



---

## MV PLC NODE TYPE ZBP-1



### USER GUIDE

V01 - May 2019

M0ZBP11905lv01

ZIV  
Carrer de les Ciències, 149-151  
08908 L'Hospitalet de Llobregat  
Barcelona-Spain

Tel.: +34 933 490 700  
Fax: +34 933 492 258  
Mail to: [ziv@zivautomation.com](mailto:ziv@zivautomation.com)

[www.zivautomation.com](http://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 device or even injury to the personnel handling it.



### **NOTE:**

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

## TABLE OF CONTENTS

	<b>Page</b>
<b>1</b>	<b>INTRODUCTION</b> <span style="float: right;"><b>5</b></span>
1.1	GENERAL <span style="float: right;">5</span>
1.2	CONNECTION PROTOCOL <span style="float: right;">5</span>
1.2.1	PLUG&PLAY connection phase <span style="float: right;">6</span>
1.2.2	Route search and selection phase <span style="float: right;">6</span>
1.3	OFDM PARAMETERS <span style="float: right;">7</span>
1.4	TECHNICAL CHARACTERISTICS <span style="float: right;">10</span>
1.4.1	PLC node characteristics <span style="float: right;">10</span>
1.4.2	PLC node interfaces <span style="float: right;">10</span>
1.4.3	PLC transmission characteristics <span style="float: right;">10</span>
1.4.4	PLC node management <span style="float: right;">11</span>
1.4.5	Additional services <span style="float: right;">11</span>
1.4.6	Accessories <span style="float: right;">11</span>
1.4.7	Certifications <span style="float: right;">12</span>
1.4.8	Mechanical characteristics <span style="float: right;">12</span>
1.4.9	Operating conditions <span style="float: right;">12</span>
1.4.10	Conditions of transport and storage <span style="float: right;">13</span>
1.5	WARNINGS <span style="float: right;">14</span>
1.5.1	Warnings before installing <span style="float: right;">14</span>
1.5.2	Device safety considerations <span style="float: right;">15</span>
<b>2</b>	<b>MECHANICAL AND ELECTRICAL CHARACTERISTICS</b> <span style="float: right;"><b>16</b></span>
2.1	POWER SUPPLY <span style="float: right;">21</span>
2.2	ETHERNET CONNECTOR <span style="float: right;">21</span>
2.3	OPTICAL INDICATIONS <span style="float: right;">24</span>
<b>3</b>	<b>ACCESS TO THE DEVICE</b> <span style="float: right;"><b>26</b></span>
3.1	CONSOLE <span style="float: right;">26</span>
3.2	HTTP SERVER OF THE DEVICE <span style="float: right;">26</span>

	<b>Page</b>
<b>4</b>	<b>CONFIGURATION AND MANAGEMENT</b> <span style="float: right;"><b>28</b></span>
4.1	GENERAL PARAMETERS <span style="float: right;">30</span>
4.1.1	Device identification <span style="float: right;">30</span>
4.1.2	Access control <span style="float: right;">31</span>
4.1.3	Others <span style="float: right;">32</span>
4.2	ADMINISTRATION CONFIGURATION <span style="float: right;">32</span>
4.3	LAN CONFIGURATION <span style="float: right;">33</span>
4.3.1	Odfm configuration <span style="float: right;">33</span>
4.3.2	Vlan configuration <span style="float: right;">35</span>
4.4	ROUTING CONFIGURATION <span style="float: right;">37</span>
4.4.1	Static routes configuration <span style="float: right;">37</span>
4.4.2	DNS server configuration <span style="float: right;">39</span>
4.5	SNMP CONFIGURATION <span style="float: right;">40</span>
4.6	ACCESS CONFIGURATION <span style="float: right;">42</span>
4.7	REBOOT <span style="float: right;">44</span>
4.8	CODE REFLASH <span style="float: right;">44</span>
4.9	CONFIGURATION FILE <span style="float: right;">45</span>
4.9.1	Upload (from the computer to the device) <span style="float: right;">45</span>
4.9.2	Download (from the device to the computer) <span style="float: right;">46</span>
<b>5</b>	<b>STATISTICS</b> <span style="float: right;"><b>47</b></span>
5.1	GENERAL DATA <span style="float: right;">48</span>
5.2	STATISTICS RELATED TO LAN <span style="float: right;">49</span>
5.3	STATISTICS RELATED TO ROUTING <span style="float: right;">49</span>
5.4	STATISTICS RELATED TO ADAPTATION PARAMETERS <span style="float: right;">50</span>
5.5	STATISTICS RELATED TO LOCAL OFDM ROUTES <span style="float: right;">51</span>
5.6	STATISTICS RELATED TO REMOTE OFDM ROUTES <span style="float: right;">52</span>
	<b>APPENDIX A</b>
	<b>DATA STRUCTURE IN CLI</b> <span style="float: right;"><b>53</b></span>

## 1 INTRODUCTION

### 1.1 GENERAL

The ZBP-1 allows high data rate transmission (up to 28.8 Mbit/s) over medium-voltage power lines, in a frequency range selectable by the user (from 2 to 14 MHz).

To achieve this goal, the system makes use of an Orthogonal frequency-division multiplexing (**OFDM**) modulation.

The bit stream is dynamically assigned to a set of carriers of different frequencies, each of which carries information modulated in QPSK or QAM.

The channel is constantly evaluated in such a way that the carriers that are affected by noise or interferences can automatically reduce its base modulation or even not be used at all. In addition, to get a more reliable communication, the Turbo Code ratio can also change.

### 1.2 CONNECTION PROTOCOL

The ZBP-1 can operate as a level 3 router for IPv4 or as a level 2 switch (bridge) between the Ethernet interface and the PLC interface, and includes support for IEEE802.1Q (VLANs).

The connection protocol between ZBP-1 nodes is based on the search of routes for **IP/MAC addresses** and consists of two distinct phases: the **PLUG&PLAY connection** phase and the **Route search and selection** phase, which are described below.

The MAC medium access layer is based on **IEEE 802.15.4** that provides access to a shared medium, security and automatic packet retrieval.

The routing PLC protocol used is **LOADnG**, due to its reactive nature and its adaptation to IEEE 802.15.4.

The LOADnG protocol is a dynamic routing system that easily adapts to the topology changes of the medium using the redundant paths and the overreaching capacity of the device.

# ZBP-1

## 1.2.1 PLUG&PLAY connection phase

The first phase of the connection between ZBP-1 nodes, called *PLUG&PLAY connection*, is the starting and identification of all neighbouring nodes (NEIGHBORS) by the local node, and it is the phase that allows obtaining the optimum data rate and power value that the local node must use to communicate with each of its neighbours.

Each ZBP-1 must be identified in a specific and unambiguous way within the network in which it is located by means of its device identification number (*Local ID* parameter) and it must also have its IP address (*IP address* parameter) and mask (*Mask* parameter).

Once programmed, the local ZBP-1 starts, after the start up, the transmission of specific broadcast packets whose feedback will allow it to identify the different neighbouring ZBP-1 nodes, as well as to establish the optimum operating values for each of them.

These values are the **power value** and the **data rate in bit/s** (associated to the type of modulation and operation mode) for each of the carriers, which must use the local node in order to transmit packets to neighbouring nodes.

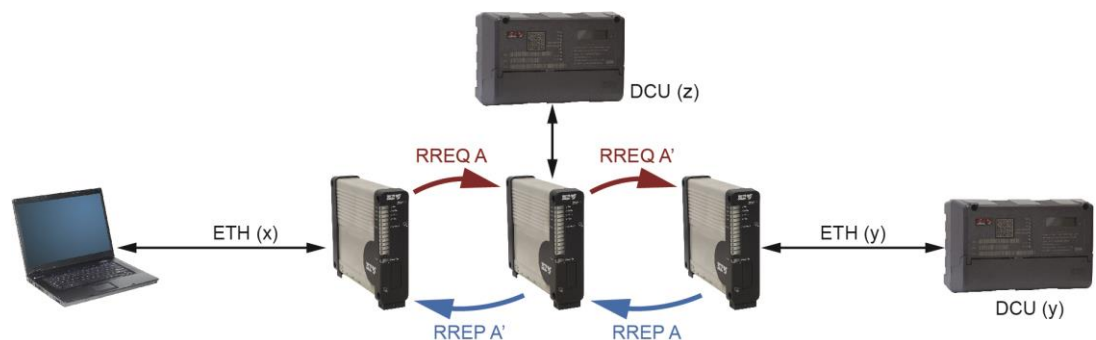
As a guide, section 1.3, *OFDM parameters*, give some data rate values.

## 1.2.2 Route search and selection phase

After the *PLUG&PLAY Connection*, the originator node starts both the route search and route selection phases.

The route search procedure for IP/MAC addresses is summarized in FIGURE 1.

FIGURE 1 Route search procedure



As shown in FIGURE 1, once the originator PLC node receives a search request for a given IP/MAC address from the Ethernet (arp) port, it sends a broadcast message, called **RREQ**, via the PLC port.

This search message reaches all neighbouring devices. PLC nodes that do not know the address will retransmit the RREQ message. On the contrary, the PLC node that has the IP/MAC address into its local IP/MAC table, will respond the originator node by means of a unicast message, called **RREP**, using the same path as the one used by the RREQ message.

The route is formed when the RREP answering messages arrive at the originator node.

Of all the routes formed, the originator node will choose the optimal route for the transmission. The route chosen will remain valid while in use. If it is no longer used after two minutes (this value is programmable), the route will be deleted, and it will be necessary to establish a new route to start communication.

In each segment of the route, the corresponding node uses the optimum **data rate in bit/s** and **power** value obtained from the PLUG&PLAY connection.

## 1.3 OFDM PARAMETERS

As a guide for the user, this section shows tables with values of data rates in bit/s that the PLC node automatically selects for each of the carriers, depending on the noise measured in the line.

It also indicates the values of bandwidth and frequency range that the user can configure from the management system.

# ZBP-1

Ofdm mode	Turbo Code	Repetition	Data rate with QPSK	Data rate with 16-QAM
0	8/9	NO	9.6 Mbps	19.2 Mbps
1	1/3	NO	3.2 Mbps	6.4 Mbps
2	1/3	YES	640 Kbps	1.28 Mbps
3	3/4	NO	7.2 Mbps	14.4 Mbps

**TABLE 1** Data rates for BW=6 MHz (the PLC node automatically selects this value for each of the carriers)

Ofdm mode	Turbo Code	Repetition	Data rate with QPSK	Data rate with 16-QAM
0	8/9	NO	2.4 Mbps	4.8 Mbps
1	1/3	NO	0.8 Mbps	1.6 Mbps
2	1/3	YES	160 Kbps	320 Kbps
3	3/4	NO	1.8 Mbps	3.6 Mbps

**TABLE 2** Data rates for BW=1.5 MHz (the PLC node automatically selects this value for each of the carriers)

Ofdm mode	Turbo Code	Repetition	Data rate with QPSK	Data rate with 16-QAM
0	8/9	NO	19.2 Mbps	-
1	1/3	NO	6.4 Mbps	12.8 Mbps
2	1/3	YES	1.28 Mbps	2.56 Mbps
3	3/4	NO	14.4 Mbps	28.8 Mbps

**TABLE 3** Data rates for BW=12 MHz (the PLC node automatically selects this value for each of the carriers)





# ZBP-1

Modulation	Modulation type
0	QPSK
1	16-QAM

TABLE 4 Modulation type (the PLC node automatically selects this value for each of the carriers)

Tone Mask	Repetition	BW (1.5 MHz)	BW (6 MHz)	BW (12 MHz)
<i>Low band</i>	NO	-	2 ÷ 8 MHz	-
<i>High band</i>	YES	2 ÷ 3.5 MHz	8 ÷ 14 MHz	-
<i>Full band</i>	NO	-	-	2 ÷ 14 MHz

TABLE 5 Frequency spectrum (the user programs this value)

Compact Band	Bandwidth (BW)
OFF	6 MHz
ON	1.5 MHz

TABLE 6 Bandwidth (BW) (the user programs this value)

## 1.4 TECHNICAL CHARACTERISTICS

### 1.4.1 PLC node characteristics

The **software/firmware** services offered by the ZBP-1 are:

- possibility to operate as a **level 3 router** for IPv4
- or as a **level 2 switch (bridge)** between the Ethernet interface and the PLC interface,
- and support for **IEEE802.1Q** (Management of up to 8 **VLANs**).

### 1.4.2 PLC node interfaces

- 1 Ethernet (Eth) port in 10/100Base-Tx configuration with RJ-45 female connector. It is used for both user data and node configuration (HTTP, Telnet or SSH).
- 1 BNC (PLC) female connector for RG-58 cable. It is used for line connection.
- 1 DB9 female (COM) connector as a service port for the configuration of the equipment through a *CLI* (Command Line Interface) console.

### 1.4.3 PLC transmission characteristics

- PLC routing protocol: **LOADnG**
- The connection protocol between ZBP-1 nodes is based on the search of routes for **IP/MAC addresses** and consists of two distinct phases: the **PLUG&PLAY connection** phase and the **Route search and selection** phase.
- User selectable route lifetime.  
The minimum value is 5 s. The factory value is 120 s.
- Frequency range and bandwidth (user selectable) between:

Tone Mask	BW (1.5 MHz)	BW (6 MHz)	BW (12 MHz)
<i>Low band</i>	-	2 ÷ 8 MHz	-
<i>High band</i>	2 ÷ 3.5 MHz	8 ÷ 14 MHz	-
<i>Full band</i>	-	-	2 ÷ 14 MHz

# ZBP-1

- Transmission data rate of up to 28.8 Mbit/s.  
The ZBP-1 automatically selects the data rates for each of the carriers, depending on the noise measured in the line. See TABLE 1 to TABLE 3.
- OFDM modulation with 380 useful carriers. Depending on the noise measured on the line, the ZBP-1 can automatically cancel the affected carriers.
- QPSK/16-QAM modulation independently applied to each carrier.  
The ZBP-1 automatically selects it for each of the carriers, depending on the noise measured in the line.
- Turbo code with FEC (Forward Error Correction) of ratio 8/9, 1/3 and 3/4.  
The ZBP-1 automatically selects the ratio of the Turbo Code for each of the carriers, depending on the noise measured in the line.
- Output power between 0 and 15.  
The ZBP-1 automatically selects this value, depending on the signal measured in the line.
- Distance of up to 5 km.

