Teldat C

Menú rápido

Doc. *DM211* Rev. *6.0*
Abril, 2003

ÍNDICE

Capítulo 1
Introducción

1. Introducción

La gama de routers **TELDAT C** se compone de una familia de routers IP de propósito general con amplio espectro de aplicación: entornos personales, PYME y corporativos; por otro lado, gracias a su versatilidad, son adecuados para una gran variedad de escenarios IP: desde proporcionar acceso simultáneo a Internet a los usuarios de una red privada de área local hasta la adaptación a redes de teleproceso y soporte SNA, pasando por el soporte de terminales de puntos de venta (Datáfono).

La gama **TELDAT C** cubre las necesidades de acceso por ADSL, RDSI y línea serie (conexión a un módem telefónico externo, Frame Relay, X.25, PPP, etc.).

La versatilidad del router **TELDAT C** requiere una alta configurabilidad para poder adaptarse a las distintas necesidades y entornos, y por tanto, la cantidad de parámetros de configuración disponibles es muy extensa. Para facilitar el proceso de configuración y monitorización, los routers **TELDAT C** disponen de un entorno de configuración y monitorización reducido, adecuado para la mayoría de entornos PYME o personales. Dicho entorno, conocido como **configuración / monitorización rápida** o **menú rápido** es el objeto de este manual, y forma parte de una solución completa de gestión denominada **TMS** (Teldat Management System).

Figura 1.: Aspecto externo de los routers Teldat C

2. Características del router TELDAT C

Interfaces

- Interfaz Ethernet 10BaseT.
- (*) Interfaz WAN serie multinorma (V.24,V.35, X.21 y V.36) mediante drivers insertables.
- (*) Hasta 4 interfaces asíncronos para el soporte de terminales de puntos de venta.
- (*) Hasta 2 interfaces ADSL sobre POTS (Plain Old Telephone System).
- (*) Interfaz básico RDSI 2B+D.
- Interfaz de configuración RS-232.

(*) Interfaces disponibles según el modelo.

Funcionalidades

- NAT/PAT

  Permite la salida de un número ilimitado de puestos de una red de área local (LAN) a Internet simultánea e indistintamente, e impide la entrada desde el exterior a su red privada.

- Conectividad garantizada mediante mecanismos de backup (disponible según modelo).

  Si el interfaz principal no está disponible, la conectividad con el exterior queda garantizada al establecerse, de forma transparente, la comunicación por un canal alternativo (RDSI, línea telefónica). En cuanto el canal principal se recupera, se libera el canal alternativo.

- Filtrado IP

  Aumenta la seguridad de su red, impidiendo el acceso desde o hacia determinadas direcciones IP o puertos TCP/UDP.

- Encaminamiento automático de peticiones de DNS

  Le permite configurar como servidor DNS de su red el router ***TELDAT C***

- Servidor DHCP

  Le permite asignar las direcciones IP a su red de forma dinámica y controlada desde el propio ***TELDAT C***

- IPSec

  Cifre sus comunicaciones mediante el estándar de cifrado IP.

3. Modos de configuración y monitorización

Los routers ***TELDAT C*** ofrecen distintas vías de configuración y monitorización para adecuarse a las necesidades o preferencias de cada usuario. Las posibilidades son:

- Consola local, mediante la interfaz de línea de comandos.
- TELNET, mediante la interfaz de línea de comandos.
- Navegador de Internet, mediante interfaz gráfico accediendo al servidor Web incluido en el equipo.
- Gestor SNMP.

a) Mediante consola local

Para acceder a la interfaz de consola, debe conectar el ***TELDAT C*** al puerto serie de su ordenador personal o estación de trabajo y disponer un programa de emulación de terminal. Para realizar la conexión debe utilizar el adaptador RJ45Hembra-DB9Hembra y un cable de 6 hilos (un cable de LAN o RDSI le servirá).

La configuración del emulador de terminal debe ser 9600-8N1, es decir:

Velocidad de 9600 bps

Ocho bits de datos

Sin bit de paridad

Un bit de parada

Sin control de flujo (ni software ni hardware)

Si la conexión y configuración son correctas, le aparecerá el "prompt" del sistema; si el equipo tiene configurada clave de acceso, ésta le será solicitada antes de mostrarle el prompt.

```
Teldat              (c)1996 - 2001

Router model C2B 1 18 CPU MPC860      S/N: xxxx/xxxxx
1 LAN, 1 WAN Line 1 ISDN Line

*
```

b) Mediante consola remota vía TELNET

Si usted desea configurar remotamente y utilizar el interfaz de comandos en línea, puede utilizar una aplicación Telnet. En la mayoría de sistemas operativos se incluye una aplicación de cliente Telnet.

Para acceder al equipo deberá conocer la dirección IP del interfaz por el que vaya a acceder al equipo o la dirección IP interna (inicialmente, y dado que el router carecerá de configuración, puede acceder a la dirección 192.168.1.1 asignada por defecto a la interfaz de LAN del router).

Si tiene configurada clave de acceso por consola, ésta le será solicitada antes de poder acceder al equipo.

La dirección por defecto del interfaz de LAN es 192.168.1.1, excepto en aquellos casos en los que exista configuración por defecto dependiente de cliente y esté ésta activada.

c) Mediante Navegador de Internet

Los router ***TELDAT C*** disponen de un servidor WEB que hace posible su gestión mediante cualquier navegador de Internet. Para ello debe acceder con el navegador a la dirección: http://direccion_IP_del_equipo. El equipo le solicitará un nombre de usuario (**`teldat`**) y una clave (la de acceso por consola o la clave por defecto del servidor Web, **`teldatc`**)

La dirección por defecto de la interfaz de LAN es 192.168.1.1

Usuario y clave por defecto del servidor Web: **`teldat / teldatc`**

En caso de tener activada la configuración por defecto dependiente de cliente, la dirección IP, el usuario y la password pueden variar.

Para acceder al equipo deberá conocer la dirección IP de la interfaz por el que vaya a acceder al equipo o la dirección IP interna (inicialmente, y dado que el router carecerá de configuración, puede acceder a la dirección 192.168.1.1 asignada por defecto a la interfaz de LAN del router)

d) Mediante gestor SNMP

El protocolo SNMP es un estándar para la gestión de equipos de comunicaciones.

El router ***TELDAT C*** soporta las siguientes MIBs:

MIB-II estándar (System, Interfaces, IP, TCP, ADSL-LINE-MIB, etc)

MIB privada de configuración / monitorización rápida TeldatC-MIB

Otras MIBs privadas de Teldat

Para acceder al equipo mediante SNMP es necesario haber configurado previamente en el equipo (mediante consola local, Telnet o Web) la dirección IP de acceso SNMP y la comunidad asociada.

Capítulo 2
Configuración por línea de comandos

1. Acceso al menú

Este apartado describe las posibilidades de configuración del menú de configuración rápida. La configuración del equipo desde el menú de configuración rápida se realiza en tres etapas:

1. **Configurar los parámetros** deseados, mediante las órdenes del propio menú. En esta fase se configuran todos los parámetros deseados, como dirección IP de la LAN, etc.
2. **Generar y salvar la configuración** mediante el comando <MAKE> del menú de configuración rápida. En esta fase, el equipo toma como configuración válida la del menú de configuración rápida y guarda dicha configuración en la SRAM.
3. **Reiniciar** desde el menú general del equipo mediante el comando <RESTART> para que los valores configurados tomen efecto.

El comando* <MAKE> *borra toda la configuración* existente en el equipo y la regenera por completo a partir de la información contenida en el menú rápido; por tanto, cualquier modificación de la configuración realizada fuera de dicho menú, se perderá.

* Borra toda la configuración existente de aquellos aspectos configurables en el menú rápido (por ejemplo, no modifica la configuración del servidor FTP, la configuración de eventos, etc). Para realizar un borrado completo de la configuración utilice el comando <SET DEFAULT-CONFIGURATION> o configure el micro interruptor 5 a ON y realice un <RESTART>

Para acceder al menú de configuración rápida debe teclear <QUICK-CONFIGURATION> en el menú general de configuración:

```
*process 4
User configuration
Config>quick-configuration
Internet quick configuration
QUICK Config>
```

Para salir del menú de configuración rápida debe introducir el comando <EXIT> desde el propio menú de configuración rápida:

```
QUICK Config>exit
Config>
```

Para obtener el listado de opciones disponibles, introduzca el comando <?>

```
QUICK Config>?
ADD
CHANGE
CLEAR
DELETE
DISABLE
ENABLE
IPSEC Quick Menu
LIST
MAKE and save configuration
SAVE configuration
SET
POS Quick Menu
EXIT
Config>
```

2. Parámetros de acceso al equipo

Los equipos **TELDAT C** disponen de un sistema de control de acceso estándar basado en usuarios y passwords. Dicho control se aplica al acceso por consola local, Telnet, FTP y servidor Web.

Desde el menú rápido solo es posible configurar un único usuario, usuario que dispondrá de todos los permisos (gestión de usuarios, configuración, monitorización y eventos). Existe la posibilidad de no configurar el usuario, en cuyo caso, solo se solicitará el password; incluso puede no configurarse password, en cuyo caso, el acceso al equipo será libre (no se solicitará nada por consola/Telnet, en FTP bastará con indicar usuario "`root`" sin password y usuario "`teldat`" con password "`teldatc`" para el servidor Web interno).

Si se activa el mecanismo de configuración por defecto dependiente de cliente, el usuario y password necesarios dependerán de dicha configuración.

Para configurar el nombre de usuario dispone del comando `<SET USER>`, y para configurar el password de `<SET PASSWORD>`. Si quiere borrar el usuario o el password, simplemente debe configurarlos como vacíos. Siempre que configure el usuario se le solicitará el password.

Si borra el password se borrará automáticamente el usuario, pero no a la inversa, dado que puede querer un control basado únicamente en password.

```
Quick Config>set user
User (case insensitive, 31 characters maximum)[]? FREDDY
New password (31 characters maximum) : KRUGGER
Confirm password : KRUGGER

Quick Config>set password
New password (31 characters maximum) : KRUGGER
Confirm password : KRUGGER

Quick Config>
```

El nombre de usuario no distingue entre mayúsculas y minúsculas, mientras que en el password, dicha diferenciación sí se realiza.

3. Nombre asignado al equipo (hostname)

Es posible asignar un nombre al equipo que lo identifique. Ese nombre aparecerá delante de los distintos prompts de consola (una vez efectuado el MAKE de la configuración rápida). El comando utilizado para configurar un hostname es <SET HOSTNAME>.

```
Quick Config>set hostname
Host name (31 characters max)[]? gateway
Quick config>
```

Mediante el comando <LIST HOSTNAME> puede verse el hostname configurado. También se muestra éste al ejecutar <LIST USER> o <LIST PASSWORD>.

```
Quick config>list hostname

Host name : gateway
User :
Password :

Quick config>list user

Host name : gateway
User :
Password :

Quick config>list password

Host name : gateway
User :
Password :

Quick config>
```

4. Parámetros ADSL/ATM

Los parámetros ADSL se modifican mediante <SET ADSL> y son los siguientes:

```
Quick Config>set adsl
Type ADSL number(1..2)[1]?
Type max/min transmission rates ratio (1..200) [25]?
Type Open Mode:
 1. Multimode
 2. G.Lite [1]?
Quick Config>
```

- **ADSL number**

  En el caso de que su equipo disponga de más de un interfaz ADSL, se le solicitará el identificador del interfaz ADSL que desea configurar.

- **Max/min transmission rates ratio**

  Un interfaz ADSL puede contener múltiples conexiones ATM, cada una con una velocidad de transmisión distinta: este parámetro indica la relación entre la velocidad más alta que se va a configurar en una conexión ATM sobre ADSL y la más baja. La velocidad más alta coincide con la velocidad de la línea ADSL (que puede variar dependiendo de las condiciones de la línea).

  Por ejemplo, tomando el valor por defecto y una velocidad de línea de 1024 Kbps, la conexión ATM configurable de menor velocidad sería de 1024Kbps/25 = 41 Kbps.

- **Open mode**

  La interfaz ADSL permite dos modos de funcionamiento: el denominado *multimodo*, en el que el equipo se ajusta al modo de funcionamiento del equipo de la central telefónica y el modo *G.Lite*, un modo de potencia reducida y velocidades también menores.

  El valor por defecto es *multimodo*.

Para listar los valores configurados se dispone del comando <LIST ADSL>

```
Quick Config>list adsl

--- ADSL line parameters ---

 Id    Max/min ratio    Mode
-----  ------------ ----------
ADSL1       25       MULTIMODE
ADSL2      200       G.LITE

Quick Config>
```

5. Parámetros SNMP

Los parámetros SNMP solo son necesarios para acceder a la configuración, monitorización y generación de alarmas a través del protocolo SNMP.

Las peticiones SNMP pueden ir dirigidas a cualquier dirección IP configurada.

Los parámetros SNMP se configuran mediante el comando **<SET SNMP>** y son los siguientes:

```
Quick Config>set snmp
Type community (0 (zero) to clear)[]? manager
Type traps level (1-NONE 2-LOW 3-MEDIUM 4-HIGH) [1]? 4
Type traps IP destination address  [0.0.0.0]? 192.6.1.154
Type mask [255.255.255.0]? 255.255.255.0
Check if manager is reachable before sending traps
0 – No
1 – Yes UDP
2 – Yes ICMP
[1]?2
Quick Config>
```

- **Community**

  Nombre de la comunidad SNMP de gestión. La comunidad que se genere con este nombre poseerá los permisos READ, WRITE y TRAP, es decir, el gestor, podrá leer y escribir variables SNMP, además de recibir traps.

  Por defecto está configurada la comunidad "public" con permiso READ sobre la MIB II únicamente; esta comunidad no puede ser eliminada desde la configuración rápida.

- **Traps level**

  Se puede establecer uno de los cuatro niveles de traps definidos.

  - **NONE:** No se envían traps.
  - **LOW:** Se envían las traps genéricas siguientes:

    ```
    Cold Restart
    Warm Restart
    Link Down
    Link Up
    Authentication Failure
    ```

    y las "Enterprise Specific" definidas como ERROR:

    ```
    UI-ERROR
    CI-ERROR
    UE-ERROR
    CE-ERROR
    ```

  - **MEDIUM:** las traps LOW junto con las "Enterprise Specific" definidas como U-INFO
  - **HIGH:** las traps MEDIUM junto con las "Enterprise Specific" definidas como C-INFO.

- **Traps IP destination address / Mask**

  Estos parámetros determinan la dirección IP destino de traps y controlan el acceso al agente SNMP (solo se permite la gestión desde aquellos gestores SNMP cuya dirección IP coincide con la subred definida por estos campos).

  Si la dirección destino de traps es 0.0.0.0 no se envían traps.

- **Check if manager is reachable before sending traps**

  Por defecto, los equipos Teldat C realizan una petición de ECHO UDP a la estación destinataria de las traps para comprobar que éstas tienen garantías de llegar a dicha estación. Si se configura a NO, dicha comprobación no se realizará. La accesibilidad a la estación receptora de traps puede comprobarse también mediante ECHO ICMP (ping).

La configuración rápida permite una única dirección destino de traps. Si se deseara más de una dirección de traps o más de una comunidad o definir vistas específicas para una comunidad, se deberá utilizar el menú general de configuración SNMP.

6. Parámetros DHCP

El router **TELDAT C** ofrece la posibilidad de actuar como servidor DHCP o como agente "relay" DHCP. Los parámetros DHCP se configuran mediante el comando **<SET DHCP>**

a) Servidor DHCP

Mediante el servidor DHCP, el router **TELDAT C** se encarga de asignar dinámicamente direcciones IP (además de otros parámetros de configuración) a los clientes DHCP que, generalmente, se encuentran en su LAN.

Cuando se opera con el servidor DHCP, el router asigna dinámicamente las direcciones a los clientes. El servidor DHCP cede las direcciones IP durante un periodo de tiempo programable. Si transcurrido ese tiempo no se ha renovado la dirección, ésta queda disponible para que el servidor DHCP la asigne a cualquier cliente que realice una petición DHCP.

Es importante asegurarse de que no existen varios servidores DHCP en la misma LAN, porque si más de un servidor DHCP se encuentra asignando direcciones en la misma red local puede llegar a generar conflictos de direcciones.

Para configurar el **Servidor DHCP** es necesario indicar los parámetros siguientes, como se muestra en este ejemplo:

```
Quick Config>set dhcp
Select DHCP protocol service (0-NONE 1-RELAY 2-SERVER) [0]? 2
Type start IP range [0.0.0.0]? 192.168.1.2
Type end IP range [0.0.0.0]? 192.168.1.254
Type subnet mask [0.0.0.0]? 255.255.255.0
Type default router address [0.0.0.0]? 192.168.1.1
Type DNS server [0.0.0.0]? 195.53.0.2
Type lease time in minutes (1..525600) [720]? 720
Quick Config>
```

- **Start IP range / End IP range**
  Rango de direcciones IP que el servidor DHCP irá asignado a los clientes DHCP. El rango se especifica mediante las direcciones IP inicial y final (ambas quedan incluidas dentro del rango y podrán ser asignadas).

- **Subnet mask**
  Configura la máscara de subred del cliente DHCP.

- **Default router address**
  Dirección IP del router por defecto que utilizará el cliente DHCP.

- **DNS server**
  Dirección IP del servidor DNS que empleará el cliente DHCP para la resolución de nombres.

- **Lease time in minutes**
  Tiempo durante el que se cede la dirección IP: si transcurrido dicho tiempo no se ha renovado la dirección, ésta queda disponible para que el servidor DHCP la asigne a cualquier cliente que realice una petición DHCP.

Utilizando el comando **<LIST DHCP>** se puede observar la configuración actual del protocolo DHCP en el equipo:

```
Quick Config>list dhcp

--- DHCP Configuration ---
DHCP service : Server
IP address range : 192.168.1.1 - 192.168.1.254
Subnet mask : 255.255.255.0
Default router : 192.168.1.1
DNS server : 195.53.0.2
Lease time : 720 min.

Quick Config>
```

b) Agente Relay DHCP

En el caso de Agente Relay DHCP, el router se encarga de capturar los mensajes DHCP generados por los posibles clientes que están conectados en la LAN y enviarlos a un servidor DHCP conocido que está situado fuera de la LAN, al que, de otro modo, no llegarían las peticiones debido a que las peticiones de los clientes DHCP se realizan mediante datagramas IP tipo *broadcast* y éstos, no se encaminan.

En el siguiente ejemplo se muestra cómo configurar el agente Relay DHCP y cómo se visualiza el estado del protocolo DHCP en este caso:

```
Quick Config>set dhcp
Select DHCP protocol service (0-NONE 1-RELAY 2-SERVER) [0]? 1
Type primary DHCP server address [0.0.0.0]? 203.34.5.67
Type secondary DHCP server address [0.0.0.0]? 0.0.0.0

Quick Config>list dhcp

--- DHCP Configuration ---
DHCP service : Relay
Primary server : 203.34.5.67
Secondary server : 0.0.0.0

Quick Config>
```

- **Primary DHCP server address**
  Dirección IP del servidor DHCP al que se enviarán las peticiones de los clientes.
- **Primary DHCP server address**
  Dirección IP de un segundo servidor DHCP al que se enviarán las peticiones de los clientes (opcional).

7. Parámetros DNS

Para traducir direcciones IP en formato alfanumérico, que son fáciles de entender, por ejemplo "www.teldat.es" a direcciones IP en formato numérico, que son las que realmente usan los equipos, por ejemplo 195.53.0.2, el protocolo IP dispone de un servicio de nombres de dominio DNS. Mediante el servicio de DNS, los equipos finales, por ejemplo PCs, realizan peticiones DNS a servidores DNS. En dichas peticiones generalmente se solicita la traducción de un nombre en formato alfanumérico a una dirección IP en formato numérico, pero también se pueden solicitar más cosas, como información de cuentas de correo, etc.

En un entorno de utilización del router **TELDAT C**, las redes externas a las que se conecta pueden disponer de servidores DNS para resolver las peticiones DNS de los puestos finales. El ejemplo más claro es Internet, ya que todos los proveedores de Internet ofrecen servidores DNS a sus usuarios. Pero el servicio de DNS no es exclusivo de Internet, sino que puede ofrecerse en cualquier red IP privada o en cualquier Intranet.

El router **TELDAT C** dispone de una funcionalidad de encaminamiento de las peticiones DNS que reciba de los puestos de la LAN, siendo posible definir hasta tres servidores DNS en el router, de tal forma que las peticiones DNS que el router reciba de los equipos de la red local, las reenvía a los servidores que tenga configurados, en el orden en que están configurados. Esta funcionalidad se denomina *DNS proxy*.

Con esta funcionalidad, es posible configurar como servidor DNS de los puestos locales los servidores dados por el proveedor de la red externa (por ejemplo Internet) o bien configurar como servidor DNS la dirección IP del router en la LAN y agregar los servidores DNS al propio router. Esta última es la solución recomendada, pues implica una configuración centralizada más simple, en la que si se cambia de proveedor no es necesario reconfigurar todos los puestos, sino solamente el router. Además el tratamiento de los reintentos de las peticiones DNS en un entorno con varios servidores DNS puede ser mejor en el router que en ciertas implementaciones del protocolo IP de algunos fabricantes.

Lo normal será configurar en primer lugar el servidor DNS primario y en segundo el servidor DNS secundario. Ambos son datos del proveedor del servicio.

Si se configuran servidores DNS para más de una red externa conviene recordar que el router sigue un orden secuencial en la resolución de las consultas, primero al primer servidor configurado, luego al segundo servidor y luego al tercero, independientemente de las redes externas a las que dichos servidores pertenezcan; no habiendo manera de saber a priori a qué red externa pertenece una determinada dirección IP en formato alfanumérico. Por ello, el router podría llegar a realizar accesos por otros circuitos alternativos antes de utilizar el adecuado para intentar acceder a unos servidores que no van a saber resolver la petición, si son servidores DNS de una red externa diferente a la de la petición. Por lo tanto se recomienda no agregar servidores DNS de más de una red externa para evitar accesos a circuitos y retardos innecesarios.

