Annexos del treball:

Acoblament del senyal del *power line communications* d'alta freqüència en línies d'alta tensió per la transmissió de dades per les *smart grids*

1.1 Acoblador capacitiu ACA

ACOPLAMIENTO PLC ENCHUFABLE EN EL INTERIOR DE UN CONECTOR EN T SIMÉTRICO

DESCRIPCIÓN ACA-500

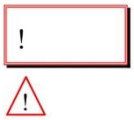
Rev. 7 - Abril 2014

ZIV communications S.A.U.
Antonio Machado,78-80
08840 Viladecans, Barcelona-Spain

Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: communications@ziv.es

www.communications.ziv.es

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

1 INTRODUCCIÓN

1.1 GENERALIDADES

El ACA-500 es un acoplamiento capacitivo diseñado para la transmisión en la denominada banda ancha, de señales de alta frecuencia moduladas por equipos de comunicaciones basados en la tecnología Powerline Communications (PLC), entre una fase de las líneas de Media Tensión (MT) y tierra.

El acoplamiento se instala roscado en el vástago del conector en T, accesible en celdas de distribución de Media Tensión. Para que la unión sea perfecta las medidas del cono roscado encajan perfectamente con el hueco de la "T". Incluso es necesario el uso de un lubricante adecuado para poder introducir el acoplamiento hasta el final, garantizando así que no quede aire, y el máximo aislamiento entre partes externas y el contacto interno, sometido a la tensión de la línea.

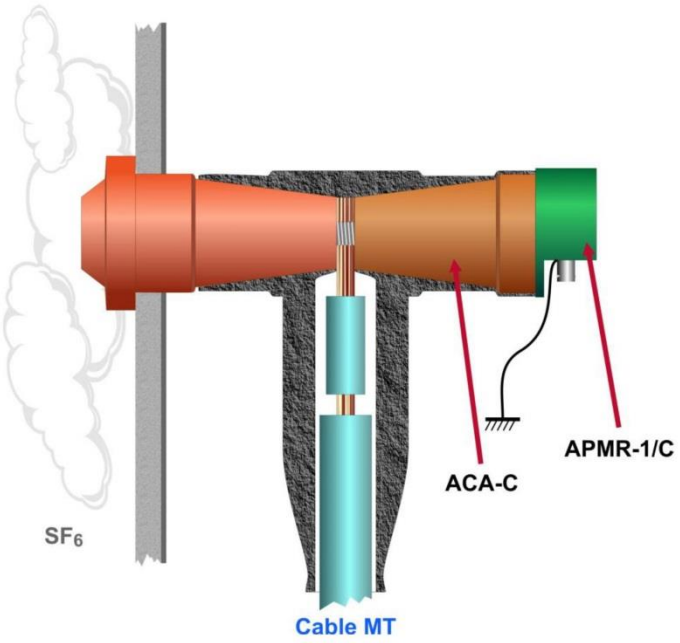


Figura 1 Detalle de instalación del ACA-500 en el interior de un conector en T simétrico

1.2 CONSTITUCIÓN

El aspecto exterior del ACA-500 puede verse en la Figura 2. El ACA-500 se compone de dos bloques bien diferenciados. El primer bloque, ACA-C, contiene el condensador de acoplamiento, diseñado para ser insertado en el interior de un conector en T simétrico para cable con aislamiento seco.

El segundo bloque, APMR-1/C, véase detalle en Figura 3, permite la conexión al equipo de comunicaciones a través de una toma BNC. Contiene asimismo los elementos de protección, adaptación y aislamiento.