## 1.4.4 PLC node management

- The ZBP-1 can be managed locally and remotely, through a *CLI* (Command Line Interface) console or through a built-in web server (HTTP/HTTPS), SSH and Telnet server.

## 1.4.5 Additional services

- DHCP client.
- DNS server.
- TACACS+ client.
- SNMP (SNMPv1, SNMPv2c and SNMPv3) agent.

## 1.4.6 Accessories

- Screws and fixing accessories for DIN rail installation.

## 1.4.7 Certifications

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

## 1.4.8 Mechanical characteristics

- Dimensions: Height: 150 mm; Width: 40 mm; Depth: 177 mm.  
See FIGURE 2.
- Weight: 539 g.
- Wall mount. The device has 4 fixing holes suitable for standard M4 screws.  
See FIGURE 3.  
DIN rail mounting by means of optional accessory.
- IP protection level: IP 2xB.
- Material: varnishing (RAL 9006) aluminium 6060 T5 alloy and Fireproof (UL 94 V0) STAREX ABS VH-0800 (RAL 7024) plastic.

## 1.4.9 Operating conditions

- Power supply: 48 V<sub>DC</sub> isolated (19-72V<sub>DC</sub>).  
The device is protected against polarity inversion.
- Minimum power consumption at 48 V<sub>DC</sub>: 6 W
- Maximum power consumption at 48 V<sub>DC</sub>: 48 W
- Temperature range: -25°C to +60°C.
- Relative humidity not greater than 95%, in accordance with IEC 721-3-3 class 3K5 (climatogram 3K5).
- R.F. emissions: in accordance with EN 55022 standard.
- Dielectric strength: in accordance with EN 60255-5 standard.

- Electromagnetic compatibility.
  - Electrostatic discharge immunity test:  
in accordance with EN 61000-4-2 standard.
  - Radiated, radio-frequency, electromagnetic field immunity test:  
in accordance with EN 61000-4-3 standard.
  - Electrical fast transient/burst immunity test:  
in accordance with EN 61000-4-4 standard.
  - Surge immunity test:  
in accordance with EN 61000-4-5 standard.
  - Immunity to conducted disturbances, induced by radio-frequency fields:  
in accordance with EN 61000-4-6 standard.
  - Power frequency magnetic field immunity test:  
in accordance with EN 61000-4-8 standard.
  - Damped oscillatory wave immunity test:  
in accordance with EN 61000-4-18 (EN 61000-4-12) standard.
  - Voltage dips, short interruptions and voltage variations on d.c. input power port  
immunity tests:  
in accordance with EN 61000-4-29 standard.
  
- Mechanical operating conditions.
  - Vibration in accordance with ETSI EN 300019-2-2 standard.
  - Shock in accordance with ETSI EN 300019-2-2 standard.

## 1.4.10 Conditions of transport and storage

- Temperature range: -40°C to +70°C in accordance with EN 60870-2-2 standard.

## 1.5 WARNINGS

### 1.5.1 Warnings before installing



- !
1. The installation of the ZBP-1 in Secondary Substations is generically subject to the fulfilment of all the safety measures and prevention of risks established for this type of work by the electricity company that will use these devices and the Safety standards (EN 50110).
  2. In order to install and handle the ZBP-1 the following points must be complied with:
    - Only qualified personnel appointed by the electricity company that owns the installation should carry out the installation and handling of the ZBP-1.
    - The environment in which it is to operate should be suitable for the ZBP-1, fulfilling all the conditions indicated in section 1.4.9.
  3. ZIV will not accept responsibility for any injury to persons, installations or third parties, caused by the non-fulfilment of points 1 and 2.

## 1.5.2 Device safety considerations



- ! 1. Earth connection must be made before connecting any other power-supply cable.
- 2. ZIV will not accept responsibility for any injury to persons or third parties, caused by the non-fulfilment of point 1.

- ! 1. The device contains components sensitive to static electricity, the following must be observed when handling it:
  - Personnel appointed to carry out the installation and maintenance of the ZBP-1 must be free of static electricity. An anti-static wristband and/or heel connected to earth should be worn.
  - The room housing the ZBP-1 must be free of elements that can generate static electricity. If the floor of the room is covered with a carpet, make sure that it is anti-static.
- 2. ZIV will not accept responsibility for any damage to the device caused by the non-fulfilment of point 1.

## 2 MECHANICAL AND ELECTRICAL CHARACTERISTICS

FIGURE 2 shows the general dimensions in mm of the ZBP-1.

The chassis is ready for wall mount or DIN rail mounting by means of optional accessory.

The ZBP-1 has 4 fixing holes suitable for standard M4 screws, the arrangement of which can be seen in FIGURE 3.

FIGURE 4 shows the position of the slit for the placement of the DIN rail fixing accessory. The installation procedure can be seen in the attached detailed drawings.

FIGURE 2 Overall dimensions in mm of the ZBP-1





# ZBP-1

FIGURE 3 Fixing holes detail

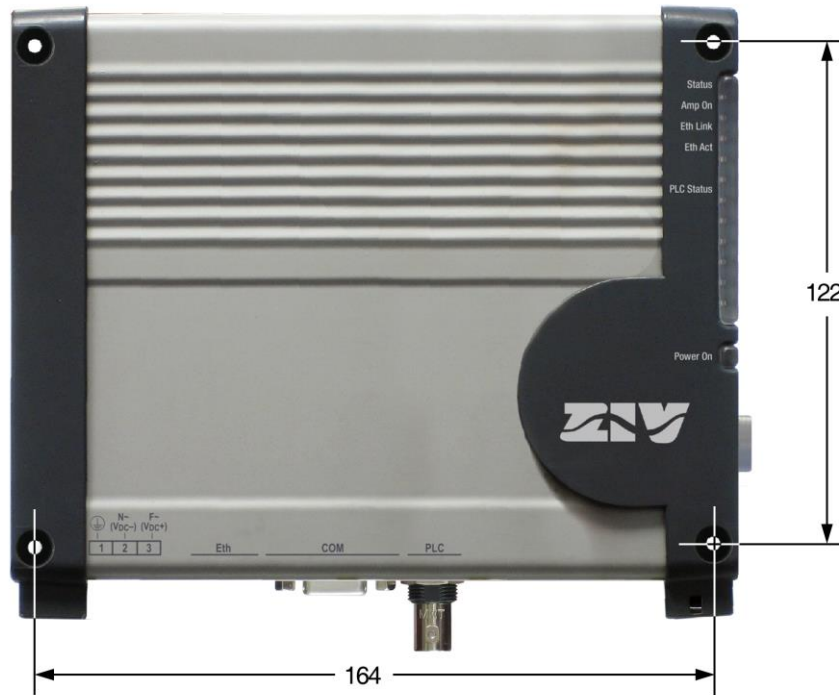
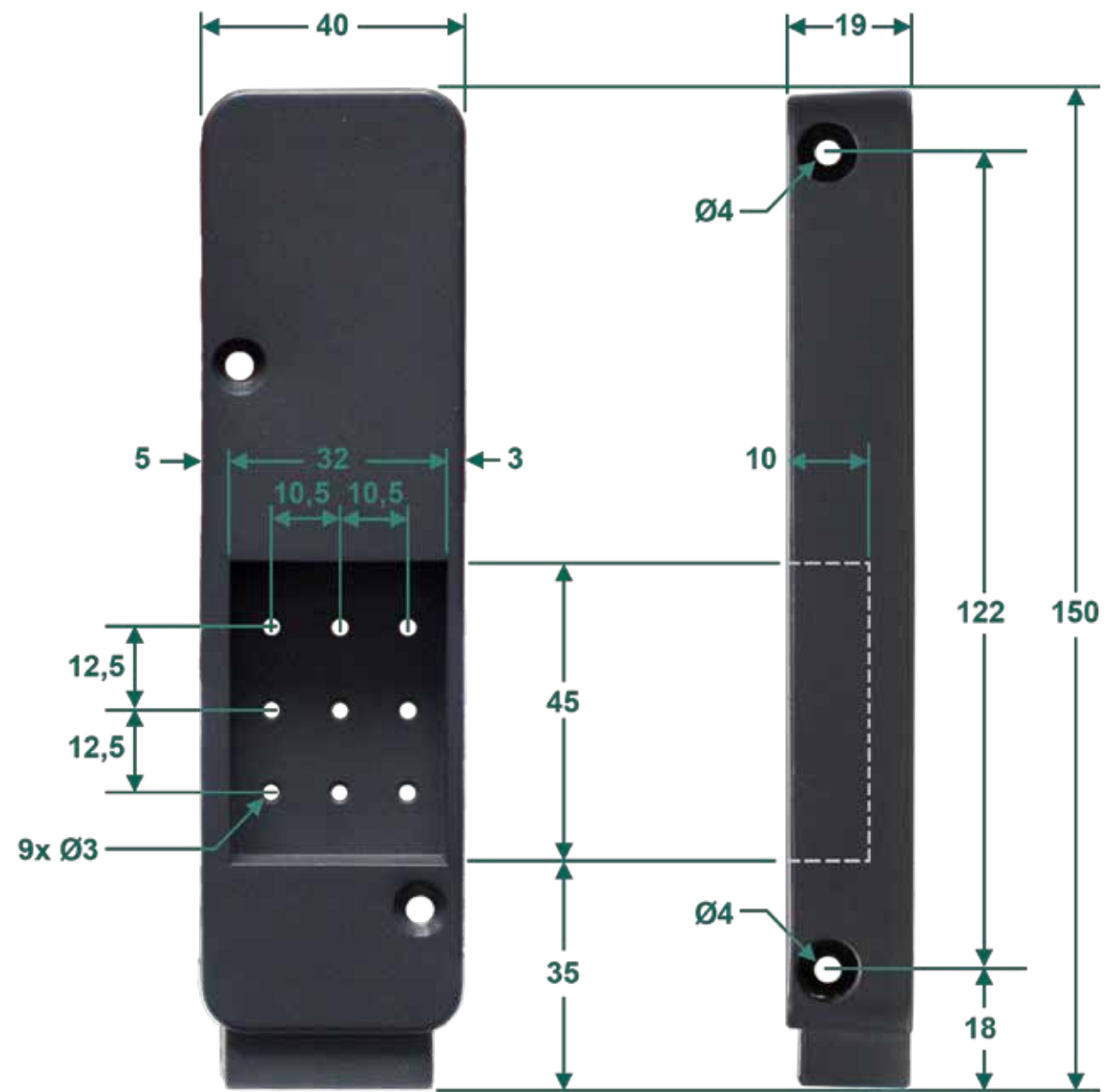


FIGURE 4 Detail of the slit for fixing the DIN rail optional accessory






Rear cover dimensions



Equipment without accessory for DIN rail



Equipment with accessory for DIN rail

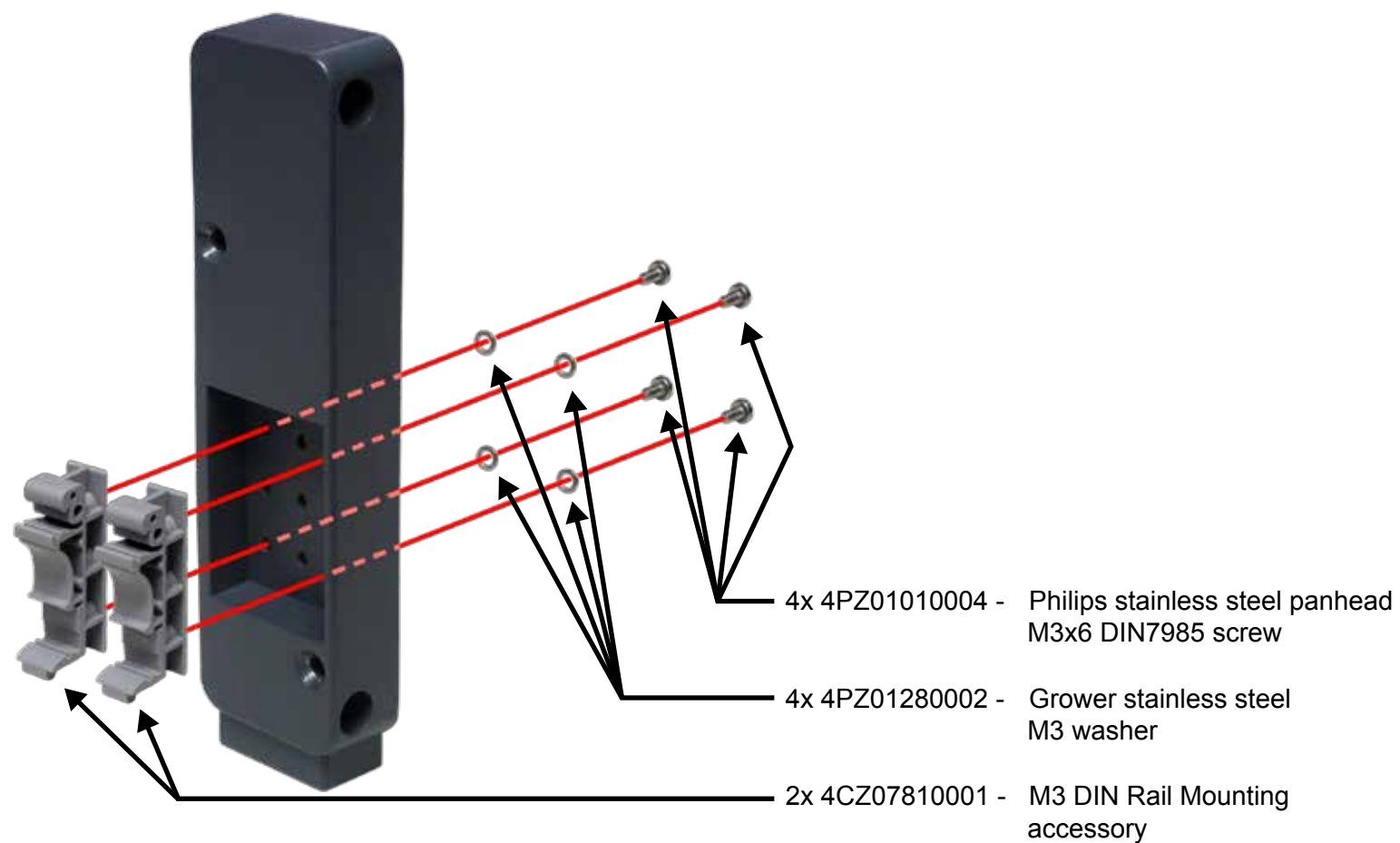
Pertenece a: ZBP-1						Cód. Prod.	Rev.
						-	0
Fecha	Realizado	V° B°	Comprobado	V° B°	Aprobado	V° B°	Archivo
08-02-2017	J. F. Gil						MGZBP10200
						Siglas	Hoja
<b>INSTALLATION PROCESS OF THE ACCESSORY FOR DIN RAIL (1/2)</b>						<b>ZBP-1</b>	1/3



