Teldat C

Quick Menu

Doc. *DM211-I* Rev. *6.0*
April, 2003

INDEX

Chapter 1
Introduction

1. Introduction

The ***TELDAT C*** router family is made up of a range of IP routers for general purposes with a wide application area: personal environments, SOHO/SME and corporate; thanks to this versatility, they are perfectly adaptable to a wide variety of IP scenarios: from providing simultaneous access to Internet for private LAN users to the adaptation of teleprocess networks and SNA support and the support of POS (Point of Sale terminals – dataphone).

The ***TELDAT C*** family covers the access needs for ADSL, ISDN and serial lines (connection to an external telephone modem, Frame Relay, X.25, PPP, etc.).

The ***TELDAT C*** router's enormous versatility requires a high level of configuration in order to adapt to different needs and environments, and for this reason there is a large number of configuration parameters available. To simplify the configuration and monitoring process, the ***TELDAT C*** routers possess a reduced configuration and monitoring environment suited to the majority of SOHOs/SMEs or personal environments. This environment known as **quick configuration** / **monitoring** or **quick menu** is the objective of this manual, and forms part of a complete management solution known as **TMS** (Teldat Management System).

Figure 1.: External aspect of the Teldat C routers

2. TELDAT C router characteristics

Interfaces

- Ethernet 10BaseT Interface.
- (*) Multistandard serial WAN interface (V.24, V.35, X.21 and V.36) through insertable drivers.
- (*) Up to 4 asynchronous interfaces to support point of sale terminals.
- (*) Up to 2 ADSL Interfaces over POTS (Plain Old Telephone System).
- (*) ISDN 2B+D Basic interface.
- RS-232 configuration interface.

(*) Interfaces available, depending on the model.

Functionalities

- NAT/PAT

  Permits the connection of an unlimited number of workstations from a local network area network (LAN) to Internet simultaneously and indistinctively as well as preventing connection from the exterior to your private network.

- Guaranteed connectivity through backup mechanisms (available depending on the model).

  If the main interface is not available, connectivity with the exterior remains transparently guaranteed on establishing the communication through an alternative channel (ISDN, telephone line). Once the channel has recovered, the alternative channel is released.

- IP Filtration

  Increases the security of your network, preventing the access from or to determined IP addresses or TCP/UDP ports.

- Automatic routing of DNS requests

  This permits you to configure the ***TELDAT C*** router as your network DNS server.

- DHCP Server

  This permits you to assign IP addresses to your network in a dynamic and controlled form from the ***TELDAT C*** itself.

- IPSec

  This encrypts your communications through standard IP encryption.

3. Configuration and monitoring modes

The ***TELDAT C*** routers offer different ways of configuration and monitoring in order to adjust to the needs or preferences of each user. The possibilities are as follows:

- Local console through the commands line interface
- TELNET, accessed through the commands line interface
- Internet browser, through a graphic interface accessing the Web server included in the device.
- SNMP Manager

a) Configuration through a local console

In order to access the interface console, you need to connect the ***TELDAT C*** to a PC or workstation serial port and this must have a terminal emulation program. To carry out the connection you must use an RJ45Female-DB9Female adapter and a cable with 6 wires (a LAN cable or an ISDN cable can be used).

The terminal emulation configuration must be 9600-8N1, i.e.:

Speed: 9600 bps

Eight data bits

Without parity bit

One stop bit

Without flow control (neither software nor hardware)

If the connection and configuration are correct, the system "prompt" appears; if the device has an access password configured, this will be requested before the prompt is displayed.

```
Teldat               (c)1996 - 2001

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

*
```

b) Configuration through a remote console via TELNET

If you wish to remotely configure and use the line commands interface, you can use a Telnet application. A Telnet client application is included in the majority of operating systems.

To access the device you need to know the interface IP address through which you are going to access the device or the internal IP address (initially, and given that the router has not as yet been configured, you can access the 192.168.1.1 address assigned to the router's LAN interface by default).

If you have an access password configured, this will be requested before you are able to access the device.

By default the LAN interface address is 192.168.1.1, except in those cases where a default configuration exists pertaining to the client and this is activated.

c) Configuration through the Internet Browser

The ***TELDAT C*** router has a WEB server available that makes management possible through any Internet browser. To carry this out you need to access address http://device_IP_address with the browser. The device will request a user name (**`teldat`**) and a password (the password to access via console or the Web server default password, **`teldatc`**).

By default the LAN interface address is 192.168.1.1

Web server default user and password: **`teldat / teldatc`**

In cases where the default configuration pertaining to the client is activated, the IP address, the user and password may vary.

To access the device you need to know the interface IP address through which you are going to access the device or the internal IP address (initially, and given that the router has not as yet been configured, you can access the 192.168.1.1 address assigned to the router's LAN interface by default).

d) Configuration through SNMP manager

The SNMP protocol is a standard for the management of communication devices.

The ***TELDAT C*** router supports the following MIBs:

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

Private MIB quick configuration/ monitoring TeldatC-MIB

Other private MIBs from Teldat

To access the device through SNMP you need to have previously configured in the device (through local console, Telnet or Web) the SNMP access IP address and the associated community.

Chapter 2
Configuration through commands line

1. Accessing the menu

This section describes the quick configuration menu configuration possibilities. Configuring the device from the quick configuration menu is carried out in three stages:

1. **Configure the required parameters** through the appropriate commands from the menu itself. In this phase, all the required parameters are configured, such as the LAN IP address etc.
2. **Generate and save the configuration** through the quick configuration menu's <MAKE> command. In this phase the device takes as a valid configuration the one from the quick configuration menu and saves this in the SRAM.
3. **Restart** the device from the general configuration menu. This is executed through the <RESTART> command in order for the configuration values to become active.

The** <MAKE> **command deletes all the configuration* currently existing in the device and completely regenerates this starting from the information contained in the quick menu; therefore any configuration modification carried out outside of this menu is lost.

* Deletes all the existing configuration of those configurable aspects in the quick menu (for example, this does not modify the FTP server configuration, events configuration, etc). To completely delete the configuration, use the <SET DEFAULT-CONFIGURATION> command or set the microswitch 5 to ON and carry out <RESTART>

To access the quick configuration menu, enter <QUICK-CONFIGURATION> in the general configuration menu:

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

To exit the quick configuration menu, enter <EXIT> from the quick configuration menu itself:

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

To obtain the list of available options, enter the <?> command.

```
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. Device access parameters

The ***TELDAT C*** devices have a standard access control system based on users and passwords. This control is applied to the access via the local console, Telnet FTP and Web server.

From the quick menu it is only possible to configure a single user. This user will have all the permissions needed available (user management, configuration, monitoring and events). There also exists the possibility of not configuring the user, in which case only the password is requested; there is also the possibility of not configuring the password, in which case there is free access to the device (the console/Telnet requests nothing, in FTP simply indicate the user "`root`" without a password and user "`teldat`" with the "`teldatc`" password for the internal Web server).

If the default configuration mechanism pertaining to the client is activated, the necessary user and password will depend on the said configuration.

To configure the user name, there is a `<SET USER>` command available and to configure the password, there is the `<SET PASSWORD>` command. If you wish to delete the user or password, simply configure these as empty. A password will always be requested when a user is configured.

If the password is deleted the user is automatically deleted, but not vice versa, as you may want control solely based on the 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>
```

The user name does not distinguish between upper and lower case letters, while with the password this distinction is carried out.

3. Name assigned to the device (hostname)

It is possible to assign a name to the device in order to identify it. This name will appear in front of the distinct console prompts (once the quick configuration MAKE has been effected). The command used to configure a hostname is <SET HOSTNAME>.

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

Through the <LIST HOSTNAME> command, you can see the configured hostname. This is also displayed by executing <LIST USER> or <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. ADSL/ATM Parameters

The ADSL parameters are modified through the `<SET ADSL>` command and are as follows:

```
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**

  In cases where your device has more than one ADSL interface, the identifier of the ADSL interface you wish to configure will be requested.

- **Max/min transmission rates ratio**

  An ADSL interface can contain multiple ATM connections, each one with a different transmission speed: this parameter indicates the relationship between the highest speed to be configured in an ATM connection over ADSL and the lowest speed. The highest speed coincides with the ADSL line speed (this can vary depending on the condition of the line).

  For example, taking the default value and a line speed of 1024 Kbps, the configurable ATM connection at the lowest speed will be 1024Kbps/25 = 41 Kbps.

- **Open mode**

  The ADSL interface permits two operation modes: *multimode*, where the device adjusts to the operating mode of the main telephone center and the *G.Lite* mode, a mode with reduced power and slower speeds.

  The default value is *multimode.*

To list the configurable values, execute the `<LIST ADSL>` command.

```
Quick Config>list adsl

--- ADSL line parameters ---

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

Quick Config>
```

5. SNMP Parameters

The SNMP parameters are only necessary to access the configuration, monitoring and alarm generation through the SNMP protocol.

The SNMP petitions can be sent to any configured IP address.

The SNMP parameters are configured with the **<SET SNMP>** command and are as follows:

```
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**

  Name of the management SNMP community. The community generated with this name, possess the READ, WRITE and TRAP permissions i.e. the manager can read and write the SNMP variables as well as receive traps.

  By default, this is configured as a "public" community with permission to only READ over MIB II; this community cannot be eliminated from the quick configuration.

- **Traps level**

  One of the four levels of defined traps can be established.

  - **NONE:** Traps are not sent.
  - **LOW:** Generic traps are sent.

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

    And the "Enterprise Specific" defined as ERROR:

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

  - **MEDIUM:** the LOW traps together with "Enterprise Specific" defined as U-INFO
  - **HIGH:** the MEDIUM traps together with "Enterprise Specific" defined as C-INFO.

- **Traps IP destination address / Mask**

  These parameters determine the traps destination IP address and control the access to the SNMP agent (management is only permitted from those SNMP managers whose IP address coincides with the subnet defined in these fields).

  If the trap destination address is 0.0.0.0 traps are not sent.

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

  By default, the ***TELDAT C*** devices carry out an ECHO UDP petition to the traps destination station to check if the traps have arrival guarantee for the said station. If NO is configured, the said check is not carried out. The accessibility of a traps reception station can also be checked through ECHO ICMP (ping).

The quick configuration permits a single destination address for traps. If you wish to have more than one trap address or more than one community or define specific views for a community, you must use the general SNMP configuration menu.

6. DHCP Parameters

The ***TELDAT C*** router offers the possibility to act as a DHCP server or as a DHCP "relay" agent. The DHCP parameters are configured through the **<SET DHCP>** command.

a) DHCP Server

The ***TELDAT C*** router, through the DHCP server, dynamically assigns IP addresses (as well as other configuration parameters) to the DHCP clients, generally found in its LAN.

When you operate with a DHCP service, the router dynamically assigns the addresses to the clients. The DHCP server provides IP addresses for a programmable period of time. If once this period has expired the address has not been renewed, the address becomes available again and the DHCP server can assign it to any client making a DHCP petition.

It's very important to ensure that various DHCP servers do not exist in the same LAN. Should there be more than one DHCP server assigning addresses in the same local network, address confliction can arise.

In order to configure the **DHCP Server**, you need to indicate the following parameters as seen in the example below:

```
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**
  This is the range of IP addresses that the DHCP server assigns to the DHCP clients. The range is specified through the start and end IP addresses (both addresses are included within this range and can be assigned).

- **Subnet mask**
  Configures the DHCP client's subnet mask.

- **Default router address**
  Default router. The router's default IP address used by the DHCP client.

- **DNS server**
  DNS server's IP address used by the DHCP client for name resolution.

- **Lease time in minutes**
  Period of time in which the IP address is assigned. Once this period has timed out and the address has not been renewed, the address becomes available once more and the DHCP server can assign it to any client making a DHCP petition.

By using the **<LIST DHCP>** command, you can view the current DHCP protocol configuration in the device:

```
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) DHCP Relay Agent

In the case of the DHCP Relay Agent, the router captures the DHCP messages generated by the possible clients connected to this LAN and forwards them to a known DHCP server which is situated outside the LAN. The messages would not reach the server in any other way as the DHCP client petitions are carried out through *broadcast* IP datagrams and these are not routed.

