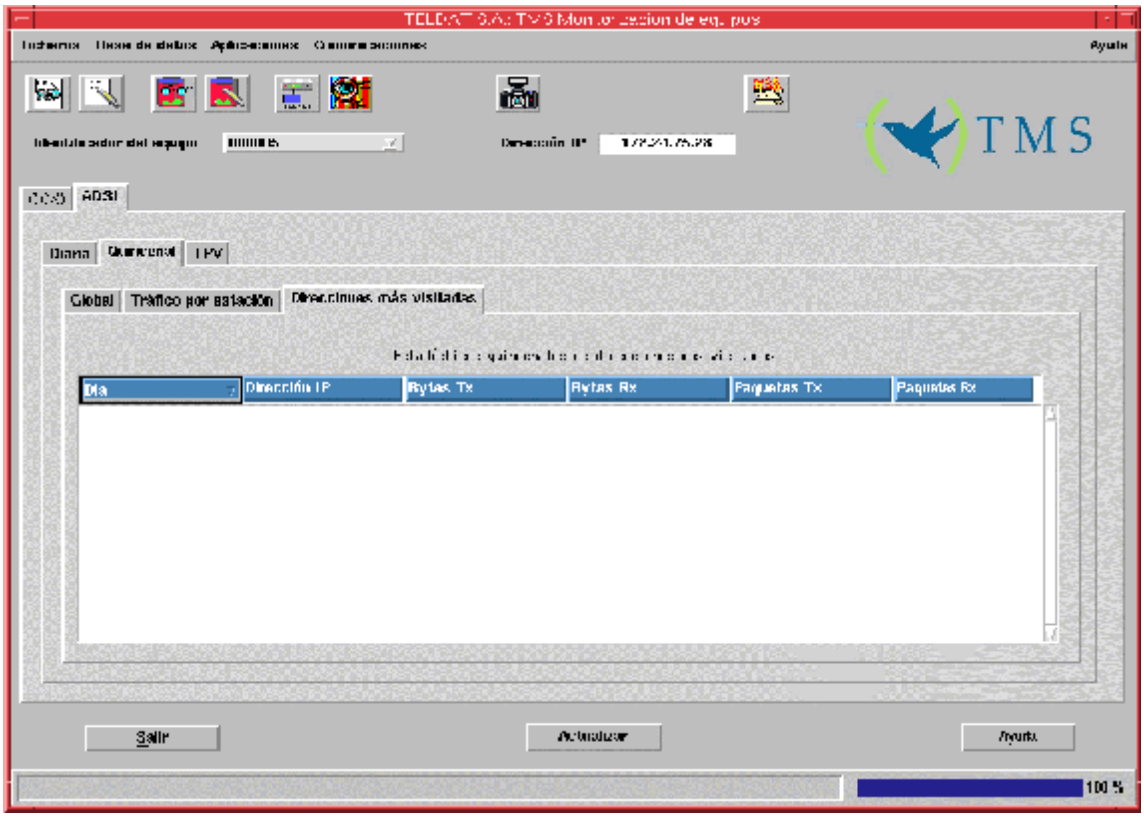


Figura 72 : Monitorización quincenal de direcciones más visitadas

Los datos son los siguientes:

- **Día:** Día en que se realizó la conexión.
- **Dirección IP:** Dirección IP con la que se estableció la conexión.
- **Bytes Tx:** Bytes transmitidos por el interfaz ADSL con destino la dirección IP anterior.
- **Bytes Rx:** Bytes recibidos en el interfaz ADSL del router remitidos por la dirección anterior.
- **Paquetes Tx:** Paquetes transmitidos por el interfaz ADSL con destino la dirección IP anterior.
- **Paquetes Rx:** Paquetes recibidos en el interfaz ADSL del router remitidos por la dirección anterior.

2.4. Monitorización de TPV

En las solapas de TPV se monitoriza la información (para los equipos que la guarden) acerca de las transacciones que han realizado (hayan sido correctas o no). En la monitorización de transacciones se presentan los estadísticos almacenados en el equipo sobre ellas. Para refrescar la ventana es necesario situarse en la carpeta de monitorización de transacciones y pulsar **Actualizar** o el icono de la esquina superior derecha de la ventana. Cada vez que se solicitan estos estadísticos al equipo se almacenan automáticamente en los ficheros de estadísticos del directorio **`$TELDATMS/acounts/$TMSLANG`**.

La información mostrada es idéntica para los equipos RDSI y los ADSL.

a) ***Transacciones correctas***

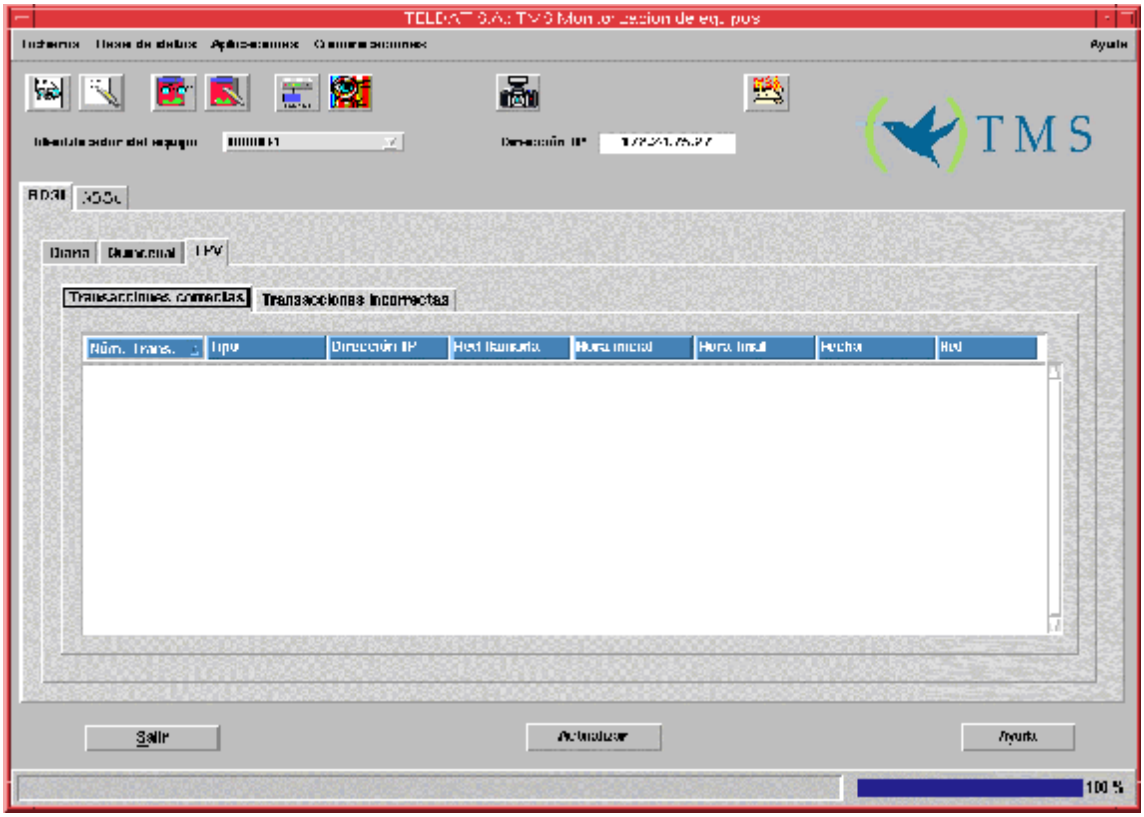


Figura 73 : Monitorización de las transacciones correctas

Cada línea muestra los datos de una transacción realizada correctamente por un terminal punto de venta.

Se muestran los siguientes campos para cada transacción

- **Num. Trans.:** Número de la transacción realizada.
- **Tipo:** Clase a la que pertenece la transacción.
- **Dirección IP:** Dirección IP del centro de validación de la transacción.
- **Red llamada:** Red a la que se ha llamado para realizar la transacción.
- **Hora inicial:** Hora en la que comenzó a realizarse la transacción.
- **Hora final:** Hora en la que finalizó la transacción.
- **Fecha:** Fecha de realización de la transacción.
- **Red:** Entidad contra la que se realiza la transacción.

b) ***Transacciones erróneas***

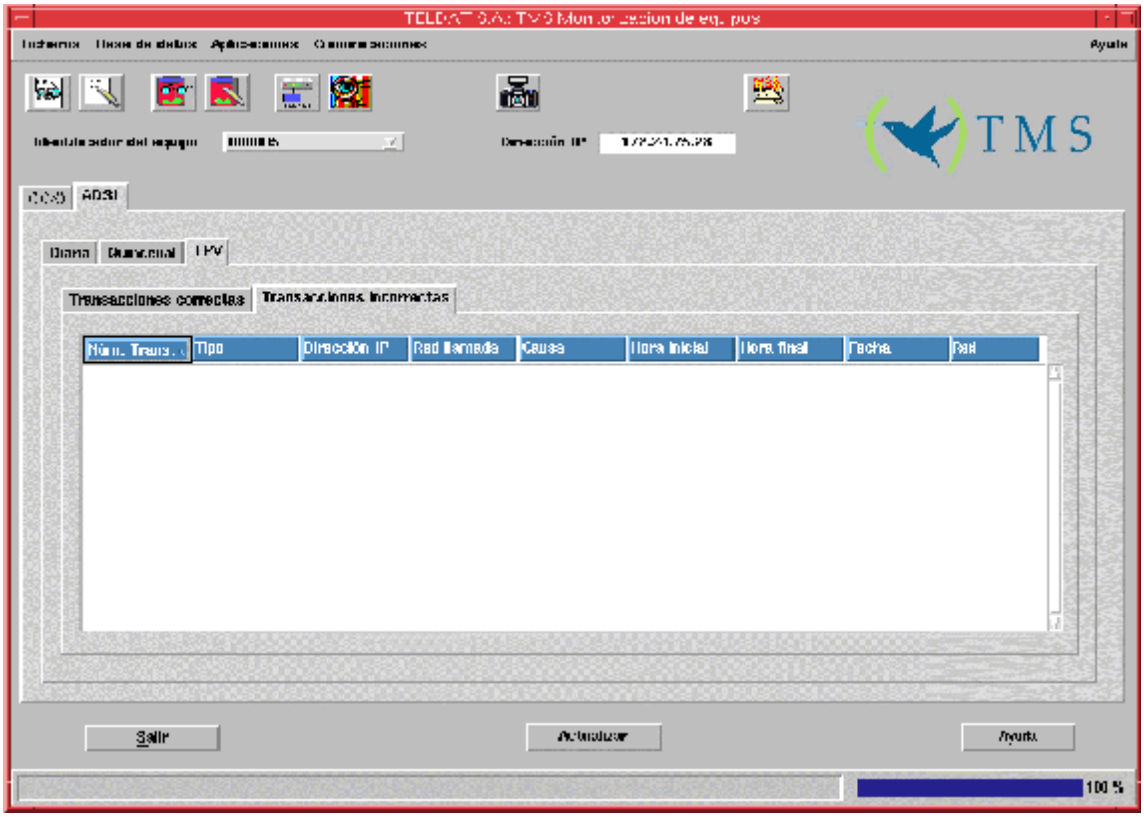


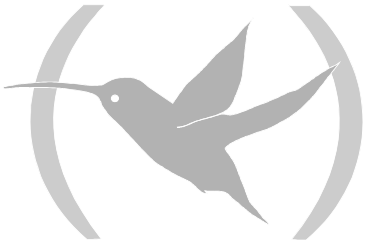
Figura 74 : Monitorización de las transacciones erróneas

Cada línea muestra los datos de una transacción realizada de forma incorrecta por un terminal punto de venta.