Para agregar un servidor DNS se debe teclear `<ADD DNS>`:

```
Quick Config>add dns
Type DNS server IP address  [0.0.0.0]? 193.152.63.197
Quick Config>
```

En el ejemplo se ha agregado el servidor DNS 193.152.63.197.

Para listar los servidores DNS configurados se debe teclear <LIST DNS>:

```
Quick Config>list dns


--- DNS Servers ---

Ix DNS Server Address
-- ------------------
1  193.152.63.197

Quick Config>
```

Para borrar un servidor DNS se debe teclear <DELETE DNS>:

```
Quick Config>delete dns
Type index of DNS server to delete [0]? 1
Quick Config>
```

8. Parámetros RDSI

Los parámetros RDSI se modifican mediante **<SET ISDN>** y son los siguientes:

```
Quick Config>set isdn
B Channel: [1]?1
Permanent ISDN channel (Yes/No)(N)? N
Enable incoming calls (Yes/No)(N)? y
Authorized Calling number  []? 123456789
Quick Config>
```

- **B Channel**

  El interfaz básico RDSI tiene dos canales configurables: canal 1 y canal 2.

La configuración refleja canales lógicos, no canales RDSI físicos, dado que la asignación del canal B1 o el B2 la realiza la red y no el equipo.

- **Permanent ISDN channel**

  Si 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 realiza llamadas RDSI y siempre está conectado. Si habilita un canal B como permanente, los parámetros "`call number`" y "`PPP release time`" de la conexión IP basada en RDSI, los controles horarios y la configuración de retrollamada o *callback* no tendrán sentido en dicha conexión. En la contratación del canal B permanente se especifica qué canal B (B1, B2 o ambos) responde a este perfil.

- **B1 + B2 connection**

  Si se quiere ampliar el ancho de banda disponible en un canal, 64Kbits, se puede unir los anchos de banda de los dos canales(128Kbits), siempre y cuando ambos canales estén contratados como permanentes.

```
Quick Config>set isdn
B Channel: [1]?
Permanent ISDN channel (Yes/No)(N)? Y
B1 + B2 connection (Yes/No)(N)? Y
Quick Config>
```

- **Enable incoming calls**

  El router, por defecto, no permite las llamadas entrantes. Con este parámetro se puede habilitar las llamadas entrantes.

- **Authorized Calling number**

  Con este parámetro se puede restringir las llamadas entrantes a un número de teléfono, si este parámetro se deja a 0 cualquier llamada entrante será respondida. **Esta funcionalidad está desactivada y su configuración no tendrá efecto (como si se configurara a 0).**

Se puede ver la configuración de los parámetros RDSI con el comando <LIST ISDN>.

```
Quick Config>list isdn

--- ISDN parameters ---
Channel    Type     Incoming Calls  Auth Caller
-------  ---------  --------------  ------------
B1       Permanent  -------         -------
B2       Switched    Enabled        123456789

Quick Config>
```

9. Parámetros WAN

Los parámetros de la línea serie (WAN) se modifican mediante <SET WAN> y son los siguientes:

```
Quick Config>set wan
WAN identifier[1..3]?1
WAN mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 5-X25
[1]? 1
Line speed (bps): [57600]?
Quick Config>
```

Ejemplo de configuración AT o línea asíncrona.

```
Quick Config>set wan
WAN identifier[1..3]?1
WAN mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 5-X25
 [1]? 2
Line speed (bps): [57600]?
TCP port (1-65535): [34]?
Flow Control:
 1-HW
 2-XON/XOFF: [1]?
Quick Config>
```

Ejemplo de configuración ASDP.

```
Quick Config>set wan
WAN identifier[1..3]?1
WAN mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 5-X25
 [1]? 3
Line speed (bps): [9600]?
Quick Config>
```

Ejemplo de configuración POS.

```
Quick Config>set wan
WAN identifier[1..3]?1
WAN mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 5-X25
[1]? 5
Line speed (bps): [57600]?
Activate XOT(Yes/No)(N)?
Quick Config>
```

Ejemplo de configuración X.25.

- **WAN identifier**
  Si su equipo dispone de más de una línea WAN, se le solicitará el identificador de la línea WAN que desea configurar.

- **WAN mode**
  La línea WAN se puede configurar de cinco modos.
  AT commands: configuración para soporte de comandos AT (módem externo).
  ASDP: Permite acceder a la línea serie mediante una conexión TCP.
  POS: Modo para conectar a la línea serie un TPV (Terminal Punto de Venta).
  Async line: Configuración como línea serie asíncrona para PPP.
  X25: configura la línea para soporte de X25.

- **Line speed**
  Velocidad en bps de la línea serie. Máximo 2048000 bps.

- **TCP port** (sólo ASDP)
  Puerto TCP al cual se podrá acceder para tener conectividad con la interfaz serie.

- **Flow Control** (sólo ASDP)
  HW: Control de flujo Hardware.
  XON/XOFF: Control de flujo XON/XOFF.

- **Activate XOT** (sólo X.25)
  Si configura esta opción así, al realizar el <MAKE> se creará un interfaz XOT en el caso de que no exista, y si existe, se respetará el interfaz XOT.

***Si configura una WAN en X25 y ésta ya está así configurada, la configuración no se perderá al realizar el* <MAKE>.**

Se puede consultar la configuración de los parámetros WAN con el comando <LIST WAN>.

```
Quick Config>list wan

--- WAN parameters ---
 Id    Mode Line Speed  TCP Port    Flow Cntrl    Xot Active
----   ---- ----------  --------  -------------  ------------
WAN1   ASDP 57600       34        HW             ---

Quick Config>
```

10. Parámetros UART

Los parámetros de la línea serie asíncrona (UART) se modifican mediante <SET UART> y son los siguientes:

```
Quick Config>set uart
UART identifier(1..4): [1]?
UART mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 [1]? 1
Line speed (bps): [57600]?
Quick Config>
```

Ejemplo de configuración AT o línea asíncrona

```
Quick Config>set uart
UART identifier(1..4): [1]?
UART mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 [1]? 2
Line speed (bps): [57600]?
TCP port (1-65535): [34]?
Flow Control:
 1-HW
 2-XON/XOFF: [1]?
Quick Config>
```

Ejemplo de configuración ASDP.

```
Quick Config>set uart
UART identifier(1..4): [1]?
UART mode:
 1-AT commands (PSTN)
 2-ASDP
 3-POS
 4-Async line
 [1]? 3
Line speed (bps): [9600]?
Quick Config>
```

Ejemplo de configuración POS.

- **UART identifier**

  En el caso de que su equipo disponga de más de un interfaz de tipo UART, se le solicita el identificador de la UART que desea configurar.

- **UART mode**

  La línea UART se puede configurar de cuatro modos:

  AT commands: configuración para soporte de comandos AT (módem externo).

  ASDP: Permite acceder a la línea serie mediante una conexión TCP.

  POS: Modo para conectar a la línea serie un TPV (Terminal Punto de Venta).

  Async line: Configuración como línea serie asíncrona para PPP.

- **Line speed**
  Velocidad en bps de la línea serie. Máximo 115200 bps.

- **TCP port** (sólo ASDP)
  Puerto TCP al cual se podrá acceder para tener conectividad con la interfaz serie.

- **Flow Control** (sólo ASDP)
  HW: Control de flujo Hardware. (No disponible si basado en interfaces UART)
  XON/XOFF: Control de flujo XON/XOFF.

Se puede consultar la configuración de los parámetros UART con el comando `<LIST UART>`

```
Quick Config>list uart

--- UART parameters ---
 Id     Mode Line Speed  TCP Port    Flow Cntrl
-----   ---- ----------  --------  -------------
UART1   AT   57600       --        --

Quick Config>
```

Los interfaces UART no disponen de señales para realizar el control de flujo, por tanto, en el caso de comandos AT, se requiere la activación de control de flujo por software del tipo XON/XOFF; en la mayoría de los casos el comando AT necesario para activar en el módem el control XON/XOFF es &K6, valor que se configura por defecto: si el módem conectado al equipo requiere un comando distinto, deberá configurar manualmente el valor de dicho comando en la configuración normal. Además, se configurará el ACCM (Asynchronous Control Character Map) del nivel LCP de PPP a 000A0000 para que el extremo remoto realice la transparencia a los caracteres XON y XOFF como mínimo.

11. Parámetros RTC

Los parámetros de RTC sólo se pueden configurar sobre aquellos interfaces de tipo WAN o UART configurados en modo "AT commands", y se configuran mediante <SET PSTN>:

```
Quick Config>set pstn
Interface:
 1 - WAN
 2 – UART
[1]? 1
WAN identifier[1..3]?:1
Enable incoming calls (Yes/No)(N)? y
Do you want to enable ring pattern detection (Yes/No)(N)? y
Number of tones[2]?
Silence duration[8]?
Local telephone[]? 123456789
Quick Config>
```

- **Interface**

  En el caso de que su equipo disponga de interfaces de tipo WAN y UART, se le solicitará el tipo de interfaz al que se aplicarán los parámetros aquí definidos.

- **WAN/UART identifier**

  Si su equipo dispone de más de un interfaz de tipo WAN o UART, se le solicitará el identificador del interfaz.

- **Enable incoming calls**

  El router por defecto no permite las llamadas entrantes. Con este parámetro se puede habilitar las llamadas entrantes.

- **Do you want to enable ring pattern detection?**

  Ante la imposibilidad de conocer el número llamante en una línea telefónica analógica se puede configurar la detección de un patrón de llamada para no procesar las llamadas entrantes que no cumplan ese patrón.

- **Number of tones:**

  Número de tonos del patrón de llamada.

- **Silence duration:**

  Duración de los silencios del patrón de llamada.

- **Local telephone:**

  Número de teléfono del abonado.

Se puede consultar la configuración de los parámetros RTC con el comando <LIST PSTN>.

```
Quick Config>list pstn

--- PSTN parameters ---
Itfc   Inc Calls  Ring Pattrn   Tones   Silence  Loc. Telephone
-----  ---------  -----------  -------  -------  --------------
WAN1    Enabled    Enabled       02       08       123456789

Quick Config>
```

Es importante asegurarse de que la línea serie (interfaz WAN o UART) esté configurada en modo AT y con la velocidad adecuada al MODEM externo que se utilice.

12. Dirección IP Interna

La dirección IP Interna se configura con el comando <SET INTERNAL-IP-ADDRESS>

```
Quick Config>set internal-ip-address
Internal IP address [0.0.0.0]? 192.168.101.1
Quick Config>
```

La configuración se puede consultar con el comando <LIST INTERNAL-IP-ADDRESS>.

```
Quick Config>list internal-ip-address

Internal IP address: 192.168.101.1

Quick Config>
```

Para borrar la dirección IP interna es suficiente con configurar la dirección 0.0.0.0 como dirección IP interna.

```
Quick Config>set internal-ip-address
Internal IP address [0.0.0.0]? 0.0.0.0
Quick Config>
```

13. Dirección origen de traps (dirección de gestión)

La dirección de gestión o dirección origen con que saldrán las traps (management IP address) se configura mediante el comando <SET MANAGEMENT-IP-ADDRESS>. Esta dirección es tratada de forma similar a la dirección IP interna, y asimismo puede ser utilizada para identificar un determinado equipo.

```
Quick Config>set managemet-ip-address
Management IP address [0.0.0.0]? 192.168.200.1
Quick Config>
```

La configuración se puede consultar con el comando <LIST MANAGEMENT-IP-ADDRESS>.

```
Quick Config>list managemet-ip-address

Management IP address: 192.168.200.1

Quick Config>
```

Para borrar la dirección de gestión es suficiente con asignar a esta dirección el valor 0.0.0.0.

```
Quick Config>set management-ip-address
Management IP address [0.0.0.0]? 0.0.0.0
Quick Config>
```

O bien se puede emplear el comando <DELETE MANAGEMENT-IP-ADDRESS>.

```
Quick Config>delete managemet-ip-address
Do you want to delete the management IP address(Yes/No)(N)? y
Quick Config>
```

14. Parámetros de los circuitos ATM

Los parámetros de los circuitos AAL-ATM se configuran con el comando <ADD AAL-ATM>

```
Quick Config>add aal-atm

Type AAL-ATM connection identifier (1-99) [0]? 1
ADSL identifier[1..2]?1
Type VPI (0-255) [0]? 5
Type VCI (32-65535) [0]? 40
Select multiplexation method (VC=1, LLC=2) [1]?
Select category (CBR=2, VBR_RT=3, VBR_NRT=4, UBR=6) [6]?
Type transmission PCR (in kbps) [1000]?
Quick Config>
```

- **AAL-ATM connection identifier (1-99)**

  Identificador del circuito AAL-ATM.

  Este parámetro permite identificar en otros puntos de la configuración una conexión AAL-ATM determinada.

- **ADSL identifier**

  En el caso de que su equipo disponga de más de un interfaz ADSL, se le solicitará el interfaz sobre el que se desea configurar la conexión.

- **Type VPI (0-255)**

  Con este parámetro configuramos el Virtual Path Identifier.

  El rango es de 0 a 255.

- **Type VCI (32-65535)**

  Con este parámetro configuramos el Virtual Channel Identifier.

  El rango es de 32-65535.

- **Select multiplexation method (VC=1, LLC=2)**

  Con este parámetro podemos elegir entre dos métodos de multiplexación de la conexión: Virtual Channel (VC) o Logical Link Control (LLC)

- **Select category (CBR=2, VBR_RT=3, VBR_NRT=4, UBR=6) [6]?**

  Esta opción selecciona el tipo de tráfico ATM que se va a utilizar en esta conexión. Estas categorías de tráfico tienen distinta prioridad y características de transmisión sean en tiempo real o no lo sean. De este modo, CBR y VBR_RT tienen más prioridad que VBR_NRT y UBR.

  - **UBR:** Unspecified Bit Rate.

    Se genera en transmisión un tráfico con un límite superior determinado por el parámetro PCR y un límite inferior determinado por el ancho de banda no utilizado por otras conexiones o disponible en la interfaz física.

- **CBR:** Constant Bit Rate.

  Se genera en transmisión un tráfico de tasa constante. El valor de esta tasa en Kbits por segundo se configura con el parámetro PCR.

  PCR: Peak cell Rate, en Kbps.

- **VBR_RT / VBR_NRT:** Variable Bit Rate, Real Time o No Real Time.

  Se genera en transmisión un tráfico de tasa variable y caracterizado por los parámetros: PCR, SCR y MBS.

  PCR: Peak Cell Rate, en Kbps.

  Velocidad máxima permitida para las ráfagas de transmisión de datos.

  SCR: Sustained Cell Rate, en Kbps.

  Velocidad máxima permitida para un tráfico sostenido.

  MBS: Maximum Burst Size, en celdas ATM

  Tamaño máximo de las ráfagas en número de celdas.

Todos los parámetros, a excepción del identificador de conexión AAL, son datos que debe proporcionarle su proveedor de acceso ADSL y cuya correcta configuración es fundamental para el establecimiento de la conexión de datos.

Para consultar la configuración de los parámetros de los circuitos ATM AAL dispone del comando <LIST AAL-ATM>

```
Quick Config>list aal-atm

--- AAL-ATM Connections ---

Ident Interf. VPI VCI   Mx  Category PCR   MBS   SCR
----- ------- --- ----- --- -------- ----- ----- -----
ATM1  ADSL1   5   40    VC  UBR      1000

Quick Config>
```

Para eliminar una conexión específica debe que usar el comando <DELETE AAL-ATM> indicando el identificador de la conexión que se desea eliminar.

También es posible modificar una conexión AAL-ATM con <CHANGE AAL-ATM>, aunque con este comando es imposible modificar el identificador de conexión.

Para eliminar todas las conexiones definidas se puede usar el comando <CLEAR AAL-ATM>, que exige que el usuario confirme su ejecución.

Cuando se elimina una conexión AAL-ATM se eliminan también, de forma automática, todas las conexiones IP asociadas, así como todas las rutas de salida por alguna de las conexiones IP anteriores.

Se ha limitado el número de conexiones AAL-ATM que se pueden definir simultáneamente a cinco.

15. Parámetros de las conexiones IP

En puntos anteriores se han configurado los interfaces físicos del equipo, y ahora es el momento de configurar los parámetros del protocolo IP. Dado que a nivel IP todos los interfaces son iguales, la configuración se ha concentrado en lo que denominaremos "conexiones IP" y que le permiten, de una forma centralizada, configurar dichos parámetros.

Las conexiones IP pueden configurarse sobre cualquiera de los interfaces disponibles en el equipo, es decir, una conexión IP podrá estar asociada al interfaz Ethernet (LAN), a los canales B del acceso básico RDSI (B1 y B2), a la conexión por módem (PSTN o RTC) o a una conexión AAL-ATM.

El comando para añadir una conexión IP es `<ADD IP>`.

El comando para modificar una conexión IP es `<CHANGE IP>` y para borrarla `<DELETE IP>`. Para eliminar todas las conexiones IP definidas se puede usar el comando `<CLEAR IP>`, que exige que el usuario confirme su ejecución.

a) Conexiones IP LAN:

Se utiliza para configurar direcciones del interfaz LAN.

```
Quick Config>add ip
Type IP connection identifier (1-99) [0]? 1
Underlying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.WAN
 5.UART [1]? 1
Type local IP address [0.0.0.0]? 192.168.101.10
Type subnet mask [255.255.255.0]?
Do you want to enable NAPT (Yes/No)(N)?Y
Type NAPT peer address [0.0.0.0]? 192.168.101.17
Type NAPT entries duration (1-240 min.) [5]? 25
Type description []? Conexion LAN
Quick Config>
```

- **IP connection identifier (1-99)**
  Identificador de la conexión IP, el rango es 1 a 99.

- **Underlying Connection Type**
  Interfaz base de la conexión IP.

- **Local IP address / Subnet Mask**
  Dirección IP de la interfaz y máscara de red.

- **Do you want to enable NAPT (Yes/No)**
  Habilita o deshabilita la facilidad NAPT.

- **NAPT peer address**

  Dado que la LAN es una red multipunto, necesita indicar con qué destino desea realizar NAPT. Sólo tiene sentido si el parámetro anterior se ha configurado a "sí".

- **NAPT entries duration (1-240 min.)**

  Este parámetro se configurará si se ha habilitado la facilidad NAPT.

  Duración en la caché del router de la entrada del puerto visible sin tráfico.

- **Description:**

  Cadena de caracteres para describir una conexión IP.

b) Conexiones IP RTC:

Se utiliza para configurar una conexión punto a punto (PPP) por RTC utilizando una línea WAN o UART y un módem externo que acepte comandos AT.

```
Quick Config>add ip
Type IP connection identifier (1-99) [0]? 2
Underlaying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.WAN
 5.UART [1]? 4
Type WAN identifier (1..2) [1]?
Type local IP address [0.0.0.0]? 192.168.102.10
Type subnet mask [255.255.255.0]?
Do you want to enable NAPT (Yes/No)(Y)? N
Type user  []? userTeldat
Type password  : ******
Confirm password  : ******
Call Number  []? 123456789
Select Remote Authentication Protocol: None(1), PAP(2), CHAP(3)[1]? 2
Type user  []? papUser
Type password  : ***
Confirm password  : ***
Type PPP release time (0 - 65535)s [0]? 60
Type description []? Conexion PPP por RTC
Quick Config>
```

En el caso de conexiones IP en modo PPP con asignación dinámica de dirección, debe configurar con una dirección cualquiera válida que será cambiada por la dirección negociada cuando se establezca la sesión PPP.

- **WAN/UART identifier**

  En el caso de que su equipo disponga de más de un interfaz de tipo WAN o UART, se le solicitará el identificador del interfaz sobre el que desea definir la conexión.

- **User**

  Al utilizar PPP es posible que el extremo remoto pida un usuario y password para poder realizar la conexión. Con este parámetro se configura el usuario.

- **Password**

  Con este parámetro se configura el password que nos pedirá el extremo remoto para permitir la conexión.

- **Call Number**

  El número de teléfono del extremo remoto.

- **Select Remote Authentication Protocol: None(1), PAP(2), CHAP(3)**

  Se puede configurar un protocolo de autenticación (PAP o CHAP) que exigirá al extremo remoto un usuario y un password para conectarse.

  El usuario y el password que se pide a continuación son los que deberá proporcionar el extremo remoto para realizar la conexión.

- **PPP release time (0 - 65535) s**

  Con este parámetro se configura el tiempo que permanece la conexión PPP establecida cuando no hay tráfico. **Este parámetro solo aplica en el caso de conexiones conmutadas y no en el caso de permanentes**.

c) Conexiones IP RDSI:

Se utiliza para configurar una conexión punto a punto (PPP) por RDSI utilizando el interfaz básico RDSI.

```
Quick Config>add ip
Type IP connection identifier (1-99) [0]? 3
Underlying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.PSTN [1]? 3
Type B Channel to use: 1.-B1, 2.-B2 [1]? 1
Type local IP address [0.0.0.0]? 192.168.103.10
Type subnet mask [255.255.255.0]?
Do you want to enable NAPT (Yes/No)(Y)? Y
Type NAPT entries duration (1-240 min.) [5]?
Type user  []? userTeldat
Type password  : ******
Confirm password  : ******
Call Number  []? 789456123
Select Remote Authentication Protocol: None(1), PAP(2), CHAP(3)[1]? 3
Type user  []? userChap
Type password  : ****
Confirm password  : ****
Type PPP release time (0 - 65535)s [0]? 100
Type description []? Conexion RDSI
Quick Config>
```

- **B Channel to use: 1.-B1, 2.-B2**

  Permite seleccionar el canal B "lógico" al que se asociará la configuración (la comunicación se establecerá por el canal físico B1 o B2 según determine la red RDSI).

El router TeldatC permite dos conexiones PPP por el interfaz RDSI excepto en los siguientes casos:

1) configuración ISDN en modo <Permanente B1+B2>, en cuyo caso sólo se permitirá una conexión PPP sobre dicho agregado.

