



---

## EQUIPO PLC DE MT TIPO ZBP-1



### MANUAL DE USUARIO

V01 - Abril 2019

MOZBP11904Ev01

ZIV  
Antonio Machado,78-80  
08840 Viladecans, Barcelona-España

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

[www.zivautomation.com](http://www.zivautomation.com)

## SÍMBOLOS DE SEGURIDAD



### **ADVERTENCIA O PRECAUCIÓN:**

Este símbolo denota un riesgo. No seguir el procedimiento, operación o similar indicado puede suponer la avería total o parcial del equipo e incluso la lesión del personal que lo manipule.



### **NOTA:**

Información o aspecto importante a tener en cuenta en un procedimiento, operación o similar.

## ÍNDICE

	Pág.
<b>1</b>	<b>INTRODUCCIÓN</b> <span style="float: right;"><b>5</b></span>
1.1	GENERALIDADES <span style="float: right;">5</span>
1.2	PROTOCOLO DE CONEXIÓN <span style="float: right;">5</span>
1.2.1	Fase de Conexión PLUG&PLAY <span style="float: right;">6</span>
1.2.2	Fase de Búsqueda y selección de rutas <span style="float: right;">6</span>
1.3	PARÁMETROS OFDM <span style="float: right;">7</span>
1.4	ESPECIFICACIONES TÉCNICAS <span style="float: right;">10</span>
1.4.1	Características del equipo <span style="float: right;">10</span>
1.4.2	Interfaces del equipo <span style="float: right;">10</span>
1.4.3	Características de la transmisión PLC <span style="float: right;">10</span>
1.4.4	Gestión del equipo <span style="float: right;">11</span>
1.4.5	Servicios adicionales <span style="float: right;">12</span>
1.4.6	Accesorios <span style="float: right;">12</span>
1.4.7	Certificaciones <span style="float: right;">12</span>
1.4.8	Características mecánicas <span style="float: right;">12</span>
1.4.9	Condiciones de funcionamiento <span style="float: right;">13</span>
1.4.10	Condiciones de transporte y almacenaje <span style="float: right;">13</span>
1.5	ADVERTENCIAS <span style="float: right;">14</span>
1.5.1	Advertencias previas <span style="float: right;">14</span>
1.5.2	Consideraciones de seguridad del equipo <span style="float: right;">15</span>
<b>2</b>	<b>CARACTERÍSTICAS MECÁNICAS Y ELÉCTRICAS</b> <span style="float: right;"><b>16</b></span>
2.1	ALIMENTACIÓN <span style="float: right;">21</span>
2.2	CONECTOR ETHERNET <span style="float: right;">21</span>
2.3	INDICACIONES ÓPTICAS <span style="float: right;">24</span>
<b>3</b>	<b>ACCESO AL EQUIPO</b> <span style="float: right;"><b>26</b></span>
3.1	CONSOLA <span style="float: right;">26</span>
3.2	SERVIDOR HTTP DEL EQUIPO <span style="float: right;">26</span>

	Pág.
<b>4</b>	<b>CONFIGURACIÓN Y GESTIÓN</b> <span style="float: right;"><b>28</b></span>
4.1	PARÁMETROS GENERALES <span style="float: right;">30</span>
4.1.1	Identificación del equipo <span style="float: right;">30</span>
4.1.2	Control de acceso <span style="float: right;">31</span>
4.1.3	Otros <span style="float: right;">32</span>
4.2	CONFIGURACIÓN ADMINISTRATION <span style="float: right;">32</span>
4.3	CONFIGURACIÓN LAN <span style="float: right;">33</span>
4.3.1	Configuración Ofdm <span style="float: right;">33</span>
4.3.2	Configuración Vlan <span style="float: right;">35</span>
4.4	CONFIGURACIÓN ROUTING <span style="float: right;">37</span>
4.4.1	Configuración Static routes <span style="float: right;">37</span>
4.4.2	Configuración DNS servers <span style="float: right;">39</span>
4.5	CONFIGURACIÓN SNMP <span style="float: right;">40</span>
4.6	CONFIGURACIÓN ACCESS <span style="float: right;">43</span>
4.7	REINICIO (REBOOT) <span style="float: right;">44</span>
4.8	ACTUALIZACIÓN DEL CÓDIGO (REFLASH) <span style="float: right;">45</span>
4.9	FICHERO DE CONFIGURACIÓN <span style="float: right;">46</span>
4.9.1	Upload (del ordenador al equipo) <span style="float: right;">46</span>
4.9.2	Download (del equipo al ordenador) <span style="float: right;">47</span>
<b>5</b>	<b>ESTADÍSTICAS</b> <span style="float: right;"><b>48</b></span>
5.1	DATOS GENERALES <span style="float: right;">49</span>
5.2	ESTADÍSTICA RELATIVA A LAN <span style="float: right;">50</span>
5.3	ESTADÍSTICA RELATIVA A ROUTING <span style="float: right;">50</span>
5.4	ESTADÍSTICA RELATIVA A ADAPTATION PARAMETERS <span style="float: right;">51</span>
5.5	ESTADÍSTICA RELATIVA A LOCAL OFDM ROUTES <span style="float: right;">52</span>
5.6	ESTADÍSTICA RELATIVA A REMOTE OFDM ROUTES <span style="float: right;">53</span>
	<b>APÉNDICE A</b>
	<b>ESTRUCTURA DE DATOS EN CLI</b> <span style="float: right;"><b>54</b></span>

## 1 INTRODUCCIÓN

### 1.1 GENERALIDADES

El ZBP-1 permite la transmisión de datos a alta velocidad (hasta 28,8 Mbit/s) a través de líneas de Media Tensión, en un rango de frecuencias seleccionable por el usuario (de 2 a 14 MHz).

Para conseguir este objetivo, el sistema utiliza una modulación **OFDM** (Multiplexación por División de Frecuencias Ortogonales).

El flujo de bits se asigna dinámicamente a un conjunto de portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QPSK o QAM.

El canal se examina constantemente de forma que las portadoras afectadas por el ruido o por las interferencias pueden reducir su modulación automáticamente e incluso anularse. Además, para conseguir una comunicación más fiable, el ratio del Turbo Código también puede variar.

### 1.2 PROTOCOLO DE CONEXIÓN

El ZBP-1 puede operar como encaminador de nivel 3 para IPv4 (router) o como conmutador de nivel 2 (bridge) entre la interfaz Ethernet y la interfaz PLC, e incluye soporte para IEEE802.1Q (VLANs).

El protocolo de conexión entre equipos se basa en la búsqueda de rutas para **direcciones IP/MAC** y consta de dos fases bien diferenciadas: la fase de **Conexión PLUG&PLAY** y la fase de **Búsqueda y selección de rutas**, las cuales se describen a continuación.

La capa de acceso al medio MAC está basada en la **IEEE 802.15.4** que proporciona acceso al medio compartido, seguridad y recuperación automática de paquetes.

El protocolo de enrutamiento PLC usado es **LOADnG**, debido a su naturaleza reactiva y a su adaptación al IEEE 802.15.4.

El protocolo LOADnG es un sistema de enrutamiento dinámico que se adapta fácilmente a los cambios de topología del medio utilizando los caminos redundantes y la capacidad de sobrealcance del equipo.

# ZBP-1

## 1.2.1 Fase de Conexión PLUG&PLAY

La primera fase de la conexión entre equipos, llamada de *Conexión PLUG&PLAY*, es la fase de inicio y de identificación de todos los equipos vecinos (NEIGHBORS) por parte del equipo local, y es la fase que permite obtener los valores óptimos de velocidad y de potencia que el equipo local debe utilizar para comunicarse con cada uno de sus vecinos.

Cada equipo ZBP-1 tiene que estar identificado de forma específica e inequívoca dentro de la red en la que se encuentra ubicado mediante su número de identificación de equipo (parámetro *Local ID*) y tener, además, programada su dirección IP (parámetro *IP address*) y máscara (parámetro *Mask*).

Una vez programado, el equipo ZBP-1 local inicia, tras el arranque, el envío de unos paquetes de *Broadcast* específicos cuyo *feedback* le permitirá ir identificando a los distintos equipos ZPB-1 vecinos, así como establecer para cada uno de los mismos los valores óptimos de funcionamiento.

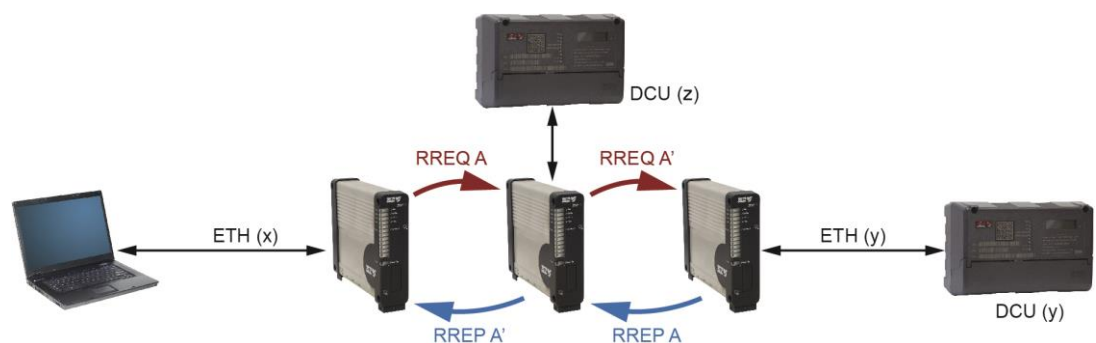
Estos valores son el **valor de potencia** y la **velocidad en bit/s** (asociada al tipo de modulación y al modo de trabajo) para cada una de las portadoras, los cuales deberá utilizar el equipo local para poder transmitir paquetes hacia un equipo vecino. Como orientación, en el apartado 1.3, *Parámetros OFDM*, se indican algunos valores de velocidad.

## 1.2.2 Fase de Búsqueda y selección de rutas

Tras la *Conexión PLUG&PLAY*, se inicia la fase de búsqueda de rutas y de selección de las mismas por parte del equipo originador.

El procedimiento de búsqueda de rutas para direcciones IP/MAC se resume en la FIGURA 1.

FIGURA 1 Procedimiento de búsqueda de rutas



Como puede verse en la FIGURA 1, una vez recibe una petición de búsqueda de la dirección IP/MAC desde el puerto Ethernet (arp), el equipo originador lanza un mensaje de *Broadcast*, llamado **RREQ**, por el puerto PLC.

Este mensaje de búsqueda llega a todos los equipos vecinos. El equipo que no conozca la dirección, retransmitirá el mensaje RREQ. En cambio, el equipo que tenga esa dirección IP/MAC dentro de su tabla de IP/MAC locales, contestará al equipo originador mediante un mensaje *Unicast*, llamado **RREP**, utilizando el mismo camino que el utilizado por el mensaje RREQ.

La ruta se forma cuando los mensajes de contestación RREP llegan al equipo originador.

De entre todas las rutas formadas, el equipo originador escogerá la ruta más óptima para la transmisión. La ruta escogida se mantendrá válida mientras esté en uso. Si deja de utilizarse, transcurridos dos minutos (este valor es programable), la ruta se eliminará y deberá volverse a establecer una nueva ruta para iniciar una nueva comunicación.

En cada tramo de la ruta, el equipo correspondiente utiliza los valores óptimos de **potencia** y **velocidad en bit/s** que ha obtenido en un inicio en la conexión PLUG&PLAY.

## 1.3 PARÁMETROS OFDM

Como orientación para el usuario, en este apartado se muestran unas tablas con valores de velocidad en bit/s que el equipo establece automáticamente para cada una de las portadoras, en función del ruido medido en la línea.

Asimismo, se indican los valores de ancho de banda y rango de frecuencia que el usuario puede configurar desde la gestión del equipo.

# ZBP-1

Ofdm mode	Turbo Código	Repetición	Velocidad con QPSK	Velocidad con 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	SÍ	640 Kbps	1,28 Mbps
3	3/4	NO	7,2 Mbps	14,4 Mbps

TABLA 1

Velocidades para BW=6 MHz (el valor lo establece el equipo automáticamente para cada una de las portadoras)

Ofdm mode	Turbo Código	Repetición	Velocidad con QPSK	Velocidad con 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	SÍ	160 Kbps	320 Kbps
3	3/4	NO	1,8 Mbps	3,6 Mbps

TABLA 2

Velocidades para BW=1,5 MHz (el valor lo establece el equipo automáticamente para cada una de las portadoras)

Ofdm mode	Turbo Código	Repetición	Velocidad con QPSK	Velocidad con 16-QAM
0	8/9	NO	19,2 Mbps	-
1	1/3	NO	6,4 Mbps	12,8 Mbps
2	1/3	SÍ	1,28 Mbps	2,56 Mbps
3	3/4	NO	14,4 Mbps	28,8 Mbps

TABLA 3

Velocidades para BW=12 MHz (el valor lo establece el equipo automáticamente para cada una de las portadoras)



# ZBP-1

Modulation	Tipo de modulación
0	QPSK
1	16-QAM

TABLA 4 Tipo de modulación (el valor lo establece el equipo automáticamente para cada una de las portadoras)

Tone Mask	Repetición	BW (1,5 MHz)	BW (6 MHz)	BW (12 MHz)
<i>Low band</i>	NO	-	2 ÷ 8 MHz	-
<i>High band</i>	SÍ	2 ÷ 3,5 MHz	8 ÷ 14 MHz	-
<i>Full band</i>	NO	-	-	2 ÷ 14 MHz

TABLA 5 Espectro de frecuencias (el valor lo establece el usuario)

Compact Band	Ancho de banda (BW)
OFF	6 MHz
ON	1,5 MHz

TABLA 6 Ancho de banda de transmisión (BW) (el valor lo establece el usuario)

## 1.4 ESPECIFICACIONES TÉCNICAS

### 1.4.1 Características del equipo

Las prestaciones *software/firmware* ofrecidas por el ZBP-1 son las siguientes:

- posibilidad de operar como **encaminador de nivel 3** para IPv4 (**router**)
- o como **conmutador de nivel 2 (bridge)** entre la interfaz Ethernet y la interfaz PLC,
- y soporte para **IEEE802.1Q** (Gestión de hasta 8 **VLANS**).

### 1.4.2 Interfaces del equipo

- 1 puerto Ethernet (Eth) en configuración 10/100Base-Tx con conector RJ-45 hembra. Este conector se utiliza para la conexión de los datos de usuario, y para la configuración del equipo (por HTTP, Telnet o SSH).
- 1 conector BNC (PLC) hembra para cable RG-58. Este conector se utiliza para la conexión a línea.
- 1 conector DB9 hembra (COM) como puerto de servicio para la configuración del equipo por Consola de Usuario (CLI).

### 1.4.3 Características de la transmisión PLC

- Protocolo de enrutamiento PLC: **LOADnG**
- El protocolo de conexión entre equipos se basa en la búsqueda de rutas para **direcciones IP/MAC** y consta de dos fases bien diferenciadas: la fase de **Conexión PLUG&PLAY** y la fase de **Búsqueda y selección de rutas**.
- Tiempo de vida de las rutas (*lifetime routes*) seleccionable por el usuario. El valor mínimo es 5 s. El valor establecido en fábrica es de 120 s.

# ZBP-1

- Rango de frecuencias y ancho de banda seleccionable por el usuario entre:

<b>Tone Mask</b>	<b>BW (1,5 MHz)</b>	<b>BW (6 MHz)</b>	<b>BW (12 MHz)</b>
<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

- Velocidad de transmisión de hasta 28,8 Mbit/s.  
La velocidad la establece el equipo automáticamente para cada una de las portadoras, en función del ruido medido en la línea. Véase TABLA 1 a TABLA 3.
- Modulación OFDM de 380 portadoras útiles. En función del ruido medido en la línea, el equipo puede anular automáticamente las portadoras afectadas.
- Modulación QPSK/16-QAM con aplicación independiente en cada portadora.  
Este valor lo establece automáticamente el equipo para cada una de las portadoras, en función del ruido medido en la línea.
- Turbo código con FEC (Forward Error Correction) de ratio 8/9, 1/3 y 3/4.  
El ratio del Turbo código lo establece automáticamente el equipo para cada una de las portadoras, en función del ruido medido en la línea.
- Potencia de salida entre 0 y 15.  
El valor lo establece automáticamente el equipo, en función de la señal medida en la línea.
- Alcance de hasta 5 km.

## 1.4.4 Gestión del equipo

- Acceso local y remoto mediante consola de CLI (Command Line Interface) o servidor web incorporado (HTTP/HTTPS), servidor Telnet y SSH.