The following example shows how to configure the DHCP Relay Agent and how to view the DHCP protocol status for this case:

```
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**
  This is the DHCP server IP address to which all the client petitions are sent.
- **Primary DHCP server address**
  IP address of a second DHCP server to which the client petitions are sent (optional).

7. DNS Parameters

To translate the IP addresses in alphanumerically format, more easily understood e.g. “www.teldat.es”, to IP addresses in a numerical format really used by the devices e.g. 195.53.0.2, the IP protocol has a domain name system DNS available. Through this DNS service, the end devices i.e. PCs carry out DNS petitions to the DNS servers. Generally these petitions request the alphanumerically translation of a name to an IP address in numerical format but more things can be requested such as information on mail accounts etc.

In an environment where a ***TELDAT C*** router is used, the external networks they are connected to can have DNS servers available in order to resolve the DNS petitions in the end stations. A clear example is Internet, as all Internet suppliers offer DNS servers to their users. The DNS service however is not exclusive to Internet can be offered in any private IP network or Intranet.

The ***TELDAT C*** router has a routing functionality for DNS petitions received from the LAN workstations. It’s possible to define up to three DNS servers in the router in such a way that the DNS petitions received by the router from the local network devices are resent to the configured servers in the order that they are configured. This operation is known as *DNS proxy*.

With this feature it is possible to configure as DNS server for the local workstations, the servers given by the external network supplier (e.g. Internet). Or configure the router’s IP address as the DNS server in the LAN and add the DNS servers to the router itself. We recommend the latter solution as it involves a simpler centralized configuration. If you change your supplier you won’t have to reconfigure all the workstations, only the router. Also the treatment of the DNS petition retries in an environment with various DNS servers can be better in the router than in certain IP protocol implementations from some manufactures.

The most normal way is to first configure the primary DNS server followed by the secondary one. The data of both is from the service supplier.

If you configure DNS servers for more than one external network, you should remember that the router follows an established order in the query resolution. First to the configured primary server and then to the secondary server and later to the third independently of the external networks to which they belong; there is no way to know beforehand which external network a determined IP address (alphanumerically) belongs to. Due to this, the router could carry out accesses through other alternative circuits before using the most adequate one in order to access some servers who will not know how to resolve the petition, if these are DNS servers for an external network that is different to that of the petition. Therefore we recommend not aggregating DNS servers from more than one external network in order to avoid accesses to circuits and unnecessary delays.

To add a DNS server, enter <ADD DNS>:

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

In the example the DNS server 193.152.63.197, has been added.

To list the configured DNS servers, enter <LIST DNS>:

```
Quick Config>list dns


--- DNS Servers ---

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

Quick Config>
```

To delete a DNS server, enter <DELETE DNS>:

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

8. ISDN Parameters

The ISDN parameters are modified through `<SET ISDN>` and are as follows:

```
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**

  The basic ISDN interface has two configurable channels: channel 1 and channel 2.

The configuration reflects the logical channels, not the physical ISDN channels, given that the assignment of channel B1 or B2 is carried out by the network and not the device.

- **Permanent ISDN channel**

  If you have a permanent ISDN B channel contracted with an ISDN supplier, this should be indicated with this parameter. A permanent B channel is a special ISDN B channel which does not use signaling as its destination is fixed when the service is contracted. This B channel does not carry out ISDN calls and is always connected. If you enable B channel as permanent, the "`call number`" and "`PPP release time`" parameters for the IP connection based in ISDN, schedule controls and the callback have no significance for this connection. When contracting a permanent B channel, you specify which B channel (B1, B2 or both) should respond to this profile.

- **B1 + B2 connection**

  If you wish to increase the available bandwidth in a channel, 64Kbits, you join the bandwidths of the two channels (128Kbits), as long as both channels are contracted as permanent.

```
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**

  By default, the router does not permit incoming calls. With this parameter you can enable incoming calls.

- **Authorized Calling number**

  With this parameter you can limit the incoming calls to one telephone number, if this parameter is left as 0 any incoming call will be answered. **This feature is deactivated and its configuration will not have any effect (as if this was configured to 0).**

To view the ISDN configuration parameters, execute <LIST ISDN>.

```
Quick Config>list isdn

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

Quick Config>
```

9. WAN Parameters

The serial line parameters (WAN) are modified through <SET WAN> and are as follows:

```
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>
```

AT or asynchronous line configuration example.

```
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>
```

ASDP configuration example.

```
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>
```

POS configuration example.

```
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>
```

X.25 configuration example.

- **WAN identifier**
  If your device has more than one WAN line available, the identifier of the WAN line you wish to configure will be requested.

- **WAN mode**
  The WAN mode can be configured in five modes.
  AT commands: configuration to support AT commands (external modem).
  ASDP: permits access to the serial line through a TCP connection.
  POS: mode to connect to the POS serial line (Point of Sale Terminal).
  Async line: configuration of an asynchronous serial line for PPP.
  X25: configures the line to support X.25.

- **Line speed**
  Serial line speed in bps. Maximum 2048000 bps.

- **TCP port** (only ASDP)
  TCP port which can be accessed in order to have connectivity with the serial interface.

- **Flow Control** (only ASDP)
  HW: Hardware flow control.
  XON/XOFF: XON/XOFF flow control.

- **Activate XOT** (only X.25)
  If this is configured as such, on carrying out the <MAKE>, an XOT interface will be created if this does not exist. Contrariwise, if it does exist, the XOT interface will be respected.

***If you configure a WAN in X.25 and this already exists, the configuration will not be lost on carrying out the* <MAKE>.**

To consult the WAN Configuration parameters, execute the <LIST WAN> command.

```
Quick Config>list wan

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

Quick Config>
```

10. UART Parameters

The asynchronous serial line (UART) parameters are modified through the <SET UART> and are as follows:

```
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>
```

AT or asynchronous line configuration example

```
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>
```

ASDP configuration example.

```
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>
```

POS configuration example.

- **UART identifier**

  If your device has more than one UART interface available, the identifier of the UART you wish to configure will be requested.

- **UART mode**

  The UART line can be configured in four modes:

  AT commands: configuration to support AT commands (external modem).

  ASDP: permits access to the serial line through a TCP connection.

  POS: mode to connect a POS to the serial line (Point of Sale Terminal).

  Async line: configuration as asynchronous serial line for PPP.

- **Line speed**
  Serial line speed in bps. Maximum 115200 bps.

- **TCP port** (only ASDP)
  TCP port which can be accessed in order to have connectivity with the serial interface.

- **Flow Control** (only ASDP)
  HW: Hardware flow control. (This is not available if based on UART interfaces).
  XON/XOFF: XON/XOFF flow control.

You can consult the configuration of the UART parameters through the <LIST UART> command.

```
Quick Config>list uart

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

Quick Config>
```

The UART interfaces do not have signals available to carry out the flow control. Therefore, in cases of AT commands you need to activate the flow control through software type XON/XOFF; in the majority of cases, the necessary AT command to activate the XON/XOFF control modem is &K6, a value that is configured by default: if the modem connected to the device requires a distinct command, you must manually configure the value of the said command in the normal configuration. Additionally, you need to configure the ACCM (Asynchronous Control Character Map) at the PPP LCP level to 000A0000 so that the remote end can at least carry out transparency to the XON and XOFF characters.

11. PSTN Parameters

The PSTN parameters can only be configured over interfaces type WAN or UART, configured in "AT commands" mode. These are configured through <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**

  In cases where your device has WAN and UART interfaces available, the type of interface to which the parameters defined here are applied will be requested.

- **WAN/UART identifier**

  If your device has more than one WAN or UART interface available, the interface identifier will be requested.

- **Enable incoming calls**

  By default, the router does not permit incoming calls. You can enable incoming calls through this parameter.

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

  Faced with the impossibility of knowing the calling number in an analogical telephone line, you are able to configure a ring pattern detection so the incoming calls that do not comply with this pattern are not processed.

- **Number of tones:**

  Number of call pattern tones.

- **Silence duration:**

  Duration of the call pattern silences.

- **Local telephone:**

  This is the subscriber's telephone number.

To consult the PSTN configuration parameters, execute the <LIST PSTN> command.

```
Quick Config>list pstn

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

Quick Config>
```

It is important to ensure that the serial line (WAN or UART interface) is configured in AT mode and with adequate speed to the external MODEM used.

12. Internal IP Address

The Internal IP address is configured with the <SET INTERNAL-IP-ADDRESS> command.

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

To consult the configuration, execute the <LIST INTERNAL-IP-ADDRESS> command.

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

Internal IP address: 192.168.101.1

Quick Config>
```

To delete an internal IP address, simply configure the 0.0.0.0 address as internal IP address.

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

13. Traps source address (management address)

The traps exit through the management or source address (management IP address). This is configured through the <SET MANAGEMENT-IP-ADDRESS> command. This address is dealt with in a similar way to the internal IP address and as such can be used to identify a determined device.

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

You can query the configuration through the <LIST MANAGEMENT-IP-ADDRESS> command.

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

Management IP address: 192.168.200.1

Quick Config>
```

To delete the management address, simply assign this a value of 0.0.0.0

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

Or you can use the <DELETE MANAGEMENT-IP-ADDRESS> command.

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

14. ATM circuits parameters

The AAL-ATM circuits' parameters are configured with the <ADD AAL-ATM> command.

```
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)**

  This is the AAL-ATM circuit identifier.

  This parameter permits you to identify a determined AAL-ATM connection at other configuration points.

- **ADSL identifier**

  If your device has more than one ADSL interface available, the interface over which you wish to configure the connection will be requested.

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

  You configure the Virtual Path Identifier through this parameter.

  The range is from 0 to 255.

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

  With this parameter you configure the Virtual Channel Identifier.

  The range is from 32-65535.

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

  Through this parameter you can choose between two multiplexation methods from the connection: Virtual Channel (VC) or Logical Link Control (LLC)

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

  This option selects the type of ATM traffic that will be used in this connection

  These traffic categories have distinct priorities and transmission characteristics, this being in real time or not. In this way, CBR and VBR_RT have greater priority than VBR_NRT and UBR.

  - **UBR:** Unspecified Bit Rate.

    Traffic is generated in transmission with a limit higher than that determined by the PCR parameter and below that determined by the bandwidth unused for other connections or available in the physical interface.

- **CBR:** Constant Bit Rate.

  Traffic is generated in transmission with a constant rate. The value of this rate in Kbits per second is configured with the PCR parameter.

  PCR: Peak cell Rate, in Kbps.

- **VBR_RT / VBR_NRT:** Variable Bit Rate, Real Time or Not Real Time.

  Variable rate traffic is generated in transmission and characterized by the parameters PCR, SCR and MBS

  PCR: Peak Cell Rate, in Kbps.

  This is the maximum speed permitted for all the data transmission bursts.

  SCR: Sustained Cell Rate, in Kbps.

  This is the maximum speed permitted for sustained traffic.

  MBS: Maximum Burst Size, in ATM cells

  This is the maximum burst size, in number of cells.

All the parameters, with the exception of the AAL connection identifier, are data that must be provided by your ADSL access supplier. Correct configuration is essential in order to establish the data connection.

To consult the ATM AAL circuits' configuration parameters, execute the <LIST AAL-ATM> Command.

```
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>
```

To eliminate a specific connection you must execute the <DELETE AAL-ATM> command indicating the identifier of the connection you wish to delete.

It is also possible to modify an AAL-ATM connection with <CHANGE AAL-ATM>, although it is impossible to modify the connection identifier through this command.

To eliminate all the defined connections, execute the <CLEAR AAL-ATM> command. The user is requested to confirm this execution.

When you eliminate an AAS-ATM connection, you also automatically eliminate all the associated IP connections, as well as all the outgoing routes through one of the previous IP connections.

The number of AAL-ATM connections that can be simultaneously defined has been limited to five.

15. IP connection Parameters

In earlier sections you have configured the device's physical interfaces, and now you need to configure the IP protocol parameters. Given that at IP level all the interfaces are the same, the configuration has been concentrated in what is known as "IP connections" which permits you centrally configure the said parameters.

The IP connections can be configured over any of the available interfaces in the device, i.e. an IP connection can be associated to the Ethernet (LAN) interface, ISDN basic access B channels (B1 and B2), connection via modem (PSTN) or an AAL-ATM connection.

The command to add an IP connection is <ADD IP>.

The command to modify an IP connection is <CHANGE IP> and to delete the connection, <DELETE IP>. In order to eliminate all the defined IP connections use the <CLEAR IP> command. This will request the user to confirm execution.

a) LAN IP Connections:

This is used to configure LAN interface addresses.

```
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)**
  This is the IP connection identifier. The range is from 1 to 99.

- **Underlying Connection Type**
  IP connection base interface.

- **Local IP address / Subnet Mask**
  IP interface address and subnet mask.

- **Do you want to enable NAPT (Yes/No)**
  Enables or disables the NAPT facility.

- **NAPT peer address**

  Given that the LAN is a multipoint network, you need to indicate what destination you wish NAPT to be carried out. This is only significant if the previous parameter has been configured as "yes".

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

  This parameter is configured if the NAPT facility has been enabled.

  Duration of the device cache memory from the visible port entry without traffic.

- **Description:**

  This is the string of characters describing an IP connection.

b) IP PSTN Connections:

This is used to configure a point-to-point connection (PPP) via PSTN using a WAN or UART line and an external modem that accepts AT commands.

```
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>
```

In cases of IP connections in PPP mode with dynamic address assignment, you must configure any valid address that will be changed for the negotiated address when the PPP session is established.

- **WAN/UART identifier**

  If your device has more than one WAN or UART interface available, the identifier of the interface over which you wish to define the connection will be requested.

- **User**

  When using PPP it is possible that the remote end requests a user and password in order to carry out the connection. This parameter is used to configure the user.

- **Password**

  Through this parameter you configure the password that the remote end will request in order to permit the connection.

- **Call Number**

  This is the remote end telephone number.

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

  You can configure an authentication protocol (PAP or CHAP) which demands a user and a password from the remote end in order to connect.

  The user and password subsequently requested are those that the remote end must provide in order to carry out the connection.

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

  Through this parameter, you configure the time period that the PPP connection remains established when there is no traffic. **This parameter is only applied in cases of switched connections and not in cases of permanent connections.**

c) IP ISDN Connections:

This is used to configure a point-to-point connection (PPP) via ISDN using the basic ISDN interface.

```
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**

  This permits you to select the "logical" B channel that the configuration will be associated to (the communication will be established via the B1 or B2 physical channel depending on what the ISDN network determines).