2) configuración de una conexión PPP sobre un canal B configurado como permanente y que además tenga habilitado Multilink (en cuyo caso se considera el segundo canal B como permanente).

d) Conexiones IP AAL-ATM:

Se utiliza para configurar una conexión punto a punto (PPP) o IP por ATM utilizando la interfaz ADSL. Se necesita haber añadido y configurado algún circuito AAL-ATM para poder añadir la conexión IP.

```
Quick Config>add ip
Type IP connection identifier (1-99) [0]? 4
Underlying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.PSTN [1]? 2
Type AAL-ATM connection to use [0]? 1
Select traffic type (IP=1, PPP=2, PPPoE=3) [1]? 2
Type local IP address [0.0.0.0]? 192.168.104.10
Type subnet mask [255.255.255.0]?
Do you want to enable NAPT (Yes/No)(Y)? N
Type user  []? usuarioTeldat
Type password  : ******
Confirm password  : ******
Type description []? Conexion ADSL
Quick Config>
```

- **AAL-ATM connection to use**

  Identificador de circuito AAL-ATM que sirve de base para la conexión IP.

- **Traffic type (IP=1, PPP=2, PPPoE=3)**

  Selección del tipo de tráfico que manejará la conexión IP, y que puede ser IP, PPP o PPPoE.

  Si elegimos PPP nos preguntará además por usuario y password (**user** y **password**) necesarios para que el extremo remoto autorice la conexión.

Para ver los parámetros de las conexiones IP existen dos formas: una general, donde vemos una tabla con todas las conexiones y los datos más importantes de cada conexión, y una pormenorizada, donde vemos todos los datos de una conexión en concreto.

El comando para mostrar la configuración es `<LIST IP>` y opcionalmente, puede indicar el identificador de la conexión IP que desee: si no se proporciona este valor, se lista un resumen de todas las conexiones IP configuradas.

```
Quick Config>list ip

--- IP Connections ---

Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth  NAPT
----  ------ -------  ------------------  -------  ----  ---------
IP1    LAN1    ----    192.168.101.10/24   IP       ---   YES -  25
IP2    WAN1    ----    192.168.102.10/24   PPP      PAP   NO
IP3    ISDN1   B1      192.168.103.10/24   PPP      CHAP  YES -   5
IP4    ADSL1   ATM1    192.168.104.10/24   PPPoE    ---   NO
IP5    ADSL1   ATM2    192.168.105.10/24   IP       ---   YES -   5

Quick Config>
```

```
Quick Config>list ip 1

 IP Connection: IP1
 Underlying Connection: LAN1
 Local IP address: 192.168.101.10      Mask: 255.255.255.0
 Encapsulation: IP
 NAPT: Enabled                         Time out: 25 minutes
 NAPT Peer Address 192.168.101.15
 Description: Conexion LAN

Quick Config>
```

```
Quick Config>list ip 3

 IP Connection: IP3
 Underlying Connection: ISDN1
 Subinterface: B1
 Local IP address: 192.168.103.10      Mask: 255.255.255.0
 Encapsulation: PPP
 User: userTeldat
 Password: ****
 Remote Authentication Protocol: CHAP
 Remote user: userChap
 Call Number: 789456123
 Release Time: 100
 NAPT: Enabled                         Time out: 5 minutes
 Description: Conexion RDSI

Quick Config>
```

```
Quick Config>list ip 5

 IP Connection: IP5
 Underlying Connection: ADSL1
 Subinterface: ATM2
 Local IP address: 192.168.105.10      Mask: 255.255.255.0
 Encapsulation: IP
 NAPT: Enabled                         Time out: 5 minutes
 Description: Conexión ADSL

Quick Config>
```

Cuando se elimina una conexión IP se eliminan también, en cascada, todos los parámetros configurados que hayan requerido de dicha conexión, tales como las rutas, backup, multilink, callback, etc.

16. Parámetros del Callback

Es posible "despertar" remotamente al equipo para que se conecte, a pesar de que las estaciones locales de la LAN no tengan tráfico que cursar. La forma de despertar al equipo es realizar una llamada de *callback*: cuando el equipo recibe una llamada de callback, la rechaza, pero realiza una llamada al número desde el que se originó ésta. Se puede habilitar la posibilidad de aceptar llamadas de callback en los dos canales B de forma independiente.

Adicionalmente, se puede indicar el teléfono desde el que se aceptará la llamada de callback: si se configura este número, el equipo sólo se "despertará" si recibe la llamada RDSI desde dicho número, y realizará la llamada únicamente a ese número.

Los parámetros del Callback se configuran mediante el comando <ENABLE CALLBACK>.

```
Quick Config>enable callback
IP connection identifier (1-99): [0]? 3
Authorized Calling number  []? 963852741
Quick Config>
```

- **IP connection identifier (1-99)**

  Se elige la conexión a la que se desea habilitar el callback.

Actualmente sólo podrá habilitar callback en conexiones IP sobre RDSI y en canales que NO estén configurados como permanentes.

- **Authorized Calling number**

  Se puede restringir el número que provocará la llamada de callback. Si se deja en blanco, todas las llamadas se considerarán llamadas de callback.

Para consultar la configuración del callback dispone del comando <LIST CALLBACK>.

```
Quick Config>list callback

--- CALLBACK Parameters ---
IP Conn       Auth Caller
-------  --------------------
  IP3      963852741

Quick Config>
```

Para deshabilitar el callback sobre una conexión IP determinada, dispone del comando <DISABLE CALLBACK>.

17. Parámetros de Multilink PPP

Es posible combinar sesiones PPP para formar un único canal virtual o mazo Multilink. El protocolo Multilink es un estándar de la comunidad Internet y su especificación se encuentra recogida en [MPPP-96]. El protocolo Multilink es un método para trocear, recombinar y secuenciar datagramas a través de múltiples enlaces de datos.

Las posibilidades de configuración del protocolo Multilink PPP en el menú rápido tienen las siguientes características:

1. Sólo es posible agregar las sesiones PPP asociadas a canales B del acceso básico de RDSI.
2. La adición y posterior substracción del segundo canal B se puede realizar en cualquier momento en función de los parámetros de ancho de banda por demanda de la sesión Multilink PPP.
3. Cuando están establecidos los dos canales B del acceso básico, el tráfico PPP se alterna entre ambos canales.

La sesión Multilink PPP se establece con el perfil de una conexión IP. Esto implica que la nueva conexión lógica Multilink PPP tendrá los parámetros de dicha conexión IP (usuario, password, tiempo de liberación por ausencia de datos y teléfono del servidor de acceso remoto). Además, adoptará las rutas, subredes visibles, puertos visibles e intervalos de conexión de la conexión IP. También soportará la facilidad de callback si ésta estaba configurada en la conexión IP.

La sesión Multilink PPP responde al patrón de ancho de banda bajo demanda, es decir, el segundo canal B se establece o libera en función del tráfico existente en la sesión Multilink, de acuerdo a los parámetros que se describen más adelante.

Para habilitar Multilink en una conexión IP dispone del comando <ENABLE MULTILINK>.

```
Quick Config>enable multilink
IP connection [1]?
Type the Interval Activation    (4 - 1800):[120]?
Type the Interval Deactivation  (4 - 1800):[300]?
Type the Threshold Activation   (0 - 100):[90]?
Type the Threshold Deactivation (0 - 100):[50]?
Type the direction of load In(1), Out(2) or Both(3): [3]?
Do you wish to configure the multilink bundle as pre-emptive(Yes/No)(N)?
Quick Config>
```

- **IP connection**

  Se elige la conexión a la que se desea habilitar Multilink.

Multilink sólo se podrá habilitar en conexiones IP que tengan como base un canal B del acceso básico RDS, y siempre que el conector RDSI no esté configurado como permanente B1 más B2I.

- **Type the Interval Activation (4 - 1800)**

  Si durante los segundos indicados en este parámetro la ocupación media del canal sobre el que está habilitado el multilink supera el umbral de activación, se activará el otro canal y se establecerá el mazo multilink.

  Este parámetro se mide en segundos y su valor por defecto es 120 segundos.

- **Type the Interval Deactivation (4 - 1800)**

  Si durante los segundos indicados en este parámetro la ocupación media del mazo multilink es inferior al umbral de desactivación, se desactivará el segundo canal B. Este parámetro se mide en segundos y su valor por defecto es 300 segundos.

- **Type the Threshold Activation (0 - 100)**

  Porcentaje de ocupación del canal B necesario para la activación del segundo canal B en el Multilink. Si, durante el intervalo de activación, la ocupación media del primer canal B supera este valor, se activará el segundo canal B.

  El valor por defecto de este parámetro es 90 %.

- **Type the Interval Deactivation (28 - 1800)**

  Mínimo porcentaje de ocupación del mazo multilink necesario para el mantenimiento del multilink. Si, durante el intervalo de desactivación, la ocupación media del mazo multilink no llega a este valor, se desactivará el segundo canal B.

  El valor por defecto de este parámetro es 50 %.

- **Type the direction of load In(1), Out(2) or Both(3)**

  Indica el sentido del tráfico considerado para calcular la carga media de los canales. Puede ser entrante (desde la red externa hacia el equipo), saliente (desde el equipo hacia la red externa) o ambos. Para circunstancias normales de acceso a una red externa, como por ejemplo Internet, en donde la mayoría del trafico es entrante, se recomienda configurar el valor entrante. Si se dispone de servidores visibles o puertos visibles y se presupone que dichos servidores van a ser frecuentemente accedidos desde la red externa, se recomienda configurar los valores de "saliente" o "ambos". El valor por defecto de este parámetro es "ambos".

- **Do you wish to configure the multilink bundle as pre-emptive(Yes/No)**

  Podemos configurar el mazo Multilink como expropiable, es decir, cuando el Multilink esté usando los dos canales B del acceso básico RDSI y se reciba una llamada, el segundo canal B del Multilink será expropiado y se encargará de atender a esa llamada.

  Como excepción, las llamadas procedentes de un "gestor autorizado" siempre provocan la expropiación del segundo canal del Multilink, aunque este no esté configurado como expropiable.

Para deshabilitar Multilink dispone del comando `<DISABLE MULTILINK>`.

Para consultar la configuración de los parámetros Multilink dispone del comando `<LIST MULTILINK>`.

```
Quick Config>list multilink

--- MULTILINK PPP parameters ---
Multilink PPP:            Enabled
IP connection:            IP1
Interval of activation:   120
Interval of deactivation: 300
Activation Threshold:     90
Deactivation Threshold:   50
Direction of load:        BOTH
Pre-emptive:              No

Quick Config>
```

18. Parámetros de los Gestores Autorizados

El equipo ***TELDATC*** puede ser gestionado mediante el protocolo SNMP desde una estación de gestión remota autorizada (perteneciente a la subred de gestión definida y conocedora de la comunidad SNMP configurada).

Existe el caso particular en el que la red de gestión sea una red privada y el router disponga de interfaz RDSI y/o RTC: en funcionamiento normal, el router proporciona acceso a los usuarios a las redes que tenga configuradas (Internet, …); si el gestor quiere establecer una comunicación desde su red privada con el equipo, Teldat ha desarrollado un mecanismo para ello cuyo elemento principal es un equipo denominado ***ROUTER MAESTRO***: cuando el gestor quiere conectar con el equipo, ordena al router maestro que realice una llamada al equipo a gestionar, y si éste tiene configurado el número RDSI (o el patrón en caso de RTC) desde el que llama el ***ROUTER MAESTRO*** como gestor autorizado, el equipo a gestionar realiza una llamada al número configurado con los parámetros indicados: entre el ***TELDATC*** y el ***ROUTER MAESTRO*** se establecerá una comunicación propietaria de Teldat mientras dure la gestión del equipo, que servirá para que el ***TELDAT C*** comunique al router maestro la dirección IP que se le ha asignado, y así poder comunicársela a la estación de gestión.

Para configurar y añadir los gestores autorizados, use el comando <ADD MANAGER>. Se permite configurar hasta 15 gestores.

```
Quick Config>add manager
Authorized manager telephone:  []? 123456789
Master router address:  [0.0.0.0]? 169.69.101.1
Master router mask:  [255.255.0.0]?
Manager station address:  [0.0.0.0]? 172.24.78.73
Manager station mask:  [255.255.0.0]?
Login:  []? teldat
Password:  : ******
Repeat password:  : ******
Destination telephone of the management connection:  []? 987654321
Quick Config>
```

- **Authorized manager telephone**

  Teléfono de gestor autorizado (número desde el que llamará el ***ROUTER MAESTRO***): cuando el equipo ***TELDATC*** recibe una llamada por la línea RDSI comprueba si el llamante coincide con el número de algún gestor autorizado. Si coincide, considera que la llamada es de gestión y se pasa al estado de gestión. En caso contrario, trata la llamada como una llamada entrante normal.

  Si la llamada se recibe por la línea RTC, el equipo ***TELDATC*** comprueba si la llamada se ajusta al patrón de llamada definido en los parámetros globales. Si coincide, considera que la llamada es de gestión por RTC, pero para pasar a estado de gestión, deberá existir un perfil de gestión cuyo teléfono de gestor autorizado sea "0".

- **Master router address / Master router mask**

  Dirección IP del ***ROUTER MAESTRO*** y máscara de red, es decir, dirección IP a la que el equipo ***TELDATC*** mandará los paquetes IP para establecer la comunicación con dicho ***ROUTER MAESTRO***. (La máscara es necesaria para agregar una ruta a la subred a la que pertenece el ***ROUTER MAESTRO***)

- **Manager station address / Manager station mask**

  Dirección IP y máscara de la estación de gestión: la estación de gestión sobre la que se ejecuta el programa de gestión remota del equipo ***TELDATC*** puede pertenecer a una subred distinta a la subred del router maestro. Por tanto, se puede definir una segunda subred de forma que se añada una ruta a esa subred por la conexión de gestión. Si no se especifica ninguna dirección IP ni máscara, no se creará la ruta.

- **Login / Password**

  Usuario y clave: estos valores serán los que se utilicen al establecer la conexión de gestión siempre que el extremo remoto nos pida que nos identifiquemos.

- **Destination telephone of the management connection**

  Teléfono de destino de la conexión de gestión: teléfono del nodo al que el equipo se conectará a la hora de establecer la conexión de gestión.

Se pueden definir hasta 15 perfiles de gestión. Para ver los perfiles de gestión que ya están creados se debe ejecutar el comando <LIST MANAGER>. Con el comando <DELETE MANAGER> es posible eliminar el perfil de gestión que se desee y con el comando <CHANGE MANAGER> se podrá modificar un perfil de gestión.

```
Quick Config>list manager

--- MANAGER parameters ---
   Manager    Master Router      Manager Station                    Dest.
Id Telephone  IP Address/Mask    IP Address/Mask    User            Telephone
-- ---------- ----------------- ----------------- --------------- ----------
1  123456789  169.69.101.1/16    172.24.78.73/16    teldat          987654321

Quick Config>
```

19. Parámetros RIP

El protocolo RIP es un protocolo de enrutamiento dinámico: con él, el router aprenderá dinámicamente rutas a todas las redes que estén conectadas a routers que tengan habilitado el RIP.

Para habilitar globalmente el protocolo RIP dispone del comando <ENABLE RIP>, y para deshabilitar globalmente el comando <DISABLE RIP>

Para configurar los parámetros del protocolo RIP sobre una conexión IP dispone del comando <SET RIP>.

```
Quick Config>enable rip
Quick Config>set rip
Connection identifier [1]? 1
Available:
 1.- Do not send
 2.- RIP1
 3.- RIP2 Broadcast
 4.- RIP2 Multicast
What kind of sending compatibility do you wish? [3]? 2
Available:
 1.- RIP1
 2.- RIP2
 3.- RIP1 or RIP2
 4.- Do not receive
What kind of receiving compatibility do you wish? [3]? 1
Quick Config>
```

- **Connection identifier**

  Podemos configurar el RIP para cada conexión IP.

- **What kind of sending compatibility do you wish?**

  Permite configurar el envío de los paquetes RIP como paquetes de la versión 1 de RIP o la versión 2 de RIP; en este último caso, es necesario indicar el tipo de dirección destino a utilizar (multicast o broadcast)

- **What kind of receiving compatibility do you wish?**

  Al igual que en el anterior, podemos elegir la versión del protocolo o deshabilitar el aprendizaje RIP por la conexión IP.

Por defecto, cuando se habilita RIP globalmente, todos los interfaces tienen activado el envío y recepción de paquetes RIP.

Para ver la configuración RIP dispone del comando <LIST RIP>.

```
Quick Config>list rip

--- RIP configuration ---

RIP status: Enabled
Ident Sending compatibility Receiving compatibility
----- -------------------- ----------------------
IP1   RIP1                 RIP1
IP2   RIP2 Broadcast       RIP1 or RIP2
IP3   RIP2 Broadcast       RIP1 or RIP2

Quick Config>
```

20. Parámetros de encaminamiento IP

Para añadir una ruta estática a la tabla de rutas dispone del comando <ADD ROUTE>.

```
Quick Config>add route
Type destination subnetwork address [0.0.0.0]? 172.25.0.0
Type destination subnetwork mask [255.255.0.0]?
Type outgoing connection identifier [1]? 1
Type cost (1..16) [1]?

Quick Config>add route
Type destination subnetwork address [0.0.0.0]? 65.0.0.0
Type destination subnetwork mask [255.0.0.0]?
Type outgoing connection identifier [1]? 2
Type next hop address [0.0.0.0]? 172.24.78.55
Type cost (1..16) [1]?
Quick Config>
```

- **Destination subnetwork address / Destination subnetwork mask**
  Permiten determinar la red destino.

- **Outgoing connection identifier**
  Permite determinar la conexión IP por la que es alcanzable la red configurada.

- **Next hop address**
  En el caso de conexiones IP que no sean de tipo punto a punto (PPP), deberá configurar la dirección del router al que se deben enviar los paquetes destinados a la red configurada.

- **Cost**
  Coste de la ruta; ante dos rutas a un mismo destino, el router escogerá aquella de coste menor (menor número de saltos, etc.).

Para consultar las rutas configuradas dispone del comando <LIST ROUTES>, y puede modificarlas mediante <CHANGE ROUTE>.

```
Quick Config>list routes

--- IP Routes ---

Ix Conn Dest. Address   Dest. Mask      Next Hop        Cost
-- ---- --------------- --------------- --------------- ----
1  IP1  172.25.0.0      255.255.0.0                     1
2  IP2  65.0.0.0        255.0.0.0       172.24.78.55    1

Quick Config>
```

21. Parámetros del Control horario

El objetivo del control horario es fijar el intervalo de tiempo en el que el router permitirá el flujo de información por una determinada conexión IP.

Sólo se podrá establecer control horario en conexiones IP cuyo tráfico sea sobre PPP.

Para añadir un nuevo perfil de control horario se usa el comando <ADD TIME>.

```
Quick Config>add time
Type IP connection identifier (1-99) [0]? 1
Insert hour of the beginning of the allowed interval of connection [0]? 8
Insert minute of the beginning of the allowed interval of connection [0]? 30
Insert hour of the end of the allowed interval of connection [23]? 18
Insert minute of the end of the allowed interval of connection [59]? 30
Sunday (Yes/No)(N)?
Monday (Yes/No)(N)? y
Tuesday (Yes/No)(N)? y
Wednesday (Yes/No)(N)? y
Thursday (Yes/No)(N)? y
Friday (Yes/No)(N)? y
Saturday (Yes/No)(N)?
Quick Config>
```

En este ejemplo a la conexión IP 1 se le ha añadido un perfil de control horario que le permite conectarse de 8:30 a 18:30 de lunes a viernes.

Para borrar un perfil de control horario se usa el comando <DELETE TIME>.

Para listar los perfiles de control horario se usa el comando <LIST TIME>.

```
Quick Config>list time

--- Time Controls ---

Conn. Init  End   Days
----- ----- ----- -------------
 IP1  08:30 18:30 .-M-T-W-T-F-.

Quick Config>
```

22. Parámetros de Backup

Si al intentar establecer una conexión e producen problemas que imposibilitan la conexión es posible configurar una conexión PPP alternativa de backup (normalmente sobre un interfaz conmutado).

El backup que configura el menú rápido es backup por WAN ReRoute (WRR). En líneas generales este backup actúa activando la ruta de backup cuando el interfaz principal pasa a **DOWN,** y vuelve a activar la ruta principal cuando el interfaz principal pasa a **UP**.

Cuando se configura un backup para una conexión PPP sobre un interfaz conmutado, las condiciones que provocan el paso a backup son dos:

1. **Timeout de IPCP**
   Si en el tiempo indicado no se consigue establecer el nivel IPCP, se intenta establecer la conexión de backup

2. **Número máximo de intentos de llamada**
   En el caso de RDSI, si se realizan el número de intentos de llamada configurados y no se consigue establecer la llamada RDSI, se procede con el backup.

Estas dos condiciones actúan simultáneamente, de tal forma que la primera que se cumpla provoca el paso a backup. Si la llamada se establece normalmente y el IPCP se negocia en el plazo fijado, el paso a backup no se produce. Si se pasa a backup, los parámetros de backup se activan, las rutas del canal con fallo se cambian a la conexión de backup, para garantizar el tráfico del usuario, y se realiza la llamada de backup.

En el caso de que el interfaz PPP esté configurado sobre un interfaz permanente, el salto a backup se produce al vencer el tiempo de estabilización de la facilidad de WRR, cuyo valor por defecto está configurado a 50 segundos.

Los parámetros configurables en el backup son los siguientes, y se configuran mediante el comando `<ENABLE BACKUP>`.

```
Quick Config>enable backup
Main IP connection identifier (1-99) [0]? 2
Backup IP connection identifier (1-99) [0]? 4
IPCP timeout: [60]?
Call attempts before entering backup: [2]?
Maximum backup time (min) [30]?
Quick Config>
```

- **Main IP connection identifier (1-99)**
  La conexión IP de la cual se hará backup. Cuando está conexión esté caída se establecerá la conexión de backup.
- **Backup IP connection identifier (1-99)**
  Es la conexión IP de backup sobre la cual se encaminará el tráfico de la conexión principal cuando ésta esté caída.
- **IPCP timeout: [60]**
  Es el tiempo máximo que puede transcurrir desde que se solicita una conexión hasta que se dispara el backup de esa conexión, si en dicho tiempo no se ha establecido el

nivel IPCP. El rango de valores permitidos para este parámetro es de 20 a 200 segundos.

- **Call attempts before entering backup**

  Es el número máximo de intentos de llamada RDSI consecutivos y sin éxito, permitidos antes de que se dispare el backup. El valor máximo permitido para este parámetro es 5 reintentos.