## 1.4.5 Servicios adicionales

- Cliente DHCP.
- Servidor DNS.
- Cliente TACACS+.
- Agente SNMP (SNMPv1, SNMPv2c y SNMPv3).

## 1.4.6 Accesorios

- Tornillos y material de anclaje para sujeción del equipo en carril DIN.

## 1.4.7 Certificaciones

- CE.
- Diseñado para Centros de Transformación.
- Diseñado para aplicaciones industriales.

## 1.4.8 Características mecánicas

- Dimensiones: Altura: 150 mm ; Anchura: 40 mm; Profundidad: 177 mm.  
Véase FIGURA 2.
- Peso: 539 g.
- Montaje mural. Dispone de 4 taladros de fijación mediante tornillería estándar M4.  
Véase FIGURA 3.  
Carril DIN mediante accesorio adicional.
- Grado de protección IP: IP 2xB.
- Material: Aleación de aluminio 6060 T5 lacado (RAL 9006) y plástico (RAL 7024) STAREX ABS VH-0800 Ignífugo (UL 94 V0).

## 1.4.9 Condiciones de funcionamiento

- Alimentación: 48 V<sub>CC</sub> aislada (19-72V<sub>CC</sub>).  
La fuente está protegida mediante diodo contra inversión de polaridad.
- Consumo de potencia mínimo a 48 V<sub>CC</sub>: 6 W
- Consumo de potencia máximo a 48 V<sub>CC</sub>: 48 W
- Rango de temperatura: -25°C a +60°C.
- Humedad relativa no superior al 95%, según CEI 721-3-3 clase 3K5 (climatograma 3K5).
- Emisiones R.F.: según la norma EN 55022.
- Rigidez dieléctrica: según la norma EN 60255-5.
- Compatibilidad electromagnética.
  - Inmunidad a las descargas electrostáticas: según la norma EN 61000-4-2.
  - Inmunidad a los campos electromagnéticos permanentes de R.F.: según la norma EN 61000-4-3.
  - Inmunidad a los transitorios rápidos en ráfagas: según la norma EN 61000-4-4.
  - Inmunidad a la onda de choque: según la norma EN 61000-4-5.
  - Inmunidad a las perturbaciones conducidas por campos de R. F.: según la norma EN 61000-4-6.
  - Inmunidad a los campos electromagnéticos a frecuencia industrial: según la norma EN 61000-4-8.
  - Inmunidad a la onda oscilatoria amortiguada: según la norma EN 61000-4-18 (EN 61000-4-12).
  - Inmunidad a los huecos, interrupciones y variaciones de tensión en c.c.: según la norma EN 61000-4-29.
- Condiciones mecánicas de funcionamiento.
  - Vibración según norma ETSI EN 300019-2-2.
  - Caída según norma ETSI EN 300019-2-2.

## 1.4.10 Condiciones de transporte y almacenaje

- Rango de temperatura: -40°C a +70°C según la norma EN 60870-2-2.

## 1.5 ADVERTENCIAS

### 1.5.1 Advertencias previas



- !
1. La instalación del ZBP-1 en Centro de Transformación (CT) está sujeta de modo genérico al cumplimiento de todas las medidas de seguridad y de prevención de riesgos laborales que para este entorno de trabajo tenga establecida la compañía eléctrica usuaria de estos dispositivos y de los estándares de seguridad (EN 50110).
  2. De modo específico, para la instalación y manipulación del ZBP-1 se deben cumplir los siguientes requisitos:
    - Únicamente personal cualificado y designado por la compañía propietaria de la instalación debe llevar a cabo la instalación y manipulación del ZBP-1.
    - El entorno de funcionamiento debe ser el apropiado para el ZBP-1, asegurando el cumplimiento de las condiciones indicadas en el apartado 1.4.9.
  3. ZIV no se hace responsable de cualquier daño a personas, instalaciones o a terceros derivados del no cumplimiento de los puntos 1 y 2.

### Consideraciones de seguridad del equipo



- ! 1. Debe realizarse la conexión de la toma de tierra antes de conectar cualquier cable de alimentación.
- 2. ZIV no se hace responsable no se hace responsable de cualquier daño a personas o a terceros derivados del no cumplimiento del punto 1.

- ! 1. El equipo contiene componentes sensibles a la electricidad estática, por lo que se deben cumplir los siguientes requisitos:
  - El personal designado para llevar a cabo la instalación y mantenimiento del ZBP-1 debe estar siempre libre de electricidad estática, por lo que siempre debe emplear una pulsera antiestática y/o talonera conectada a tierra.
  - El habitáculo del ZBP-1 debe estar libre de elementos que faciliten la generación de electricidad estática y, en el caso de los suelos provistos de moqueta, que ésta sea antiestática.
- 2. ZIV no se hace responsable de cualquier daño que pueda sufrir el equipo derivado del no cumplimiento del punto 1.

## 2 CARACTERÍSTICAS MECÁNICAS Y ELÉCTRICAS

Las dimensiones generales en mm del ZBP-1 se muestran en la FIGURA 2.

La caja está preparada para su instalación en montaje mural (*Wall mount*) o en carril DIN mediante accesorio adicional.

El ZBP-1 dispone de 4 taladros de fijación mediante tornillería estándar M4, cuya posición puede verse en la FIGURA 3.

La posición de la hendidura para la instalación del accesorio de fijación en carril DIN puede verse en la FIGURA 4. El detalle de instalación puede verse en los planos adjuntos.

FIGURA 2 Dimensiones generales en mm del ZBP-1





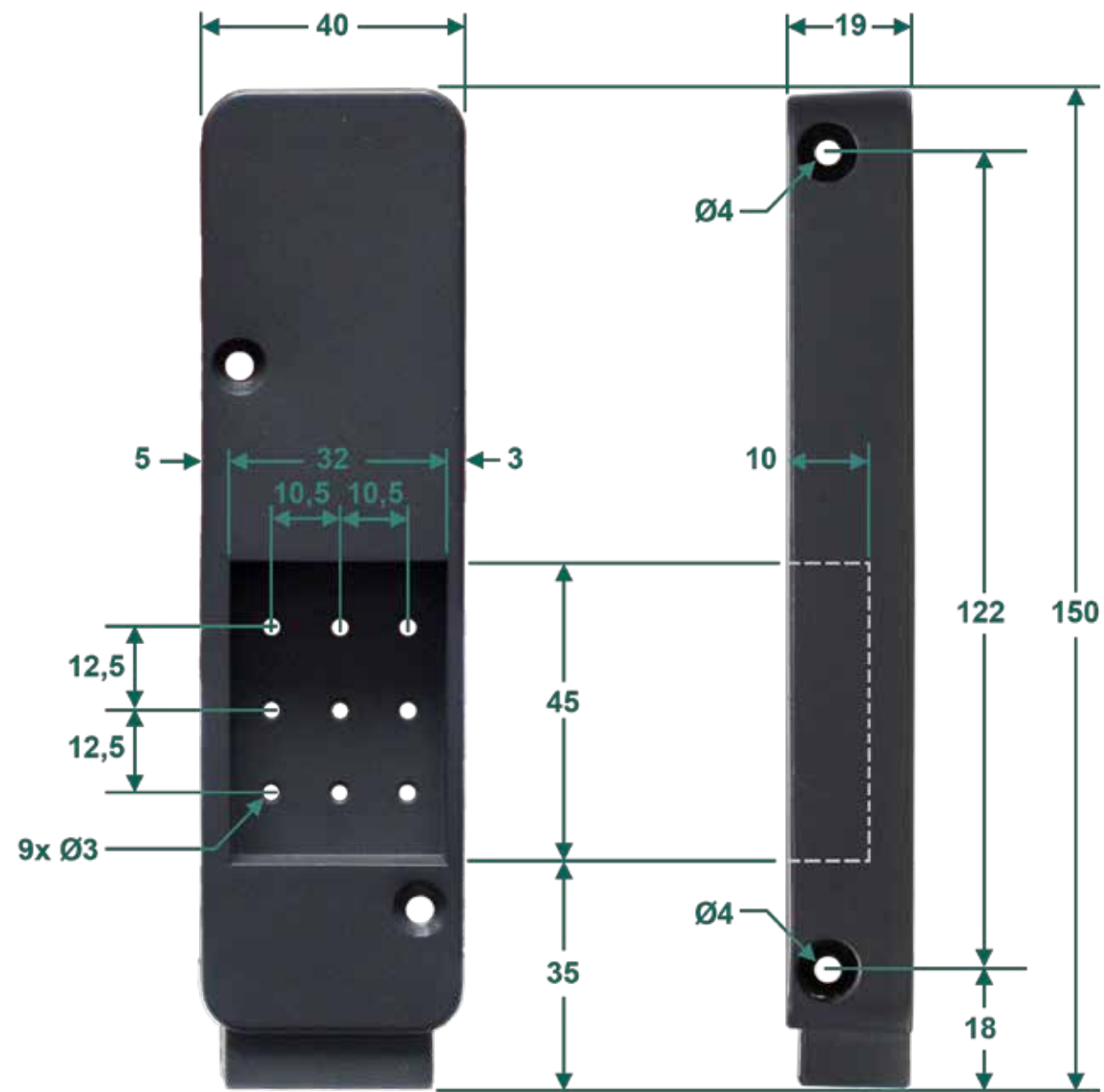
# ZBP-1

FIGURA 3 Detalle de la fijación mural



FIGURA 4 Detalle de la hendidura para la instalación del accesorio de fijación en carril DIN






Dimensiones de la tapa posterior



Equipo sin soportes para carril DIN



Equipo con soportes para carril DIN

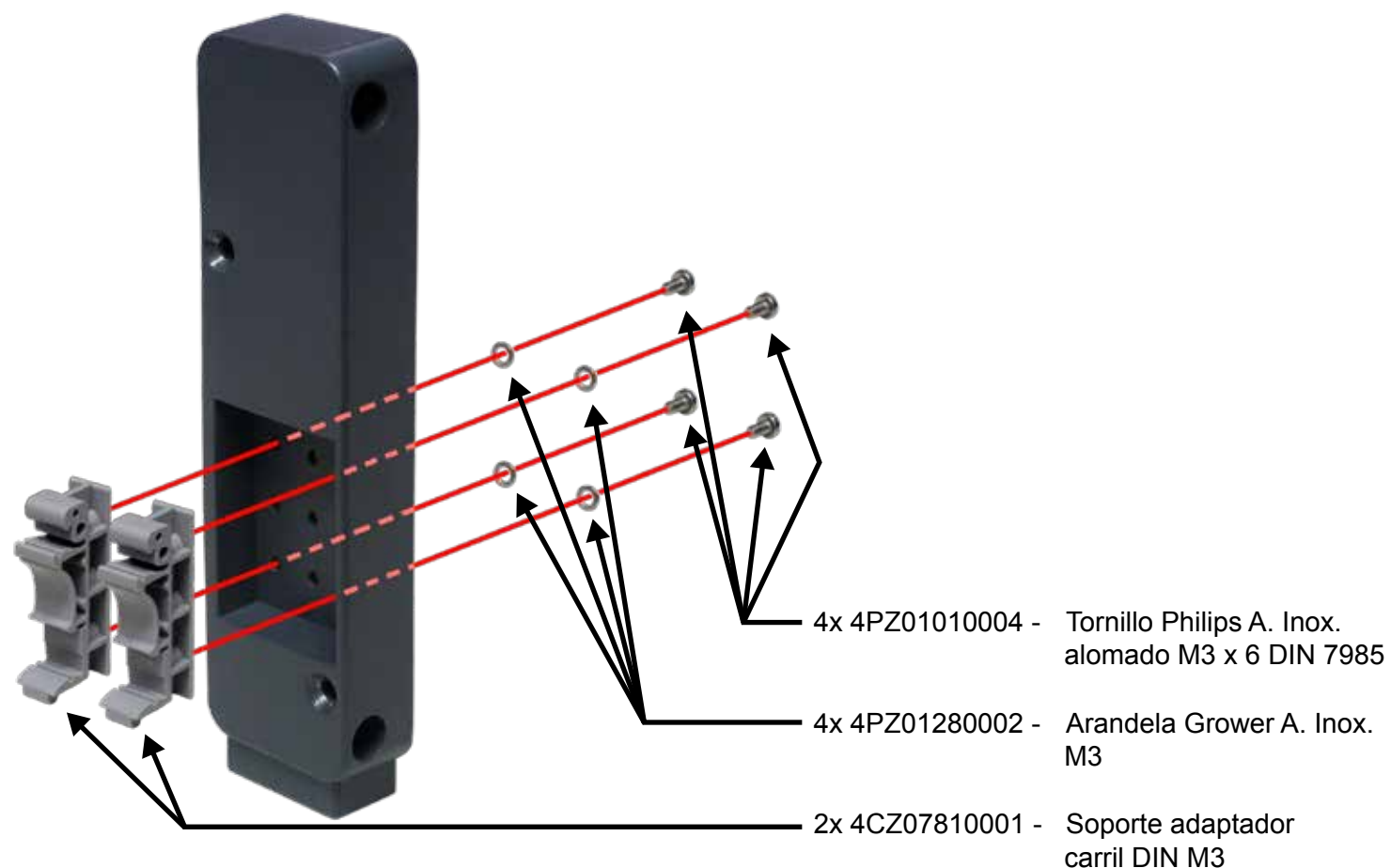
Pertenece a: ZBP-1					Cód. Prod.		Rev.	
					-		0	
Fecha	Realizado	V° B°	Comprobado	V° B°	Aprobado	V° B°	Archivo	
08-02-2017	J. F. Gil						MGZBP10200	
							<b>PROCESO DE FIJACIÓN DE LOS SOPORTES PARA INSTALACIÓN EN CARRIL DIN (1/2)</b>	
							Siglas	Hoja
							<b>ZBP-1</b>	1/3



**Paso 1:** Retirar los tornillos y extraer la tapa posterior.




**Paso 2:** Retirar la cinta adhesiva que protege los orificios para los tornillos de los soportes de carril DIN.



**Paso 3:** Atornillar los soportes de carril DIN a la tapa posterior tal como se muestra en la imagen.



**Paso 4:** Volver a colocar la tapa posterior, sujetándola con los tornillos extraídos en el paso 1.

Pertenece a: ZBP-1					Cód. Prod.	Rev.
					-	0
Fecha	Realizado	V° B°	Comprobado	V° B°	Aprobado	Archivo
08-02-2017	J. F. Gil					MGZBP10300
					<b>PROCESO DE FIJACIÓN DE LOS SOPORTES PARA INSTALACIÓN EN CARRIL DIN (2/2)</b>	
					Siglas	Hoja
					<b>ZBP-1</b>	2/3

## Fijación en el carril DIN



**Paso 1:** Encajar las uñas superiores de las pinzas en el perfil superior del carril DIN.



**Paso 2:** Enderezar el equipo haciéndolo pivotar sobre las uñas superiores de la pinza hasta hacer encajar las uñas inferiores en el perfil inferior del carril DIN.

## Liberación del carril DIN




**Paso 1:** Con ayuda de un destornillador, liberar las uñas inferiores de las pinzas.

**Paso 2:** Tirar levemente del equipo, haciéndolo pivotar sobre las uñas superiores.



**Paso 3:** Extraer completamente el equipo tirando de él hacia arriba.

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

INSTALACIÓN Y DESINSTALACIÓN EN CARRIL DIN

# ZBP-1

## 2.1 ALIMENTACIÓN

El ZBP-1 se alimenta a una tensión nominal de 48 Vcc aislada (19-72 Vcc), a través del conector que se muestra en la FIGURA 5.

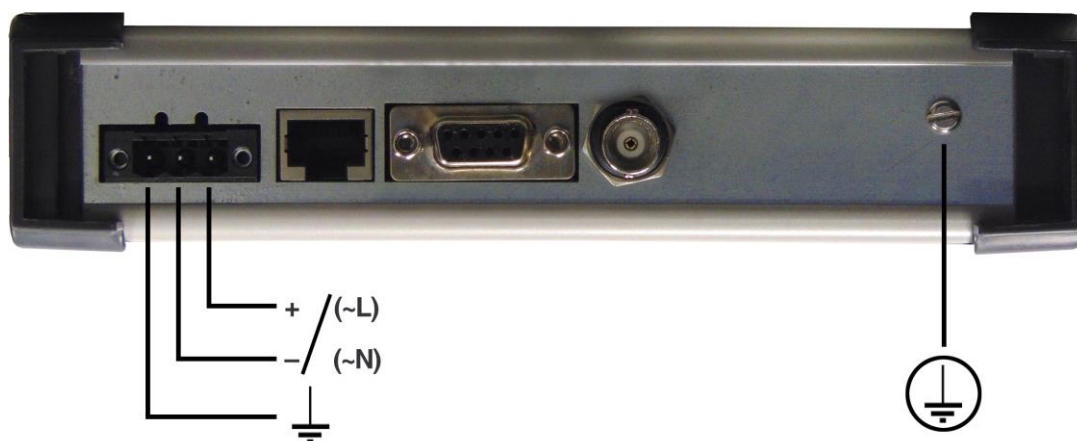
El conector hembra suministrado con el equipo es apto para conductores rígidos o flexibles de hasta 2.5 mm<sup>2</sup>.