Se muestran los siguientes campos para cada transacción

- **Num. Trans.:** Número de la transacción realizada.
- **Tipo:** Clase a la que pertenece la transacción.
- **Dirección IP:** Dirección IP del centro de validación de la transacción.
- **Red llamada:** Red a la que se ha llamado para realizar la transacción.
- **Causa:** Motivo por el que la transacción no se ha realizado correctamente. El significado de estos valores se encuentra en Errores en las transacciones.
- **Hora inicial:** Hora en la que comenzó a realizarse la transacción.
- **Hora final:** Hora en la que finalizó la transacción.
- **Fecha:** Fecha de realización de la transacción.
- **Red:** Entidad contra la que se realiza la transacción.

Capítulo 5
Recogida automática de estadísticos



1. Recogida automática de Estadísticos

La recogida automática de estadísticos surge de la necesidad de recolectar periódicamente los estadísticos quincenales de todos los equipos TMS de la base de datos y se integra dentro del concepto de operaciones sobre grupos.

Se lanza todas las noches a las 0 horas y recolecta primero aquellos equipos a los que nunca se les ha recolectado y luego, los que no se han recolectado desde hace más de 7 días. Además se fuerza a que termine antes de las 7 de la mañana. Los equipos se recolectan en paralelo pudiéndose configurar el grado de paralelismo para no saturar el canal de comunicaciones.

1.1. Instalación

Internamente, se vincula a la tabla CRON del usuario, de manera que, para comprobar si efectivamente está instalada la recogida automática, el usuario de gestión tiene que ejecutar el comando:

```
>crontab -l
```

Si en la ventana aparece la línea:

```
0 0 * * * $TELDATMS/scripts/autocron.sh
```

es que está instalada.

Para instalar la recogida automática, ejecutar el script **`$TELDATMS/scripts/install_autocron.sh`** como usuario de gestión. Este script añade a la tabla CRON del usuario la línea arriba mencionada que arranca la recogida automática.

1.2. Arranque

Para lanzar la recogida automática de estadísticos hay que ejecutar el gestor de operaciones sobre grupos **tmsgroupop** con la operación **sincrogetaccounts** (NOVACOM, NOVACOM-X25 y Teldat C3B) **sincrogetaccounts46** (Teldat C2 y Teldat C3) (o **getaccounts/getaccounts46** si no se quieren sincronizar los equipos).

```
$TELDATMS/bin/tmsgroupop -acc [-auto] -o [sincro]getaccounts[46] -f <fichero> -m
<maestro> [-hour <HH:MM>]
```

-acc	Le indica al gestor de operaciones sobre grupos que actualice la tabla de auto de recogida automática de estadísticos.
-auto	Los registros de la tabla auto se actualizaran como pertenecientes a la aplicación automática.
-f <fichero>	Fichero con el grupo de equipos a recolectar.

-m <maestro>	Router maestro en el que se gestionarán los equipos.
sincrogetaccounts	Sincroniza los equipos antes de recolectar.
sincrogetaccounts46	
getaccounts	No sincroniza los equipos.
getaccounts46	

Existen además las opciones pertenecientes a la propia recogida y que se configuran en el campo de parámetros del registro de la operación **getaccounts/getaccounts46** de la tabla **go_op** en la que se definen las operaciones sobre grupos.

1.3. Sincronización de los equipos

Como se ha visto en el apartado anterior, para sincronizar se utiliza la operación **sincrogetaccounts/sincrogetaccounts46.**

1.4. Progreso

Para monitorizar el estado de la recogida de todos los equipos de la base de datos se utiliza la aplicación **tmsmonauto** cuya ventana principal es la siguiente:

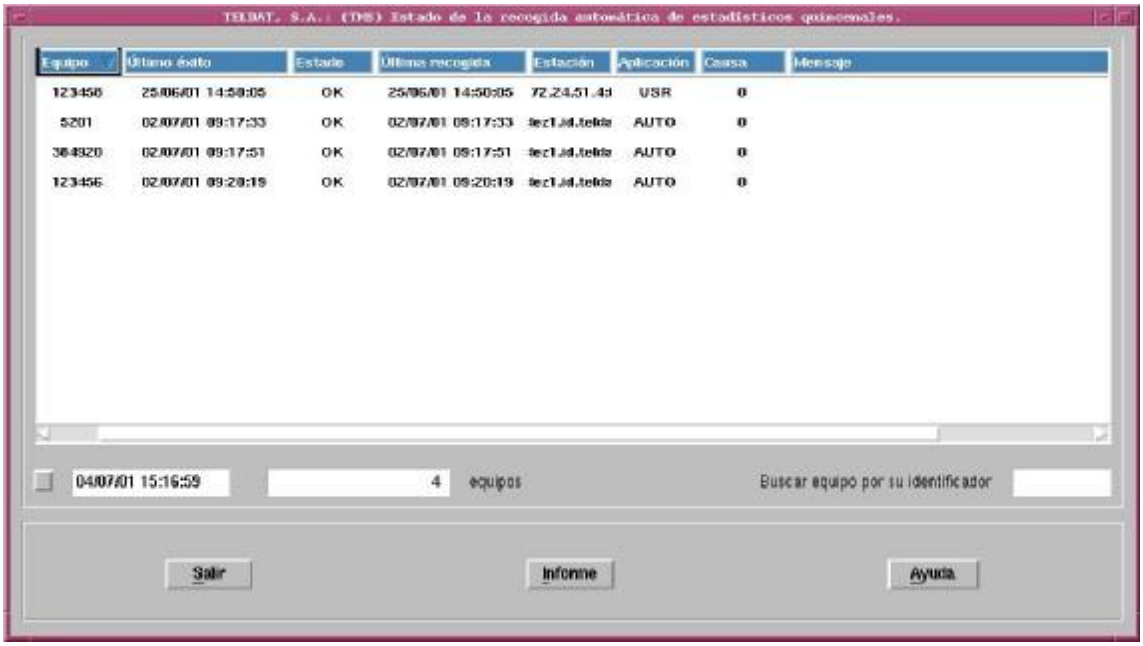


Figura 75 : Monitorización de la recogida automática de estadísticos

La aplicación consulta periódicamente (por defecto cada 10 segundos) el contenido de la tabla **auto** que es actualizada por el gestor de operaciones sobre grupos, la aplicación de monitorización (cuando se leen estadísticos quincenales) y la aplicación de recogida automática de estadísticos.

Si el usuario pulsa sobre cualquiera de las cabeceras de columna, la aplicación lee todos los registros de la tabla y los ordena según el contenido de la columna seleccionada. Si se produce una segunda

pulsación sobre la misma columna, se vuelven a leer los datos de nuevo, pero ordenando en sentido inverso.

En ausencia de iteraciones de usuario, la aplicación sólo actualiza los registros que cambiaron desde la anterior lectura y, con dichos registros, no realiza ordenación cuando son modificados en la ventana.

La anchura de las columnas de la tabla puede ser modificada por el usuario para mejorar su visualización. Para ello, se sitúa el puntero del ratón entre dos cabeceras de columna hasta que cambia su apariencia a '↔' y, a continuación, se redimensiona. Cuando arranca la aplicación recuerda los tamaños de su última ejecución.

El significado de las columnas de la tabla es el siguiente:

Equipo	Identificador del equipo asociado al registro.
Último éxito	Fecha y hora de la última recogida de estadísticos realizada con éxito sobre el equipo.
Estado	Estado resultante de la última recolección.
Última recogida	Fecha y hora de la última recogida realizada sobre equipo.
Estación	Identificador de la estación desde la que se realizó la última recogida (variable de entorno DISPLAY).
Aplicación	Aplicación desde la que se recogió por última vez. Si es la recogida automática su contenido será AUTO, si es la aplicación de monitorización será USR.
Causa	Causa de liberación RDSI o pseudocausa (véase "Causas de liberación RDSI") asociada a la última recolección.
Mensaje	Información acerca del estado y sus causas.

A partir de la versión 1.4.1 del router maestro la causa de liberación RDSI sólo es significativa cuando el número de equipos gestionados en estado CONSULTANDO en el router maestro es menor o igual a dos.

Bajo la esquina inferior izquierda de la tabla se encuentra el indicador de lectura de la base de datos y la fecha y hora en curso para contrastarlas con las de la tabla.

Junto a la esquina inferior derecha existe una entrada en la que el usuario puede introducir el número de teléfono del equipo que desee supervisar y la aplicación se lo seleccionará en la lista.

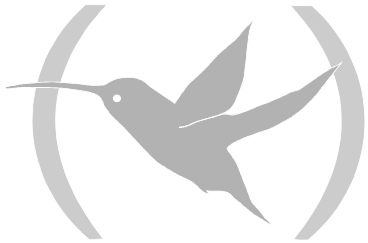
1.5. Resultados

La ejecución de la recogida automática de estadísticos se confirma consultando el correo del usuario de gestión.

La aplicación envía mensajes de depuración, información y error a través del demonio **syslogd** de log del sistema con la facilidad **local7** y prioridades **debug**, **err** e **info**. El usuario puede configurar dicho demonio para que le presente en consola, le guarde en fichero o reenvíe a otra estación los mensajes que genera la aplicación. Para más información consultar el Registro de sucesos.

Además, los resultados finales se guardan en la tabla auto de la base de datos y se pueden visualizar con la aplicación **tmsmonauto** como se explicó anteriormente.