The TeldatC router permits two PPP connections via the ISDN interface, except in the following cases:

1) ISDN configuration in <B1+B2Permanent> mode, in which case only one PPP connection will be permitted over the said addition.

2) configuration of a PPP connection over a B channel configured as permanent and that also has Multilink enabled (in which case the second B channel is considered permanent).

d) IP AAL-ATM Connections:

This is used to configure a point-to-point connection (PPP) or IP via ATM using the ADSL interface. You need to have added and configured an AAL-ATM circuit in order to add an IP connection.

```
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**

  This is the AAL-ATM circuit identifier which serves as the base for the IP connection.

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

  This is the selection of the traffic type that the IP connection will handle. This can be IP, PPP or PPPoE.

  If you select PPP, you will also be asked for the **user** and **password** needed so that the remote end authorizes the connection.

There are two ways to view the IP connection parameters: a general one, where you can view a table with all the most important connections and data of each connection and a more detailed one, where you can view all the data for a specific connection.

The command to display the configuration is `<LIST IP>` and optionally you can indicate the IP connection identifier you wish: if this value is not provided, a summary of all the configured IP connections is given.

```
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>
```

When you eliminate an IP connection, you also automatically eliminate all the configured parameters required for the said connection, such as routes, backup, multilink, callback, etc.

16. Callback Parameters

It is possible to remotely "wake" the device so it connects, even if the local LAN stations do not have any traffic to transmit. In order to wake the device, carry out a *callback* call: when the device receives a callback call, it is rejected however, it carries out a call to the number that originally called. You can also enable the possibility to accept callback calls in the two B channels independently.

Additionally, you can indicate the telephone number that will accept the callback call: if this number is configured, the device will only "wake" if receiving an ISDN call from the said number and will only carry out the call to this number.

The Callback parameters are configured through the `<ENABLE CALLBACK>` command.

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

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

  Choose the connection where you wish to enable the callback.

Currently you can only enable callback in IP connections over ISDN and in channels that are NOT configured as permanent.

- **Authorized Calling number**

  You are able to restrict the number that will provoke the callback call. If this is left blank, all the calls will be considered as callback.

To consult the callback configuration, execute the `<LIST CALLBACK>` command.

```
Quick Config>list callback

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

Quick Config>
```

To disable the callback over a determined IP connection, execute the `<DISABLE CALLBACK>` command.

17. Multilink PPP Parameters

It is possible to combine PPP sessions to form a single virtual channel or a Multilink bundle. The Multilink protocol is an Internet community standard and its specification is found in [MPPP-96]. The Multilink protocol is a method for splitting, recombining and sequencing datagrams across multiple data links.

The Multilink PPP protocol configuration possibilities in the quick menu have the following characteristics:

1. It's only possible to add PPP sessions associated to ISDN basic access B channels.
2. The addition and subsequent subtraction of a second B channel can be carried out at any moment depending on the bandwidth on demand parameters of the Multilink PPP session.
3. When the two basic access B channels are established, the PPP traffic alternates between both of them.

The Multilink PPP session is established with the IP connection profile. This implies that the new Multilink PPP logical connection will have the parameters of the said IP connection (user, password, connection interval, release time due to the absence of data and the telephone number of the remote access server). It will also adopt the IP connection routes, visible subnets and the connection intervals. The callback feature is supported if it is configured in the IP connection.

The Multilink PPP session responds to the bandwidth on demand pattern. I.e. the second B channel will establish or release depending on the existing traffic in the Multilink session, in accordance with the parameters, which will be described further on.

To enable the Multilink in an IP connection, execute the <ENABLE MULTILINK> command.

```
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**

  Choose the connection in which you wish to enable the Multilink.

Multilink can only be enabled in IP connections that have as a base an ISDN basic access B channel, and provided that the ISDN connector is not configured as permanent B1 plus B2I.

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

  If during the seconds indicated in this parameter, the average occupation of the channel over which the multilink is enabled surpasses the activation threshold, the other channel will active and the multilink bundle will be established.

  This parameter is measured in seconds and the default value is 120 seconds.

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

  If during the seconds indicated in this parameter, the average occupation of the multilink bundle is lower than the deactivation level, the second B channel will deactivate. This parameter is measured in seconds and the default value is 300 seconds.

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

  This is the occupation percentage of the B channel required in order to activate the second B channel in the Multilink. If during the activation interval the average occupation of the first B channel surpasses this value, the second B channel is activated.

  The default value for this parameter is 90%.

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

  Minimum occupation percentage of the Multilink bundle needed in order to maintain the Multilink. If during the deactivation interval, the average occupation of the multilink bundle does not reach this value, the second B channel will be deactivated.

  The default value for this parameter is 50%.

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

  This indicates the direction of the traffic which is taken into account in order to calculate the average load of the channels. This can be incoming (from the external network to the device), outgoing (from the device to the external network) or both. In normal circumstances for access to an external network, for example Internet, where most of the traffic is incoming, we recommend configuring the incoming value. If the visible servers or visible ports are available and assuming that these servers are going to be frequently accessed from the external network, we recommend configuring the "outgoing" or "both" values. The default value for this parameter is "both".

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

  You can configure the Multilink bundle as expropriate, i.e. when the Multilink is using both ISDN basic access B channels and receives a call, the second Multilink B channel will be expropriated and will attend this call.

  As an exception, the calls coming from an "authorized manager" will always provoke expropriation of the second Multilink channel, although this is not configured as such.

To disable the Multilink, execute the `<DISABLE MULTILINK>` command.

To consult the Multilink configuration parameters, execute the `<LIST MULTILINK>` command.

```
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. Authorized Managers Parameters

The ***TELDATC*** device can be managed through the SNMP protocol from an authorized remote management station (pertaining to a defined management subnet and a known configured SNMP community).

A specific case exists where the management network is a private network and the router has an ISDN and/or PSTN interface available: under normal operation conditions, the router provides the users with access to the networks that they have configured (Internet, etc.); if the manager wants to establish communication from his private network with the device, Teldat has developed a mechanism for this whose main element is a device known as ***MASTER ROUTER***: when the manager wants to connect to the ***TELDATC***, he orders the master router to carry out a call to the device to be managed. If this device has the ISDN number configured (or the pattern in cases involving PSTN) that the ***MASTER ROUTER*** calls as an authorized manager, the device to be managed will carry out a call to the number configured with the indicated parameters: a Teldat proprietor communication is established between the ***TELDATC*** and the ***MASTER ROUTER*** for as long as the management of the device continues, this serves so that the ***TELDAT C*** can communicate the IP address assigned to it to the master router and in this way can inform the management station.

To configure and add authorized managers, execute the `<ADD MANAGER>` command. Up to 15 managers can be configured.

```
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**

  The authorized manager telephone number (number that will call the ***MASTER ROUTER***): when the ***TELDATC*** device receives a call via the ISDN line and a check is carried out to see if the caller coincides with an authorized manager. If the number coincides, the call is considered as a management call and is passed to a management state. Contrariwise, the call is handled as a normal incoming call.

  If a call is received via a PSTN line, the ***TELDATC*** checks if the call adjusts to the call pattern defined in the global parameters. If this coincides, the call is considered to be a management call via PSTN, however in order to pass to a management status, there must exist a management profile whose authorized manager telephone number is "0".

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

  This is the ***MASTER ROUTER*** IP address and the network mask, i.e. the IP address to which the ***TELDATC*** device will send the IP packets in order to establish communication with the said ***MASTER ROUTER***. (The mask is needed in order to add a route to the subnet that the ***MASTER ROUTER*** pertains to).

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

  This is the management station IP address and mask: the management station over which the ***TELDATC*** device remote management program is executed can pertain to a distinct subnet from the master router subnet. Therefore, you can define a second subnet to add a route to this subnet via the management connection. If no IP address or mask has been specified, the route will not be created.

- **Login / Password**

  User and password; these values will be ones used when the remote end requests identification on establishing the management connection.

- **Destination telephone of the management connection**

  This is the management connection destination telephone number: telephone number of the node to which the device will connect when establishing a management connection.

Up to 15 management profiles can be defined. In order to view the already created management profiles, execute the <LIST MANAGER> command. With the <DELETE MANAGER> command it is possible to eliminate the management profile you wish and with the <CHANGE MANAGER> command you are able to modify a management profile.

```
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. RIP Parameters

The RIP protocol is a dynamic routing protocol: with this, the router dynamically learns the routes to all the networks that are connected to routers that have RIP enabled.

To globally enable the RIP protocol, execute the `<ENABLE RIP>` command and to globally disable the RIP, execute the `<DISABLE RIP>` command.

To configure the RIP protocol parameters over an IP connection, execute the `<SET RIP>` command.

```
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**

  You are able to configure RIP for each IP connection.

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

  This permits you to configure transmission of the RIP packets as RIP version 1 or RIP version 2 packets; in this latter case, it is necessary to indicate the destination address type to be used (multicast or broadcast).

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

  In the same way as the previous paragraph, you can choose the protocol version or disable the RIP learning via the IP connection.

By default, when you globally enable RIP, all the interfaces will have the RIP packets transmission and reception enabled.

To view the RIP configuration, execute the <LIST RIP> command.

```
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. IP Routing Parameters

To add a static route to the routes table, execute the <ADD ROUTE> command.

```
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**

  This permits you to determine the destination network.

- **Outgoing connection identifier**

  This permits you to determine the IP connection through which the configured network can be reached.

- **Next hop address**

  In cases of IP connections that are not point-to-point types (PPP), you must configure the device address to which the packets destined to the configured network are sent.

- **Cost**

  The cost of the route; faced with two routes with the same destination, the router will choose the cheaper route (lowest number of hops, etc).

To consult the configured routes, execute the <LIST ROUTES> command and to modify the routes execute the <CHANGE ROUTE> command.

```
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. Schedule Control Parameters

The objective of the schedule control is to set the interval time in which the router permits information flow via a determined IP connection.

You can only establish schedule control in IP connections whose traffic is over PPP.

To add a new schedule control profile, execute the <ADD TIME> command.

```
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>
```

In this example a schedule control profile has been added to IP connection 1 that permits connection from 8:30 to 18:30, Monday to Friday.

To delete a schedule control profile, execute the <DELETE TIME> command.

To list the schedule control profiles, execute the <LIST TIME> command.

```
Quick Config>list time

--- Time Controls ---

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

Quick Config>
```

22. Backup Parameters

If on trying to establish a connection problems occur preventing connection, it is possible to configure an alternate backup PPP connection (normally over a switched interface).

The backup configured in the quick menu, is backup via the WAN ReRoute (WRR). Generally, this backup performs by activating the backup route when the main interface is **DOWN** and returns to the main route when the main interface passes to **UP**.

When you configure backup for a PPP connection over a switched interface, there are two conditions that caused the switch to backup. These are as follows:

1. **IPCP Timeout**
   If within the indicated time period the IPCP level cannot be established, then an attempt is made to establish the backup connection.

2. **Maximum number of call attempts**
   In cases of ISDN, if the configured number of calls has been made and it has not been possible to establish the ISDN call, the backup is activated.

These two conditions act simultaneously so that the switch to backup is provoked by whichever condition happens first. If the call is established normally and the IPCP negotiates within the set time, switch to backup does not occur. If backup occurs, the backup parameters activate, the channel routes containing the error change to the backup connection in order to guarantee the user traffic and to carry out the backup call.

In cases where the PPP interface is configured over a permanent interface, the switch to backup is produced when the WRR facility establishment time times out. This default value is configured to 50 seconds.

The configurable backup parameters are as follows and are configured through the <ENABLE BACKUP> command:

```
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)**
  This is the IP connection from which backup is carried out. When this connection is down the backup connection is established.
- **Backup IP connection identifier (1-99)**
  This is the IP backup connection over which the main connection traffic will be routed when the main connection is down.
- **IPCP timeout: [60]**
  This is the maximum period of time that can lapse from the moment the connection is requested until the backup connection activates if, within this period, the IPCP level

has not been established. The range of values permitted for this parameter is from 20 to 200 seconds.

- **Call attempts before entering backup**

  This is the maximum number of unsuccessful consecutive ISDN call attempts allowed before the backup activates. The maximum permitted value for this parameter is 5 retries.

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

  When the main interface is a switched line and the communication has been cut (**DOWN**) and passes to backup, the system cannot know when the main interface can pass to **UP**. For this reason, the system periodically attempts to establish communication via the main channel and if communication is not established the backup continues. Through this parameter you are able to program the time period of the attempts. If left at 0 there are no attempts made to re establish the communication via the main channel. In cases where the main interface is a permanent line, the termination of the backup connection is automatically produced.

If the Maximum backup time parameter is left at 0 in backup for a switched line, once you enter the backup the system will not exit the backup until the communication has finished or the device is reset.

To list the Backup parameters, execute the `<LIST BACKUP>` command.

```
Quick Config>list backup

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

Quick Config>
```

To disable backup in an IP connection, execute the `<DISABLE BACKUP>` command.

You cannot establish as a backup connection, a connection based in a B channel which is configured as permanent.

If backup of a B channel is configured via the other B channel and Multilink is enabled, backup will never be established.

When you carry out `make`***, the backup configuration involves the automatic creation of a route (the same as the one existing through the main interface but at a higher cost) via the secondary interface or backup.***

23. Access Control Parameters

The aim of the access control system is to control user access (internal or external) to determined subnet and/or services. The control is based in an ordered list of inclusive filters (if a packet complies with the condition defined in the filter, it is allowed to progress) and exclusive (if a packet complies with the condition defined in the filter, it is not allowed to progress, i.e. it is discarded).