Realizar la conexión de la toma de tierra, véase FIGURA 5, antes de conectar cualquier cable de alimentación.

La fuente está protegida mediante diodo contra inversión de polaridad.

FIGURA 5 Disposición del conector de alimentación y de la toma de tierra del ZBP-1



## 2.2 CONECTOR ETHERNET

El conector Ethernet se encuentra dispuesto junto al conector de alimentación, véase FIGURA 5. Dicho conector corresponde a una interfaz 10/100Base-Tx con conector RJ-45.

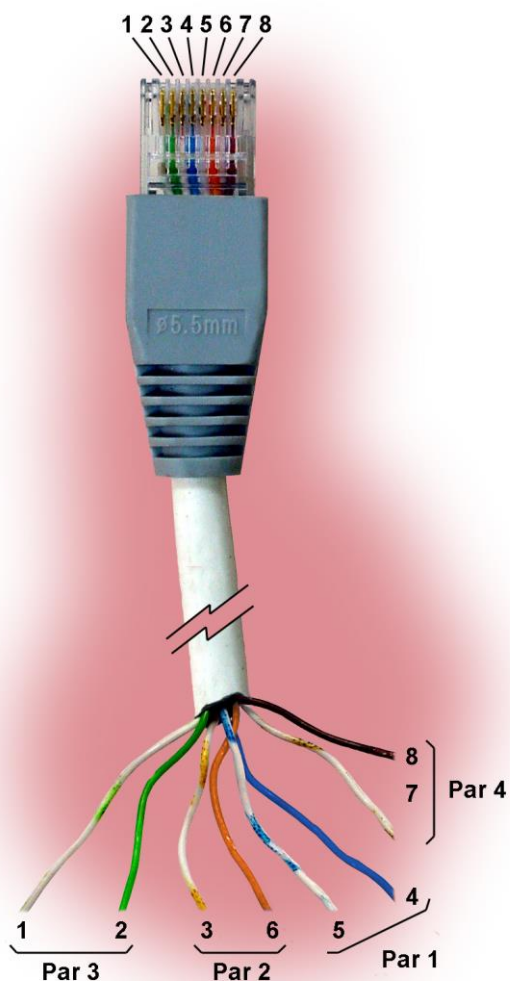
En el puerto 10/100Base-Tx, el cable utilizado para llevar a cabo la conexión correspondiente debe ser cable de 4 pares trenzados no blindados categoría cinco (UTP-5) con conectores RJ-45 de 8 contactos. La longitud del cable no debe ser superior a 100 m.

# ZBP-1

El cable UTP-5 está formado por ocho hilos de cobre, que componen los cuatro pares trenzados, cubiertos por un plástico de aislamiento de diferente color. El color de los hilos que componen cada uno de los pares, según el estándar ANSI/TIA/EIA-568-A, es el que se indica en la FIGURA 6.

FIGURA 6

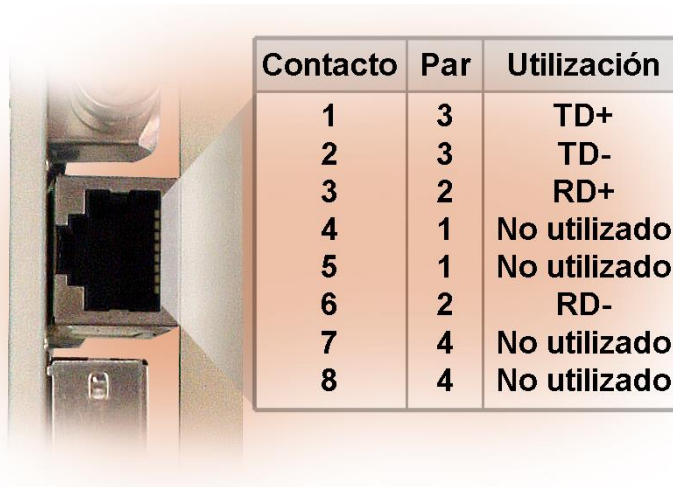
Cable de pares trenzados no blindados categoría cinco (UTP-5) con conector RJ-45 según el estándar ANSI/TIA/EIA-568-A



En la FIGURA 7 se indica la utilización de cada uno de los contactos del conector RJ-45 además del par al que pertenecen según el estándar ANSI/TIA/EIA-568-A, en la interfaz de red 10/100Base-Tx.

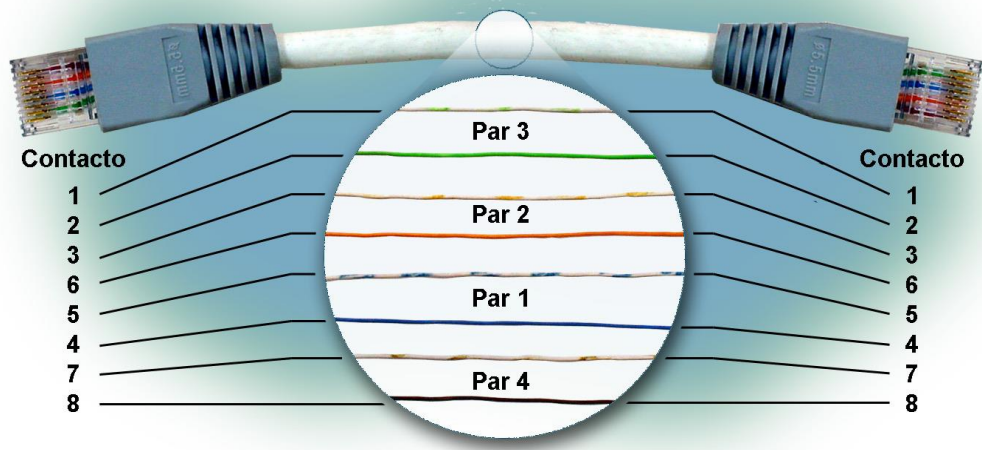
# ZBP-1

FIGURA 7 Señales del conector RJ-45 en la interfaz 10/100Base-Tx



Los cables utilizados deben ser cables de conexión directa, véase FIGURA 8, en los que los 4 pares se corresponden en ambos extremos del cable.

FIGURA 8 Cable de conexión directa



# ZBP-1

## 2.3 INDICACIONES ÓPTICAS

El ZBP-1 dispone en su parte frontal de distintos LEDs, véase FIGURA 9, cuya descripción se indica a continuación.

FIGURA 9 Detalle de los distintos LEDs del ZBP-1





# ZBP-1

LED Power On	<b>Verde.</b> Se ilumina en permanencia cuando al equipo se le suministra tensión de alimentación externa.
LED Status	<b>Bicolor.</b> Se ilumina en <b>rojo</b> cuando la unidad de modem digital está arrancando.  Se ilumina en <b>verde</b> cuando la unidad de modem digital ha arrancado correctamente y está operativa.
LED Amp On	<b>Ámbar.</b> Se ilumina cuando el amplificador está activo, es decir, se transmite señal a la línea.
LED Eth Link	<b>Ámbar.</b> Se ilumina en permanencia cuando el enlace está establecido de forma correcta.
LED Eth Act	<b>Verde.</b> Se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.
LED PLC Status	<b>Tricolor.</b> Se ilumina en <b>verde</b> cuando la carga útil ( <i>Payload</i> ) es OK.  Se ilumina en <b>ámbar</b> cuando la carga útil es incorrecta. Se ilumina en <b>rojo</b> cuando la trama de control es incorrecta.

# ZBP-1

## 3 ACCESO AL EQUIPO

El ZBP-1 es gestionable de forma local y remota, bien mediante consola o a través de un servidor web incorporado (HTTP/HTTPS).

### 3.1 CONSOLA

El equipo proporciona una aplicación de consola de usuario, denominada *CLI (Command Line Interface)*, accesible de forma local a través del conector DB9 en modo DCE, y que opera a 115200 bit/s, con caracteres de 8 bits, sin paridad y con un bit de stop.

También es posible obtener acceso a la consola de forma local o remota mediante una sesión Telnet o SSH.

El *Apéndice A* contiene toda la información necesaria para la utilización de la consola de usuario *CLI*. El apéndice explica los métodos de acceso, local y remoto, y los comandos disponibles desde la consola.

### 3.2 SERVIDOR HTTP DEL EQUIPO

El servidor HTTP incluido en el equipo proporciona el acceso a las páginas HTML que ofrecen el acceso a la totalidad de los datos de configuración. Para poder acceder al servidor HTTP del equipo ZIV, es necesario configurar adecuadamente la dirección IP y máscara del ordenador (PC).

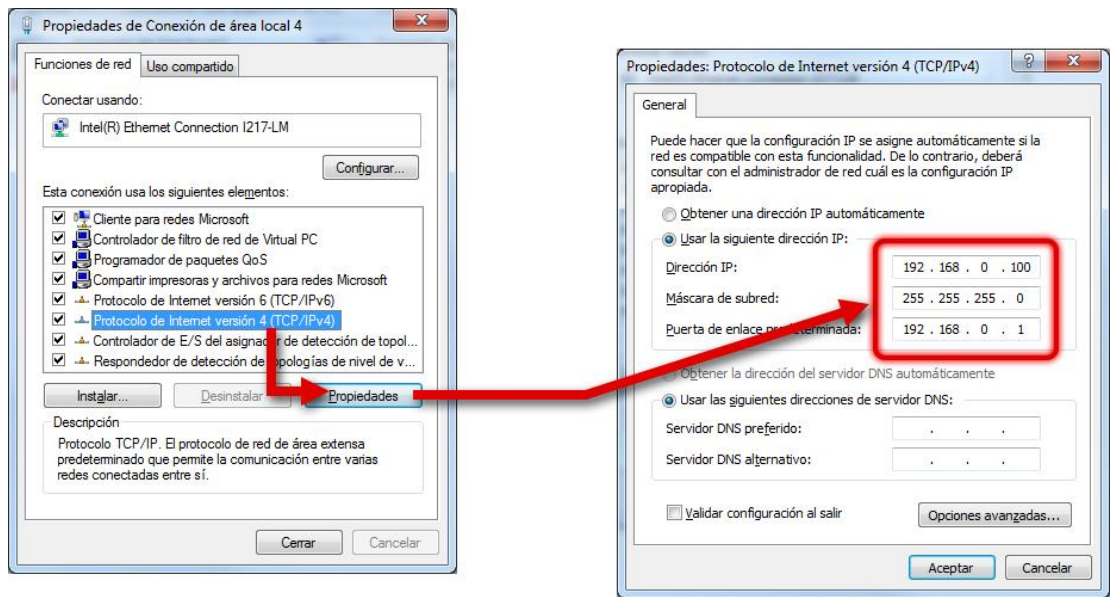
Se asume que el usuario dispone de unos conocimientos mínimos de direccionamiento IP y de dispositivos de *networking* tales como *hubs*, *switches*, *routers*, etc.

Así, si el ZBP-1 y el ordenador están conectados directamente o a través de una LAN (pertenecen a la misma red), la dirección IP de cada uno de ellos debe tener el mismo número de red y distinto número de host, por lo que la máscara de subred debe ser la misma para ambos. La puerta de enlace predeterminada no es necesario configurarla.

En cambio, si el ZBP-1 y el ordenador pertenecen a distintas LANs y la conexión entre ellos es vía WAN, sus direcciones IP pueden tener distinto número de red, pero ambos deben estar conectados a algún dispositivo (puerta de enlace predeterminada o Gateway) que sea capaz de interconectar LANs

De fábrica, la dirección IP del ZBP-1 es 192.168.0.1 con máscara 255.255.255.0.

FIGURA 10 Acceso al equipo mediante servidor HTTP



- IP LAN por defecto: 192.168.0.1/255.255.255.0
- Configurar la IP del PC con un rango 192.168.0.0/24 (Ej: 192.168.0.100). Para ello, acceder a *Centro de redes y recursos compartidos* del Panel de control.

## 4 CONFIGURACIÓN Y GESTIÓN

La configuración y la gestión del ZBP-1 puede llevarse a cabo tanto mediante la consola como mediante el acceso a las páginas HTML del equipo.

A continuación, se describen en detalle la totalidad de los parámetros que controlan el funcionamiento del equipo, habiéndose usado las páginas HTML reales como muestra gráfica auxiliar.

El árbol de menús de las páginas HTML puede verse en la FIGURA 11.

Los comandos **Apply** y **Save** se hallan en la zona inferior del árbol de menús, y únicamente son visibles cuando el perfil del usuario tiene derecho de administración.

Para el detalle de los comandos **Reboot**, **Reflash** y **Configuration files**, véanse respectivamente los apartados 4.6, 4.7 y 4.8.

Los comandos **Apply**, **Save** y **Reboot** solicitan confirmación de la operación al usuario antes de su ejecución efectiva.

Siempre que se realicen cambios, con independencia de si es vía consola o servidor HTTP, es necesario indicar al equipo que se desea hacer con ellos. Existen dos opciones:

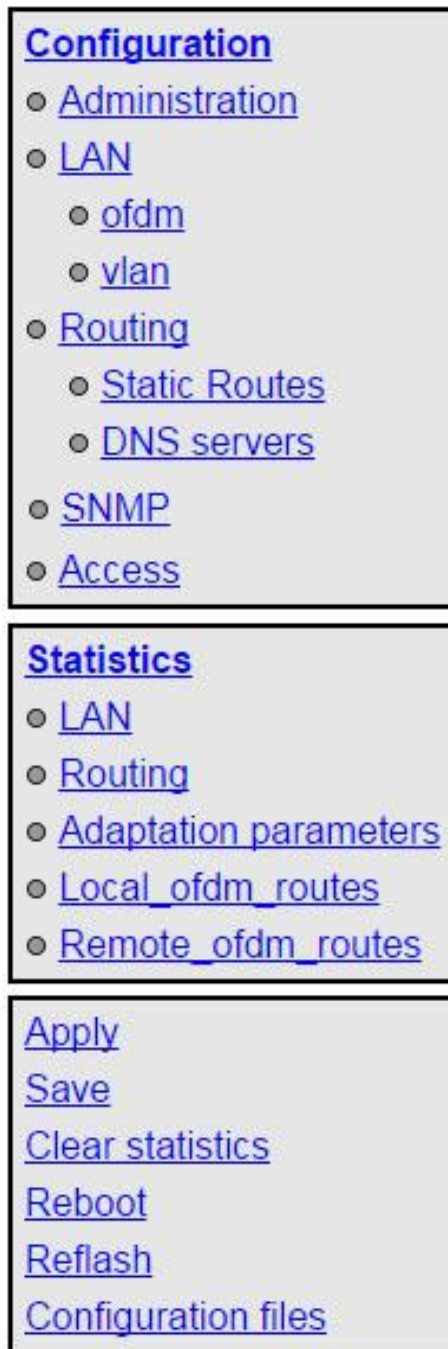
- la primera es ejecutar el comando **Apply**, lo que supone el uso inmediato de los cambios realizados.
- la segunda es ejecutar el comando **Save**, lo que supondrá que los cambios serán operativos cuando se reinicialice el equipo.

En el caso de acceder mediante el servidor HTTP, después de realizar los cambios y antes de ejecutar bien **Apply** o **Save**, es imprescindible lanzar el botón **Send** para que el equipo obtenga los nuevos valores deseados.

En el caso de ejecutar el comando **Apply**, si se desea que los cambios tengan carácter permanente, deberá ejecutarse también el comando **Save**.

La única excepción son los cambios que afectan a la configuración SNMP. Cualquier cambio efectuado en la configuración del agente SNMP **únicamente** será activo después de realizar un **RESET** al equipo. El comando **Apply** no es suficiente, por lo que los cambios deberán almacenarse previamente con el comando **Save** antes de solicitar la reinicialización.

FIGURA 11 Árbol de menús de páginas HTML



El árbol de menús tiene una presencia permanente en todas las páginas empleadas por el servidor HTTP.

## 4.1 PARÁMETROS GENERALES

Los parámetros generales se agrupan en tres zonas bien diferenciadas, véase FIGURA 12, las cuales se describen en los apartados siguientes.