Capítulo 6
Operaciones sobre grupos



1. Operaciones sobre grupos

Las operaciones sobre grupos están concebidas como una herramienta muy potente para facilitar la gestión de los equipos, pero potencialmente peligrosa si se utilizan sin extremar las precauciones (supongamos el caso de lanzar una operación de telecarga de software a todo el conjunto de equipos de la base de datos pasando como parámetro un fichero de programa inválido). Adicionalmente, las operaciones de configuración de grupos requieren considerables conocimientos de SQL para poder alterar las configuraciones a enviar en la base de datos. Es por esto, que se espera que dichas operaciones sean lanzadas siempre por personal de gestión suficientemente capacitado y se recomienda que el número de administradores autorizados a realizarlas sea reducido.

El usuario que quiera realizar una operación sobre un subconjunto de equipos de la base de datos deberá seguir los siguientes pasos:

1. Definir la operación.
2. Definir el grupo de equipos sobre el que se aplicará.
    2.1. Por medio de un fichero con un teléfono identificador de equipo (teléfono) por línea.
    2.2. En la tabla **groups** de la base de datos con consultas SQL.

Las operaciones sobre grupos siempre se lanzan contra un fichero de grupo.

3. Si es una operación de configuración …
    3.1. Generar las tablas temporales de configuración.
    3.2. Modificar las configuraciones a enviar.
4. Ejecutar la operación sobre grupos.
5. Monitorizar el progreso de la operación.

Operaciones sobre grupos simultáneas.

La aplicación soporta el lanzamiento de varias operaciones sobre grupos de forma simultánea, aunque no es lo recomendado. Sin embargo, en operaciones de configuración, es imprescindible que los grupos sean disjuntos, es decir, que un equipo no puede pertenecer a más de un grupo sobre el que se esté ejecutando alguna operación. Si esto no se cumple, las configuraciones temporales de dichos equipos serán alteradas en función de las necesidades de cada operación permaneciendo las últimas modificaciones.

1.1. Definición de operaciones sobre grupos

En la tabla **go_op** de la base de datos están definidas las operaciones más comunes:

Operación	Descripción
getaccounts	Recolección de estadísticos quincenales y parámetros informativos del equipo para equipos NOVACOM, Teldat C2B, Teldat C3B y parámetros RDSI de los equipos Teldat C4I.
sincrogetaccounts	Sincronización y recolección de estadísticos quincenales y parámetros informativos del equipo para equipos NOVACOM, Teldat C2B, Teldat C3B y parámetros RDSI de los equipos Teldat C4I.
getaccounts46	Recolección de estadísticos quincenales y parámetros informativos del equipo para equipos Teldat C2, Teldat C2-UP y Teldat C3
sincrogetaccounts46	Sincronización y recolección de estadísticos quincenales y parámetros informativos del equipo para equipos Teldat C2, Teldat C2-UP y Teldat C3
getaccounts53	Recolección de estadísticos de transacciones de los equipos Teldat C3 y Teldat C3B
telecarga37	Telecarga de la última versión para los equipos NOVACOM.
telecarga46	Telecarga de la última versión para los equipos Teldat Cx.
tmsgetconf51	Petición de configuración a equipos NOVACOM y almacenamiento en la base de datos.
tmsgetconf46	Petición de configuración a equipos Teldat C2 y almacenamiento en la base de datos.
tmsgetconf53	Petición de configuración a equipos Teldat C3 y almacenamiento en la base de datos.
tmsgetconf57	Petición de configuración a equipos Teldat C2B y almacenamiento en la base de datos.
tmsgetconf60	Petición de configuración a equipos Teldat C3B y almacenamiento en la base de datos.
tmsgetconf68	Petición de configuración a equipos Teldat C4I y almacenamiento en la base de datos
tmsgetconf72	Petición de configuración a equipos Teldat C2-UP y almacenamiento en la base de datos
tmsgetinfo	Obtención de parámetros informativos del equipo.
tmsreset	Reset del equipo.
tmssetconf51	Reconfiguración de equipos NOVACOM. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.
tmssetconf46	Reconfiguración de equipos Teldat C2. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.
tmssetconf53	Reconfiguración de equipos Teldat C3. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.

tmssetconf57	Reconfiguración de equipos Teldat C2B. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.
tmssetconf60	Reconfiguración de equipos Teldat C3B. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.
tmssetconf68	Reconfiguración de equipos Teldat C4I. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.
tmssetconf72	Reconfiguración de equipos Teldat C2-UP. Envía la configuración temporal, la pide de nuevo al equipo, la almacena en base de datos, la salva a memoria FLASH y lo resetea.
tmssettime	Puesta en hora del equipo NOVACOM, Teldat C2B, Teldat C3B.
tmssettime46	Puesta en hora del equipo Teldat C2, Teldat C2-UP y Teldat C3

La gestión de grupos y operaciones sobre grupos se lleva a cabo desde la aplicación **tmsdefgo**.

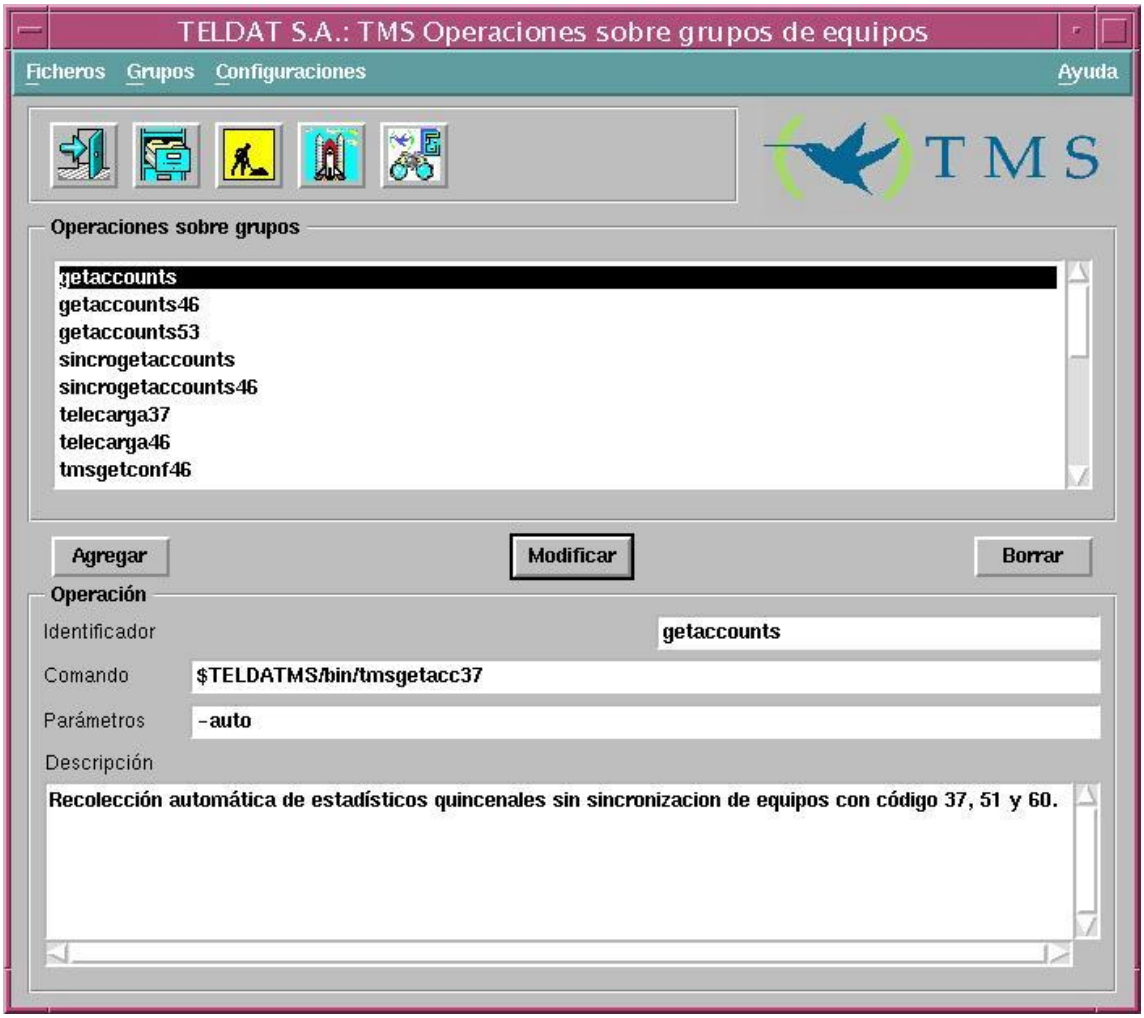


Figura 76 : Definición de operaciones sobre grupos

Cada operación se caracteriza por los siguientes campos:

Identificador:
Es una cadena de caracteres que se asigna a la operación.
Admite hasta 30 caracteres.
No puede haber dos operaciones con el mismo nombre.

Comando:
Es un comando UNIX que puede corresponderse con un ejecutable o un script de la shell. En ambos casos la secuencia de llamada tiene que ser:

```
<aplicacion> -i <direccion IP> [-id <id. de equipo>] [-ppid
<ppid>] [-c <comunidad SNMP>] [...]
```

<direccion IP>	Dirección IP del equipo.
<id. equipo>	Identificador de equipo (número de teléfono).
<comunidad SNMP>	Comunidad SNMP del equipo.

Los parámetros entre corchetes son opcionales pero si no se indican el identificador de equipo y el identificador de proceso no se podrá actualizar el estado de la operación. Admite un máximo de 255 caracteres.

Parámetros:
Parámetros adicionales para el comando anterior. Admite hasta 255 caracteres.

Descripción
Información para que el usuario conozca el propósito de la operación. Se dispone de 255 caracteres.

Para **agregar** una nueva operación a la lista se rellenan sus campos y se pulsa el botón **Agregar**.

Para **modificar** una operación de la lista se selecciona y tras alterar los campos correspondientes se pulsa el botón **Modificar**.

Para **borrar** una operación de la lista se selecciona y se pulsa el botón **Borrar**.

Para salir de la aplicación pulsar  .

A la gestión de grupos se accede por medio el botón  .

Cuando se quieren modificar las configuraciones temporales que se enviarán a los equipos se utiliza el botón  .

Para lanzar una operación sobre grupos se pulsa el botón  .