- **Maximum backup time (min) [30]?**

  Cuando el interfaz principal es una línea conmutada y se corta la comunicación (**DOWN**) pasando a backup, el sistema no puede saber cuándo la interfaz principal puede pasar a **UP**. Por ello, el sistema intenta periódicamente establecer la comunicación por el canal principal y si no puede establecerla sigue en backup. Mediante este parámetro podemos programar la periodicidad de los intentos. Si se deja a 0 no intentará restablecer la comunicación por el canal principal. En el caso de que el interfaz principal sea una línea permanente, la finalización de la conexión de backup se produce automáticamente.

Si el parámetro Maximum backup time se deja a 0 en backup de una lína conmutada una vez que se entre en backup el sistema no saldrá del backup hasta que la comunicación no termine o se haga un reset al equipo.

Para listar los parámetros de Backup se usa el comando <LIST BACKUP>.

```
Quick Config>list backup

--- BACKUP parameters ---
Main IP conn  Backup IP conn  Retries TimeOut MxTimeBk
------------  --------------  ------- ------- --------
    IP2           IP4           2      60      30

Quick Config>
```

Para deshabilitar el backup de una conexión IP se usa el comando <DISABLE BACKUP>.

No se puede establecer como conexión de backup una conexión basada en un canal B que esté configurado como permanente.

Si está configurado backup de un canal B por el otro canal B y se habilita Multilink, el backup no se establecerá nunca.

Cuando se realice el `make`***, la configuración de un backup implica la creación automática de una ruta (igual a la que exista por la interfaz principal pero con un coste mayor) por la interfaz secundaria o de backup.***

23. Parámetros del Control de Acceso

El sistema de control de accesos tiene como misión controlar el acceso de los usuarios (internos o externos) a determinadas subredes y/o servicios. El control se basa en una lista ordenada de filtros inclusivos (si un paquete cumple la condición definida en el filtro, se le dejará progresar) y exclusivos (si un paquete cumple la condición definida en el filtro, no se le dejará progresar, es decir, se descartará).

Cuando se recibe un paquete, se aplican los filtros en el orden establecido y, en cuanto cumple la condición de un filtro, se procesa del modo que indique el filtro, sin pasar por ningún otro filtro de la lista.

Para añadir un control de acceso se usa el comando <ADD ACCESS>.

```
Quick Config>add access
Select control type (1-EXCLUSIVE, 2-INCLUSIVE) [2]? 1
Type source IP address [0.0.0.0]? 172.24.51.75
Type source mask [255.255.0.0]? 255.255.255.255
Type destination IP address [0.0.0.0]?
Type destination mask [0.0.0.0]?
Type first IP protocol (0-255) [0]?
Type last IP protocol (0-255) [255]?
Type first source port (0-65535) [0]? 20
Type last source port (0-65535) [65535]? 20
Type first destination port (0-65535) [0]?
Type last destination port (0-65535) [65535]?
Quick Config>
```

- **Control type (1-EXCLUSIVE, 2-INCLUSIVE)**

  Los inclusivos permiten progresar a los paquetes. Los exclusivos los descartan impidiéndoles el paso.

- **Source IP address / Source mask**

  Los paquetes que tengan como dirección origen una dirección IP de esta subred serán objeto de lo que indique el control de acceso (incluir, excluir).

- **Destination IP address / Destination mask**

  Los paquetes que tengan como dirección destino una dirección IP de esta subred serán objeto de lo que indique el control de acceso (incluir, excluir).

- **First IP protocol (0-255) / Last IP protocol (0-255)**

  El número del protocolo transportado en el paquete debe estar incluido en el rango de protocolos definido por los campos protocolo comienzo y protocolo final del control de acceso. Si se programa la opción "todos" en este campo en el control de acceso, siempre habrá coincidencia.

Los números de protocolo más usados son:

6 para TCP (Transmission Control Protocol).

17 para UDP (User Datagram Protocol).

- **First source port (0-65535) / Last source port (0-65535)**

  El número de puerto origen del paquete debe estar incluido en el rango de puertos definido por los campos puerto origen comienzo y puerto origen final del control de acceso.

  Sólo se aplica si el campo Número de Protocolo del Control de acceso es 6 o 17.

- **First destination port (0-65535) / Last destination port (0-65535)**

  El número de puerto destino del paquete debe estar incluido en el rango de puertos definido por los campos puerto destino comienzo y puerto destino final del control de acceso.

  Sólo se aplica si el campo Número de Protocolo del Control de acceso es 6 o 17.

Los números de puertos usados más frecuentemente son:

20/21 para FTP

23 para TELNET

25 para SMTP (mail/correo)

80 para HTTP (web/Internet)

Para más información sobre números de puertos y de protocolos IP en la RFC 1700.

Una vez que el paquete coincide con un filtro del control de acceso, se realiza la operación asociada con el elemento (progresar o descartar), y no se sigue verificando el resto de la lista de controles de acceso.

Por tanto, el ORDEN de los elementos de la lista de control de acceso es muy IMPORTANTE.

Si tras consultar toda la lista de controles de acceso configurados no se ha encontrado coincidencia, el paquete se progresa. Esto equivale a configurar un control de acceso que permita todo tipo de tráfico, al final de la lista de controles de acceso.

Para ver los controles de acceso configurados dispone del comando <LIST ACCESS>:

```
Quick Config>list access

--- Access Controls ---

Ix T Source             Destination        Protocols Src. Ports  Dest. Ports
-- - ------------------ ------------------ --------- ----------- -----------
1  E 172.24.51.75/32    0.0.0.0/0             0-255     20-20        0-65535

Quick Config>
```

Para borrar un control de acceso configurado, se debe teclear el comando <DELETE ACCESS> e indicar el control de acceso que se desea borrar.

En el caso de tener configurado PAT y/o NAT, el orden de aplicación es el siguiente:

$$NAPT_A \leftrightarrow FILTROS \leftrightarrow NAT_{(A \leftrightarrow B)} \leftrightarrow FILTROS \leftrightarrow NAPT_B$$

24. Parámetros de las reglas NAT

El NAT (Network Address Translation) permite realizar traducción de direcciones IP de modo que los paquetes procesados por una determinada conexión IP y procedentes de una estación local con dirección IP en el rango configurado como direcciones locales, salga al exterior como si procediera de una dirección del rango configurado como global si la dirección destino se alcanza por la conexión IP configurada, y viceversa.

Existen diferentes tipos de NAT: el denominado "N a N" o NAT estático, en el que cada dirección IP se traduce por otra dirección IP sin solapamientos, el denominado "N a 1" o NAT de puertos o PAT, en el que todas las direcciones se traducen a una misma dirección, etc.

En este punto se explica la configuración de reglas NAT estático.

Para añadir una regla de NAT se usa el comando <ADD NAT>.

```
Quick Config>add nat
Type local connection identifier [1]?
Type local subnet address [0.0.0.0]?192.168.1.0
Type local subnet mask [0.0.0.0]?255.255.255.0
Type global connection identifier [1]?2
Type global subnet address [0.0.0.0]?212.43.5.0
Quick Config>
```

- **Local connection identifier**
  La conexión IP a la cual se le aplicará la regla de NAT estático.

- **Local subnet address / Local subnet mask**
  Dirección de la subred local a la que se le aplicará NAT estático.

- **Global connection identifier**
  La conexión IP con la que el router se conecta a la red global.

- **Global subnet address**
  Dirección de red para el rango de direcciones globales.

Para listar los parámetros de las reglas NAT, utilice el comando <LIST NAT>.

```
Quick Config>list nat


--- NAT Rules ---

Ix Type Direction L.Conn. Local address/mask G.Conn. Global address/mask
-- ---- --------- ------- ------------------ ------- ------------------
1  SRC  BOTH      IP1     192.168.1.0/24     IP2     212.43.5.0/24

Quick Config>
```

Para borrar una regla NAT, dispone de <DELETE NAT>, y mediante el comando <CHANGE NAT> puede modificarla; en ambos comandos deberá indicar el número de regla a borrar o a modificar.

25. Parámetros de puertos visibles

Cuando tiene configurado la utilización de NAPT o PAT o NAT de puertos, puede definir excepciones al comportamiento general de PAT: por defecto, cuando el router recibe un paquete dirigido a la dirección IP del interfaz que recibe el paquete (dirección con la que está haciendo PAT dicho interfaz), consulta una tabla interna buscando el puerto destino contenido en el paquete: si el puerto destino no está en la tabla, significa que ningún host interno realizó una petición, y por tanto, el paquete se rechaza; si por el contrario, el puerto está en la tabla, el router realiza la traducción inversa para enviar el paquete al host correcto y en el puerto correcto.

La configuración de un puerto visible permite saltarse dicha comprobación: cuando llega un paquete, se consulta la tabla de puertos definidos como visibles, y si está presente, reencamina el paquete al puerto y host indicado; si no está presente en la tabla de puertos visibles, el paquete se procesa de modo normal (consulta de la tabla interna de puertos abiertos, etc.)

Para configurar un puerto como visible se usa el comando <ADD PORT>. En el siguiente ejemplo, cuando se reciba un paquete destinado al puerto 2000, el paquete se enviará al host 172.24.51.75 y el puerto se sustituirá por el 20.

```
Quick Config>add port
Type IP connection identifier (1-99) [0]? 1
Type host IP address  [0.0.0.0]? 172.24.51.75
Type internal port (0-65535) [0]? 20
Type external port (0-65535) [0]? 2000
Select port type (1-GENERIC, 2-FTP) [1]? 2
Quick Config>
```

- **IP connection identifier (1-99)**

  La conexión IP por la que se hará visible el puerto.

- **Host IP address**

  La dirección del host del que se hará visible el puerto.

- **Internal port (0-65535)**

  El puerto que se desea hacer visible.

- **External port (0-65535)**

  El número de puerto con el que se hará visible.

- **Port type (1-GENERIC, 2-FTP)**

  Se indica si el puerto es genérico o FTP (FTP establece dos conexiones: una de datos y otra de control).

Para borrar la configuración de un puerto visible, dispone del comando <DELETE PORT>, <CHANGE PORT> para cambiar algún parámetro y <LIST PORT> para mostrar los puertos visibles configurados.

```
Quick Config>list port


--- Visible Ports ---

Ix Conn. IP Address      Int.Port Ext.Port Type
-- ----- --------------- -------- -------- -------
1  IP1   172.24.51.75    20       2000     FTP

Quick Config>
```

El router ofrece una serie de servicios en los puertos estándar, concretamente servidor FTP (20/21), Telnet (23), DNS (53) y HTTP (80); dichos servicios pueden trasladarse de puerto para dejar libres dichos puertos estándar y permitir así su utilización para configurar puertos visibles de hosts internos.

26. Parámetros de las subredes visibles

Otro tipo de excepción al NAPT/PAT es la definición de subredes visibles: por defecto, todo tráfico saliente por una conexión IP con NAPT/PAT habilitado sufre la sustitución de la dirección IP origen por la dirección del interfaz, y viceversa cuando el paquete es de respuesta. Una subred visible no sufre dicha transformación, es decir, se mantiene la dirección origen invariable.

Para añadir una subred visible se usa el comando <ADD SUBNETWORK>.

```
Quick Config>add subnetwork
Type IP connection identifier (1-99) [0]? 1
Type visible subnet address  [0.0.0.0]? 172.24.0.0
Type visible subnet mask  [255.255.0.0]?
Type IP address of the default gateway  [0.0.0.0]? 172.24.0.98
Quick Config>
```

- **IP connection identifier (1-99)**

  La conexión IP por la cual se hará visible la subred.

- **Visible subnet address / Visible subnet mask**

  Es la dirección IP de la subred que se va a hacer visible a través de la conexión IP definida en el parámetro anterior.

- **IP address of the default gateway**

  En el caso de que la subred visible esté directamente conectada al router de acceso a través de la interfaz LAN y el router no disponga de dirección en dicha subred visible, es necesario configurar la dirección que los hosts de la subred visible tiene configurada como router por defecto y de este modo conseguir que el router conteste a las peticiones ARP lanzadas por los hosts.

Para borrar la configuración de una subred visible utilice el comando <DELETE SUBNETWORK>, <CHANGE SUBNETWORK> para modificar la configuración y <LIST SUBNETWORK> para listar la configuración.

```
Quick Config>list subnetwork

--- Visible Subnets ---

Ix Conn. Subnet Address  Subnet Mask     Gateway
-- ----- --------------- --------------- ---------------
1  IP1   172.24.0.0      255.255.0.0     172.24.0.98

Quick Config>
```

27. Parámetros de IPSec

En este apartado se describen los comandos para configurar el protocolo IPSec. Para acceder al entorno de configuración del protocolo IPSec se debe introducir el comando <IPSEC>.

```
Quick config>?
ADD
CHANGE
CLEAR
DELETE
DISABLE
ENABLE
IPSEC Quick Menu
LIST
MAKE and save configuration
SAVE configuration
SET
POS Quick Menu
EXIT
Quick config>IPSEC
IPSec Quick Configuration Menu
IPSec Quick config>
```

Dentro del entorno de configuración del protocolo IPSec (indicado por el prompt **IPSec Quick config**>) se dispone de los siguientes comandos:

```
IPSec Quick config>?
ADD
CHANGE
CLEAR
DELETE
DISABLE
ENABLE
LIST
EXIT
IPSec Quick config>
```

La siguiente tabla resume los comandos de configuración del protocolo IPSec. Las letras que están escritas en **negrita** son el número mínimo de caracteres que hay que teclear para que el comando sea efectivo.

Comando	Función
? (AYUDA)	Lista comandos u opciones.
ADD	Permite agregar un template o entrada en la tabla de definición de túneles, un control de acceso o selector de tráfico IPSec o bien una clave.
CHANGE	Permite modificar alguno de los parámetros correspondientes a un template o entrada en la tabla de definición de túneles, a un control de acceso o selector de tráfico IPSec o bien a una clave que previamente se habían introducido.
CLEAR	Borra todas las entradas existentes en la tabla de definición de túneles, todos los controles de acceso o selectores de tráfico IPSec o bien todas las claves configuradas.
DELETE	Borra una entrada de la tabla de definición de túneles, o un control de acceso o bien una clave IPSec.
DISABLE	Deshabilita IPSec.
ENABLE	Habilita IPSec.
LIST	Lista configuración de IPSec.
EXIT	Vuelve al prompt anterior.

La configuración por defecto de IPSec es "IPSec deshabilitado" y sin ningún túnel ni selector de tráfico creados, ni tampoco entradas en la tabla de claves.

27.1. ?(AYUDA)

Tecleando ? se muestran todos los comandos disponibles. También puede usar el símbolo ? para visualizar las distintas opciones de cada comando.

```
IPSec Quick config>?
ADD
CHANGE
CLEAR
DELETE
DISABLE
ENABLE
LIST
EXIT
IPSec Quick config>
```

27.2. ADD

El comando <ADD> permite añadir una clave, una entrada en la tabla de definición de túneles o un control de acceso:

```
IPSec Quick config>add ?
KEY
REMOTE tunnel endpoint
TRAFFIC selector
IPSec Quick config>
```

a) ADD KEY

Con ayuda de este comando se configuran las claves que el extremo local espera recibir del extremo o extremos remotos que traten de comunicarse con él a través de un túnel IPSec, asociadas al correspondiente identificador del otro extremo (dirección IP o hostname).

```
IPSec Quick config>add key
Remote peer id type (HOSTNAME=1, IP ADDRESS=2)[2]?
IP Address [0.0.0.0]? 200.200.200.3
Key[]? ********
IPSec Quick config>
```

El significado de los distintos parámetros solicitados es el siguiente:

- *Remote peer id type*: Indica el tipo de identificador que utiliza el extremo remoto para ser reconocido por el extremo local. Los posibles tipos de identificación son a través de la dirección IP si el extremo remoto hace el papel de servidor (es decir, el extremo local es un cliente de túneles IPSec) o mediante el hostname si el extremo remoto funciona como cliente (el servidor de túneles es por tanto el extremo local).
- *IP Address/Hostname*: Es el identificador del extremo remoto en sí. Al establecer un túnel, un equipo que va a utilizar una clave determinada se identifica ante el otro extremo del

túnel mediante su identificador (hostname si es un cliente, dirección IP si es servidor). Por eso al configurar las claves que el equipo reconoce, éstas deben ir asociadas además a un identificador.

- *Clave*: Con este parámetro se configura una de las claves que el equipo considera válidas en el sentido de que permitirá el establecimiento del túnel con el equipo que utiliza esa clave y que se identifica ante el extremo local con la dirección IP o hostname al que va asociada esa clave.

Cuando un equipo funciona como cliente de túneles IPSec, y por tanto va a utilizar su hostname para identificarse ante el otro extremo, es importante que dicho hostname esté configurado. Para ello hay añadir éste mediante el comando <SET HOSTNAME> del menú rápido global.

b) ADD REMOTE tunnel endpoint

Permite configurar los templates, o lo que es lo mismo, las entradas en la tabla de definición de túneles. Cada entrada contendrá los parámetros necesarios para configurar un túnel IPSec hacia un determinado destino.

```
IPSec Quick config>add remote
Type IPSec remote tunnel endpoint identifier[0]? 11
Choose an IP connection as source address of local tunnel endpoint:

--- IP Connections ---

 Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth  NAPT
----  ------- -------  ------------------  -------  ----  ---------
IP1    LAN1    ----    172.24.78.8/16      IP       ---   NO
IP2    WAN1    ----    210.10.10.1/32      PPP      NONE  NO

IP connection identifier[0]? 2
Enter remote tunnel endpoint IP address [0.0.0.0]? 200.200.200.2
Do you want to configure remote backup IP addresses(Yes/No)(Y)?
Enter remote backup IP address [0.0.0.0]?
No remote backup IP addresses configured
Id type (HOSTNAME=1, IP ADDRESS=2)[1]? 2
NAPT enabled(Yes/No)(N)?
Enter lifetime (in seconds)[3600]? 4200
UDP encapsulation(Yes/No)(N)?
IPSec Quick config>
```

Los distintos parámetros solicitados y su significado son los indicados a continuación:

- *Remote tunnel endpoint identifier*: Identificador del túnel. Sirve para poder hacer referencia a esa entrada y determinar así el túnel concreto al que se asocia un cierto selector de tráfico o control de acceso, o para borrar una entrada concreta o modificar alguno de sus parámetros.
- *Source address of local tunnel endpoint*: Se escoge una conexión IP de entre las configuradas en el equipo, que constituirá el origen del túnel. Esto es una forma de elegir el interfaz y la dirección IP que se consideran origen del túnel al que se refiere la entrada.
- *Remote tunnel endpoint IP address*: Dirección del extremo remoto del túnel. Sólo se permiten direcciones IP, no nombres equivalentes (que se puedan resolver mediante DNS).
- *Remote backup IP addresses*: Direcciones de backup para el extremo remoto. Pueden configurarse ninguna, una, dos o hasta tres direcciones de backup. Una dirección 0.0.0.0 de backup es tratada a todos los efectos como inexistente. Al igual que ocurre con la dirección principal del extremo remoto, sólo pueden configurarse direcciones IP, no nombres equivalentes.

- *Id type*: Tipo de identificación que utilizará el extremo local al tratar de establecer el túnel con el extremo remoto. Si el equipo local actúa como cliente del túnel, su forma de identificarse ante el otro extremo será mediante su hostname (deberá tenerlo configurado), mientras que si es el servidor se identifica ante el otro extremo con su dirección IP.
- *NAPT enabled:* Al habilitar este parámetro se indica que van a aplicarse reglas NAPT antes que IPSec en el origen del túnel. Esto implica que el tráfico a través de dicho túnel tendrá siempre como origen la dirección IP resultante tras aplicar NAPT, y por tanto solamente tendrán sentido los controles de acceso cuyo origen venga dado por la misma conexión IP que se toma como origen del túnel IPSec, y con máscara de host.
- *Lifetime:* Tiempo de vida del template isakmp generado a partir de esta entrada en la tabla de definición de túneles. El tiempo de vida del correspondiente template dinámico se calcula a partir de este valor aplicándole el factor 3300/3600, que es la relación existente entre los valores por defecto de los túneles dinámico e isakmp.
- *UDP encapsulation:* Si se habilita este parámetro se aplicará encapsulado UDP a los paquetes ESP que vayan a través del túnel IPSec. Esto es necesario si se quiere aplicar NAPT a esos paquetes en uno de los equipos intermedios situados antes de la salida del túnel.

c) ADD TRAFFIC selector

Este comando se utiliza para añadir selectores de tráfico o controles de acceso IPSec.

```
IPSec Quick config>add traffic
Type IPSec traffic selector identifier[0]? 4
Destination IP address [0.0.0.0]? 172.60.1.163
Destination IP mask [0.0.0.0]? 255.255.255.255
Type IPSec remote tunnel endpoint identifier[1]? 11
IPSec Quick config>
```

De cada control de acceso debe configurarse:

- *IPSec traffic selector identifier*: Identificador del selector de tráfico. Sirve para hacer referencia a una entrada concreta de la tabla a la hora de modificar alguno de sus parámetros o bien borrarla.
- *Destination IP address*: Dirección IP destino.
- *Destination IP mask*: Máscara asociada a la dirección IP destino. Con este parámetro y el anterior se fija que el tráfico que vaya con ese destino será encaminado por el túnel que indica el siguiente campo.
- *IPSec remote tunnel endpoint identifier*: Identificador del túnel por el que se encaminará el tráfico dirigido al destino determinado por la dirección y máscara anteriormente configuradas. El identificador debe referirse a un túnel que previamente se haya configurado en la tabla de definición de túneles.