FIGURA 12 Pantalla de configuración principal

The screenshot displays the main configuration interface, organized into three distinct sections:

- Identification:** A table-like form with the following fields:
  - Hostname: zbp
  - DHCP client ID: (empty)
  - Location: unknown
  - Contact: unknown
  - Product: 4ZBP010000000100
  - Firmware version: 3.35.1.36897
  - Firmware reference: 4WF71300040-R001
  - Tracking #: d4790d38bc8e18e3
  - Serial #: 1900128
- Access Control:** A form with the following fields:
  - Guest's login: guest
  - Guest's password: [Change](#)
  - Admin's login: admin
  - Admin's password: [Change](#)
- Others:** A form with the following fields:
  - Time zone: UTC (dropdown menu)
  - Serial Log:
  - Enable Periodic Reset:
  - Periodic reset period (days): 1

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

### 4.1.1 Identificación del equipo

La zona de identificación incluye el nombre del equipo (**hostname**), su ubicación (**location**) y los datos de contacto de la persona o entidad al cargo (**contact**). Se exige como mínimo una cadena de texto con al menos un carácter.

Además, el sistema proporciona información sobre la versión de software en ejecución (**firmware version**), el número de serie del equipo (**serial**) y el número de seguimiento (**tracking**).

El parámetro **DHCP client ID** permite la configuración de la opción *Client ID* de la RFC 2131 en las solicitudes de configuración DHCP. Si este parámetro no se configura, la dirección MAC de la interfaz en la que se envía la solicitud se utiliza como valor por defecto del *Client ID*.

## 4.1.2 Control de acceso

El control de acceso permite determinar los nombres de usuario (**login**) y la contraseña asociada (**password**) para los dos perfiles predeterminados: invitado (**guest**) y administrador (**admin**).

El perfil de invitado únicamente tiene acceso a operaciones de consulta. Por el contrario, el perfil administrador tiene acceso a la totalidad de los datos de configuración del sistema.

Tal y como se resume en la TABLA 7, los valores de estos parámetros por defecto son **guest** y **admin** como nombres de usuario, siendo **passwd01** y **passwd02** las contraseñas correspondientes.

No olvidar que el sistema distingue los caracteres en minúscula de los caracteres en mayúscula.

TABLA 7

Claves de acceso por defecto del sistema

	Nombre de usuario ( <i>login</i> )	Contraseña ( <i>password</i> )
Usuario Invitado	guest	passwd01
Usuario Administrador	admin	passwd02

Es altamente recomendable modificar, como mínimo, la contraseña del perfil administrador en la primera configuración de cada equipo.

Es aconsejable almacenar la nueva contraseña en algún tipo de registro ya que, de olvidarla, no podría accederse al servidor web.

## 4.1.3 Otros

Esta zona contiene cuatro parámetros. El primero de ellos, **Time zone**, establece la zona horaria en relación a UTC.

El segundo parámetro, **Serial log**, indica si el equipo activa la transmisión de los datos de log sobre el puerto serie de servicio desde el momento inicial de arranque (control *Checkbox* seleccionado) o no.

El tercer parámetro, **Enable periodic reset**, permite al usuario indicar si desea que el equipo se reinicialice de forma automática cada cierto tiempo, el cual se establece en días mediante el último parámetro, **Periodic reset period**.

## 4.2 CONFIGURACIÓN ADMINISTRATION

El equipo dispone de un servidor HTTP integrado para la gestión del mismo. El servidor soporta el protocolo HTTP y también el protocolo HTTPS, pudiendo el usuario habilitar de forma selectiva su uso, así como el puerto correspondiente.

FIGURA 13 Pantalla de configuración del menú **Administration**

**Web Access**

HTTP

HTTP port

HTTPS<sup>1</sup>

HTTPS port

1 Certificates must be loaded in CLI

El procedimiento para instalar los certificados está descrito en el apartado A.3 del Apéndice A, *Estructura de datos en CLI*.



## 4.3 CONFIGURACIÓN LAN

El menú **LAN** presenta dos submenús: **ofdm** y **vlan**.

### 4.3.1 Configuración Ofdm

En este submenú se lleva a cabo la configuración de los parámetros relacionados con la transmisión de la información.

La pantalla asociada presenta tres zonas bien diferenciadas, las cuales se describen a continuación.

FIGURA 14 Pantalla de configuración del submenú **ofdm** del menú **LAN**

The screenshot shows the 'OFDM parameters' configuration screen. It is divided into three main sections:

- OFDM parameters:** Contains five settings: 'Band' (dropdown menu set to 'HIGH\_BAND'), 'Compact Band' (dropdown menu set to 'OFF'), 'Lifetime routes' (text input field with '120'), 'Thres. safe mode' (dropdown menu set to 'LOW'), and 'Adj. adapt. datarate' (dropdown menu set to 'VERY\_HIGH').
- OFDM device:** Contains one setting: 'Local ID' (text input field with '1').
- Blacklisted Identifiers:** Contains 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.	Action
1	3	Delete
2	6	Delete
3		Add

#### OFDM parameters:

Esta zona contiene los parámetros siguientes:

- **Band.** Permite especificar el espectro de frecuencias de trabajo del equipo. En **LOW\_BAND** el equipo trabaja en la parte baja del espectro (2 a 8 MHz para BW de 6 MHz). En **HIGH\_BAND** el equipo trabaja en la parte alta del espectro (8 a 14 MHz para BW de 6 MHz). En **FULL\_BAND** el equipo trabaja en todo el espectro de frecuencias (2 a 14 MHz para BW de 12 MHz).

- **Compact Band.** Permite especificar el ancho de banda de transmisión (BW) del equipo. En **OFF** el equipo trabaja en un ancho de banda de 6 MHz, mientras que en **ON** en un ancho de banda de 1,5 MHz. En **ON** es necesario configurar el campo **Band** en modo **HIGH\_BAND**.
- **Lifetime routes.** Permite especificar el tiempo de vida de las rutas, siendo el valor mínimo de 5 segundos. El equipo sale de fábrica con el valor 120 segundos.
- **Thres. safe mode.** Permite especificar la rapidez con la que el equipo pasará a trabajar en modo robusto (con redundancia) cuando detecta que las condiciones del canal no son las más óptimas. En ALWAYS el equipo siempre trabaja en modo robusto. La rapidez para pasar a modo robusto es alta en modo HIGH, siendo menor en modo MEDIUM y más lenta en modo LOW.
- **Adj. adapt. datarate.** Permite especificar la rapidez con la que se desea que el equipo adapte el **datarate** a las nuevas condiciones del canal una vez se detectan. Existen cinco niveles: AGGRESSIVE, VERY\_HIGH, HIGH, MEDIUM y LOW. Así, en modo VERY\_HIGH el equipo detecta muy rápidamente las nuevas condiciones del canal y adapta el **datarate** rápidamente a las mismas, mientras que en modo LOW necesita mucho más tiempo.

#### OFDM device:

Esta zona contiene el parámetro siguiente:

- **Local ID.** Identificador del equipo. Por defecto, está configurado el ID=1. Este indicador tiene que ser diferente en cada equipo. Se utiliza para identificar los equipos vecinos (NEIGHBOR) y para los ajustes de reloj.  
En una subred, siempre debe configurarse un equipo con Local ID=1. Este equipo se considera el Master y, como tal, es el encargado de enviar el reloj al resto de equipos de la subred para que todos los equipos de la red estén sincronizados.

#### Blacklisted Identifiers:

Esta zona contiene el parámetro siguiente:

- **Ident ID.** Identificador del Local ID a descartar. Se descartarán todos los mensajes procedentes de los equipos añadidos en la lista negra. Estos equipos no podrán identificarse como equipos vecinos (NEIGHBORS).

## 4.3.2 Configuración Vlan

En este submenú se lleva a cabo la asignación de los puertos Ethernet y PLC del equipo a alguna de las VLAN definidas.

La pantalla asociada presenta tres zonas bien diferenciadas, las cuales se describen a continuación.

FIGURA 15 Pantalla de configuración del submenú **vlan** del menú **LAN**

#	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:

Cada VLAN se distingue del resto gracias a un identificador específico, denominado usualmente como **Vid**, que se propaga en el tag estándar especificado en el IEEE 802.1q. El uso del tag permite que varias VLAN puedan compartir recursos, bien sean éstos equipos de conmutación, o enlaces entre equipos de conmutación, con la garantía que los tráficos de cada una de las VLAN llegarán al destino adecuado.

Las distintas VLAN también son de forma simultánea las interfaces lógicas en las que se lleva a cabo el encaminamiento, y es por eso que como parte de la configuración de las VLAN se incluye la dirección IP y la máscara correspondiente.

### Vlan Virtual Interfaces:

Gestión de hasta 8 VLANs.

Para cada VLAN, esta zona contiene los parámetros siguientes:

- **#.** Indicador de posición en la tabla.
- **VID.** Permite establecer el identificador de la VLAN a la que estará vinculada la interfaz lógica. El rango admitido comprende del **1** al **4094**.

- **IP y MASK.** Valores para la dirección IP y la máscara de la interfaz cuando opera en modo estático.
- **Description.** Campo de texto auxiliar, como mnemotécnico para el usuario. No condiciona la operación del equipo en modo alguno.
- **eth0.** Este parámetro permite habilitar y deshabilitar el puerto Ethernet marcando o desmarcando, respectivamente, la casilla.
- **ofdm.** Este parámetro permite habilitar y deshabilitar el puerto PLC marcando o desmarcando, respectivamente, la casilla.

Cuando las casillas **eth0** y **ofdm** están ambas habilitadas, el equipo se comporta como un **Bridge**. De no ser así, el equipo se comporta como un **Router**.

#### Ethernet eth0 properties:

Esta zona contiene los parámetros siguientes:

- **VLAN function.** Especifica el comportamiento del puerto Ethernet en relación al procesamiento del tag 802.1q, siendo las opciones *tagged* y *untagged*.  
**Tagged:** Las tramas 802.1 se transmitirán **con tag**, independientemente de que en el momento de ser recibidas por el equipo tuvieran tag o no.  
**Untagged:** Las tramas 802.1 se transmitirán **sin tag**, independientemente de que en el momento de ser recibidas por el equipo tuvieran tag o no.
- **VID (VLAN id por defecto).** Identificador numérico de la VLAN en la que está incluido el puerto. También constituye el identificador de VLAN que se asignará a las tramas recibidas en el puerto y que no incluyan tag (*untagged*).

#### ofdm properties:

Esta zona contiene los parámetros siguientes:

- **VLAN function.** Especifica el comportamiento del puerto PLC en relación al procesamiento del tag 802.1q, siendo las opciones *tagged* y *untagged*.  
**Tagged:** Las tramas 802.1 se transmitirán **con tag**, independientemente de que en el momento de ser recibidas por el equipo tuvieran tag o no.  
**Untagged:** Las tramas 802.1 se transmitirán **sin tag**, independientemente de que en el momento de ser recibidas por el equipo tuvieran tag o no.

- **VID (VLAN id por defecto).** Identificador numérico de la VLAN en la que está incluido el puerto. También constituye el identificador de VLAN que se asignará a las tramas recibidas en el puerto y que no incluyan tag (*untagged*).

## 4.4 CONFIGURACIÓN ROUTING

El menú **Routing** presenta dos submenús: **Static Routes** y **DNS servers**.

### 4.4.1 Configuración Static routes

En este submenú se configuran dos tipos de datos, rutas estáticas explícitas, en el apartado **Static Routes**, y la dirección que actúa como ruta por defecto, en el apartado **Default Static Routes**, en el caso en que el servicio no disponga de datos concretos para alcanzar un destino.

FIGURA 16 Pantalla de configuración del submenú **Static Routes** del menú **Routing**

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

2 Add

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

2 Add

Send Reload

#### Static Routes:

Los parámetros de configuración de una ruta estática son:

- **Destination.** Permite especificar la dirección IP y máscara de subred de la red remota o destino. El campo requiere que los valores se introduzcan en el formato del direccionamiento IP. Ejemplo: 192.168.0.0/255.255.255.0 ó 192.168.0.0/24.
- **Gateway.** Permite especificar la dirección IP del router al que se debe enviar el tráfico cuyo destino sea la red remota del campo anterior.

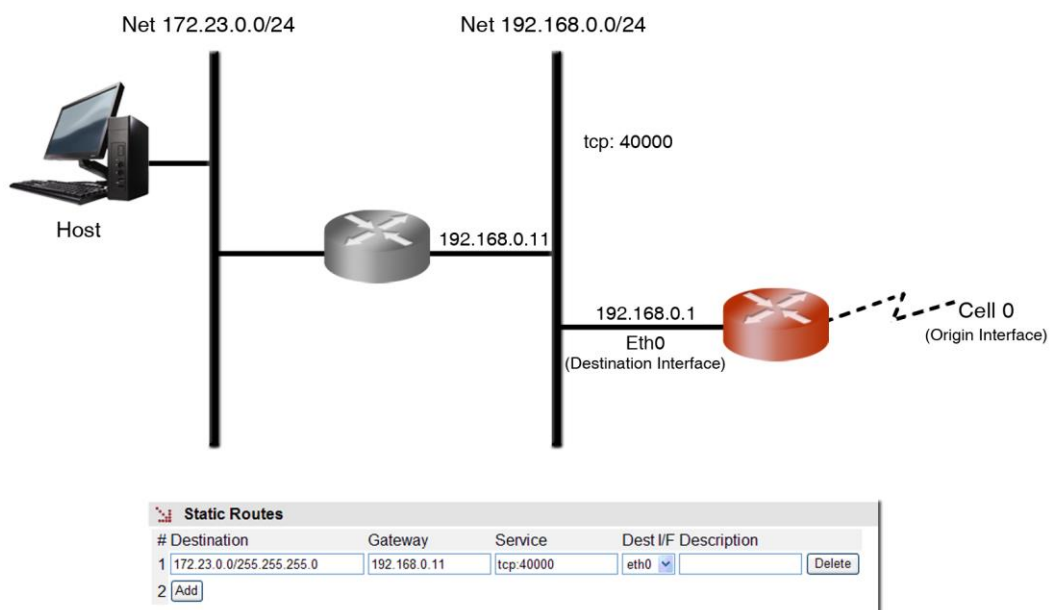
# ZBP-1

- **Service.** Permite establecer un filtro adicional a la dirección IP remota para determinar la elección del siguiente salto. La condición se establece en base a un servicio específico (tcp/udp/icmp). A continuación del servicio debe indicarse el número de puerto (1÷65535), separado con dos puntos. El valor por defecto es **any**, es decir, la ruta aplica para todo tipo de tráfico (únicamente se toma en consideración el destino IP). Ejemplo: tcp:5000, quiere decir que todos los paquetes con tráfico tcp sobre el puerto 5000 se enviarán al router indicado.
- **Dest I/F (Destination interface).** Permite especificar la interfaz a través de la cual se enviará el tráfico encaminado que coincida con esta ruta. Las interfaces se identifican por el dispositivo asociado, bien sea real, o virtual, los distintos dispositivos asociados a cada una de las VLAN definidas, p.e. vlan1.
- **Description.** Permite especificar una descripción de hasta 15 caracteres alfanuméricos.

## Ejemplo de configuración de ruta estática:

La figura muestra un ejemplo de asignación de ruta estática entre dos segmentos de red distintos. Todos los paquetes TCP del puerto 40000 podrán alcanzar el segmento de red 172.23.0.0/24 a través del router 192.168.0.11.

FIGURA 17 Ejemplo de configuración de ruta estática



## Default Static Routes:

Los parámetros de configuración de una ruta estática por defecto son:

- **Gateway.** Permite especificar la dirección IP del siguiente router para el enrutamiento del tráfico cuyo destino no coincida con ninguna ruta conocida.
- **Dest I/F (Destination interface).** Permite especificar la interfaz a través de la cual se enviará el tráfico encaminado hacia el router indicado en el campo anterior. Las interfaces se identifican por el dispositivo asociado, bien sea real, o virtual, los distintos dispositivos asociados a cada una de las VLAN definidas, p.e. vlan1.
- **Metric.** Permite fijar un valor de precedencia entre las distintas rutas por defecto que puedan crearse. Una métrica mayor significa menor prioridad.
- **Description.** Permite especificar una descripción de hasta 15 caracteres alfanuméricos.