1.2. Gestión de grupos

La gestión de grupos se realiza desde la siguiente ventana que se abre desde la aplicación **tmsdefgo** con el botón  :

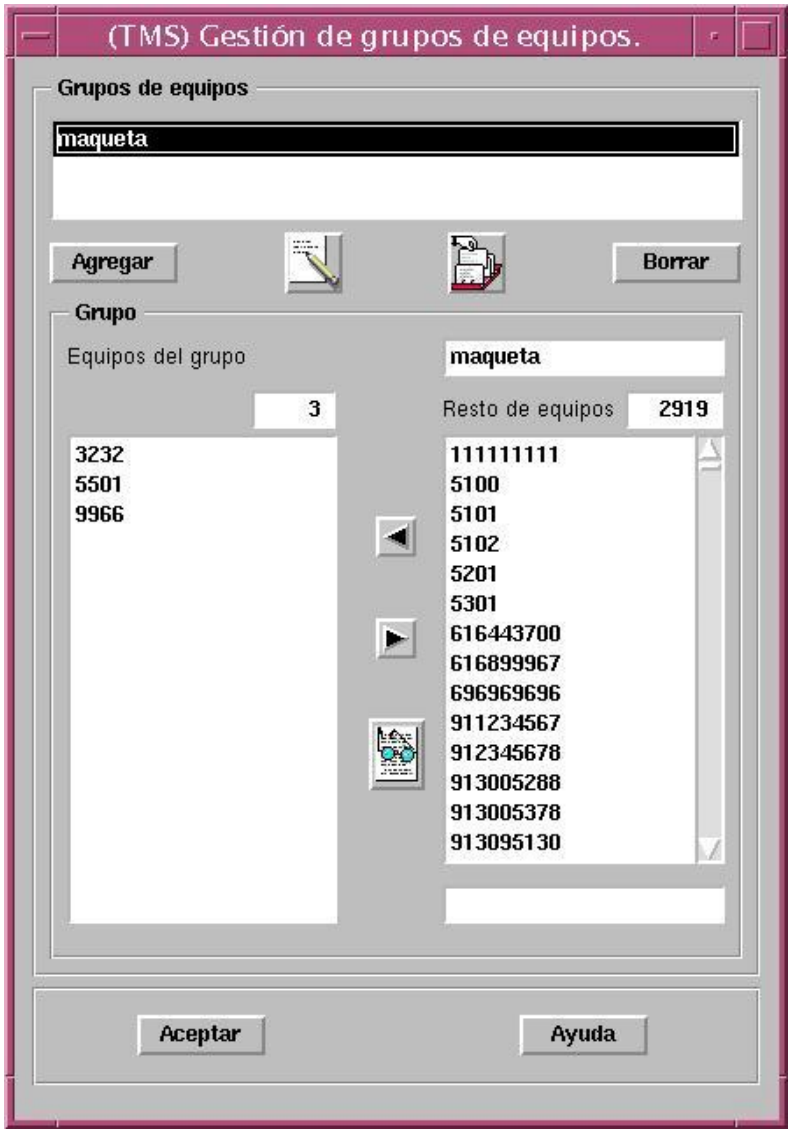


Figura 77 : Definición de grupos

En la lista superior aparecen los grupos definidos en la tabla **groups** de la base de datos. Cuando se selecciona un grupo en esta lista aparecen sus componentes en la lista inferior izquierda y el resto de equipos de la base de datos en la lista inferior derecha, bajo los cardinales de ambas listas.

Si no hay definido ningún grupo las listas aparecen vacías.

Cuando se agrega el primer grupo aparecen en la lista inferior derecha los equipos de la base de datos.

Para ***agregar*** un nuevo grupo se escribe su nombre en el campo del identificador y se pulsa el botón **Agregar**.

Para ***borrar*** un grupo se selecciona y se pulsa el botón **Borrar** y a continuación aparecerá una ventana de confirmación de la acción.

Para ***generar un fichero de grupo*** a partir de un grupo de la base de datos se pulsa 

Para ***añadir*** los equipos de un fichero de grupo a un grupo de la base de datos se pulsa el botón  .

Es necesario que todos los equipos del fichero estén dados de alta en la tabla **device** de equipos de la base de datos.

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).

Para ***generar las configuraciones temporales*** asociadas a un grupo y que el usuario pueda alterarlas para enviárselas a los equipos se utiliza el botón  .

Con los botones en forma de flecha que hay entre las listas se añaden o borran equipos del grupo. Puede realizarse selección múltiple en ambas listas. Para seleccionar múltiples equipos pulse la tecla <Control> y, manteniéndola pulsada, seleccione con el ratón los equipos. Para seleccionar un grupo consecutivo de equipos seleccione el primero con el ratón, pulse la tecla de mayúsculas y, manteniéndola pulsada, seleccione el último.

Para **buscar** un equipo se puede escribir el teléfono del equipo en el recuadro de texto que hay bajo la lista derecha y el equipo más próximo se mostrará el primero en la lista.

También pueden generarse grupos a partir de consultas SQL en la aplicación SQL*Plus® que se puede lanzar desde la ventana de definición de operaciones sobre grupos con el botón  .

Veamos algunos ejemplos:

1. Grupo de todos los equipos de Madrid:

```
(tmsgrp)SQL>insert into groups
  2  select 'madrid', id from device
  3  where id like '91%';
```

2. Grupo con todos los equipos que llevan mas de un día (8640000 centésimas de seg.) en funcionamiento:

```
(tmsgrp)SQL>insert into groups
 2  select 'mas_de_un_dia', id from infodevice
 3  where sysuptime > 8640000;
```

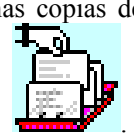
3. Equipos a los que hace más de 7 días que no se recogen los estadísticos:

```
(tmsgrp)SQL>insert into groups
 2  select 'acc_mas_7', id from auto
 3  where datetime < (sysdate - 7);
```

¡Atención!

La operación siempre trabaja con un fichero de grupo, por lo que siempre hay que volcar el grupo a fichero antes de lanzarla. Por eso, es conveniente mantener actualizados los ficheros de grupo y los grupos de la base de datos y que ambos contengan los mismos equipos.

1.3. Operaciones de configuración de grupos de equipos

Antes de iniciar la operación se define el grupo como se indicó en el apartado anterior. Después, se generan las configuraciones temporales que son unas copias de las originales que el usuario puede alterar si así lo desea. Para generarlas pulsar el botón  .

Cuando se quieren modificar las configuraciones temporales que se enviarán a la base de datos se utiliza el botón  .

Aparece una ventana con el prompt de SQL*Plus® de ORACLE que es un interprete SQL desde el que podemos alterar las tablas. La conexión a la base de datos se realiza como usuario **tmsgrp** de gestión de grupos. Dicho usuario puede consultar las tablas del usuario **tms** que es el usuario principal de la gestión TMS, pero únicamente tiene privilegios para alterar las tablas temporales de configuración. Antes de modificar las configuraciones temporales es imprescindible que se hayan generado desde la ventana de gestión de grupos de la aplicación **tmsdefgo**.

Todas las acciones que se realicen desde la ventana de SQL*Plus® se guardan en el fichero **`$TELDATMS/log/tmsgrp.log`**.

Para facilitar la tarea del administrador de operaciones sobre grupos (usuario **tmsgrp**) se han creado scripts SQL en el directorio **`$TELDATMS/etc`/dbx.**

a) Ejemplos de operaciones de configuración sobre grupos

Veamos a continuación algunos ejemplos típicos de modificación de las configuraciones temporales. Para los ejemplos trabajaremos con el grupo **maqueta_teldat** constituido por un sólo equipo cuyo teléfono es **918060405**. El grupo se creará siguiendo las indicaciones del apartado "Gestión de grupos" recordando guardarlo también en fichero con el mismo nombre.

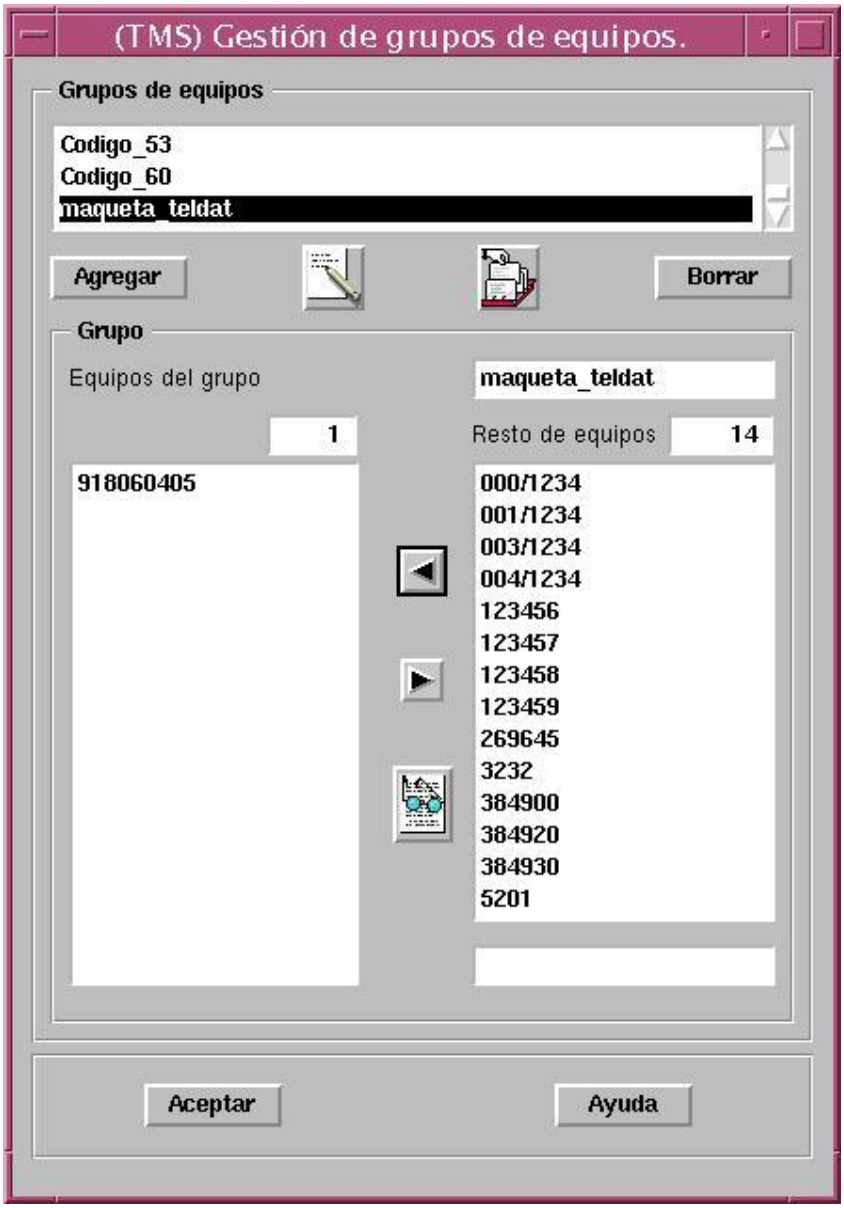


Figura 78 : Grupo de ejemplo 'maqueta_teldat'

Para generar las configuraciones temporales del grupo lo seleccionamos y pulsamos  .