When a packet is received, the filters are applied in the order established. As soon as the filter condition is complied with, the packet is processed in the mode indicated by the filter without passing through any other filter on the list.

To add an access control, execute the <ADD ACCESS> command.

```
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)**

  The inclusive permits packet progressing. The exclusives discard the packets preventing them from passing.

- **Source IP address / Source mask**

  The packets that have an IP address from this subnet as source will be subject to that indicated by the access control (include, exclude).

- **Destination IP address / Destination mask**

  The packets that have an IP address from this subnet as destination will be subject to that indicated by the access control (include, exclude).

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

  The number of the protocol transported in the packet should be included in the protocol range defined by the first and last protocol fields of the access control. If you program the "all" option in this field in the access control, coincidences will always occur.

The most used protocol numbers are:

6 for TCP (Transmission Control Protocol).

17 for UDP (User Datagram Protocol).

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

  The packet's source port number should be included in the ports range defined by the first and last source port fields of the access control.

  This is only applied if the Access Control Protocol Number field is 6 or 17.

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

  The packet's destination port number should be included in the ports range defined by the first and last destination port fields of the access control.

  This is only applied if the Access Control Protocol Number field is 6 or 17.

The most frequently used port numbers are:

20/21 for FTP

23 for TELNET

25 for SMTP (mail)

80 for HTTP (web/Internet)

For further information on the port numbers and IP protocols, consult the RFC 1700.

Once that the packet coincides with an access control filter, the operation associated with the element is carried out (progress or discard) and the rest of the access control list is not verified.

Therefore, the ORDER of the elements in the access control list is very IMPORTANT.

If after consulting all the access controls configured in the list, no coincidences have been found, the packet is progressed. This means configuring an access control that permits all types of traffic at the end of the access control list.

To view the access control list, execute the `<LIST ACCESS>` command:

```
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>
```

To delete a configured access control, you must execute the `<DELETE ACCESS>` command and indicate the access control you wish to delete.

In the case of having PAT and/or NAT configured, the application order is as follows:

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

24. NAT rule Parameters

The NAT (Network Address Translation) permits the translation of IP addresses. This occurs in such a way that the packets processed by a determined IP connection and coming from a local station with an IP address in the range configured as local addresses, exit to the exterior as if coming from an address configured from the range configured as global, if the destination address is reached via the configured IP connection and vice versa.

Different types of NAT exist: the one known as "N to N" or static NAT, where each IP address is translated to another IP address without overlapping, the "N to 1" or port NAT or PAT, where all the addresses are translated to the same address, etc.

The static NAT rules configuration is explained here.

To add a NAT rule, execute the <ADD NAT> command.

```
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**

  This is the IP connection to which the static NAT rule will be applied.

- **Local subnet address / Local subnet mask**

  Local subnet address to which the static NAT will be applied.

- **Global connection identifier**

  This is the IP connection through which the router connects to the global network.

- **Global subnet address**

  This is the network address for the range of global addresses.

To list the NAT rule parameters, execute the <LIST NAT> command.

```
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>
```

To delete a NAT rule, execute the <DELETE NAT> command and to modify it execute the <CHANGE NAT>; in both commands you must indicate the number of the rule to delete or modify.

25. Visible Port Parameters

When you have the configured the uses of the NAPT, PAT or port NAT, you can define exceptions to the general PAT behavior: by default, when the router receives a packet directed to the IP address of the interface receiving the packet (address where PAT is being carried out over the said interface), this consults an internal table searching for the destination port contained in the packet: if the destination port is not found in the table, this means no internal host carried out a petition and therefore the packet is rejected; if on contrary, the port is found in the table, the router carries out the inverted translation to send the packet to the correct host and port.

The configuration of a visible port permits skipping the said test: when a packet arrives, the list of port tables defined as visible is checked, if the port is present, the packet is rerouted to the indicated port and host; if this is not present in the visible ports table, the packet is processed in the normal way (checking of the open ports internal table, etc).

To configure a port as visible, execute the <ADD PORT> command. As seen in the following example, when you receive a packet destined to port 2000, the packet will be sent to the host 172.24.51.75 and the port is substituted for 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)**

  This is the IP connection through which the port is made visible.

- **Host IP address**

  This is the host address that will make the port visible.

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

  This is the port you wish to make visible.

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

  This is the port number that will make the port visible.

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

  This indicates if the port is generic or FTP (FTP establishes two connections: one data connection and the other control).

To delete the visible port configuration, execute the <DELETE PORT> command, <CHANGE PORT> to change a parameter and <LIST PORT> to display the configured visible ports.

```
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>
```

The router offers a series of services in the standard ports, specifically the FTP server (20/21), Telnet (23), DNS (53) and HTTP (80); these services can be transferred from a port in order to leave the said standard ports free and in this way permitting their use to configure visible ports from internal hosts.

26. Visible Subnet Parameters

Another exception to the NAPT/PAT is the definition of visible subnets: by default, all the traffic leaving an IP connection with NAPT/PAT enabled, undergoes the substitution of the source IP address for the interface address and vice versa when the packet is a response. A visible subnet does not undergo the said transformation, i.e. the source address is maintained as invariable.

To add a visible subnet, execute the <ADD SUBNETWORK> command.

```
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)**

  This is the IP connection through which the subnet is visible.

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

  This is the subnet IP address that will be made visible through the IP connection defined in the previous parameter.

- **IP address of the default gateway**

  In cases where the visible subnet is directly connected to the access router through the LAN interface and the router does not have the address for the said visible subnet available, it is necessary to configure the address that the visible subnet hosts have configured as the default router and in this way the router is able to respond to the ARP petitions sent by the hosts.

To delete the configuration of the visible subnet, execute the <DELETE SUBNETWORK> and <CHANGE SUBNETWORK> command to modify the configuration and <LIST SUBNETWORK> in order to list the configuration.

```
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. IPSec Parameters

This section describes the commands needed to configure the IPSec protocol. In order to access the IPSec protocol configuration environment, you need to introduce the <IPSec> command.

```
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>
```

The following commands are available within the IPSec protocol configuration environment (indicated by the **IPSec Quick config>** prompt):

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

The following table summarizes the IPSec protocol configuration commands. The letters written in **bold** are the minimum number of characters that must be entered in order to activate the command.

Command	Function
? (HELP)	Lists the commands or their options.
ADD	Permits you to add a template or entry in the tunnels definition table, an IPSec access control or traffic selector or a key.
CHANGE	Permits you to modify some of the parameters corresponding to a template or entry in the tunnels definition table, an IPSec access control or traffic selector or a key that has been previously introduced.
CLEAR	Clears all the entries existing in the tunnels definition table, all the IPSec access controls or traffic selectors or all the configured keys.
DELETE	Deletes an entry in the tunnels definition table or an IPSec access control or a key.
DISABLE	Disables IPSec.
ENABLE	Enables IPSec.
LIST	Lists the IPSec configuration.
EXIT	Returns to the previous prompt.

The IPSec default configuration is "IPSec disabled" without any created tunnels or traffic selectors nor entries in the keys table.

27.1. ?(HELP)

By entering **?** this displays all the available commands. You can also use the ? symbol to view the various options for each command.

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

27.2. ADD

The <ADD> command permits you to add a key, an entry in the tunnels definition table or an access control:

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

a) ADD KEY

With the help of this command, you can configure the keys that the local endpoint expects to receive from the remote endpoint(s) that are trying to communicate with this through the IPSec tunnel, associated with the corresponding identifier of the other end (IP address or 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>
```

The meaning of the distinct requested parameters is as follows:

- *Remote peer id type*: Indicates the type of identifier that the remote endpoint uses in order to be acknowledged by the local endpoint. The possible identification types are through the IP address if the remote endpoint is acting as server (i.e. the local endpoint is an IPSec tunnel client) or through the hostname if the remote endpoint is behaving as client (the tunnel server is therefore the local endpoint).
- *IP Address/Hostname*: This is the identifier of the remote endpoint itself. On establishing a tunnel, a device which is going to use a determined key identifies itself to the other tunnel endpoint through its identifier (hostname if this is client or IP address is this is server).

Therefore, on configuring the keys that the device acknowledges, these must also be associated to an identifier.

- *Key*: With this parameter, you configure one of the keys that the device considers valid i.e. that will permit the establishment of the tunnel with the device going to use this key and that identifies itself to the local endpoint with the IP address or hostname associated with this key.

When a device operates as an IPSec tunnels client and therefore going to use its hostname in order to identify itself to the other endpoint, it is very important that the said hostname is configured. In order to do this, add the hostname through the <SET HOSTNAME> command in the global quick menu.

b) ADD REMOTE tunnel endpoint

Permits you to configure the templates or the entries in the tunnels definition table (which is the same thing). Each entry will contain the necessary parameters to configure an IPSec tunnel towards a determined destination.

```
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>
```

The distinct requested parameters and their meanings are indicated below:

- *Remote tunnel endpoint identifier*: Tunnel identifier. This serves to make reference to this entry and to determine in this way the specific tunnel, to which a certain traffic selector or access control is associated, or to delete a specific entry or modify one of its parameters.
- *Source address of local tunnel endpoint*: An IP connection is selected from those configured in the device which make up the tunnel source. This is a way to select the interface and IP address considered as the tunnel source to which the entry refers.
- *Remote tunnel endpoint IP address*: Remote tunnel endpoint address. This only admits IP addresses, not equivalent names (which can be resolved through DNS).
- *Remote backup IP addresses*: Remote endpoint backup addresses. You can configure none, one, two or up to three backup addresses. A 0.0.0.0 backup address is dealt with to all effects as non-existent. In the same way as the main remote endpoint address, only IP addresses can be configured, not equivalent names.

- *Id type*: Type of identification used by the local endpoint in trying to establish the tunnel with the remote endpoint. If the local device behaves as a tunnel client, this identifies itself to the other endpoint through its hostname (this must be configured), while if this is the server, it identifies itself to the other end with its IP address.
- *NAPT enabled:* On enabling this parameter, this indicates if the NAPT rules are going to be applied before IPSec at the tunnel source. This implies that the traffic going through this tunnel will always have the resulting IP address after applying NAPT as source. This means therefore that only the access controls whose source is given by the same IP connection taken as source from the IPSec tunnel and with the host mask are significant.
- *Lifetime:* Lifetime of the isakmp template generated from this entry in the tunnels definition table. The lifetime of the corresponding dynamic template is calculated from this value applying the 3300/3600 factor which is the relation existing between the dynamic tunnels and isakmp default values.
- *UDP encapsulation:* If this parameter is enabled then UDP encapsulation is applied to the ESP packets that go through the IPSec tunnel. This is important if you wish to apply NAPT to these packets in one of the intermediate devices located before the tunnel exit.

c) ADD TRAFFIC selector

This command is used to add IPSec traffic selectors or access controls.

```
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>
```

For each access control, you need to configure:

- *IPSec traffic selector identifier*: Traffic selector identifier. Serves to refer to a specific entry in the table when modifying one of its parameters or deleting it.
- *Destination IP address*: Destination IP address.
- *Destination IP mask*: Mask associated to the destination IP address. Through this parameter and the previous one, you configure that the traffic transmitted to this destination is routed through the tunnel indicated by the following field.
- *IPSec remote tunnel endpoint identifier*: Tunnel identifier through which the traffic is routed to the destination determined by the previously configured address and mask. The identifier must refer to a tunnel previously configured in the tunnels definition table.

27.3. CHANGE

It is possible to modify one or various parameters for an entry in the keys table, for an entry in the tunnels definition table or access control, previously introduced by using the <CHANGE> command.

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

a) CHANGE KEY

Permits you to change the key associated to a determined remote endpoint identifier.

```
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

With this command it is possible to modify an entry previously introduced in the tunnels definition table. The specific entry, whose parameters are going to be changed, is indicated through its identifier.

```
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

This command is used to modify one or some previously configured IPSec access control parameters, which will be from the given identifier.

```
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

Through the <CLEAR> command, you can clear all the entries in the keys table, all the entries in the tunnels definition table or all the configured IPSec access controls.

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

a) CLEAR KEY

Clears all the configured IPSec keys i.e. the remote endpoints identifiers (hostname or IP address) and their associated keys that the local device is capable of acknowledging in such a way that an IPSec tunnel can be established between them.

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

No IPSec keys configured

IPSec Quick config>
```

b) CLEAR REMOTE tunnel endpoints

With this command, you clear all the entries in the tunnels definition table. Each table entry contains the parameters required to configure an IPSec tunnel towards a determined destination.

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

No IPSec remote tunnel endpoints configured

IPSec Quick config>
```

You need to be aware that if you have a traffic selector table configured and another tunnels definition table to which the traffic selectors are associated, on eliminating the tunnels you automatically eliminate the traffic selectors associated to the said tunnels. The same thing occurs if you delete the IP connections table: as all tunnels must have an existing IP connection as source, if you delete them all you also eliminate all the entries in the tunnels definition table and consequently also delete all the configured traffic selectors.

c) CLEAR TRAFFIC selectors

This clears all the existing IPSec traffic selectors or access controls.

