

SERIAL TO IP ENCAPSULATION TYPE CIC



USER GUIDE

V03 - June 2018

M0CIC1806IV03

ZIV
Antonio Machado, 78-80
08840 Viladecans, Barcelona-Spain
Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: ziv@zivautomation.com
www.zivautomation.com

SAFETY SYMBOLS



WARNING OR CAUTION:

This symbol denotes a hazard. Not following the indicated procedure, operation or alike could mean total or partial breakdown of the equipment or even injury to the personnel handling it.



NOTE:

Information or important aspects to take into account in a procedure, operation or alike.

CONTENTS

	Page
1 INTRODUCTION	5
1.1 GENERAL	5
1.2 PORT INTERCONNECTION	7
1.3 AVAILABLE MODELS	10
1.4 TECHNICAL SPECIFICATIONS	11
1.4.1 Equipment interfaces	11
1.4.2 Encapsulation protocols	11
1.4.3 Equipment management	12
1.4.4 Additional services	12
1.4.5 Accessories	12
1.4.6 Certifications	12
1.4.7 Asynchronous serial data ports (DCE) characteristics	13
1.4.8 Optical fiber transducers characteristics	13
1.4.9 Optional WAN interface characteristics	14
1.4.10 Mechanical characteristics	14
1.4.11 Operating conditions	14
2 MECHANICAL AND ELECTRICAL CHARACTERISTICS	15
3 LED SIGNALLING	22
4 ACCESS TO THE EQUIPMENT	25
4.1 CONSOLE	25
4.2 HTTP SERVER	26
5 CONFIGURATION AND MANAGEMENT	28
5.1 GENERAL PARAMETERS	29
5.1.1 Equipment identification	30
5.1.2 Access control	30
5.1.3 Others	31

	Page
5.2 ADMINISTRATION	31
5.3 LAN CONFIGURATION	31
5.4 SERIAL PORTS CONFIGURATION	32
5.5 WAN CONFIGURATION	35
5.6 STATIC ROUTES CONFIGURATION	42
5.7 FILTERING CONFIGURATION	44
5.8 DHCP SERVER CONFIGURATION	46
5.9 SNMP CONFIGURATION	48
5.10 NTP CONFIGURATION	50
5.11 ACCESS CONFIGURATION	51
5.12 DATA FLOW CONFIGURATION	52
5.12.1 Encapsulation protocols	53
5.12.2 Connection	60
5.12.3 Policy	63
5.12.4 Other	65
5.13 CONFIGURATION OF THE SERIAL PORT AS <i>ModemEmulator</i>	66
5.14 REBOOT	69
5.15 CODE REFLASH	69
6 STATISTICS	71
APPENDIX A	
BIBLIOGRAPHY AND ABBREVIATIONS	76
APPENDIX B	
DATA STRUCTURE IN CLI	81

1 INTRODUCTION

1.1 GENERAL

The CIC is a serial to IP encapsulator with a larger number of access ports than the serial to IP encapsulator type SIP.

The CIC has two possible configurations as far as the number of serial ports is concerned; a basic serial port with RS-232/RS-485 interface, and four or eight additional RS-232 serial ports. The basic port always operates with a 9-pin SUB-D connector, while the additional serial ports are offered either with 9-pin SUB-D connectors or optical fiber transducers, in groups of four.

The CIC has two Ethernet interfaces that work as a part of a two-port Ethernet switch, 10/100Base-Tx or 100Base-Fx.

The equipment also allows traffic to be routed, working as a level 3 router.

All serial ports are configured as **DCE** (Data Communications Equipment).

Optionally, the CIC may be equipped with a WAN GPRS or UMTS network device.

FIGURE 1

Serial to IP encapsulation on wired interface

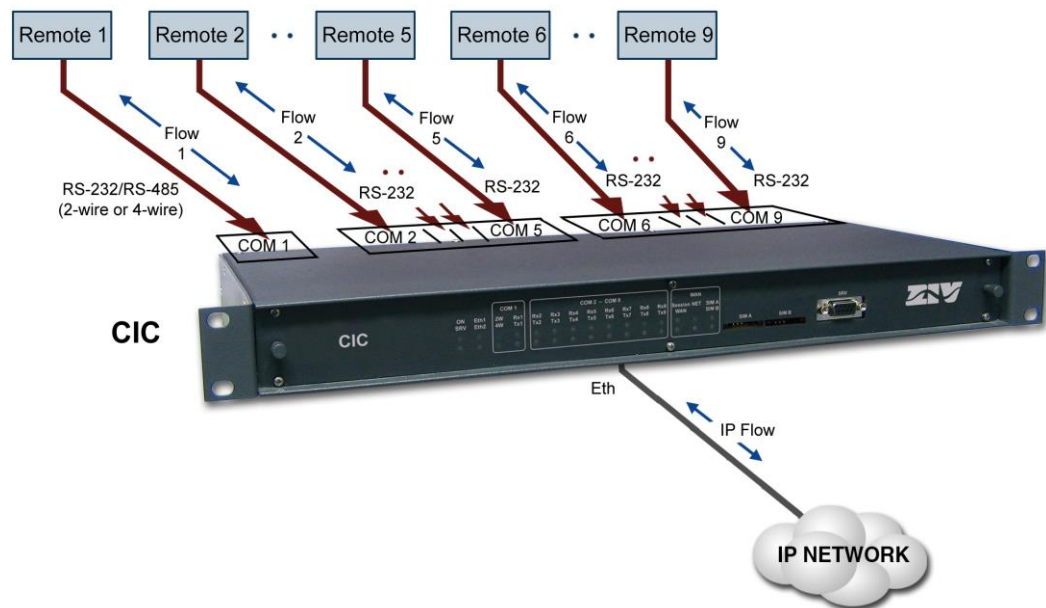


FIGURE 2

CIC application example

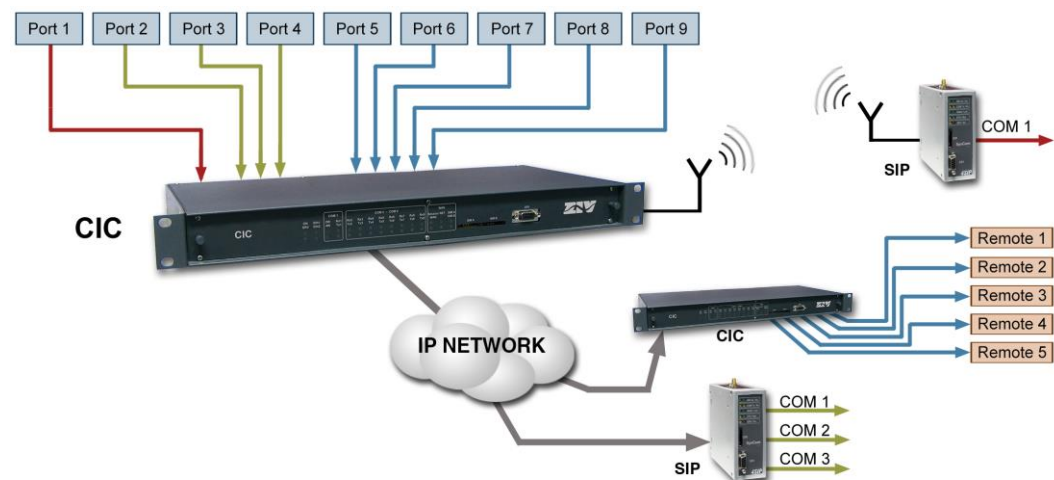
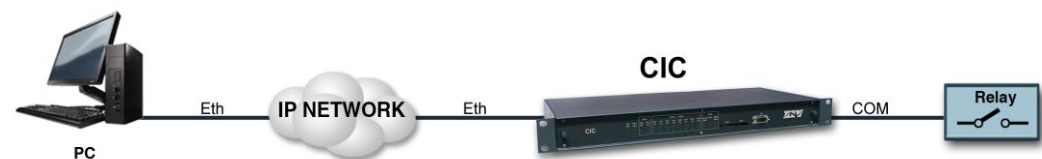


FIGURE 3

Serial to IP encapsulation application example



The CIC can be managed locally and remotely, through a local console, Telnet server and SSH server, or through a built-in web server, HTTP.

The CIC also supports the SNMPv1 and SNMPv2c protocols, as well as other protocols and services such as DHCP, NTP and TACACS+.

The basic encapsulation function is the creation of a point-to-point connection, equivalent to a direct connection between two serial devices, even when the actual data transfer is done on a TCP/IP network.

The encapsulation function guarantees delivery of the data accepted in one of the serial ports of an end, free of errors, and with unaltered order at the other end of the connection. This function is usually called PAD (Packet Assembler-Disassembler).

The encapsulation function does not depend on the user data content. The equipment admits two processing modes with the PAD function: direct or with packets.

Even though the encapsulator basic function is the execution of the PAD processes, the CIC equipment has the necessary procedures to perform an intelligent encapsulation so as to process the data as higher level transmission units for a series of specific protocols of Telemetry and Telecontrol. Thus, the operations on the data are not limited to their mere transmission, but possible errors are identified, or the CIC is capable of identifying different data flows in a unique shared channel and of transferring them towards differentiated destinations (demultiplexing).

Some of the supported protocols are IEC 60870-5-101/102/103, DLMS, GESTEL, DNP3.0, PROCOME, SAP20, MODBUS, Pid1, Twc, etc.

Another additional characteristic for any of the encapsulator operations modes is the CIC capability to offer the basic HAYES modem behaviour towards the client equipment, so that the encapsulator point-to-point connections are made upon demand and with the determined receiver by application or the client equipment. The operation in HAYES mode is enabled separately for each one of the serial ports present in the CIC.

1.2 PORT INTERCONNECTION

In addition to the serial ports -which are called **physical ports**-, the equipment operates with resources that are TCP/UDP connections, which are used to encapsulate data on the TCP/IP networks; these TCP/UDP connections are called **virtual ports**, as opposed to the tangible ports.

The equipment basic operation is the determination of the port characteristics, both physical as well as virtual, and then establishes the “connections” between them; which in practice sets the ends where the transfer of encapsulated data is done.

On the other hand, if the equipment has an optional WAN interface, there will be an additional virtual port related to the GSM data call, in order to establish a connection between said virtual port and a serial port.

Next, for a better understanding when approaching the CIC configuration by accessing the equipment HTML pages, there is a description of the main operations that should be performed for **the interconnection between physical ports (COM) and virtual ports (TCP/UDP)**. It is advisable to perform the indicated operations in the order that they appear.

See chapter 5 for more detailed information about the configuration menus and their parameters.

1. Configure the serial port parameters. For this, access the **Serial** menu (see section 5.4 for more information).

El **Serial** menu has two well differentiated sections: **Physical** and **Logical**.

In the **Physical** section, configure the basic operation parameters of the COM ports (speed, data bits, parity and stop bits).

In the **Logical** section, configure either the encapsulation protocol or the use of an encapsulation policy (*policy-based* option), and an identifier for it. The policy configuration itself is done from the **Policy** submenu from the **Flow** menu.

The identification of each COM port, that is, the name, is done in the **Physical Ports** section of the **Flow** menu configuration screen.

2. Create and configure the parameters of the TCP/UDP virtual ports. For this, access the **Flow** menu configuration screen (see section 5.12 for more detailed information).

The **Flow** menu configuration screen has two well differentiated sections. **Physical Ports** and **Virtual Ports**.

Establish a different and unequivocal name for each COM port in the **Physical Ports** section.

All the ports have the name *serial0* configured by default and, therefore, it is essential to assign a specific name to each of them.

On the other hand, if the equipment has a WAN interface, the *Use autocli* box should be OFF, that is, not ticked, in the *Datacall* parameter so that the data call-serial connection (GSM) is effective.

Define the configuration of the virtual ports in the **Virtual Ports** section. For this, take into account the following:

- The **TCP** connections may have two behaviours, active and passive. Active means that the equipment will take the initiative as regards establishing the TCP connection. On the contrary, passive means that the equipment will await for external connection requests. The behaviours are complementary between them.
- The **UDP** connections do not need any prior establishment procedure; it is just assumed that the receiver is configured to accept data in the indicated port. The UDP connections do not offer end-to-end confirmation, or any guarantee as long as the delivery sequence is the original one.
- It is usual to configure ports with values above 1000 since there are pre-established ports for the use of general services in TCP/IP networks; thus, possible collisions are avoided.

- The virtual ports may also have an assigned encapsulation protocol or policy, although, as a general rule, just one encapsulation protocol or policy is assigned to a sole end of each connection, understanding that it already includes a physical and a virtual port as well. Thus, **it is usual to assign the encapsulation protocol to the physical port and leave the virtual port without a protocol, that is, with the raw protocol option (default option).**

! The inactivity time is the maximum period of time desired to maintain the connection in the case of a lack of data, either in transmission or reception. This parameter is configured at 0 by default, that is, the activity is not monitored at the data level, which implies that the connection will be permanent regardless of its activity. The parameter units are seconds.

- The active TCP connections have an **On Demand** parameter. Said parameter indicates if the establishment should start just because the connection is configured, or just when the equipment has encapsulated data to be transmitted.

! The **On Demand** parameter is configured by default to establish the communication start permanently. If the *On Demand* option is activated, the duration of the connection will be established by the inactivity parameter, which limits the connection to the activity periods.

3. Establish the connections between the ports through their identifiers. For this, access the **Connection** submenu (see section 5.12.2 for more information) from the **Flow** menu.



For an effective connection it is essential to correctly enter the name of the identifiers established in the **Physical Ports** and **Virtual Ports** sections of the **Flow** menu configuration screen. In order to avoid possible errors, it is advisable to use the commands *Ctrl.+C* (copy) and *Ctrl.+V* (paste) instead of the keyboard.

Second, for connection to be operative, the *CheckBox* for the *Enable* parameter should be active, that is, ticked.

1.3 AVAILABLE MODELS

The CIC includes, as standard features, a **serial maintenance interface**, **two Ethernet interfaces** type 10/100Base-Tx (with RJ-45 connector) or 100Base-Fx multimode (with MT-RJ connector), and **1 asynchronous serial port** configurable by software with V.24/V.28 electrical interface or RS-485 interface (2 or 4 wires).

The equipment may be completed with **four** or **eight additional RS-232 serial ports**, with 9-pin SUB-D connectors and/or optical fiber transducers.

Optionally, it may be equipped with **1 wireless WAN interface** (GPRS/UMTS/HSDPA) which, in turn, can be equipped with **one or two slots for SIM cards**.

There are two versions for the power supply:

- Multirange (85-360 Vdc, 60-260 Vac).
- Isolated DC (20-75 Vdc).

As regards its installation, the CIC is made up of a 19" shelf that is 1 standard unit (s.u.) in height, prepared for rack mounting.

1.4 TECHNICAL SPECIFICATIONS

1.4.1 Equipment interfaces

- 2 ports with Fast Ethernet interfaces type 10/100Base-Tx with RJ-45 connector or type 100Base-Fx multimode (1300 nm) with MT-RJ connector.
- 1 asynchronous serial port (COM1), configurable by software for RS-232 interface or RS-485 interface (2-wire or 4-wire).
- Optional Block 1: 4 asynchronous serial ports (COM2 to COM5), configurable by software for RS-232 interface, all of them with 9-pin SUB-D connectors or optical fiber transducers (plastic or glass).
- Optional Block 2: 4 asynchronous serial ports (COM6 to COM9), configurable by software for RS-232 interface, all of them with 9-pin SUB-D connectors or optical fiber transducers (plastic or glass).
- 1 service console.
- Optionally, 1 wireless WAN interface (GPRS/UMTS/HSDPA), with one or two slots for Mini Sim (2FF) cards.

See for more electrical details chapter 2, *Mechanical and electrical characteristics*.

1.4.2 Encapsulation protocols

- IEC 60870-5-101/102/103 (the first two with the variants to support link addresses of 1 or 2 bytes).
- DLMS.
- GESTEL.
- MODBUS.
- DNP 3.0.
- SAP20.
- PROCOME.
- Pid1.
- Twc.

1.4.3 Equipment management

- Local and remote access, through a local console, Telnet server and SSH server, or through a built-in web server, HTTP.

1.4.4 Additional services

- SNMP agent (SNMPv1 and SNMPv2c).
- DHCP server and client.
- NTP server and client.
- IPSec or SSL/TLS client (according to configuration).
- TACACS+ client.

1.4.5 Accessories

- Ethernet cables.
- Serial cables.
- Optical fiber pigtails.
- Antenna cables.
- Antennas.

1.4.6 Certifications

- CE.
- Designed for Electrical Substations.
- Designed for industrial applications.

1.4.7 Asynchronous serial data ports (DCE) characteristics

- Data bits: 5, 6, 7 or 8.
- Stop bits: 1 or 2.
- Parity: odd, even or none.
- Speed: 600 bit/s to 115200 bit/s.
- Flow control: none, hardware or software.
- Interface: V.24/V.28 of the ITU-T (EIA RS-232C) and RS-485 (2-wire or 4-wire) for COM 1.

See for COM connector use details chapter 2, *Mechanical and electrical characteristics*.

1.4.8 Optical fiber transducers characteristics

- Glass fiber.
 - Type of connector: ST
 - Wavelength: 820 nm
 - Transmission rate: 5 MBd
 - Type of fiber: 50/125 µm, 62.5/125 µm, 100/140 µm and 200 µm
 - Typical maximum distance: 2 km with 62.5/125 µm fiber
 - Type of emitter: LED
- Plastic fiber.
 - Type of connector: Versatile Link
 - Wavelength: 660 nm
 - Transmission rate: 40 kBd
 - Type of fiber: POF (Plastic Optical Fiber) with a diameter of 1mm
 - Typical maximum distance: 120 m
 - Type of emitter: LED

See for connector details chapter 2, *Mechanical and electrical characteristics*.

1.4.9 Optional WAN interface characteristics

- Quad band: 850/900/1800/1900MHz.
 - Class 4 (+33dBm \pm 2dB) for EGSM850
 - Class 4 (+33dBm \pm 2dB) for EGSM900
 - Class 1 (+30dBm \pm 2dB) for GSM1800
 - Class 1 (+30dBm \pm 2dB) for GSM1900
- UMTS/HSDPA: Dual band, 900/2100MHz.
- GSM/GPRS: Dual band, 900/1800MHz.
 - Class 4 (+33dBm \pm 2dB) for EGSM900
 - Class 1 (+30dBm \pm 2dB) for GSM1800
 - Class E2 (+27dBm \pm 3dB) for GSM 900 8-PSK
 - Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK
 - Class 3 (+24dBm +1/-3dB) for UMTS 2100, WCDMA FDD BdI
 - Class 3 (+24dBm +1/-3dB) for UMTS 900,WCDMA FDD BdVIII

1.4.10 Mechanical characteristics

- A shelf that is 19" wide and 1 s.u. high, which is prepared for rack mounting.
Height: 45 mm; Width: 484 mm; Depth: 213 mm (with connector).
- Weight: 2 kg

See for more mechanical details chapter 2, *Mechanical and electrical characteristics*.

1.4.11 Operating conditions

- Power supply: 20-75 Vdc (isolated) or multirange (85-360 Vdc, 60-260 Vac).
- Temperature and humidity: from -20°C to +70°C and relative humidity not greater than 95%, in accordance with IEC 721-3-3 class 3K5 (climatogram 3K5).
- Maximum power consumption: 20 W.
- Electrical safety: in accordance with EN 60950 standard.
- R.F. emissions: in accordance with EN 55022 standard.
- Immunity to electrostatics discharges: In accordance with UNE-EN 61000-4-2 standard.
- Immunity to R.F. permanent electromagnetic fields: In accordance with UNE-EN 61000-4-3 standard.

2 MECHANICAL AND ELECTRICAL CHARACTERISTICS

The diverse elements comprising the CIC are supplied in a shelf that is 19" wide and one standard unit (s.u.) high, which is prepared for rack mounting.

FIGURE 4 shows the general dimensions of the shelf in mm, as well as the position of the fastening holes.