Para modificar las configuraciones temporales se pulsa el botón  y se presentará la siguiente ventana:

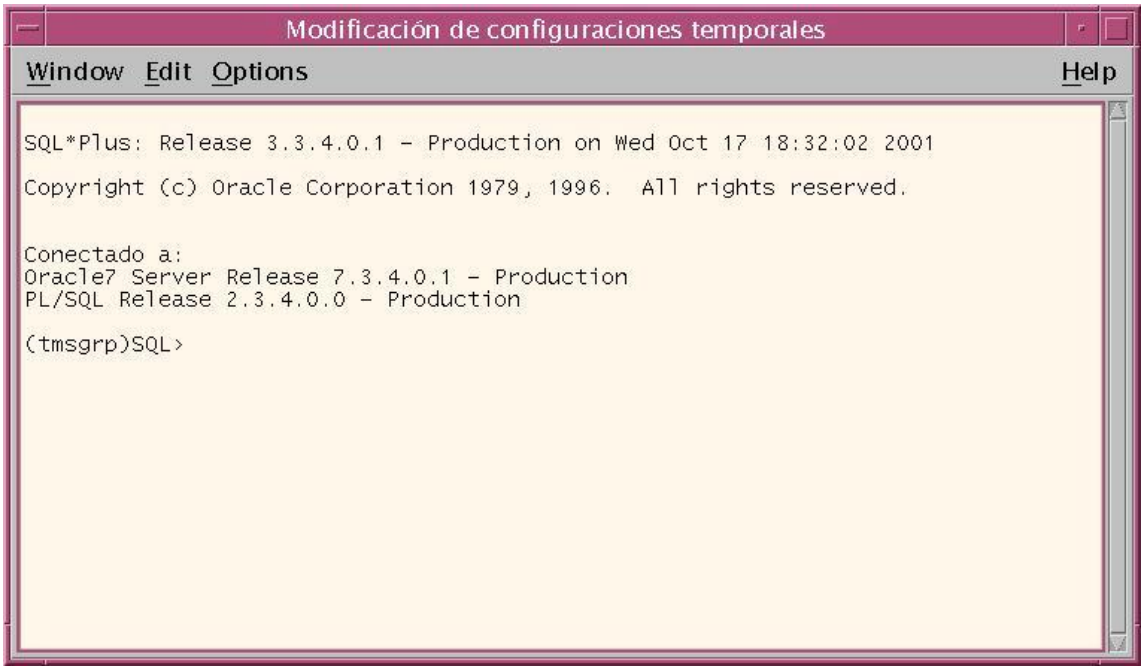


Figura 79 : ORACLE-SQL *PLUS. Modificación de configuraciones temporales

Veamos los casos típicos (el texto sombreado en negrita son los comandos que introduce el usuario).

La descripción de la tabla temporal de maestros autorizados **conf37_masters** es la siguiente:

```
(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)
```

- ***Inserción de un nuevo router maestro autorizado para todos los equipos de un grupo***

```
 (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
```

- ***Modificación de un router maestro autorizado en todos los equipos de un grupo***

```
(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
```

- ***Borrado de un maestro autorizado en todos los equipos de un grupo***

```
(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
```

Cuando se quieren enviar configuraciones almacenadas en la base de datos a un grupo de equipos se utilizará la operación **tmssetconf37** de la base de datos.

Confirmación de sentencias SQL.

Todas las sentencias que modifiquen registros de las tablas deben confirmarse con la orden "commit" (o rectificarse con la orden "rollback") antes de lanzar la operación.

Cuando se abandona SQL*Plus® con la orden "quit" se produce un "commit" implícito de todas las sentencias de la sesión.

1.4. Ejecución de operaciones sobre grupos

Para lanzar una operación sobre grupos se pulsa el botón  en la ventana principal de la aplicación **tmsdefgo**

Figura 80 : Ejecución de operaciones sobre grupos

Operación:

Identificador de operación sobre grupos a lanzar.

Se muestran todas las operaciones contenidas en la tabla **go_op** de la base de datos.

Router maestro a utilizar:

Es el router maestro en el que se gestionarán los equipos del grupo para aplicarles la operación.

Fichero de grupo de equipos:

Nombre completo del fichero en el que se define el grupo de equipos sobre el que se aplica la operación. Su formato es de un identificador por línea.

Si se pulsa en el botón  aparece una ventana de selección de fichero de grupo.

Equipos reservados en el maestro para aplicación de usuario:

Por defecto, el gestor de operaciones sobre grupos utiliza la máxima capacidad del router maestro para gestionar los equipos. Actualmente, el router maestro puede gestionar hasta 50 equipos simultáneamente. Si no se reserva ningún equipo para la aplicación de usuario (valor por defecto) el

gestor de operaciones sobre grupos acapara para sí el maestro y no dejará ningún "hueco" para que un usuario gestione ningún equipo. Si, por ejemplo, el valor es 10, entonces el gestor intentará dejar siempre 10 "huecos" para que el usuario pueda gestionar equipos. Se admiten valores en el rango [0 .. 50].

Máximo número de equipos operando simultáneamente:

Este parámetro se introduce para impedir la saturación del canal de comunicaciones de la estación de gestión. El número de equipos en estado CONSULTANDO, ACCESIBLE u OPERANDO pertenecientes a esta aplicación nunca superará este valor.

El valor por defecto es 100 para que, prácticamente, no limite.

Hora de finalización:

Si se establece una hora de finalización, la operación sobre grupos no gestionará ningún equipo después de dicha hora y finalizará cuando haya terminado de procesar los que ya estaban en gestión. Si la hora es anterior al instante del arranque se supone que pertenece al día siguiente.

Cuando se lanza la operación la aplicación envía todas las ordenes de gestión que le sean posibles al router maestro garantizando que quedan libres un número de "huecos" igual al parámetro "equipos reservados para la aplicación manual" y sin superar en ningún caso el "Máximo número de equipos operando simultáneamente". Si los equipos tienen dirección IP estática, primero se intenta gestionarlo por ella y, si falla, se gestiona a través del maestro.

La aplicación espera unos 4 minutos a que cada equipo en gestión se ponga en estado ACCESIBLE y si no lo consigue lo retira por time-out.

Cuando el equipo se pone en estado ACCESIBLE el gestor de operaciones lanza la operación y envía la orden de desgestión al router maestro porque confía en que el tráfico generado por la propia operación mantenga la conexión. De esta forma permite poner inmediatamente otro equipo en gestión optimizando la rapidez de las operaciones sobre grupos.

El gestor de operaciones sobre grupos termina cuando ha aplicado la operación a todos los equipos del grupo que han conseguido obtener el estado ACCESIBLE o cuando se produce un error en la comunicación con el router maestro o una interrupción de usuario que le impidan continuar su trabajo.

Los botones de la ventana causan las siguientes acciones:

Aceptar	Presenta una ventana en la que se solicita una contraseña de seguridad. Sólo los usuarios autorizados que conozcan la contraseña pueden lanzar una operación sobre grupos. Si se desea cambiar la contraseña se debe ejecutar la aplicación **$TELDATMS/bin/tmsgrpwd**
Cancelar	Cierra la ventana cancelando la operación.
Ayuda	Presenta ventana de ayuda.

Si el usuario entra en la ventana de entrada de contraseña pero después se arrepiente y quiere cancelar la operación basta con que pulse Aceptar con una contraseña incorrecta (o vacía).

1.5. Monitorización de operaciones sobre grupos

Al igual que el resto de aplicaciones de gestión TMS, las operaciones sobre grupos envían mensajes al demonio de log del sistema (syslogd) para que este las curse en función de su fichero de configuración.

La aplicación **tmsmongo** se utiliza para monitorizar el estado de las operaciones sobre grupos.

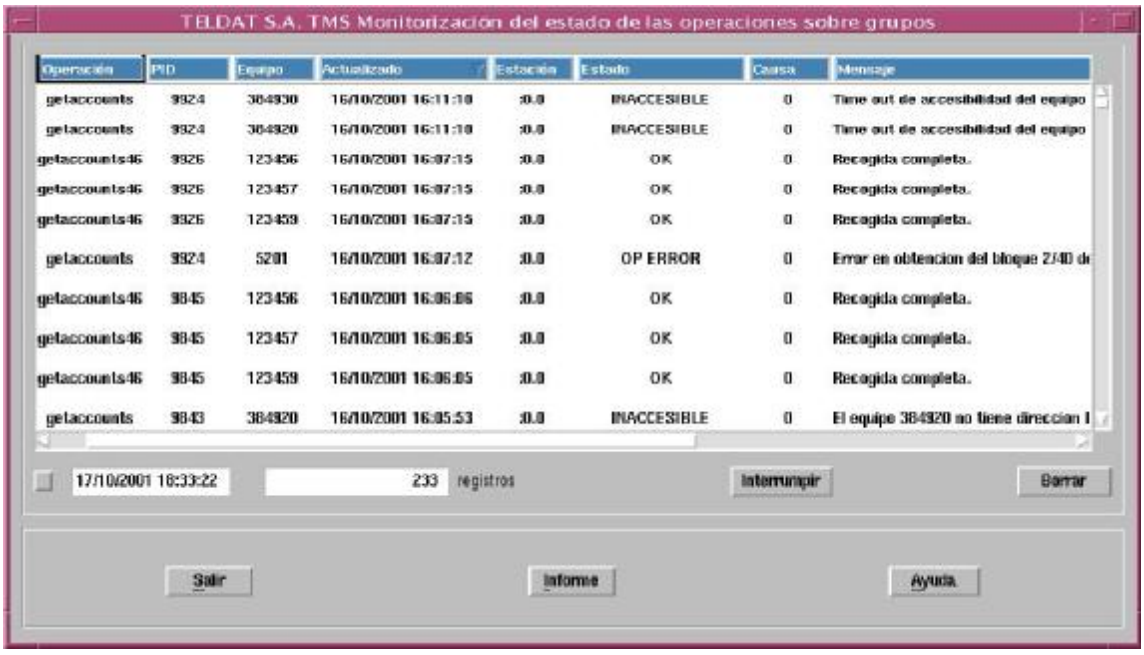


Figura 81 : Monitorización de operaciones sobre grupos

La aplicación consulta periódicamente (por defecto cada 10 segundos) el contenido de la tabla **go_log** que es actualizada por el gestor de operaciones sobre grupos y por las propias operaciones cuando terminan o se establecen condiciones de error.