**Step 1 :** Remove the screws and extract the rear cover.




**Step 2 :** Remove the adhesive strip that secures the holes for screwing the DIN rail accessory.



**Step 3 :** Screw the DIN rail accessory to the rear cover as is shown in the figure.



**Step 4 :** Place the rear cover, by securing it with the screws removed in step 1.

Pertenece a: ZBP-1					Cód. Prod.		Rev.	
					-		0	
Fecha	Realizado	V° B°	Comprobado	V° B°	Aprobado	V° B°	Archivo	
08-02-2017	J. F. Gil						MGZBP10300	
							<b>INSTALLATION PROCESS OF THE ACCESSORY FOR DIN RAIL (2/2)</b>	
							Siglas	Hoja
							<b>ZBP-1</b>	2/3

## Inserting in the DIN rail



**Step 1 :** Fit the upper claws of the fastening piece into the upper profile of the DIN rail.



**Step 2 :** Straighten the equipment by pivoting it on the upper claws of the clamp until the lower claws fit into the lower profile of the DIN rail.

## Removing from the DIN rail




**Step 1 :** Using a screwdriver, release the lower claws of the fastening piece.

**Step 2 :** Pull slightly from the equipment, swinging it over the upper nails.



**Step 3 :** Remove fully the equipment by pulling it upwards.

Pertenece a: ZBP-1					Cód. Prod.		Rev.	
					-		0	
Fecha	Realizado	V° B°	Comprobado	V° B°	Aprobado	V° B°	Archivo	
08-02-2017	J. F. Gil						MGZBP10100	
		<b>INSTALL AND UNINSTALL IN DIN RAIL</b>					Siglas	Hoja
							<b>ZBP-1</b>	3/3

# ZBP-1

## 2.1 POWER SUPPLY

EI ZBP-1 is powered with a nominal voltage of 48 V<sub>DC</sub> isolated (19-72 V<sub>DC</sub>), through the connector shown in FIGURE 5.

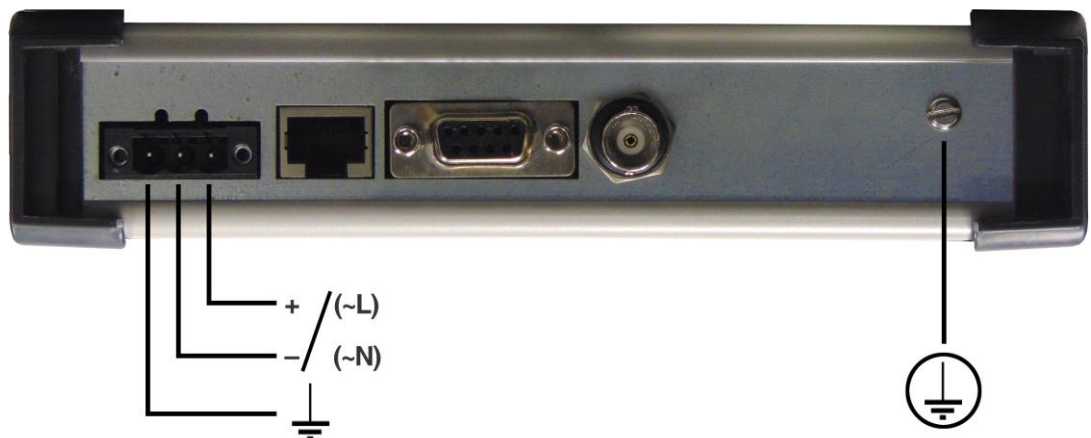
The female connector supplied with the device is suitable for rigid or flexible conductors of up to 2.5 mm<sup>2</sup>.



Earth connection must be made, see FIGURE 5, before connecting any other power-supply cable.

The device is protected against polarity inversion.

FIGURE 5 Location of the power supply connector and earth terminal in the ZBP-1



## 2.2 ETHERNET CONNECTOR

Next to the power-supply connector, there is the Ethernet connector, see FIGURE 5. The said connector corresponds to a 10/100Base-Tx interface with RJ-45 connector.

In the 10/100Base-Tx port, the cable used to perform the corresponding connection should be an unshielded twisted 4 pair category five cable (UTP-5) with 8-pin RJ-45 connector. The cable length should not be more than 100 m.



# ZBP-1

The UTP-5 cable is made up of eight copper wires that form the four twisted pairs, covered in different coloured insulating material. FIGURE 6 shows the colour of the wires that make up each one of the pairs, according to ANSI/TIA/EIA-568-A standard.

**FIGURE 6** Unshielded twisted pair category five cable (UTP-5) with RJ-45 connector according to ANSI/TIA/EIA-568-A standard

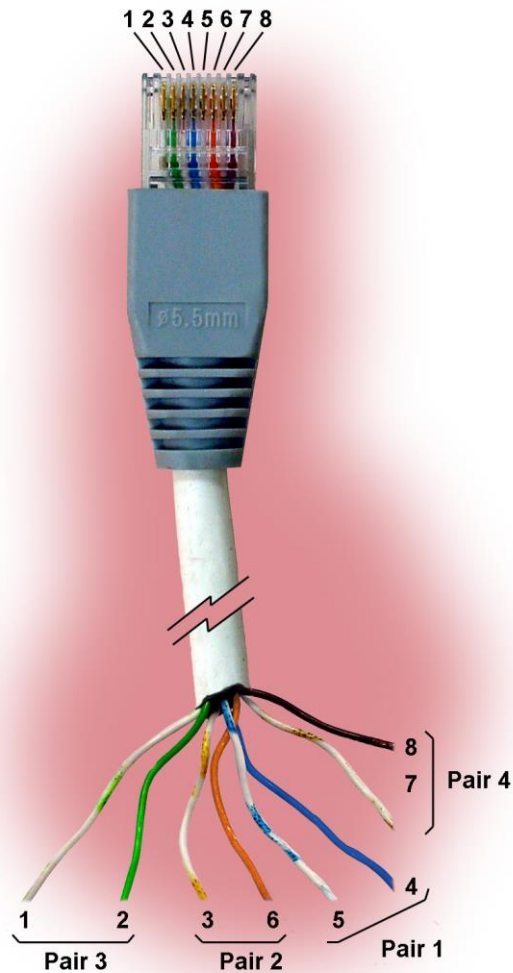
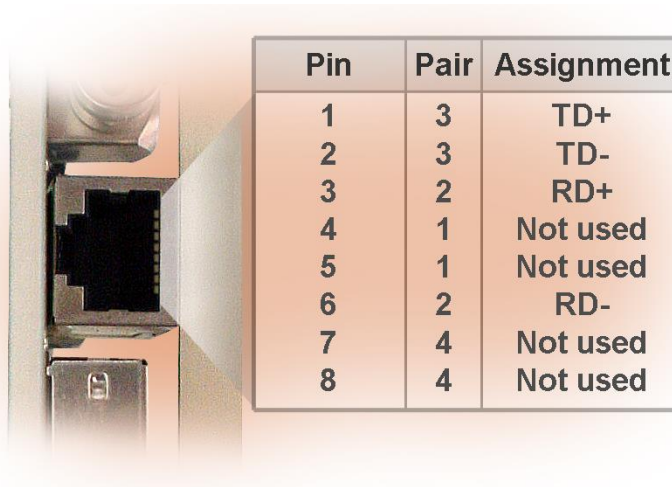


FIGURE 7 shows the use of each one of the pins of the RJ-45 connector, as well as the pair it belongs to according to ANSI/TIA/EIA-568-A standard, in the 10/100Base-Tx LAN interface.

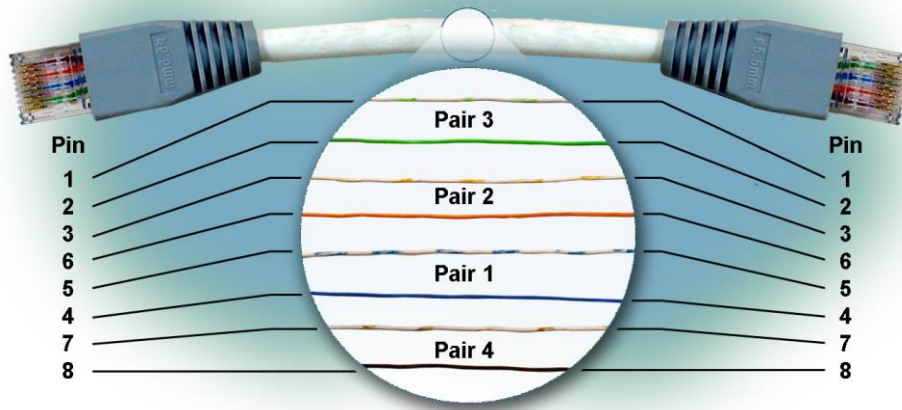
# ZBP-1

FIGURE 7 Signals of the RJ-45 connector in the 10/100Base-Tx interface



Straight-through cables must be used, see FIGURE 8, where the 4 pairs correspond at both ends of the cable.

FIGURE 8 Straight-through cable



# ZBP-1

## 2.3 OPTICAL INDICATIONS

The ZBP-1 has different LEDs on the front plate, see FIGURE 9, the description of which is given below.

FIGURE 9 Detail of the different LEDs of the ZBP-1





# ZBP-1

LED Power On	<b>Green.</b> It is permanently lit when the device is powered with an external power-supply voltage.
LED Status	<b>Two-coloured.</b> It illuminates in <b>red</b> when the digital modem unit is starting.  It illuminates in <b>green</b> when the digital modem unit has started up satisfactorily and it works properly.
LED Amp On	<b>Amber.</b> It illuminates when the amplifier is active, and signals are transmitted to line.
LED Eth Link	<b>Amber.</b> It stays on when the link is established correctly.
LED Eth Act	<b>Green.</b> It flashes in case of emission or reception activity in the interface.
LED PLC Status	<b>Three-coloured.</b> It illuminates in <b>green</b> when the payload is correct.  It illuminates in <b>amber</b> when the payload is incorrect. It illuminates in <b>red</b> when the control frame is incorrect.

## 3 ACCESS TO THE DEVICE

The ZBP-1 can be managed locally and remotely, through a console or through a built-in web server (HTTP/HTTPS).

### 3.1 CONSOLE

The equipment provides a user console application called *CLI (Command Line Interface)*, accessible locally through the DB9 connector in DCE mode that operates at 115200 bit/s, with 8-bit characters, without parity and with a stop bit.

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

*Appendix A* contains all the information required to use the *CLI* user console. The appendix explains the local and remote access methods, and the commands available on the console.

### 3.2 HTTP SERVER OF THE DEVICE

The HTTP server included in the device provides access to the HTML pages that gives access to all the configuration data. In order to access the HTTP server included in the ZIV device, the IP address and mask of the PC have to be properly configured.