FIGURE 4 General dimensions in mm of the CIC shelf

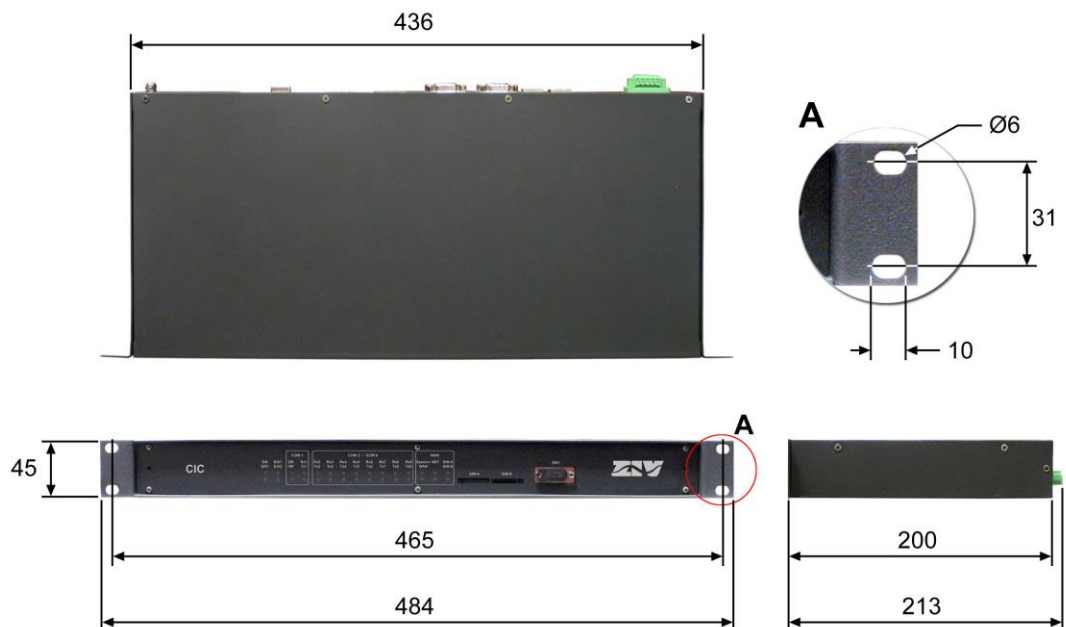


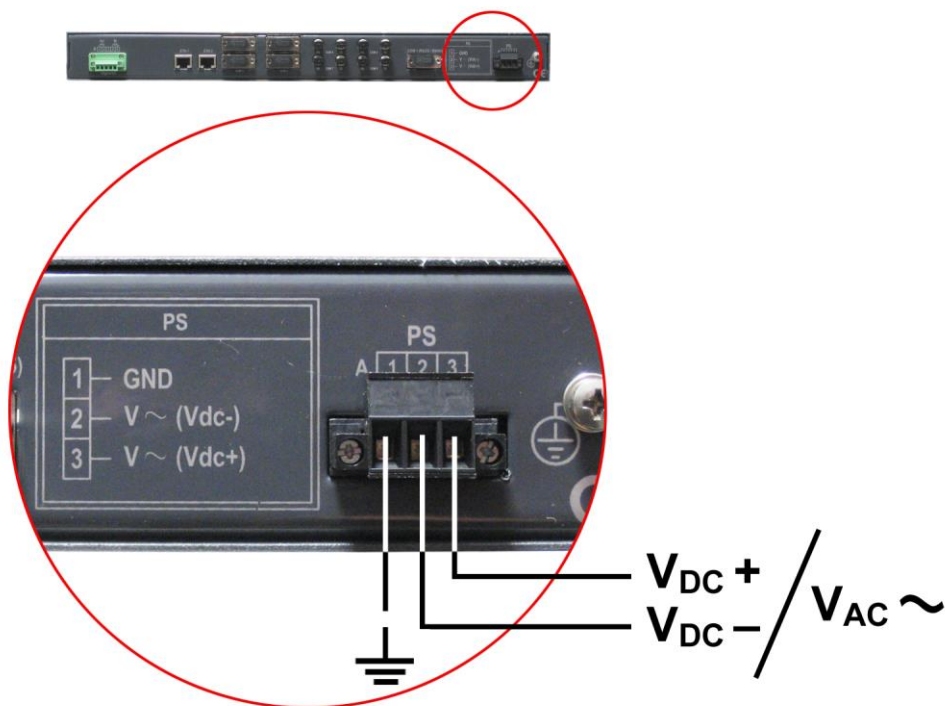
FIGURE 5 shows the rear view of the CIC shelf equipped with 8 additional ports, the first four have a 9-pin SUB-D connector and the other four are for optical fiber connectors.

FIGURE 5 Rear view of the CIC shelf with 8 additional ports (SUB-D and glass optical fiber)



The CIC is powered with a nominal voltage of 48 V_{DC} (isolated) or allows DC and AC supply-voltage operation (85-360 Vdc, 60-260 Vac), through the connector shown in FIGURE 6.

FIGURE 6 Location of the power-supply connector in the CIC shelf



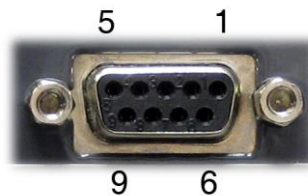
Next to the power-supply connector, see FIGURE 7, there is the asynchronous serial port (COM1), configurable by software for RS-232 interface or RS-485 (2-wire or 4-wire) interface.

FIGURE 7

Location of the COM1 connector in the CIC shelf



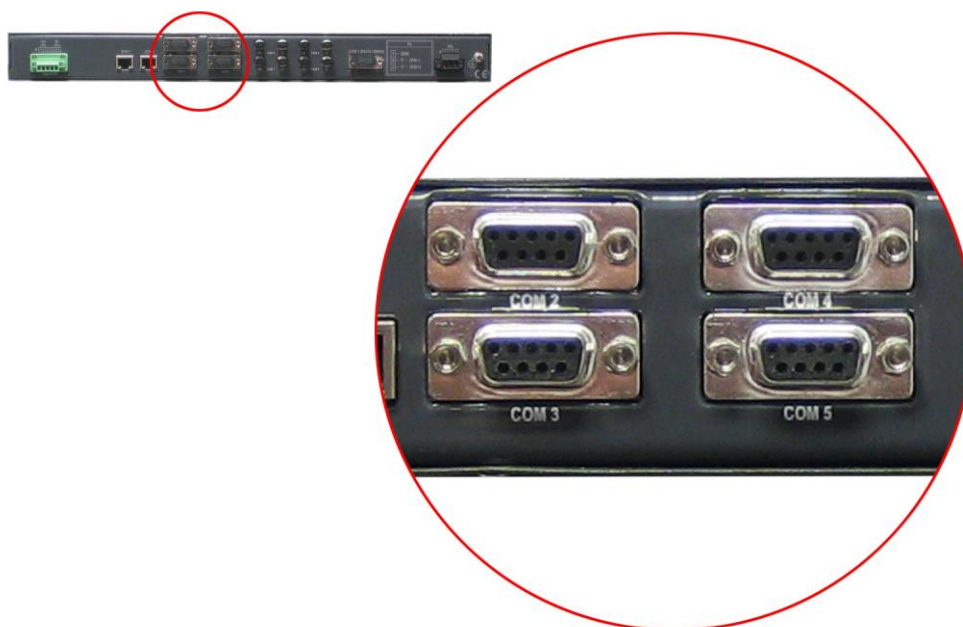
The electrical characteristics of the connector are configured by software among the ones indicated in the technical characteristics; see section 1.4.7, *Asynchronous serial data ports (DCE) characteristics*. Its use is indicated below. The connector has a protective cap.



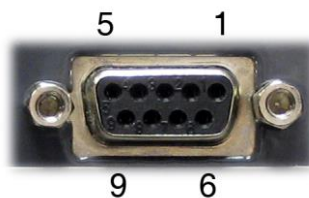
Pin	RS-232	RS-485 (4-wire)	RS-485 (2-wire)
1	DCD		
2	RD		
3	TD		
4	DTR		
5	GND		
6	DSR	RX-	
7	RTS	RX+	
8	CTS	TX-	TX/RX-
9	RI	TX+	TX/RX+

FIGURE 8 shows the location of the four additional connectors for RS-232 interface (COM2 to COM5) with 9-pin SUB-D connector.

FIGURE 8 Location example of the additional RS-232 connectors (SUB-D) in the CIC shelf



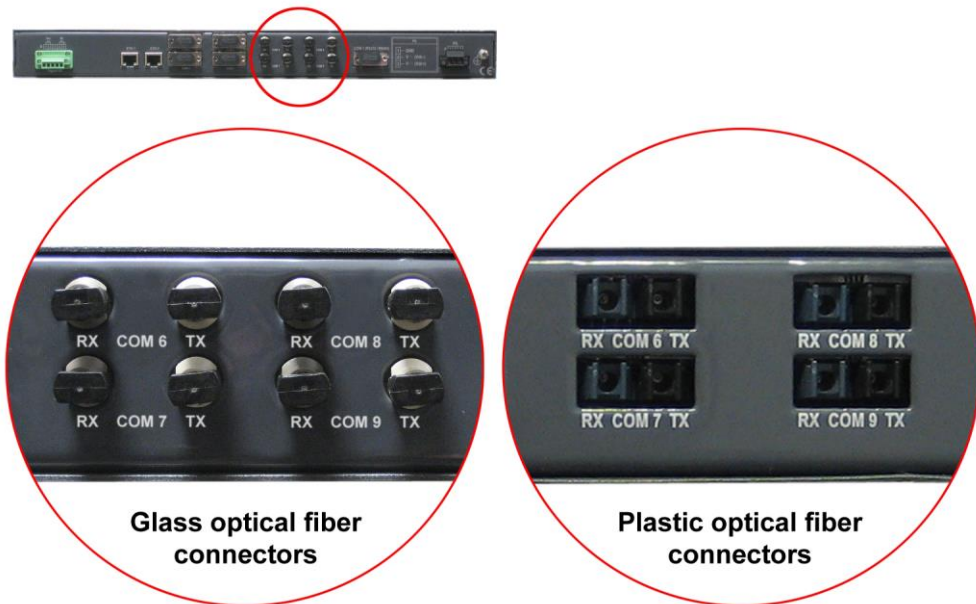
Each connector has a protective cap. Connector use is indicated below.



Pin	RS-232
1	DCD
2	RD
3	TD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

FIGURE 9 shows the location of the four additional connectors for plastic or glass optical fiber (COM6 to COM9). The characteristics of the connectors are indicated in the technical characteristics; see section 1.4.8, *Optical fiber transducers characteristics*.

FIGURE 9 Location example of additional connectors (COM) in the CIC shelf



As regards the network interface, it may have 10/100Base-Tx Fast Ethernet interfaces with RJ-45 connectors, as it can be seen in FIGURE 10, or 100Base-Fx multimode (1300 nm) interfaces with MT-RJ type optic connector.

FIGURE 10 Location of Ethernet ports in the CIC shelf

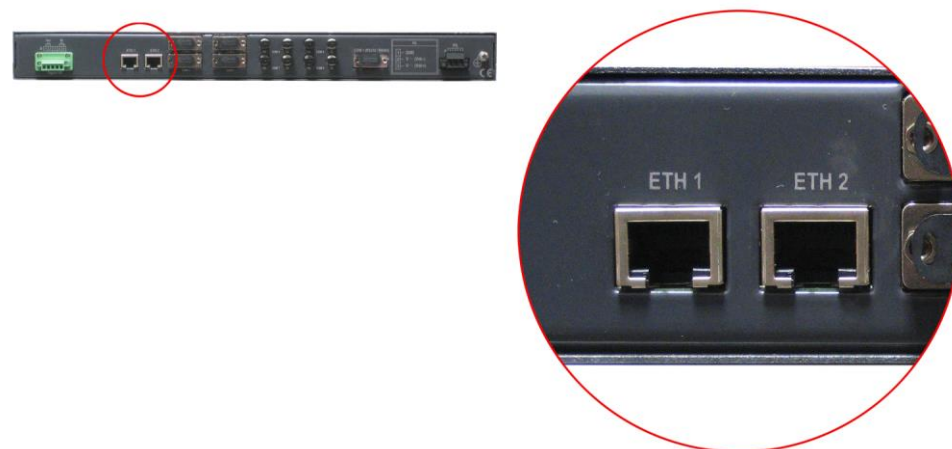
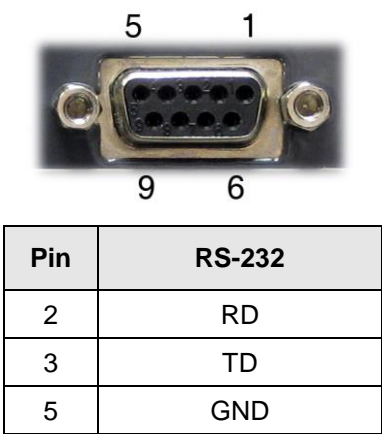


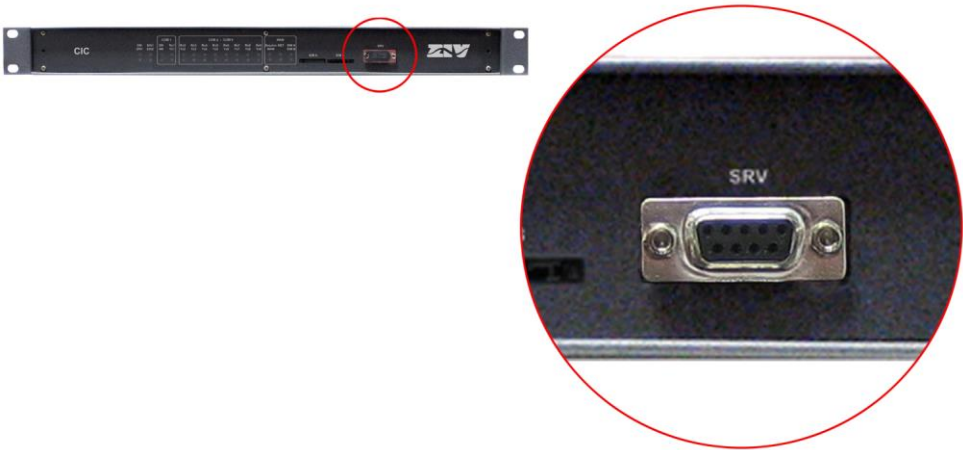
FIGURE 11 shows that there is a maintenance connector, identified as SRV, on the front plate of the shelf, for accessing the equipment through a console. The electrical characteristics of the connector and its use are indicated below. The connector has a protective cap.



Pin	RS-232
2	RD
3	TD
5	GND

	SRV CONNECTOR
Interface type	ITU-T V.24/V.28 (EIA RS-232)
Connector	DB9 female
Data	Asynchronous
Speed	115200 bit/s
Protocol	CLI (system console)

FIGURE 11 Location of the maintenance connector on the front plate of the CIC shelf



Optionally, the CIC may be equipped with a WAN GPRS or UMTS network device. In this case, next to the Ethernet connectors, there is a SMA female connector for GSM/GPRS antenna and, on the front plate, there is two slots for housing Mini Sim (2FF) cards.

Both SIMs **CANNOT** be activated simultaneously. It is used a *dual SIM* operation, that is to say, one SIM acting as the primary one and the other as the secondary or back-up one.

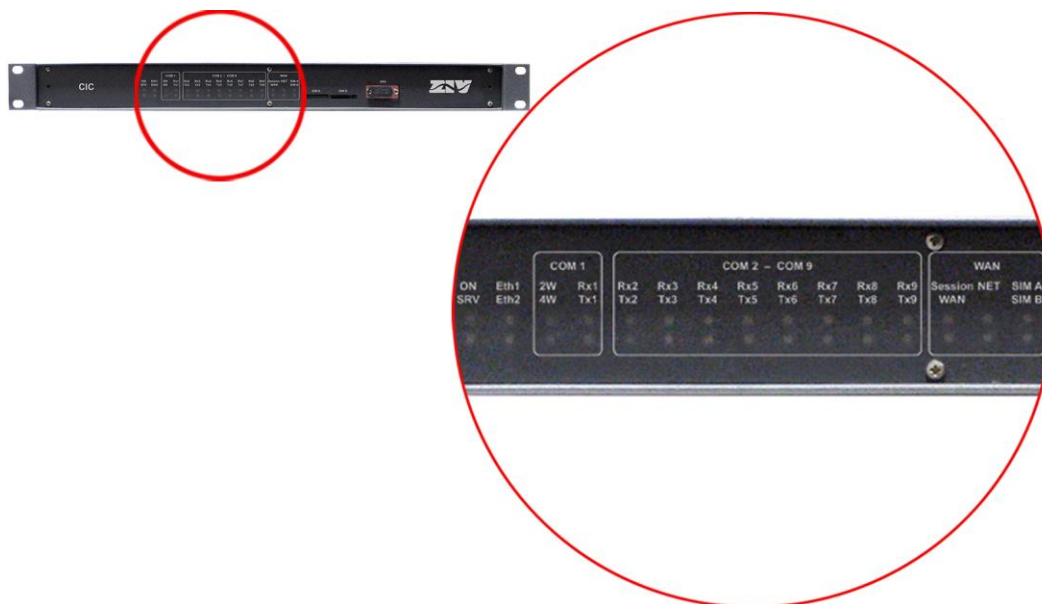
3 LED SIGNALLING

The CIC has on the front plate two basic LEDs (ON and SRV), two LEDs related to the Ethernet ports (Eth1 and Eth2), four LEDs related to the COM1 basic port, up to sixteen LEDs related to the eight additional ports (COM2 to COM9), two per port, and several LEDs associated with the optional WAN interface.

FIGURE 12 Front view of the CIC shelf



FIGURE 13 Front view detail of the LEDs related to the interfaces



The function of the different LEDs is described below.

On LED	Red. It is permanently lit when the equipment is powered with an external power-supply voltage.
SRV LED	Amber. It flashes when there is emission or reception activity by the SRV serial service interface.
Eth1 LED	Amber. It flashes in the case of emission or reception activity in the LAN interface.
Eth2 LED	Amber. It flashes in the case of emission or reception activity in the LAN interface.
2w (COM1) LED	Green. It is permanently lit when the COM 1 port is configured with a 2-wire RS-485 interface.
4w (COM1) LED	Green. It is permanently lit when the COM 1 port is configured with a 4-wire RS-485 interface.
Rx1 (COM 1) LED	Amber. It flashes in the case of data reception in the COM1 port.
Tx1 (COM 1) LED	Amber. It flashes in the case of data transmission in the COM1 port.
RxX (COM X) LED	Amber. It flashes in the case of data reception in the COM X port (<i>X being: 2 to 9</i>).
TxX (COM X) LED	Amber. It flashes in the case of data transmission in the COM X port (<i>X being: 2 to 9</i>).

LED WAN	Green. It lights up permanently when the session with the operator has been established for the wireless interface.
LED NET	Green. It flashes when the wireless interface has been registered in the operator network.
LED SIM X	<p>Green. It lights up permanently indicating that SIM X is in use.</p> <p>Both SIMs CANNOT be activated simultaneously. It is used a <i>dual SIM</i> operation, that is to say, one SIM acting as the primary one and the other as the secondary or back-up one.</p>

4 ACCESS TO THE EQUIPMENT

The CIC can be managed locally and remotely, through a console or through a built-in web server. The server operates with the HTTP protocol.

4.1 CONSOLE

The equipment provides a user console application called *CLI* (see *Appendix B*), accessible through the SRV connector, a standard DB9 female connector in DCE mode that operates at 115200 bit/s, with 8-bit characters, without parity and with a stop bit.

The system makes a distinction between upper and lower case characters.

Depending on the user identity, the user console provides full access to all the equipment configuration data.

The console has a small help section about the available commands that is obtained by executing the **help** command.

The data are grouped virtually into directories and subdirectories. To browse through the directories the **cd (change directory)** command is used. The value of an individual data item or a group of data is obtained in response to a **get** command, indicating the specific data item or giving the value of all the data located in the current directories and subdirectories. To establish a new value, it is necessary to execute the **set** command, indicating the parameter to be changed and then the desired value; if the value to be configured is not provided, the system will explicitly request it.

The data stored in tabulate form, identified by the inclusion in the variable name of the symbol [], have specific commands for adding and removing rows, which are **add** and **remove** respectively. To query or establish the value of the data in one row, the row identifier must be included between square brackets in the **get** or **set** command.

Changes made with the **set** command are not operative merely because they have been executed. Effective, immediate use of the changes made is achieved by executing the **Apply** command. On the contrary, the **Save** command entails storing the changes made permanently, without requiring their immediate use, but applied in the case of an initialisation.

In this way, the changes are implemented as an operating procedure through the **Apply** command, and after checking that the behaviour is correct, it is saved using the **Save** command. Consequently in the case of obtaining undesirable results, it is always possible to eliminate the **Save** command and reboot the equipment to recover the previous status, even in the case that the changed activated lead to the user not being able to obtain access.

Access can also be obtained to the console remotely through SSH connection and Telnet.

4.2 HTTP SERVER

The HTTP server included provides access to the HTML pages giving access to all the configuration data.

The procedures for the effective configuration of the parameters are identical, that is to say, it is necessary to execute the **Apply** command and/or the **Save** command, as indicated in the section on using the console, but before executing these commands, the system must be informed that the data have been changed through the **Send** command (the button is present in all the HTML pages).