Si el usuario pulsa sobre cualquiera de las cabeceras de columna, la aplicación lee todos los registros de la tabla y los ordena según el contenido de la columna seleccionada. Si se produce una segunda pulsación sobre la misma columna, se vuelven a leer los datos de nuevo, pero ordenando en sentido inverso.

En ausencia de iteraciones de usuario, la aplicación sólo actualiza los registros que cambiaron desde la anterior lectura y, con dichos registros, no realiza ordenación cuando son modificados en la ventana.

La anchura de las columnas de la tabla puede ser modificada por el usuario para mejorar su visualización. Para ello, se sitúa el puntero del ratón entre dos cabeceras de columna hasta que cambia su apariencia a '⊂' y, a continuación, se redimensiona. Cuando arranca la aplicación recuerda los tamaños de su última ejecución.

El significado de las columnas de la tabla es el siguiente:

Operación	Es el identificador de la operación asociada al registro de la tabla.
PID	(Process IDentifier) Identificador del proceso UNIX asignado a la aplicación **groupop** de operaciones sobre grupos.
Equipo	Teléfono RDSI del equipo asociado al registro.
Última recogida	Fecha y hora de la última actualización del registro.
Estación	Identificador de la estación desde la que se lanzó la operación sobre grupos.
Estado	Estado actual de la operación en lo que respecta al equipo asociado al registro (ver tabla).
Causa	Causa de liberación RDSI o pseudocausa (véase "Causas de liberación RDSI") asociada al registro. Si el estado es de error puede ayudar a determinar la causa del error.
Mensaje	Información acerca del estado y sus causas.
Suboperación	Contiene el nombre de la aplicación que deja el mensaje en el caso de que la operación principal lance nuevas aplicaciones.

Estados de los registros de la tabla de operaciones sobre grupos:

Valor numérico	Estado	Significado
-8	**DESGESTIONADO**	El equipo ha sido desgestionado inesperadamente (por ejemplo, si el usuario entra por TELNET o por consola en el router maestro y lo desgestiona).
-7	**OP ERROR**	La operación lanzada sobre el equipo ha terminado con error. El campo "mensaje" de la tabla **go_op** informará al usuario de la causa del error. También pueden consultarse los ficheros de log.
-6	**INACCESIBLE**	Ha vencido el plazo de espera de accesibilidad (aproximadamente 4 minutos) sin obtener el equipo una dirección IP.
-5	**OCUPADO**	El equipo está siendo gestionado por otra aplicación.
-4	**SNMP TIME-OUT**	Se ha enviado una petición SNMP al equipo y ha vencido el plazo de espera.
-3	**SNMP ERROR**	Se ha producido un error en una petición SNMP al equipo.
-2	**TIME-OUT MAESTRO**	El maestro no responde a las peticiones de la tabla de equipos en gestión. Se llega a este estado cuando se producen 3 ciclos de los plazos de intento/espera configurados para el router maestro. Ejemplo: El router maestro tiene configurados 2 intentos de 5 segundos en sus peticiones SNMP, entonces se llega ha este estado después de 30 segundos y 6 intentos. Este estado provoca la terminación de la operación sobre grupos.

-1	**ERROR MAESTRO**	Se ha producido un error en la obtención de la tabla de equipos en gestión del maestro. Este estado provoca la terminación de la operación sobre grupos.
0	**ESPERANDO**	El equipo está a la espera de un "hueco" libre en el maestro para ser gestionado.
1	**GESTIONADO**	Se ha enviado la orden de gestión al maestro, pero aún no está en la tabla de equipos en gestión leída del maestro.
2	**CONSULTANDO**	El equipo ha sido gestionado sobre el maestro y está en su tabla de equipos en gestión.
3	**ACCESIBLE**	El equipo está en estado accesible e inmediatamente el gestor de operaciones sobre grupos lanzará la operación sobre él.
4	**OPERANDO**	Se ha lanzado la operación sobre el equipo y se ha desgestionado en el maestro. El gestor de operaciones sobre grupos ha terminado su trabajo con el equipo.
5	**OK**	Operación concluida con éxito sobre el equipo.
6	**APLAZADO**	Se ha alcanzado la hora de finalización antes de procesar este equipo.
7	**INT USR**	El usuario a interrumpido la operación sobre grupos antes de que se haya lanzado la operación sobre este equipo. Este estado provoca la terminación de la operación sobre grupos.

A partir de la versión 1.4.1 del router maestro la causa de liberación RDSI sólo es significativa cuando el número de equipos gestionados en estado CONSULTANDO en el router maestro es menor o igual a dos.

Bajo la esquina inferior izquierda de la tabla se encuentra el indicador de lectura de la base de datos y la fecha y hora en curso para contrastarlas con las de la tabla. A su derecha se muestra el número de registros que contiene la tabla. A mayor número de registros más lentitud en las consultas y más tráfico en la red. Se recomienda borrar frecuentemente el contenido de la tabla. Si se quieren guardar históricos pueden generarse informes o insertar los registros en otra tabla auxiliar que no sea la que se consulta habitualmente.

Se puede generar un informe a un fichero de texto pulsando el botón **Informe**. A continuación, se solicita al usuario que indique el fichero destino del informe y después se genera con un formato como el que se muestra seguidamente:

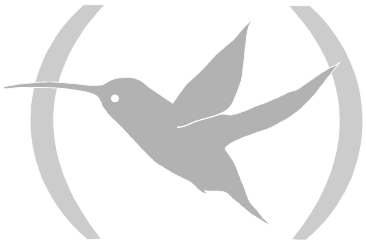
```
TELDAT, S.A.: Estado de operaciones sobre grupos de equipos TMS.

                                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
```

Para interrumpir una operación sobre grupos en curso se selecciona cualquiera de sus registros y se pulsa el botón Interrumpir. La aplicación ejecuta la llamada al sistema **`kill -QUIT <PID>`** donde PID es el identificador del proceso asociado a la operación.

Los registros de la tabla se seleccionan con el botón izquierdo del ratón y se deseleccionan con el botón central. Para seleccionar un rango de registros se selecciona el primero y manteniendo pulsada la tecla de mayúsculas se selecciona el último. Si queremos quitar algunos lo hacemos con el botón central.

Para **borrar** registros de la tabla se seleccionan y se pulsa el botón **Borrar**.

Capítulo 7
Base de datos ORACLE



1. Tablas utilizadas en la base de datos

La gestión TMS utiliza una base de datos ORACLE en la que se definen las siguientes tablas:

acc<codigo_equipo>_<entidad>	Tablas con los estadísticos quincenales que el operador haya guardado de los equipos en BD. En los router C3 y C3B se usan para almacenar las transacciones de los terminales punto de venta.
conf<codigo_equipo>_<entidad>	Tablas que almacenan las configuraciones de los equipos con código de equipo <codigo_equipo>.
infomanaged	Tabla que contiene a la tabla **managed** y además todos los equipos que están siendo gestionados a través de su dirección IP estática.
infodevice	Tabla de información del equipo: Número de serie, número de placa, versión de software, versión de BIOS.
managed	Tabla que indica qué equipos está gestionando cada maestro.
mancalls	Tabla que contiene la duración de todas las llamadas de gestión.
master	Tabla de los routers maestros disponibles.
device	Tabla de los equipos disponibles.

Dichas tablas están a disposición del usuario para ser exportadas a otros formatos o bases de datos, para hacer informes o construir cualquier otra aplicación sobre ellas.

La gestión se conecta a la base de datos como usuario **tms** a la instancia identificada por la variable de entorno **ORATMS**.

Se crea también un usuario, **tmsmon** de monitorización de tablas de la base de datos sin permiso para modificar objetos.

Todas las tablas son propiedad del usuario **tms**, por eso si el administrador de grupos, es decir, el usuario **tmsgrp** quiere referenciarlas tendrá que anteponer al propietario. Sin embargo, para facilitar la labor del administrador, se han definido sinónimos para el usuario **tmsgrp**. Todas las tablas **tms.tmp_conf<codigo_equipo>_<entidad>** se pueden referenciar desde dicho usuario como **conf<codigo_equipo>_<entidad>.**

Por ejemplo,

```
(tmsgrp)SQL>select * from conf37_masters;
```

es lo mismo que

```
(tmsgrp)SQL>select * from tms.tmp_conf37_masters;
```

Cuando el usuario quiere realizar una operación de configuración sobre grupos altera las tablas temporales de configuración. El gestor de operaciones pone el equipo en gestión y le envía la configuración temporal, la guarda en la memoria FLASH y se la pide de nuevo guardándola esta vez en las tablas principales de la base de datos. Finalmente, resetea el equipo para que arranque con la nueva configuración.

2. Actualización de la base de datos

El proceso **tmssynchro** se ejecuta en segundo plano y se encarga de realizar peticiones SNMP a los routers maestros definidos en la tabla **master** de la base de datos. De las respuestas obtiene el estado de los equipos en gestión y actualiza la base de datos con estos valores.

Cuando se inicia la aplicación **tmsmanager** comprueba que se esté ejecutando este proceso y, si no es así, da la opción de iniciarlo desde la propia aplicación.

Sólo es necesario que se ejecute un proceso **tmssynchro** en cada estación de gestión. Si se ejecutase más de uno supondría un perjuicio considerable de las prestaciones de la estación pero no causaría daños.

> ***NOTA: Proceso "tmssynchro".***
>
> ***Si este proceso no se ejecuta, la base de datos no se actualiza y el resto de aplicaciones que la consultan funcionarán de forma incorrecta.***

Además de este proceso, la actualización automática de algunas tablas es realizada por una serie de triggers (funciones que se lanzan cuando se producen ciertos eventos en la base de datos):

UPDATE_AUTO
UPDATE_GO_LOG
UPDATE_INFOMANAGED
UPDATE_MANCALLS
UPDATE_MANINFOMANAGED
UPDATE_MASTER
UPDATE_DEVICE

Para verificar que están todos instalados y funcionando se puede ejecutar el script **`$TELDATMS/etc/db/showtriggers.sql`**

3. Copias de seguridad

Para poder restaurar el contenido de la base de datos en el caso de que se produzca un fallo hardware o software que la dañe es conveniente realizar backups periódicos.