27.3. CHANGE

Es posible modificar uno o varios parámetros de una entrada de la tabla de claves, de una entrada de la tabla de definición de túneles, o de un control de acceso, previamente introducida/o, utilizando el comando <CHANGE>.

```
IPSec Quick config>change ?
KEY
REMOTE tunnel endpoint
TRAFFIC selector
IPSec Quick config>
```

a) CHANGE KEY

Permite cambiar la clave asociada a determinado identificador del extremo remoto.

```
IPSec Quick config>change key
Type the remote peer id to change[]? 200.200.200.3
Key[]? ********
IPSec Quick config>
```

b) CHANGE REMOTE tunnel endpoint

Con este comando es posible modificar una entrada de la tabla de definición de túneles previamente introducida. Se indica la entrada concreta cuyos parámetros van a cambiarse a través de su identificador.

```
IPSec Quick config>change remote
Type IPSec remote tunnel endpoint identifier[0]? 11
Choose an IP connection as source address of local tunnel endpoint:

--- IP Connections ---

 Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth  NAPT
----  ------- -------  ------------------  -------  ----  ---------
IP1    LAN1    ----    172.24.78.8/16      IP       ---   NO
IP2    WAN1    ----    210.10.10.1/32      PPP      NONE  NO

IP connection identifier[2]?
Enter remote tunnel endpoint IP address [200.200.200.2]?200.200.200.3
Do you want to configure remote backup IP addresses(Yes/No)(Y)?
Enter remote backup IP address [0.0.0.0]? 200.200.200.4
Another remote backup IP address(Yes/No)(Y)?
Enter second remote backup IP address [0.0.0.0]?
No more remote backup IP addresses configured
Id type (HOSTNAME=1, IP ADDRESS=2)[2]? 1
NAPT enabled(Yes/No)(N)?
Enter lifetime (in seconds)[4200]? 3600
UDP encapsulation(Yes/No)(N)? y
IPSec Quick config>
```

c) CHANGE TRAFFIC selector

Este comando se utiliza para modificar alguno o algunos parámetros de un control de acceso IPSec previamente configurado, que será el del identificador dado.

```
IPSec Quick config>change traffic
Type IPSec traffic selector identifier[4]?
Destination IP address [172.60.1.163]? 172.60.1.1
Destination IP mask [255.255.255.255]?
Type IPSec remote tunnel endpoint identifier[11]?
IPSec Quick config>
```

27.4. CLEAR

Mediante el comando <CLEAR> pueden borrarse todas las entradas de la tabla de claves, todas las entradas de la tabla de definición de túneles o todos los controles de acceso IPSec configurados.

```
IPSec Quick config>clear ?
KEY
REMOTE tunnel endpoints
TRAFFIC selectors
IPSec Quick config>
```

a) CLEAR KEY

Borra todas las claves IPSec configuradas, es decir, los identificadores (hostname o dirección IP) de los extremos remotos y sus claves asociadas que el equipo local sería capaz de reconocer de modo que se pudiese establecer un túnel IPSec entre ambos extremos.

```
IPSec Quick config>clear key
IPSec Quick config>list key

No IPSec keys configured

IPSec Quick config>
```

b) CLEAR REMOTE tunnel endpoints

Con este comando se borran todas las entradas de la tabla de definición de túneles. Cada entrada de la tabla contiene los parámetros necesarios para configurar un túnel IPSec hacia un determinado destino.

```
IPSec Quick config>clear remote
IPSec Quick config>list remote

No IPSec remote tunnel endpoints configured

IPSec Quick config>
```

Hay que señalar que si se tiene configurada una tabla de selectores de tráfico y otra de definición de túneles a los que van asociados los selectores de tráfico, al eliminar los túneles, automáticamente se eliminan los selectores de tráfico asociados a dichos túneles. Lo mismo ocurre si se borra la tabla de conexiones IP: como todo túnel debe tener como origen una conexión IP existente, si se borran todas, necesariamente se eliminan también todas las entradas de la tabla de definición de túneles, y por extensión se borran además todos los selectores de tráfico configurados.

c) CLEAR TRAFFIC selectors

Provoca el borrado de todos los selectores de tráfico o controles de acceso IPSec existentes.

```
IPSec Quick config>clear traffic
IPSec Quick config>list traffic

No IPSec traffic selectors configured

IPSec Quick config>
```

27.5. DELETE

A través del comando <DELETE> es posible borrar una de las claves configuradas, una entrada de la tabla de definición de túneles o un control de acceso IPSec previamente introducido.

```
IPSec Quick config>delete ?
KEY
REMOTE tunnel endpoint
TRAFFIC selector
IPSec Quick config>
```

a) DELETE KEY

Borra una de las claves IPSec configuradas, la correspondiente a cierto identificador del extremo remoto (hostname o dirección IP): al introducir el comando <DELETE KEY> se pide el identificador del extremo remoto, borrándose éste y su clave asociada de la tabla de claves configuradas.

```
IPSec Quick config>list key

--- IPSec Keys ---

Remote Host Id                  Key
--------------                  --------
200.200.200.3                   ********

IPSec Quick config>delete key
Type the remote peer id to delete[]?200.200.200.3
IPSec Quick config>list key

No IPSec keys configured

IPSec Quick config>
```

b) DELETE REMOTE tunnel endpoint

Borra una entrada de la tabla de definición de túneles, aquella cuyo identificador sea el indicado.

```
IPSec Quick config>list remote

--- IPSec Remote Tunnel Endpoints ---

Ident IP Conn Remote Address   Backup Address   Loc Id Type NAPT Lifetime   UDP
----- ------- --------------   --------------   ----------- ---- --------   ---
11    IP2     200.200.200.3    200.200.200.4    HOSTNAME    NO   3600       YES

IPSec Quick config>delete remote
Type IPSec remote tunnel endpoint identifier[0]? 11
IPSec Quick config>list remote

No IPSec remote tunnel endpoints configured

IPSec Quick config>
```

c) DELETE TRAFFIC selector

Con este comando se borra el control de acceso de identificador dado.

```
IPSec Quick config>list traffic

--- IPSec Traffic Selectors ---

Identifier Destination IP Address Remote Tunnel Endpoint Id
---------- --------------------- -------------------------
4          172.60.1.1/32         11
```

```
IPSec Quick config> delete traffic
Type IPSec traffic selector identifier[0]? 4
IPSec Quick config>list traffic

No IPSec traffic selectors configured

IPSec Quick config>
```

27.6. DISABLE

El comando <DISABLE>, dentro del menú de configuración IPSec, permite deshabilitar IPSec.

```
IPSec Quick config>disable
IPSec disabled
IPSec Quick config>
```

27.7. ENABLE

Tan sólo hay que escribir el comando <ENABLE> para habilitar IPSec, aunque no entrará en funcionamiento hasta efectuar una operación MAKE desde el menú rápido global.

```
IPSec Quick config>enable
IPSec enabled
IPSec Quick config>
```

27.8. LIST

Se utiliza el comando <LIST> para visualizar el contenido de la configuración de IPSec.

```
IPSec Quick config>list ?
ALL
KEY
REMOTE tunnel endpoints
TRAFFIC selectors
IPSec Quick config>
```

a) LIST ALL

Se muestra toda la configuración de IPSec.

```
IPSec Quick config>list all

IPSec enabled

--- IP Connections ---

 Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth  NAPT
----  ------- -------  ------------------  -------  ----  ---------
IP1    LAN1    ----    172.24.78.8/16      IP       ---   NO
IP2    WAN1    ----    210.10.10.1/32      PPP      NONE  NO

--- IPSec Remote Tunnel Endpoints ---

Ident IP Conn Remote Address   Backup Address   Loc Id Type NAPT Lifetime   UDP
----- ------- --------------   --------------   ----------- ---- --------   ---
11    IP2     200.200.200.3    200.200.200.4    HOSTNAME    NO   3600       YES
```

```
--- IPSec Traffic Selectors ---

Identifier Destination IP Address Remote Tunnel Endpoint Id
---------- ---------------------- -------------------------
4          172.60.1.163/32        11

--- IPSec Keys ---

Remote Host Id                    Key
--------------                    --------
200.200.200.3                     ********
200.200.200.4                     ********

IPSec Quick config>
```

b) LIST KEY

Mediante este comando se pueden ver todas las entradas existentes en la tabla de claves; es decir, permite conocer qué extremos remotos, identificados por su dirección IP o por su hostname, tienen clave configurada.

```
IPSec Quick config>list key

--- IPSec Keys ---

Remote Host Id                    Key
--------------                    --------
200.200.200.3                     ********
200.200.200.4                     ********

IPSec Quick config>
```

c) LIST REMOTE tunnel endpoints

Se visualizan todas las entradas de la tabla de definición de túneles. Cada una de esas entradas contiene los parámetros necesarios para configurar un túnel IPSec hacia un determinado destino.

```
IPSec Quick config>list remote

--- IPSec Remote Tunnel Endpoints ---

Ident IP Conn Remote Address   Backup Address   Loc Id Type NAPT Lifetime   UDP
----- ------- --------------   --------------   ----------- ---- --------   ---
11    IP2     200.200.200.3    200.200.200.4    HOSTNAME    NO   3600       YES

IPSec Quick config>
```

d) LIST TRAFFIC selectors

Con este comando se procede a mostrar por pantalla todos los selectores de tráfico o controles de acceso IPSec configurados.

```
IPSec Quick config>list traffic

--- IPSec Traffic Selectors ---

Identifier Destination IP Address Remote Tunnel Endpoint Id
---------- ---------------------- -------------------------
4          172.60.1.163/32        11

IPSec Quick config>
```

27.9. EXIT

Use este comando para volver al prompt anterior.

```
IPSec Quick config> EXIT
Quick config>
```

27.10. EJEMPLO DE GENERACIÓN DE LA CONFIGURACIÓN REAL DE IPSEC A PARTIR DE LA CONFIGURACIÓN RÁPIDA

Al efectuar la operación MAKE para que a partir de la configuración introducida a través del menú rápido se genere la configuración real del equipo, en el caso de IPSec estos son los pasos a seguir:

- Debe borrarse la configuración existente en los registros de SRAM correspondientes a IPSec.
- Con la información que contenga la variable global para habilitar/deshabilitar IPSec se procede a inicializar la variable utilizada con este fin en la configuración real de IPSec.
- QOS Preclassify deshabilitado por defecto.
- Por cada una de las entradas existentes en la tabla de definición de túneles se crean dos templates o túneles IPSec: uno de tipo isakmp (para la fase I) y otro dinámico (para la fase II). En los dos casos se utilizará cifrado 3DES y autenticación MD5, anti-replay habilitado, grupo Oakey 1, PFS deshabilitado, modo agresivo con identificación por Fully-Qualified Domain Name (ID_FQDN) si el extremo local actúa como cliente, utilizando su hostname como identificador, y si es servidor se identificará a través de su dirección IP. El tiempo de vida de la fase I será el configurado en la correspondiente entrada de la tabla, y el de la fase II, el resultante tras multiplicar ese valor por el factor 3300/3600. Como dirección origen de los templates se coge la correspondiente a la conexión IP indicada en la entrada de la tabla de definición de túneles a partir de la cual se crean los dos templates IPSec, y también se sacan de ahí la dirección principal y las de backup del extremo remoto del túnel. Para los templates dinámicos, si se trata de un Teldat C3, y alguna de las direcciones configuradas en los perfiles TRMTP o TCP corresponde a una subred definida por alguno de los controles de acceso asociados a ese template, se debe habilitar el KeepAlive. Los valores para el KeepAlive (a nivel global) se determinan de la siguiente forma: se van revisando todas las direcciones configuradas en los perfiles TCP (en primer lugar), y se escoge el mayor valor del parámetro que indica el timeout configurado para aquellas direcciones pertenecientes a alguna subred definida por alguno de los controles de acceso como número máximo de segundos sin respuesta, y como número máximo de paquetes sin respuesta se coge el valor 10.

  Solamente en el caso de que no se haya encontrado ninguna dirección de esas subredes en los perfiles TCP, se pasa a buscar entre las direcciones configuradas en perfiles TRMTP aquellas que pertenezcan a las subredes destino de los controles de acceso, escogiendo como valor del número máximo de segundos sin respuesta el mayor de los productos T1*N2, y como número máximo de paquetes sin respuesta, 2. Si no se encuentra ninguna dirección de las subredes destino de los controles de acceso ni en los perfiles TCP ni en los TRMTP se cogen los valores por defecto:

  - Número máximo de paquetes sin respuesta 2.
  - Número máximo de segundos sin respuesta 20.
  - Si el equipo no es un Teldat C3, KeepAlive (a nivel global) deshabilitado.
- Por cada uno de los selectores de tráfico configurados se creará un control de acceso IPSec por cada conexión IP, con dirección origen la subred definida por dicha conexión IP, y la

dirección destino y su máscara los configurados; si la dirección es no numerada o coincide con el origen del túnel al que va asociado el selector se utiliza máscara de host. Ese control de acceso irá asociado al template dinámico originado a partir de la entrada de la tabla de definición de túneles cuyo identificador sea el que se ha configurado para el selector de tráfico. También se creará a partir de cada entrada de la tabla de selectores de tráfico un control de acceso por cada ruta directamente conectada, siempre que no se trate de la ruta por defecto y que la ruta no utilice la misma conexión IP sobre la que va el túnel al que se asocia el selector. En caso de que se habilite NAPT en el túnel al que va asociado el selector de tráfico, tan sólo se creará un control de acceso IPSec a partir del citado selector, cuya dirección origen será la de la IP Connection que se toma como origen del túnel y con máscara de host. Cada control de acceso generado va asociado a una conexión o regla IP, regla que corresponde a la conexión IP origen del túnel al que va asociado dicho control de acceso. Si ya existía una regla para esa conexión IP, no se modifica (si correspondía a una regla NAPT, seguirá utilizándose para NAPT, por ejemplo), y si no existe una regla IP generada a partir de esa conexión IP, se crea una, con origen la dirección IP origen del túnel al que se asocia el selector, destino la dirección 0.0.0.0, NAPT deshabilitado y firewalling también deshabilitado. Además en el caso de tratarse de un Teldat C3, se comprueban los Centrix-D configurados en el menú rápido de POS, y si los destinos de los selectores de tráfico configurados en el menú rápido de IPSec coinciden con dichos Centrix-D, se generan controles de acceso IPSec que tengan restringidos los puertos y protocolos a los empleados en transporte POS sobre IP usado por el Teldat C3; es decir, si alguna de las direcciones configuradas en los perfiles TRMTP y TCP pertenece a la subred definida por la dirección y máscara del correspondiente selector de tráfico, el rango de puertos asociados a ese control de acceso comprenderá tan sólo el número de puerto configurado en ese perfil y para esa dirección concreta, y el rango de protocolos se reducirá al protocolo TCP si es éste el modo de transporte POS sobre IP que se ha configurado para ese Centrix-D como destino (es decir, si esa dirección se encontró en un perfil TCP), o al protocolo UDP si se utilizará modo de transporte basado en TRMTP hacia ese Centrix-D (la dirección pertenecía a un perfil TRMTP).

- A partir de las claves configuradas y los hostnames/direcciones IP asociados a ellas se crea la lista real de claves IPSec.
- Se guarda la configuración.

Si se tiene la siguiente configuración de IPSec en el menú rápido:

```
IPSec Quick config>list all

IPSec enabled

--- IP Connections ---

 Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth  NAPT
----  ------- -------  ------------------  -------  ----  ---------
IP1    LAN1    ----    172.24.78.8/16      IP       ---   NO
IP2    WAN1    ----    210.10.10.1/32      PPP      NONE  NO


--- IPSec Remote Tunnel Endpoints ---

Ident IP Conn Remote Address   Backup Address   Loc Id Type NAPT Lifetime   UDP
----- ------- --------------   --------------   ----------- ---- --------   ---
11    IP2     200.200.200.3    200.200.200.4    HOSTNAME    NO   3600       YES
```

```
--- IPSec Traffic Selectors ---

Identifier Destination IP Address Remote Tunnel Endpoint Id
---------- ---------------------- ------------------------
4          172.60.1.163/32        11


--- IPSec Keys ---

Remote Host Id                   Key
--------------                   --------
200.200.200.3                    ********
200.200.200.4                    ********
IPSec Quick config>
```

La configuración IPSec generada tras realizar la operación MAKE y reiniciar es la siguiente:

```
Config>protocol ip
IP config>ipsec
IPSec config>list all
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

ACCESS-LIST
1     IPS SRC=172.24.0.0/16 DES=172.60.1.163/32 Conn:1   (DB8B34)
        NORMAL ENTRY. Templates: 2

2     IPS SRC=210.10.10.1/32 DES=172.60.1.163/32 Conn:1   (DB8B34)
        NORMAL ENTRY. Templates: 2

TEMPLATES
1 isakmp 3DES MD5  DES=200.200.200.3
         BACKUP DES 1=200.200.200.4
   LifeTime:1h0m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
   OAKLEY GROUP 1
   UDP Encapsulation

2 dynamic ESP-3DES ESP-MD5  SRC=210.10.10.1 DES=200.200.200.3
   LifeTime:0h55m0s 4608000 kbytes
   PFS disabled

2 key entries
   200.200.200.3 ************
   200.200.200.4 ************
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 2.
   Timeout after last packet encoded: 20 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

IPSec config>
```

Podemos observar que aunque los identificadores han cambiado con respecto a la configuración en el submenú rápido de IPSec, las asociaciones entre túneles y selectores de tráfico sí son las correctas como se ha explicado con anterioridad.

28. Parámetros de terminales punto de venta

La configuración y monitorización rápida (submenú POS) puede consultarla en el manual específico para la configuración del soporte de terminales de punto de venta que incluye tanto la configuración y monitorización rápida como la configuración y monitorización estándar.

29. Parámetros de IP-Discovery (TIDP)

El TIDP (Teldat IP Discovery Protocol) es un protocolo que permite a los equipos ***TELDATC*** notificar la dirección IP obtenida en una conexión IP a una serie de estaciones de descubrimiento de direcciones para que el equipo pueda ser accedido por las estaciones remotas de gestión con el fin de gestionarlo.

Para ello el equipo envía unos mensajes especiales a las estaciones de descubrimiento de direcciones IP. Estos paquetes se envían periódicamente, mediante UDP, a unas direcciones y puertos configurados en los equipos ***TELDATC***. De este modo las estaciones de descubrimiento de direcciones IP notificarán a las aplicaciones de gestión en qué dirección se encuentra el equipo que originó los mensajes y así podrán acceder al mismo para gestionarlo.

Para configurar y añadir las estaciones de descubrimiento de direcciones IP (IP Discovery Stations), use el comando `<ADD DISCOVERY>`. Se permite configurar hasta 99 estaciones.

```
Quick config>add discovery
Type Discovery Station identifier (1-99)[0]? 1
Type Discovery Station IP address [0.0.0.0]? 123.45.67.89
Type Discovery Station port (Destination Port)[0]? 5005
Type Local port (Source Port)[0]? 4004
Type Notification interval (seconds)[0]? 60
Quick config>
```

- **Discovery Station identifier**

  Identificador de la Discovery Station. El rango permitido está entre 1 y 99.

- **Discovery Station IP address**

  Dirección IP de la Discovery Station. Es la dirección a la que el equipo ***TELDATC*** enviará las notificaciones de dirección.

- **Discovery Station port**

  Puerto de transporte (UDP) al que se envían los mensajes.

- **Local port**

  Puerto de transporte (UDP) local en el que se escuchan los mensajes.

- **Notification interval**

  Tiempo entre envíos de notificaciones (en segundos).

Se pueden definir hasta 99 estaciones de descubrimiento de direcciones. Para ver las estaciones configuradas se debe ejecutar el comando `<LIST DISCOVERY>`.

```
Quick Config>list discovery

--- IP DISCOVERY Stations ---
ID  IP address       Dest. Port  Source Port  Notif. Time  Protocol
--  ---------------  ----------  -----------  -----------  --------
 1  123.45.67.89         5005        4004        60 secs.     UDP
 2  212.95.195.132      24000       24001        30 secs.     UDP

Quick config>
```

Se puede eliminar la IP Discovery Station que se desee con el comando `<DELETE DISCOVERY>` y modificar los parámetros configurados con el comando `<CHANGE DISCOVERY>`.

30. Grabación y generación de configuración

Para grabar la configuración dispone del comando <SAVE>, y <MAKE> para generarla; la generación de la configuración implica su grabación.

```
Quick Config>save
Do you really want to save the configuration (Yes/No)(N)? y
Configuration saved successfully
Quick Config>
```

```
Quick Config>make
Do you really want to make the configuration (Yes/No)(N)? y
Configuration generated and saved successfully
Quick Config>
```

Es muy recomendable reiniciar el equipo una vez generada la configuración dado que muchos parámetros no toman efecto hasta el reinicio del equipo; no realizar el reinicio puede provocar inestabilidades en la configuración del equipo.

31. Valores de la configuración por defecto

El equipo presenta de fábrica una configuración por defecto. Dicha configuración puede volver a ser activada por el usuario, mediante el procedimiento de recarga de la configuración por defecto descrito en el manual de instalación (activación del micro interruptor 5 situado en la base del equipo durante la secuencia de arranque) o mediante el comando de configuración <SET DEFAULT-CONF>. Cuando activa la configuración por defecto mediante este comando, únicamente se modifica la configuración "visible", no se modifica la configuración que está en ejecución, por lo que si está accediendo remotamente no perderá la conectividad; tampoco perderá la configuración si no se graba la configuración antes de reiniciar, es decir, si ejecuta el comando y reinicia, no pierde la configuración anterior.

```
Config>set default-conf
All your session changes will be lost.
Activate default configuration (Yes/No)? y
Config>
```

Los valores por defecto pueden son los siguientes, excepto casos especiales:

- Parámetros de acceso:
  - usuario y password de acceso vacíos
- Parámetros RDSI
  - canales B en tipo conmutado y llamadas entrantes deshabilitadas
- Parámetros WAN:
  - en modo de comandos AT, velocidad 57600 (excepto modelos C3x)
  - en modo POS, velocidad 9600 (modelos C3x)
- Parámetros RTC
  - llamadas entrantes deshabilitadas
  - detección de patrón de llamada deshabilitado
- Parámetros SNMP
  - comunidad "public" de lectura con acceso restringido a la MIB-2
  - envío de ECHO UDP antes de envío de traps
- Parámetros ADSL
  - velocidad mínima de transmisión será 1/25 de la velocidad de transmisión obtenida.
  - Funcionamiento en modo MULTIMODO
- Conexiones IP
  - conexión IP basada en LAN con dirección 192.168.1.1 máscara 255.255.255.0 sin NAPT
- Servidor DHCP activado:
  - rango de direcciones: 192.168.1.1 - 192.168.1.255.
  - máscara de subred: 255.255.255.0.
  - router por defecto: 192.168.1.1 (el propio equipo).
  - servidor DNS: 192.168.1.1
  - tiempo de sesión: 1 día (1440 minutos).