### 4.4.2 Configuración DNS servers

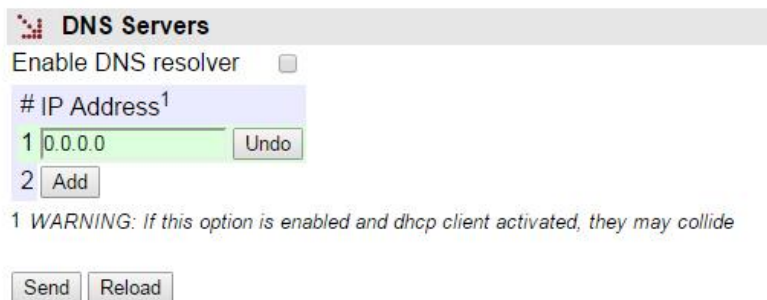
Este submenú da acceso a la pantalla de configuración que permite al usuario configurar las direcciones del servidor o servidores DNS manualmente.

Los parámetros de la pantalla son los siguientes:

- **Enable DNS resolver.** Permite activar el servicio DNS. Debe marcarse si se quieren utilizar los servidores DNS configurados manualmente.
- **IP Address.** Permite especificar las direcciones IP de servidores DNS. Estas direcciones serán efectivas siempre y cuando la casilla *Enable DNS resolver* esté seleccionada.

! Para la correcta operación de este servicio, no debe estar habilitado el cliente DHCP.

FIGURA 18 Pantalla de configuración del submenú **DNS servers** del menú **Routing**



## 4.5 CONFIGURACIÓN SNMP

El equipo dispone de un agente SNMP con capacidad para generar mensajes espontáneos hacia equipos de gestión basados en dicho protocolo.

El agente admite la emisión de mensajes según el protocolo SNMPv1, SNMPv2c y SNMPv3, así como la elección del tipo de mensajes, *trap* e *inform*.

Cualquier cambio efectuado en la configuración del agente SNMP **únicamente** será activo después de realizar un **RESET** al equipo. El comando **Apply** no es suficiente, por lo que el cambio debe necesariamente almacenarse con el comando **Save** antes de solicitar la reinicialización.

Los parámetros de configuración son:

- **Enable.** Habilita/inhabilita la ejecución del agente SNMP. El agente está operativo cuando la opción está seleccionada.
- **Community.** Parámetro asociado a SNMPv1/v2c. Dato tabular que permite definir varios perfiles de operación, incluidos los derechos de acceso (*Access*) asociados a cada uno, derechos de únicamente lectura (*ro*) o lectura/escritura (*rw*). Los perfiles se denominan *communities*.



FIGURA 19 Pantalla de configuración del menú **SNMP**

### SNMP

Enable

SNMP v1/v2c

#	Community	Access
1	<input type="text" value="public"/>	<input type="text" value="ro"/>
2	<input type="button" value="Add"/>	

SNMP v3

#	User	Access	Security	Auth Alg.	Auth Password	Priv Alg.	Priv Password
1	<input type="text" value="public"/>	<input type="text" value="ro"/>	<input type="text" value="clear"/>	<input type="text" value="MD5"/>	<input type="text" value="Change"/>	<input type="text" value="DES"/>	<input type="text" value="Change"/>
2	<input type="button" value="Add"/>						

### SNMP Traps

Enable Traps

Traps SNMP v1/v2c

#	Community	Type	IP	Port	
1	<input type="text" value="public"/>	<input type="text" value="v2c"/>	<input type="text" value="158.126.40.30"/>	<input type="text" value="162"/>	<input type="button" value="Delete"/>
2	<input type="button" value="Add"/>				

Trap v1 agent address

Traps SNMP v3

#	User	Type	Security	Auth Alg.	Auth Password	Priv Alg.	Priv Password	IP	Port
1	<input type="button" value="Add"/>								

- User.** Parámetro asociado a SNMPv3. Dato tabular que permite definir tanto a los usuarios en sí mismos como los privilegios y el modo de operación de cada usuario, es decir, los derechos de acceso (*Access*), derechos de únicamente lectura (*ro*) o lectura/escritura (*rw*), y el modo en que se llevará a cabo la transferencia de datos (*Security*), no cifrada (*clear*), autenticada (*auth*) o autenticada y cifrada (*priv*).

En caso de transmisión autenticada (*auth*), es necesario seleccionar el tipo de algoritmo (*Auth Alg.*), MD5 o SHA, y establecer la contraseña de autenticación (*Auth Password*). La contraseña establece la palabra que se empleará para la generación de la información de autenticación. La palabra de autenticación debe ser conocida por el destinatario para poder verificar la autenticidad de la identidad del equipo emisor.

En caso de transmisión cifrada (*priv*), además de seleccionar el tipo de algoritmo de autenticación (*Auth Alg.*) y la contraseña de autenticación (*Auth Password*), es necesario seleccionar el tipo de algoritmo de cifrado (*Priv Alg.*), DES o AES, y establecer la contraseña de cifrado (*Priv Password*).

El password no se muestra por razones de seguridad, por lo que cuando se modifica (opción **Change**) debe ser introducido por duplicado.

Una vez introducido el **Password** desde la opción **Change**, ejecutar el comando **send** de dicha opción y, a continuación, si dicho valor se desea aplicar y salvar en el equipo, **NO olvidar** ejecutar los comandos **apply** y **save** del árbol de menús principal.

## SNMP Traps:

- **Enable Traps.** Habilita/inhabilita la generación y transmisión de mensajes espontáneos por parte del agente SNMP. El agente enviará los traps seleccionados por el usuario cuando los distintos eventos se produzcan.

- **Traps SNMPv1/v2c.** Dato tabular que permite definir varios equipos destinatarios de los *traps*.

Para cada uno de los destinatarios de los mensajes espontáneos SNMP, es necesario proporcionar el perfil que se incluirá en el mensaje espontáneo, la versión del protocolo SNMP con el que se codificará, la dirección IP del destinatario y el puerto UDP al que se enviarán los mensajes. El valor por defecto establecido en el estándar es el puerto 162. Admite su modificación para adaptarse a los datos de operación de cada destinatario.

La transmisión de los mensajes de forma confirmada (*inform*) sólo es admitida por las versiones v2c y v3 del protocolo.

- **Trap v1 agent address.** Establece cuál será la dirección IP que el agente comunicará como propia cuando se envíe mensajes espontáneos. Este parámetro únicamente se emplea en la creación de los traps cuando se emplea SNMPv1.

- **Traps SNMPv3.** Dato tabular que permite definir varios equipos destinatarios de las notificaciones.

Los destinatarios se identifican mediante su dirección IP y el puerto UDP al que se enviarán las notificaciones. El puerto UDP estándar para las notificaciones SNMP es el 162, que es el valor por defecto.

El control *Type* establece si la transmisión de las notificaciones se realizará de forma no confirmada (*trap*) o confirmada (*inform*).

## 4.6 CONFIGURACIÓN ACCESS

El equipo ofrece varios medios de acceso al usuario.

Los usuarios locales predefinidos en el sistema están siempre presentes, pero se puede emplear un recurso externo para la validación de los usuarios para los distintos tipos de acceso, de modo que la base de datos de usuarios sea un recurso centralizado e independiente de los propios equipos. A este fin, el equipo dispone de un cliente TACACS+.

**TACACS+** (acrónimo de **Terminal Access Controller Access Control System**) es un protocolo de autenticación remota que se usa para gestionar el acceso a servidores y dispositivos de comunicaciones, y proporciona servicios separados de autenticación, autorización y registro.

FIGURA 20 Pantalla de configuración del menú **Access**

The screenshot displays the configuration interface for the 'Access' menu, organized into five sections:

- TACACS+**:
  - 1 Server IP: 0.0.0.0
  - 2 Server IP: 0.0.0.0
  - Encrypted:
  - Secret shared Key: [Change](#)
  - Guest Privilege Level: 1
  - Admin Privilege Level: 2
- Console Access**:
  - Authentication method<sup>1</sup>: local
  - 1 Fallback to local access always enabled
- Web Access**:
  - Authentication method: local
  - Fallback to local access:
- Telnet Access**:
  - Authentication method: local
  - Fallback to local access:
- SSH Access**:
  - Authentication method: local
  - Fallback to local access:

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

Los parámetros generales de configuración son los siguientes:

- **Server IP 1.** Establece la dirección IP del servidor TACACS+ primario.
- **Server IP 2.** Establece la dirección IP del servidor TACACS+ secundario.
- **Encrypted.** Permite seleccionar si la comunicación del equipo con los servidores TACACS+ debe realizarse en modo cifrado o no.
- **Secret Shared Key.** Establece la clave a emplear para el cifrado de la comunicación cuando la opción **encrypted** está activa.
- **Guest Privilege Level.** Establece el nivel de privilegio (0 a 15) del perfil invitado (**guest**). Este nivel debe de coincidir con el establecido en el servidor TACACS+.
- **Admin Privilege Level.** Establece el nivel de privilegio (0 a 15) del perfil administrador (**admin**). Este nivel debe de coincidir con el establecido en el servidor TACACS+.

A continuación, se hallan los parámetros asociados a cada opción de acceso, y que son los siguientes:

- **Authentication method.** Establece si la validación de los usuarios debe realizarse de forma local o por consulta a los servidores tacacsplus configurados.
- **Fallback to local access.** Cuando esta opción está habilitada, en caso de no accesibilidad de los servidores TACACS+ configurados, se permitirá a los usuarios validarse con lo usuario locales. En caso de que la opción esté inhabilitada, si los servidores TACACS+ no son accesibles, el acceso por parte de los usuarios no estará disponible. El acceso vía consola siempre tiene esta opción habilitada, por lo que no se presenta como susceptible de ser configurada.

## 4.7 REINICIO (REBOOT)

El equipo puede ser reiniciado mediante la ejecución del comando **Reboot**.

El comando está disponible únicamente para el perfil administrador.

### ACTUALIZACIÓN DEL CÓDIGO (REFLASH)

El equipo admite la actualización del software de aplicación mediante la ejecución del comando **Reflash**, disponible únicamente para el perfil administrador.

El proceso de actualización de código no altera los datos de configuración, a no ser que se indique de forma expresa. No obstante, una vez ha finalizado, supone la pérdida momentánea de servicio, por el reinicio automático del equipo.

Es necesario disponer de la imagen binaria adecuada para el equipo, que será seleccionada mediante el botón *Examinar*.

Una vez seleccionada la imagen, la ejecución de la actualización se realiza con el botón **Reflash**. El proceso suele durar unos 5 minutos, durante los cuales, se muestra el resultado de los distintos pasos en la ventana del navegador HTML, aunque en función del mismo, es posible que únicamente muestre el resultado al final del proceso.

La opción **Only verify** permite comprobar que el código almacenado coincide con la imagen binaria seleccionada, sin afectar a la imagen instalada.

FIGURA 21

Pantalla asociada a la opción *Reflash*

**Reflash**

Reflash image  Ningún archivo seleccionado

Only verify

**Reflash status**

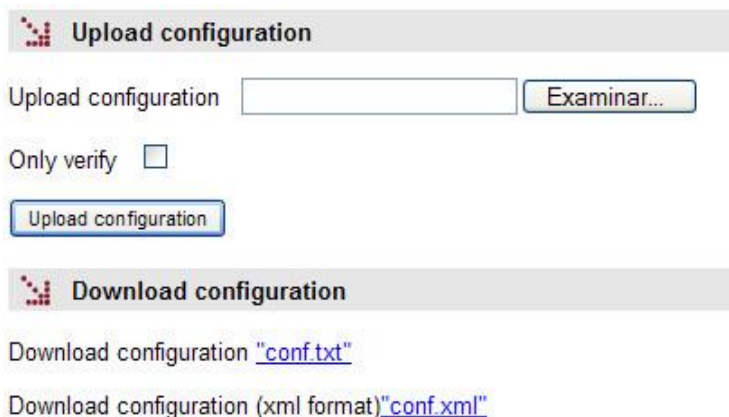
Last reflash process result

- 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 FICHERO DE CONFIGURACIÓN

El equipo permite tanto la obtención (**Download**) como el volcado (**Upload**) de la configuración del mismo mediante un fichero de texto o un fichero XML.

FIGURA 22 Opciones para el volcado (Upload) y obtención (Download) del fichero de configuración



The screenshot shows a web interface for configuration management. It is divided into two main sections: 'Upload configuration' and 'Download configuration'.  
The 'Upload configuration' section features a text input field labeled 'Upload configuration' and a button labeled 'Examinar...'. Below this is a checkbox labeled 'Only verify' which is currently unchecked. At the bottom of this section is a button labeled 'Upload configuration'.  
The 'Download configuration' section provides two links: 'Download configuration "[conf.txt](#)"' and 'Download configuration (xml format)"[conf.xml](#)"'.

### 4.9.1 Upload (del ordenador al equipo)

El usuario debe seleccionar el fichero que contiene la configuración que se desea volcar en el equipo, mediante el botón Examinar.

Para poder examinar la configuración sin volcarla en el equipo, debe marcarse la casilla **Only verify**, la cual permite realizar únicamente una verificación.

El sistema, una vez el equipo ha recibido el fichero de texto, comprueba el contenido del mismo, verificando tanto que las variables incluidas sean válidas, como que los valores asignados a las mismas cumplan con los requerimientos sintácticos existentes. De detectarse errores en el fichero, tanto si la opción de únicamente verificación está seleccionada como si no lo está, el sistema descarta automáticamente toda la información recibida y se lo indica al usuario.

Si la configuración recibida es válida, el sistema lo comunica al usuario y le ofrece la opción de proseguir, botón *Continue*, lo que supondrá el almacenamiento de la configuración enviada en el equipo y su activación.

El sistema avisa de que en el momento de aplicar la nueva configuración se perderá momentáneamente el acceso al equipo.

De haber seleccionado la opción de únicamente realizar la verificación (***Only verify***), de ser satisfactoria, el sistema lo comunica al usuario y éste, si lo desea, puede aplicar la configuración en el equipo utilizando los comandos *Apply*, *Save* o ambos.

#### 4.9.2 Download (del equipo al ordenador)

Mediante esta opción, el usuario obtiene una copia local de la configuración del equipo en un fichero tipo texto (con extensión **.txt**) o tipo XML (con extensión **.xml**).

El procedimiento para la obtención del fichero dependerá del navegador HTTP empleado por el usuario, así como de las acciones que deban realizarse con el fichero recibido (por ejemplo, ubicación de dónde almacenarlo, etc).

## 5 ESTADÍSTICAS

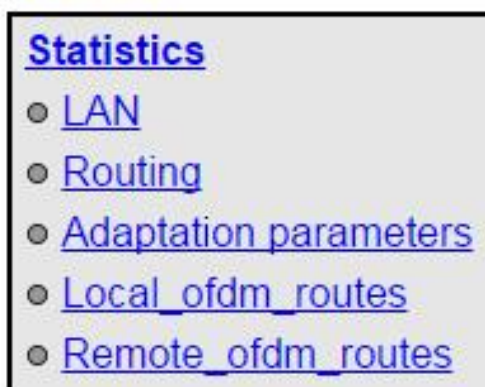
Las estadísticas proporcionan información derivada del propio uso del equipo como, por ejemplo, los datos relativos a la configuración LAN, los datos relativos al encaminamiento, los datos de las rutas encontradas en el canal PLC, etc.

El sistema proporciona estadísticas estructuradas en bloques, cada uno de ellos perteneciente a una funcionalidad concreta.

El primer bloque muestra datos generales relativos al equipo, y se muestra de forma automática cuando se selecciona el objeto estadísticas (*Statistics*).

Al resto de estadísticas se accede seleccionando la etiqueta correspondiente bajo el epígrafe *Statistics*, véase FIGURA 23.

FIGURA 23 Opciones del menú **Statistics** de la Gestión Web



Cada una de las tablas de datos estadísticos se puede actualizar mediante el botón *Reload* sin tener que volver a seleccionar la opción correspondiente en el árbol de menús.

Las estadísticas pueden ser **INICIALIZADAS** por el usuario a voluntad mediante la opción de menú **Clear Statistics**.



## 5.1 DATOS GENERALES

Los datos generales relativos al equipo se muestran de forma automática cuando se selecciona el objeto estadísticas (*Statistics*).

FIGURA 24 Ejemplo de estadística relativa a Datos Generales (*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

Para actualizar la fecha y hora del equipo, seleccionar la opción [Change](#) correspondiente a *Time (UTC)* o *Time (Local)*.

En la página asociada, véase FIGURA 25, introducir los datos de fecha y hora (YYYY/MM/DD, hh:mm:ss) y, a continuación, ejecutar los comandos **Send**, **Save** y **Apply**.

FIGURA 25 Ejemplo de actualización de fecha y hora

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 ESTADÍSTICA RELATIVA A LAN

Los datos relativos a la configuración LAN del equipo se muestran cuando se selecciona *LAN* bajo el epígrafe *Statistics*.