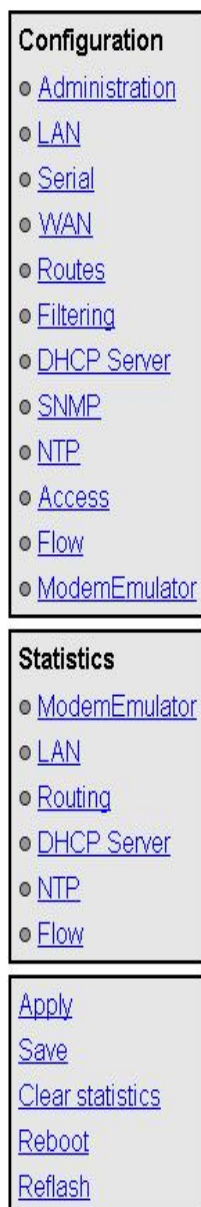
The **Apply** and **Save** commands are at the bottom of the tree menu and are only visible when the user profile has administration rights. The commands indicated are shown on FIGURE 14.

For information about the **Reboot** and **Reflash** commands see sections 5.15 and 5.16, respectively.

The **Apply**, **Save** and **Reboot** commands request confirmation of the operation from the user before it is actually executed.

FIGURE 14

HTML page tree menu



In the HTML pages the commands for adding and removing elements from the tabulate data are explicitly shown as buttons labelled *Add* and *Delete*, located on each of the objects that use them.

The factory IP address of the equipment is 192.168.0.1, meaning it is possible to access the HTTP server to configure it from the very start (see chapter 5).

It should be borne in mind that if the IP address is changed, the IP address of the client equipment must also be changed accordingly.

5 CONFIGURATION AND MANAGEMENT

Configuration and management of the CIC is performed through the console and through access to the equipment HTML pages.

All the parameters controlling the equipment operation are described below in detail, using the real HTML pages, as shown in the auxiliary graph.

Whenever changes are made, regardless of whether they are made through the console or the HTTP server, the equipment must be informed what is to be done with them.

There are two options:

- the first is to execute the **Apply** command, which entails the immediate use of the changes made.
- the second is to execute the **Save** command, which means that the changes will be operative once the equipment is rebooted.

If accessing through the HTTP server, after making the changes and before executing **Apply** or **Save**, the **Send** button must be pushed to allow the equipment to obtain the new desired values.

If executing the **Apply** command, if the changes are required to be permanent, the **Save** command must also be executed.

The only exceptions are changes affecting the SNMP configuration. Changes made to the SNMP agent configuration will **only** be active after **RESETTING** the equipment. The **Apply** command is not sufficient, and so the changes must previously be saved using the **Save** command before requesting the re-initialisation.

5.1

GENERAL PARAMETERS

The general parameters are grouped on the first page, see FIGURE 15, which is shown when the CIC validates the user identity.

In addition to the configuration parameters, which will be described in the following sections, as shown in the figure, the system provides information about the equipment software, that is to say, version being executed, and equipment hardware, that is to say, serial and tracking number.

The tree menu is permanently located on all the pages used by the HTTP server.

FIGURE 15 Main HTML page

The screenshot displays a web interface with three main sections: Identification, Access Control, and Others. Each section contains various input fields and controls.

Identification	
Hostname	<input type="text" value="CIC"/>
Location	<input type="text" value="unknown"/>
Contact	<input type="text" value="unknown"/>
Product	4CIC02031001000A
Firmware version	3.21.6.6.18257
Firmware reference	4WF7130026
Tracking #	d65215000000
Serial #	1234567

Access Control	
Guest's login	<input type="text" value="guest"/>
Guest's password	Change
Admin's login	<input type="text" value="admin"/>
Admin's password	Change

Others	
Time zone	<input type="text" value="UTC"/> ▼
Serial Log	<input type="checkbox"/>
Enable Periodic Reset	<input type="checkbox"/>
Periodic reset period (days)	<input type="text" value="1"/>

5.1.1 Equipment identification

The identification zone has three parameters; the equipment name (**hostname**), its location (**location**) and the contact data of the responsible person or company (**contact**). At least one string of text is required, with at least one character.

The **hostname** is used automatically as a prompt value on the console.

The identification parameters coincide with those assigned with the same name in the SNMP data.

5.1.2 Access control

Access control allows the user logins and associated passwords to be determined for the two pre-established profiles: guest and admin.

The guest profile can only access query operations. On the contrary, the admin. profile has access to all the system configuration data.

As summarised in TABLE 1, the default values of these parameters are **guest** and **admin** as the logins, with **passwd01** and **passwd02** being the respective passwords.

It should be borne in mind that the system makes a distinction between upper and lower case characters.

TABLE 1

System default access codes

	Login	Password
Guest profile	guest	passwd01
Admin. profile	admin	passwd02

It is highly recommended to change at least the password of the admin. profile when executing the first configuration in each equipment.

It is advisable to store the new password in some type of register as, should the new password be forgotten, it is not possible to access the web server.

5.1.3 Others

This section deals with four parameters. The first of them establishes the hour zone in relation to UTC.

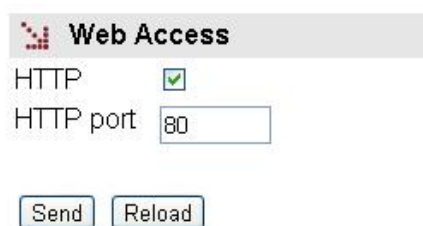
The second parameter, **Serial log**, indicates whether the log data transmission on the service serial port is activated from the initial start-up time (*Checkbox* control selected) or not.

The third parameter, **Enable periodic reset**, allows users to indicate whether they want to reboot the equipment automatically every so often. This is established in days through the last parameter, **Periodic reset period**.

5.2 ADMINISTRATION

The equipment has an integrated HTTP server for management purposes.

FIGURE 16 **Administration** configuration screen



Web Access

HTTP ☒

HTTP port

5.3 LAN CONFIGURATION

The **LAN** menu has the configuration data for the network connection.

The screen related to the **eth0** submenu has two well differentiated sections, which are described below.

FIGURE 17 Configuration screen associated with the **eth0** submenu

LAN

Static IP ☐

IP Address

Mask

MAC address 00:E0:AB:01:80:FF

IP Alias

# IP Address	Mask
1	0.0.0.0 255.255.255.0 <input type="button" value="Undo"/>
2	<input type="button" value="Add"/>

LAN:

The main IP address and its mask may be obtained automatically through the DHCP client, which is called dynamic or NON-static configuration.

The user can activate the static configuration through the *CheckBox* type control with the **Static IP** label. When the control is ticked, the equipment uses the data provided by the user.

IP Alias:

The equipment is capable of responding to IP addresses different from the main one if they have been previously added through the **Add CommandButton**.


5.4 SERIAL PORTS CONFIGURATION

The **Serial** menu provides access to the equipment serial port (COM) configuration screen.

The basic equipment has 1 asynchronous serial port, COM 1, configurable by software for RS-232 interface or RS-485 (2-wire or 4-wire) interface. In addition, the equipment may be completed with four (COM2 to COM5) or eight (COM6 to COM9) additional RS-232 serial ports with 9-pin SUB-D connector and/or optical fiber transducers.


The screen related to the **Serial** menu has two well differentiated sections, which are described below. See section 1.2 for more general information about the port interconnection.

FIGURE 18 **Serial ports (COM) configuration screen**

 **Physical**

#	Interface ¹	Baudrate	Databits	Parity	Stopbits	Flow control
1	rs485-4w	9600	8	odd	1	none
2	rs232	9600	8	even	1	none
3	rs232	9600	8	odd	1	none
4	rs232	9600	8	odd	1	none
5	rs232	9600	8	none	1	none
6	rs232	9600	8	none	1	none
7	rs232	9600	8	none	1	none
8	rs232	9600	8	none	1	none
9	rs232	9600	8	none	1	none

¹ Just first port can be configured in 485 modes

 **Logical**

#	Mode	Protocol	Policy	Packed time (ms)	Packed size
1	flow	pid1		50	262
2	flow	iec101		50	262
3	flow	pid1		50	262
4	flow	pid1		50	262
5	flow	raw		10	16
6	flow	raw		10	16
7	flow	raw		10	16
8	flow	raw		10	16
9	flow	raw		10	16

Physical:

- **#.** It establishes the equipment physical port number. Port 1 for port COM1, Ports 2 to 5 for block COM2 to COM5, and Ports 6 to 9 for block COM6 to COM9.
- **Interface.** It establishes the type of the interface. RS-232 by default. Port 1 is the only one that also admits the RS-485 interface with 2-wire or 4-wire.
- **Baudrate.** It establishes the serial port speed. The available values are the following: 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200 bit/s.

- **Databits.** It establishes the character length. The available values are the following: 5, 6, 7 and 8.
- **Parity.** It establishes the parity. The available values are the following: odd, even or none.
- **Stopbits.** It establishes the number of stop bits. The available values are the following: 1 and 2.
- **Flow control.** It establishes the flow control mechanism. The available values are the following: none, hardware (control signals) and software (Xon and Xoff).

Logical:

- **#.** It establishes the equipment physical port number. Port 1 for port COM1, Ports 2 to 5 for block COM2 to COM5, and Ports 6 to 9 for block COM6 to COM9.
- **Mode.** It establishes the port operation mode: **flow** or **emulator**. **Flow**, that is, serial port mode. The **emulator** mode implies the activation of the HAYES modem emulator additional characteristic, and it should only be selected to define a *ModemEmulator* behaviour for the port, which is similar to a HAYES modem. In this last case, there are additional options in the *ModemEmulator* menu.
- **Protocol.** It establishes the protocol of the data to be encapsulated; the possible values are the following: **raw** (without processing, it is transparent to the information), **packed**, (the data will be grouped in packets according to the related parameters, being also transparent as regards the encapsulated information), one of the identifiers of the **telecontrol protocols being hold** (iec101_1, iec101, iec102_1, iec102, pid1, dlms, gestel, sap20, twc, dnp3, procome, iec103, modbusrtu, modbusrtu_cc) or the policy-based mode (**policybased**).
- **Policy.** This field should be configured when the **policybased** mode has been established in the *Protocol* parameter. It establishes an identifier, whose policy should be configured in the *Policy* submenu of the *Flow* menu.
- **Packed time (ms).** This field should be configured when the **packed** mode has been established in the *Protocol* parameter. It establishes the maximum waiting time after receiving the last character, in ms, before sending a packet with the data received so far. It forces sending the data for inactivity time when not reaching the data established as desired packet size (see following parameter).
- **Packed size.** This field should be configured when the **packed** mode has been established in the *Protocol* parameter. It establishes the maximum number of characters to be transmitted in a packet on the network.

This menu only appears when the CIC equipment has the optional wireless WAN interface (GPRS/UMTS/HSDPA).

FIGURE 19 WAN interface configuration screen

WAN

Enable Wireless WAN

☐

Primary SIM

alternated ▾

Request DNS

☒

Maximum number of retries

6

Maximum time to connect (min)

6

Low Coverage Level Alarm

-105

Low Coverage Alarm Period

300

Max time in secondary(min)

0

Enable dual SIM

☐

Enable inactivity time for datacalls

☒

Inactivity time for datacalls (s)

2:00.000000000

SIM A

PIN1 value

[Change](#)

PIN2 value

[Change](#)

APN

Force Home Network

☐

Authentication method

pap ▾

User

Password

[Change](#)

Minimum Signal (dBm)

-113

SIM B

PIN1 value

[Change](#)

PIN2 value

[Change](#)

APN

Force Home Network

☐

Authentication method

pap ▾

User

Password

[Change](#)

Minimum Signal (dBm)

-113

Dynamic DNS

Enable Dyn Service

☐

Dyn Service Id

dyndns ▾

Dyn Service Login

Dyn Service Password

Host name1

Time Interval (s)

86400

1 Example: support.usyscom.com

Ping Keep Alive

Remote IP1

0.0.0.0

Remote IP2

0.0.0.0

Frequency (min)

5

Size of ICMP Packets (+28)

1

Number of ICMP Packets

2

Action

none ▾

Strict

☒

Send

Reload

The menu has four different sections, which are described below.

WAN:

- **Enable Wireless WAN.** This allows the WAN interface of the equipment to be enabled and disabled by selecting ON and OFF, respectively.

Selecting the **ON** option will make the equipment try a new GPRS/UMTS/HSDPA session, in accordance with the subscriber data (PIN, APN, Authentication method, user, password). In the case of **dual SIM** functionality, the subscriber data will be those corresponding to the primary SIM.

The **OFF** option disables the WAN interface, and is the default option. Consequently, you should enable this option if you want the GPRS/UMTS service, after FIRST configuring the necessary parameters for establishing the operator session.

- **Primary SIM.** In the case of **dual SIM** functionality, this permits users to determine which of the two available SIMs will act as the primary one: SIMA or SIMB. In this operating mode the SIM that is not selected is therefore the secondary or back-up SIM.
- **Request DNS.** Tick this box and the equipment will request the addresses for DNS servers to the operator when the connection with it is available.
- **Maximum number of retries.** This gives the number of retries (3 to 10) that can be made to try and establish the operator session. If the number of retries is used up, the equipment will be rebooted.

In the case of **dual SIM** functionality, the number of retries is for each of the SIMs. In this way, once the number of retries with the primary SIM has been used up, the equipment will try to establish connection using the secondary SIM. If it is not possible to connect with the secondary SIM, once the number of retries has been used up, or if the secondary SIM is disabled, the equipment will be rebooted.
- **Maximum time to connect (minutes).** This specifies the time in minutes (3 to 20) for the equipment to wait in order to obtain the WAN IP address from the operator. If after that time, a WAN IP has not been obtained, the equipment will be rebooted. In the case of **dual SIM** functionality, it must be taken into account that the **Maximum time to connect** counter starts operation at the same time that the **Maximum number of retries** counter. In this way, the equipment will be rebooted when one of the two counters reaches at zero, that is to say, when it is not possible to connect once the number of retries of both SIMs has been used up (see Maximum number of retries counter) or once the time configured in the Maximum time to connect counter has been used up.

- **Low Coverage Level Alarm.** It specifies the coverage level under which the low coverage level alarm should be activated.
- **Low Coverage Alarm Period.** It specifies the time the coverage level should remain below the level indicated in the previous paragraph before the low coverage alarm is activated.
- **Max time in secondary (minutes).** This parameter is associated with the **dual SIM** functionality. It allows the time during which the equipment is connected to the secondary SIM to be limited. After that time, the equipment will again try to connect to the primary SIM. The maximum time permitted is 1440 minutes.
- **Enable dual SIM.** This box must be ticked to determine whether the equipment will use the secondary SIM or not.
- **Enable inactivity time for datacalls.** Selecting this box determines if the equipment will use the following parameter.
- **Inactivity time for datacalls (s).** It establishes the inactivity time in seconds that will imply the voluntary and controlled shutdown of the GSM datacall connection.

SIM:

- **PIN 1 and PIN 2 values.** These are the safety codes associated with the SIM card. Normally, PIN1 is sufficient to access the general services provided by the operator. Check that the code entered is correct. Entering a wrong code will block the SIM card.

Once the **PIN 1** and **PIN 2** values are introduced from the **Change** option, execute the **send** command of said option, and then, if you want the values to be applied and saved in the equipment, **DO NOT forget** to execute the **apply** and **save** commands from the main menu tree.

- **Preferred network. Only for the UMTS interface.** This allows the equipment behaviour to be specified in the case of a failure in UMTS/HSDPA coverage. When **UMTS** is selected, the equipment will always try to connect to a UMTS/HSDPA network. This option therefore involves the disconnection of the equipment, due to the lack of UMTS/HSDPA reception. If **UMTS/GPRS** is selected, the equipment will try to connect to a UMTS/HSDPA network, but if there is no UMTS/HSDPA coverage it will connect to a GPRS network. With this option, the equipment will permanently monitor the UMTS/HSDPA network coverage, and as soon as the

UMTS network becomes available again, it will switch from a GPRS network to a UMTS/HSDPA network.

- **APN.** This establishes the identity of the operator access point.
- **Force Home Network.** On ticking this box connection with the operator of the local network associated with the SIM card is forced (home network). If this option is selected, the equipment will not connect to any operator other than the one specified.
- **Authentication method.** The authentication method to be used when establishing the PPP session must be selected. The possible values are None, PAP and CHAP.
- **User Name.** User name established by the operator during the authentication process (see preceding point).
- **Password.** Password established by the operator to validate the user name in the preceding point. The password is not shown for security reasons and so when it is changed (**Change** option), it must be entered twice.

Once the **Password** is introduced from the **Change** option, execute the **send** command of said option, and then, if you want the password to be applied and saved in the equipment, **DO NOT forget** to execute the **apply** and **save** commands from the main menu tree.

- **Minimum Signal (dBm).** This parameter allows a minimum coverage level to be specified (in dBm) as a quality parameter for WAN connection. When the coverage level is below this value the equipment will not try to establish the operator session and will remain disconnected. The default values are -113 dBm (0%, no coverage) and -51 dBm (100%, coverage).

TABLE 2 relates the AT command for coverage measurement (AT+CSQ), the value in dBm of said coverage, and the level of coverage the equipment is receiving, which is shown in the coverage bar on the upper strip of any of the pages on the user interface.

TABLE 2

AT command for coverage measurement (AT+CSQ)

AT+CSQ	Coverage (GPRS)	Coverage (3G)	Received power	Number of bars on screen
0	0%	0%	<-113 dBm	-
1	0%	0%	-111 dBm	-
2	1%	1%	-109 dBm	-
3	1%	3%	-107 dBm	-
4	2%	4%	-105 dBm	-
5	2%	6%	-103 dBm	-
6	3%	7%	-101 dBm	-
7	3%	8%	-99 dBm	-
8	4%	11%	-97 dBm	-
9	5%	14%	-95 dBm	-
10	6%	15%	-93 dBm	1
11	11%	21%	-91 dBm	2
12	17%	29%	-89 dBm	2
13	23%	35%	-87 dBm	3
14	29%	43%	-85 dBm	3
15	35%	49%	-83 dBm	4
16	41%	57%	-81 dBm	5
17	47%	66%	-79 dBm	5
18	53%	74%	-77 dBm	6
19	59%	85%	-75 dBm	6
20	65%	99%	-73 dBm	7
21	71%	100%	-71 dBm	8
22	77%	100%	-69 dBm	8
23	83%	100%	-67 dBm	9
24	90%	100%	-65 dBm	10
25	92%	100%	-63 dBm	10
26	94%	100%	-61 dBm	10
27	96%	100%	-59 dBm	10
28	97%	100%	-57 dBm	10
29	98%	100%	-55 dBm	10
30	99%	100%	-53 dBm	10
31	100%	100%	>-51 dBm	10
>31	0%		Unknown	-

Dynamic DNS:

A dynamic DNS service permits the assigning of a DNS name to equipment with a non-permanent IP address, and the Dynamic DNS client is responsible for updating it when it changes. In this way, from the user standpoint the equipment is always accessible via a DNS name, and so it is not necessary to always know the IP address assigned.

The Dynamic DNS client is entrusted with connecting to the chosen server and updating the IP address.

To use the Dynamic DNS client, users must first register the DNS name of the equipment with the service provider. The client can only update the IP address.

The parameters are as follows:

- **Enable Dyn Service.** Enables the Dynamic DNS client execution.
- **Dyn Service Id.** Allows you to select one of the dynamic DNS service providers supported.
- **Login and Password.** Establishes the user name (login) and password (password) for accessing the service provider.
- **Host name.** Name of the equipment registered with the service provider, i.e., the name of the equipment used to identify the CIC via DNS.
- **Time interval (seconds).** Time between accesses for the Dynamic DNS client to update the IP address.

Ping Keep Alive:

This is a facility for checking the status of the WAN interface.


- **Remote IP1 and Remote IP2.** This establishes the IP addresses of the equipment with which accessibility will be checked, through the sending of ICMP (ping) packets. If the fields are at 0.0.0.0 this means the "Ping Test" function is disabled. It is sufficient for any one of the remote equipment to respond to consider the accessibility test valid. A field with the value 0.0.0.0 means that the option is not enabled.
- **Frequency (minutes).** This allows the time passing between the sending of ICMP (ping) packets to be specified.