La masa de la conexión BNC no está conectada al borne de tierra, el cual es accesible mediante un espárrago M6. La salida, por tanto, es balanceada aunque puede ser suministrada, bajo demanda, no balanceada

Figura 2 Aspecto exterior del ACA-500 y detalle del bloque APMR-1/C

Figura 3 Detalle del conector BNC y del borne de tierra del bloque APMR-1/C

1.3 CARACTERÍSTICAS TÉCNICAS

1.3.1 Características eléctricas

Tipo de acoplamiento	Fase-Tierra mediante condensador de 500 pF
Tensión máxima línea MT	24 kV_{ef} (entre fases)
Capacidad de acoplamiento nominal	500 pF
Rigidez dieléctrica (50 Hz/1 min)	50 kV_{ef} según UNE 21333/(CEI 60358)
Onda de impulso (1,2/50 μs)	125 kV con 15(+) y 15 (-) impulsos según UNE 21333/(CEI 60358)
Descargas parciales	<5 pC a 16,63 kV_{ef} ($1{,}2V_{máx}/\sqrt{3}$) según UNE 21333/(CEI 60358)
Aislamiento del transformador de adaptación [1]	5 kV_{ef} /1 minuto
Distorsión armónica e intermodulación	70 dB a 2 MHz
Potencia media	10 W
Aplicación	Interior

1.3.2 Elementos de protección

Drenaje a tierra de la corriente de 50 Hz

Impedancia a 50/60 Hz	< 1Ω
Corriente soportada a 50/60 Hz	1 A_{ef} permanente. 50 A_{ef} durante 0,2 s

Descargador de gas

Modelo	CG-230

[1] Los transformadores son completamente ensayados individualmente.

Tensión nominal	230 VP
Corriente de descarga CA nominal	20 A (10 x 1 s)
Impulso de corriente de descarga nominal	20 kA (10 impulsos de 8/20 µs)

1.3.3 Características de transmisión

Rango de frecuencias nominales	2 ÷ 30 MHz
Impedancias nominales	50 Ω
Pérdidas de inserción [2]	Según gráfica de la Figura 4

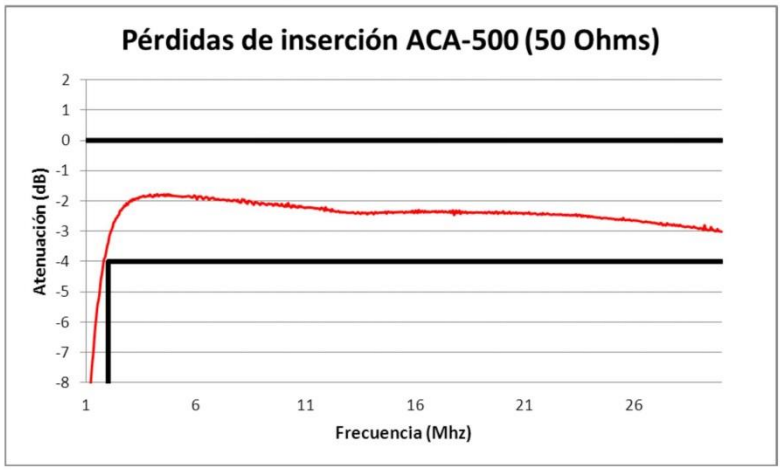


Figura 4 Pérdidas de inserción dB/MHz para impedancia de línea de 50 Ω

[2] Las pérdidas de inserción dependerán de la impedancia del generador y de la impedancia presentada por la línea. La gráfica muestra las pérdidas para 50 Ω de generador y 50 Ω de línea.

1.3.4 Características mecánicas

Conexión al equipo	Mediante conector BNC [3] y cable RG-58. (Balanceada)
Conexión a tierra	Mediante espárrago roscado M6 de acero inox. A2-70
Dimensiones bloque ACA-C [4]	Véase Figura 5
Dimensiones bloque APMR-1/C	Véase Figura 6
Longitud total del conjunto	148 mm
Peso total	0,965 kg
Par de apriete nominal bloque ACA-C	Consultar el valor determinado por el fabricante del conector enchufable. Recomendable de 30 a 40 Nm. Nunca superior a 60 Nm

1.3.5 Condiciones de funcionamiento y almacenamiento

Rango de temperatura	-10 °C a +60 °C
Temperatura y humedad	Según EN 60870-2-2 clase C2 (climatograma 3K6)
Condiciones de almacenamiento	-20 °C a +70 °C

[3] La masa de la conexión BNC no está conectada al borne de tierra. La salida, por tanto, es balanceada aunque puede ser suministrada, bajo demanda, no balanceada.

[4] Las dimensiones del bloque ACA-C son adecuadas para poder ser instalado en los conectores enchufables en T, simétricos, cuyas dimensiones cumplen con la norma UNE EN-50181.