En estas condiciones, los clientes DHCP conectados a la LAN del router obtendrán una dirección IP de la red 192.168.1.0/24, exceptuando la dirección 192.168.1.1 que está asignada al interfaz LAN del propio router. Se puede acceder al router mediante Telnet, a través de FTP (accediendo como usuario "root" sin clave) o por http (usuario “teldat” con clave “teldatc”).

También es posible obtener estadísticos del equipo a través de SNMP y la comunidad "public". Por defecto sólo se tendrá acceso de lectura a las variables de la MIB-2.

Capítulo 3
Monitorización por línea de comandos

1. Menú rápido de monitorización

Mediante el menú de monitorización rápida dispone de una visión global de los estadísticos asociados a la configuración generada a través del menú de configuración rápida. Para acceder a esta monitorización, introduzca los siguientes comandos desde el menú del sistema:

```
*process 3
Console Operator
+quick
Quick Monitor Menu
Quick Monitor>
```

La monitorización rápida se divide en dos partes claramente diferenciadas:

- Monitorización diaria: estadísticos desde la iniciación del equipo. Si se apaga el equipo o se reinicia, estos estadísticos se borran.
- Monitorización quincenal: estadísticos de los últimos quince días. Periódicamente se guardan en memoria no volátil los estadísticos acumulados para el día en curso, y cuando se produce el cambio de día, se reinician los estadísticos.

A continuación se detallan los estadísticos que se pueden consultar en cada uno de estos menús de monitorización.

El número de estadísticos que puede almacenar en memoria el router TELDAT C está limitado, y varía según los interfaces que tenga disponibles el equipo.

En un apéndice de este manual se detalla el número exacto de estadísticos según los interfaces del router.

2. Estadísticos diarios

Dos son los comandos que se pueden ejecutar relacionados con la monitorización de los estadísticos diarios: con el comando `<LIST DAILY>` se pueden visualizar los estadísticos, y con el comando `<CLEAR DAILY>` se reinician dichos estadísticos. A continuación se muestra un ejemplo de visualización de los estadísticos asociados a la monitorización diaria:

```
Quick Monitor>list daily

--- LAN statistics ----
Status             : UP
Collisions         : 3
Errors             : 3
Bytes received     : 1848321
Bytes transmitted  : 38692

--- ADSL statistics ---
Authentications accepted   : 0
Authentications refused    : 0
Packets with invalid port  : 0

--- ISDN statistics ---
Authentications accepted B1 channel : 1
Authentications rejected B1 channel : 0
Authentications accepted B2 channel : 0
Authentications rejected B2 channel : 5

--- PSTN statistics ---
Authentications accepted PSTN : 0
Authentications rejected PSTN : 0

Stations that caused calls:
Ind Date     Time     IP Source       IP Target       Prtcl Src. port Trgt. port
--- ----     ----     ---------        ---------       -----  --------- ----------
 1  09:14:01 11:57:33 192.69.101.1    192.69.100.5    1     0          0
 2  09:14:01 11:58:47 192.69.101.1    192.69.100.5    1     0          0
 3  09:14:01 11:59:55 192.69.101.2    172.24.78.47    17    2006       2006
 4  09:14:01 12:04:05 192.69.101.1    192.69.102.5    1     0          0
 5  09:14:01 12:05:08 192.69.101.2    172.24.78.47    17    2006       2006

There are no active calls

--- Released calls ---
L T CALLED N.    CALLING N.   CC  DC  T/START  T/END    D/START  D/END    CHARGE
- - ---------    ----------   --- --- -------  -----    -------  -----    ------
1 O 5300         5200         102 000 11:57:37 11:57:41 09/14/01 09/14/01 000000
1 O 5300         5200         027 000 11:57:48 11:58:33 09/14/01 09/14/01 000000
1 I 5201         5301         016 000 11:59:16 11:59:50 09/14/01 09/14/01 000000
1 O 5300         5200         016 000 11:58:49 12:01:09 09/14/01 09/14/01 000000
1 O 5400         5201         016 000 11:59:55 12:03:18 09/14/01 09/14/01 000000
1 I 5201         5301         016 000 12:04:32 12:05:02 09/14/01 09/14/01 000000
1 O 5300         5200         016 000 12:04:05 12:06:30 09/14/01 09/14/01 000000


There are not visible subnets defined


There are not visible ports defined


Management status : FALSE

Quick Monitor>
```

Entre los estadísticos diarios podemos destacar los siguientes grupos:

- Estadísticos de la interfaz LAN: estado, número de colisiones, número de errores y bytes transmitidos y recibidos.

- Estadísticos de la interfaz ADSL: Autenticaciones exitosas y fracasadas (para conexiones tipo PPP) y paquetes recibidos por una conexión con NAPT habilitado cuyo destinatario es un puerto no válido (paquetes TCP/UDP) o con identificador no válido (paquetes ICMP).

- Estadísticos de la interfaz RDSI: autenticaciones exitosas y fracasadas para los dos canales B del acceso básico.

- Estadísticos de la interfaz RTC: autenticaciones exitosas y fracasadas.

- Estadísticos de las estaciones que han causado la llamada, indicando la fecha y la hora de la llamada, la dirección IP origen, la dirección IP destino, el tipo protocolo que originó la llamada y el puerto origen y destino de la llamada.

- Las llamadas activas en el momento de pedir los estadísticos.

- Estadísticos de las llamadas liberadas. Donde se pueden ver los siguientes parámetros: la línea RDSI de la llamada (L), el tipo de la llamada (T), con (I) si es entrante o (O) si saliente, número llamado y número llamante, causa de la liberación(CC), diagnostico de la liberación(DC), hora y fecha en que se estableció la llamada, hora y fecha en que se liberó la llamada, coste de la llamada si lo proporciona la operadora.

- Estadísticos de las subredes visibles definidas: estadísticos de tráfico entrante y saliente, tanto en bytes como en número de paquetes, por subred visible.

- Estadísticos de los puertos visibles definidos: estadísticos de tráfico entrante y saliente, tanto en bytes como en número de paquetes, por puerto visible. También se muestran unos estadísticos totales para los puertos visibles (paquetes enviados / recibidos).

3. Estadísticos quincenales

Dos son los comandos que se pueden ejecutar relacionados con la monitorización de los estadísticos quincenales: con los comandos <LIST FORTNIGHLY ISDN> o <LIST FORTNIGHLY ADSL> se pueden visualizar los estadísticos, y con el comando <CLEAR FORTNIGHLY> se reinician dichos estadísticos.

A continuación se muestra un ejemplo de visualización de los estadísticos asociados a la monitorización quincenal de los estadísticos de RDSI:

```
Quick Monitor>list fortnightly isdn

--- Last Fortnight ISDN statistics ---

Ix Date     Bytes B1   Packs B1   Time B1    Calls B1   Auth OK B1
           Bytes B2   Packs B2   Time B2    Calls B2   Auth OK B2
-- -------- ---------- ---------- ---------- ---------- ----------
1  09/14/01 299380     4058       177200     12         0
           38340      469        28100      0          0
2  09/13/01 59376      860        105300     21         0
           6300       75         0          0          0
3  09/12/01 0          0          0          0          0
           0          0          0          0          0
4  09/11/01 0          0          0          0          0
           0          0          0          0          0
5  09/10/01 0          0          0          0          0
           0          0          0          0          0
6  09/09/01 28944976   28768      457600     65         0
           683092     5130       30600      8          0
7  09/08/01 62580      745        56400      26         0
           8820       105        12000      4          0

Type index of the day whose ISDN statistics you want to view [0]? 1

--- Per host ISDN statistics ---

Ix Host Address    Total Packets B1 Total Packets B2
-- --------------- ---------------- ----------------
1  192.69.101.1    0                1697
2  192.69.102.5    973              0
3  0.0.0.9         0                1500
4  192.69.100.3    348              0


--- Favorite sites ISDN statistics ---

Ix Favorite Site   Total Packets
-- --------------- ----------------
1  192.69.100.5    1697
2  192.69.102.5    973
3  192.69.102.3    9
4  192.69.103.5    1500
5  192.69.100.3    348

Quick Monitor>
```

Los estadísticos quincenales RDSI muestran la siguiente información:

- Una tabla con los estadísticos de cada uno de los días de la quincena: la primera línea de la tabla corresponde al día actual, la segunda al día anterior y así sucesivamente hasta los quince días. En la tabla se pueden ver los siguientes parámetros:

- Fecha
- tráfico por B1 y B2 en bytes
- tráfico por B1 y B2 en paquetes
- tiempo que han estado los canales con la llamada establecida (el valor está expresado en tic time, 1s = 360 tic time)
- llamadas por B1 y B2
- autorizaciones exitosas en B1 y B2.

- Estadísticos de un día en concreto. Podemos ver dos tablas:
  - los host que han originado el tráfico
    - Dirección IP del host
    - Tráfico en paquetes por B1 y B2.
  - las direcciones accedidas (favoritas)
    - Direcciones IP accedidas
    - Tráfico total en paquetes.

Los estadísticos quincenales ADSL muestran la siguiente información:

- Una tabla con los estadísticos de cada día de la quincena, la primera línea de la tabla corresponde al día actual, la segunda al día anterior y así sucesivamente hasta los quince días. En la tabla se pueden ver los siguientes parámetros:
  - Fecha
  - Última vez que la entrada fue actualizada
  - Tráfico entrante y saliente en bytes
  - Tráfico entrante y saliente en paquetes
  - Autenticaciones exitosas y fallidas en enlaces PPP sobre ADSL.

- Estadísticos de un día en concreto. Podemos ver dos tablas:
  - los host que han originado el tráfico
    - Dirección IP del host
    - Tráfico en bytes y en paquetes dirigido a ese host y originado por él
  - las direcciones accedidas (favoritas):
    - Direcciones IP accedidas
    - Tráfico en bytes y en paquetes dirigido a esa dirección y procedente de ella

Capítulo 4
Apéndices

1. Visión global del menú rápido

En la figura siguiente se pretende dar una visión gráfica de los elementos de la configuración rápida: se presentan cinco bloques principales representando cada uno de los interfaces físicos de los que puede disponer el equipo:

1) LAN
2) ADSL sobre POTS
3) RDSI
4) WAN
5) UART

Cada escalón representa un nivel de configuración, por ejemplo: se puede configurar parámetros de la línea ADSL, posteriormente y solo sobre la línea ADSL, se pueden configurar conexiones AAL-ATM, sobre las que a su vez se pueden definir conexiones IP que pueden ser de dos tipos: IP y PPP; a su vez, relacionado con las conexiones IP se pueden definir rutas, reglas NAT, etc.

En el caso de la WAN, se puede configurar en varios modos (PSTN, ASDP, POS....), y si se configura en modo PSTN, se pueden configurar MANAGERS y conexiones IP de tipo PPP.

Aisladamente, está la configuración de DHCP, DNS, SNMP, etc.

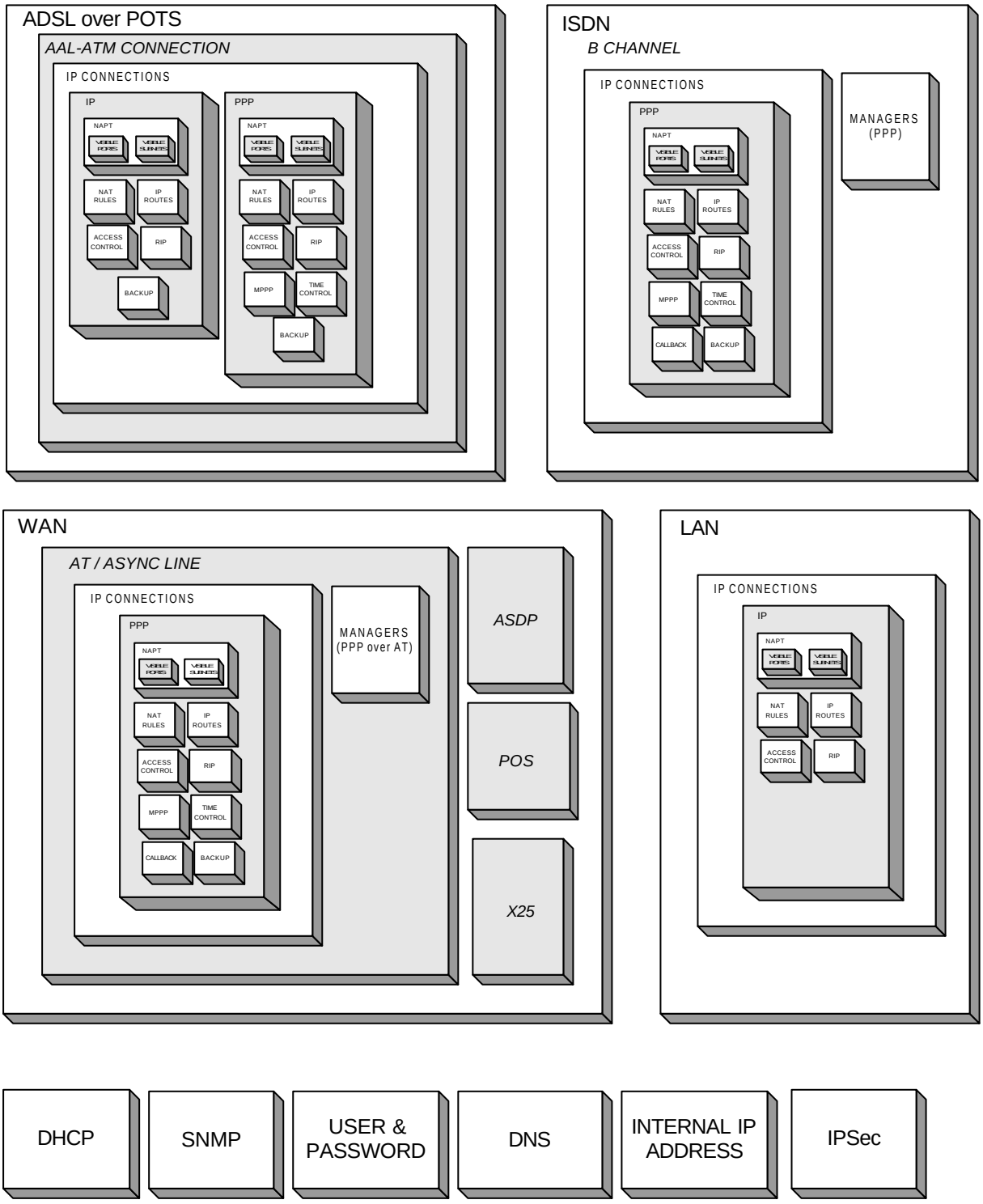

Figura 4.1: Visión gráfico de la configuración rápida

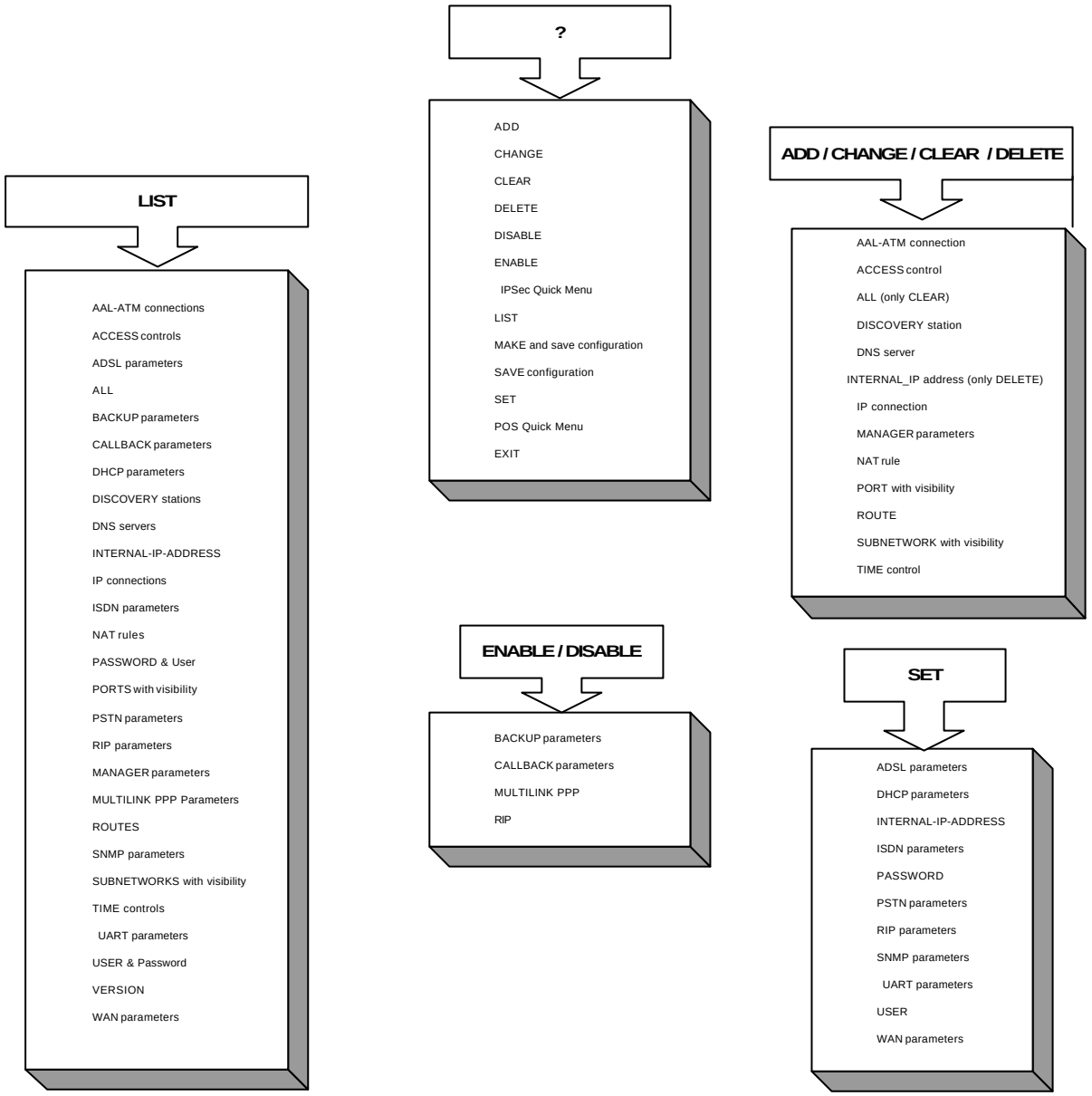

Figura 4.2: Esquema de los menús de configuración y monitorización rápida

2. Estadísticos no volátiles

A continuación se presenta una tabla donde se muestra el número de estadísticos almacenados en router ***TELDAT C*** según el número de interfaces de que disponga.

	ADSL	ISDN	POS	
Destinos más frecuentes	256			Transacciones OK
Hosts más activos	50			Transacciones KO
Destinos más frecuentes		256		Transacciones OK
Hosts más activos		50		Transacciones KO
Destinos más frecuentes	128	128		Transacciones OK
Hosts más activos	25	25		Transacciones KO
Destinos más frecuentes	128		1000	Transacciones OK
Hosts más activos	25		500	Transacciones KO
Destinos más frecuentes		256	1000	Transacciones OK
Hosts más activos		50	500	Transacciones KO
Destinos más frecuentes	64	64	1000	Transacciones OK
Hosts más activos	12	12	500	Transacciones KO

La forma de consultar la tabla anterior consiste en buscar una pareja de filas que tengan aspas en aquellos interfaces de los que no dispone su equipo; por ejemplo, si su equipo dispone de ADSL y RDSI pero no soporta TPVs, la pareja de filas que le corresponden es la tercera, donde se observa que el número de destinos más frecuentes accedidos por ADSL son 128, al igual que por RDSI, y que el número de hosts más activos (que provocan mayor tráfico), es de 25 en ambos casos. Si su equipo dispone de línea RDSI y soporta TPVs, su pareja de filas es la quinta, donde se observa que el número de destinos más frecuentes es 256, los 50 hosts más activos y el almacenamiento de 1000 transacciones realizadas con éxito y 500 fallidas.

3. Configuración de los hosts

En este apartado se muestran posibles ejemplos de configuración de los puestos de la red de área local (LAN), en los sistemas operativos más comunes, para acceder a las redes externas a través del router ***TELDAT C.*** Los ejemplos de configuración reflejan un escenario en el que el puesto local ocupa la dirección 192.6.1.168/24 en la LAN y el router ***TELDAT C*** ocupa la dirección 192.6.1.224/24.

No se intenta dar una descripción detallada del proceso de configuración en cada plataforma, objetivo que se sale de la intención de este manual, sino indicar el proceso básico de configuración en los aspectos que más pueden influenciar al funcionamiento con el router ***TELDAT C***. Para una descripción detallada de cada plataforma, consultar los manuales del fabricante de la misma.

3.1. Puestos con el sistema operativo Windows 95 o 98

a) Configuración básica

La configuración básica del protocolo TCP/IP de un PC con sistema operativo Windows 95 se realiza desde el icono "Entorno de Red" del "Panel de control". La Figura 4.3 muestra el cuadro de diálogo de "Entorno de Red" de un PC al que se le ha configurado el protocolo TCP/IP sobre una tarjeta Ethernet.