- **Size of ICMP packets.** This allows the size of the ICMP packet to be specified. The configuration consists of indicating the extra bytes to be added to the smallest ICMP packet, which is, by default, 28 bytes.
- **Number of ICMP packets.** This allows the number of ICMP packets that are sent in each verification to be specified.
- **Action.** This establishes the desired behaviour of the equipment if the accessibility test is failed. The options are: **None** (no action taken), **Reconnect** (set up a new GPRS/UMTS session) or **Reboot** (reboot the equipment).
- **Strict.** This option allows users to inhibit the accessibility test in the presence of traffic. If the option is not activated, the test will only be executed when the period of time indicated in **frequency** without traffic has passed. When the option is enabled, the test will be performed regardless of whether traffic is present or not.

In the figure given as an example in the Ping Keep Alive configuration, connectivity of the IP addresses 192.168.1.5 and 192.168.1.10 is verified every **15** minutes by sending **2** ICMP packets of 29 bytes (28+1). If there is no response to the "Ping Test", the equipment will be rebooted.

To prevent "Ping Test" failures occurring due to the simultaneous reception of traffic, the equipment will check the activity through the WAN interface for 30 seconds prior to executing the "Ping Test". If the reception of traffic is detected, the "Ping Test" function will not be executed.

FIGURE 20 Example of the **Ping Keep Alive** configuration

 **Ping Keep Alive**

Remote IP1	<input type="text" value="192.168.1.5"/>
Remote IP2	<input type="text" value="192.168.1.10"/>
Frequency (min)	<input type="text" value="15"/>
Size of ICMP Packets (+28)	<input type="text" value="1"/>
Number of ICMP Packets	<input type="text" value="2"/>
Action	<input type="text" value="reboot"/> ▼
Strict	<input checked="" type="checkbox"/>

STATIC ROUTES CONFIGURATION

The **Routes** menu provides access to the configuration screen through which the user can provide the system with the static and permanent data for the routing service.

The screen related to the *Routes* menu has two well differentiated sections. Explicit static routes are configured in the *Static Routes* section. The address acting as a route by default in the case that the service has no specific data for reaching a destination is configured in the *Default Static Routes* section.

If the equipment has the optional wireless interface, the operator will not only provide the IP address of the interface but also establish a default router associated with that interface, which takes precedence over any configuration established by the user.

FIGURE 21 Static routes configuration screen

Static Routes

#	Destination	Gateway	Service	Dest I/F	Description
1	0.0.0.0/255.255.255.0	0.0.0.0	any	eth0	

2

Default Static Routes

#	Gateway	Dest I/F	Metric	Description
1	10.250.8.1	eth0	1	

2

The parameters for configuring a static route are:

- **Destination.** This allows the IP address to be specified, and the remote or destination network subnet mask. The field requires the values to be entered in the IP address format. Example: 192.168.0.0/255.255.255.0 or 192.168.0.0/24.
- **Gateway.** This allows the IP address of the router to which the traffic destined for the remote network of the previous field must be sent.
- **Service.** This allows an additional filter to be established in the remote IP address for determining the selection of the next jump. The condition is established based on a specific service (tcp/udp/icmp). After the service the port number (1-65535) must be indicated, separated by two points. The default value is **any**, that is to say, the route applies for all types of traffic (only the IP destination is taken into account). Example:

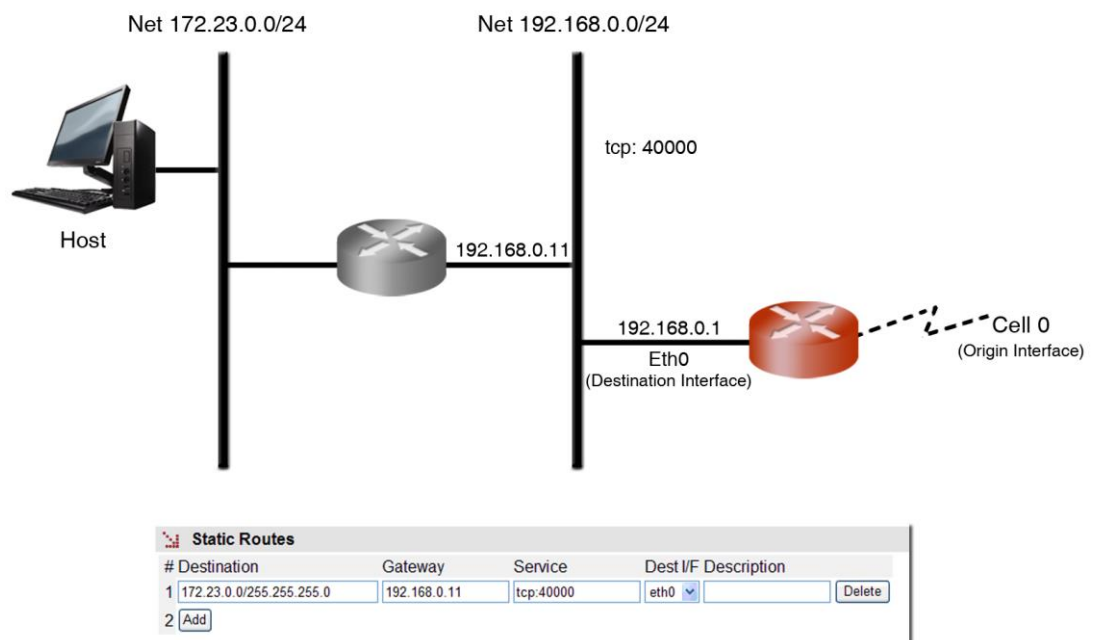
tcp:5000, which means that all the packets with tcp traffic on port 5000 will be sent to the indicated router.

- **Dest I/F (Destination interface).** This allows the interface through which the routed traffic coinciding with this route will be sent.
- **Description.** This permits a description of up to 15 alphanumeric characters to be specified.

Example:

The figure shows an example of assigning a static route between two different network segments. All the TCP packets of port 40000 can reach the network segment 172.23.0.0/24 through router 192.168.0.11.

FIGURE 22 Example of how a static route is configured



The default parameters for configuring a static route are:

- **Gateway.** This allows the IP address of the next router to be specified for routing traffic whose destination does not coincide with any known route.
- **Dest I/F (Destination interface).** This permits the specification of the interface through which traffic routed to the router indicated in the previous field will be sent.

- **Metric.** This permits a value to be established originating from among the default different routes that could be created. A higher metric means a lower priority.
- **Description.** This permits a description of up to 15 alphanumerical characters to be specified.

5.7 FILTERING CONFIGURATION

The *Filtering* menu permits firewall functionalities, defining which traffic is allowed and which traffic is rejected and the application of additional conditions to the traffic processed through the routing function.

The menu parameters are divided into three quite different blocks, which are:

- Filtering of packets for local services (http, Telnet or **any**)
- Filtering of packets through the incoming/outgoing service for the GPRS/UMTS (cell0) interface, if the equipment has the optional WAN interface.
- Filtering of packets through the incoming/outgoing service for the Ethernet (eth0) interface.

FIGURE 23 *Filtering menu* configuration screen

Packet Filtering for Local Services

#	Origin	Service	Policy	Description	Enable
1	any	any	drop		<input checked="" type="checkbox"/>
2	Add				

Default Policy: [accept](#)

Forwarding Packet Filtering in cell0 interface

#	Origin	Destination	Service	Dir.	Policy	Description	Enable
1	any	any	any	in	drop		<input checked="" type="checkbox"/>
2	Add						

Default Policy: [accept](#)

Forwarding Packet Filtering in eth0 interface

#	Origin	Destination	Service	Dir.	Policy	Description	Enable
1	any	any	any	in	drop		<input checked="" type="checkbox"/>
2	Add						

Default Policy: [accept](#)

[Send](#) [Reload](#)

The configuration parameters in each block are:

- **Origin.** This allows the IP source of the traffic to be specified, i.e., from a specific IP address or any IP address (**any**). The default value is **any**. The specification of a particular IP address requires the values to be entered in the IP address format. Example: Subnet (192.168.50.0/255.255.255.0 or 192.168.50.0/24) or Host (192.168.50.5/255.255.255.255 or 192.168.50.5/32 or 192.168.50.5). Only present in the sections in which this makes sense.
- **Destination.** This allows the IP source of the traffic to be specified, i.e., to a specific IP address or from any IP address (**any**). The default value is **any**. The specification of a particular IP address requires the values to be entered in the IP address format. Example: Subnet (192.168.50.0/255.255.255.0 or 192.168.50.0/24) or Host (192.168.50.5/255.255.255.255 or 192.168.50.5/32 or 192.168.50.5).
- **Service.** This allows any type of traffic to be specified (**any**) or a specific traffic (**tcp/udp/icmp**). The default value is **any**. If a specific traffic is indicated, the port number can be indicated together with the service, if required (1÷65535) or a range. Example: tcp or tcp:23 or udp:5001-5005.
- **Dir.** This allows the traffic direction to be specified, i.e., whether it is incoming (**in**) or outgoing (**out**).
- **Policy.** This allows the filtering policy to be specified (**accept**, **drop** or **reject**). When the filtering policy is **accept**, only packets complying with the established rule are accepted. When the filtering policy is **drop**, on the other hand, packets complying with the established rule are dropped. The **reject** filtering policy also rules out packets complying with the established rule, but unlike drop, when the packet is ruled out, the appropriate ICMP message is sent to the source address of the packet.
- **Description.** This permits a description of up to 15 alphanumerical characters to be specified.
- **Default Policy.** This allows the behaviour of the equipment filtering to be determined as regards not being included in any specific rule of the respective section.

Example:

A filtering policy is to be established to eliminate traffic present in the ethernet (eth0) interface coming from host 10.0.0.5, whose destination is within the IP range 192.168.0.0/24. The **eth0** block configuration will be that shown in the figure.

FIGURE 24 Example of filtering configuration

Packet Filtering for Local Services

Origin Service Policy Description Enable

1

Default Policy

Forwarding Packet Filtering in cell0 interface

Origin Destination Service Dir. Policy Description Enable

1

Default Policy

Forwarding Packet Filtering in eth0 interface

#	Origin	Destination	Service	Dir.	Policy	Description	Enable
1	10.0.0.5	192.168.0.0/24	any	in	drop		<input checked="" type="checkbox"/>

2

Default Policy

5.8 DHCP SERVER CONFIGURATION

The CIC has a built-in DHCP server which allows IP addresses to be assigned automatically to the equipment requesting this.

This service is available for the **eth0** interface (ETH1 physical) only.

The configuration parameters are:

- **Enable DHCP server.** This allows the DHCP service to be activated. Users should indicate whether they want to use a DHCP server.

! This parameter is activated by default.

FIGURE 25 **DHCP server** configuration screen

DHCP Server	
Enable DHCP Server	<input type="checkbox"/>
First IP Addr	192.168.0.10
Last IP Addr	192.168.0.254
Maximum number of leases	100
Mask	255.255.255.0
Default gateway	192.168.0.1
Lease Time	5000
1st DNS Server	0.0.0.0
2nd DNS Server	0.0.0.0
WINS Server	0.0.0.0
DNS Domain Name	usyscom.com
Boot TFTP Server	192.168.0.1
Bootfile Name	bootfile

- **First IP Addr.** Allows the **first** IP address of the IP addresses pool managed by the DHCP Server to be specified.
- **Last IP Addr.** Allows the **last** IP address of the IP addresses pool managed by the DHCP Server to be specified.
- **Maximum number of leases.** Allows the maximum number of IP addresses simultaneously assigned in use to be specified.
- **Mask.** This establishes the net mask that will communicate with the DHCP clients.
- **Default Gateway.** This establishes the default router address (Default Gateway) that will communicate with the DHCP clients.
- **Lease time.** This allows the time in seconds to be specified for an IP address to be assigned following a request from a DHCP client. After the indicated time, if the DHCP has not requested a renewal, the IP address will be considered available for dealing with new requests.
- **1st DNS server.** This allows the specification of the primary DNS server IP address which the DHCP server will provide to the DHCP client. If left blank (0.0.0.0) no information on DNS servers will be sent to the client.

- **2nd DNS server.** This allows the IP address of a secondary DNS server to be specified to the DHCP client. If left blank (0.0.0.0) this means that no information will be sent to the client in this respect.
- **WINS server.** This allows the IP address of the WINS server to be established, which will be notified to the DHCP client. WINS is a names resolution system owned by Microsoft for equipment executing the Windows operating system.
- **DNS Domain Name.** This establishes the DNS domain to be used by the client for creating its full DNS name.
- **Boot TFTP Server.** This establishes the IP address of the TFTP server that stores the remote boot file, thereby allowing the client to execute a request to download the file.
- **Bootfile Name.** This establishes the name of the remote boot file which the client will request from the TFTP server configured in the preceding point.

5.9 SNMP CONFIGURATION

The equipment has an SNMP agent with the capacity to generate spontaneous messages to control equipment, based on that protocol.

The agent admits the emitting of messages based on the SNMPv1 [1] and SNMPv2c [2] protocol, and the selection of the type of message, *trap* and *inform*.

Changes made to the SNMP agent configuration will **only** be active after **RESETTING** the equipment. The **Apply** command is not sufficient, and so the changes must previously be saved using the **Save** command before requesting the reboot.

The configuration parameters are:

- **Enable:** Enables/disables the execution of the SNMP agent. The agent is operative when the option is selected.
- **Community:** Tabulate information that allows several operating profiles to be defined, including the rights of access associated with each one, read only rights (*ro*) or reading/writing rights (*rw*). The profiles are called *communities*.

- **Enable Traps:** Enables/disables the generation and transmission of spontaneous messages by the SNMP agent. The agent will send messages when the option is selected.
- **Traps:** Tabulate information allowing several destination equipment for the *traps* to be defined.
- **Trap v1 agent address:** This establishes the IP address the agent will communicate as being its own when sending spontaneous messages. This parameter is only used to create the traps when using SNMPv1.

For each of the spontaneous SNMP message addressees, a profile must be provided, which must be included in the spontaneous message, the SNMP protocol version with which it will be coded, the IP address of the addressee and the UDP port to which the messages will be sent. The default value established in the standard is port 162. It can be changed to adapt to the operating data of each addressee.

FIGURE 26 **SNMP menu** configuration screen

SNMP

Enable ☒

Community

#	Name	Access
1	public	ro
2	Add	

SNMP Traps

Enable Traps ☒

Traps

#	Community	Type	IP	Port	
1	public	v1	172.17.201.88	162	Delete
2	Add				

Trap v1 agent address: none

Enable Wan Linkup Trap ☐

Enable Wan Low Coverage Trap ☐

Enable Wan High Coverage Trap ☐

[Send](#) [Reload](#)

5.10 NTP CONFIGURATION

The equipment has an NTP client, meaning that it can synchronise time-related information by accessing NTP servers. The NTP [3] protocol is a standard that is widely used in TCP/IP-based networks. It admits the use of several NTP servers simultaneously, and the option of using authentication.

FIGURE 27 *NTP menu* configuration screen

The screenshot shows the NTP configuration interface. It is divided into two main sections: 'NTP' and 'NTP client'.

NTP Section:

- Enable:** A checkbox that is currently unchecked.
- Authentication Keys:** A table with columns '# Key Number' and 'Key'.

# Key Number	Key
1	1 [XXXXXXXXXX] [Delete]
2	[Add]

NTP client Section:

- Server:** A table with columns: '# IP', 'Type', 'minpoll', 'maxpoll', 'Authentication Enable', 'Authentication Key', and 'Low traffic'.

#	IP	Type	minpoll	maxpoll	Authentication Enable	Authentication Key	Low traffic
1	192.168.0.1	unicast	5	10	<input type="checkbox"/>	1	<input type="checkbox"/>
2	[Add]						
- Accept Broadcast:** A checkbox that is currently unchecked.
- Buttons:** 'Send' and 'Reload' buttons are located at the bottom of the NTP client section.

The usage parameters are:

- **Enable:** Enables/disables the execution of the NTP client. The client is operative when the option is selected.
- **Authentication keys:** Tabulate information allowing the definition of different authentication codes to be used subsequently in communicating with the different NTP servers.
- **Server:** Tabulate data that includes the NTP servers access data. Each row contains data related to one NTP server.
- **Accept broadcast:** This establishes whether the NTP client will accept messages transmitted with broadcast-type NTP messages.

For each of the NTP servers configured, an IP address must be provided, as well as the type of IP message it will use to access the individual server (*unicast*) or collective Server (*multicast*), the minimum time between requests, with the parameter establishing the exponent of the power of 2 in seconds; the maximum time between requests, also as the exponent of the power of 2 in seconds, and a selection option that determines whether authentication should be used, in which case it is necessary to indicate which previously-defined code the client with the server in question will use.

5.11 ACCESS CONFIGURATION

The equipment offer users several means of access: operating console, access via HTTP server (web) and telnet.

Local users predefined in the system are always present but an external resources can be used to validate users for different types of access, for which reason the user database is a centralised and independent resource with respect to the equipment itself. For this purpose the equipment has a TACACS+ client.

TACACS+ (Terminal Access Controller Access Control System) is a remote authentication protocol used to manage access to servers and communication devices; it provides separate authentication, authorisation and registration services.

FIGURE 28 **Access menu** configuration screen

The screenshot displays the 'Access menu' configuration interface. It is organized into four main sections, each with a red icon and a title bar:

- TACACS+**: Contains two input fields for '1 Server IP' and '2 Server IP', both set to '0.0.0.0'. There is a checked checkbox for 'Encrypted' and a blue link labeled 'Change' for 'Secret shared Key'.
- Console Access**: Features a dropdown menu for 'Authentication method1' set to 'local'. Below it, a note states '1 Fallback to local access always enabled'.
- Web Access**: Includes a dropdown menu for 'Authentication method' set to 'local' and a checked checkbox for 'Fallback to local access'.
- Telnet Access**: Includes a dropdown menu for 'Authentication method' set to 'local' and a checked checkbox for 'Fallback to local access'.

At the bottom of the configuration area, there are two buttons: 'Send' and 'Reload'.

The general configuration parameters are the following:

- **Server IP 1.** This establishes the IP address of the primary TACACS+ server.
- **Server IP 2.** This establishes the IP address of the secondary TACACS+ server.
- **Encrypted.** This permits user to select whether the equipment communication with the TACACS+ servers must be made in the ciphered mode or not.
- **Secret Shared Key.** This establishes the code to be used for ciphering the communication when the **encrypted** option is active.

The parameters associated with each access option (**console**, **web access** and **telnet**) are the following:

- **Authentication method.** This establishes whether the user validation must be made locally or by consulting the configured tacacsplus servers.
- **Fallback to local access.** When this option is enabled, if there is no accessibility to the configured TACACS+ servers, users are permitted to validate themselves with local user names. If the option is disabled, and the TACACS+ servers are not accessible, users will not be granted access. Access through the console has this option permanently enabled, for which reason it is not configurable.

5.12 DATA FLOW CONFIGURATION

The **Flow** menu basically permits the virtual ports (TCP/UDP) configuration parameters to be established, as well as to define the connections and/or flows between any of the available interfaces. See section 1.2 for more general information about the port interconnection.

The **UDP** protocol is a **connectionless protocol**. The data is transmitted as independent blocks (packets).

The **TCP** protocol is a **connection-oriented protocol**; thus, a prior establishment phase is necessary, and with it the data is transmitted as a continuous character flow.

5.12.1 Encapsulation protocols

Each one of the ports should be configured for operation with a specific protocol, either to operate in **transparent mode** (*raw* and *packed*), with one of the **telecontrol protocols being hold** or with a **policy** defined by the user.

Some protocols have multiple identifiers, which not only indicate the protocol itself, but also the **size of the link address**, when the standard requires it as a user option.

The protocols without multiple identifiers are the following:

- **pid1, dlms, gestel, sap20, twc, dnp3, procome** and **iec103**.

The protocols with multiple identifiers and values related to them are listed below:

- **iec101_1**. IEC 60870-5 101, with FT1.2 frame and a link address size of **1** byte.
- **iec101**. IEC 60870-5 101, with FT1.2 frame and a link address size of **2** byte.
- **iec102_1**. IEC 60870-5 102, with FT1.2 frame and a link address size of **1** byte.
- **iec102**. IEC 60870-5 102, with FT1.2 frame and a link address size of **2** byte.
- **modbusrtu**. Modbus protocol in RTU mode for operation in the encapsulator connected to the remote equipment.
- **modbusrtu_cc**. Modbus protocol in RTU mode for operation in the encapsulator connected to the controlling equipment (control center).

Although always present in the configuration registers, the following parameters are only useful when the *packed* protocol is selected.

- **Packed time (ms)**. It establishes the maximum waiting time after receiving the last character, in ms, before sending a packet with the data received so far. It forces sending the data for inactivity time when not reaching the data established as desired packet size (see following parameter).
- **Packed size**. It establishes the maximum number of characters to be transmitted in a packet on the network.