La estrategia a seguir en el mantenimiento de backups depende fuertemente del tipo de base de datos que se quiere salvaguardar, de las características de la estación en la que se gestiona y del tipo de uso que se hace de ella.

Considerando el funcionamiento típico de la gestión TMS, en lo que a la base de datos se refiere, en la referencia {Velpuri, 95} se recomienda seguir las siguientes reglas:

1. Hacer un backup físico off line cada vez que se produzca una actualización de aplicación de gestión.
2. Realizar exportaciones diarias en horas de poco uso (por ejemplo, por la noche).
3. Verificar dichas exportaciones al menos una vez por semana importando en una base de datos local de otra estación.
4. En función de la actividad de la base de datos, compactar las tablas realizando una exportación, borrado e importación una vez al mes o cada varios meses.

3.1. Backup físico off line de la base de datos

Un backup físico off line consiste en copiar todos los ficheros con la base de datos parada. Para ello seguir los siguientes pasos.

Primero, hay que identificar que ficheros es necesario salvaguardar. A tal efecto, se ejecutará el script **$TELDATMS/script/tmsfiles.sh** que produce como resultado el fichero **$TELDATMS/etc/db/OFFLINEBACKUP.FILES**. Editar dicho fichero para eliminar un par de líneas que no contienen nombres de fichero al comienzo y al final. Después añadir a dicho fichero los siguientes:

```
$ORACLE_HOME/initGEST.ora
$ORACLE_HOME/configGEST.ora
listener.ora
tnsnames.ora
```

A continuación, antes de parar la base de datos, es conveniente avisar a los usuarios que tengan una sesión abierta en la base de datos y parar todas las aplicaciones de gestión (tmssynchro incluido).

Para detener la base de datos ejecutar los comandos:

```
>svrmgrl
svrmgrl>connect internal
svrmgrl>shutdown immediate
```

Si todo ha ido bien, devuelve un mensaje indicando que la base de datos está detenida.

Entrar como usuario propietario del software ORACLE y hacer copia de los ficheros a cinta con el comando:

```
>tar cvf /dev/rmt/0m -I $TELDATMS/etc/db/OFFLINEBACKUP.FILES
```

Para arrancar de nuevo la base de datos:

```
svrmgrl>startup
```

3.2. Exportación de la base de datos

El script **$TELDATMS/script/tmsexportdb.sh** realiza una exportación de las tablas de la base de datos TMS al fichero **$TELDATMS/accounts/expdat.dmp**. Dicho script se puede lanzar desde un terminal o desde la aplicación de configuración con la opción **Base de Datos->Exportar**.

Hay varios tipos de exportaciones posibles: completa, por usuario o por tablas. Se ha decidido utilizar la exportación por usuario porque se considera la más apropiada en este caso.

La importación recomendada en caso de desastre consiste en ejecutar como usuario de gestión el comando:

```
> $TELDATMS/script/tmsimportdb.sh -drop
```

que destruye las actuales tablas de la base de datos (perdiendo los datos en uso) que son creadas de nuevo y compactadas en el proceso de importación de los datos del fichero **$TELDATMS/accounts/expdat.dmp**.

Si no se quieren perder los datos en uso ni destruir las tablas, puede utilizarse sin la opción **-drop**.

Si se dañan ficheros críticos de la base de datos será necesario recuperar del backup físico off line. En tal caso, se detendría la base de datos y se restaurarían los ficheros. Después, se realizaría una importación de los datos como se indicó anteriormente.

3.3. Backup de todos los datos de la gestión TMS

El script **$TELDATMS/script/tmsbackup.sh** realiza una exportación de toda la información de la base de datos perteneciente al usuario de gestión sobre el fichero **$TELDATMS/accounts/expdat.dmp** y, a continuación, almacena en un fichero **tar** el directorio **$TELDATMS/accounts** (en el que se encuentran los ficheros de estadísticos quincenales y el fichero destino de la exportación de la base de datos) y el **$TELDATMS/cfgs** (en el que se encuentran configuraciones de equipos que también pueden estar duplicadas en la base de datos). Dichos directorios no se almacenan con la ruta completa, sino relativa, para que puedan restaurarse en cualquier directorio. Puede lanzarse desde un terminal o desde la aplicación de configuración con la opción **Ficheros->Backup TMS**.

El script anterior está preparado para que, con ligeras modificaciones, después de almacenar todos los datos importantes en un fichero **tar**, lo envíe a la estación que se designe.

Una vez generado el fichero **tar** puede guardarse en cinta magnética con el siguiente comando root:

```
#cp $TELDATMS/accounts/tmsbackup.tar /dev/rmt/0m
```

3.4. Recuperación de los datos en caso de desastre

Para recuperar los datos en caso de desastre, proceder de la siguiente forma:

1. En función del origen de la restauración:

   1.1 Desde cinta magnética:

```
>cd $TELDATMS
>tar xvf /dev/rmt/0m
```

   1.2 Desde fichero:

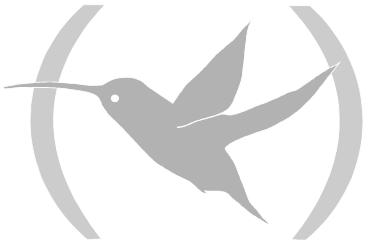
   Suponiendo que el fichero en cuestión es tmsbackup.tar:

```
>cp tmsbackup.tar $TELDATMS
>cd $TELDATMS
>tar xvf tmsbackup.tar
```

2. Importación de los datos de la base de datos:

```
>cd $TELDATMS/script
>tmsimportdb.sh -drop
```

Capítulo 8
Registro de sucesos



1. Registro de sucesos

Las distintas aplicaciones que constituyen el Centro de Gestión TMS envían mensajes de depuración, información y error a través del demonio **syslogd** de log del sistema con la facilidad **local7** y prioridades **debug**, **err** e **info**. El usuario puede configurar dicho demonio para que le presente en consola, le guarde en fichero o reenvíe a otra estación los mensajes que genera la aplicación. Por ejemplo, las siguientes líneas en el fichero "`/etc/syslog.conf`" ...

```
# Para log de TMS.
local7.debug   /dev/console
local7.info    /$TELDATMS/log/tms.log
local7.err     @sharon
```

... hacen que todos los mensajes sean presentados por consola, los mensajes de información y error se guarden en el fichero "`/$TELDATMS/log/tms.log`" y los mensajes de error se reenvíen a la estación "sharon".

Las aplicaciones encabezan sus mensajes con la siguiente estructura:

`TELDAT:<aplicación>(<display>)[<PID>]` donde <display> es el identificador de la estación en la que se está ejecutando la aplicación.

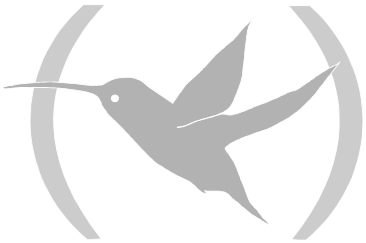
Como ejemplo, las siguientes líneas están tomadas de un fichero de log de la estación "cantabria":

```
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.
```

El nombre que sigue a "TELDAT:" es la aplicación que genera el mensaje y el número entre corchetes su identificador de proceso (PID).

Capítulo 9
Apéndices



1. Revisiones

1.1. Versión 1.0.0

Primera revisión de gestión TMS que gestiona equipos NOVACOM y NOVACOM-X25

1.2. Versión 1.1.0

Se introduce en la gestión TMS la posibilidad de gestionar routers Teldat C2.

1.3. Versión 1.2.0

Se introduce en la gestión TMS la posibilidad de gestionar routers Teldat C3.

1.4. Versión 1.2.1

Se introduce en la gestión TMS la posibilidad de gestionar el interfaz ASDP en los NOVACOM-X25.

1.5. Versión 1.3.0

Se introduce en la gestión TMS la posibilidad de gestionar routers Teldat C3B.

1.6. Versión 1.4.0

Se introduce en la gestión TMS el descubrimiento dinámico de direcciones IP.

1.7. Versión 1.5.0

Se introduce en la gestión TMS la posibilidad de gestionar routers Teldat C2-UP.

1.8. Versión 1.6.0

Se introduce en la gestión TMS la posibilidad de gestionar routers Teldat C4I.

1.9. Versión 1.7.0

Se introduce en la gestión TMS la posibilidad de gestionar routers Teldat C2B.

2. Formato de los ficheros de estadísticos quincenales

2.1. Equipos NOVACOM, NOVACOM-X25, Teldat C2B, Teldat C3B y Teldat C4i (RDSI)

La tabla de direcciones más visitadas se guarda en ficheros con extensión **fav** en campos con el siguiente formato

Campo	Tipo	Longitud	Descripción
Equipo	char19	19	Nº de teléfono asociado al router.
Fecha	char10	10	Día al que corresponden los estadísticos con formato “dd/mm/aaaa” en idioma español y "mm/dd/aaaa" en el resto de idiomas.
DirIP	char16	16	Dirección IP visitada.
Paquetes	int4	4	Tráfico total (paquetes) relacionado con la dirección anterior.

La tabla de tráfico por estación se guarda en ficheros con extensión **tra** con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Equipo	char19	19	Nº de teléfono asociado al router.
Fecha	char10	10	Día al que corresponden los estadísticos con formato “dd/mm/aaaa” en español y "mm/dd/aaaa" en el resto de idiomas.
DirIP	char16	16	Dirección IP de la estación.
RDSIB1_paquetes	int4	4	Tráfico total (paquetes) a través del canal B1 RDSI.
RDSIB2_paquetes	int4	4	Tráfico total (paquetes) a través del canal B2 RDSI.

La tabla de estadísticos globales se guarda en ficheros con extensión **wan** con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Equipo	char19	19	Nº de teléfono asociado al router.
Fecha	char10	10	Día al que corresponden los estadísticos con formato "dd/mm/aaaa" en español y "mm/dd/aaaa" en el resto de idiomas.
Hora	char8	8	Hora de la última grabación de estadísticos con formato "hh:mm:ss"..
RDSIB1_bytes	int4	4	Tráfico total a través del canal B1 RDSI (bytes).
RDSIB1_paquetes	int4	4	Tráfico total a través del canal B1 RDSI (paquetes).
RDSIB1_llamadas	int4	4	Nº total de llamadas a través del canal B1 RDSI.
RDSIB1_llamadas_ok	int4	4	Nº total de llamadas a través del canal B1 RDSI que tuvieron éxito.
RDSIB1_tiempo	int4	4	Tiempo total de conexión a través del canal B1 RDSI (segundos).
RDSIB2_bytes	int4	4	Tráfico total a través del canal B2 RDSI (bytes).
RDSIB2_paquetes	int4	4	Tráfico total a través del canal B2 RDSI (paquetes).
RDSIB2_llamadas	int4	4	Nº total de llamadas a través del canal B2 RDSI.
RDSIB2_llamadas_ok	int4	4	Nº total de llamadas a través del canal B2 RDSI que tuvieron éxito.
RDSIB2_tiempo	int4	4	Tiempo total de conexión a través del canal B2 RDSI (segundos).