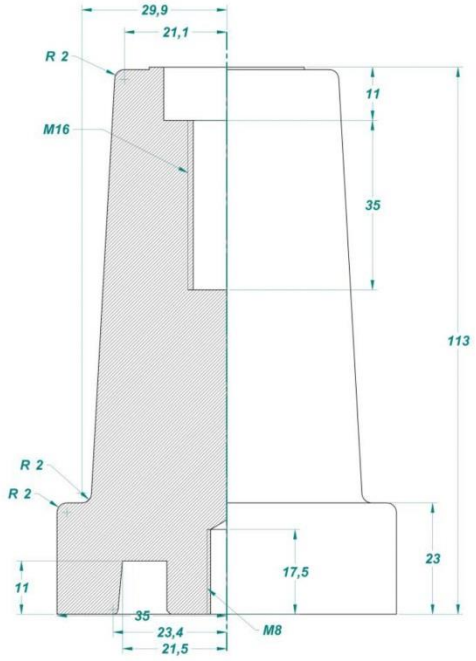


Figura 5 Dimensiones bloque ACA-C

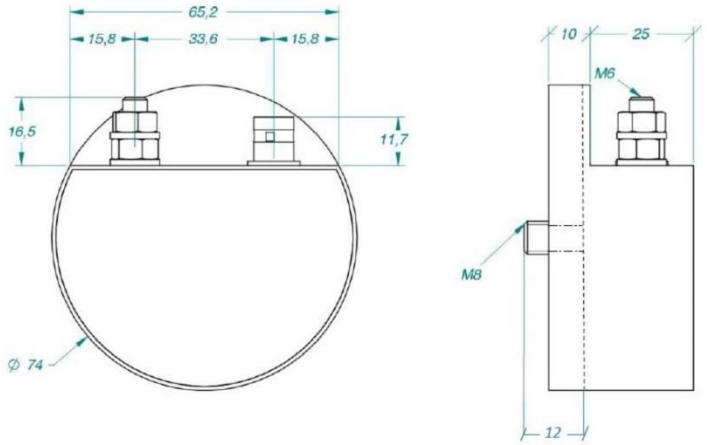


Figura 6 Dimensiones bloque APMR-1/C

2 INSTALACIÓN DEL ACA-500

2.1 ADVERTENCIAS PREVIAS A LA INSTALACIÓN ⚠

! **1.** El acoplador ACA-500 debe instalarse y manipularse cumpliendo los estándares de seguridad (EN 50110-1 y EN 50110-2).

2. Especial consideración deben tener los puntos siguientes:

- Únicamente personal cualificado y designado por la compañía propietaria de la instalación debe llevar a cabo la instalación y manipulación del ACA-500.
- Deben tenerse en consideración 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.
- Debe suprimirse el voltaje de la línea de Media Tensión y conectar ésta a tierra.
- El entorno de funcionamiento debe ser el apropiado para el acoplador, asegurando el cumplimiento de las condiciones indicadas en el apartado 1.3, *Características técnicas*.

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.

2.2 INSTRUCCIONES DE INSTALACIÓN

La Figura 8 muestra un ejemplo de instalación del acoplamiento ACA-500. El detalle de instalación de los distintos bloques puede verse en la Figura 7.

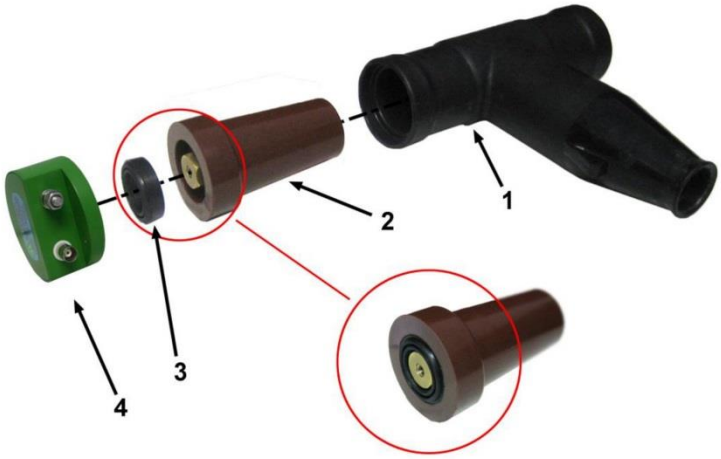


Figura 7 Instrucciones para la colocación de los bloques ACA-C (2) y APMR-1/C (4)