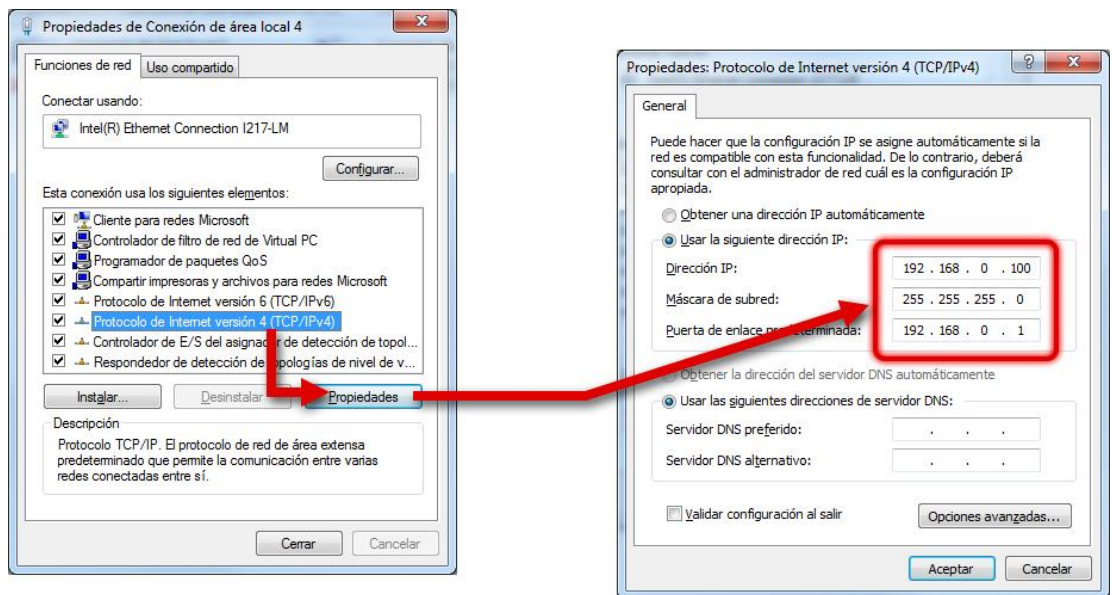
It is assumed that the user has a basic knowledge of IP addressing and networking devices such as hubs, switches, routers, etc.

If the ZBP-1 and the PC are connected directly or through a LAN (they belong to the same network), the IP address of each of them must have the same network number and different host numbers. The subnet mask must be the same for both. The default gateway does not need to be configured.

If the ZBP-1 and the PC belong to different LANs and the connection between them is via WAN, their IP addresses may have different network numbers, but both must be connected to some device (default Gateway) capable of interconnecting LANs.

The factory IP address of the ZBP-1 is 192.168.0.1 with mask 255.255.255.0.

FIGURE 10 Accessing the device via HTTP server



- IP LAN by default: 192.168.0.1/255.255.255.0
- Configure the IP of the PC within the range 192.168.0.0/24 (e.g.: 192.168.0.100). To do this, access to *Network and Sharing Center* of the Control Panel.

## 4 CONFIGURATION AND MANAGEMENT

Configuration and management of the ZBP-1 can be carried out either through the console and through access to the device HTML pages.

All the parameters controlling the device operation are described in detail in the following sections, using the real HTML pages as an auxiliary graph example.

HTML page tree menu is shown in FIGURE 11.

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

For information about the **Reboot**, **Reflash** and **Configuration files** commands, see sections 4.6, 4.7 and 4.8, respectively.

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

Whenever changes are made, regardless of the fact that they are made through the console of the HTTP server, the device must be informed what is to be done with them.

There are two options:

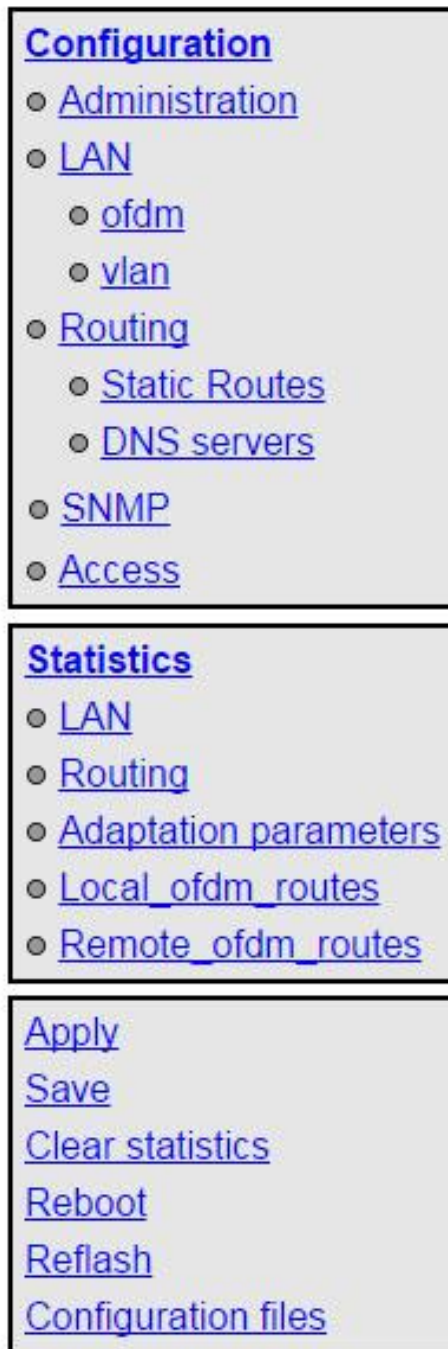
- the first is to execute the **Apply** command, which entails the immediate use of the changes made.
- the second is to execute the **Save** command, which means that the changes will be operative once the device is rebooted.

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 device 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 enough, and so the changes must previously be saved using the **Save** command before requesting the re-initialisation.

FIGURE 11 HTML page tree menu



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

## 4.1 GENERAL PARAMETERS

The general parameters are grouped into three well differentiated zones, see FIGURE 12, which are described in the following sections.

FIGURE 12 Main HTML page

The screenshot displays a web interface with three distinct configuration zones, each with a grey header bar and a red icon:

- Identification:** A table of fields including Hostname (zbp), DHCP client ID (empty), Location (unknown), Contact (unknown), Product (4ZBP010000000100), Firmware version (3.35.1.36897), Firmware reference (4WF71300040-R001), Tracking # (d4790d38bc8e18e3), and Serial # (1900128).
- Access Control:** Fields for Guest's login (guest), Guest's password (Change), Admin's login (admin), and Admin's password (Change).
- Others:** Time zone (UTC), Serial Log (checkbox), Enable Periodic Reset (checkbox), and Periodic reset period (days) (1).

At the bottom of the form are two buttons: "Send" and "Reload".

### 4.1.1 Device identification

The identification zone has the device 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 system also provides information about the software version being executed (**firmware version**), the device serial number (**serial**) and tracking number (**tracking**).

The **DHCP client ID** configures the *Client ID* option of the RFC 2131 in DHCP configuration requests. If this parameter is not configured, the MAC address of the interface on which the request is sent is used as a default value for the *Client ID*.

## 4.1.2 Access control

Access control allows the user logins (**login**) and associated passwords (**password**) to be determined for the two pre-established profiles: guest (**guest**) and admin (**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 7, 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 7 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 administrator profile when executing the first configuration in the device.

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.

## 4.1.3 Others

This zone deals with four parameters. The first of them, **Time zone**, configures the hour zone in relation to UTC.

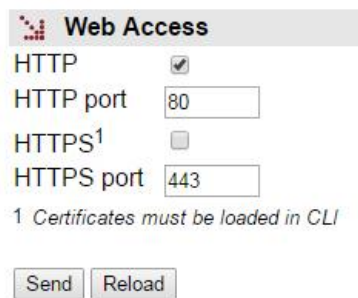
The second parameter, **Serial log**, indicates whether the log data transmission on the service serial port is activated from the initial start-up time (*Checkbox control selected*) or not.

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

## 4.2 ADMINISTRATION CONFIGURATION

The device has an integrated HTTP server for management purposes. The server supports the HTTP and the HTTPS protocols, and users can selectively enable their use and the respective port.

FIGURE 13 Configuration page of the **Administration** menu



**Web Access**

HTTP

HTTP port

HTTPS<sup>1</sup>

HTTPS port

1 Certificates must be loaded in CLI

The procedure for the installation of the certificates is described in section A.3 of Appendix A, *Data structure in CLI*.



## 4.3 LAN CONFIGURATION

The **LAN** menu contains two submenus: **ofdm** and **vlan**.

### 4.3.1 Ofdm configuration

This submenu allows the configuration of all the parameters related with the transmission of data.

The associated screen has three well differentiated sections, which are described in the following sections.

FIGURE 14 Configuration page of the **ofdm** submenu of the **LAN** menu

The screenshot shows the configuration page for the OFDM submenu. It is divided into three main sections:

- OFDM parameters:** Contains five settings: Band (HIGH\_BAND), Compact Band (OFF), Lifetime routes (120), Thres. safe mode (LOW), and Adj. adapt. datarate (VERY\_HIGH).
- OFDM device:** Contains a single setting: Local ID (1).
- Blacklisted Identifiers:** A table with three rows. The first two rows have 'Delete' buttons, and the third row has an 'Add' button. Below the table are 'Send' and 'Reload' buttons.

#	Ident.	
1	3	Delete
2	6	Delete
3		Add

#### OFDM parameters:

This section contains the following parameters:

- **Band.** This configures the operation frequencies of the device. In **LOW\_BAND** the device operates in the low part of the spectrum (2 to 8 MHz for BW of 6 MHz). In **HIGH\_BAND** the device operates in the high part of the spectrum (8 to 14 MHz for BW of 6 MHz). In **FULL\_BAND** the device operates on the whole frequency spectrum (2 to 14 MHz for BW of 12 MHz).

- **Compact Band.** This configures the transmission bandwidth (BW) of the device. In **OFF** the device operates in a bandwidth of 6 MHz, whilst in **ON** in a bandwidth of 1.5 MHz. In **ON** it is necessary to configure the **Band** field in **HIGH\_BAND** mode.
- **Lifetime routes.** This configures the lifetime of the routes. The minimum value is 5 seconds. The Factory value is 120 seconds.
- **Thres. safe mode.** This configures how quickly the device will pass to work in robust mode (with redundancy) when it detects that the channel conditions are not the most desirable. In ALWAYS the device always works in robust mode. How quickly the device changes to robust mode is high in HIGH mode, being lower in MEDIUM mode and slower in LOW mode.
- **Adj. adapt. datarate.** This configures how quickly the device will adapt the **datarate** to the new conditions of the channel once they are detected. There are five levels: AGGRESSIVE, VERY\_HIGH, HIGH, MEDIUM and LOW. In this way, in VERY\_HIGH mode, the device detects very quickly the new channel conditions and the **datarate** is adapted to them very quickly, while in LOW mode it needs much more time.

#### OFDM device:

This section contains the following parameters:

- **Local ID.** Identifier of the device. By default, it is configured at ID=1. This indicator has to be different in each device. It is used to identify neighbouring devices (NEIGHBOR) and for clock settings.  
In a subnetwork, one of the devices must always be configured with Local ID=1. This device is considered the Master and, functioning as such, is in charge of sending the clock to the rest of the devices in the subnetwork so that all the devices in the network are synchronized.

#### Blacklisted Identifiers:

This zone contains the following parameter:

- **Ident ID.** Identifier of the Local ID to be discarded. All messages coming from the devices added in the blacklist will be discarded. These devices cannot be identified as neighbouring nodes (NEIGHBORS).

## 4.3.2 Vlan configuration

This submenu permits the assigning of the Ethernet and PLC ports to any of the VLANs defined.

The associated screen has three well differentiated sections, which are described in the following sections.

FIGURE 15 Configuration page of the **vlan** submenu of the **LAN** menu

#	VID	IP	MASK	Description	eth0	ofdm	
1	1	10.212.2.128	255.255.254.0		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
2	Add						

**Ethernet eth0 properties**  
VLAN Function:   
VID:

**ofdm properties**  
VLAN Function:   
VID:

Each VLAN is distinguished from the rest by a specific identifier, usually called a **Vid**, which spread in the standard tag specified in the IEEE 802.1q. The tag allows several VLANs to share resources, including switching devices, or links between switching devices, with the guarantee that the traffic from each VLAN will reach the correct destination.

The VLANs are also simultaneously the logical interfaces in which the routing is performed, and that is why the IP address and the corresponding mask are included as part of the configuration of the VLANs.

### Vlan Virtual Interfaces:

Management of up to 8 VLANs.

For each VLAN, this section contains the following parameters:

- **#**. Indicates the position in the table.
- **VID**. It configures the VLAN identifier to be linked to the logical interface. Valid values are **1** to **4094**.

- **IP and MASK.** Values for the IP address and interface mask when operating in static mode.
- **Description.** A mnemonic descriptive field available to users. No conditions the operation of device in any way.
- **eth0.** This permits the Ethernet port to be enabled or disabled, by ticking or not ticking the box.
- **ofdm.** This permits the PLC port to be enabled or disabled, by ticking or not the box.

If both of the **eth0** and **ofdm** boxes are ticked, the device behaves as a **Bridge**. Otherwise, the device behaves as a **Router**.

#### Ethernet eth0 properties:

This section contains the following parameters:

- **VLAN function.** It specifies the Ethernet port behaviour when processing the tag 802.1q, where the options are *tagged* and *untagged*.  
**Tagged:** The 802.1 frames will be transmitted **with tag**, regardless of the fact that they have a tag or not when they are received by the device.  
**Untagged:** The 802.1 frames will be transmitted **without a tag**, regardless of the fact that they have a tag or not when they are received by the device.
- **VID (VLAN id by default).** VLAN numeric identifier in which the port is included. It is also the VLAN identifier to be assigned to the frames received in the port that is untagged.

#### ofdm properties:

This section contains the following parameters:

- **VLAN function.** It specifies the PLC port behaviour when processing the tag 802.1q, where the options are *tagged* and *untagged*.  
**Tagged:** The 802.1 frames will be transmitted **with tag**, regardless of the fact that they have a tag or not when they are received by the device.  
**Untagged:** The 802.1 frames will be transmitted **without a tag**, regardless of the fact that they have a tag or not when they are received by the device.

- **VID (VLAN id by default).** VLAN numeric identifier in which the port is included. It is also the VLAN identifier to be assigned to the frames received in the port that is untagged.

## 4.4 ROUTING CONFIGURATION

The **Routing** menu contains two submenus: **Static Routes** and **DNS servers**.

### 4.4.1 Static routes configuration

This submenu 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.