FIGURA 26 Ejemplo de estadística relativa a *LAN*

General Data						
#	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

OFDM devices						
#	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 ESTADÍSTICA RELATIVA A ROUTING

Los datos relativos al encaminamiento se muestran cuando se selecciona *Routing* bajo el epígrafe *Statistics*.

FIGURA 27 Ejemplo de estadística relativa a *Routing*

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

Reload

## 5.4 ESTADÍSTICA RELATIVA A ADAPTATION PARAMETERS

Los parámetros de conexión que utiliza el equipo local para comunicarse con sus vecinos se muestran cuando se selecciona *Adaptation parameters* bajo el epígrafe *Statistics*.

En primer lugar, se muestra la identificación del equipo local (ID = 4 en la FIGURA 28 de ejemplo).

A continuación, se muestran los parámetros de conexión en emisión (velocidad y potencia) que el equipo local debe utilizar para poder comunicarse con los equipos vecinos que ha identificado (equipo con ID = 5 en la FIGURA 28 de ejemplo).

El equipo local asigna a cada equipo vecino una velocidad (Data rate) en bit/s y una potencia (Power). La velocidad está relacionada con el tipo de modulación y el modo de trabajo de cada una de las portadoras.

Finalmente, se muestran los valores de los parámetros de conexión en recepción (velocidad en bit/s).

FIGURA 28 Ejemplo de estadística relativa a *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 ESTADÍSTICA RELATIVA A LOCAL OFDM ROUTES

La tabla de direcciones MAC/IP locales del equipo se muestra cuando se selecciona *Local ofdm routes* bajo el epígrafe *Statistics*.

En primer lugar, se muestra la identificación del equipo local (ID = 4 en la FIGURA 29 de ejemplo).

A continuación, se muestra la tabla de rutas locales en donde, para cada ruta, se indica la dirección MAC, la dirección IP, la VLAN incluida en la ruta, y el tiempo de vida (*Life time*) de la ruta.

FIGURA 29 Ejemplo de estadística relativa a *local ofdm routes*

**Local equipment**  
LOCAL\_ID 4

**LOCAL OFDM ROUTES**

#	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

Reload

## 5.6 ESTADÍSTICA RELATIVA A REMOTE OFDM ROUTES

Los datos de las rutas encontradas en el canal PLC se muestran cuando se selecciona *Remote ofdm routes* bajo el epígrafe *Statistics*.

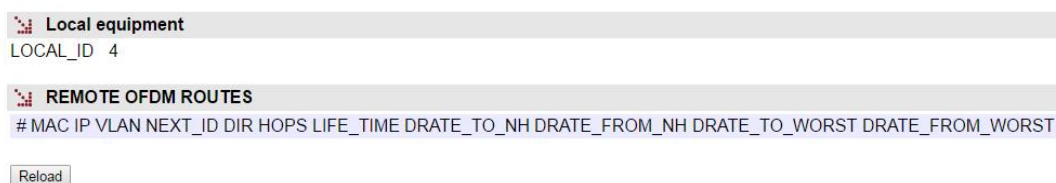
En primer lugar, se muestra la identificación del equipo local (ID = 4 en la FIGURA 30 de ejemplo).

A continuación, si hubiera, se muestran los datos asociados a las distintas rutas.

En cada una de las rutas se detalla:

- la **dirección MAC**, su correspondiente **dirección IP**, y la **VLAN** incluida en la ruta,
- el número de identificación del equipo siguiente en la ruta (**NEXT ID**),
- la dirección (**DIR**) del enlace, siendo B (bidireccional) o M (monodireccional) cuando no existe una ruta de vuelta,
- el número de enlaces (**HOPS**) que tiene la ruta,
- el tiempo de vida (**LIFE TIME**) de la ruta, el cual se va actualizando mientras se reciba información a través de la ruta,
- cuatro velocidades (**DRATE**) de la ruta en bit/s. Velocidad de emisión y de recepción del siguiente enlace, y la peor velocidad en emisión y en recepción de todos los enlaces de la ruta

FIGURA 30 Ejemplo de estadística relativa a *remote ofdm routes*



## APÉNDICE A

### ESTRUCTURA DE DATOS EN CLI

## APÉNDICE A

### ESTRUCTURA DE DATOS EN CLI

Este apéndice contiene toda la información necesaria para la utilización de la consola de usuario CLI. En él se explican los métodos de acceso, los comandos disponibles desde la consola y, finalmente, se muestra, paso a paso, el ejemplo de cómo obtener información del estado y la configuración de un equipo.

#### Convenciones:

Los parámetros de configuración de los equipos están organizados a modo de árbol de directorios, en los que se agrupan parámetros y subdirectorios relacionados, donde:

- Un nombre seguido de “/” corresponde al nombre de un directorio. *Ej. Main/*
- Un nombre seguido de “[ ]” corresponde a un parámetro con estructura matricial ya que contiene varios atributos. *Ej. nat[ ]/*
- Un nombre sin nada detrás es un parámetro en sí. *Ej. Action*

El sistema distingue los caracteres en minúscula de los caracteres en mayúscula.

La navegación en los directorios se lleva a cabo con el comando **cd** (*change directory*).

Los datos almacenados en forma tabular, identificados por incluir en el nombre de la variable el símbolo [], disponen de comandos específicos para añadir y eliminar filas, y que son respectivamente **add** y **remove**. Para consultar o establecer el valor de los datos de una de las filas, es necesario incluir en el comando **get** o **set** el identificador de la fila, entre corchetes.

Los cambios realizados con el comando **set** no son operativos por el simple hecho de haber sido ejecutados. El uso efectivo e inmediato de los cambios realizados se consigue mediante la ejecución del comando **Apply**. Por el contrario, el comando **Save** supone el almacenamiento de los cambios realizados con carácter permanente, y no conlleva su uso inmediato, sino que serán aplicados en el caso de producirse una inicialización.

De este modo, como procedimiento operativo, los cambios se ponen en operación con el comando **Apply**, y una vez verificado que el comportamiento es el deseado, se procede a salvar el mismo con el comando **Save**. Así, en el caso de obtener resultados indeseados, siempre es posible obviar el comando **Save** y proceder a la inicialización del equipo para recuperar el estado previo, incluso en el supuesto que los cambios activados conllevasen la pérdida de acceso al usuario.

Los nombres de usuario y contraseñas son, por defecto, los mismos que en la interfaz web, es decir:

	Nombre de usuario ( <i>login</i> )	Contraseña ( <i>password</i> )
Usuario Invitado	guest	passwd01
Usuario Administrador	admin	passwd02

## A.1 MÉTODOS DE ACCESO

Existen dos métodos para acceder al equipo a través de la consola de usuario CLI:

- en modo local, a través del conector DB9.
- en modo local o remoto mediante Telnet/SSH, a través del puerto Ethernet.

### Acceso a través del conector DB9

El acceso en modo local se realiza conectando con un cable serie plano el puerto serie del ordenador (o, en su defecto, un conversor de serie a USB) al puerto DB9 del equipo (puerto de servicio).



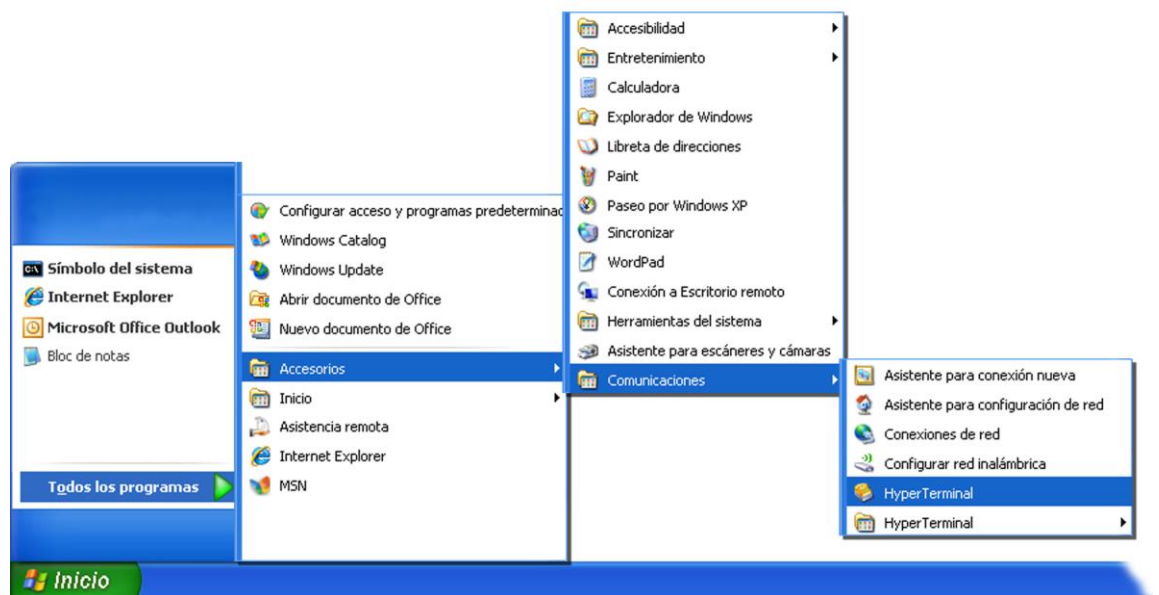
# ZBP-1

Para la comunicación del ordenador con el equipo deberá utilizarse un programa de emulación de terminal como, por ejemplo, *HyperTerminal* de Windows®, configurando una conexión serie con las siguientes características:

- Velocidad: 115.200 bps
- Bits de datos: 8
- Paridad: No
- Bits de stop: 1
- Control de flujo: No

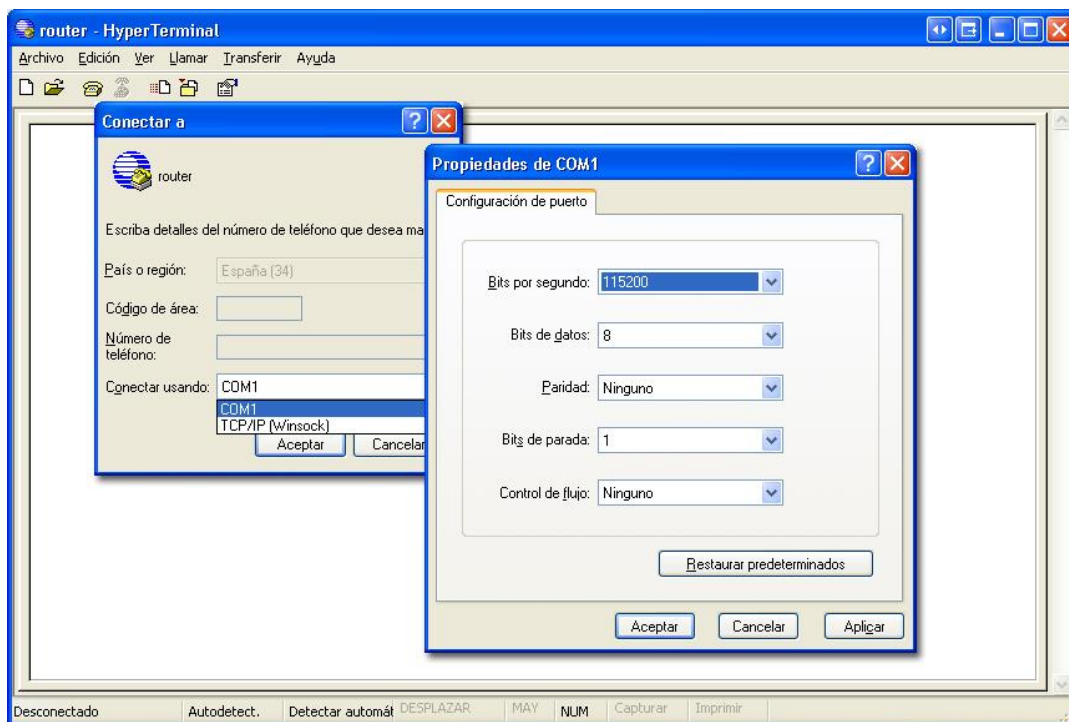
En Windows XP® se puede ejecutar *HyperTerminal* desde *Inicio* → *Todos los Programas* → *Accesorios* → *Comunicaciones* → *HyperTerminal* (véase FIGURA 31).

FIGURA 31 Localización de *HyperTerminal* en Windows XP®



Al abrir *HyperTerminal* una ventana de diálogo solicitará la información necesaria para el establecimiento de la conexión (véase FIGURA 32).

FIGURA 32 Configuración de la conexión por puerto serie con *HyperTerminal*



A continuación, deberá ejecutarse la opción *Llamar* del menú *Llamar* (o pulsar, bajo las opciones del menú principal, el icono del teléfono colgado).

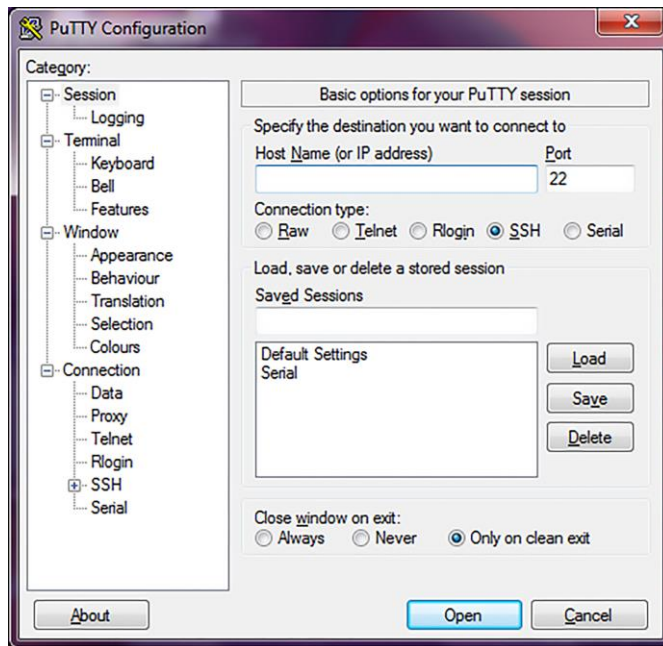
Tras las trazas de arranque, pulsar la tecla return. Cuando en el prompt se muestre el texto **zbp login**, introducir el nombre de usuario y pulsar return. Cuando en el prompt se muestre el texto **zbp password**, introducir la contraseña y pulsar return (el nombre de usuario y contraseña son los mismos que en la interfaz web).

Hay que tener en cuenta que en la ventana de *HyperTerminal* no aparece texto alguno mientras se introduce el password.

Puesto que sistemas operativos como Microsoft Windows 7© ya no incluyen el programa *HyperTerminal*, también se considera el programa *Putty*, gratuito y ejecutable.

El programa *Putty* se encuentra accesible en la web [www.putty.org](http://www.putty.org). Basta seleccionar el *Putty* que se adecúe al sistema operativo en uso (normalmente el primero, llamado **putty.exe**), copiarlo en el ordenador y ejecutarlo.

FIGURA 33 Ventana principal de *PuTTY*



En el menú **Serial** (último de todos) se configura el puerto serie.

! El acceso mediante Telnet se lleva a cabo configurando el puerto 23.  
El acceso mediante SSH se lleva a cabo configurando el puerto 22.

Si se usa un conversor USB, previamente, consultar el número de COM en el *Administrador de dispositivos* (Panel de control).