Physical Ports

Serial

Identifier

1 Serial1

2 Serial2

3 Serial3

4 Serial4

5 serial0

6 serial0

7 serial0

8 serial0

9 serial0

Virtual Ports

TCP

Identifier

Port

Destination

Retry Time (s)

Inactivity Time (s)

On Demand

Protocol

Policy

Packed time (ms)

Packed size

TLS Password

Enable

1 tcp0 1024 255.255.255.255 1.000000000 0.000000000 ☐ raw 10 16 ☐ Change ☒ Delete

2 Add

Passive TCP

Identifier

Interface

Port

Origin

Inactivity Time (s)

Protocol

Policy

Packed time (ms)

Packed size

TLS Password RFC2217

Enable

1 passivetcpTodos all 1030 any 0.000000000 raw 50 262 ☐ Change ☐ ☒ Delete

2 passivetcpPto1 all 1021 any 0.000000000 raw 50 262 ☐ Change ☐ ☒ Delete

3 passivetcpPto4 all 1024 any 0.000000000 raw 50 262 ☐ Change ☐ ☒ Delete

4 passivetcpPto2 all 1022 any 0.000000000 raw 50 262 ☐ Change ☐ ☒ Delete

5 passivetcpPto3 all 1023 any 0.000000000 raw 50 262 ☐ Change ☐ ☒ Delete

6 Add

RX UDP

Identifier Interface Port Group-ID Source Address Protocol Policy Packed time (ms) Packed size Multicast Enable

1 Add

TX UDP

Identifier Port Group-ID Destination Protocol Policy Packed time (ms) Packed size Enable

1 Add

Full UDP

Identifier

Interface

Local Port

Group-ID

Remote Port

Remote Address

Protocol

Policy

Packed time (ms)

Packed size

Multicast

Enable

1 Ethernet1 all 2011 0.0.0.0 2011 10.250.8.71 pid1 50 262 ☐ ☒ Delete

2 Ethernet1 all 2012 0.0.0.0 2012 10.250.8.70 pid1 50 262 ☐ ☒ Delete

3 Ethernet1 all 2013 0.0.0.0 2013 10.250.8.61 pid1 50 262 ☐ ☒ Delete

4 Ethernet4 all 2043 0.0.0.0 2043 10.250.8.93 pid1 50 262 ☐ ☒ Delete

5 Ethernet4 all 2044 0.0.0.0 2044 10.250.8.94 pid1 50 262 ☐ ☒ Delete

6 Ethernet2 all 2021 0.0.0.0 2021 10.250.8.98 iec101 50 262 ☐ ☒ Delete

7 Ethernet1 all 2014 0.0.0.0 2014 10.250.8.17 pid1 50 262 ☐ ☒ Delete

8 Ethernet3 all 2031 0.0.0.0 2031 10.250.8.68 pid1 50 262 ☐ ☒ Delete

9 Add

Spy

Identifier

Header

Mode

Enable

1 spyserialTodos Serial-> hex ☒ Delete

2 spyudpTodos RTUS<- hex ☒ Delete

3 spyserialSerial1 SERIAL(1)-> hex ☒ Delete

4 spyudpEthernet1 RTUS(1)<- hex ☒ Delete

5 spyserialSerial4 SERIAL(4)-> hex ☒ Delete

6 spyudpEthernet4 RTUS(4)<- hex ☒ Delete

7 spyserialSerial2 SERIAL(2)-> hex ☒ Delete

8 spyudpEthernet2 RTUS(2)<- hex ☒ Delete

9 spyserialSerial3 SERIAL(3)-> hex ☒ Delete

10 spyudpEthernet3 RTUS(3)<- hex ☒ Delete

11 Add

1 Input side: Add .in to identifier | Output side: Add .out to identifier

Send Reload

The configuration screen related to the **Flow** menu has three well differentiated sections, which are described below. The first one, **Physical Ports**, permits the serial ports identification to be established and, if the equipment is configured with the optional WAN interface, to configure a serial-datacall (GSM) connection. The second one, **Virtual Ports**, permits the configuration of the virtual ports (TCP/UDP) to be defined. The third one, **Spy**, permits the configuration of a spy port to be defined.

Physical Ports:

- **Serial #.** It identifies the equipment physical port number. Port 1 for port COM1, Ports 2 to 5 for block COM2 to COM5, and Ports 6 to 9 for block COM6 to COM9.
- **Identifier.** It establishes a different and unequivocal name for each one of the serial ports configured in the *Serial* menu. All the ports have the name *serial0* configured by default, and therefore, it is essential to assign a specific name to each of them.

The parameters to configure a serial-datacall (GSM) connection appear if the CIC is equipped with the optional WAN interface.

- **Datacall #.** It is a sequence identifier provided by the equipment itself.
- **Identifier.** It establishes the identifier related to the GSM datacall; *datacall0* is the value by default.
- **Use autocli.** Upon receiving a data call, the equipment connects the call to the **cli** management service if this option is activated (ticked box); thus, it is equivalent to a remote access to the service console. If the option is NOT activated (unchecked box), the data call will be redirected to the physical port configured by the user in the *Connection* block (see section 5.12.2).
- **Escape sequence.** If the data call does not have direct access to the management service, but to a determined port (autocli parameter NOT activated), it is still possible to access the **cli** management service by inserting the escape chain defined in this parameter. If the **cli** management service is accessed through the escape sequence, it is necessary to end the call and establish it again in order to recover the initial data flow.

Virtual Ports:

- **TCP (connections in active mode):**

#. It is a sequence identifier provided by the equipment itself.

Identifier. It establishes a different and unequivocal name for each one the active TCP virtual ports. When being added, all the connections have the name *tcp0* configured by default; therefore, it is essential to change said identifier for each one of the new connections.

Port. It establishes the destination TCP port.

Destination. It establishes the destination IP address.

Retry Time (s). If the connection fails, it establishes the waiting time in seconds before retrying the connection.

Inactivity Time (s). It establishes the inactivity time in seconds that will imply the

voluntary and controlled shutdown of the connection.

On Demand. It indicates if the connection should try to be established permanently (*inactive* parameter), or just when necessary if there is data (*active* parameter).

Protocol. It establishes the protocol of the data to be encapsulated; the possible values are indicated at the beginning of section 5.12.1. Usually the virtual ports operate in *raw* mode; the corresponding physical port is configured with the desired protocol.

Policy. This field should be configured when the ***policybased*** mode has been established in the *Protocol* parameter. It establishes an identifier, whose policy should be configured in the *Policy* submenu of the *Flow* menu.

Packed time (ms). See description at the beginning of section 5.12.1.

Packed size. See description at the beginning of section 5.12.1.

TLS. It establishes if the TCP connection will use ciphered communications through Transport Layer Secure (TLS).

Password. Related to the use of TLS, it establishes the common basic password.

Enable. It establishes if the TCP connection is active or not. The TCP connection is enabled if the box is ticked. By unchecking the box, the TCP connection is disabled, and it will not be retried.

- **Passive TCP (connections in passive mode).**

#. It is a sequence identifier provided by the equipment itself.

Identifier. It establishes a different and unequivocal name for each one of the TCP virtual ports (TCP connections), which will be awaiting connection requests from other equipment. When being added, all the connections have the name *passivetcp0* configured by default; therefore, it is essential to change said identifier for each one of the new connections.

Interface. It establishes the possible interfaces the requests will be accepted on; therefore, it restricts the possible input points of the connection requests. The possible values are the following: all, eth0, or cell0, if the equipment has the optional WAN interface.

Port. It establishes the TCP port where the connection requests will be awaited.

Origin. It establishes the source IP address range from which the connection requests will be accepted. It acts as filter of the authorized source equipment. The address may be a host or network address; therefore, it is necessary to specify the IP network mask.

Inactivity Time (s). It establishes the inactivity time in seconds that will imply the voluntary and controlled shutdown of the connection.

Protocol. It establishes the protocol of the data to be encapsulated; the possible values are indicated at the beginning of section 5.12.1. Usually the virtual ports operate in *raw* mode; the corresponding physical port is configured with the desired

protocol.

Policy. This field should be configured when the *policybased* mode has been established in the *Protocol* parameter. It establishes an identifier, whose policy should be configured in the *Policy* submenu of the *Flow* menu.

Packed time (ms). See description at the beginning of section 5.12.1.

Packed size. See description at the beginning of section 5.12.1.

TLS. It establishes if the TCP connection will use ciphered communications through Transport Layer Secure (TLS).

Password. Related to the use of TLS, it establishes the common basic password.

RFC2217. It establishes if the TCP connection should operate with the serial interface control extensions established in the RFC2217, or not.

Enable. It establishes if the TCP connection is active or not. The acceptance of TCP connection requests is enabled, if the box is ticked. When unchecking the box, the TCP connection requests will be rejected.

- **RX UDP (UDP ports that will accept data).**

#. It is a sequence identifier provided by the equipment itself.

Identifier. It establishes a different and unequivocal name for each one of the UDP virtual ports where the data packets will be accepted. When added, all the ports have the name *rxudp0* configured by default and, therefore, it is essential to assign a specific name to each of them.

Interface. It establishes the possible interfaces the data will be accepted on; therefore, it restricts the possible input points of the packets. The possible values are the following: all, eth0 or cell0, if the equipment has the optional WAN interface.

Port. It establishes the UDP port to be used to receive packets.

Group-ID. *Multicast* IP address that will accept data in reception, as long as the parameter value is a valid address, and the *multicast* option is active. The *0.0.0.0* default value is not a valid IP address.

Source Address. It establishes the source IP address range from which the connection requests will be accepted. It acts as filter of the authorized source equipment. The address may be a host or network address; therefore, it is necessary to specify the IP network mask.

Protocol. It establishes the protocol of the data to be encapsulated; the possible values are indicated at the beginning of section 5.12.1. Usually the virtual ports operate in *raw* mode; the corresponding physical port is configured with the desired protocol.

Policy. This field should be configured when the *policybased* mode has been established in the *Protocol* parameter. It establishes an identifier, whose policy should be configured in the *Policy* submenu of the *Flow* menu.

Packed time (ms). See description at the beginning of section 5.12.1.

Packed size. See description at the beginning of section 5.12.1.

Multicast. It establishes if the data with the *multicast* address established on Group-ID will be accepted. When the option is not active, the IP address for reception is the equipment own *unicast* IP address.

Enable. It establishes if the RX UDP port is active or not. With the box ticked, the RX UDP port is enabled, and will accept input packets. Unchecking the box, the RX UDP port will not accept data.

- **TX UDP (UDP ports where data will be transmitted).**

#. It is a sequence identifier provided by the equipment itself.

Identifier. It establishes a different and unequivocal name for each one of the UDP virtual ports where the data packets will be transmitted. When added, all the ports have the name *txudp0* configured by default and, therefore, it is essential to assign a specific name to each of them.

Port. It establishes the destination UDP port.

Group-ID/Destination. *Unicast* or *multicast* IP address to be used for data transmission. The *0.0.0.0* default value is not a valid IP address.

Protocol. It establishes the protocol of the data to be encapsulated; the possible values are indicated at the beginning of section 5.12.1. Usually the virtual ports operate in *raw* mode; the corresponding physical port is configured with the desired protocol.

Policy. This field should be configured when the ***policybased*** mode has been established in the *Protocol* parameter. It establishes an identifier, whose policy should be configured in the *Policy* submenu of the *Flow* menu.

Packed time (ms). See description at the beginning of section 5.12.1.

Packed size. See description at the beginning of section 5.12.1.

Enable. It establishes if the TX UDP port is active or not. With the box ticked, the TX UDP virtual port may be used for packet transmission.

- **Full UDP.**

#. It is a sequence identifier provided by the equipment itself.

Identifier. It establishes a different and unequivocal name for each one the bidirectional UDP virtual ports. When added, all the ports have the name *fulludp0* configured by default and, therefore, it is essential to assign a specific name to each of them.

Interface. It establishes the possible interfaces the data will be accepted on; therefore, it restricts the possible input points of the packets. The possible values

are the following: *all*, *eth0* or *cell0*, if the equipment has the optional WAN interface.

Local Port. It establishes the UDP port to be used to receive packets.

Group-ID. *Multicast* IP address that will accept data in reception, as long as the parameter value is a valid address, and the *multicast* option is active. The *0.0.0.0* default value is not a valid IP address.

Remote Port. It establishes the destination UDP port.

Remote Address. Unicast or multicast IP address to be used for data transmission. The *0.0.0.0* default value is not a valid IP address.

Protocol. It establishes the protocol of the data to be encapsulated; the possible values are indicated at the beginning of section 5.12.1. Usually the virtual ports operate in *raw* mode; the corresponding physical port is configured with the desired protocol.

Policy. This field should be configured when the ***policybased*** mode has been established in the *Protocol* parameter. It establishes an identifier, whose policy should be configured in the *Policy* submenu of the *Flow* menu.

Packed time (ms). See description at the beginning of section 5.12.1.

Packed size. See description at the beginning of section 5.12.1.

Multicast. It establishes if the data with the *multicast* address established on Group-ID will be accepted. When the option is not active, the IP address for reception is the equipment own *unicast* IP address.

Enable. It establishes if the Full UDP port is active or not. With the ticked box, the Full UDP virtual port is enabled, and accepts packets in reception, as well as their transmission.

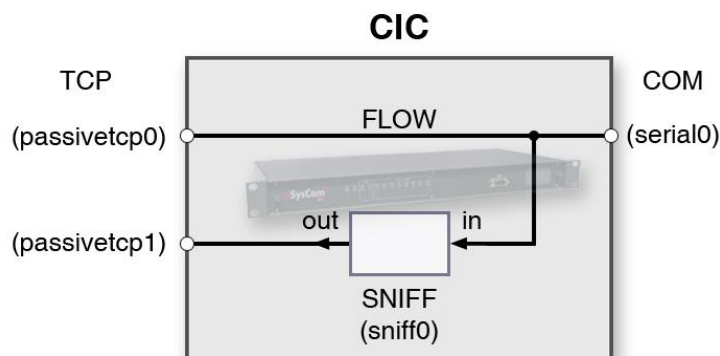
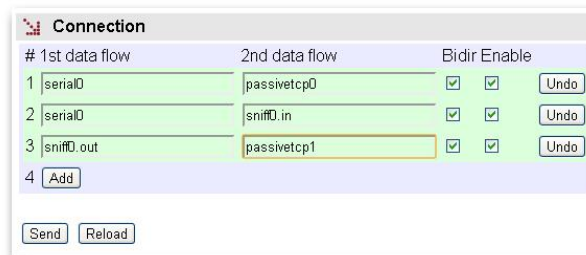
Spy:

- **#.** It is a sequence identifier provided by the equipment itself.
- **Identifier.** It establishes a different and unequivocal name for each one the spy ports. When added, all the ports have the name *sniff0* configured by default and, therefore, it is essential to assign a specific name to each of them.
- **Header.** It establishes the text appearing before each one of the messages provided by this instance in order to facilitate their origin if there are multiple spies.
- **Mode.** It establishes the representation format of the data available in the spy connection. The acceptable values are *raw* (original data format), or *hex* (hexadecimal representation).
- **Enable.** It establishes if the spy port is active or not. The spy port is enabled if the box is ticked.

Example:

The figure shows an example of a spy port definition to check the connection between a **serial0** port and a **passivetcp0** port. In addition to defining the spy port (**sniff0**), it will be necessary to define a port (**passivetcp1**) that will provide the information we are spying on.

FIGURE 30 Spy port configuration example



5.12.2 Connection

The **Connection** submenu of the **Flow** menu permits defining the connections determined by the physical and/or virtual ports, where the user traffic will be exchanged.

See section 1.2 for more general information about the port interconnection.

FIGURE 31

Connection configuration screen of the **Flow** menu

Connection					
#	1st data flow	2nd data flow	Bidir Enable		
1	Serial1	Ethernet1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
2	spyserialTodos.out	passivetcpTodos	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
3	Serial1	spyserialTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
4	Ethernet1	spyudpTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
5	spyudpTodos.out	passivetcpTodos	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
6	spyserialSerial1.out	passivetcpPto1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
7	Serial1	spyserialSerial1.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
8	spyudpEthernet1.out	passivetcpPto1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
9	spyudpEthernet1.in	Ethernet1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
10	Serial4	Ethernet4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
11	Serial4	spyserialTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
12	Ethernet4	spyudpTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
13	spyserialSerial4.out	passivetcpPto4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
14	Serial4	spyserialSerial4.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
15	spyudpEthernet4.out	passivetcpPto4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
16	spyudpEthernet4.in	Ethernet4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
17	Serial2	Ethernet2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
18	Serial2	spyserialTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
19	Ethernet2	spyudpTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
20	spyserialSerial2.out	passivetcpPto2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
21	Serial2	spyserialSerial2.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
22	spyudpEthernet2.out	passivetcpPto2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
23	spyudpEthernet2.in	Ethernet2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
24	Serial3	Ethernet3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
25	Serial3	spyserialTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
26	Ethernet3	spyudpTodos.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
27	spyserialSerial3.out	passivetcpPto3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
28	Serial3	spyserialSerial3.in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
29	spyudpEthernet3.out	passivetcpPto3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
30	spyudpEthernet3.in	Ethernet3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
31	Add				

Send Reload

The configuration parameters are the following:

- **#.** It is a sequence identifier provided by the equipment itself.
- **1st data flow.** It determines the **first port** included in this connection through its identifier.
- **2nd data flow.** It determines the **second port** included in this connection through its identifier.

It is essential to introduce the identifier name correctly in the two previous fields, so that it is one of those established in the *Physical ports* and *Virtual ports* sections of the *Flow* menu configuration screen. In order to avoid possible errors, it is advisable to use the commands *Ctrl.+C* (copy) and *Ctrl.+V* (paste) instead of the keyboard.

- **Bidir.** It determines if the connection operates both ways, that is, if it is ***bidirectional***.

In the case of ***unidirectional*** connections, the traffic flow is just from the port with the identifier specified on *1st data flow* towards the port with the identifier specified on *2nd data flow*.

- **Enable.** It establishes that the connection is active. The connection, or flow, is enabled if the box is ticked.

As can be seen in FIGURE 32, the identifiers permit a **numeric suffix**, apart from the identifier configured in previous sections, which is interpreted as the protocol message flow whose link address coincides with the established value; that is, for some of the encapsulation protocols, the equipment is capable of extracting specific conversations so that they may be demultiplexed towards differentiated destinations.

The size of the link address is specified when selecting the encapsulation protocol, or when the encapsulation policy is defined (in this last case, only for iec101/102).

FIGURE 32

Example of including a numeric suffix

#	1st data flow	2nd data flow	Bidir	Enable	
1	serial0.1	passivetcp0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
2	serial0.2	passivetcp1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
3	serial0.9	passivetcp5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
4	Add				

Send Reload

5.12.3 Policy

The **Policy** submenu of the **Flow** menu permits the creation of variants of some protocols, which enhances the encapsulator functions (see bibliography [4]).

The protocols that admit said variants are the following: iec101/iec102, pid1, gestel and sap20.

The additional functions implemented are designed for the use of the non-balanced mode protocols so as to minimize the traffic between the encapsulation equipment at the same time.

When the remote equipment is in non-balanced mode, it can only send information to the controlling equipment as a response to explicit requests (*polling* mechanism). So, in order to have response time to possible events that occurred and were detected by the remote entities, the control center should transmit cyclic inquiry messages and with a sufficiently high cadence. Therefore, these messages transit the TCP/IP network. The cyclical messages that are part of the *polling* are called **Quick Check (QC)**.

The enhanced functions imply that the cyclic inquiry of the *polling* mechanism will be created and sent by the encapsulation equipment connected directly to the remote equipment. Only when the remote responds to the **QC messages** will the encapsulation equipment from the remote side send them to the encapsulation equipment from the controlling side to be delivered to the control center. Thus, the control center is released of the cyclic inquiry mission and, in turn, the use of the related wideband is avoided.