FIGURE 16 Configuration page of the **Static Routes** submenu of the **Routing** menu

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

#	Gateway	Dest I/F	Metric	Description
1	10.212.3.254	eth0	1	

#### Static Routes:

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.

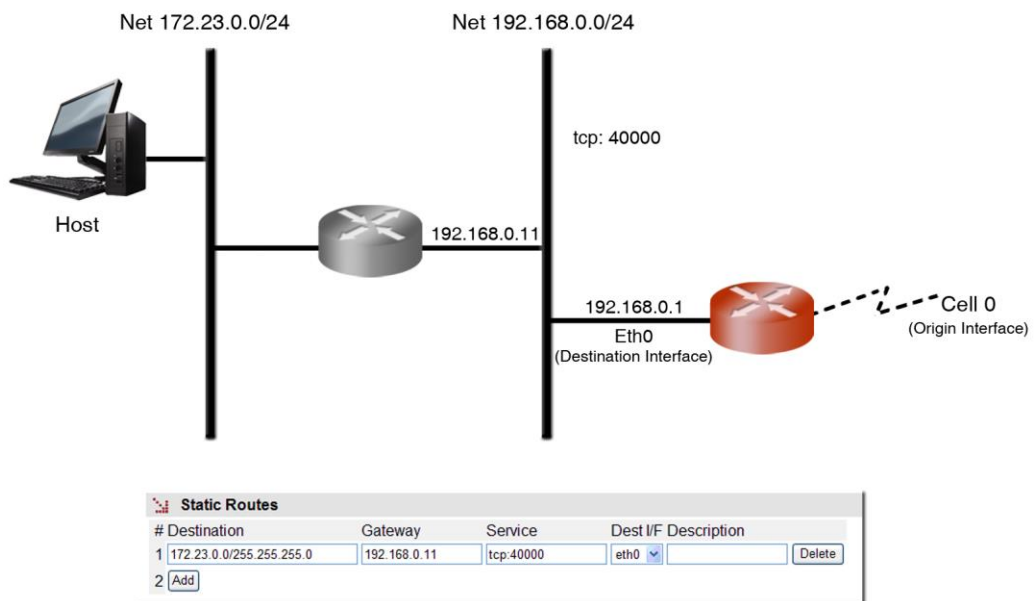
# ZBP-1

- **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. The interfaces are identified by the associated device, which may be real, or virtual, for the different devices associated with each VLAN that is defined, e.g. vlan1.
- **Description.** This permits a description of up to 15 alphanumerical characters to be specified.

### Example of static route configuration:

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 17 Example of static route configuration



## Default Static Routes:

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. The interfaces are identified by the associated device, which may be real, or virtual, for the different devices associated with each VLAN that is defined, p.e. vlan1.
- **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.

### 4.4.2 DNS server configuration

This submenu provides access to the configuration screen through which the user can configure DNS server addresses manually.

The configuration parameters are:

- **Enable DNS resolver.** Enables the DNS service. The DNS servers can be configured manually when the option is selected.
- **IP Address.** Specifies the IP addresses of DNS servers. For the addresses to be effective, the *Enable DNS resolver* box must be selected.

! For proper operation of this service, the DHCP client must NOT be configured.

FIGURE 18 Configuration page of the **DNS servers** submenu of the **Routing** menu

**DNS Servers**

Enable DNS resolver

# IP Address<sup>1</sup>

1	0.0.0.0	Undo
2	Add	

1 WARNING: If this option is enabled and dhcp client activated, they may collide

Send Reload

## 4.5 SNMP CONFIGURATION

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

The agent admits the emitting of messages based on the SNMPv1, SNMPv2c and SNMPv3 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 enough, 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.** Parameter associated with SNMPv1/v2c. Tabulate information that allows several operating profiles to be defined, including the rights of access (Access) associated with each one, read only rights (*ro*) or reading/writing rights (*rw*). The profiles are called *communities*.
- **User.** Parameter associated with SNMPv3. Tabulate information that allows the users, including the privileges and the operating mode associated with each user, to be defined. That is to say, the rights of access (Access), read only rights (*ro*) or reading/writing rights (*rw*), and the way in which the data transference (Security) will be carried out, without encryption (*clear*), authentication (*auth*) or authentication and encryption (*priv*).

In case of authentication transmission (*auth*), it is necessary to select the type of algorithm (*Auth Alg.*), MD5 or SHA, and establish the authentication password (*Auth Password*). The password sets the word to be used to generate the authentication information. The authentication word must be known by the receiver in order to be able to verify the authenticity of the identity of the transmitter.

In case of encrypted transmission (*priv*), in addition to select the type of authentication algorithm (*Auth Alg.*) and authentication password (*Auth Password*), it is necessary to select the cipher algorithm (*Priv Alg.*), DES or AES, and establish the cipher password (*Priv Password*).



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.

## SNMP Traps:

- **Enable Traps.** Enables/disables the generation and transmission of spontaneous messages by the SNMP agent. The agent will send the traps selected by the user when the different events occurred.
- **Traps SNMPv1/v2c.** Tabulate information allowing several destination equipment for the *traps* to be defined.

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.

The transmission of the messages in a confirmed (*inform*) way is only accepted for the v2c and v3 versions of the protocol.

- **Trap v1 agent address.** This configures 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.
- **Traps SNMPv3.** Tabulate information allowing several destination equipment for the notifications to be defined.

The receivers are identified by means of their IP address and the UDP port to which the notifications are to be sent. The standard UDP port for the SNMP notifications is the 162, being the value by default.

The *Type* control is used to establish whether the transmission of the notifications is carried out in an unconfirmed (*trap*) or confirmed (*inform*) way.

FIGURE 19 Configuration page of the **SNMP** menu

### SNMP

Enable

SNMP v1/v2c

#	Community	Access
1	public	ro
2	<a href="#">Add</a>	

SNMP v3

#	User	Access	Security	Auth Alg.	Auth Password	Priv Alg.	Priv Password
1	public	ro	clear	MD5	<a href="#">Change</a>	DES	<a href="#">Change</a>
2	<a href="#">Add</a>						

### SNMP Traps

Enable Traps

Traps SNMP v1/v2c

#	Community	Type	IP	Port	
1	public	v2c	158.126.40.30	162	<a href="#">Delete</a>
2	<a href="#">Add</a>				

Trap v1 agent address none

Traps SNMP v3

#	User	Type	Security	Auth Alg.	Auth Password	Priv Alg.	Priv Password	IP	Port
1	<a href="#">Add</a>								

Send
Reload

## 4.6 ACCESS CONFIGURATION

The device offers users several means of access.

Local users predefined in the system are always present, but an external resource 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 device itself. For this purpose, the device 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.

The general configuration parameters are the following:

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

- **Guest Privilege Level.** This configures the privilege level (0 to 15) of the guest profile (*guest*). This level must be the same that the one established in the TACACS+ server.
- **Admin Privilege Level.** This configures the privilege level (0 to 15) of the administrator profile (*admin*). This level must be the same that the one established in the TACACS+ server.

The parameters associated with each access option are the following:

- **Authentication method.** This configures 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.

FIGURE 20 Configuration page of the **Access** menu

The screenshot displays the configuration page for the Access menu, organized into several sections:

- TACACS+:** Includes fields for 1 Server IP (0.0.0.0), 2 Server IP (0.0.0.0), an Encrypted checkbox (checked), a Secret shared Key (Change), Guest Privilege Level (1), and Admin Privilege Level (2).
- Console Access:** Authentication method is set to local. A note below states: "1 Fallback to local access always enabled".
- Web Access:** Authentication method is set to local, and Fallback to local access is checked.
- Telnet Access:** Authentication method is set to local, and Fallback to local access is checked.
- SSH Access:** Authentication method is set to local, and Fallback to local access is checked.

At the bottom of the form, there are buttons for "Send" and "Reload".

# ZBP-1

## 4.7 REBOOT

The device can be rebooted by executing the **Reboot** command. The command is available only for the administrator profile.

## 4.8 CODE REFLASH

The device admits the updating of applicative software by executing the **Reflash** command, which is only available 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 device.

A binary image that is appropriate for the device is necessary, which can be selected by pressing the button *Examine*.

After having selected 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 is coincident with the binary image selected without affecting the installed image.

FIGURE 21 Page associated to the *Reflash* option

The screenshot shows a web interface for the 'Reflash' option. It includes a 'Reflash image' section with a file selection button and a status indicator. Below that is an 'Only verify' checkbox and a 'Reflash' button. The 'Reflash status' section displays a list of 20 steps, all marked with green circles, indicating a successful completion of the process.

**Reflash**

Reflash image  Ningún archivo seleccionado

Only verify

**Reflash status**

Last reflash process result

- Checking the image for the product
- Saving previous "conf"
- Checking "info" image
- Reflash process started
- Hash the "conf" image
- Starting the reflash process
- Flash image "loader"
- Verifying image "loader"
- Image "loader" verified successfully
- Flash image "kernel"
- Flash image "root"
- Verifying image "kernel"
- Image "kernel" verified successfully
- Verifying image "root"
- Image "root" verified successfully
- Flash image "conf"
- Verifying image "conf"
- Image "conf" verified successfully
- Reflash process finished successfully
- Rebooting the system in 15 seconds

## 4.9 CONFIGURATION FILE

The device configuration can be retrieved (**Download**) or uploaded (**Upload**) by means of a text or XML file.

FIGURE 22 Options for uploading (**Upload**) or downloading (**Download**) the configuration file

The screenshot shows a web interface for configuration file management. It is divided into two main sections: 'Upload configuration' and 'Download configuration'.  
The 'Upload configuration' section includes:

- A text input field for the file name.
- An 'Examine...' button next to the input field.
- An 'Only verify' checkbox.
- An 'Upload configuration' button.

The 'Download configuration' section includes:

- A link for 'Download configuration "conf.txt"'. The text 'conf.txt' is underlined and blue.
- A link for 'Download configuration (xml format)"conf.xml"'. The text 'conf.xml' is underlined and blue.

### 4.9.1 Upload (from the computer to the device)

The user must select the file containing the configuration to be uploaded by pressing the button *Examine*.

In order to only verify the configuration without upload it, the **Only verify** box must be ticked.

Once the device has received the file, the system checks the file contents and verifies that the variables are valid and that the values assigned to them comply with the existing syntactic requirements. If errors are detected in the received file, irrespective of whether the **Only verify** option is selected or not, the system automatically rejects all the information received and indicates the error situation to the user.

If the received configuration is valid, it is indicated by the system to the user, and it is then possible to continue (*Continue* button). When continue is selected, the configuration is activated and stored.

When applying the new configuration, the system issues a warning due to the possible loss of device access.

If the **Only verify** option has been selected, and verification has been successful, it is indicated by the system to the user. If desired, the configuration can be applied by means of the *Apply* and *Save* commands or both.

# ZBP-1

## 4.9.2 Download (from the device to the computer)

With this option the user obtains a local copy of the operating configuration in **.txt** format or **.xml** format.

The procedure for downloading this file depends on both the HTTP browser and the actions to perform with the received file (for example, where to store it).

## 5 STATISTICS

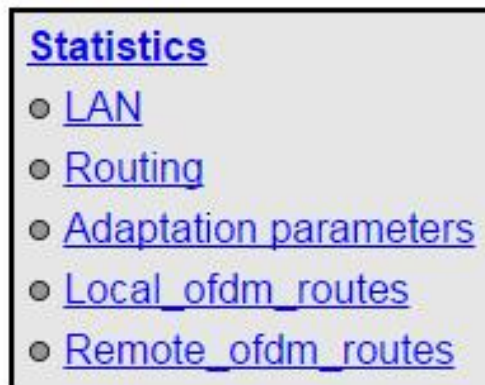
The statistics provide information resulted from the use of the device as, for example, data related to the LAN configuration, routing data, data of the routes on the PLC channel, etc.

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

The first block shows general information related to the device and is displayed automatically when the *Statistics* object is selected.

The other statistics can be accessed by selecting the respective tag located under the heading *Statistics*, see FIGURE 23.

FIGURE 23 Options of the **Statistics** menu of the Web management



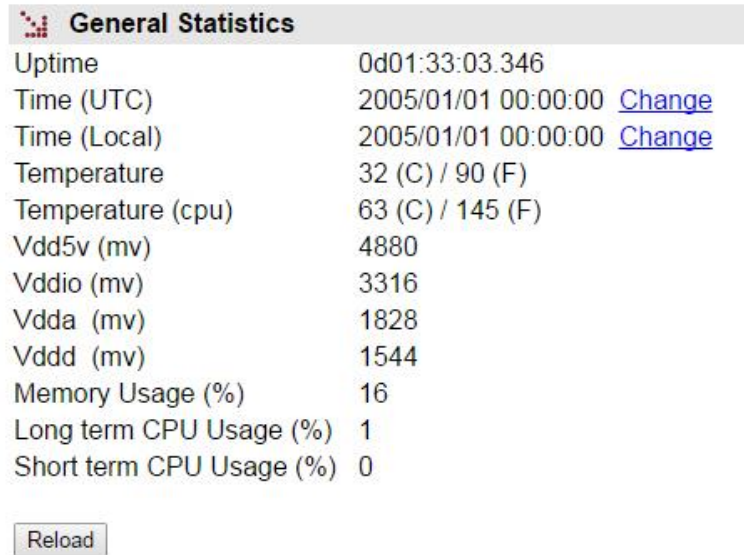
Each statistical data table can be updated by pressing the *Reload* button without having to select the respective option again in the tree menu.

The statistics can be **REBOOTED** by the user at will using the menu option **Clear Statistics**.

### GENERAL DATA

The general data relating to the device is displayed automatically when the *Statistics* object is selected.