Figura 8 Ejemplo de instalación del acoplamiento ACA-500

Las instrucciones para la instalación del ACA-500 son las siguientes:

1. Limpie bien el interior del vástago del conector en T (pieza 1 en Figura 7) y el del bloque ACA-C (pieza 2 en Figura 7), utilizando un paño que no deje restos, dejando las superficies bien secas sin que queden rastros de líquido.

2. Lubrique con grasa de silicona dieléctrica el interior del vástago del conector en T y el del bloque ACA-C.

3. Introduzca el ACA-C en el vástago del conector hasta comenzar a roscar en el espárrago del mismo. Puede ser necesario permitir la salida del aire mediante la utilización de un hilo fino de nylon introducido junto el bloque ACA-C. En ese caso, antes de apretar totalmente la pieza, el hilo debe ser totalmente extraído asegurándose de que no quede ningún trozo atrapado.

4. Utilice una llave dinamométrica del nº:24 para realizar el apriete de la pieza. El par de apriete dependerá del modelo y fabricante del conector enchufable en T, para ello consultar el fabricante, nunca se debe superar un par de apriete de 60 Nm ya que la rosca del vástago de interconexión podría dañarse.

5. Coloque hasta el fondo la arandela de goma suministrada (véase pieza 3 y detalle de colocación en Figura 7) y el bloque APMR-1/C (pieza 4 en Figura 7), apretándolo fuertemente con la mano (para de apriete recomendable 10 Nm) y asegurándose de que el conector BNC queda dispuesto en el lado de interés, generalmente hacia abajo.

6. Conecte el borne roscado de conexión a tierra (par de apriete inferior a 7 Nm) a la tierra de protección más cercana a la conexión de la pantalla de la fase por donde se transmite. El cable debe ser lo más corto posible, siendo apropiada una sección de 16 mm^2 puesto que es la utilizada para la conexión a tierra de la pantalla del propio cable de Media Tensión.

7. Tenga muy presente las advertencias siguientes:

⚠ **La conexión a tierra del borne roscado del bloque APMR-1/C es imprescindible para dar seguridad a los equipos y a las personas.**

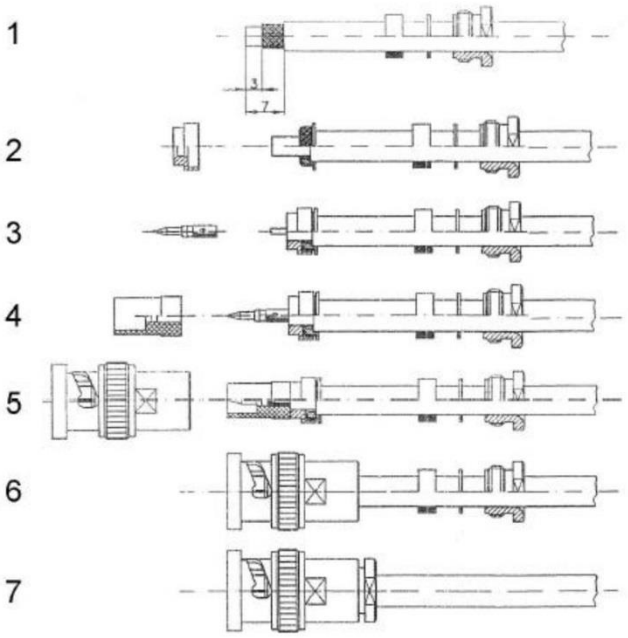
No realizarla entraña un riesgo muy importante ya que el condensador de acoplamiento quedaría conectado directamente a los bornes de salida sin que existiera drenaje a tierra.

En caso de desinstalación, los dos bloques que conforman el ACA-500 deben ser extraídas y, en su lugar, debe ser colocado el conector aislado "BASIC INSULATING PLUG" junto con el tapón semiconductor, recomendado por el fabricante del conector. ¡¡ No confundir el bloque ACA-C con un tapón de baja capacitancia!!.