FIGURE 33 **Policy** configuration screen of the **Flow** menu

Policy

iec101/iec102

# Identifier	DelayControl Mode	QuickCheck Mode	QuickCheck Period (secs)	QuickCheck Timeout	Link Address Size
1 policy0	none	none	15	0.500000000	2
2	Add				

pid1

# Identifier	DelayControl Mode	QuickCheck Mode	QuickCheck Period (secs)	QuickCheck Timeout
1 policy0	none	none	15	0.500000000
2	Add			

gestel

# Identifier	DelayControl Mode	QuickCheck Mode	QuickCheck Period (secs)	QuickCheck Timeout
1 policy0	none	none	15	0.500000000
2	Add			

sap20

# Identifier	DelayControl Mode
1 policy0	none
2	Add

Send Reload

The **Quick Check** function is regulated with the following parameters:

- **#.** It is a sequence identifier provided by the equipment itself.
- **Identifier.** It establishes a different and unequivocal name for each one the policies. When added, all the policies have the name *policy0* configured by default and, therefore, it is essential to assign a specific name to each of them.
- **Delay Control Mode.** The *none* option means that the Quick Check enhanced time control functions will not be executed. Any other option enables it and, in turn, determines if the equipment is connected to the control center (**system**), or to the remote equipment (**rtu**).
- **Quick Check Mode.** The *none* option means that the Quick Check enhanced functions will not be executed. Any other option enables the Quick Check option and, in turn, determines if the equipment is connected to the control center (**system**), or to the remote equipment (**rtu**).
- **Quick Check Period (secs).** It establishes the period of time for the local generation of the QC messages to the remote equipment.

- **Quick Check Timeout.** It establishes the maximum waiting time for a response from the remote equipment to the transmission of a QC message by the encapsulator.
- **Link Address Size. Only for the iec101/102 policies.** It establishes the size of the link address used in this profile, since these protocols admit two options as regards the size.

5.12.4 Other

The **Other** submenu of the **Flow** menu permits the activation of some additional facilities, mainly focused towards the obtainment of information to facilitate the resolution of possible configuration errors or events.

The screen related to the **Other** submenu has three well differentiated sections, which are described below.

Device:

- **Identifier.** This parameter specifies the identity of the related Control Center when using **Quick Check** policies. It only applies to the equipment working with the system profile, that is, the equipment the Control Center is connected to.

Socket:

- **Maximum time with sockets down (min).** It sets the maximum time acceptable, in minutes, during which there is no connection between the equipment executing **Quick Checks**.

Debug:

- **#.** It is a sequence identifier provided by the equipment itself.
- **Identifier.** It establishes the physical or virtual port identifier desired to generate additional information on the log files.

FIGURE 34

Other configuration screen of the **Flow** menu

Device
Identifier

Socket
Maximum time with sockets down (min)

Debug
Identifier
1 Undo
2 Add

5.13 CONFIGURATION OF THE SERIAL PORT AS *ModemEmulator*

The **ModemEmulator** menu implies that the equipment is presented as a HAYES modem to the client equipment; thus, the connections are established automatically based on the parameters provided by the client equipment, through the dialling commands.

The HAYES emulation offers the following behaviours according to the received command:

ATDT. It launches a TCP connection whose addressee and port results from the number included in the command itself. The number accepts two interpretations:

- **Direct number**, which corresponds to the IP address and the desired destination port. It is a 17-digit number: 12 correspond to the IP address, and 5 to the destination port. The IP address, as well as the port, should clearly include the digits whose value is null. That is, the destination with the *IP address* **10.89.1.123** and the port **348** would suppose that the command to be sent would be **ATDT 010 089 001 123 00348** (there are intentional blank spaces in the example chain to show the presentation mode, but there should not be included in the actual command).
- To consult the configured **Dialling Table**. The table permits the translation of a clearly arbitrary numbering plan to IP address and ports.

ATD*. The serial port acts as a PPP server, requesting the credentials (user and password) from the client equipment, and providing an IP address to it. The indicated parameters are established in the registers included in the Modem Emulator table.

ATD. It launches a GSM datacall to the destination number included in the command itself.

The following are other commands accepted by the device in emulation mode related to the management of calls:

ATA: It accepts a GSM datacall.

ATH: It implies the end of a call in progress.

In addition, as regards the behaviour management as MODEM, the equipment has the S2 register; it admits the configuration of the ECHO (E) parameters, management of the DCD (&C) signal and management of the DTR (&D) signal, and it supports the following standard commands: **ATA**, **ATO**, **ATI**, **AT&F**, **AT&W** and **AT&V**.

Modem Emulator

#	Identifier	User	Password	Authentication method	Own IP	Peer IP
1	emulator0		Change	pap	192.168.0.1	192.168.0.2
2	emulator0		Change	pap	192.168.0.1	192.168.0.2
3	emulator0		Change	pap	192.168.0.1	192.168.0.2
4	emulator0		Change	pap	192.168.0.1	192.168.0.2
5	emulator0		Change	pap	192.168.0.1	192.168.0.2
6	emulator0		Change	pap	192.168.0.1	192.168.0.2
7	emulator0		Change	pap	192.168.0.1	192.168.0.2
8	emulator0		Change	pap	192.168.0.1	192.168.0.2
9	emulator0		Change	pap	192.168.0.1	192.168.0.2

Dialling Table

Enable ☒

Telephone Entries	#	Telephone Number	Destination IP	TCP Port	
	1	100001	10.0.0.1	1001	Delete
	2	100002	10.0.0.2	1002	Delete
	3	100003	10.0.0.3	1003	Delete
	4	100004	10.0.0.4	1004	Delete
	5	100005	10.0.0.5	1005	Delete
	6	100006	10.0.0.6	1006	Delete
	7	100007	10.0.0.7	1007	Delete
	8	100008	10.0.0.8	1008	Delete
	9	100009	10.0.0.9	1009	Delete
	10	100010	10.0.0.10	1010	Delete
	11	100011	10.0.0.11	1011	Delete
	12	100012	10.0.0.12	1012	Delete
	13	100013	10.0.0.13	1013	Delete
	14	100014	10.0.0.14	1014	Delete
	15	100015	10.0.0.15	1015	Delete
	16	100016	10.0.0.16	1016	Delete
	17	100017	10.0.0.17	1017	Delete
	18	100018	10.0.0.18	1018	Delete
	19	100019	10.0.0.19	1019	Delete
	20	100020	10.0.0.20	1020	Delete
	21	100021	10.0.0.21	1021	Delete
	22	100022	10.0.0.22	1022	Delete
	23	100023	10.0.0.23	1023	Delete
	24	100024	10.0.0.24	1024	Delete
	25	100025	10.0.0.25	1025	Delete
	26	100026	10.0.0.26	1026	Delete
	27	100027	10.0.0.27	1027	Delete
	28	100028	10.0.0.28	1028	Delete
	29	100029	10.0.0.29	1029	Delete
	30	100030	10.0.0.30	1030	Delete
	31	100031	10.0.0.31	1031	Delete
	32	100032	10.0.0.32	1032	Delete
	33	100033	10.0.0.33	1033	Delete
	34	100034	10.0.0.34	1034	Delete
	35	100035	10.0.0.35	1035	Delete
	36	100036	10.0.0.36	1036	Delete
	37	100037	10.0.0.37	1037	Delete
	38	100038	10.0.0.38	1038	Delete
	39	100039	10.0.0.39	1039	Delete
	40	100040	10.0.0.40	1040	Delete
	41	100041	10.0.0.41	1041	Delete
	42	100042	10.0.0.42	1042	Delete
	43	100043	10.0.0.43	1043	Delete
	44	100044	10.0.0.44	1044	Delete
	45	100045	10.0.0.45	1045	Delete
	46	100046	10.0.0.46	1046	Delete
	47	100047	10.0.0.47	1047	Delete
	48	100048	10.0.0.48	1048	Delete
	49	100049	10.0.0.49	1049	Delete
	50	100050	10.0.0.50	1050	Delete
	51	100051	10.0.0.51	1051	Delete
	52	100052	10.0.0.52	1052	Delete
	53	100053	10.0.0.53	1053	Delete
	54	100054	10.0.0.54	1054	Delete
	55	100055	10.0.0.55	1055	Delete
	56	100056	10.0.0.56	1056	Delete
	57	100057	10.0.0.57	1057	Delete
	58	100058	10.0.0.58	1058	Delete
	59	100059	10.0.0.59	1059	Delete
	60	100060	10.0.0.60	1060	Delete
	61	100061	10.0.0.61	1061	Delete
	62	100062	10.0.0.62	1062	Delete
	63	100063	10.0.0.63	1063	Delete
	64	100064	10.0.0.64	1064	Delete
	65	100065	10.0.0.65	1065	Delete
	66	100066	10.0.0.66	1066	Delete
	67	100067	10.0.0.67	1067	Delete
	68	100068	10.0.0.68	1068	Delete
	69	100069	10.0.0.69	1069	Delete
	70	100070	10.0.0.70	1070	Delete
	71	100071	10.0.0.71	1071	Delete
	72	100072	10.0.0.72	1072	Delete
	73	100073	10.0.0.73	1073	Delete
	74	100074	10.0.0.74	1074	Delete
	75	100075	10.0.0.75	1075	Delete
	76	100076	10.0.0.76	1076	Delete
	77	100077	10.0.0.77	1077	Delete
	78	100078	10.0.0.78	1078	Delete
	79	100079	10.0.0.79	1079	Delete
	80	100080	10.0.0.80	1080	Delete
	81	100081	10.0.0.81	1081	Delete
	82	100082	10.0.0.82	1082	Delete
	83	100083	10.0.0.83	1083	Delete
	84	100084	10.0.0.84	1084	Delete
	85	100085	10.0.0.85	1085	Delete
	86	100086	10.0.0.86	1086	Delete
	87	100087	10.0.0.87	1087	Delete
	88	100088	10.0.0.88	1088	Delete
	89	100089	10.0.0.89	1089	Delete
	90	100090	10.0.0.90	1090	Delete
	91	100091	10.0.0.91	1091	Delete
	92	100092	10.0.0.92	1092	Delete
	93	100093	10.0.0.93	1093	Delete
	94	100094	10.0.0.94	1094	Delete
	95	100095	10.0.0.95	1095	Delete
	96	100096	10.0.0.96	1096	Delete
	97	100097	10.0.0.97	1097	Delete
	98	100098	10.0.0.98	1098	Delete
	99	100099	10.0.0.99	1099	Delete
	100	100100	10.0.0.100	1100	Delete
	101	100101	10.0.0.101	1101	Delete
	102	100102	10.0.0.102	1102	Delete
	103	100103	10.0.0.103	1103	Delete
	104	100104	10.0.0.104	1104	Delete
	105	100105	10.0.0.105	1105	Delete
	106	100106	10.0.0.106	1106	Delete
	107	100107	10.0.0.107	1107	Delete
	108	100108	10.0.0.108	1108	Delete
	109	100109	10.0.0.109	1109	Delete
	110	100110	10.0.0.110	1110	Delete
	111	100111	10.0.0.111	1111	Delete
	112	100112	10.0.0.112	1112	Delete
	113	100113	10.0.0.113	1113	Delete
	114	100114	10.0.0.114	1114	Delete
	115	100115	10.0.0.115	1115	Delete
	116	100116	10.0.0.116	1116	Delete
	117	100117	10.0.0.117	1117	Delete
	118	100118	10.0.0.118	1118	Delete
	119	100119	10.0.0.119	1119	Delete
	120	100120	10.0.0.120	1120	Delete
	121	100121	10.0.0.121	1121	Delete
	122	100122	10.0.0.122	1122	Delete
	123	100123	10.0.0.123	1123	Delete
	124	100124	10.0.0.124	1124	Delete
	125	100125	10.0.0.125	1125	Delete
	126	100126	10.0.0.126	1126	Delete
	127	100127	10.0.0.127	1127	Delete
	128	100128	10.0.0.128	1128	Delete
	129	100129	10.0.0.129	1129	Delete
	130	100130	10.0.0.130	1130	Delete
	131	100131	10.0.0.131	1131	Delete
	132	100132	10.0.0.132	1132	Delete
	133	100133	10.0.0.133	1133	Delete
	134	100134	10.0.0.134	1134	Delete
	135	100135	10.0.0.135	1135	Delete
	136	100136	10.0.0.136	1136	Delete
	137	100137	10.0.0.137	1137	Delete
	138	100138	10.0.0.138	1138	Delete
	139	100139	10.0.0.139	1139	Delete
	140	100140	10.0.0.140	1140	Delete
	141	100141	10.0.0.141	1141	Delete
	142	100142	10.0.0.142	1142	Delete
	143	100143	10.0.0.143	1143	Delete
	144	100144	10.0.0.144	1144	Delete
	145	100145	10.0.0.145	1145	Delete
	146	100146	10.0.0.146	1146	Delete
	147	100147	10.0.0.147	1147	Delete
	148	100148	10.0.0.148	1148	Delete
	149	100149	10.0.0.149	1149	Delete
	150	100150	10.0.0.150	1150	Delete
	151	100151	10.0.0.151	1151	Delete
	152	100152	10.0.0.152	1152	Delete
	153	100153	10.0.0.153	1153	Delete
	154	100154	10.0.0.154	1154	Delete
	155	100155	10.0.0.155	1155	Delete
	156	100156	10.0.0.156	1156	Delete
	157	100157	10.0.0.157	1157	Delete
	158	100158	10.0.0.158	1158	Delete
	159	100159	10.0.0.159	1159	Delete
	160	100160	10.0.0.160	1160	Delete
	161	100161	10.0.0.161	1161	Delete
	162	100162	10.0.0.162	1162	Delete
	163	100163	10.0.0.163	1163	Delete
	164	100164	10.0.0.164	1164	Delete
	165	100165	10.0.0.165	1165	Delete
	166	100166	10.0.0.166	1166	Delete
	167	100167	10.0.0.167	1167	Delete
	168	100168	10.0.0.168	1168	Delete
	169	100169	10.0.0.169	1169	Delete
	170	100170	10.0.0.170	1170	Delete
	171	100171	10.0.0.171	1171	Delete
	172	100172	10.0.0.172	1172	Delete
	173	100173	10.0.0.173	1173	Delete
	174	100174	10.0.0.174	1174	Delete
	175	100175	10.0.0.175	1175	Delete
	176	100176	10.0.0.176	1176	Delete
	177	100177	10.0.0.177	1177	Delete
	178	100178	10.0.0.178	1178	Delete
	179	100179	10.0.0.179	1179	Delete
	180	100180	10.0.0.180	1180	Delete
	181	100181	10.0.0.181	1181	Delete
	182	100182	10.0.0.182	1182	Delete

- **User.** It establishes the admissible user when the equipment acts as a PPP server.
- **Password.** It establishes the password related to the PPP user from the previous field.
- **Authentication method.** It establishes the standard protocol used for the exchange of credentials with the external equipment; the values are **none** (without authentication), **pap** (Password Authentication Protocol) and **chap** (Challenge Handshake Authentication Protocol).
- **Own IP.** The IP address related to the equipment serial interface when acting as a PPP server.
- **Peer IP.** The IP address to be provided to the client equipment.

Dialling Table:

- **Enable.** It establishes if the table should be used for the translation of the numbering plan of the calls made with the ATDT command, or not.
- **#.** It is a sequence identifier provided by the equipment itself.
- **Telephone Number.** The number of the numbering plan related to the register.
- **Destination IP.** The destination IP address for the number specified in the previous parameter.
- **TCP Port.** The destination TCP port for the number specified in the telephone number parameter.

5.14 REBOOT

The equipment can be rebooted by executing the **Reboot** command, through the console or through the HTML pages. The command is available only for the administrator profile.

5.15 CODE REFLASH

The equipment admits the updating of applicative software by executing the **Reflash** command, which is only available in the HTML pages and for the administrator profile.

The code reflash process does not alter the configuration data, unless this is expressly indicated. Nevertheless, once terminated, it entails a momentary loss of service due to the automatic rebooting of the equipment.

A binary image that is appropriate for the equipment is necessary, which can be selected on accessing the tree directory in the local machine, by pressing the button *Examine*.

After selecting the image, the update is executed by pressing **Reflash**. The process usually takes about 5 minutes, during which time the results of the different steps are displayed in the HTML browser window, but depending on the browser, it is possible that only the result at the end of the process is shown.

The **Only verify** option allows users to check that the code saved coincides with the binary image selected without affecting the installed image.

6 STATISTICS

The system provides statistics divided into eight blocks, each of them corresponding to a specific functionality.

The first block shows general information related to the equipment, and is displayed automatically when the statistics object is selected.

The remaining statistics are grouped into data belonging to the *ModemEmulator* function, the Ethernet (*LAN*) interface, the optional WAN interface, the *Routing* rules, DHCP server, synchronization client (*NTP*), and port interconnection (*Flow*), each of which can be accessed by selecting the respective tag located under the heading *Statistics*.

Each statistical data table can be updated by pressing the *Reload* button without having to select the respective option again in the tree menu.

The statistics can be **REBOOTED** by the user at will, from the console by executing the ***clear*** command in the prompt, or using the menu option ***Clear Statistics***.

FIGURE 36 Example of statistics with general data

General Statistics	
Uptime	0d01:45:23.834
Time (UTC)	2005/01/01,00:00:00 Change
Time (Local)	2005/01/01,00:00:00 Change
Temperature	37 (C) / 99 (F)
Memory Usage (%)	59
Long term CPU Usage (%)	3
Short term CPU Usage (%)	4
Reload	

FIGURE 37 Example of statistics of the *ModemEmulator* function

Modem Emulator					
#	Num TCP	Num PPP	Num Datacalls	State	In Octets Out Octets
1 0	0	0		0	0
2 0	0	0		0	0
3 0	0	0		0	0
4 0	0	0		0	0
5 0	0	0		0	0
6 0	0	0		0	0
7 0	0	0		0	0
8 0	0	0		0	0
9 0	0	0		0	0
Reload					

FIGURE 38 Example of statistics of LAN

General Data					
#	Status	IP Address	Status Date	TX Bytes RX Bytes	
1	Active	0.0.0.0	Thu Sep 15 14:37:49 UTC 2011	2520784	53776901
Reload					

FIGURE 39

Example of statistics of WAN

General Data	
IMEI	353229023794959
IMSI	unknown
CID	unknown
PIN Status	NO SIM
Operator	unknown
Roaming	unknown
Network	unknown
Local Area Code	unknown
Cell Identifier	unknown
Signal Strength	unknown
Total TX KBytes	0
Total RX KBytes	0
Number of Session failures	0
SIMA Tx Bytes	0
SIMA Rx Bytes	0
Current Data Session	
Status	Inactive
IP Address	unknown
Connection Date	unknown
TX Bytes	0
RX Bytes	0
TX Rate (bps)	0
RX Rate (bps)	0
Previous Data Session	
Disconnection Date	unknown
Up Time (s)	unknown
TX Bytes	unknown
RX Bytes	unknown
<input type="button" value="Reload"/>	

FIGURE 40 Example of statistics of the Routing



#	Network Gateway	I/F	Metric
1	default	172.16.50.254	eth0 0

Reload

FIGURE 41 Example of statistics of the DHCP Server




DNS1 Server IP	0.0.0.0
DNS2 Server IP	0.0.0.0



#	MAC Addr	IP Addr	Expiration time
---	----------	---------	-----------------

Reload

FIGURE 42 Example of statistics of the NTP



Offset	unknown
Frequency offset	unknown
Jitter	unknown
Allan	unknown

Reload

FIGURE 43

Example of statistics of the port interconnection (*Flow*)

Physical Ports						
Serial	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
1	Serial1	0	0	NA	NA	Connected
2	Serial2	0	0	NA	NA	Connected
3	Serial3	0	0	NA	NA	Connected
4	Serial4	0	0	NA	NA	Connected
5	serial0	0	0	NA	NA	Connected
6	serial0	0	0	NA	NA	Connected
7	serial0	0	0	NA	NA	Connected
8	serial0	0	0	NA	NA	Connected
9	serial0	0	0	NA	NA	Connected

Virtual Ports						
TCP	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
	1 tcp0	0	0	NA	NA	Connecting
Passive TCP	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
	1 passivetcpTodos	0	84	NA	NA	Connecting
	2 passivetcpPto1	0	54	NA	NA	Connecting
	3 passivetcpPto4	0	122	NA	NA	Connecting
	4 passivetcpPto2	0	54	NA	NA	Connecting
	5 passivetcpPto3	0	54	NA	NA	Connecting
TX UDP						
RX UDP						
Full UDP	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
	1 Ethernet1	0	0	NA	NA	Connected
	2 Ethernet1	0	0	NA	NA	Connected
	3 Ethernet1	0	0	NA	NA	Connected
	4 Ethernet4	0	0	NA	NA	Connected
	5 Ethernet4	0	0	NA	NA	Connected
	6 Ethernet2	0	0	NA	NA	Connected
	7 Ethernet1	0	0	NA	NA	Connected
	8 Ethernet3	0	0	NA	NA	Connected

Reload

APPENDIX A

BIBLIOGRAPHY AND ABBREVIATIONS

APPENDIX A

BIBLIOGRAPHY AND ABBREVIATIONS

A.1 BIBLIOGRAPHY

- | |
|---|
| [1] STD 15. IEEE RFC 1157. May 1990. A Simple Network Management Protocol (SNMP). |
| [2] STD 62. IEEE RFC 3416. December 2002. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (Obsoletes RFC 1905). |
| [3] IEEE RFC 1305, March 1992. Network Time Protocol (Version 3) Specification, Implementation and Analysis. |
| [4] Development specification of the terminals used for the creation of a point-multipoint channel via GPRS_Rev.06 (14/4/2008) of IBD reference GPF070302CVG. |

A.2 ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
API	Application Programming Interface
APN	Access Point Name
ASDU	Application Service Data Units
BPDU	Bridge Protocol Data Units
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name Server
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IOA	Information Object Address
IP	Internet Protocol
IP Multicast	Extension of the Internet Protocol for providing support to multidiffusion communications
IPBX	Internet Protocol Private Branch Exchange
IPS	Intrusion Prevention System
IPSec	IP Security

ISDN	Integrated Services Data Network
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
LAN	Local Area Network
NAT	Network Address Translation
NHRP	Next Hop Resolution Protocol
NTP	Network Time Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Server
RAS	Registration, Authentication and Status
RSVP	Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WPA	Wi-Fi Protected Access Client Support

APPENDIX B

DATA STRUCTURE IN *CLI*

APPENDIX B

DATA STRUCTURE IN CLI

This Appendix contains all the information required to use the CLI user console. It explains the access methods, commands available on the console and gives a step-by-step example of how to obtain information on the status and configuration of the equipment.