FIGURE 24 Example of statistics with general data (*General Statistics*)



General Statistics	
Uptime	0d01:33:03.346
Time (UTC)	2005/01/01 00:00:00 <a href="#">Change</a>
Time (Local)	2005/01/01 00:00:00 <a href="#">Change</a>
Temperature	32 (C) / 90 (F)
Temperature (cpu)	63 (C) / 145 (F)
Vdd5v (mv)	4880
Vddio (mv)	3316
Vdda (mv)	1828
Vddd (mv)	1544
Memory Usage (%)	16
Long term CPU Usage (%)	1
Short term CPU Usage (%)	0

To update the date and time of the device, select the option [Change](#) corresponding to *Time (UTC)* or *Time (Local)*.

On the associated page, see FIGURE 25, enter the date and time data (YYYY/MM/DD, hh:mm:ss) and then execute the **Send**, **Save** and **Apply** commands.

FIGURE 25 Example of date and time update



Date	
Current date and time (LOCAL)	2015/03/02,12:33:13
New date and time (YYYY/MM/DD, hh:mm:ss)	<input type="text"/>

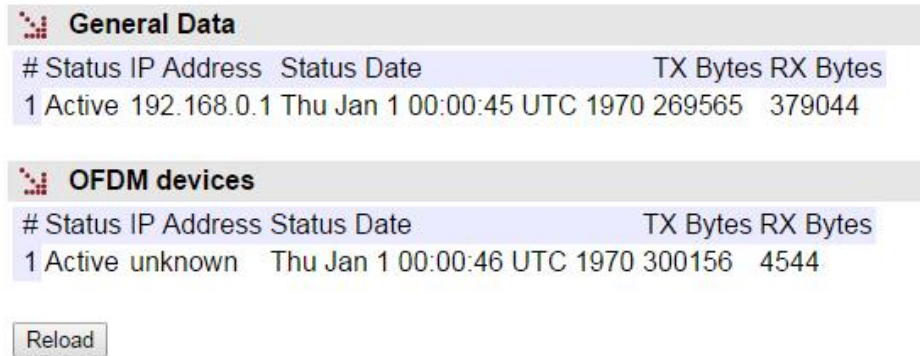


# ZBP-1

## 5.2 STATISTICS RELATED TO LAN

The data related to the LAN configuration are displayed when *LAN* is selected under the heading *Statistics*.

FIGURE 26 Example of statistics related to *LAN*



The screenshot shows two data tables under the heading 'Statistics' for LAN. The first table, 'General Data', has columns for '#', 'Status', 'IP Address', 'Status Date', 'TX Bytes', and 'RX Bytes'. The second table, 'OFDM devices', has columns for '#', 'Status', 'IP Address', 'Status Date', 'TX Bytes', and 'RX Bytes'. Both tables show one active device. A 'Reload' button is located below the tables.

#	Status	IP Address	Status Date	TX Bytes	RX Bytes
1	Active	192.168.0.1	Thu Jan 1 00:00:45 UTC 1970	269565	379044

#	Status	IP Address	Status Date	TX Bytes	RX Bytes
1	Active	unknown	Thu Jan 1 00:00:46 UTC 1970	300156	4544

Reload

## 5.3 STATISTICS RELATED TO ROUTING

The data related to routing are displayed when *Routing* is selected under the heading *Statistics*.

FIGURE 27 Example of statistics related to *Routing*



The screenshot shows a table titled 'Routing Rules' with columns for '#', 'Network Gateway', 'I/F', and 'Metric'. It displays one entry for a default gateway. A 'Reload' button is located below the table.

#	Network Gateway	I/F	Metric
1	default	10.212.3.254 dev 1	

Reload

## 5.4 STATISTICS RELATED TO ADAPTATION PARAMETERS

The connection parameters used by the local node to communicate with its neighbouring nodes are displayed when *Adaptation parameters* is selected under the heading *Statistics*.

The identification of the local node is first shown (ID = 4 in example of FIGURE 28).

The connection parameters in transmission (data rate and power value) that the local node must use to communicate with the identified neighbouring devices are then shown (node with ID = 5 in example of FIGURE 28).

The local node assigns each neighbouring node a data rate (DATA RATE) in bit/s and a power (POWER) value. The data rate is related to the type of modulation and the operation mode of each of the carriers.

Finally, the values of the connection parameters in reception (data rate in bit/s) are shown.

FIGURE 28 Example of statistics related to *adaptation parameters*

```
Local equipment
LOCAL_ID 4

TX NEIGHBOR PARAMETERS
# NEIGH ID DATARATE POWER
1 5      18006300 2

RX NEIGHBOR PARAMETERS
# NEIGH ID DATARATE
1 5      18006300

Reload
```

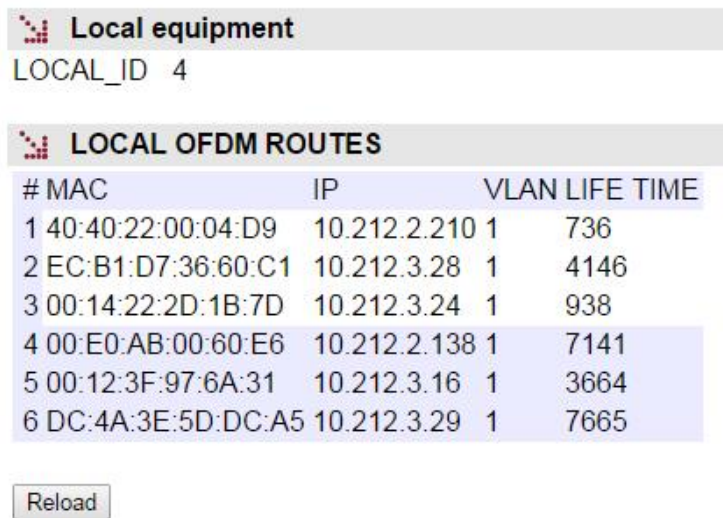
## 5.5 STATISTICS RELATED TO LOCAL OFDM ROUTES

The local MAC/IP addresses of the node are displayed when *Local ofdm routes* is selected under the heading *Statistics*.

The identification of the local node is first shown (ID = 4 in example of FIGURE 29).

The local route table is then displayed. For each route, the MAC address, IP address, VLAN included in the route and life time of the route are indicated.

FIGURE 29 Example of statistics related to *local ofdm routes*



The screenshot displays a web interface with two main sections. The first section, titled "Local equipment", shows "LOCAL\_ID 4". The second section, titled "LOCAL OFDM ROUTES", contains a table with the following data:

#	MAC	IP	VLAN	LIFE TIME
1	40:40:22:00:04:D9	10.212.2.210	1	736
2	EC:B1:D7:36:60:C1	10.212.3.28	1	4146
3	00:14:22:2D:1B:7D	10.212.3.24	1	938
4	00:E0:AB:00:60:E6	10.212.2.138	1	7141
5	00:12:3F:97:6A:31	10.212.3.16	1	3664
6	DC:4A:3E:5D:DC:A5	10.212.3.29	1	7665

Below the table is a "Reload" button.

## 5.6 STATISTICS RELATED TO REMOTE OFDM ROUTES

The data of the routes found on the PLC channel are displayed when *Remote ofdm routes* is selected under the heading *Statistics*.

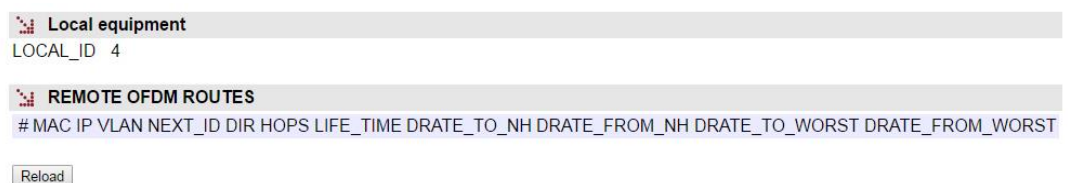
The identification of the local node is first shown (ID = 4 in example of FIGURE 30).

The data associated with the different routes, if they exist, is then displayed.

In each of the routes the following parameters are displayed:

- the **MAC address**, its corresponding **IP address**, and the **VLAN** included in the route,
- the identification number of the following node in the route (**NEXT ID**),
- the address (**DIR**) of the link, being B (two-way) or M (one-way) when there is no return route,
- the number of segments (**HOPS**) in the route,
- the life time (**LIFE TIME**) of the route, which is updated while receiving information through the route,
- four data rates (**DRATE**) of the route in bit/s. Tx and RX data rate of the next hop, and the worst Tx and Rx data rate of all the segments in the route.

FIGURE 30 Example of statistics related to *remote ofdm routes*



## APPENDIX A

### DATA STRUCTURE IN *CLI*

## APPENDIX A

### 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 itself. *E.g. **action***

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

To browse through the directories the **cd (change directory)** command is used.

The data stored in table 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** commands 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.

User names and passwords are, by default, the same as in the web interface, that is:

	Login	Password
Guest profile	guest	passwd01
Admin. profile	admin	passwd02

## A.1 ACCESS METHODS

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

- in local mode, through the DB9 connector.
- in local or remote mode via Telnet/SSH, through the Ethernet port.

### Access through the DB9 connector

Access in local mode is obtained by connecting the DB9 port of the equipment (service port) to the serial port of the PC (or in its absence via the USB serial converter), through a flat serial cable.

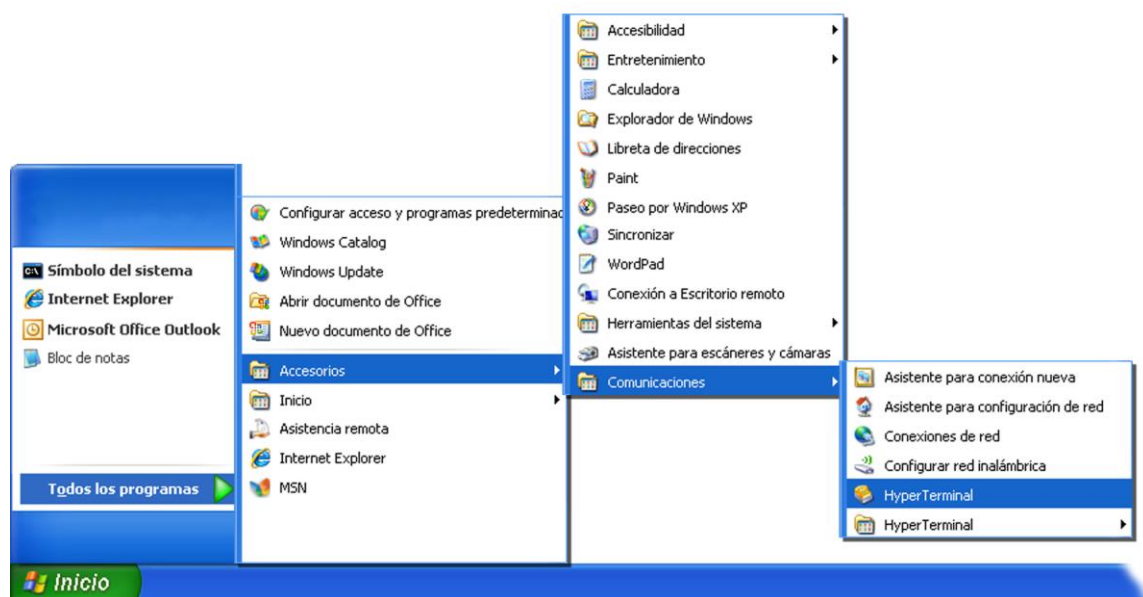
# ZBP-1

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 31).

FIGURE 31 Location of *HyperTerminal* in Windows XP®

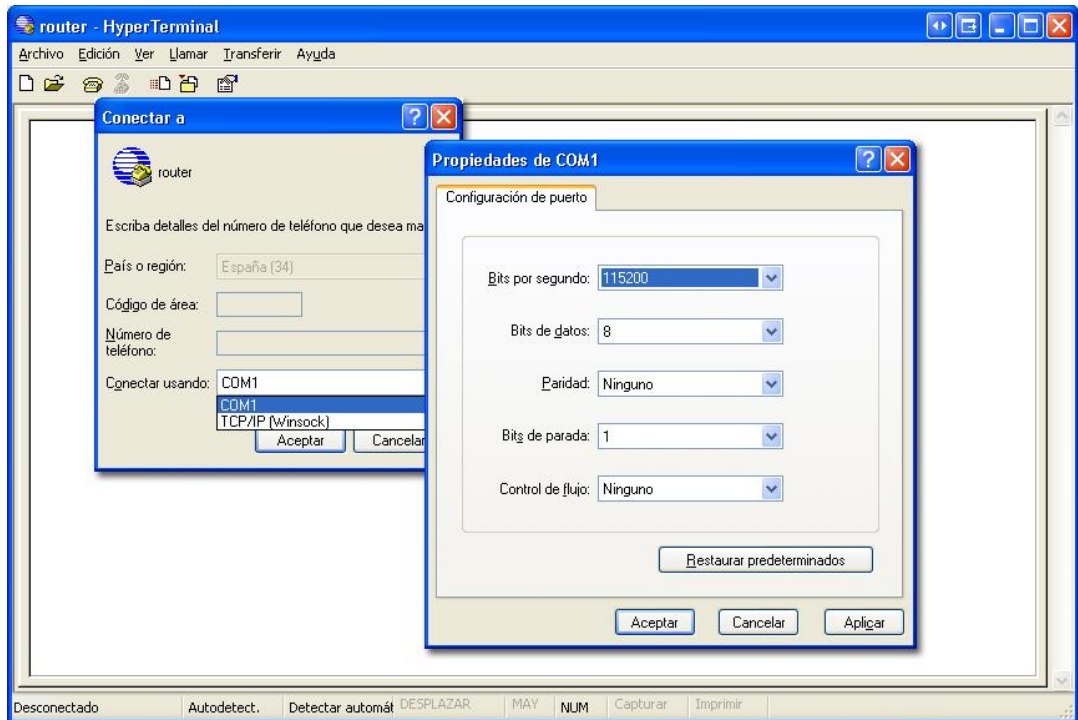


On opening *HyperTerminal*, a text box appears, requesting the necessary information to establish the connection (see FIGURE 32).