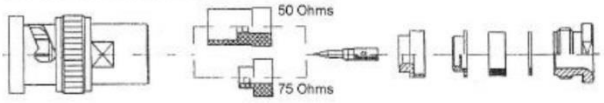
Si por alguna circunstancia el bloque ACA-C debiera permanecer conectado, es estrictamente obligatorio que el terminal roscado M8 quede conectado, mediante un cable conductor de 16 mm^2 de sección, a la tierra de protección.

8. El cable de conexión entre el equipo de comunicaciones y el ACA-500 debe ser un cable coaxial de 50 Ω de impedancia característica (tipo RG58) y longitud de 4 m. Este cable puede ser protegido, si es necesario, contra la acción de animales, insertándolo en un tubo ondulado corrugado de PVC.
   Como orientación, para el montaje del conector BNC macho en el cable coaxial, se incluyen, dos instrucciones. Una de ellas para conector soldado y otra para conector engarzado a presión o "crimpado".
   Antes de instalarlo definitivamente, el cable debe comprobarse para evitar tener que realizar una nueva descarga de la línea de media tensión debido a un defecto en el mismo.
   Una vez el conector BNC macho ha sido montado, la comprobación debe ser realizada de la siguiente manera.
   En primer lugar, sin conectar el cable coaxial al ACA-500, se debe medir un circuito abierto en el otro extremo del cable, lado equipo.
   En segundo lugar, una vez el cable ha sido conectado al ACA-500 mediante el conector BNC de la base (pieza 2), en el mismo extremo, debe medirse un cortocircuito debido ahora a la presencia del transformador del ACA-500.

Construcción del cable de conexión para conector soldado



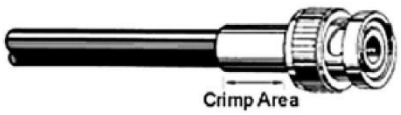
DESPIECE CONECTOR BNC



Construcción del cable de conexión para conector engarzado a presión (“crimpado”)

Retirar las piezas del conector de la forma mostrada, sin que sufran daño alguno.

Córtese el cable como se muestra, teniendo cuidado de no mellar ni el conductor ni la malla del mismo.



Coloque las piezas suministradas en la posición correcta de forma que no se produzcan cortocircuitos entre la malla y el vivo del conductor. Apriete con la herramienta adecuada.

1.2 Acoblador capacitiu CAMS

UNIDAD DE ACOPLAMIENTO
PARA EQUIPOS PLC
SOBRE LÍNEAS DE MEDIA TENSIÓN

DESCRIPCIÓN CAMS-10/C

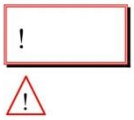
Rev. 3 - Marzo 2017

ZIV communications S.A.U.
Antonio Machado,78-80
08840 Viladecans, Barcelona-Spain

Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: communications@ziv.es

www.ziv.es

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

1 INTRODUCCIÓN

1.1 GENERALIDADES

El CAMS-10/C es un acoplador capacitivo que se utiliza para inyectar las señales de Alta Frecuencia generadas por los equipos de comunicaciones que utilizan tecnología Powerline Communications (PLC) a la línea de media tensión (MT).

La transmisión se lleva a cabo entre la fase de la línea de MT y tierra.

Así, el acoplador CAMS-10/C realiza las funciones siguientes:

- Acoplamiento de las señales eléctricas de Alta Frecuencia hacia la línea de MT.
- Adaptación de impedancias entre la línea de media tensión y el equipo de comunicación.
- Limitación de las sobretensiones procedentes de la línea y drenaje a tierra de la corriente a frecuencia industrial.
- Aislamiento eléctrico.

Puede utilizarse para cable aéreo o cable subterráneo, en exterior o en celdas con aislamiento de aire y de mampostería.

1.2 CONSTITUCIÓN

El CAMS-10/C está formado por dos bloques independientes, CEMC-10/C y ESMC-10/C, que se ensamblan entre sí formando un conjunto compacto.