FIGURA 34 Ventana del administrador de dispositivos

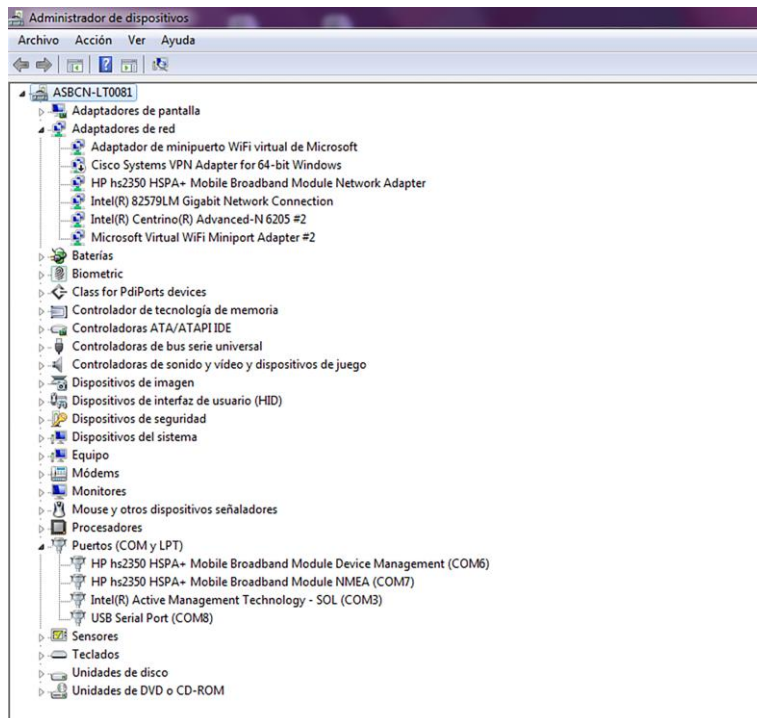
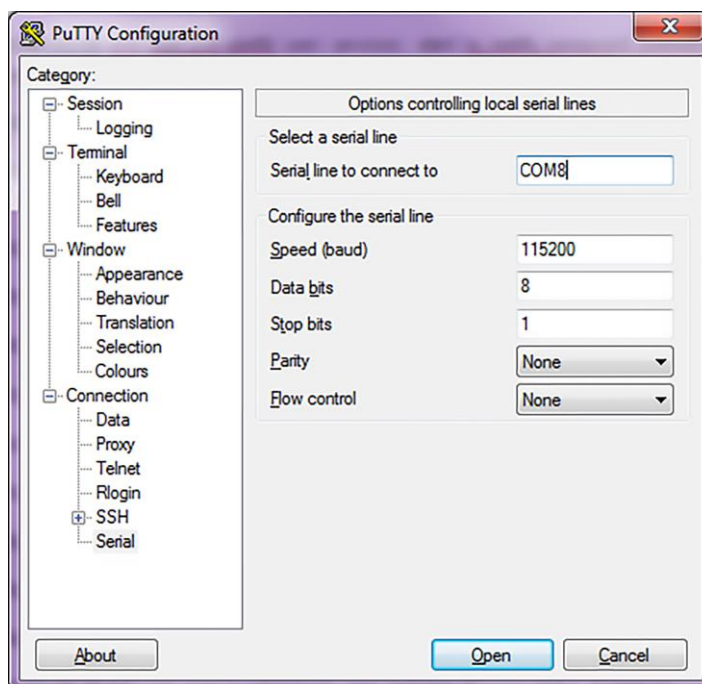


FIGURA 35 Configuración de la conexión por puerto serie con *Putty*



Pulsado el botón *Open*, y si es necesario return, se mostrará una ventana en la que aparecerá el prompt **zbp login:** esperando a que introduzcamos el *login* de usuario y, posteriormente, la contraseña de inicio de sesión (el nombre de usuario y contraseña son los mismos que en la interfaz web).

Hay que tener en cuenta que en la ventana de *Putty* no aparece texto alguno mientras se introduce el password.

### Acceso mediante Telnet

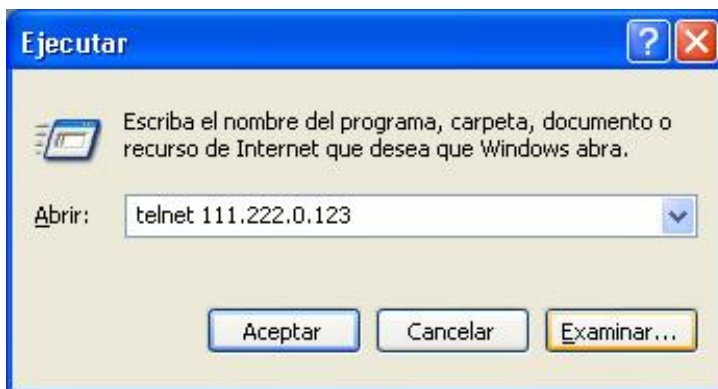
El acceso, en modo local o remoto, se realiza con el comando *Telnet* y la dirección IP del equipo.

! Para emplear este modo de acceso, el equipo debe tener configurada su dirección IP y estar conectado a la red en la que se encuentra el ordenador de gestión.

En Windows XP© se puede ejecutar Telnet desde el botón de inicio: Inicio → Ejecutar y, en la ventana de dialogo que aparece, escribir: telnet + espacio + Dirección\_IP\_del\_equipo (en el ejemplo 111.222.0.123), pulsando, seguidamente, sobre el botón Aceptar (véase FIGURA 36).

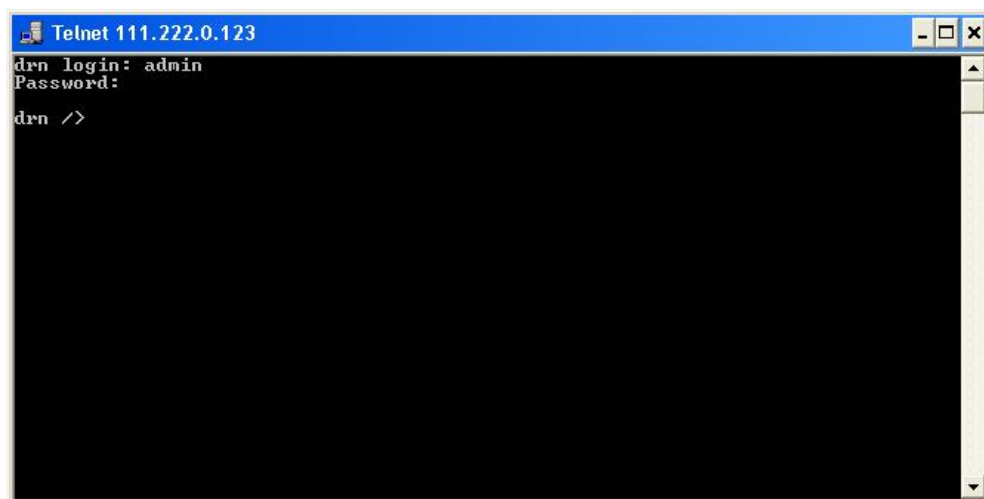
# ZBP-1

FIGURA 36 Ventana de diálogo *Ejecutar... Telnet* para establecer la conexión con el equipo



Al pulsar el botón *Aceptar* se abre una ventana de símbolo del sistema (véase FIGURA 37 de ejemplo con un equipo *drn*).

FIGURA 37 Ventana de *Telnet*



Es posible utilizar *HyperTerminal* como interfaz gráfica de *Telnet*. Para ello, al configurar la conexión seleccionaremos **TCP/IP (Winsock)** del desplegable *Conectar usando*.

También es posible ejecutar *Telnet* desde el programa *Putty*. Basta con escribir la dirección IP del equipo en la ventana principal, y pulsar *Open*.

Sea cual sea el método elegido para establecer la conexión con el equipo, aparecerá el prompt **zbp login:** esperando a que introduzcamos el *login* de usuario y, posteriormente, la contraseña de inicio de sesión (el nombre de usuario y contraseña son los mismos que en la interfaz web).

# ZBP-1

En sistemas operativos como Microsoft Windows 7®, el cliente Telnet viene deshabilitado por defecto.

Para habilitarlo, desde el botón de inicio: Inicio → Panel de control → Programas, en *Programas y características*, seleccionar *Activar o desactivar las características de Windows*.

A continuación, en la ventana de *Características de Windows*, seleccionar *Cliente Telnet*, véase FIGURA 38. Pulsando *Aceptar*, ya se podrá utilizar el cliente Telnet de Windows.

FIGURA 38 Ventana de Características de Windows



## A.2 COMANDOS DE LA CONSOLA DE USUARIO

Una vez iniciada la sesión con un usuario y password válidos, el prompt cambiará a **equipo />** a la espera de que el usuario teclee algún comando.

Los comandos son órdenes que se envían al equipo para requerir o modificar algún valor o para “navegar” a través del árbol en que están organizados los parámetros del equipo.

La tabla siguiente muestra la lista completa de comandos disponible, mostrando una breve descripción del mismo, la disponibilidad en función del tipo de usuario que ha iniciado la sesión y resaltando los de más utilidad:

**TABLA 8**

Listado completo de comandos de la consola de usuario CLI

Comando	Descripción	Usuario	
		admin	guest
add	Añade un nuevo ítem a un parámetro de tipo matricial	✓	✗
apply	Aplica la nueva configuración	✓	✗
cd	Cambia de directorio en el árbol de parámetros	✓	✓
clear	Borra las estadísticas	✓	✗
date	Muestra la fecha almacenada en el equipo	✓	✗
<b>download</b>	Genera un fichero de comandos de configuración	✓	✓
Exit	Interrumpe la conexión con el equipo	✓	✓
<b>get</b>	Muestra los valores de los parámetros	✓	✓
help	Muestra la lista de comandos disponibles	✓	✓
<b>log</b>	Muestra el fichero de log en uso (actual)	✓	✓
ls	Muestra la lista de parámetros disponible en el directorio actual	✓	✓
ping	Realiza un ping al host indicado	✓	✓
quit	Interrumpe la conexión con el equipo		
reboot	Reinicializa el equipo	✓	✗
reload	Carga una configuración guardada con anterioridad	✓	✗
remove	Elimina un ítem de un parámetro de tipo matricial	✓	✗
restore	Carga la configuración por defecto	✓	✗
Save	Guarda todos cambios efectuados durante la sesión	✓	✗
Set	Modifica el valor de un parámetro	✓	✗
<b>stats</b>	Permite obtener los parámetros de estado del equipo	✓	✓
telnet	Abre una sesión telenet sin interrumpir la conexión con el equipo	✓	✓
xmldownload	Genera un fichero de comandos de configuración en formato xml	✓	✓

Según la función que realizan cada uno de estos comandos, los podemos clasificar en diferentes grupos:

TABLA 9

Clasificación de los comandos según su función

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

### Información incluida en el log

Los eventos que se generan a nivel de sistema y se envían al log incluyen un nivel identificativo.

El sistema admite 8 niveles distintos, separados en dos bloques. El primer bloque correspondería a situaciones no deseadas, y el segundo bloque a informaciones sin afectación de la funcionalidad.

En el primer bloque, los valores incluidos son **emerg**, **alert**, **crit**, **err** y **warning**, lo que representa un nivel de severidad decreciente en cuanto a la situación detectada.

En el bloque de información, los valores son **notice**, **info** y **debug**, sin que ello tenga connotación alguna en cuanto a impacto.



## Comandos de configuración

**add** Añade un nuevo ítem a la matriz en un parámetro del tipo matricial.

**Sintaxis:** zbp /> **add** *nombre*

**Argumentos:**

*nombre* Parámetro del cual queremos añadir un nuevo ítem.

**Observaciones:** Para añadir un nuevo ítem a un parámetro del tipo matricial es necesario colocarse en el directorio en el que éste se encuentra o escribir la ruta relativa.

El nuevo ítem creado tiene el número de orden siguiente al último existente. Por ejemplo, si ya existían *nat[1]* y *nat[2]*, al ejecutar el comando **add nat** se crea el ítem ***nat[3]***.

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

**apply** Aplica, en el equipo, los cambios de configuración pero sin guardarlos.

**Sintaxis:** zbp /> **apply**

**Argumentos:** -

**Observaciones:** El uso de este comando es independiente del directorio en que nos encontremos.

Este comando NO guarda los cambios realizados.

**Ejemplo:** zbp /> **apply**

**download** Muestra los comandos necesarios para configurar un equipo con los mismos parámetros que el actual.

**Sintaxis:** zbp /> **download**

**Argumentos:** -

**Observaciones:** El uso de este comando es independiente del directorio en que nos encontremos.

La lista de comandos mostrada comienza con el comando *restore*, que aplica la configuración de fábrica, seguida de los comandos necesarios para conseguir la configuración actual.

Es útil copiar y guardar esta lista de comandos en un fichero .txt para poder ser aplicada en otro equipo de las mismas características.

Para aplicar en otro equipo la configuración guardada, éste debe ser de igual modelo y versión y, sobre todo, tener la misma versión de firmware instalada, ya que la configuración de fábrica, a partir de la cual se genera la lista de comandos, puede diferir de uno a otro.

**Ejemplo:** zbp /> **download**

**get** Muestra los valores actuales de uno o varios de los parámetros de configuración del equipo.

**Sintaxis:** zbp /> **get** [nombre]

**Argumentos:** -  
*nombre* (opcional) nombre del parámetro a mostrar.

**Observaciones:** El comando *get* sin ningún argumento muestra los valores de todos los parámetros de configuración del directorio actual y sus subdirectorios. Si el argumento es el nombre de un directorio muestra los valores de los parámetros que están bajo ese directorio. Si el argumento es el nombre de un parámetro de configuración muestra el valor de dicho parámetro.

Para mostrar la configuración completa del equipo debe ejecutarse este comando, sin argumentos, desde el directorio raíz.

Cuando se utiliza algún argumento éste debe encontrarse en el directorio actual o escribir la ruta relativa.

**Ejemplos:**

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

**remove** Elimina un ítem de la matriz de un parámetro del tipo matricial.

**Sintaxis:** zbp /> **remove nombre[nº]**

**Argumentos:**

*nombre* Parámetro del cual queremos eliminar un ítem.  
*nº* (Opcional) Número de orden del ítem del parámetro

**Observaciones:** Para eliminar un ítem de la matriz de un parámetro del tipo matricial es necesario colocarse en el directorio correspondiente o bien escribir la ruta relativa.

Si se indica el número de orden del ítem a eliminar se elimina dicho ítem. En caso de no indicar el número se elimina el último.

Cuando se elimina un ítem distinto del último, el resto de ítems restante se renumera automáticamente.

**Ejemplos:**

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

- restore**      Aplica la configuración de fábrica.
- Sintaxis:**            zbp /> **restore**
- Argumentos:**        -
- Observaciones:**    El uso de este comando es independiente del directorio en que nos encontremos.
- Ejemplo:**            zbp /> **restore**
- 
- save**            Almacena en la memoria permanente del equipo los cambios efectuados en la configuración de éste. Sin embargo, estos cambios no tendrán efecto hasta que no se reinicie el equipo.
- Sintaxis:**            zbp /> **save**
- Argumentos:**        -
- Observaciones:**    El uso de este comando es independiente del directorio en que nos encontremos.
- Ejemplo:**            zbp /> **save**
- 
- set**             Modifica el valor almacenado en los parámetros de configuración o en los atributos de un ítem de un parámetro matricial.
- Sintaxis:**            zbp /> **set** [nombre][[nº]/[nombre2]]
- Argumentos:**        -
- nombre*            nombre del parámetro a modificar.
- nº*              número de ítem de un parámetro de tipo matricial
- nombre2*        nombre de atributo de un parámetro de tipo matricial

**Observaciones:** Al ejecutar este comando el sistema espera hasta la entrada del nuevo valor.

El parámetro a modificar debe encontrarse en el directorio actual o bien escribirse la ruta relativa del mismo.

Si se desea modificar el valor de uno de los atributos de un ítem de un parámetro matricial, el argumento debe incluir el nombre del parámetro, el número de ítem y el nombre del atributo.

Debe prestarse especial atención al escribir los argumentos de este comando ya que, en caso de no indicar argumento alguno el sistema preguntará, uno por uno, el nuevo valor para cada uno de los parámetros del directorio activo y sus subdirectorios. Así, si se ejecuta el comando `set`, sin argumentos, desde el directorio raíz, el sistema pedirá un nuevo valor para todos y cada uno de los parámetros de configuración del equipo.

Si aplicamos el comando `set` a un parámetro de tipo matricial sin indicar el atributo a modificar, el sistema pedirá un nuevo valor para cada atributo del ítem indicado. En caso de omitir el número de ítem los nuevos valores entrados para cada atributo se aplicarán al último ítem de la matriz.

**Ejemplos:**

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

**xmldownload** Genera un fichero de comandos de configuración en formato xml.

**Sintaxis:** `zbp /> xmldownload`

**Argumentos:** -

**Observaciones:** A diferencia del comando `download`, los comandos mostrados con el `xmldownload` sí son dependientes del directorio en que nos encontremos, y el listado no comienza con el comando de `restore`

**Ejemplo:** `zbp /> xmldownload`

## Comandos de Control

**cd** Cambia el directorio activo.

**Sintaxis:** zbp /> **cd** *nombre*

**Argumentos:**

*nombre* Nombre del directorio de destino.

**Observaciones:** El directorio de destino debe encontrarse en el directorio actual o bien escribir la ruta relativa.

Para hacer activo el directorio del nivel inmediatamente superior deben utilizarse dos puntos: **cd ..**

Al cambiar de directorio el prompt muestra, además de las letras de identificación del equipo, el nombre del directorio activo. Ejemplo: **zbp /main>**.