# ZBP-1

FIGURE 32 Connection configuration through the serial port with *HyperTerminal*



Run the *Call* option of the *Call* menu (or press, under the main menu options, the icon of the phone hanged).

After the appearance of the starting frames, press the return key. When at the prompt is displayed the **zbp login** text, enter the user name and press return. When at the prompt is displayed the **zbp password** text, enter the password and press return (the user name and password are the same as in the web interface).

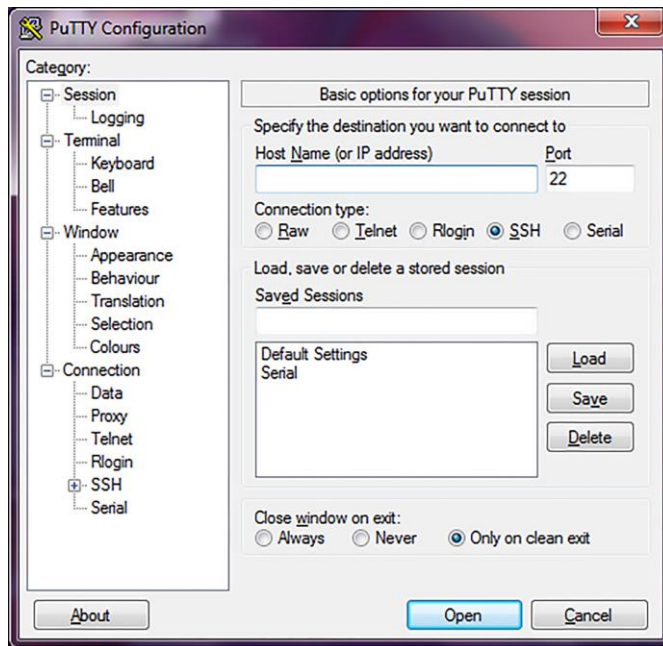
Remember that no text will appear in the *HyperTerminal* window when entering the password.

As operating systems like Microsoft Windows 7© no longer include the *HyperTerminal* program, the *Putty* program, free and executable, is also considered.

The *Putty* program is accessible on the [www.putty.org](http://www.putty.org) web. Simply select the *Putty* that suits the operating system in use (usually the first, called **putty.exe**), copy it in the PC and run it.

# ZBP-1

FIGURE 33 *Putty home window*



In the **Serial** menu (last of all) the serial port is configured.

! Telnet access is carried out by configuring the port 23.  
SSH access is carried out by configuring the port 22.

If an USB converter is used, first, consult the COM number in the *Device administrator* (Control panel).

FIGURE 34 *Device administrator window*

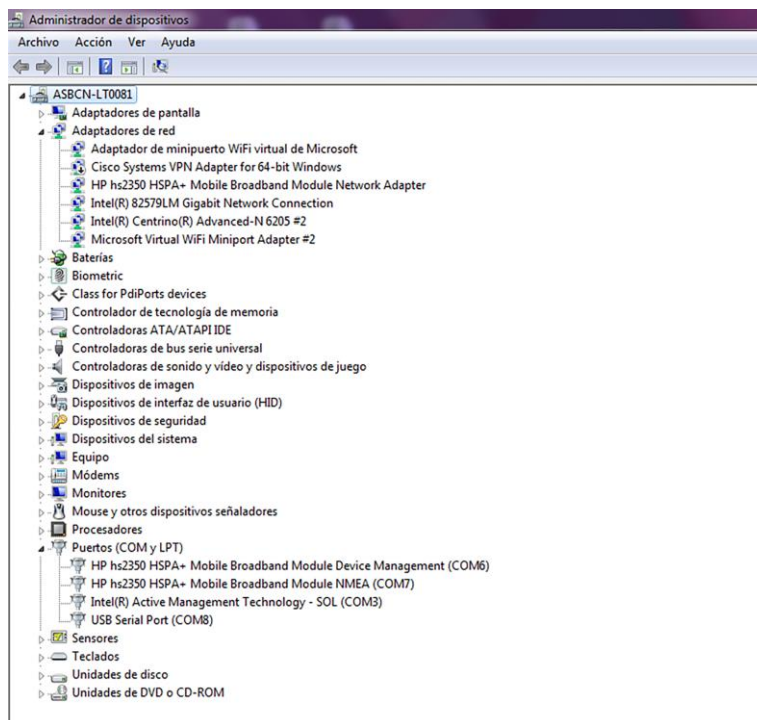
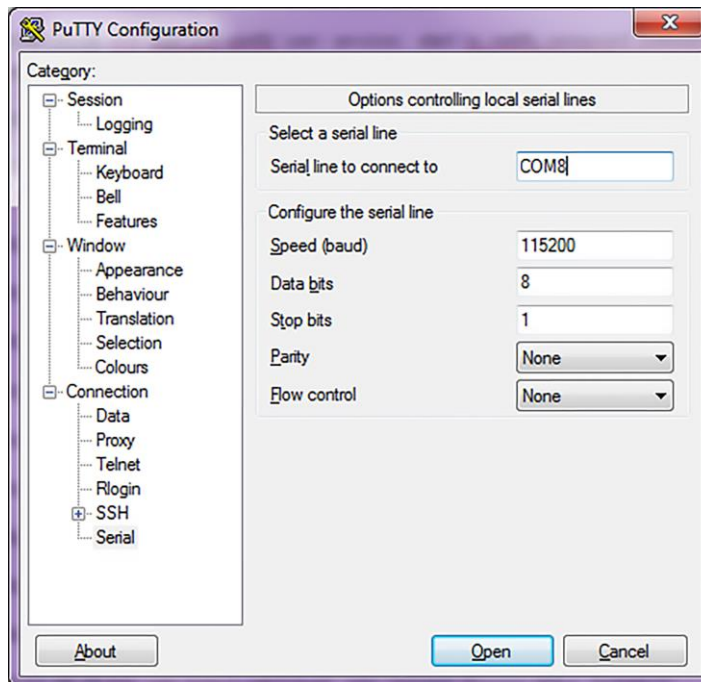


FIGURE 35 Connection configuration through the serial port with *Putty*



Pressing the *Open* button, and return if necessary, a window is shown in which the **zbp login:** prompt will appear, ready for the user to enter the *login* and *password* for starting the session (the user name and password are the same as in the web interface).

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

### Access through Telnet

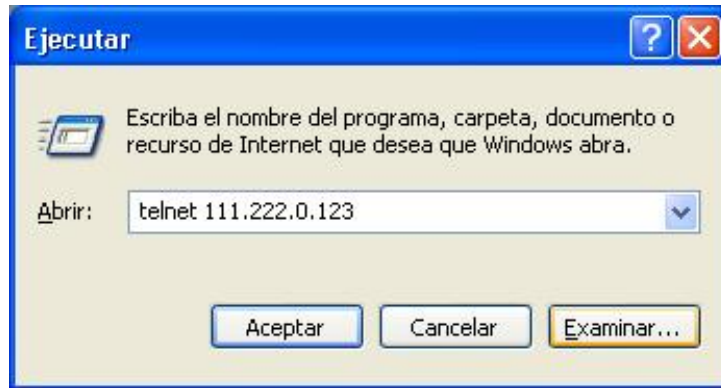
Access, in local or remote mode, is obtained with the *Telnet* command and equipment IP address.

! To use this access mode, the equipment must have its IP address configured and be connected to the network in which the management PC is located.

To execute Telnet from Windows XP®, click on *Start* → *Execute* and, in the dialog box that appears, type: telnet + space + Equipment\_IP\_address (111.222.0.123 for example), and then press the button *Accept* (see FIGURE 36).

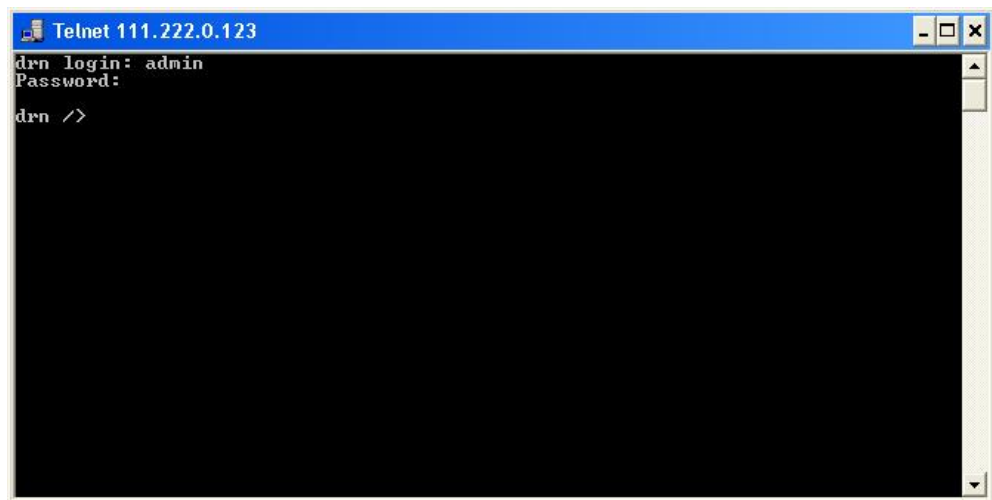
# ZBP-1

FIGURE 36 Execute.. Telnet text window to establish connection with the equipment



On pressing the Accept button a System symbol window will appear (see FIGURE 37 of example with a drn equipment).

FIGURE 37 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.

Telnet can also be run from the *Putty* program. Simply, type the IP address of the equipment in the main window, and press *Open*.

Whatever the method chosen to establish connection with the equipment, the **zbp login:** prompt will appear, ready for the user to enter the *login* and *password* for starting the session (the user name and password are the same as in the web interface).

In operating systems like Microsoft Windows 7©, the Telnet client is disabled by default.

To enable it, from the Start button: *Start* → *Control panel* → *All Programmes*, in *Programs and Features*, select *Turn on or Turn off the Windows features*.

Then, in the window of *Windows Features*, select *Telnet client*, see FIGURE 38. By pressing *Accept*, the Telnet client of Windows may be used.

FIGURE 38 Window of *Windows Features*



## A.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:

**TABLE 8** 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	✓	✗
<b>download</b>	Generates a configuration commands file	✓	✓
exit	Interrupts the connection with the equipment	✓	✓
<b>get</b>	Shows the parameter values	✓	✓
help	Shows the list of available commands	✓	✓
<b>log</b>	Shows the log file in use (current)	✓	✓
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	✓	✗
<b>stats</b>	Allows to obtain the status parameters of the equipment	✓	✓
telnet	Open a telnet session without interrupting the connection with the equipment	✓	✓
xmldownload	Generates a configuration commands file in xml format	✓	✓

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

**TABLE 9** 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		
xmldownload		

### Information in the log

The events that are generated at the system level and sent to the log include an identification level.

The system supports 8 different levels, separated into two blocks. The first set corresponds to unwanted situations, and the second block on information without affecting the functionality.

In the first block, the values are **emerg**, **alert**, **crit**, **err** and **warning**, which represents a decreasing level of severity in terms of the detected situation.

In the information block, the values are **notice**, **info** and **debug**, without having any connotation whatsoever for impact.

## Configuration commands

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

**Syntax:** zbp /> **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:** zbp /lan > **add vlan/vlan\_ifaces**  
zbp > **add routing/static/st\_rules**  
zbp /routing > **add ../lan/vlan/vlan\_ifaces**

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

**Syntax:** zbp /> **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:** zbp /> **apply**



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

**Syntax:** zbp /> **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:** zbp /> **download**

**get** This show the current values of one or several equipment configuration parameters.

**Syntax:** zbp /> **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.

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:**

```
zbp /> get
zbp /> get main
zbp /main> get hostname
zbp /> get main/hostname
zbp /admin> get ../main/hostname
```

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

**Syntax:** zbp /> **remove** *name*[*n*<sup>o</sup>]

**Arguments:**

*name* Parameter from which the item is to be removed.  
*n*<sup>o</sup> (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:**

```
zbp > remove /routing/static/st_rules
zbp /routing/static > remove /st_rules [3]
zbp /routing > remove ../lan/vlan/vlan_ifaces
```

- restore** This applies the factory configuration.
- Syntax:** zbp /> **restore**
- Arguments:** -
- Observations:** This command can be used irrespective of the directory where the user is.
- Example:** zbp /> **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:** zbp /> **save**
- Arguments:** -
- Observations:** This command can be used irrespective of the directory where the user is.
- Example:** zbp /> **save**
- 
- set** This change the value stored in the configuration parameters or in the attributes of an item in a matrix-type parameter.
- Syntax:** zbp /> **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:**

```
zbp /main> set hostname  
zbp /> set main/hostname  
zbp /admin> set ../main/hostname
```

**xmldownload** Generates a configuration command file in xml format.

**Syntax:** zbp /> **xmldownload**

**Arguments:** -

**Observations:** Unlike the download command, the commands shown with the *xmldownload* are dependent on the directory the user is, and the command list does not start with the command *restore*.