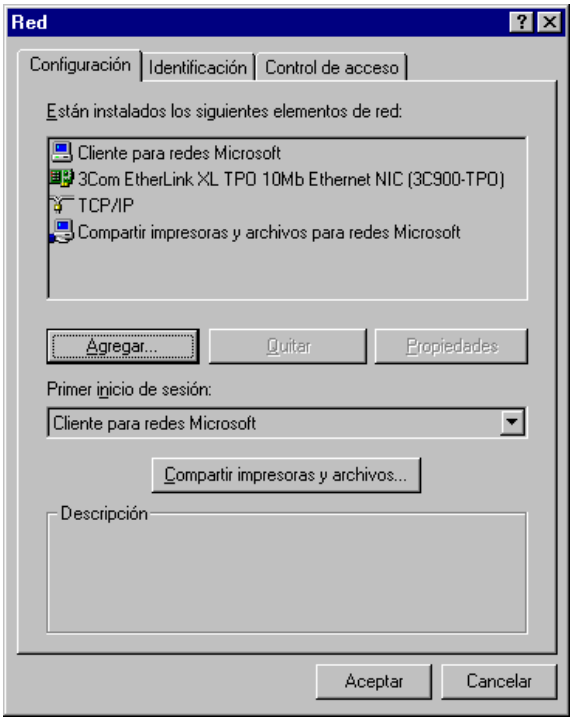

Figura 4.3: Entorno de Red de Microsoft Windows 95

Para configurar los parámetros de TCP/IP es necesario abrir el cuadro de diálogo de TCP/IP desde el anterior cuadro de diálogo de Red. La Figura 4.4 muestra la solapa en la que se configura la dirección del PC en la LAN.

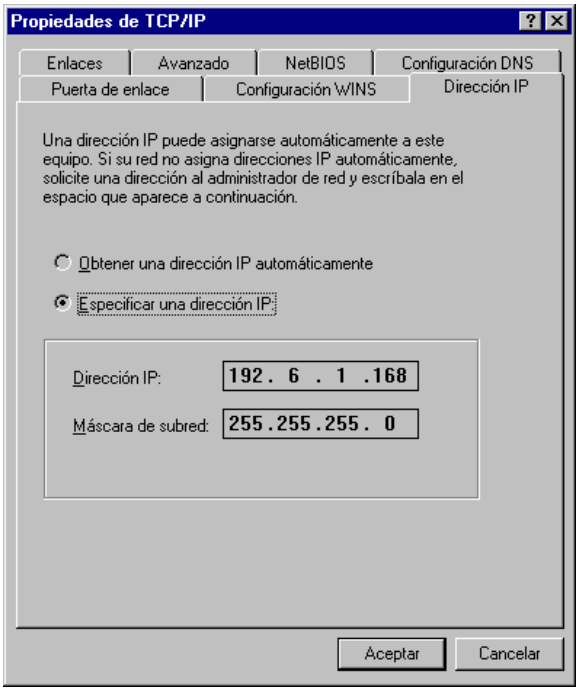

Figura 4.4: Dirección IP de un PC con Windows 95

La **Figura 4.5** muestra la solapa de configuración de la ruta por defecto del PC.

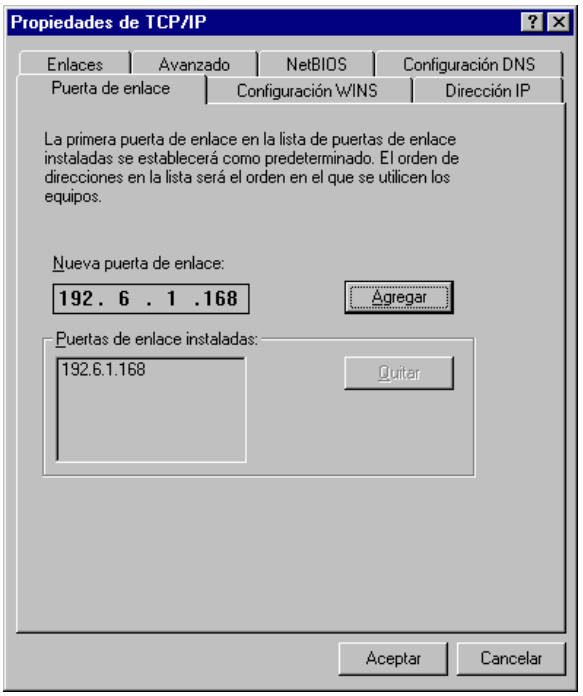

Figura 4.5: Router por defecto de un PC con Windows 95

Por último, la **Figura 4.6** muestra la configuración de parámetros DNS de un PC con el sistema operativo Windows 95.

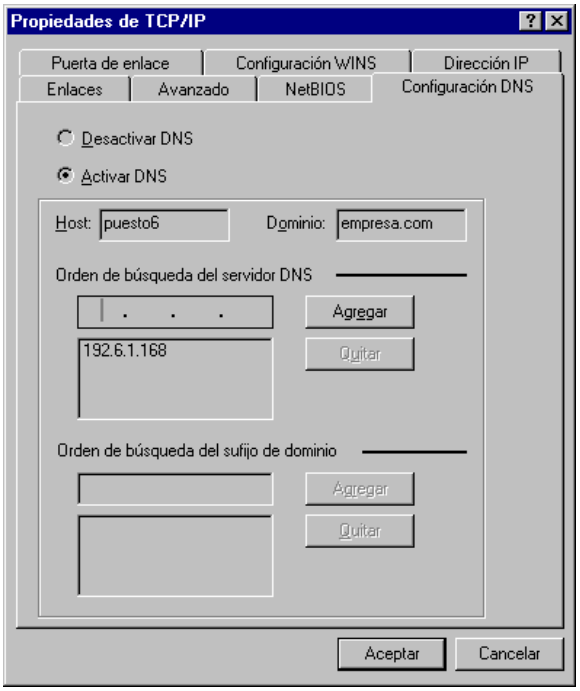

Figura 4.6: Parámetros DNS de un PC con Windows 95

b) Configuración avanzada

Configuración dinámica de rutas

Desde una sesión de MS-DOS dentro de Windows 95 es posible agregar y borrar rutas dinámicamente con el comando **ROUTE**. A continuación se muestra una ayuda de este comando.

```
c:\>ROUTE -?
Manipulates network routing tables.
ROUTE [-f] [command [destination] [MASK netmask] [gateway]]

  -f           Clears the routing tables of all gateway entries. If this is used in
               conjunction with one of the commands, the tables are cleared prior to
               running the command.

  Command      Specifies one of four commands
                     PRINT     Prints a route
                     ADD       Adds a route
                     DELETE    Deletes a route
                     CHANGE    Modifies an existing route

  destination Specifies the host to send command.

  MASK         If the MASK keyword is present, the next parameter is interpreted as
               the netmask parameter.
```

```
  Netmask      If provided, specifies a sub-net mask value to be associated with
               this route entry. If not specified, if defaults to 255.255.255.255.
  gateway      Specifies gateway.

All symbolic names used for destination or gateway are looked up in the network and
host name database files NETWORKS and HOSTS, respectively.  If the command is print
or delete, wildcards may be used for the destination and gateway, or the gateway
argument may be omitted.
```

En el escenario que se está describiendo, la salida del comando "**ROUTE PRINT**" es la que se muestra a continuación. Nótese que la pila TCP/IP se configura automáticamente para soportar las direcciones de broadcast de red, local loop y multicast.

```
c:\>ROUTE PRINT

Active Routes:

Network Address  Netmask          Gateway Address  Interface    Metric
0.0.0.0          0.0.0.0          192.6.1.224      192.6.1.168  1
127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1    1
192.6.1.0        255.255.255.0    192.6.1.168      192.6.1.168  1
192.6.1.168      255.255.255.255  127.0.0.1        127.0.0.1    1
192.6.1.255      255.255.255.255  192.6.1.168      192.6.1.168  1
224.0.0.0        224.0.0.0        192.6.1.168      192.6.1.168  1
255.255.255.255  255.255.255.255  192.6.1.168      0.0.0.0      1

c:\>
```

Parámetros del Registro del Sistema

Además de la configuración gráfica explicada, es posible configurar ciertos parámetros de la pila TCP/IP de Microsoft para Windows 95 directamente en el registro del sistema. Consultar [MICROSOFT-95] para más información. Para modificar el registro del sistema se puede usar el editor del registro del sistema de Windows 95 (regedit.exe). A continuación se da una breve descripción de los parámetros que más pueden tener que ver con el router ***TELDAT C***. Para que dichos parámetros tomen efecto es necesario reiniciar el PC.

Rama Hkey_Local_Machine\System\CurrentControlSet\Services\VxD\MSTCP:

Valor	**Tamaño**	**Descripción**
DefaultRcvWindow	16-bit	Especifica la ventana de recepción por defecto anunciada por TCP. Por defecto 8192.
DefaultTOS	8-bit	Especifica el tipo de servicio (TOS) por defecto para los paquetes IP. Por defecto 0.
DefaultTTL	8-bit	Especifica el TTL inicial por defecto. Por defecto 32.
DnsServerPort	16-bit	Especifica el puerto del servidor DNS al que mandar las consultas. Por defecto 53.
KeepAliveTime	32-bit	Especifica, en milisegundos, el tiempo de inactividad, pasado el cual TCP empezará a mandar "keepalives", si los "keepalives" están permitidos en la conexión TCP. Por defecto 2 horas (7200000).
KeepAliveInterval	32-bit	Especifica el tiempo, en milisegundos, entre retransmisiones de "keepalives", una vez que el KeepAliveTime ha expirado. Una vez que el KeepAliveTime ha expirado, los "keepalives" se envían cada KeepAliveInterval milisegundos hasta que se reciba respuesta o hasta un máximo de MaxDataRetries antes de abortar la conexión. Por defecto, un segundo (1000).
MaxConnections	32-bit	Especifica el máximo número de conexiones concurrentes. Por defecto, 100.

MaxConnectRetries	32-bit	Especifica el número de veces que un intento de conexión (SYN) será transmitido antes de abandonar. El timeout inicial de retransmisión es 3 segundos y se dobla cada vez, hasta un máximo de dos minutos. Por defecto, 3.
MaxDataRetries	32-bit	Especifica el máximo número de veces que un segmento TCP de datos o un fin de conexión (FIN) será retransmitido antes de que la conexión sea abortada. El tiempo de retransmisión por sí mismo varía según las condiciones del enlace. Por defecto, 5.

Rama Hkey_Local_Machine\System\CurrentControlSet\Services\Class\netTrans\000n:

Valor	**Tamaño**	**Descripción**
MaxMTU	16-bit	Especifica el tamaño máximo de datagrama IP que se puede pasar al controlador de acceso del medio (MAC). Cabeceras SNAP y de source routing (si se usan en el medio) no están incluidas en este valor. Por ejemplo, en una ethernet, MaxMTU valdrá 1500. El valor usado será el mínimo del valor especificado por este parámetro y del tamaño que indica el controlador de acceso del medio. El valor por defecto es el tamaño indicado por el controlador de aceso del medio.

3.2. Puestos con el sistema operativo Windows NT 4.0

a) Configuración básica

La configuración básica del protocolo TCP/IP de un PC con sistema operativo Windows NT 4.0 se realiza desde el icono "Entorno de Red" del "Panel de control". La **Figura 4.7** muestra el cuadro de diálogo de "Entorno de Red" de un PC al que se le ha configurado el protocolo TCP/IP sobre una tarjeta Ethernet.

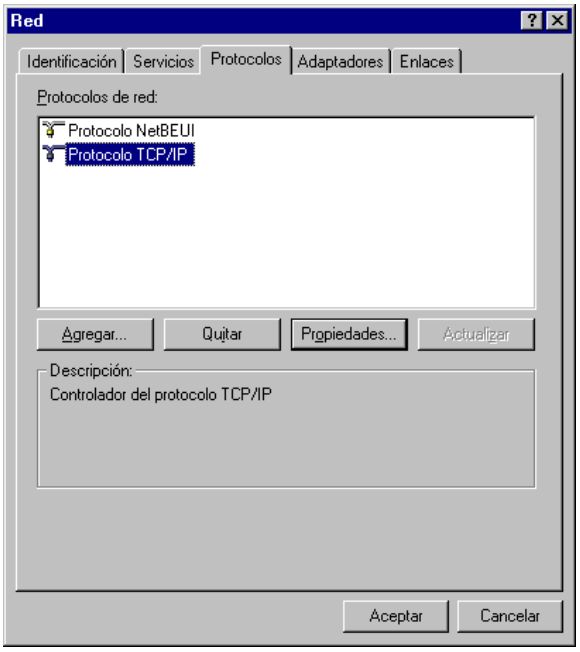

Figura 4.7: Entorno de Red de Windows NT 4.0

Para configurar los parámetros de TCP/IP es necesario abrir el cuadro de diálogo de TCP/IP desde el anterior cuadro de diálogo de Red. La **Figura 4.8** muestra la solapa en la que se configura la dirección del PC en la LAN y la ruta por defecto.

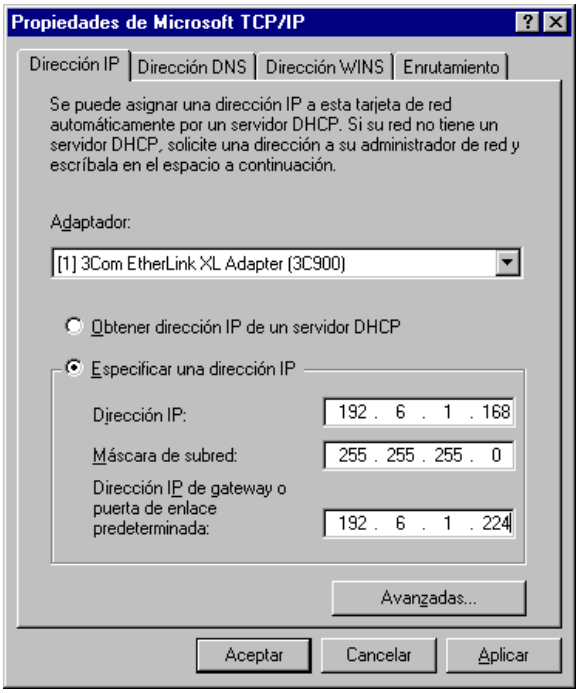

Figura 4.8: Dirección IP y router por defecto en Windows NT 4.0

La configuración de los parámetros relativos al DNS se configura en la solapa DNS como muestra la **Figura 4.9**:

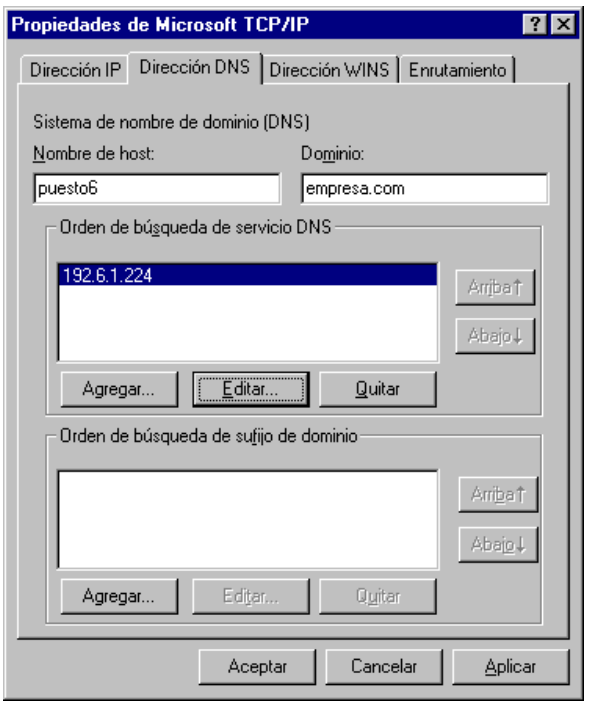

Figura 4.9: Parámetros DNS en Windows NT 4.0

b) *Configuración avanzada*

Configuración dinámica de rutas

Desde una sesión DOS dentro de Windows NT 4.0 es posible agregar y borrar rutas dinámicamente con el comando **ROUTE**. La principal diferencia frente a Windows 95 es que las rutas introducidas se pueden hacer permanentes, esto es, no desaparecen al reiniciarse la máquina. A continuación se muestra una ayuda de este comando.

```
C:\>ROUTE -?

Manipulates network routing tables.

ROUTE [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]

  -f           Clears the routing tables of all gateway entries. If this is used in
               conjunction with one of the commands, the tables are cleared prior to
               running the command.

  -p           When used with the ADD command, makes a route persistent across boots
               of the system. By default, routes are not preserved when the system
               is restarted. When used with the PRINT command, displays the list of
               registered persistent routes. Ignored for all other commands, which
               always affect the appropriate persistent routes.
```

```
  Command     Specifies one of four commands
                    PRINT      Prints a route
                    ADD        Adds a route
                    DELETE     Deletes a route
                    CHANGE     Modifies an existing route

  destination Specifies the host.

  MASK        If the MASK keyword is present, the next parameter is interpreted as
              the netmask parameter.

  Netmask     If provided, specifies a sub-net mask value to be associated with
              this route entry. If not specified, it defaults to 255.255.255.255.

  gateway     Specifies gateway.

  METRIC      specifies the metric/cost for the destination

All symbolic names used for destination are looked up in the network database file
NETWORKS. The symbolic names for gateway are looked up in the host name database
file HOSTS.
If the command is print or delete, wildcards may be used for the destination and
gateway, or the gateway argument may be omitted.
```

Parámetros del Registro del Sistema

Además de la configuración gráfica explicada, es posible configurar ciertos parámetros de la pila TCP/IP de Microsoft para Windows NT 4.0 directamente en el registro del sistema. Consultar [MICROSOFT-97] para más información. Para modificar el registro del sistema se puede usar el editor del registro del sistema de Windows NT 4.0 (regedit.exe). A continuación se da una breve descripción de los parámetros que más pueden tener que ver con el router **ADSL TELDAT C**. Para que dichos parámetros tomen efecto es necesario reiniciar el PC.

Rama HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters:

Valor	Tamaño	Descripción
ArpCacheLife	32-bit	Determina en segundos el tiempo de vida de las entradas de la cache de ARP. Por defecto, 600 segundos para entradas usadas y 120 segundos para entradas no usadas.
ArpUseEtherSNAP	32-bit	Determina si TCP/IP transmite los paquetes en Ethernet usando codificación 802.3 SNAP o formato DIX. Por defecto 0, formato DIX.
DatabasePath		Especifica el path a los ficheros de Internet, como Hosts, Networks, etc. Por defecto, Systemroot\ System32\Drivers\Etc
DefaultTOS	32-bit	Especifica el tipo de servicio (TOS) por defecto de los paquetes IP enviados. Por defecto, 0.
DefaultTTL	32-bit	Especifica el TTL por defecto. Por defecto, 128.
KeepAliveInterval	32-bit	Determina en milisegundos el intervalo de envío de "keepalives". TCP envía "keepalives" para verificar que conexiones que no transmiten datos están todavía activas. Por defecto, 0x3E8 (1 segundo).
KeepAliveTime	32-bit	Especifica, en milisegundos, el tiempo de inactividad, pasado el cual TCP empezará a mandar “keepalives”, si los “keepalives” están permitidos en la conexión TCP. Por defecto 2 horas (7200000).
TcpMaxConnectRetransmissions	32-bit	Determina cuantas veces TCP retransmite una solicitud de conexión antes de abandonar el intento. Por defecto, 3.
TcpMaxDataRetransmissions	32-bit	Especifica el máximo número de veces que un segmento TCP de datos será retransmitido antes de que la conexión sea abortada. El tiempo de retransmisión por sí mismo varía según las condiciones del enlace. Por defecto, 5.
TcpNumConnections	32-bit	Determina el número máximo de conexiones que TCP puede tener abiertas simultáneamente. Por defecto, 0xFFFFFE.
TcpWindowSize	32-bit	Determina la máxima ventana ofrecida por TCP.

Rama
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AdapterName#\Parameters\Tcpip:

Valor	Tamaño	Descripción
MTU	32-bit	Especifica el tamaño máximo de datagrama IP que se puede pasar al controlador del medio. El valor usado será el mínimo del valor especificado por este parámetro y del tamaño que indica el controlador del medio.

3.3. Puestos con el sistema operativo Solaris 2.5.1

La configuración del protocolo TCP/IP en una máquina Solaris 2.5.1 se realiza en la fase de instalación de la máquina. Si se desea cambiar dicha configuración es posible efectuar el cambio modificando una serie de ficheros de configuración. La configuración básica de parámetros IP en

Solaris 2.5.1 se realiza tradicionalmente mediante ficheros de configuración, principalmente en el directorio /etc. En este apartado se describen los parámetros que son requeridos para usar el router **ADSL TELDAT C** como gateway de una máquina Solaris 2.5.1. Para una descripción detallada de la configuración del protocolo TCP/IP de Solaris se puede consultar la referencia [SUN-95] de la bibliografía.

La dirección IP de la estación en la LAN se obtiene del fichero */etc/hostname.medion*, donde *medion* suele ser le0 o hme0, dependiendo de la tarjeta de red empleada. En dicho fichero puede aparecer la dirección en formato numérico de puntos o alfanumérico. En el segundo caso, la dirección IP numérica se obtiene tradicionalmente del fichero *etc/hosts*. A continuación se muestra un ejemplo de fichero /etc/hostname.mhe0.

```
/etc> more hostname.hme0
192.6.1.224
```

La resolución de nombres se configura mediante los ficheros */etc/nsswitch.conf*, */etc/resolv.conf* y */etc/netconfig*. Es importante hacer notar que la experiencia dicta que es muy fácil que una máquina UNIX configurada para acceder a Internet y usando servicio DNS realice peticiones DNS casi constantemente, por lo que se debe tener cuidado si se dispone de tales estaciones, en previsión de tener permanentemente la llamada a Internet establecida por culpa de las peticiones DNS. Lógicamente esto no debe ocurrir si el administrador del sistema sabe y controla las aplicaciones o servicios que usan DNS. A continuación se muestra un ejemplo de los ficheros mencionados:

```
/etc> more nsswitch.conf
# /etc/nsswitch.files:
#
# "hosts:" and "services:" in this file are used only if the  /etc/
# netconfig file has a "-" for nametoaddr_libs of "inet" transports.

passwd:     files
group:      files
hosts:      files dns
networks:   files
protocols:  files
rpc:        files
ethers:     files
netmasks:   files
bootparams: files
publickey:  files
# At present there isn't a 'files' backend for netgroup;  the system
# will figure it out pretty quickly, and won't use netgroups at all.
netgroup:   files
automount:  files
aliases:    files
services:   files
sendmailvars:   files

/etc> more resolv.conf
domain empresa.com
nameserver 194.179.1.101

/etc> more /etc/netconfig
#
# The "Network Configuration" File.
```

```
#
# Each entry is of the form:
#
#  <network_id> <semantics> <flags> <protofamily> <protoname> \
#               <device> <nametoaddr_libs>
#
# The "-" in <nametoaddr_libs> for inet family transports indicates
# redirection to the name service switch policies for "hosts" and
# "services". The "-" may be replaced by nametoaddr libraries that
# comply with the SVr4 specs, in which case the name service switch
# will not be used for netdir_getbyname, netdir_getbyaddr,
# gethostbyname, gethostbyaddr, getservbyname, and getservbyport.
# There are no nametoaddr_libs for the inet family in Solaris anymore.
#
udp    tpi_clts      v  inet  udp   /dev/udp     -
tcp    tpi_cots_ord  v  inet  tcp   /dev/tcp     -
rawip  tpi_raw       -  inet  -     /dev/rawip   -
```

Para indicar a la estación cuál es el gateway por defecto se puede incluir el fichero */etc/defaultrouter* con dicho gateway:

```
/etc> more defaultrouter
192.6.1.224
```

3.4. Puestos con el sistema operativo Linux

La configuración del protocolo TCP/IP en una máquina Linux se realiza en la fase de instalación de la máquina. Si se desea cambiar dicha configuración es posible efectuar el cambio modificando una serie de ficheros de configuración, de forma similar al caso de Solaris. Los ficheros de configuración y parámetros afectados dependen además de la versión de Linux y de la distribución de Linux usada. En este apartado se da un ejemplo para la distribución Red Hat 5 de Linux 2.0.32.

a) Configuración mediante ficheros

De forma parecida a Solaris, los ficheros de configuración del protocolo TCP/IP en Linux se encuentran a partir del directorio */etc*. Es necesario que el adaptador de red esté debidamente instalado en el sistema. Supuesto esto, los ficheros */etc/sysconfig/network*, */etc/resolv.conf* y */etc/sysconfig/network-scripts/ifcfg-eth0*, que se muestran a continuación, configuran los parámetros básicos de TCP/IP.