Conventions:

The equipment configuration parameters are laid out in a tree directory, in which parameters and related subdirectories are grouped, where:

- A name followed by “/” indicates the name of a directory. *E.g. **Main/***
- A name followed by “[]” indicates a parameter with a matrix structure, as it contains several attributes. *E.g. **nat[]/***
- A name with nothing after it is a parameter in itself. *E.g. **action***

B.1 ACCESS METHODS

There are two ways of accessing the equipment through the CLI user console:

- in the local mode, through the serial port (SRV port).
- in the remote mode, through Telnet.

Local mode access

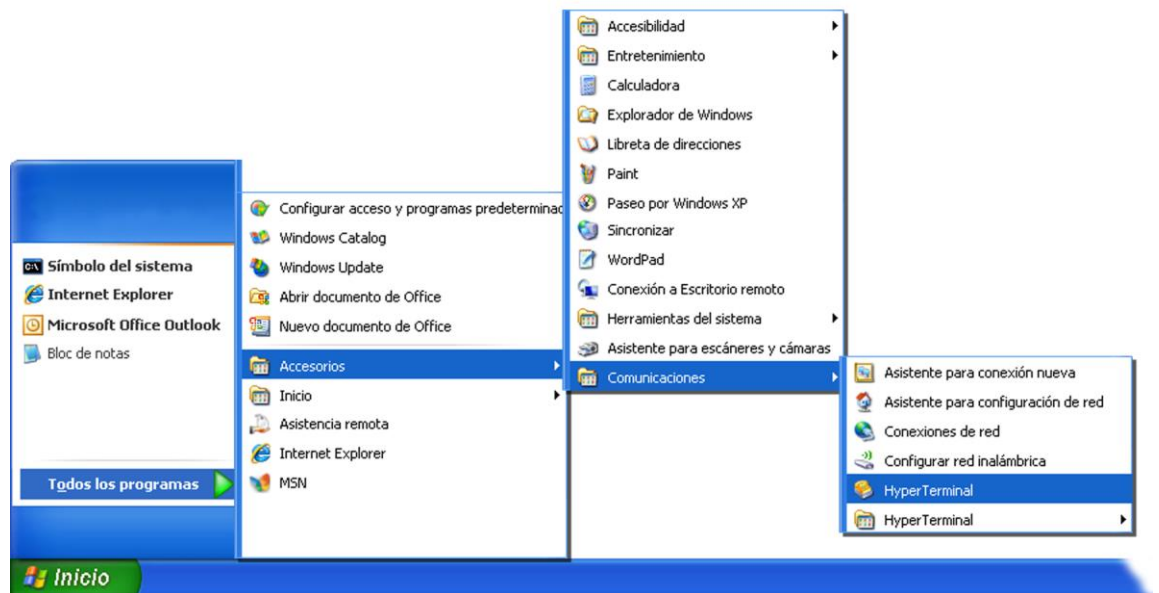
Local mode access is obtained through a flat serial cable that connects the serial port of the computer to the serial port of the equipment (SRV).

Communication between the computer and the equipment is established through a terminal emulation programme, such as Windows® *HyperTerminal*, configuring a serial connection with the following characteristics:

- Speed: 115.200 bps
- Data bits: 8
- Parity: No
- Stop bits: 1
- Flow control: No

In Windows XP® execute *HyperTerminal* from *Start* → *All Programmes* → *Accessories* → *Communications* → *HyperTerminal* (see FIGURE 43).

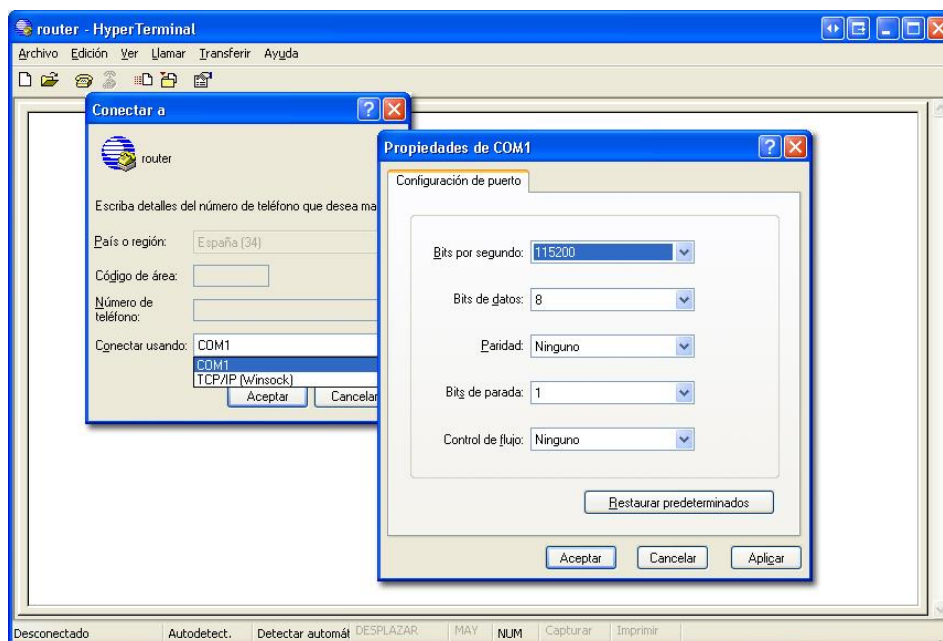
FIGURE 44 Location of *HyperTerminal* in Windows XP®



On opening *HyperTerminal* a text box appears, requesting the necessary information to establish the connection (see FIGURE 44).

FIGURE 45

Connection configuration through the serial port with *HyperTerminal*



Remote mode access

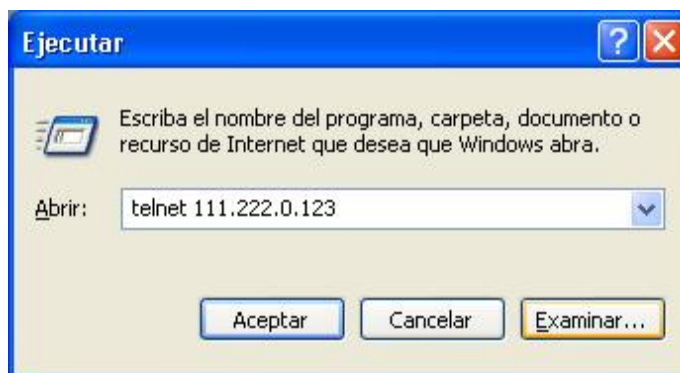
Remote mode access is obtained with the *Telnet* command and equipment IP address.

! To use this access mode the equipment must have its IP address configured and be connected to the management computer network.

Telnet can be executed in Windows XP® from the Start button: Start → Execute, and in the text box, enter: telnet + space + Equipment_IP_address, and then press Accept (see FIGURE 45).

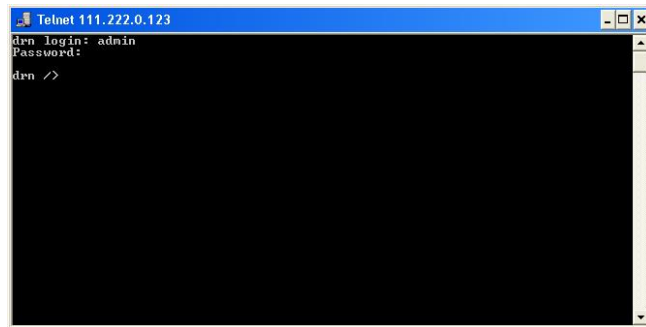
FIGURE 46

Execute... *Telnet* text window to establish connection with the equipment



On pressing the Accept button a System symbol window will appear with the Telnet programme connected to the equipment (see FIGURE 46).

FIGURE 47 *Telnet window*



HyperTerminal can be used as the *Telnet* graphic interface. To do this, when configuring the connection select **TCP/IP (Winsock)** in the *Connect using* drop down menu.

Whatever the method chosen to establish connection with the equipment, the **equipment login** prompt will appear: (where *equipment* will be the 3 letters that identify it. *E.g. dnr login:*) ready for the user to enter the *login* and code for starting the session (the logins and their respective passwords are the same as in the web interface).

B.2 USER CONSOLE COMMANDS

After starting the session with a valid login and password, the prompt will change to **equipment />** waiting for the user to enter a command.

The commands are instructions sent to the equipment to request or change a value or to “browse” through the tree in which the equipment parameters are organised.

The following table shows a full list of available commands with a brief description of each one and their availability depending on the type of user starting the session, highlighting the most useful ones:

TABLA 3

Full list of CLI user console commands

Command	Description	User	
		admin	guest
add	Adds a new item to a matrix-type parameter	✓	✗
apply	Applies the new configuration	✓	✗
cd	Changes the directory in the parameters tree	✓	✓
clear	Deletes the statistics	✓	✗
date	Shows the date stored in the equipment	✓	✗
download	Generates a configuration commands file	✓	✓
Exit	Interrupts the connection with the equipment	✓	✓
get	Shows the parameter values	✓	✓
help	Shows the list of available commands	✓	✓
Log / Log all	Shows the list of events	✓	✓
ls	Shows the lists of available parameters in the current directory	✓	✓
ping	Sends a ping to the indicated host	✓	✓
quit	Interrupts the connection with the equipment		
reboot	Reboots the equipment	✓	✗
reload	Loads a previously-saved configuration	✓	✗
remove	Eliminates an item from a matrix-type parameter	✓	✗
restore	Loads a default configuration	✓	✗
Save	Saves all the changes made during the session	✓	✗
Set	Modifies the value of a parameter	✓	✗
stats	Shows the equipment status	✓	✓
telnet	Open a telnet session without interrupting the connection with the equipment	✓	✓

Depending on the function of each command, they can be classified into different groups:

TABLA 4

Classification of commands based on their functions

Configuration	Control	Diagnostic
add	cd	clear
apply	exit	date
download	quit	help
get	reboot	log
remove	reload	ls
restore	telnet	ping
save		stats
set		

Configuration commands

add Adds a new item to the matrix of a matrix-type parameter.

Syntax: `drn /> add name`

Arguments:

name Parameter to which a new item is to be added.

Observations: To add a new item to a matrix-type parameter, it is necessary to be in the directory in which it is located or enter the relative route.

The new item created has the next order number with respect to the last one. For instance, if *nat[1]* and *nat[2]* already existed, on executing the command `add nat` the item *nat[3]* is created.

Examples:

```
drn /> add nat
drn /wan> add tunnel/tunnel
drn /admin> add ../nat
```

apply This applies the configuration changes in the equipment, but without saving them.

Syntax: `drn /> apply`

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

This command DOES NOT save the changes made.

Example: `drn /> apply`

download This shows the necessary commands for configuring equipment with the same parameters as the current one.

Syntax: `drn /> download`

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

The list of commands shown starts with the command *restore*, which applies the factory configuration, followed by the commands required to obtain the current configuration.

It is a good idea to copy and save this list of commands in a .txt file, so it can be used in other equipment with the same characteristics.

To apply the saved configuration in different equipment, it must be of the same model and version, and above all, have the same firmware version installed, since the factory configuration used to generate the commands list may be different in each one.

Example: drn /> **download**

get

This shows the current values of one or several equipment configuration parameters.

Syntax: drn /> **get** [name]

Arguments: -

name (optional) name of the parameter to be shown.

Observations: The command *get* with no argument shows the values of all the configuration parameters in the current directory and its subdirectories. If the argument is the name of a directory it shows the values of the parameters in that directory. If the argument is the name of a configuration parameter it shows the value of that parameter.

To show the complete configuration of the equipment, this command must be executed with no arguments, from the root directory.

If an argument is used, it must be in the current directory or the relative route must be entered.

Examples: drn /> **get**
 drn /> **get main**
 drn /main> **get hostname**
 drn /> **get main/hostname**
 drn /admin> **get ../main/hostname**

remove This eliminates an item from the matrix of a matrix-type parameter.

Syntax: `drn /> remove name[nº]`

Arguments:

name Parameter from which the item is to be removed.

nº (Optional) Order number of the parameter item

Observations: To remove an item from the matrix of a matrix-type parameter, it is necessary to be in the respective directory or enter the relative route.

If the order number of the item to be removed is indicated, that item will be removed. If the number is not indicated, the last one will be removed.

When removing an item that is not the last one, the other remaining items will be automatically renumbered.

Examples: `drn /> remove nat[2]`
`drn /> remove nat`
`drn /admin> remove ../nat`

restore This applies the factory configuration.

Syntax: `drn /> restore`

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

Example: `drn /> restore`

save This saves the changes made in configuring the equipment in its permanent memory. However, these changes will not take effect until the equipment is rebooted.

Syntax: `drn /> save`

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

Example: `drn /> save`

set This changes the value stored in the configuration parameters or in the attributes of an item in a matrix-type parameter.

Syntax: `drn /> set [name][[n°]/[name2]]`

Arguments: -

name name of the parameter to be changed.

n° item number of a matrix-type parameter.

name2 name of an attribute in a matrix-type parameter.

Observations: When this command is executed the system waits for the new value to be entered.

The parameter to be changed must be in the current directory or its relative route must be entered.

In the case of wanting to change the value of any attribute in the item of a matrix-type parameter, the argument must include the parameter name, the item number and the attribute number.

Special attention should be paid when entering the arguments of this command, as if no argument is indicated the system will request the new value of each of the parameters in the active directory and its subdirectories, one by one. Consequently, if the `set` command is executed without an argument in the root directory, the system will request a new value for all the equipment configuration parameters.

If the `set` command is applied to a matrix-type parameter without indicating the attribute to be modified, the system will request a new value for each attribute of the indicated item. If the item number is omitted, the new values entered for each attribute will be applied to the last item in the matrix.

Examples:

```
drn /main> set hostname
drn /> set main/hostname
drn /admin> set ../main/hostname
drn /> set nat[2]/origin
```

Control commands

cd Changes the active directory.

Syntax: drn /> **cd** *name*

Arguments:

name Name of the destination directory.

Observations: The destination directory must be in the current directory or its relative route must be entered.

To activate the directory on the level immediately above it, two dots must be entered: **cd ..**

When the directory is changed the prompt shows the equipment identification letters and the name of the active directory. Example: **drn /main>**.

Examples: drn /> **cd main**
drn /main> **cd ../admin**

exit This closes the connection between the computer and the equipment, and therefore the CLI programme session.

Syntax: drn /> **exit**

Arguments: -

Observations: -

Example: drn /> **exit**

quit This closes the connection between the computer and the equipment, and therefore the CLI programme session.

Syntax: drn /> **quit**

Arguments: -

Observations: -

Example: drn /> **quit**

reboot This reboots the equipment without having to turn it off and on again, for instance, in order to apply the saved configuration changes.

Syntax: `drn /> reboot`

Arguments: -

Observations: -.

Example: `drn /> reboot`

reload Reloads the saved configuration in the equipment.

Syntax: `drn /> reload`

Arguments: -

Observations: This command may be useful if it is required to reload the configuration saved in the equipment after the time it was saved.

Example: `drn /> reload`

telnet Open a telnet session, keeping the connection established between the computer and the equipment open.

Syntax: `drn /> telnet Host[Port]`

Arguments:

Host Name of the destination host to which open a Telnet session.

Port (optional) Number of the destination port where to open a Telnet session.

Observations: To restart the session, it is necessary to re-enter the login and password.
The 3 letters identifying the equipment can be used as the host name.

Example: `drn /> telnet drn`
`drn /> telnet 172.16.50.38 23`

Status and Diagnostic Commands

clear Deletes the statistics.

Syntax: `drn /> clear`

Arguments: -

Observations: -

Example: `drn /> clear`

date Shows the date and time recorded in the equipment.

Syntax: `drn /> date`

Arguments: -

Observations: -

Example: `drn /> date`

help Displays a list of all the available commands and a brief description of their functions.

Syntax: `drn /> help`

Arguments: -

Observations: -

Example: `drn /> help`

Log / Log all They show the list of events taking place in the equipment. This command is useful for monitoring the equipment and detecting potential errors during operation.

Syntax: `drn /> log [all]`

Arguments:

- Without arguments, this command shows the events recorded in the equipment's non-volatile memory.
- all* (Optional) Shows all the events taking place in the equipment in real time until the user presses a key.

Observations: All the events taking place in the equipment are stored in a memory buffer with sufficient capacity for 100 records and if an important event occurs (starting of sessions, changes in configuration, etc.) this is recorded in the equipment non-volatile memory which also has capacity for 100 records.

Both the buffer and non-volatile memory are of the circular type, i.e., once the memory is full, the oldest event is removed every time a new event occurs.

Example: `drn /> log`
 `drn /> log all`

ls Shows a list from the active directory. This command is useful for verifying whether the configuration parameter to be consulted/changed is in the active directory.

Syntax: `drn /> ls`

Arguments: -

Observations: -

Example: `drn /> ls`

ping This sends ICPM ECHO_REQUEST packets to a specific host.

Syntax: `drn /> ping host`

Arguments:
 host Host name or destination IP address.

Observations: When this command is executed the equipment starts to send pings to the indicated host until the user presses the **Ctrl.+C** keys.

Example: `drn /> ping 172.16.50.38`
 `drn /> ping emr`

stats

This shows the equipment status parameters. These parameters are derived from the use made of the equipment, for instance, Use of the memory of CPU, temperature, bytes transmitted, etc.

Syntax: `drn /> stats [parameter]`

Arguments:

parameter (Optional) Name of the parameter whose status is to be consulted.

Observations: Like the configuration parameters, these are classified by categories, in the form of a directories tree.

The normal use of this command is without arguments and from the root directory, it shows all the equipment status parameters.

To show a parameter for a specific status or those of a specific directory, the names of each one must be known.

Examples:

```
drn /> stats
drn /> stats main
drn main/> stats temperature
drn main/> stats ../lan/eth0/txbytes
```

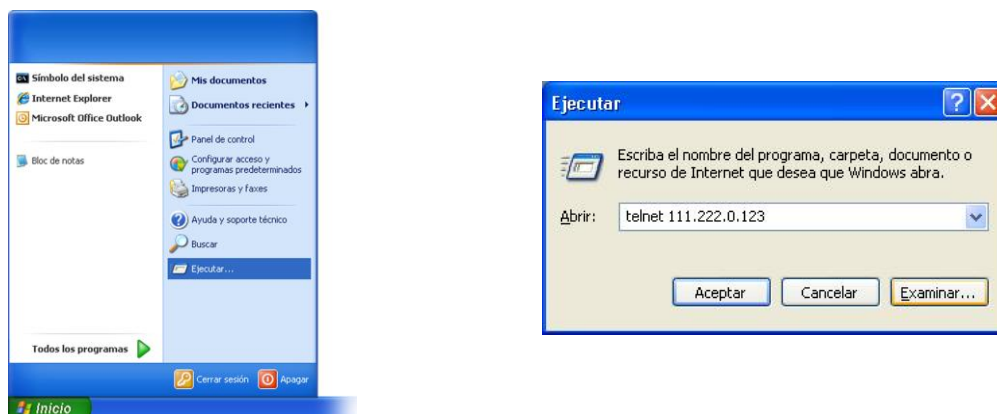
B.3 OBTAINING INFORMATION ABOUT THE STATUS AND CONFIGURATION OF A EQUIPMENT

To obtain information about the status and configuration of a equipment, proceed as follows:

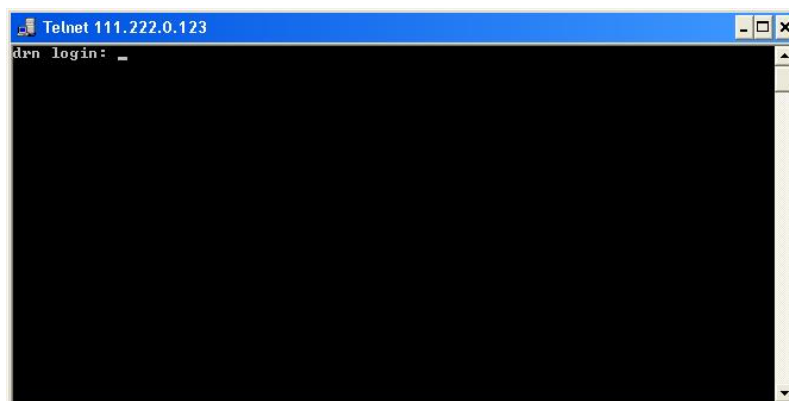
1- Connection with the equipment

As explained in chapter **B.1**, the equipment connection differs slightly depending on the chosen method. In this example, it is assumed that the equipment is a **DRA-2**, connected to a network and with an IP address configured, which in the case of this example will be 111.222.0.123. In addition the computer used to make the connection is also connected to that network and the O.S. used is *Windows XP®*.