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

No IPSec traffic selectors configured

IPSec Quick config>
```

27.5. DELETE

Through the <DELETE> command, you can delete one of the configured keys, an entry in the tunnels definition table or a previously introduced IPSec access control.

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

a) DELETE KEY

Deletes one of the configured IPSec keys, that corresponding to a certain identifier for the remote endpoint (hostname or IP address): on introducing the <DELETE KEY> command, you will be asked for the remote endpoint identifier, deleting this and its associated key from the configured keys table.

```
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

Deletes an entry in the tunnels definition table. The identifier will be that indicated.

```
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

Through this command you delete access control for the given identifier.

```
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

The <DISABLE> command within the IPSec configuration menu permits you to disable IPSec.

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

27.7. ENABLE

Simply enter the <ENABLE> command to enable IPSec although this will not begin to operate until you have carried out a MAKE operation from the global quick menu.

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

27.8. LIST

The <LIST> command is used to view the content of the IPSec configuration.

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

a) LIST ALL

This displays the whole of the IPSec configuration.

```
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

Through this command, you can view all the existing entries in the keys table; i.e. permits you to know which remote endpoints, identified by their IP address or hostname, have configured keys.

```
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

With this you can view all the entries in the tunnels definition table. Each entry contains the parameters required to configure an IPSec tunnel towards a specific destination.

```
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

Through this command all the configured IPSec traffic selectors or access controls are displayed on screen.

```
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 this command to return to the previous prompt.

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

27.10. EXAMPLE OF GENERATING THE IPSEC REAL CONFIGURATION FROM THE QUICK CONFIGURATION

On executing the MAKE operation so that starting from the configuration introduced through the quick menu, the real configuration of the device is generated. In the case of IPSec the steps to carry out are as follows:

- You need to delete the configuration existing in the SRAM registers corresponding to the IPSec.
- With the information contained by the global variable to enable/disable IPSec, proceed to initialize the variable using the real IPSec configuration.
- QOS Preclassify disabled by default.
- For each of the entries existing in the tunnels definition table, two templates or IPSec tunnels are created: one isakmp type (for phase I) and the other dynamic (for phase II). In both cases 3DES encryption and MD5 authentication are used, anti-replay enabled, Oakey 1 group, PFS disabled, aggressive mode with identification through Fully-Qualified Domain Name (ID_FQDN) if the local endpoint behaves as client, using its hostname as identifier and if this is server, this identifies through its IP address. The lifespan of phase I is that configured in the corresponding table entry, and for phase II, the result after multiplying this value by the 3300/3600 factor. As source address for the templates, that corresponding to the IP connection indicated in the tunnels definition table entry is taken. From here the two IPSec templates are created and also the main address and the tunnel remote endpoint backup addresses are taken from here. For the dynamic templates, if dealing with a Teldat C3 device and one of the addresses configured in the TRMTP profiles corresponds to a subnet defined by one of the access controls associated to this template, you must enable the KeepAlive. The values for the KeepAlive (at a global level) are determined in the following way: the maximum number of seconds without a response are taken by checking all the configured addresses in the TCP profiles (in the first place) and the largest value is taken from the parameters indicating the timeout configured for addresses pertaining to a subnet defined by some access controls, and the maximum number of packets without response take the value 10.

  Only in cases where no address for these subnets in the TCP profiles is found, does the search extend to the addresses configured in the TRMTP profiles which pertain to the access controls destination subnets, choosing as the value from the maximum number of seconds without response, the biggest of the T1*N2 products and as the maximum number of packets without response 2. If no address is found for the access controls destination subnets either in the TCP profiles or in those of the TRMTP then the default values are taken.

  - Maximum number of queued packets without response: 2.
  - Maximum number of seconds without response: 20 seconds.
  - If the device is not a Teldat C3, the KeepAlive (at a global level) is disabled.

- For each one of the configured traffic selectors an IPSec access control for each IP connection is created, with source address being the subnet defined by the said IP connection and the destination and mask address being those configured; if the address is unnumbered or coincides with the tunnel source to which the selector is associated, the host mask is used. This access control will be associated to dynamic template originating from the entry in the tunnels definition table, whose identifier will be that configured for the traffic selector. An access control is also created from each entry in the traffic selectors table for each directly connected route, provided that this does not deal with a default route and that the route does not use the same IP connection used by the tunnel to which the selector is associated. In cases where NAPT is enabled in the tunnel to which the traffic selector is associated, only one IPSec access control is created from the said selector whose source address will be that of the IP Connection taken as tunnel source and with the host mask. Each generated access control is associated to an IP connection or rule, a rule that corresponds to the tunnel source IP connection to which the said access control is associated. If a rule already exists for this IP connection, it is not modified (if it corresponds to an NAPT rule, it will continue using this for NAPT for example), and if an IP rule does not exist generated from this IP connection, one is created with source being the source IP address of the tunnel to which the selector is associated, destination address 0.0.0.0, NAPT disabled and firewalling also disabled. Additionally in cases of dealing with a Teldat C3, the Centrix-Ds configured in the POS quick menu are checked and if the traffic selectors destinations configured in the IPSec quick menu coincide with the said Centrix-Ds, IPSec access controls are generated which restrict the ports and protocols used to those used in POS transport over IP employed by the Teldat C3; i.e. if some of the addresses configured in the TRMTP and TCP profiles pertain to the subnet defined by the address and mask of the corresponding traffic selector, the range of ports associated to the said access control will only consist of the port number configured in the profile and for this specific address. The range of protocols will be reduced to the TCP protocol if this is the POS transport mode over IP configured for this Centrix-D as destination (i.e. if this address is found in a TCP profile) or to the UDP protocol if you are going to use a transport mode based on TRMTP towards this Centrix-D (the address pertains to a TRMTP profile).
- From the configured keys and hostname/IP addresses associated to these, the real list of the IPSec keys is created.
- Save the configuration.

If you have the following IPSec configuration in the quick menu:

```
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>
```

The IPSec configuration generated after carrying out the MAKE operation and restarting is as follows:

```
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>
```

You can see that although the identifiers have changed with respect to the configuration in the IPSec quick submenu, the associations between tunnels and traffic selectors are correct as previously explained.

28. Point of Sale Terminals Parameters

The quick configuration and monitoring (POS submenu) can be consulted in the specific manual for the configuration for the support of point of sale terminals. This manual includes both the quick configuration and monitoring as well as the standard configuration and monitoring.

29. IP Discovery Parameters (TIDP)

The TIDP (Teldat IP Discovery Protocol) is a protocol that allows the ***TELDATC*** devices to inform a series of address discovery stations of the IP address obtained in an IP connection so that the device can be accessed by the remote management stations for management purposes.

In order to do this the device sends some special messages to the IP address discovery stations. These packets are periodically sent through UDP to some addresses and ports configured in the ***TELDATC DEVICES***. In this way the IP address discovery stations notify the management applications at which address the device originating the messages is located and therefore access it for management.

In order to configure and add IP address Discovery Stations, use the <ADD DISCOVERY>. You can configure up to 99 stations.

```
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**

  Discovery Station Identifier. The permitted range is between 1 and 99.

- **Discovery Station IP address**

  Discovery Station IP Address. This is the address that the ***TELDATC*** devices will send the address notifications to.

- **Discovery Station port**

  Transport port (UDP) to which the messages are sent.

- **Local port**

  Local transport port (UDP) where the messages are listened to.

- **Notification interval**

  Time between notifications being sent (in seconds).

You can define up to 99 address discovery stations. In order to see the configured stations, execute the <LIST DISCOVERY> command.

```
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>
```

You can delete any IP Discovery Station you wish through the <DELETE DISCOVERY> command and modify the configured parameters through the <CHANGE DISCOVERY> command.

30. Configuration and recording generation

To record the configuration, execute the <SAVE> command and the <MAKE> command to generate it; the configuration generation implies recording.

```
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>
```

We strongly recommend restarting the device once the configuration has been generated. Many of the parameters do not take effect until the device is restarted; if the restart is not executed, this can provoke instabilities in the device configuration.

31. Configuration default values

The device exits the factory with a default configuration. This configuration can be reactivated by the user through reloading the default configuration as described in the installation manual (activating microswitch 5 located in the base of the device during the start up sequence) or through the configuration command <SET DEFAULT-CONF>. When the default configuration is activated through this command, only the "visible" configuration is modified, the configuration being executed is not modified. Therefore if you are remotely accessing you do not lose the connectivity; also you will not lose the configuration if you do not record the this before restarting, i.e. if you execute the command and restart, the previous configuration is not lost.

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

The default values can be the following, except in special cases:

- Access parameters:
  - User and access password empty.
- ISDN parameters
  - Switched B channels and incoming calls are disabled.
- WAN parameters:
  - In AT command mode, speed 57600 (except C3x models).
  - In POS mode, speed 9600 (C3x models).
- PSTN parameters:
  - Incoming calls disabled.
  - Call pattern detection disabled.
- SNMP parameters:
  - "Public" reading community with restricted access to the MIB-2.
  - ECHO UDP sent before the traps are sent.
- ADSL parameters:
  - Minimum transmission speed will be 1/25 of the obtained transmission speed.
  - Operating in MULTIMODE.
- IP connections:
  - IP connection based in the LAN with address 192.168.1.1 mask 255.255.255.0 without NAPT.
- DHCP server activated:
  - Range of addresses: 192.168.1.1 - 192.168.1.255.
  - Subnet mask: 255.255.255.0.
  - Default Router: 192.168.1.1 (the device itself).
  - DNS server: 192.168.1.1
  - Session time: 1 day (1440 minutes).

Under these conditions, the DHCP clients connected to the router LAN will obtain an IP address from the network 192.168.1.0/24, with the exception of address 192.168.1.1. This is assigned to the LAN interface of the router itself. You are able to access the router through Telnet, via FTP (accessing as "root" user without a password) or by http ("teldat" user with the password "teldatc").

It is also possible to obtain device statistics through SNMP and the "public" community. By default you only have read access for the MIB-2 variables.

Chapter 3
Command line monitoring

1. Quick monitoring menu

Through the quick monitoring menu, you can obtain a global view of the statistics associated to the configuration generated through the quick configuration menu. In order to access the monitoring, you need to enter the following commands from the system menu:

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

The quick monitoring is divided into two distinct parts:

- Daily monitoring: these are statistics taken from the moment the device is switched on. When the device is switched off or restarted, these statistics are deleted.
- Fortnightly monitoring: these are statistics taken from the last fifteen days. The current day statistics are periodically accumulated and stored in a non-volatile memory. The statistics are restarted at the beginning of each new day.

The statistics that can be viewed in each of these monitoring menus are detailed below.

The number of statistics that can be stored in the TELDAT C is limited and varies according the interfaces the device has available.

The appendix of this manual details the exact number of statistics depending on the router interfaces.

2. Daily statistics

Two commands can be executed in relation to the daily statistics monitoring: through the <LIST DAILY> command, you can view the statistics, and through the <CLEAR DAILY> command you can restart these statistics. The example given below shows the display of statistics associated with daily monitoring:

```
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>
```

These are the most important groups among these daily statistics:

- LAN interface statistics: status, number of collisions, number of errors and transmitted and received bytes.

- ADSL interface statistics: successful and failed authentications, (for PPP connections) and packets received through a connection with enabled NAPT whose destination is a non-valid port (TCP/UDP packets) or with a non-valid identifier (ICMP packets).

- ISDN interface statistics: successful and failed authentications for the two basic access B channels.

- PSTN interface statistics: successful and failed authentications.

- Statistics from the stations provoking the call, indicating the date and time of the call, the source IP address, the destination IP address, the type of protocol originating the call and the source port and call destination.

- The calls that are active at the time the statistics are requested.

- Released calls statistics. This is where you are able to view the following parameters: the ISDN call line (L), type of call (T), with (I) if incoming or (O) if outgoing, called number and caller number, cause of the release (CC), release diagnosis (DC), time and date the call was established, time and date the call was released, cost of the call if this is provided by the operator.

- Statistics for the defined visible subnets: statistics for incoming and outgoing traffic, both in bytes and number of packets through the visible subnet.

- Statistics for the defined visible ports: statistics for incoming and outgoing traffic, both for bytes and number of packets through the visible port. This also displays some total statistics for the visible ports (transmitted and received packets).

3. Fortnightly Statistics

There are two commands that can be executed regarding monitoring of the fortnightly statistics: with the <LIST FORTNIGHLY ISDN> or <LIST FORTNIGHLY ADSL> commands you are able to view the statistics and with the <CLEAR FORTNIGHLY> command you restart the said statistics.

Below you will find a statistics viewing example associated to the fortnightly monitoring of the ISDN statistics:

```
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>
```

The ISDN fortnightly statistics display the following information:

- A table containing the statistics for each day contained in the fortnight: the first line in the table corresponds with the current day, the second the previous day and so on up to fifteen days. In the table you can see the following parameters:

- Date
- Traffic via B1 and B2 in bytes
- Traffic via B1 and B2 in packets
- The time the channels have used with an established call (the value is expressed in tic time, 1s = 360 tic time)
- Calls via B1 and B2
- Successful authorizations in B1 and B2

- Statistics for a specific day. There are two tables:
  - The hosts that originated the traffic

    Host IP address

    Traffic in packets through B1 and B2.
  - Accessed addresses (favorites):

    Accessed IP addresses

    Total traffic in packets.

The ADSL fortnightly statistics display the following information:

- A table containing the statistics for each day in the fortnight: the first line in the table corresponds with the current day, the second the previous day and so on up to fifteen days. In the table you can see the following parameters:
  - Date
  - Last time the entry was updated
  - Incoming and outgoing traffic in bytes
  - Incoming and outgoing traffic in packets
  - Successful and failed authentication in PPP links over ADSL

- Statistics for a specific day. There are two tables:
  - The hosts that originated the traffic

    Host IP address

    Traffic in bytes and in packets directed to this host and originated by the same
  - Accessed addresses (favorites):

    Accessed IP addresses

    Traffic in bytes and in packets directed to this address and coming from the same

Chapter 4
Appendix

1. Global view of the quick menu

The following figure aims to provide a graphic view of the quick configuration elements: five main blocks are presented, representing each one of the physical interfaces the device has available:

1) LAN
2) ADSL over POTS
3) ISDN
4) WAN
5) UART

Each step represents a configuration level, for example: you can configure ADSL line parameters, subsequently and only over an ADSL line you can configure AAL-ATM connections over which in turn you can define IP connections. There can be two types of IP connection : IP and PPP; over which in turn, related to the IP connections, you can define routes, NAT rules, etc.

In cases of WAN, this can be configured in varaious modes (PSTN, ASDP, POS, etc.): If you configure in PSTN mode, you can configure MANAGERS and IP PPP connections:

The configuration of DHCP, DNS, SNMP etc., is separate.

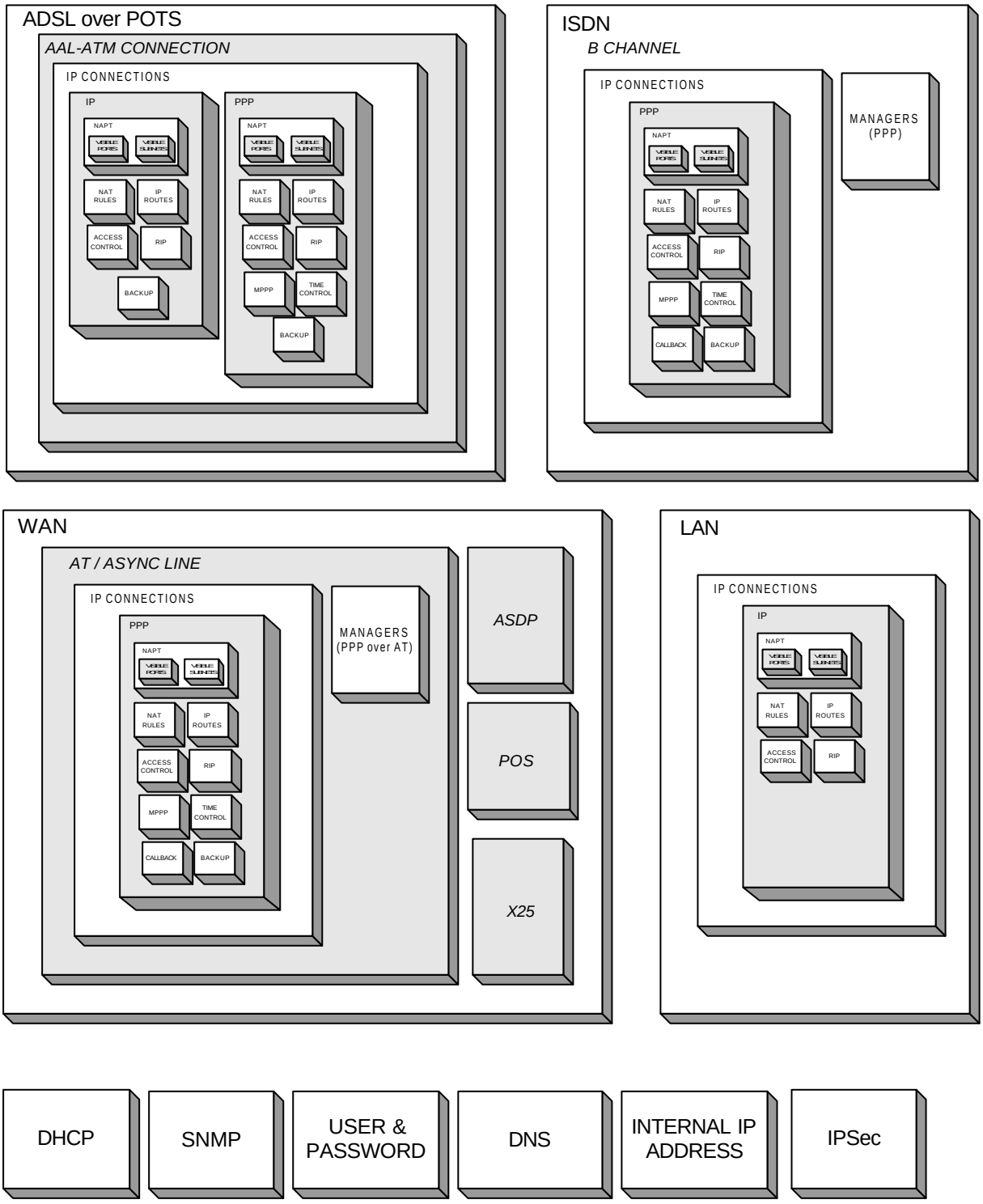

Figure 4.1: Graphic view of the quick configuration

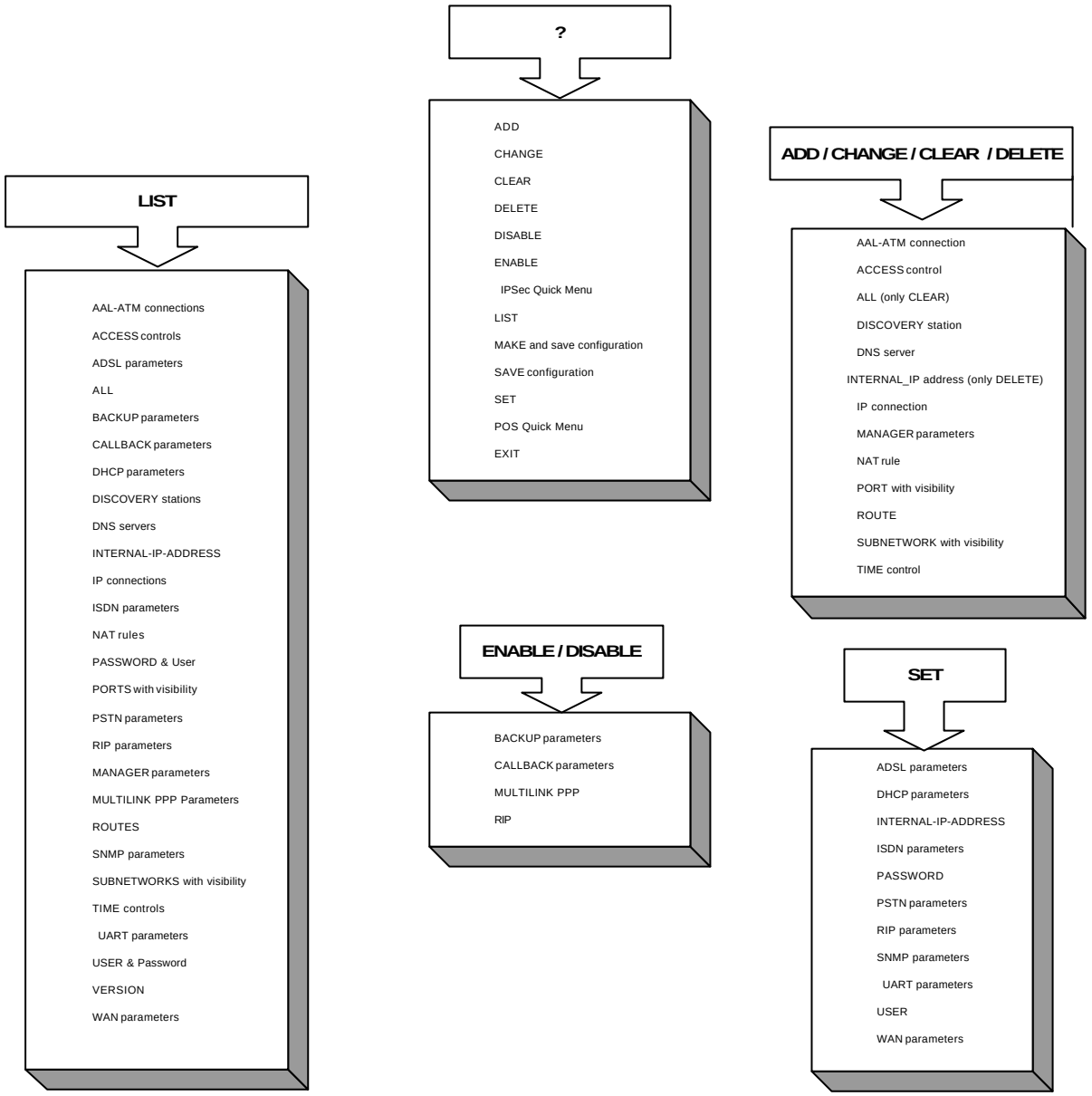

Figure 4.2: Quick configuration and monitoring schemes.

2. Non volatile statistics

Below you will see a table where the number of statistics stored in the ***TELDAT C*** router is displayed depending on the number of available interfaces.

	ADSL	ISDN	POS	
Most frequent destinations	256			Transactions OK
Most active hosts	50			Transactions KO
Most frequent destinations		256		Transactions OK
Most active hosts		50		Transactions KO
Most frequent destinations	128	128		Transactions OK
Most active hosts	25	25		Transactions KO
Most frequent destinations	128		1000	Transactions OK
Most active hosts	25		500	Transactions KO
Most frequent destinations		256	1000	Transactions OK
Most active hosts		50	500	Transactions KO
Most frequent destinations	64	64	1000	Transactions OK
Most active hosts	12	12	500	Transactions KO

To consult the above table, you need to search for a pair of columns that have a cross in those interfaces that your device does not have available; for example, if your device has ADSL available and ISDN but does not support POSs, the pair of columns it corresponds to is the third one, where you can see that the number of destinations most frequently accessed by ADSL is 128, the same for ISDN. The number of most active hosts (that provoke the most traffic) is 25 in both cases. If your device has an ISDN line and supports POSs, your pair of columns is the fifth. Here you can see that the number of destinations most frequently accessed is 256, the 50 most active hosts and the storing of 1000 successful transactions and 500 failed.

3. Configuring the Hosts

This section displays possible configuration examples for the local area network (LAN) workstations, in the most common operating systems, in order to access the external networks through the ***TELDAT C*** router. The configuration examples reflect a scenario where the local workstation occupies address 192.6.1.168/24 in the LAN and the ***TELDAT C*** router occupies address 192.6.1.224/24.

It is not our intention to give a detailed description of the configuration process in each platform; this is not the primary aim of this manual. The idea here is to indicate the basic configuration process in the aspects that most influence operations with the ***TELDAT C*** router. For a more detailed description of each platform, consult the manufacture's manual.

3.1. Workstations with Windows 95 or 98 operating system

a) Basic Configuration

The PC TCP/IP protocol basic configuration with a Windows 95 operating system is carried out through the "Network Environment" icon found in the "Control Panel". Figure 4.3 shows the "Network Environment" dialogue box in a PC to which the TCP/IP protocol has been configured over an Ethernet card.

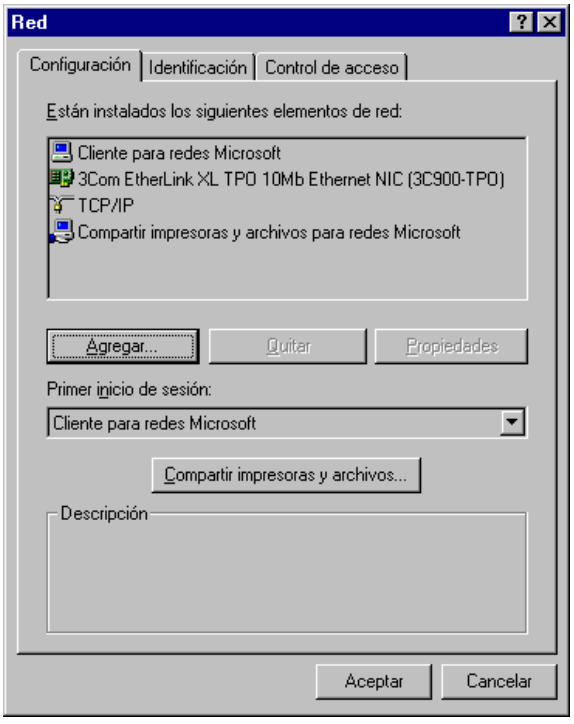

Figure 4.3: Microsoft Windows 95 Network screen

To configure the TCP/IP parameters you need to open the TCP/IP dialogue box from the previous network dialogue box. Figure 4.4 shows the tab where the LAN's PC address is configured.

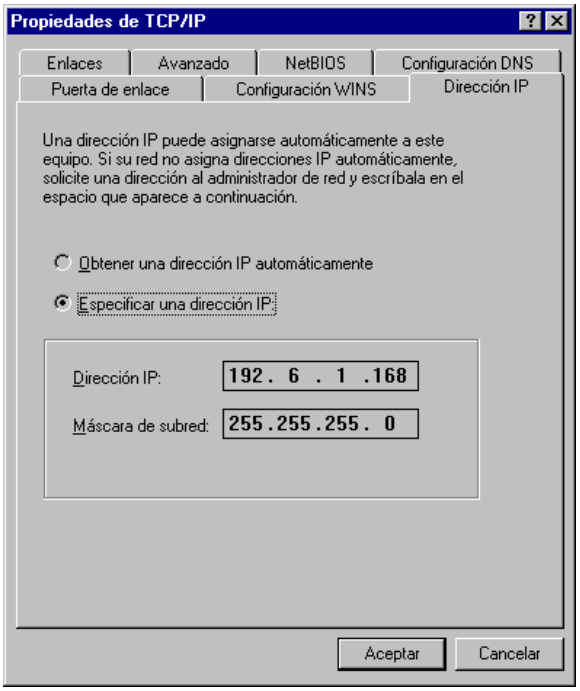

Figure 4.4: Windows 95 IP Address screen

Figure 4.5 shows the PC's default route configuration tab.

Figure 4.5: PC default router with Windows 95

Lastly, **Figure 4.6** shows the DNS parameters configuration of a PC with a Windows 95 operating system.

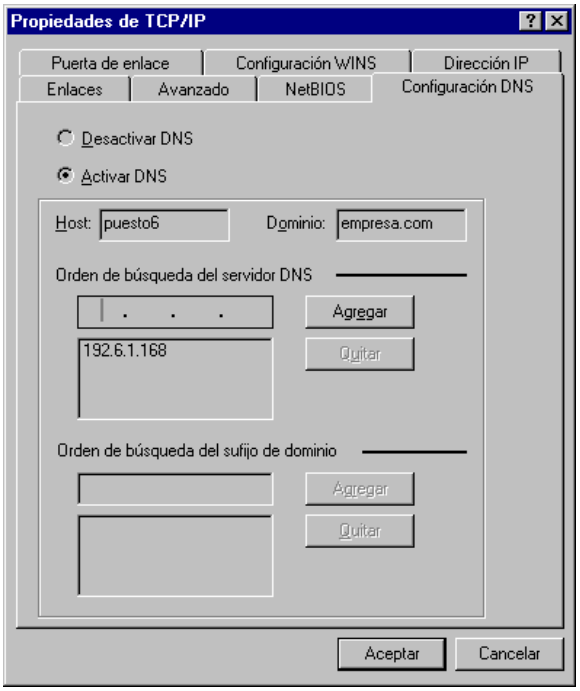

Figure 4.6: PC DNS Parameters with Windows 95

b) Advanced Configuration

Dynamic route configuration

From an MS-DOS session in Windows 95 you can dynamically add and delete routes through the **ROUTE** command. Below, the help for this command is shown.