**Example:** zbp /> **xmldownload**

## Control commands

**cd** Changes the active directory.

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

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

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

**Syntax:** zbp /> **exit**

**Arguments:** -

**Observations:** -

**Example:** zbp /> **exit**

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

**Syntax:** zbp /> **quit**

**Arguments:** -

**Observations:** -

**Example:** zbp /> **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:** zbp /> **reboot**

**Arguments:** -

**Observations:** -.

**Example:** zbp /> **reboot**

**reload** Reloads the saved configuration in the equipment.

**Syntax:** zbp /> **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:** zbp /> **reload**

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

**Syntax:** zbp /> **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.

**Examples:** zbp /> **telnet zbp**  
zbp /> **telnet 172.16.50.38 23**

## Status and Diagnostic Commands

**clear** Deletes the statistics.

**Syntax:** zbp /> **clear**

**Arguments:** -

**Observations:** -

**Example:** zbp /> **clear**

**date** Shows the date and time recorded in the equipment.

**Syntax:** zbp /> **date**

**Arguments:** -

**Observations:** -

**Example:** zbp /> **date**

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

**Syntax:** zbp /> **help**

**Arguments:** -

**Observations:** -

**Example:** zbp /> **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:** zbp /> **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.

Operationally two logs are created, which is permanent (**log** command) and having temporal and global (**log all** command).

You can filter at will the temporary log, using the text as a filter after the command. This operation works with any text in the filter, not only with the category (see section **Information in the log**), so it is possible to filter traces of individual processes or selected events.

**Examples:**

```
zbp /> log
zbp /> log all
zbp /> log crit
zbp /> log debug
```

**Is** 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:** zbp /> **ls**

**Arguments:** -

**Observations:** -

**Example:** zbp /> **ls**

## ping

This sends ICMP ECHO\_REQUEST packets to a specific host.

**Syntax:** zbp /> **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.

**Examples:** zbp /> **ping 172.16.50.38**  
zbp /> **ping zbp**

## stats

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

**Syntax:** zbp /> **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:** zbp /> **stats**  
zbp /> **stats main**  
zbp main/> **stats temperature**  
zbp main/> **stats ../lan/eth0/txbytes**

## A.3 CERTIFICATE INSTALLATION FOR HTTPS MANAGEMENT

The server integrated in the equipment supports the HTTP and the HTTPS protocols, in the last case being necessary the installation of certificates.

The procedure for loading the certificates for HTTPS management, ***once the certificate, the private key and the password of the last one have been got***, is the following:

1- Access the configuration section of the web interface.

(**"cd /admin/web"**)

2- Load in "**cert**" a valid **certificate** with the command "**upload cert raw**".

The procedure for loading the certificate is the following. **Copy** in the clipboard **the certificate**. Then, **execute the indicated upload command** and, when it is in wait period, **paste the data from the clipboard**. Wait approximately 30s. When the time is elapsed, the data are shown.

3- Load in "**privatekey**" a valid **private key** with the command "**upload privatekey raw**".

The procedure is the same that the one indicated previously for the certificate.

4- Introduce the **password of the private key** in "**privatekeypwd**" with the command "**set privatekeypwd**".

Confirmation of the password is required twice as much.

5- In the equipment, activate the access by means of HTTPS

(**"set https on"**)

6- Apply the changes

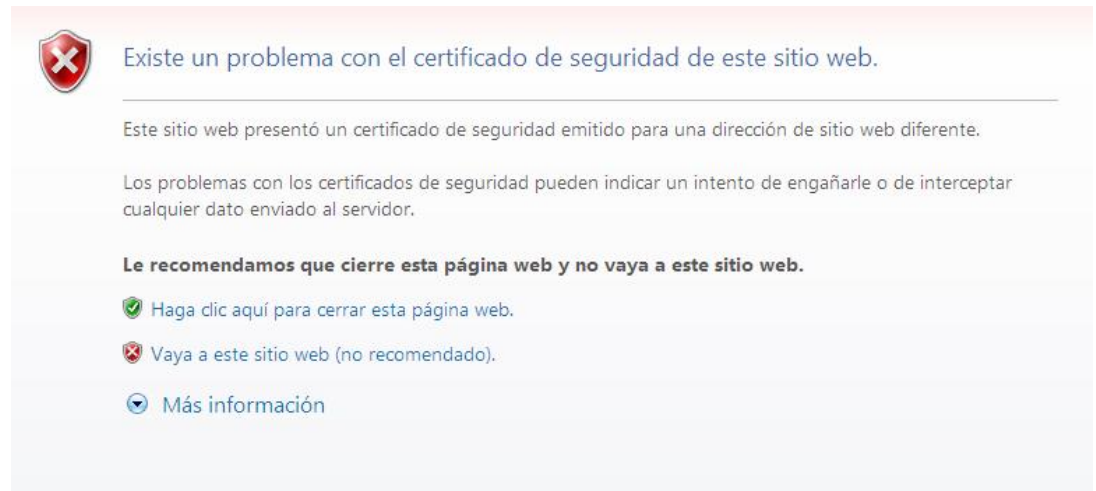
(**"apply"**)

7- Save the new data (optional)

(**"save"**)

8- **Load** the equipment configuration web page in the browser (Microsoft Internet Explorer, Mozilla Firefox, etc. Google Chrome is not supported) <sup>(1)</sup> typing “**https://**” instead of **http://**”.

The following message appears:



Although the certificate operates correctly, this message is a warning indicating that the certificate has not been validated by a trusted authority.

Select “**Go to this web site (not recommended)**”.

Then, the equipment access control requires the user login and password.

In the equipment with HTTPS operation, the **certificate**, the **private key** and the **password of the last** are part of the data obtained by means of the “**download**” command. Therefore, it is possible to add this information to the configuration pattern.

---

<sup>(1)</sup> The operation is a success with Microsoft Internet Explorer and Mozilla Firefox. Google Chrome doesn't accept the certificates authorized by you.

Example of download command in the equipment (EMR-2) with HTTPS operation:

```
emr2 /> download
restore
set /main/hostname emr2
set /main/timezone Madrid
set /admin/web/https on
set /admin/web/cert "-----BEGIN CERTIFICATE-----
\nMIICWzCCACQCCQCCL+NbBdYynDANBqkqhkiG9w0BAQUFADByMQswCQYDVQQGEWJF\
nUZESMBAGA1UECBMJQmFyY2Vsb25hMRITwEAYDVQQHEWlCYXJjZWxvbmExDDAKBGNV\n
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWdmouc2FsYXRRA\ne
m12LmVzMB4XDTEzMDMyNzE1NTAzOVowXDE0MMDMyNzE1NTAzOVowc2E1MAkGA1UE\n
BhMCRVVMxejAQBGNVBAGTCUJhcmlbG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww\n
nCgYDVQQKEWNaSVYxZjAMBGNVBAMTBUpvc2VwMR0wGwYJKozIhvcNAQkBFg5qLnNh\n
\nbGF0QHppdi5lczCBnzANBqkqhkiG9w0BAQEFAAOBjQAwYkCgYEA49IfdfD/xVO\n
\nGsqL217s6aumdfwr9NYoJw68LbrHY0Vz9OGwen+a1XajBc121qLZjf11Oh250awE\n
\nnezLH317D5bxS9c+w8YrXowEnYoxUQpK49YGVH7DnqLayI5ptyQbdyMoTKmCxB0Z\n
\nnjNoToViogIz9GRBg6nKCDC4+Pxn3/90CAWEAATANBqkqhkiG9w0BAQUFAAOBqQAT\n
\n7Qt00JT61LcGciF4R5aooiRoZEiTJQBfM6PotZ21apGGhF1Bz0FPn3LRxC1Mb6PI\n
\nnknatYteCq5FJNjGunF8hDIQVc1x702ju2vmG0iyVfsz1eqiy+Tx0dMYsgpBeY3K+\n
\nn8fb+J1jmlPNzPhgMlzPK6VGNA70/QhfCG915xK1owQ==\n
\n-----END CERTIFICATE-----"
set /admin/web/privatekey "-----BEGIN RSA PRIVATE KEY-----
\nMIICWwIBAAKBgQCj0h918P/FU4ayovbxuzpq6z0Vav01ignDrwtusdjRVn04bB6\n
\nnf5qVcCMFyXawotmN/WU6HbnRprYR5ksffwUP1vFL1z7DxivBehYSdg7FRckrj1ga8\n
\nnfsOeosDIjmm3JBt3IyhOQxzEE5mM2hohwKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB\n
\nnaoGAOVDzYhVKhjodHlUzm3lbsZzAk1KAKNorgn8kxbyE/RM8mkv9f/Lb3jwhiEu\n
\nnxyf7m7BmNmCex8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S\n
\nnApuozFYmh34uBl6SJKudihCs4jM1ocQBQMhQ7mXe7Sk1sgECQDgpdSDx45vm8Yk+\n
\nnGoX4UzcRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcnOpU8bFtQbwfxjkThhthQBN\n
\nnrUeERej9AkeA0S4ernXQGVJGm7b6JhJXFKkILVyo5vP0C3jx7ByRIMt41k11417Q\n
\n\ntzNepkjlcmimzLWuHJAiyTbtvzfVcnu4YQJAaX0aX3HkwSgosIpp0QLfGp7yJNQu\n
\n\nnqt5h+vZ06FTuSFPm3t0D4G0K6M1N0nKNIEm2CAJpg0JU8BY66jupEqGrUQJAW7\n
\n\nwp\n\nns/1pJEDjPg/p+lkeHqvBLwdQZx1dbM442rjn1AZBNzq01ZuwTEvUWCLG3fMt9iBN\n
\n\nnvq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1Xst5nxH8U2Zk1u7ZWZZhOTcw\n
\n\nnezG/TDLBwkROF2n9VX6TYGesnZ2Ve/+DiMPhk7ZVQA==\n
\n-----END RSA PRIVATE KEY-----"
set /admin/web/privatekeypwd testhttps
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn gnftsg.com
set /wan/cell0/login pruebas_ziv1
set /wan/cell0/passwd pruebas_ziv1
set /snmp/enable on
set /access/tacacsplus/server1_ip 10.132.2.148
set /access/tacacsplus/server2_ip 10.132.2.168
set /access/tacacsplus/shared_key Sm4rt3Sy13
set /access/tacacsplus/admin_lv1 15
set /access/web/method tacacsplus
```

If there are no available certificate, private password and password of the last, it is possible to create them. For example, following the instructions in [http://www.akadia.com/services/ssh\\_test\\_certificate.html](http://www.akadia.com/services/ssh_test_certificate.html), but in this case it is necessary a Linux equipment to execute the instructions.

An example of certificate, as well as private key, is shown the following.

Pay attention that both the header and bottom lines are part of the certificate.

Example of a valid **certificate**:

```
-----BEGIN CERTIFICATE-----
MIICWzCCACQCCQCCL+NbBdYynDANBggkqhkiG9w0BAQUFADByMQswCQYDVQQGEwJF
UzESMBAGA1UECBMJQmFyY2Vsb25hMRIwEAYDVQQHEw1CYXJjZWxvbmExDDAKBgNV
BAoTA1pJVjE0MAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWdmouc2FsYXRA
eml2LmVzMB4XDTEzMDMyNzE1NTAzOV0xOTU0MDMyNzE1NTAzOV0wZjElMAKGA1UE
BhMCRVMxEjAQBGNVBAgTCUJhcml1bG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww
CgYDVQQKEwNaSVYxZjAMBGNVBAmtBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh
bGF0QHppdi5lczCBnzANBggkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA49IfdFD/xVO
GsQL217s6aumdfwr9NYoJw68LbrHY0VZ90Gwen+a1XajBcl2lqLZjf110h250awe
eZLH311D5bxS9c+w8YrwxowEnYoxUqPK49YgVH7DnqLayI5ptyQbdyMotkMcXBOZ
jNoToVioGiZ9GRBg6nKCDc4+Pxn3/90CAWEAATANBgkqhkiG9w0BAQUFAAOBQAT
7Qt00JT6lLcGciF4R5aooiRoZEiTJQBfM6PoTZ21apGGhF1Bz0FPn3LRxC1Mb6PI
kNatYteCq5FJNjGunF8hDIQvc1x702ju2vmGoiyvFsZleqiy+Tx0dMYsgpBeY3K+
8fb+J1jmlPNzPhgMlzPK6VGNA70/QhfCG915xK1owQ==
-----END CERTIFICATE-----
```

Example of a valid **private key**:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6Z0Vav01ignDrwtusdjRVn04bB6
f5qVccMFyXawotmN/WU6HbnRpYR5ksffwUP1vFL1z7DxivBehYSdg7FRckrj1ga8
fs0eosDIjmm3JBt3IyhOQxzEE5mM2hOhwkgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB
AoGA0vDzYhVKhjodHlUzm3lbsZzAk1KAKNorgn8kxbyE/RM8mkv9f/Lb3jwhiEu
xyf7m7BmNMcx8bSRwduzrUnk66Dw8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S
ApuoZFYmh34uBl6SJKUdihCs4jm1ocQBQMHQ7mXe7sk1sgECQQDgppSDx45vm8Yk+
GoX4UzCRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcnOpU8bFtQbWfxjkThHthQBN
rUeEREj9AkeA0S4ernXQGVJGm7b6JhJXFkKILVyo5vP0C3jx7ByRIMt41k11417Q
tzNepKj1cmimzLWuHJAiyTbtvzfvCnu4YQJAax0ax3HkwSgosIpp0QLfGp7yJNQu
qt5h+vZ06FTuSFPm3t0D4G0K6M1N0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7wp
s/lpJEDjPg/p+1keHqvBLwdQZX1dbM442rjn1AZBNzq01ZuWTEVUWCLG3fMt9iBN
Vq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1Xst5nxH8U2Zk1u7ZWZZhOTcw
ezG/TDLBwkROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==
-----END RSA PRIVATE KEY-----
```