Fichero */etc/sysconfig/network:*

```
/etc/sysconfig> more network
NETWORKING=yes
FORWARD_IPV4=false
HOSTNAME=puesto6
DOMAINNAME=empresa.com
GATEWAYDEV=eth0
GATEWAY=192.6.1.224
```

Fichero */etc/sysconfig/network-scripts/ifcfg-eth0*:

```
/etc/sysconfig/network-scripts> more ifcfg-eth0
DEVICE=eth0
IPADDR=192.6.1.168
NETMASK=255.255.255.0
NETWORK=192.6.1.0
BROADCAST=192.6.1.255
ONBOOT=yes
BOOTPROTO=none
```

Fichero */etc/resolv.conf*:

```
/etc> more resolv.conf
search empresa.com
nameserver 192.6.1.224
```

b) Configuración mediante el configurador de red

La distribución Red Hat 5 de Linux ofrece la posibilidad de usar la herramienta "Network Configuration" del panel de control para configurar las opciones básicas de TCP/IP.

La **Figura 4.10** y la **Figura 4.11** muestran dos ventanas ejemplo de configuración mediante el configurador de red de Linux:

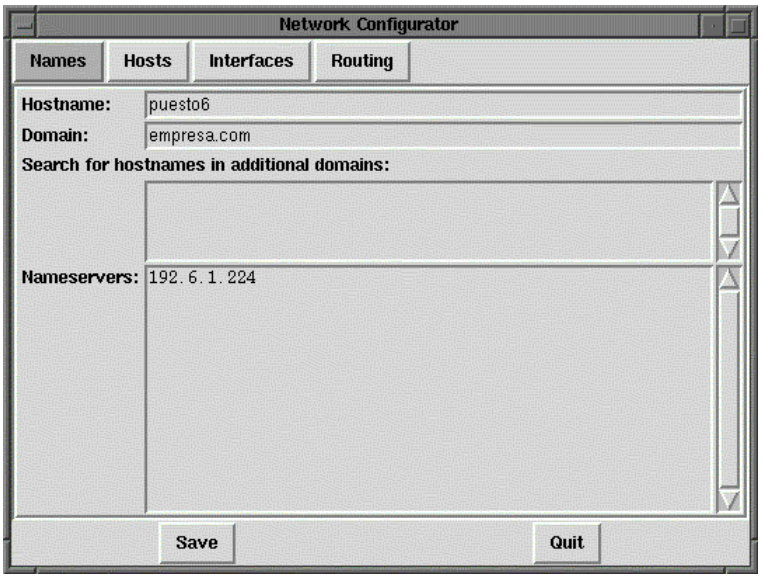

Figura 4.10: Parámetros DNS en Linux

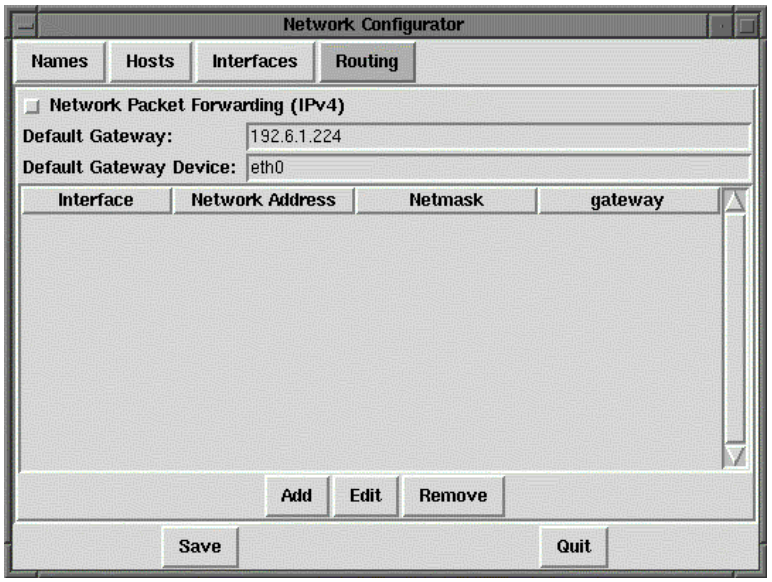

Figura 4.11: Router por defecto en Linux

4. Ejemplos de configuración

Imaginemos un escenario en el que queremos proporcionar acceso a Internet a una red privada (hay que realizar NAPT) por ADSL con una conexión PPP cuya dirección debe negociarse dinámicamente, con la posibilidad de realizar backup por un canal de RDSI cuando se pierda la conectividad IP. Además, se desea hacer visible un servidor FTP en el puerto 21000.

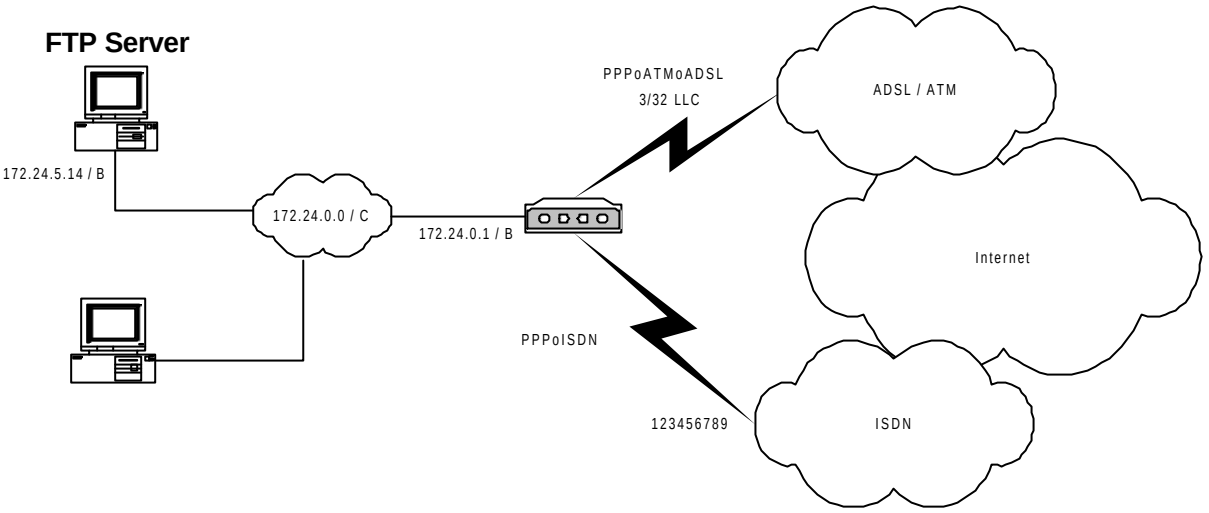

Figura 4.12: Ejemplo de configuración

1) Configurar la conexión AAL-ATM

Los datos VPI/VCI, tipo de multiplexación y tipo de tráfico debe proporcionárselos su proveedor de acceso ADSL

```
Quick Config>add aal
Type AAL-ATM connection identifier (1-99) [0]? 1
Type VPI (0-255) [0]? 3
Type VCI (32-65535) [0]? 32
Select multiplexation method (VC=1, LLC=2) [1]? 2
Select category (CBR=2, VBR_RT=3, VBR_NRT=4, UBR=6) [6]?
Type transmission PCR (in kbps) [1000]?
Quick Config>
```

2) Modificar la conexión IP sobre LAN

```
Quick Config>list ip

--- IP Connections ---

Ix  Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth NAPT
-- ----  ------- -------  ------------------  -------  ---- ---------
1  IP1    LAN1    ----    192.168.0.1/24       IP      ---   NO

Quick Config>change ip
Type identifier of IP connection to change [0]? 1
Underlaying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.PSTN [1]?
Type local IP address [192.168.1.1]? 172.24.0.1
Type subnet mask [255.255.0.0]?
Do you want to enable NAPT (Yes/No)(N)?
Type description []? LAN
Quick Config>
```

3) Crear la conexión IP sobre ATM

El usuario y password de su conexión debe proporcionárselos su proveedor de acceso

Se configura NAPT a sí y como dirección la 0.0.0.0, lo cual obliga al equipo a solicitar dirección al extremo remoto.

```
Quick Config>add ip
Type IP connection identifier (1-99) [0]? 2
Underlaying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.WAN
 5.UART[1]? 2
Type AAL-ATM connection to use [0]? 1
Select traffic type (IP=1, PPP=2, PPPoE=3) [1]? 2
Type local IP address [0.0.0.0]?
Type subnet mask [0.0.0.0]?
Do you want to enable NAPT (Yes/No)(Y)?
Type NAPT entries duration (1-240 min.) [5]?
Type user  []? adsl_user
Type password  : adsl_password
Confirm password  : adsl_password
Type description []? ADSL
Quick Config>
```

4) Crear la conexión IP sobre ISDN

El número al que llamar, el usuario y password de su conexión debe proporcionárselos su proveedor de acceso

Se configura NAPT a sí y como dirección la 0.0.0.0, lo cual obliga al equipo a solicitar dirección al extremo remoto.

```
Quick Config>add ip
Type IP connection identifier (1-99) [0]? 3
Underlaying Connection Type:
 1.LAN
 2.AAL-ATM
 3.ISDN
 4.WAN
 5.UART[1]? 3
Type B Channel to use: 1.-B1, 2.-B2 [0]? 1
Type local IP address [0.0.0.0]?
Type subnet mask [0.0.0.0]?
Do you want to enable NAPT (Yes/No)(Y)?
Type NAPT entries duration (1-240 min.) [5]?
Type user  []? isdn_user
Type password  : isdn_password
Confirm password  : isdn_password
Call Number  []? 123456789
Select Remote Authentication Protocol: None(1), PAP(2), CHAP(3)[1]?
Type PPP release time (0 - 65535)s [0]? 120
Type description []? RDSI
```

5) Agregar rutas por defecto

Configuramos dos rutas por defecto: una por la conexión ADSL y otra por la conexión RDSI; al tener mayor coste la ruta por RDSI, si puede encaminar los paquetes por ADSL, los encaminará por ADSL dado que el coste es menor; si no puede encaminarlos por ADSL, los encaminará por RDSI, realizando la llamada pertinente. En cuanto se recupere la conexión PPP sobre ADSL, se dejará de encaminar tráfico por RDSI, y la llamada se acabará cancelando por ausencia de tráfico.

```
Quick Config>add route
Type destination subnetwork address [0.0.0.0]?
Type destination subnetwork mask [0.0.0.0]?
Type outgoing connection identifier [1]? 2
Type cost (1..16) [1]?
Quick Config>
```

```
Quick Config>add route
Type destination subnetwork address [0.0.0.0]?
Type destination subnetwork mask [0.0.0.0]?
Type outgoing connection identifier [1]? 3
Type cost (1..16) [1]? 4
Quick Config>
```

6) Agregar puerto visible

```
Quick Config>add port
Type IP connection identifier (1-99) [0]? 2
Type host IP address  [0.0.0.0]? 172.24.5.14
Type internal port (0-65535) [0]? 21
Type external port (0-65535) [0]? 21000
Select port type (1-GENERIC, 2-FTP) [1]? 2

Quick Config>add port
Type IP connection identifier (1-99) [0]? 3
Type host IP address  [0.0.0.0]? 172.24.5.14
Type internal port (0-65535) [0]? 21
Type external port (0-65535) [0]? 21000
Select port type (1-GENERIC, 2-FTP) [1]? 2
Quick Config>
```

```
Quick Config>list aal

--- AAL-ATM Connections ---

Ident Interf. VPI VCI   Mx  Category PCR   MBS   SCR
----- ------- --- ----- --- -------- ----- ----- -----
ATM1  ADSL1   3   32    LLC UBR      1000

Quick Config>list ip

--- IP Connections ---

Id    Under  Subitfc  Local-Address/Mask  Traffic  Auth NAPT
----  ------- -------  ------------------  -------  ---- ---------
IP1    LAN1    ----    172.24.0.1/16       IP      ---   NO
IP2    ADSL1   ATM1    0.0.0.0/0           PPP     ---   YES -   5
IP3    ISDN1   B1      0.0.0.0/0           PPP     NONE  YES -   5

Quick Config>list routes

--- IP Routes ---

Ix Conn Dest. Address   Dest. Mask      Next Hop        Cost
-- ---- --------------- --------------- --------------- ----
1  IP2  0.0.0.0         0.0.0.0                         1
2  IP3  0.0.0.0         0.0.0.0                         4

Quick Config>list port


--- Visible Ports ---

Ix Conn. IP Address      Int.Port Ext.Port Type
-- ----- --------------- -------- -------- -------
1  IP2   172.24.0.15     21       21000    FTP
2  IP3   172.24.0.15     21       21000    FTP

Quick Config>
```

5. Bibliografía

Este manual explica el menú de configuración rápida. Si desea realizar alguna configuración especial, monitorizar algún protocolo exhaustivamente, o realizar alguna función no descrita en este documento, pida a su proveedor habitual el manual o manuales genéricos del Router Teldat.

[IANA-94]. "Request for Comments: 1700. ASSIGNED NUMBERS". J. Reynolds & J. Postel. Network Working Group. IETF 1994.

[NAT-94] "Request for Comments: 1990. The IP Network Address Translator (NAT)". K. Egevang & P. Francis. Network Working Group. IETF 1996".

[STEVENS-96] "TCP/IP Illustrated, Volume 1. The Protocols". W. Richard Stevens. Addison-Wesley. 1996. ISBN 0-201-63346-9.

[SUN-95] "TCP/IP and data Communications Administration Guide". Sun Microsystems, Inc. 1995.

[TELDAT1-00] "Dm701 Protocolo ARP e InARP"

[TELDAT2-00] "Dm702 Configuración TCP-IP"

[TELDAT3-00] "Dm703 Frame Relay"

[TELDAT4-00] "Dm704 Configuración y Monitorización"

[TELDAT5-00] "Dm705 Interfaces Serie Genéricos"

[TELDAT6-00] "Dm706 Protocolo SDLC"

[TELDAT7-00] "Dm707 Configuración X.25"

[TELDAT9-00] "Dm709 Interfaces LAN"

[TELDAT10-00] "Dm710 Interfaz PPP"

[TELDAT12-00] "Dm712 Agente SNMP"

[TELDAT13-00] "Dm713 Configuración de X.25 sobre (XOT)"

[TELDAT14-00] "Dm714 Protocolo OSPF"

[TELDAT15-00] "Dm715 Priorización y reserva de ancho de banda (BRS)"

[TELDAT16-00] "Dm716 Data Link Switching"

[TELDAT17-00] "Dm717 Bridge"

[TELDAT18-00] "Dm718 Protocolo RIP"

[TELDAT19-00] "Dm719 Interfaz Túnel IP"

[TELDAT20-00] "Dm720 Protocolo NAT"

[TELDAT21-00] "Dm721 Interfaz ASTM"

[TELDAT24-00] "Dm724 Protocolo FTP"

[TELDAT25-00] "Dm725 Protocolo TVRP"

[TELDAT30-00] "Dm730 Protocolo DHCP"

6. Glosario

A continuación se expone un breve glosario de términos relacionados con el entorno de este equipo.

10Base-T - 10 megabits per second Baseband Twisted par. Se refiere al interfaz eléctrico utilizado para transmitir y recibir en una conexión Ethernet.

ADSL - Asymmetric Digital Subscriber Line. Es la tecnología de transmisión para alta velocidad que utiliza el bucle de abonado (línea telefónica entre el usuario y la central) y que puede alcanzar 8 Mbps en sentido descendente, y 1 Mbps en sentido ascendente. La conexión ADSL puede compartir el bucle de abonado con la telefonía vocal.

ATM - Asynchronous Transfer Mode es una tecnología de transmisión de voz, video y datos de muy alta velocidad basado en la fragmentación de la información en bloques de longitud fija denominados "celdas". Estas celdas pueden ser procesadas muy rápidamente mediante conmutadores hardware reduciendo el retardo de transito por la red.

BRIDGE - Un bridge intercambia paquetes de datos entre dos o mas LAN que usan el mismo protocolo de comunicación basándose en la dirección hardware (MAC).

CO - Central Office. La oficina central de la operadora telefónica donde todos los bucles de abonado de una zona son recogidos. En el caso de una instalación con ADSL, esto ocurre en un DSLAM.

CONSOLA - Es un equipo que puede ser un PC, y que sirve para configurar localmente el equipo.

DHCP - Dynamic Host Configuration Protocol . Es un protocolo que asigna automáticamente direcciones IP a un elemento de la LAN llamado cliente DHCP . Gracias a esto se puede evitar , la configuración manual de cada equipo.

DMT - Discrete multitone. Es el tipo de modulación recomendada por la UIT para el ADSL. Consiste en utilizar 256 moduladores/demoduladores QAM.

DNS - Domain Name Server. Es un servidor que recoge una dirección de Internet basada en texto, y la convierte en una dirección IP numérica que le permitirá conectarse con otro sitio web.

DSLAM - Digital Subscriber Line Access Multiplexer. Es un equipo situado en la central telefónica , que recibe y concentra las conexiones ADSL de muchos abonados en una línea ATM de alta velocidad.

DOWNSTREAM - Canal descendente - Es el trafico de datos en sentido Central-abonado.

ENCAPSULADO - Se refiere a la suma de uno o mas cabeceras utilizadas por protocolos de comunicaciones dentro de un paquete de datos.

ETHERNET - Es la conexión física y de datos que permite juntar equipos en una LAN.

FILTRO - Es un elemento de configuración que permite discriminar tráfico en función de la dirección IP origen, destino, protocolo o puerto, según el criterio programado.

IP dirección – Es un campo del datagrama IP utilizado para identificar un interfaz en la red. Es un número de 32-bits escrito en 4 campos decimales, octetos, separados mediante puntos. Por ejemplo 192.6.1.228.

LAN - Local Area Network. Red de Área Local. Es una red de datos de alta velocidad situada en un área geográfica pequeña (cientos de metros). Las LAN conectan estaciones de trabajo, ordenadores, periféricos y otros equipos situados en un área pequeña o edificio.

MAC - Media Access Control. Acceso de Control al Medio. Es la dirección de nivel 2 requerida por cada puerto e equipo que se conecta a una LAN. Tiene 6 bytes de longitud y es conocida también como dirección hardware o dirección física.

NAT - Network Address Translation . Traslación de dirección de red.

PAT - Port Address Translation.

PING - Packet INternet Grouper. Es un comando o programa de Internet que se usa para determinar si una dirección IP es accesible.

PPP - Point-to-Point Protocol . Es un protocolo que permite interconectar dos routers o un host y la red con líneas síncronas o asíncronas.

PVC - CVP - Circuito Virtual Permanente. Está caracterizado localmente por la pareja (VPI/VCI).
RFC 1483 - RFC 1483 SubNetwork Access Protocol (SNAP) es un método para encapsular datos multiprotocolo en redes ATM.

RIP - Routing Information Protocol. Protocolo de enrutamiento.

ROUTER - Un router es un equipo de red que pasa paquetes de una red a otra según un criterio basado en direcciones IP.

SNMP - Simple Network Management Protocol. Es un protocolo de gestión de equipos a través de Internet, normalizado.

SUBNETMASK – MÁSCARA DE SUBRED - Es una máscara de dirección de 32 bits, que determina el número de direcciones de una subred.

SUBNET – SUBRED - Una subred es una red segmentada arbitrariamente por un administrador de red para proporcionar una estructura multinivel.

TCP/IP - Transmission Control Protocol/Internet Protocol es un conjunto de protocolos desarrollados en los años 70 y que constituyen la base de Internet.

TELNET - TELNET es una emulación estándar de terminal basado en el protocolo TCP/IP. Permite a los usuarios acceder remotamente al interfaz de comandos del equipo.

UPSTREAM - Canal ascendente - Es el tráfico de datos en sentido abonado –central.

VPI/VCI - El VPI (Virtual Path Identifier) campo de 8-bits en la cabecera de celda ATM). Combinado con el VCI (Virtual Channel Identifier, campo de 16-bits en la cabecera de celda ATM), es utilizado para identificar el próximo destino de una celda que pasa a través de un switch ATM.

VPN - Virtual Private Network . Red privada virtual. Permite al tráfico IP viajar con seguridad a través de una red TCP/IP.

WAN - Wide Area Network . Una red que al contrario que la LAN, cubre un área geográfica extensa.

WRR- Wan ReRoute. Backup que se basa en activar una u otra ruta dependiendo de que la interfaz principal esté **UP** o **DOWN**