```
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.
```

In the scenario being described, the outgoing command "**ROUTE PRINT**" is shown below. Please note that the TCP/IP stack automatically configures in order to support network broadcast addresses, local loop and 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:\>
```

System Register Parameters

Apart from the explained graphic configuration, it is also possible to directly configure various Microsoft TCP/IP stack parameters for Windows 95 in the system register. Please consult [MICROSOFT-95] for further information. To modify the system register you can use the Windows 95 system register editor (regedit.exe). Below, you can see a brief description of the parameters that are associated with the ***TELDAT C*** router. You need to restart the PC in order for the said parameters to take effect.

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

Value	**Size**	**Description**
DefaultRcvWindow	16-bit	Specifies the default reception window announced by TCP. Default is 8192.
DefaultTOS	8-bit	Specifies the type of default service (TOS) for the IP packets. Default is 0.
DefaultTTL	8-bit	Specifies the initial TTL by default. Default is 32.
DnsServerPort	16-bit	Specifies the DNS server port where the requests are sent. Default is 53.
KeepAliveTime	32-bit	Specifies in milliseconds, the inactive time delay after which the TCP begins to send "keepalives" should these be permitted in the TCP connection. Default is 2 hours (7200000).
KeepAliveInterval	32-bit	Specifies in milliseconds the time between "keepalives" retransmission, once the KeepAliveTime has expired. Once this has happened the "keepalives" send each KeepAliveInterval milliseconds until it receives an answer or until a maximum of MaxDataRetries before aborting the connection. Default is one second (1000).
MaxConnections	32-bit	Specifies the maximum number of concurrent connections. Default is 100.

MaxConnectRetries	32-bit	Specifies the number of times a connection attempt (SYN) is transmitted before being abandoned. The initial retransmission timeout is 3 seconds and is doubled each time up to a maximum of two minutes. Default is 3.
MaxDataRetries	32-bit	Specifies the maximum number of times a data TCP segment or an end of connection (FIN) is transmitted before the connection is aborted. The retransmission time varies according to the link conditions. Default is 5.

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

Value	**Size**	**Description**
MaxMTU	16-bit	Specifies the maximum IP datagram size that can be passed to the Media Access Control. SNAP and source routing headers (if used in the interfaced) are not included in this value. E.g. in Ethernet MaxMTU is valued at 1500. The value used is the minimum value specified for this parameter and the size indicated by the Media Access Control. The default value is that indicated by the Media Access Control interface.

3.2. Workstations with Windows NT 4.0 operating system

a) Basic Configuration

The TCP/IP protocol basic configuration of a PC with Windows NT 4.0 operative system is carried out through the "Network Environment" icon in the "Control Panel". **Figure 4.7** shows the "Network Environment" dialogue box in a PC which has the TCP/IP protocol configured over an Ethernet card.

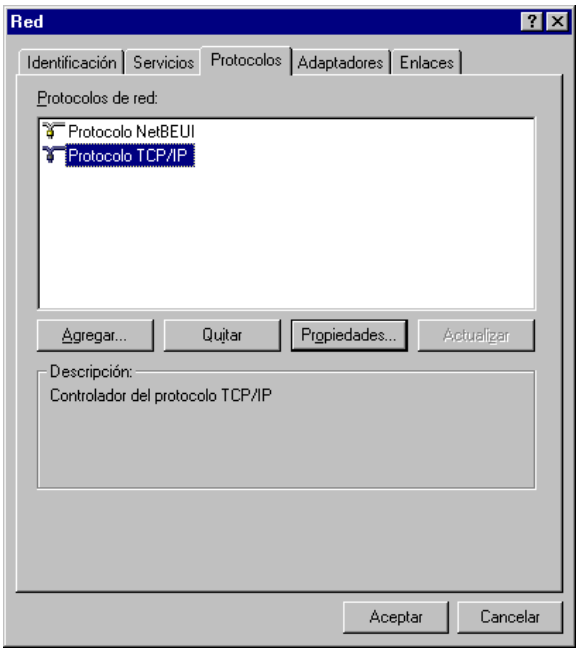

Figure 4.7: Windows NT 4.0 Network Environment screen

To configure the TCP/IP parameters you need to open the TCP/IP dialogue box from the previous "Network" dialogue box. **Figure 4.8** shows the tab where the LAN PC address and default route are configured.

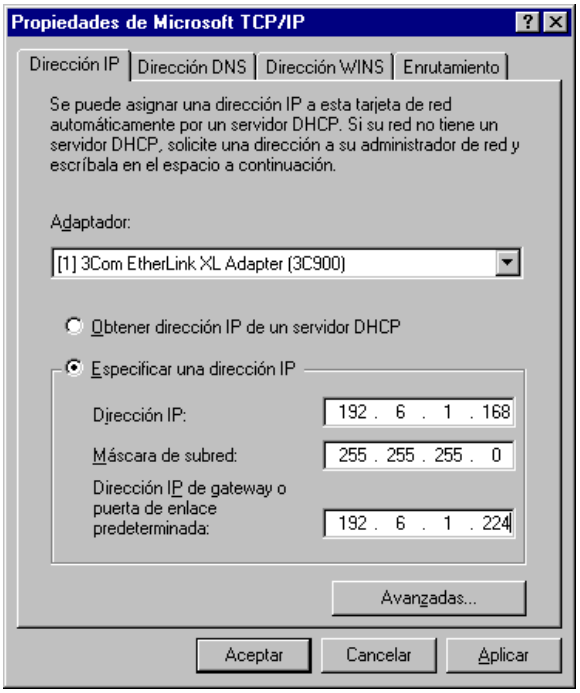

Figure 4.8: Windows NT 4.0 IP Address and default router

The parameters relative to DNS are configured in the "DNS" tab as seen in **Figure 4.9**:

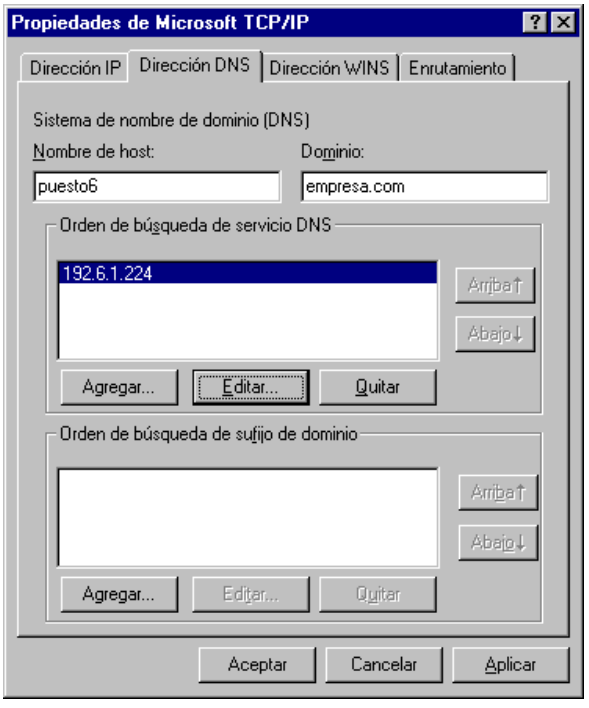

Figure 4.9: Windows NT 4.0 DNS parameters

b) *Advanced Configuration*

Dynamic route configuration

From a DOS session in Windows NT 4.0 you can dynamically add and delete routes through the **ROUTE** command. The main difference between this and Windows 95 is that the introduced routes can be made permanent i.e. they do not disappear on restarting the device. Below, the help for this command is shown.

```
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.
```

System Register parameters

Apart from the explained graphic configuration, it is possible to configure various Microsoft TCP/IP stack parameters for Windows NT 4.0 directly in the system register. Please consult [MICROSOFT-97] for further information. To modify the system register you can use the Windows NT 4.0 system register editor (regedit.exe). You can see a brief description of the parameters that are associated with the ***TELDAT C*** **ADSL** router. You need to restart the PC in order for the parameters to take effect.

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

Value	Size	Description
ArpCacheLife	32-bit	Determines in seconds the lifetime of the ARP cache entries. Default is 600 seconds for used entries and 120 for unused entries.
ArpUseEtherSNAP	32-bit	Determines if TCP/IP transmits the packets in Ethernet using 802.3 SNAP or DIX format encoding. Default is 0, DIX format.
DatabasePath		Specifies the path to the Internet files such as Hosts, Networks, etc. Systemroot\ System32\ Drivers\Etc by default.
DefaultTOS	32-bit	Specifies the default type of service (TOS) of the sent IP packets. Default is 0.
DefaultTTL	32-bit	Specifies the default TTL. Default is 128.
KeepAliveInterval	32-bit	Determines in milliseconds the "keepalives" sending interval. TCP sends "keepalives" in order to check the connections which are not transmitting data are still active. 0x3E8 (1 second) by default.
KeepAliveTime	32-bit	Specifies in milliseconds, the inactive time delay after which the TCP begins to send “keepalives” should these be permitted in the TCP connection TCP. Default is 2 hours (7200000).
TcpMaxConnectRetransmissions	32-bit	Determines the number of times TCP retransmits a connection request before abandoning it. Default is 3.
TcpMaxDataRetransmissions	32-bit	Specifies the maximum number of times a data TCP segment is retransmitted before the connection is aborted. The retransmission time varies according to the link conditions. Default is 5.
TcpNumConnections	32-bit	Determines the maximum number of connections that the TCP can have open at the same time. 0xFFFFFE by default.
TcpWindowSize	32-bit	Determines the maximum window offered by TCP.

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

Value	Size	Description
MTU	32-bit	Specifies the maximum size of the IP datagram that can be passed through the Media Access Control (MAC). The value taken is the minimum specified by this parameter and the size indicated by the Media Access Control.

3.3. Workstation with Solaris 2.5.1 operating system

The TCP/IP protocol configuration in a Solaris 2.5.1 machine is carried out in the installation phase of the machine. If you wish to change this configuration, it is possible to do so by modifying a series of

configuration files. The basic IP parameter configuration in Solaris 2.5.1 is traditionally carried out through configuration files mainly in the directory/etc. In this section the parameters required by the ***TELDAT C* ADSL** router as a Solaris 2.5.1 gateway are described. For a more detailed description of the TCP/IP protocol configuration of Solaris, please consult in the bibliography the reference [SUN-95].

The station's IP address in the LAN is obtained from the */etc/hostname.medion* file where *medion* is usually le0 or hme0, depending on the network card used. The address in this file can appear in a numerical points or alphanumerical format. In the second case, the numerical IP address is traditionally obtained from the *etc/hosts* file. Below you can see an example of the /etc/hostname.mhe0 file.