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

**exit** Cierra la conexión entre el ordenador y el equipo y, por tanto, la sesión del programa CLI.

**Sintaxis:** zbp /> **exit**

**Argumentos:** -

**Observaciones:** -

**Ejemplo:** zbp /> **exit**

**quit** Cierra la conexión entre el ordenador y el equipo y, por tanto, la sesión del programa CLI.

**Sintaxis:** zbp /> **quit**

**Argumentos:** -

**Observaciones:** -

**Ejemplo:** zbp /> **quit**

**reboot** Reinicializa el equipo sin necesidad de apagarlo y volver a encenderlo para, por ejemplo, aplicar los cambios de configuración salvados.

**Sintaxis:** zbp /> **reboot**

**Argumentos:** -

**Observaciones:** -.

**Ejemplo:** zbp /> **reboot**

**reload** Vuelve a cargar la configuración guardada en el equipo.

**Sintaxis:** zbp /> **reload**

**Argumentos:** -

**Observaciones:** Este comando puede ser útil en el caso de que se desee volver a cargar la configuración guardada en el equipo después de la última vez que se salvó.

**Ejemplo:** zbp /> **reload**

**telnet** Manteniendo abierta la conexión establecida entre el ordenador y el equipo, abre una sesión telnet.

**Sintaxis:** zbp /> **telnet** *Host*[*Port*]

**Argumentos:**

*Host* Nombre del host de destino de la sesión telnet.

*Port* (*opcional*) Número de puerto de destino objeto de la sesión telnet.

**Observaciones:** Para volver a iniciar sesión se deberá entrar de nuevo el login y el password.

Se pueden utilizar las 3 letras que identifican el equipo como nombre de host.

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

## Comandos de Estado y Diagnóstico

**clear** Borra las estadísticas.

**Sintaxis:** zbp /> **clear**

**Argumentos:** -

**Observaciones:** -

**Ejemplo:** zbp /> **clear**

**date** Muestra la fecha y hora registrada en el equipo.

**Sintaxis:** zbp /> **date**

**Argumentos:** -

**Observaciones:** -

**Ejemplo:** zbp /> **date**

**help** Muestra un listado de todos los comandos disponibles y una breve descripción de su función.

**Sintaxis:** zbp /> **help**

**Argumentos:** -

**Observaciones:** -

**Ejemplo:** zbp /> **help**



**Log / Log all** Muestran el listado de eventos producidos en el equipo. Este comando es útil para monitorizar el equipo y detectar posibles errores durante su funcionamiento.

**Sintaxis:** zbp /> **log** [*all*]

**Argumentos:**

- Sin argumentos, este comando muestra los eventos registrados en la memoria no volátil del equipo.
- all* (Opcional) Muestra todos los eventos que se producen en el equipo en tiempo real hasta que el usuario presione una tecla.

**Observaciones:** Todos los eventos producidos en el equipo se almacenan en un buffer de memoria con capacidad para 100 registros y al ocurrir un evento importante (inicios de sesión, cambios de configuración, etc.) éste es registrado en la memoria no volátil del equipo, que también tiene una capacidad de 100 registros.

Tanto el buffer como la memoria no volátil son de tipo circular, es decir, una vez llena la memoria, cada vez que se registra un nuevo evento se elimina el más antiguo.

Operativamente, se crean dos logs, el que tiene carácter permanente (comando **log**) y el que tiene carácter temporal y global (comando **log all**).

Es posible filtrar a voluntad el log temporal, usando como filtro el texto a continuación del comando. Esta operativa funciona con cualquier texto en el filtro, no únicamente con la categoría (véase apartado **Información incluida en el log**), de modo que es posible filtrar trazas de procesos individuales o eventos seleccionados.

**Ejemplo:**

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

**ls** Muestra un listado del directorio activo. Este comando es útil para verificar si el parámetro de configuración que se quiere consultar/modificar está en el directorio activo.

**Sintaxis:** zbp /> **ls**

**Argumentos:** -

**Observaciones:** -

**Ejemplo:** zbp /> **ls**

## ping

Envía paquetes ICPM ECHO\_REQUEST a un host determinado.

**Sintaxis:** zbp /> **ping host**

**Argumentos:**

*host* Nombre del host o dirección IP de destino.

**Observaciones:** Al ejecutar este comando, el equipo comenzará a hacer pings al host indicado hasta que el usuario pulse la combinación de teclas **Ctrl.+C**.

**Ejemplo:** zbp /> **ping 172.16.50.38**  
zbp /> **ping zbp**

## stats

Muestra los parámetros de estado del equipo. Estos parámetros son los derivados del propio uso del equipo como, por ejemplo, El uso de memoria o CPU, la temperatura, los bytes transmitidos, etc.

**Sintaxis:** zbp /> **stats [parámetro]**

**Argumentos:**

*parámetro* (Opcional) Nombre del parámetro del cual queremos consultar su estado.

**Observaciones:** Al igual que los parámetros de configuración también están clasificados por categorías a modo de árbol de directorios.

El uso normal de este comando es sin argumentos y desde el directorio raíz, lo que mostrará todos los parámetros del estado del equipo.

Para mostrar un parámetro de estado determinado o los de un directorio concreto, es preciso conocer los nombres de cada uno.

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

## A.3 INSTALACIÓN DE CERTIFICADOS PARA GESTIÓN HTTPS

El servidor incluido en el equipo soporta el protocolo HTTP y HTTPS, siendo necesario para la ejecución de este último la instalación de certificados.

El procedimiento de carga de los certificados para gestión HTTPS, **una vez se tenga el certificado, la clave privada y la contraseña de esta última**, es el siguiente:

1- Acceder al apartado de configuración de la interfaz web.

(**“cd /admin/web”**)

2- Cargar un **certificado** válido en **“cert”** con el comando **“upload cert raw”**.

El procedimiento para volcar el certificado es, en primer lugar, **tener copiado previamente el certificado** en el portapapeles (**Copy**). A continuación, **ejecutar el comando de upload** indicado y, cuando el mismo está en espera, **pegar los datos del portapapeles (Paste)**. Esperar 30s aproximadamente. Transcurrido este tiempo, se mostrarán los datos.

3- Cargar una **clave privada** válida en **“privatekey”** con el comando **“upload privatekey raw”**.

El procedimiento es idéntico al indicado para la carga del certificado.

4- Introducir la **contraseña de la clave privada** en **“privatekeypwd”** con el comando **“set privatekeypwd”**.

Se pedirá confirmación de la misma dos veces.

5- Activar en el equipo el acceso mediante HTTPS

(**“set https on”**)

6- Solicitar la activación de los cambios

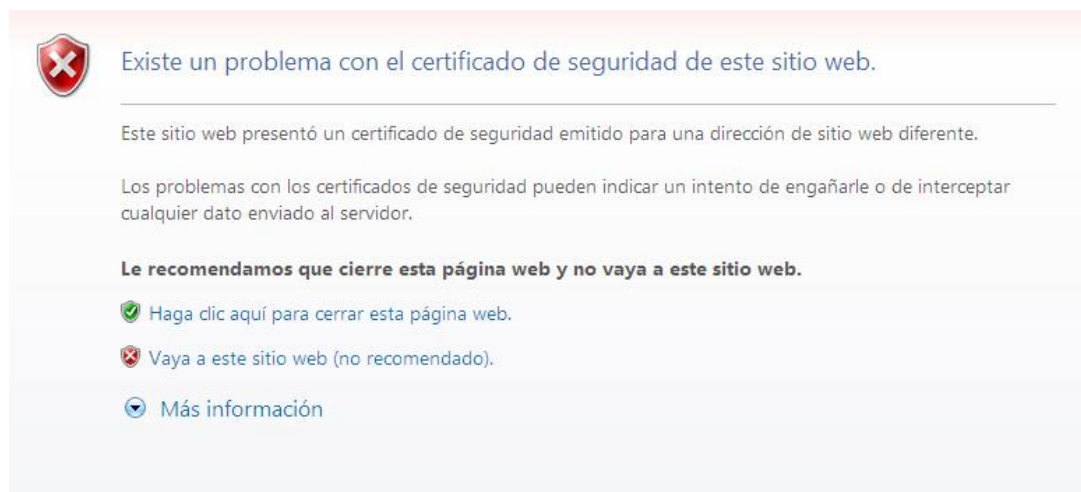
(**“apply”**)

7- Almacenar los nuevos datos (opcional)

(**“save”**)

8- **Cargar** la página web de configuración del equipo en un navegador (Microsoft Internet Explorer, Mozilla Firefox, etc. Google Chrome no está soportado) <sup>(1)</sup> usando el prefijo “**https://**”, en lugar de **http://**”.

Aparecerá el mensaje siguiente:



Dicho mensaje es una advertencia porque el certificado no ha sido validado por una entidad de confianza, pero el certificado funciona correctamente.

Seleccionar “**Vaya a este sitio web (no recomendado)**”.

El control de acceso al equipo pide la introducción del nombre de usuario (**login**) y la contraseña asociada (**password**).

En un equipo que ya opere con https, el **certificado**, la **clave privada** y la **contraseña de esta última** son parte de los datos que se obtienen con el comando “**download**”. Por tanto, es factible incorporar dichas informaciones en la plantilla de configuración.

---

<sup>(1)</sup> La operación se ha comprobado satisfactoriamente con Microsoft Internet Explorer y Mozilla Firefox. Google Chrome no acepta los certificados autofirmados.

Ejemplo de download en un equipo (EMR-2) que ya opere con HTTPS:

```
emr2 /> download
restore
set /main/hostname emr2
set /main/timezone Madrid
set /admin/web/https on
set /admin/web/cert "-----BEGIN CERTIFICATE-----
\nMIICWzCCACQCCQCCL+NbBdYynDANBqkqhkiG9w0BAQUFADByMQswCQYDQQGEWJF\
nUZESMBAGA1UECBMJQmFyY2Vsb25hMHRlWwEAYDQHQHEwIChYXjZwXvbmExDDAKBGNV\n
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWdmouc2FsYXRRA\n
m12LmVzMB4XDTEzMDMyNzE1NTAzOVowXDE0MDMyNzE1NTAzOVowc2E1MAkGA1UE\n
nBhMCRVmxEjAQBGNVBAGTCUJhcmlbG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww\n
nCgYDVQQKEWNaSVYxZjAMBGNVBAMTBUpvc2VwMWR0wGwYJKozIhvcNAQkBFg5qLnNh\n
\nbGF0QHppdi5lczCBnzANBqkqhkiG9w0BAQEFAAOBjQAwYkCgYEAat49IfdfD/xVO\n
\nGsqL217s6aumdfwr9NYoJw68LbrHY0VZ9OGwen+a1XajBcl21qLZjf1lOh250awE\n
\nnezLH317D5bxS9c+w8YrXowEnYoxUQpK49YGVH7DnqLayI5ptyQbdyMoTKmcxBOZ\n
\nnjNoToViogIz9GRBg6nKCDC4+Pxn3/90CAWEAATANBqkqhkiG9w0BAQUFAAOBqQAT\n
\n7Qt00JT61LcGciF4R5aooiRoZEiTJQBfM6PotZ21apGGhF1Bz0FPn3LRxC1Mb6PI\n
\nnkNatYteCq5FJNjGunF8hDIQVc1x7O2ju2vmG0iyVfsz1eqiy+Tx0dMYsgpBeY3K+\n
\nn8fb+J1jmlPNzPhgMlzPK6VGNA70/QhfCG915xK1owQ==\n
\n-----END CERTIFICATE-----"
set /admin/web/privatekey "-----BEGIN RSA PRIVATE KEY-----
\nMIICWwIBAAKBgQC3j0h918P/FU4ayovbxuzpq6Z0Vav01ignDrwtusdjRVn04bB6\n
\nnf5qVcCMFyXawotmN/WU6HbnRprYR5ksffwUP1vFL1z7DxivBehYSdg7FRckrj1ga8\n
\nfsOeosDIjmm3JBt3IyhOQxzEE5mM2hohwKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB\n
\naOGA0VDzYhVKhjodHlUzm3lbsZzAk1KAKNorgn8kxpbYE/RM8mkv9f/Lb3jwhiEu\n
\nnxyf7m7BmNMcx8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S\n
\n\nApuozFYmh34uBl6SJKudihCs4jM1ocQBQMhQ7mXe7Sk1sgECQDgpdSDx45vm8Yk+\n
\n\nnGoX4UzCRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcnOpU8bFtQbwfjKThHthQBN\n
\n\nnrUeEREj9AkeA0S4ernXQGVJGm7b6JhJXFKkILVyo5vP0C3jx7ByRIMt41kl1417Q\n
\n\nntzNepkjlcmimzLWuHJAiyTbtvzfVcnu4YQJAaX0aX3HkwSgosIppq0QLfGp7yJNQU\n
\n\nnqt5h+vZ06FTuSFPm3t0D4G0K6M1N0nKNIEm2CAJpg0JU8BY66jupEqGrUQJAW7wp\n
\n\n\nns/1pJEDjPg/p+1keHqvBLwdQZX1dbM442rjn1AZBNzq01ZuwTEvUWCLG3fMt9iBN\n
\n\n\nnVq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1Xst5nxH8U2Zk1u7ZWZzhOTcw\n
\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_lvl 15
set /access/web/method tacacsplus
```

De no disponer de certificado, ni de clave privada, es posible crear uno. Por ejemplo, siguiendo las instrucciones en [http://www.akadia.com/services/ssh\\_test\\_certificate.html](http://www.akadia.com/services/ssh_test_certificate.html), aunque para ello debe disponerse de un equipo Linux en el que ejecutar las instrucciones.

A continuación, se indica un ejemplo de certificado, así como de clave privada.

A tener en cuenta que las líneas de cabecera y pie se incluyen como parte del propio certificado.

Ejemplo de **certificado** válido:

```
-----BEGIN CERTIFICATE-----
MIICWzCCACQCCQCCL+NbBdYynDANBggkqhkiG9w0BAQUFADByMQswCQYDVQQGEWJF
UZESMBAGA1UECBMJQmFyY2Vsb25hMRIWEAYDVQQHEW1CYXJjZWxvbmExDDAKBgNV
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWdmouc2FsYXRA
eml2LmVzMB4XDTEzMDMyNzE1NTAzOVV0XDTEzMDMyNzE1NTAzOVV0wjcjELMAKGA1UE
BhMCRVMEjAQBGNVBAGTCUJhcmNlbg9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww
CgYDVQQKEWNaSVYxZjAMBGNVBAMTBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh
bGF0QHppdi5lczCBnzANBggkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA49IfdFD/xVO
GsqL217s6aumdfwr9NYoJw68LbrHY0VZ90Gwen+a1XajBcl2lqLZjf1lOh250awe
eZLH31lD5bxS9c+w8YrwxowEnYoxUqPK49YgVH7DnqLayI5ptyQbdyMotkMcbOZ
jNoToVioGiZ9GRBg6nKCDC4+Pxn3/90CAWEAATANBggkqhkiG9w0BAQUFAAOBgQAT
7Qt00JT6lLcGciF4R5aooiRoZEiTJQBfM6PoTZ21apGGHf1Bz0FPn3LRxC1Mb6PI
kNatYteCq5FJNjGunF8hDIQvc1x702ju2vmGoiyvFsZleqiy+Tx0dMYSgpbEY3K+
8fb+J1jmlPNzPhgMlzPK6VGNA70/QhFCG915xK1owQ==
-----END CERTIFICATE-----
```

Ejemplo de **clave privada** válida:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6Z0Vav01ignDrwtusdjRVn04bB6
f5qVccMFyXawotmN/WU6HbnRpYR5ksffwUPlvFL1z7DxivBehYSdg7FRckrj1ga8
fs0eosDIjmm3JBt3IyhOQxzEE5mM2hOhwKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB
AoGA0vDzYhVKhjodHlUzm3lbsZzAk1KAKNorgn8kxbyE/RM8mkv9f/Lb3jwhiEu
xyf7m7BmNmCex8bSRwduzrUnk66Dw8jp3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S
ApuozFYmh34uBl6SJKUdihCs4jm1ocQBQMHQ7mXe7Sk1sgECQQDgpdSDx45vm8Yk+
Gox4UzCRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcnOpU8bFtQbwfxjkThHthQBN
rUeEREj9AkeA0S4ernxQGVJGm7b6JhJXFkKILVyo5vP0C3jx7ByRIMt41k11417Q
tzNepKj1cmimzLWuHJAiyTbtvzfvcnu4YQJAaxOax3HkwSgosIppq0QLfGp7yJNQu
qt5h+vZ06FTuSFPm3t0D4G0K6MlN0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7wp
s/lpJEDjPg/p+lkeHqvBLwdQZx1dbm442rjn1AZBNzq01ZuWTEVUWCLG3fMt9iBN
Vq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1Xst5nxH8U2Zk1u7ZWZZhOTcw
ezG/TDLBwkROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==
-----END RSA PRIVATE KEY-----
```