To establish the connection through **Telnet**, click on the *Windows XP® Start* button and once the menu has appeared, click on the command **Execute**. In the window that appears, enter "**telnet 111.222.0.123**" (without inverted commas) and then press **Accept**.



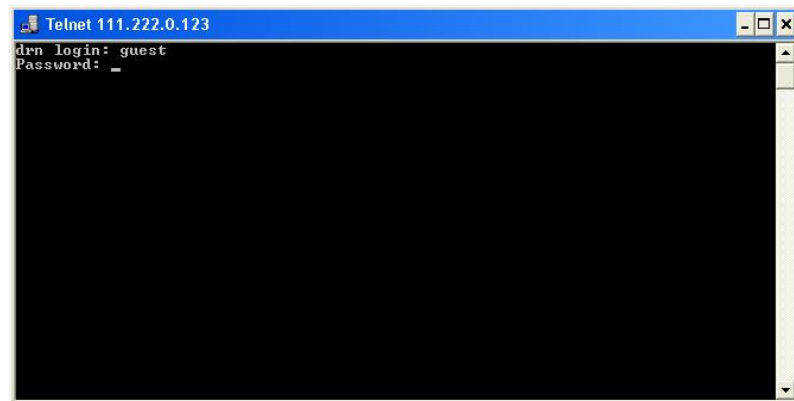
If everything is functioning normally, a window will pop up with a system symbol, which is the interface for the connection.



2- User identification

On establishing connection with the equipment, the prompt **drn login:** indicates that the system is waiting for a user name to connect with the **drn** equipment.

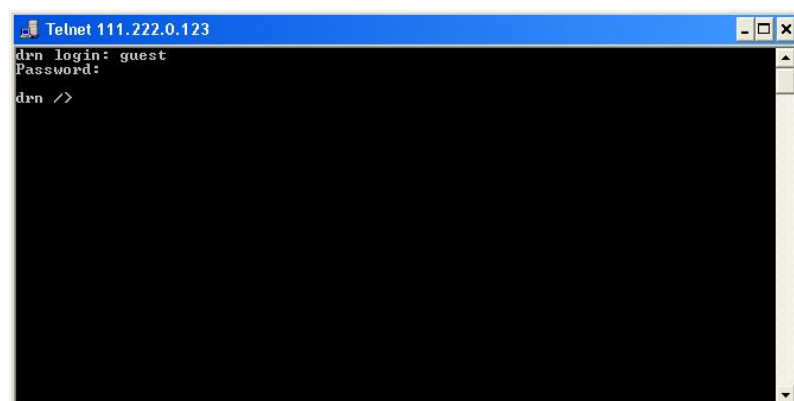
Given that we only want information, it makes no difference which login is entered (**admin** or **guest**). Enter **guest** and then press **enter**



Now the system is waiting for us to enter the respective password. Enter **passwd01** which is the one associated with the **guest** user and press **enter**.

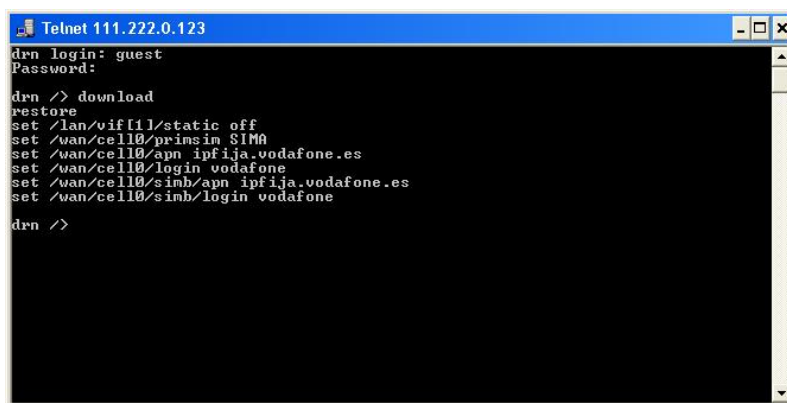
Remember that no text will appear in the *Telnet* window when entering the password.

If the login and password entered are correct, the prompt **drn />** will appear, indicating that the equipment is waiting for a command to be entered.



3- Obtaining the equipment configuration

The equipment configuration is obtained through the command **download**. On pressing **enter** after this command, the full equipment configuration will be displayed.

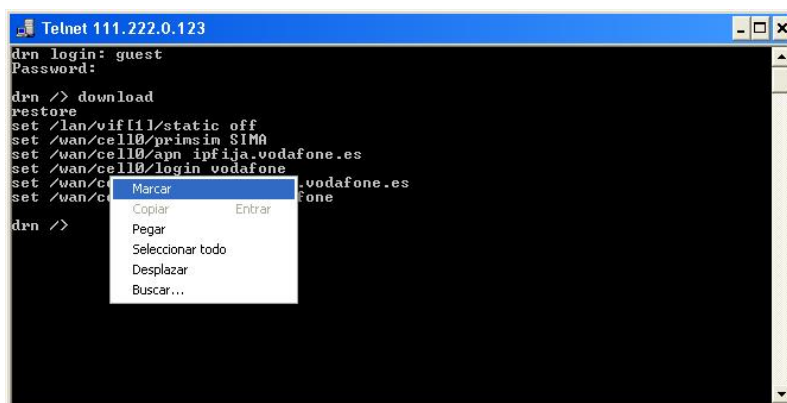


```
Telnet 111.222.0.123
drn login: guest
Password:
drn /> download
restore
set /lan/vif111/static off
set /wan/cell0/primsin SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/smb/apn ipfija.vodafone.es
set /wan/cell0/smb/login vodafone
drn />
```

If the information extends beyond the edges of the window, the system will only show the information at the start and it will be necessary to press **enter** once or several times for all the information to be shown. You will know whether the system has finished showing all the information when the equipment prompt reappears: **drn />**.

It is important to save the information in a .txt file using the **download** command so that it can be used whenever necessary.

To copy the text from the Windows XP® command window, right-click with the mouse and select **Mark** in the menu that appears.



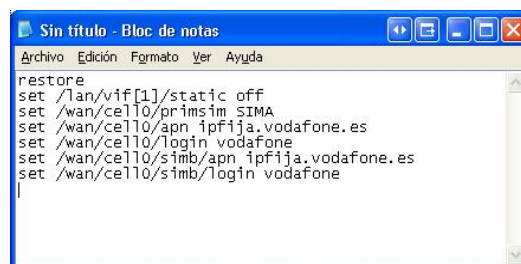
```
Telnet 111.222.0.123
drn login: guest
Password:
drn /> download
restore
set /lan/vif111/static off
set /wan/cell0/primsin SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/smb/apn ipfija.vodafone.es
set /wan/cell0/smb/login vodafone
drn />
```

Then place the cursor at the start of the text to be copied, left-click with the mouse and drag the cursor, maintaining the button pressed, until all the text has been selected. After releasing the left button, press the **enter** key. That way, you will have copied the selected text into the Windows clipboard.



```
Telnet 111.222.0.123
drn login: guest
Password:
drn /> download
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfija.vodafone.es
set /wan/cell0/simb/login vodafone
drn /> _
```

Now open Windows *Notepad* and paste the text (**Ctrl. + V**) in a *.txt* file and save it.



```
Sin título - Bloc de notas
Archivo Edición Formato Ver Ayuda
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfija.vodafone.es
set /wan/cell0/simb/login vodafone
```

4- Obtaining the equipment status

The **get** command shows the full status of the equipment. Since the information shown is very lengthy, every time a window is filled, it will wait for the user to press a key to continue displaying the information.

```

Telnet 172.16.50.38
drn /> get
main/
hostname      = drn
location      = unknown
contact       = unknown
product       = 4DRNC00100E00DA
version       = 3.27.0-beta4.17413
fw_reference  = unknown
trackingnumber = 00e3f4124e02
serialnumber  = 0124
guestlogin    = guest
questpwd      = *****
adminlogin    = admin
adminpwd      = *****
timezone      = UTC
time          = 2011/07/21.15:01:45
localtime     = 2011/07/21.15:01:45
admin/
web/
http          = on
httpport      = 80
https         = off
Press any key to continue or CTRL+C to stop.

```

You will know whether the system has finished showing all the information when the equipment prompt reappears: **drn />**.

As with the *download* command, it is useful to save the information in a *.txt* file using the method described above.

5- Obtaining the equipment statistics

The equipment statistics list is shown through the command **stats**.

```

Telnet 172.16.50.38
drn /> stats
main/
uptime        = 0d00:48:49.131
time          = 2011/07/21.15:13:34
localtime     = 2011/07/21.15:13:34
temperature    = 70 <C> / 158 <F>
memory_usage  = 15
cpu_usage     = 7
last_min_cpu_usage = 6
lan/
port[]/
[port] name   in_octets out_octets in_frames out_frames errors link
1   swt-port 1317787 1259589 13352    1697    246    up
2   swt-port 0        0        0        0        0        down
3   swt-port 0        0        0        0        0        down
4   swt-port 0        0        0        0        0        down
5   swt-port 0        0        0        0        0        down
6   swt-port 0        0        0        0        0        down
7   swt-port 0        0        0        0        0        down
8   swt-port 0        0        0        0        0        down
vif[]/
Press any key to continue or CTRL+C to stop.

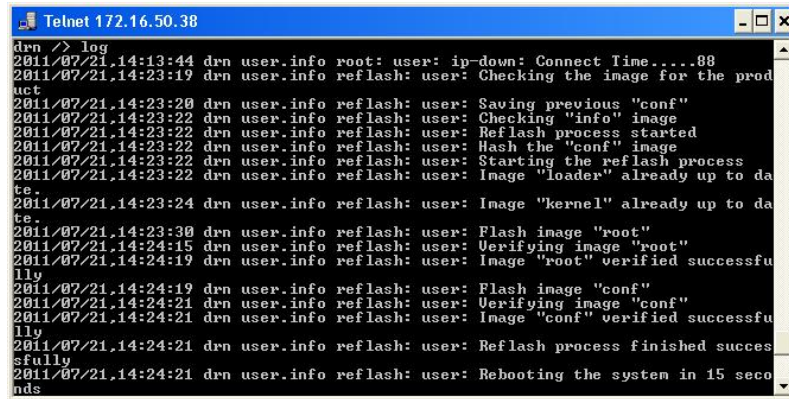
```

Like the previous commands, if the information to be displayed exceeds the edges of the window, it will stop and wait for the user to press a key to continue.

Remember to save the information in a *.txt* file, as indicated above.

6- Obtaining events recorded in the equipment

The **log** command allows you to consult the events taking place in the equipment which have been recorded in the non-volatile memory due to their importance.



```

Telnet 172.16.50.38
drn /> log
2011/07/21,14:13:44 drn user.info root: user: ip-down: Connect Time....88
2011/07/21,14:23:19 drn user.info reflash: user: Checking the image for the prod
uct
2011/07/21,14:23:20 drn user.info reflash: user: Saving previous "conf"
2011/07/21,14:23:22 drn user.info reflash: user: Checking "info" image
2011/07/21,14:23:22 drn user.info reflash: user: Reflash process started
2011/07/21,14:23:22 drn user.info reflash: user: Hash the "conf" image
2011/07/21,14:23:22 drn user.info reflash: user: Starting the reflash process
2011/07/21,14:23:22 drn user.info reflash: user: Image "loader" already up to da
te.
2011/07/21,14:23:24 drn user.info reflash: user: Image "kernel" already up to da
te.
2011/07/21,14:23:30 drn user.info reflash: user: Flash image "root"
2011/07/21,14:24:15 drn user.info reflash: user: Verifying image "root"
2011/07/21,14:24:19 drn user.info reflash: user: Image "root" verified successfu
lly
2011/07/21,14:24:19 drn user.info reflash: user: Flash image "conf"
2011/07/21,14:24:21 drn user.info reflash: user: Verifying image "conf"
2011/07/21,14:24:21 drn user.info reflash: user: Image "conf" verified successfu
lly
2011/07/21,14:24:21 drn user.info reflash: user: Reflash process finished succes
sfully
2011/07/21,14:24:21 drn user.info reflash: user: Rebooting the system in 15 seco
nds

```

Remember to save the information in a .txt file, as indicated above.

7- Obtaining events taking place in the equipment in real time

The **log all** command allows users to consult the events taking place in the equipment in real time.

The list of events will continuously be updated until the user presses the **enter** key.

Remember to save the information in a .txt file, as indicated above.

8- Example of a list showing the status of a equipment obtained with the get command and saved in a .txt file

```

drn login: guest
Password:

drn /> get
/
  main/
    hostname      = drn
    location      = unknown
    contact       = unknown
    product       = 4DRNC00100E00DA
    version       = 3.27.0-beta4.17413
    fw_reference  = unknown
    trackingnumber = 00e3f4124e02
    serialnumber  = 0124
    guestlogin    = guest
    guestpwd      = *****
    adminlogin    = admin
    adminpwd      = *****
    timezone      = UTC
    time          = 2011/07/21,15:36:44
    localtime     = 2011/07/21,15:36:44
  admin/
    web/
      http        = on
      httpport    = 80
      https       = off
      httpsport   = 443
      cert        = empty
      privatekey  = empty
      privatekeypwd = *****
    cli/
      log = off
    reset/
      enable = off
      period = 1
  lan/
    port[]/
      [port] name      enable vlan_function mode vid vid_acl
      -----
      1      swt-port on   edge          auto 1    auto
      2      swt-port on   edge          auto 1    auto
      3      swt-port on   edge          auto 1    auto
      4      swt-port on   edge          auto 1    auto
      5      swt-port on   edge          auto 1    auto
      6      swt-port on   edge          auto 1    auto
      7      swt-port on   edge          auto 1    auto
      8      swt-port on   edge          auto 1    auto
    vif[]/
      [vif] static vid ip          mask          description
      -----
      1      off    1    192.168.0.1 255.255.255.0 vlan_name
  stp/
    enable      = off
    version     = rstp
    priority    = 32768
    max_age     = 20.000000000
    hello_time  = 2.000000000
    forward_delay = 15.000000000
    tx_hold_count = 6
    port[]/
      [port] priority cost    edge ptp
      -----
      1      128      200000 auto auto
      2      128      200000 auto auto
      3      128      200000 auto auto
      4      128      200000 auto auto
      5      128      200000 auto auto
      6      128      200000 auto auto
      7      128      200000 auto auto
      8      128      200000 auto auto
  wan/
    cell0/
      enable      = off
      primsim     = SIMB
      dns_req     = on
      maxretries  = 6
      maxtoconnect = 6
      alarm_lowcov_level = -105

```

```

alarm_lowcov_period = 300
maxinsec             = 0
dualsimenable        = off
pin1                  = *****
pin2                  = *****
apn                   = ipfija.vodafone.es
force_home           = off
auth                  = pap
login                 = vodafone
passwd                = *****
minrxpower            = -113
defroute              = on
simb/
  pin1                = *****
  pin2                = *****
  apn                  = ac.vodafone.es
  force_home          = off
  auth                 = pap
  login                = vodafone
  passwd               = *****
  minrxpower          = -113
  defroute             = on
dyn/
  enable              = off
  service              = dyndns
  host                 =
  login                =
  passwd               =
  interval             = 86400
pingkeep/
  remoteip             = 0.0.0.0
  remoteip2            = 0.0.0.0
  freq                 = 5
  bytes                = 1
  count                = 2
  action               = none
  strict               = on
tunnel/
  tunnel[]/
    [tunnel] iface description type ip      source remote_gw
remote_net
enable
-----
---
-----
      1          tun1          gre  vlan1 vlan1  172.16.50.43 any
on
qos/
qos2/
  weightfair_enable = on
  priority[]/
    [priority] queue
    -----
    0          medium
    1          medium
    2          medium
    3          medium
    4          medium
    5          medium
    6          medium
    7          medium
  dscp[]/
    [dscp] queue
    -----
    0          medium
    8          medium
    16         medium
    24         medium
    32         medium
    40         medium
    48         medium
    56         medium
  port[]/
    [port] priority use_ieee8021p use_dscp
    -----
    1          0      on          off
    2          0      on          off
    3          0      on          off
    4          0      on          off
    5          0      on          off
    6          0      on          off
    7          0      on          off
    8          0      on          off
qos3/
  classify/
    def_priority = medium
routing/

```

```

static/
st_rules[]/
[st_rules] dest gateway service if
descr
-----
1 128.127.0.0/255.255.0.0 172.16.50.254 any vlan1
rip/
enable = on
advertised_policy = permit
filter/
local/
policy = accept
cell0/
policy = accept
vlan/
policy = accept
dhcps/
profiles[]/
[profiles] name lease dns1 dns2 wins domain tftp
bootfile
-----
1 profile 5000 0.0.0.0 0.0.0.0 0.0.0.0 usyscom.com
192.168.0.
1 bootfile
servers[]/
[servers] enable interface firstip lastip max_leases
mask gateway profile
-----
1 off 192.168.0.10 192.168.0.254 100
255.25
5.255.0 192.168.0.1 profile
vrrp/
enable = off
advert_int = 1
if = vlan1
vid = 1
priority = 100
vip = 192.168.0.1
vmask = 255.255.255.0
preempt = on
preempt_delay = 0
auth_method = none
auth_passwd = passwd02
pingkeep/
remoteip = 0.0.0.0
gateway = 0.0.0.0
freq = 5
action = none
vpn/
traffic/
rules[]/
[rules] tunnel_id local_net remote_gw
remote_net
iskamp saname enable valid_in
-----
1 ipsec1 172.16.50.0/255.255.255.0 77.211.25.76
172.17.90.0
/255.255.255.0 IKE1 TR1 on cell0-0
ike/
ownidtype = none
ownidvalue =
nat_t = off
dpd_delay = 10
dpd_retry = 10
dpd_maxfail = 3
dpd_invcookies = off
policy[]/
[policy] name use_fqdn fqdn_value passive exchange cipher_alg
hash_a
lg auth_method dh_group lifetime descr enable
-----
1 IKE1 disabled off main des md5
pre_shared_key modp1024 86400 IKE1 on
pshkeys/

```



```

peer_keys[]/
[peer_keys] peer_ip      key      enable
-----
1          77.211.25.76 12345 on

ipsec/
sa[]/
[sa] tunnel_id protocol cipher_alg hash_alg pfs  lifetime mode
-----
1      TR1       esp       des       hmac_md5 none 6000   tunnel

ntp/
enable = off
authkeys[]/
[authkeys] keynumber key
-----
1          1          xxxxxxxx

client/
broadcastenable = off
server[]/
[server] ip            type      minpoll maxpoll authenable authkey

lowt
raffic
-----
---
-----
1          192.168.0.1 unicast 5      10      off      1

off

snmp/
enable = off
trapenable = off
trap_v1_agent_addr = none
community[]/
[community] name      access
-----
1          public ro

traps/
cell_linkup = off
cell_covlow = off
cell_covhigh = off

access/
tacacsplus/
server1_ip = 0.0.0.0
server2_ip = 0.0.0.0
encrypted = on
shared_key = *****

console/
method = local

web/
method = local
local = on

telnet/
method = local
local = on

security/
port[]/
[port] type max_addresses max_action
-----
1      none 10              replace
2      none 10              replace
3      none 10              replace
4      none 10              replace
5      none 10              replace
6      none 10              replace
7      none 10              replace
8      none 10              replace

drn />

```