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

Name resolution is configured through the */etc/nsswitch.conf*, */etc/resolv.conf* and */etc/netconfig*. files. An important note is that experience dictates it is very easy for an UNIX machine configured to access Internet and using DNS services to continuously carry out DNS petitions. Consequently care needs to be taken if these stations are available to prevent permanent calls to Internet being established due to DNS petitions. Logically this does not occur if the system manager knows and controls the applications or services that use DNS. Below you can see an example of the said files:

```
/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   -
```

In order to indicate the default gateway to the station, you can include the */etc/defaultrouter* file with the gateway:

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

3.4. Workstation with a Linux operating system

The TCP/IP protocol configuration in a Linux machine is carried out in the installation phase of the machine. If you wish to change this configuration, it is possible to do so by modifying a series of configuration files in a similar way to the Solaris. The affected configuration and parameters files also depend on the version of the Linux and the Linux distribution used. In this section there is an example for the Linux 2.0.32 Hat 5 distribution.

a) Configuration through files

Similarly to the Solaris, the TCP/IP protocol configuration files in Linux are found in the directory */etc*. The network adapter must be correctly installed in the system. Provided this is done, the */etc/sysconfig/network*, */etc/resolv.conf* and */etc/sysconfig/network-scripts/ifcfg-eth0* files subsequently shown, configure the TCP/IP basic parameters.

File */etc/sysconfig/network:*

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

File */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
```

File */etc/resolv.conf*:

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

b) Configuration through the network configurer

The Linux Red Hat 5 distribution network offers the possibility of using the "Network Configuration" tool from the control panel in order to configure the TCP/IP basic options.

Figure 4.10 and **Figure 4.11** display two example configuration windows through the Linux network configurer:

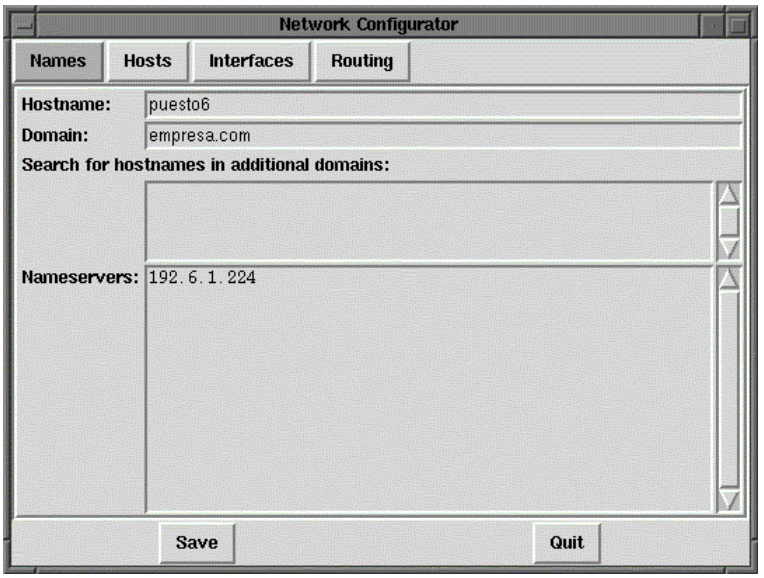

Figure 4.10: DNS parameters in Linux

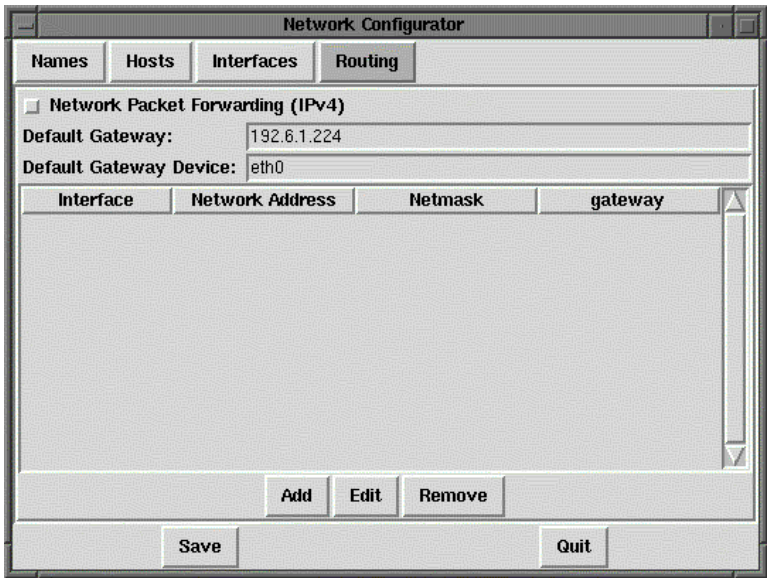

Figure 4.11: Default router in Linux

4. Configuration Examples

Imagine a scenario where you wish to provide Internet access to a private network (you must carry out NAPT) via ADSL with a PPP connection whose address must be dynamically negotiated, with the possibility of carrying out backup through an ISDN channel when IP connectivity is lost. In addition you also wish to have a visible FTP server in port 21000.

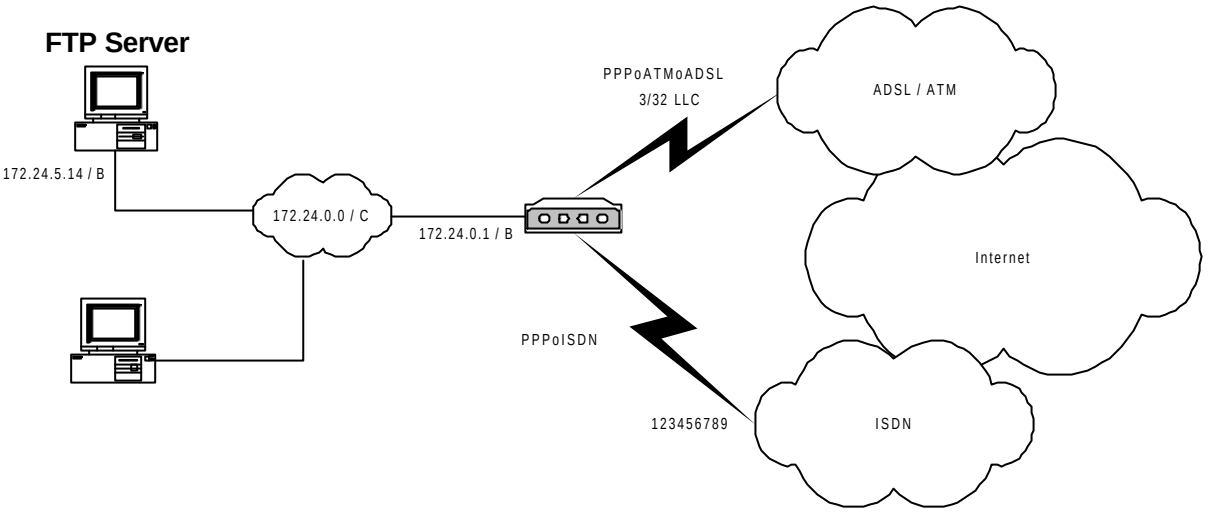

Figure 4.12:Configuration Example

1) Configuring the AAL-ATM connection

The VPI/VCI data, multiplexing type and traffic type should be provided by your ADSL access server.

```
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]?
```

2) To modify the IP connection over 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) Creating the IP connection over ATM

The user and password for your connection should be provided by you access server.

Configure NAPT with the address 0.0.0.0, which requires the device to request the address at the remote end.

```
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) Creating an IP connection over ISDN

The number to call, the user and password for your connection should be provided by your access server.

Configure NAPT with address 0.0.0.0, which requires the device to request the address at the remote end.

```
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) Adding default routes

Configure two default routes; one via the ADSL connection and the other through the ISDN connection, as the cost of an ISDN route is higher, if the packets can be routed via ADSL they will be as this is more economical. If not they will be routed through ISDN executing the pertinent call. When the PPP connection over ADSL recovers, the router will stop routing via ISDN and the call will time out due to absence of traffic.

```
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>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) Adding a visible port

```
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. Bibliography

This manual describes the quick configuration menu. If you wish to carry out a specific configuration, exhaustively monitor a protocol or carry out a function not described here, ask your usual suppliers for the manual or generic manuals on Teldat Routers.

[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 ARP and InARP Protocol"

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

[TELDAT3-00] "Dm703 Frame Relay"

[TELDAT4-00] "Dm704 Configuration and Monitoring"

[TELDAT5-00] "Dm705 Generic Serial Interfaces"

[TELDAT6-00] "Dm706 SDLC Protocol"

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

[TELDAT9-00] "Dm709 LAN Interfaces"

[TELDAT10-00] "Dm710 PPP Interface"

[TELDAT12-00] "Dm712 SNMP Agent"

[TELDAT13-00] "Dm713 X.25 over (XOT) Configuration"

[TELDAT14-00] "Dm714 OSPF Protocol"

[TELDAT15-00] "Dm715 Priority and bandwidth reservation (BRS)"

[TELDAT16-00] "Dm716 Data Link Switching"

[TELDAT17-00] "Dm717 Bridge"

[TELDAT18-00] "Dm718 RIP Protocol"

[TELDAT19-00] "Dm719 IP Tunnel Interface"

[TELDAT20-00] "Dm720 NAT Protocol"

[TELDAT21-00] "Dm721 ASTM Interface"

[TELDAT24-00] "Dm724 FTP Protocol"

[TELDAT25-00] "Dm725 TVRP Protocol"

[TELDAT30-00] "Dm730 DHCP Protocol"

6. Glossary

Below you will find a brief glossary containing the terms used in relations to this device.

10Base-T - 10 megabits per second Baseband Twisted par. This refers to the electric interface used to transmit and receive in an Ethernet connection.

ADSL - Asymmetric Digital Subscriber Line. This is the high speed transmission technology used by the subscribers loop (telephone line between the user and the central) and can reach up to 8 Mbps downstream and 1 Mbps upstream. The ADSL connection can share the subscribers' loop with voice telephony.

ATM - Asynchronous Transfer Mode is the high speed data, video and voice transmission technology based on information fragmentation in blocks of a fixed length known as cells. These cells can be quickly processed through hardware switches reducing the transit delay through the network.

BRIDGE - A bridge exchanges data packets between two or more LANs using the same communication protocol based on the hardware address (MAC).

CO - Central Office. The telephone operator central office is where all the subscriber loops from a zone are collected. In cases where there is ADSL installation, this occurs in a DSLAM.

CONSOLE - This is a device which can be a PC and serves to locally configure the device.

DHCP - Dynamic Host Configuration Protocol. This protocol automatically assigns the IP addresses to a LAN element known as DHCP client. Thanks to this we can avoid manual configuration for each device.

DMT - Discrete Multitone. This is the modulation type recommended by UIT for ADSL. It consists of using 256 QAM modulators/demodulators.

DNS - Domain Name Server. This is a server that collects an Internet address based on text and converts this into a numerical IP address permitting it to connect to another website.

DSLAM - Digital Subscriber Line Access Multiplexer. This is a device located at the exchange which receives and concentrates the ADSL connections for many subscribers on a high speed ATM line.

DOWNSTREAM - This is the data traffic transmitted in the central-subscriber direction.

ENCAPSULATION - This refers to the sum of one or more headers used for communication protocols within a data packet.

ETHERNET - This is the physical and data connection permitting the connection of devices in a LAN.

FILTER - This is a configuration element permitting traffic discrimination according to the source IP address, the destination, protocol or port according the programmed criteria.

IP address – This is the IP datagram field used to identify the network interface. It is a 32 bit number written in four fields decimal, octets, separated by points. E.g. 192.6.1.228.

LAN - Local Area Network. This is a high speed data network located in a small geographical area (hundreds of meters). The LANs connect workstations, computers, peripheral and other devices situated within the small area or building.

MAC - Media Access Control. This is the layer 2 address needed for each port and device connected to a LAN. It is 6 bytes in length and also known as the hardware or physical address.

NAT - Network Address Translation.

PAT - Port Address Translation.

PING - Packet INternet Grouper. This is an Internet command or program which is used to determine if the IP address can be accessed.

PPP - Point-to-Point Protocol. This is a protocol permitting the interconnection of two routers or host and the network with synchronous or asynchronous lines.

PVC - Permanent Virtual Circuit. This is locally characterized through the pair (VPI/VCI).

RFC 1483 - RFC 1483 SubNetwork Access Protocol (SNAP) is a method to encapsulate multiprotocol data in ATM networks.

RIP - Routing Information Protocol.

ROUTER - A router is a network device which passes packets from one network to another following a criteria based on IP addresses.

SNMP - Simple Network Management Protocol. This is a device management protocol through normal Internet.

SUBNETMASK – This is an address mask of 32 bits which determines the number of addresses in a subnet.

SUBNET – A subnet is a network arbitrarily segmented by a network administrator in order to provide a multilevel structure.

TCP/IP - Transmission Control Protocol/Internet Protocol is a set of protocols developed in the 1970s and constitutes the Internet base.

TELNET - TELNET is a terminal standard emulation based on the TCP/IP protocols. This permits users to remotely access the device's command interface.

UPSTREAM - This is the data traffic transmitted in the subscriber-central direction.

VPI/VCI - The VPI (Virtual Path Identifier) is an 8 bits field in the ATM cell header). Combined with the VCI (Virtual Channel Identifier, 16-bits field in the ATM cell header), this is used to identify the next destination of a cell passing through an ATM switch.

VPN - Virtual Private Network. This permits IP traffic to travel safely through a TCP/IP network.

WAN - Wide Area Network. This network, unlike the LAN, covers an extensive geographical area.

WRR- Wan ReRoute. Backup that is based in activating one route or another depending on whether the main interface is **UP** or **DOWN**.