En las dos primeras tablas pueden repetirse registros con la misma fecha (cambiando el "DirIP"), pero en la tercera cada registro se corresponde con un día.

Habrá un fichero secuencial de tipo ASCII asociado a cada tabla que cumplirá las siguientes condiciones:

1) Dentro de cada registro del fichero secuencial los campos deberán ir separados por el carácter '|' (barra vertical ASCII 124).
2) El separador de registros deberá ser un salto de línea.
3) Los campos dentro de cada registro deberán estar en el mismo orden en que se encuentren en las tablas anteriores.
4) La longitud de cada campo deberá ser menor o igual que el resultado de la conversión a ASCII del mayor valor de cada campo especificado en las tablas anteriores.
5) Un campo CHAR en blanco deberá ser representado en el fichero ASCII por cero o más blancos.

Ejemplo de dos registros de estadísticos diarios del router 911234567 para cada una de las tablas en español:

Direcciones más visitadas:

911234567|22/05/1997|192.6.1.102|34567
911234567|22/05/1997|192.6.1.32|23

Tráfico por estación:

911234567|22/05/1997|192.6.1.123|2345|4566
911234567|22/05/1997|192.6.1.1|265645|45

Estadísticos globales:

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. Equipos Teldat C2, Teldat C2-UP, Teldat C3 y Teldat C4i (ADSL)

La tabla de direcciones más visitadas se guarda en ficheros con extensión **fav** en campos con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Fecha	char10	10	Día al que corresponden los estadísticos con formato “dd/mm/aaaa” en idioma español y "mm/dd/aaaa" en el resto de idiomas.
DirIP	char16	16	Dirección IP visitada.
Bytes transmitidos	int10	10	Número de bytes transmitidos.
Bytes recibidos	int10	10	Número de bytes recibidos.
Paquetes transmitidos	int10	10	Número de paquetes transmitidos.
Paquetes recibidos	int10	10	Número de paquetes recibidos

La tabla de tráfico por estación se guarda en ficheros con extensión **tra** con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Fecha	char10	10	Día al que corresponden los estadísticos con formato “dd/mm/aaaa” en idioma español y "mm/dd/aaaa" en el resto de idiomas.
DirIP	char16	16	Dirección IP visitada.
Bytes recibidos	int10	10	Número de bytes recibidos.

Bytes transmitidos	int10	10	Número de bytes transmitidos.
Paquetes recibidos	int10	10	Número de paquetes recibidos
Paquetes transmitidos	int10	10	Número de paquetes transmitidos.

La tabla de estadísticos globales se guarda en ficheros con extensión **wan** con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Fecha	char10	10	Día al que corresponden los estadísticos con formato "dd/mm/aaaa" en español y "mm/dd/aaaa" en el resto de idiomas.
Hora	char8	8	Hora de la última grabación de estadísticos con formato "hh:mm:ss"..
Bytes recibidos	int10	10	Número de bytes recibidos.
Bytes transmitidos	int10	10	Número de bytes transmitidos.
Paquetes recibidos	int10	10	Número de paquetes recibidos
Paquetes transmitidos	int10	10	Número de paquetes transmitidos.
Exitos	int10	10	Número de conexiones establecidas con éxito.
Fracasos	int10	10	Número de conexiones fallidas

En las dos primeras tablas pueden repetirse registros con la misma fecha (cambiando el "DirIP"), pero en la tercera cada registro se corresponde con un día.

Habrá un fichero secuencial de tipo ASCII asociado a cada tabla que cumplirá las siguientes condiciones:

1) Dentro de cada registro del fichero secuencial los campos deberán ir separados por caracteres en blanco.
2) El separador de registros deberá ser un salto de línea.
3) Los campos dentro de cada registro deberán estar en el mismo orden en que se encuentren en las tablas anteriores.
4) La longitud de cada campo deberá ser menor o igual que el resultado de la conversión a ASCII del mayor valor de cada campo especificado en las tablas anteriores.
5) Un campo CHAR en blanco deberá ser representado en el fichero ASCII por cero o más blancos.

Ejemplo de dos registros de estadísticos diarios del equipo 172.24.75.2 para cada una de las tablas en español:

Direcciones más visitadas:

30/06/2000 192.6.1.5 222820 0 1301 0
30/06/2000 192.6.1.51 11500 0 44 0
Tráfico por estación:

04/07/2000 192.7.1.0 1682344 0 3889 0
04/07/2000 192.7.1.108 44292 44806 497 491

Estadísticos globales:

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. Formato de los ficheros de transacciones

La tabla de transacciones correctas se almacena en un fichero con extensión **".tok"** en campos con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Num. Trans.	int10	10	Número de transacción.
Tipo	char64	64	Tipo de transacción realizada.
Dirección IP	char16	16	Dirección IP llamada.
Red llamada	char16	16	Dirección de la red llamada.
Hora inicial	char8	08	Hora comienzo transacción.
Hora final	char8	08	Hora finalización transacción.
Fecha	char10	10	Fecha de la transacción
Red	int10	10	Entidad validadora de la transacción
Paquetes recibidos	int10	10	Número de paquetes recibidos

La tabla de transacciones erróneas se almacena en un fichero con extensión **".twg"** en campos con el siguiente formato:

Campo	Tipo	Longitud	Descripción
Num. Trans.	int10	10	Número de transacción.
Tipo	char64	64	Tipo de transacción realizada.
Dirección IP	char16	16	Dirección IP llamada.
Red llamada	char16	16	Dirección de la red llamada.
Causa	int10	10	Causa que provocó el error de la transacción
Hora inicial	char8	08	Hora comienzo transacción.
Hora final	char8	08	Hora finalización transacción.
Fecha	char10	10	Fecha de la transacción
Red	int10	10	Entidad validadora de la transacción
Paquetes recibidos	int10	10	Número de paquetes recibidos

Ejemplo de dos registros de transacciones del equipo 172.24.75.1 para cada una de las tablas en español:

Transacciones correctas:

|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

Transacciones erróneas:

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. Códigos y modelos de equipo

La gestión TMS gestiona los siguientes tipos de equipo:

Código	Funcionalidad	Versión de gestión
37	Equipo NOVACOM convencional	1.0.0 y posteriores
46	Equipo Teldat C2	1.1.0 y posteriores
51	Equipo NOVACOM con X.25 en lugar de RTC. Este equipo tiene la misma configuración que el 37 excepto la parte de RTC e incorpora tres nuevas entidades de configuración: XOT, X.25 y Nodo. Los estadísticos actualmente son los mismos que en el 37.	1.0.0 y posteriores
53	Equipo Teldat C3	1.2.0 y posteriores
57	Equipo Teldat C2B	1.7.0 y posteriores
59	Equipo Teldat C3-1	1.2.0 y posteriores
60	Equipo Teldat C3B	1.3.0 y posteriores
68	Equipo Teldat C4I	1.6.0 y posteriores
72	Equipo Teldat C2-UP	1.5.0 y posteriores

5. Causas de liberación RDSI

Es una indicación de la causa por la que se liberó la última llamada proporcionada por la red RDSI según la norma Q931 de ISO. Los posibles valores que pueden aparecer son:

0	Indefinido. Indica que no ha habido liberación todavía.
1	Número no atribuido.
3	No existe ruta hacia el destino.
6	Canal inaceptable.
16	Liberación normal de la llamada.
17	El usuario está ocupado.
18	El usuario no contesta.
19	El usuario ha sido avisado y no se recibe respuesta del mismo.
21	La llamada ha sido rechazada. A partir de la **versión 5.4.0** del equipo 37 y en todas las versiones del 51, cuando este recibe una llamada de gestión la rechaza y establece esta causa.
22	El número fue cambiado.
27	El número de destino está fuera de servicio.
28	El formato del número marcado no es válido.
31	Liberación normal.
34	No hay circuito o canal disponible.
38	La red se encuentra fuera de servicio.
41	Se ha producido un fallo temporal.
42	El equipo de conmutación se encuentra congestionado.
44	El circuito solicitado o el canal no están disponibles.
47	Los recursos no se encuentran disponibles en este momento.
49	La calidad del servicio no está disponible.
57	La capacidad de la portadora no está autorizada.
58	La capacidad de la portadora no está disponible actualmente.
63	La clase del servicio u otra opción no están disponibles.
65	La capacidad de la portadora no ha sido realizada.
66	El tipo de canal solicitado no se ha realizado.
79	El servicio u otra operación no realizados.
81	El valor de referencia de la llamada no es válido.
82	El canal identificado no existe.
88	El destino es incompatible con el origen.
95	Mensaje no válido.
96	Elemento de información obligatorio ausente.
97	Tipo de mensaje inexistente o no realizado.
98	Mensaje inexistente o no implantado.

99	Elemento de información inexistente o no realizado.
100	Contenido del elemento de información no válido.
101	Mensaje incompatible con el estado de la llamada.
102	Recuperación al expirar un temporizador.
111	Se ha producido un error de protocolo.
127	Interfuncionamiento.

Para identificar errores en la recogida automática de estadísticos se utiliza también este campo en la base de datos, pudiendo tomar en tal caso los siguientes valores.

500	Equipo gestionado por otra aplicación.
501	Ningún maestro accesible.
502	Time-out en petición SNMP al equipo después de estar accesible.
503	Versión de software no soportada.
504	Recogida de estadísticos interrumpida inesperadamente.
505	Error en recogida de estadísticos (bloques de datos corruptos).
506	Operación interrumpida por usuario.
507	Equipo inesperadamente desgestionado.
508	Operación aplazada (rebasada la hora de finalización).

6. Errores en las transacciones

Es una indicación de la causa por la que la transacción no se realizó de forma correcta. Los posibles valores que pueden aparecer son:

1	El NRI enviado por el datáfono no coincide con ninguno de los configurados
2	Desconexión recibida por parte del DEP
3	Operación inválida del datáfono
4	No se puede establecer conexión IP con el host
5	Finalización de la conexión TRMP
6	Finalización de la conexión TCP

7. Bibliografía

Código	Referencia
{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.