El bloque CEMC-10/C (pieza 1) contiene el condensador de acoplamiento, el cual está encapsulado en silicona.

El bloque ESMC-10/C (pieza 2) está constituido por los circuitos de adaptación, protección y aislamiento, y de conexión al equipo de comunicaciones y a la toma de tierra.

Como elementos de protección del segundo bloque destacan dos descargadores de gas, uno lado Alta Tensión (AT) y otro lado Baja Tensión (BT).

La unidad de adaptación está constituida por un transformador de aislamiento, que empareja la impedancia primaria de la línea del acoplamiento fase-tierra con la impedancia secundaria del equipo de comunicaciones.

Como puede apreciarse en la Figura 1, la unidad puede desensamblarse a fin de facilitar el proceso de instalación.

El CAMS-10/C dispone de tres elementos de conexión: el tornillo M16 de cabeza hexagonal para la conexión a línea, tres espárragos M8 para la sujeción del dispositivo y conexión a tierra, y un conector BNC para la conexión al equipo de comunicación.

> La masa de la conexión BNC no está conectada a tierra, por lo que la conexión hacia el equipo de comunicaciones es balanceada.

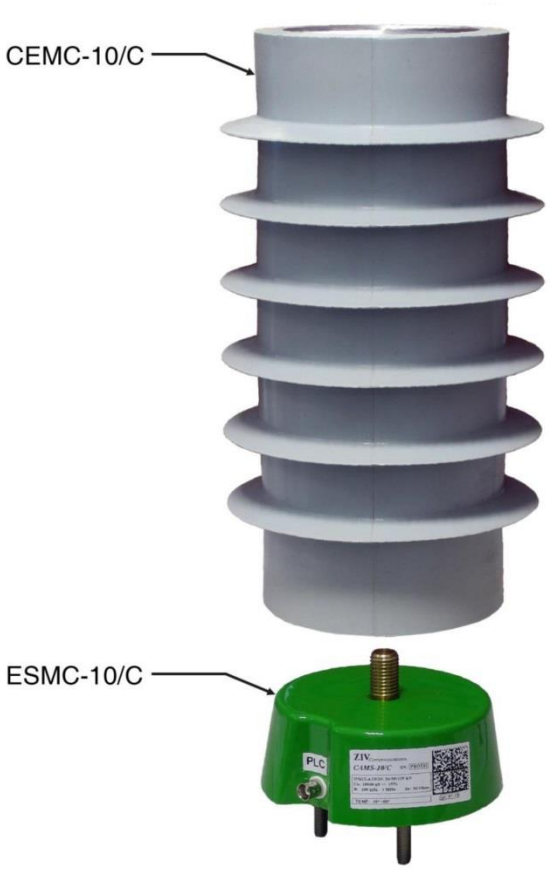


Figura 1 Elementos que conforman el acoplador CAMS-10/C

1.3 CARACTERÍSTICAS TÉCNICAS

1.3.1 Características eléctricas

Tipo de acoplamiento	Fase-tierra capacitivo
Utilización	Interior y Exterior
Tensión máxima línea MT	24 kV_{ef} (entre fases)
Capacidad de acoplamiento nominal	10 nF (±15%)
Aislamiento del bloque ESMC-10/C	5 kV_{ef}/1 min
Línea de fuga (pieza CEMC-10/C)	600 mm
Potencia reactiva	Q = 418,88 Var (a 20/$\sqrt{3}$ kV)

Ensayos individuales

Rigidez dieléctrica	100 kV_{CC} /min según UNE 21333 (CEI 60358)
	30 kV_{ef} (50 Hz/1 min)
Descargas parciales	<10 pC a 15,24 kV_{ef} (1,1$V_{máx}$/ $\sqrt{3}$) según UNE 21333 (CEI 60358)
	<100 pC a 26,4 kV_{ef} (1,1$V_{máx}$) según UNE 21333 (CEI 60358)

Ensayos de tipo

Rigidez dieléctrica (50 Hz/1 min) [1]	50 kV_{ef} según UNE 21333 (CEI 60358)
Onda de impulso (1,2/50 μs) [1]	125 kV con 15 (+) y 15 (-) impulsos según UNE 21333 (CEI 60358)

[1] Los valores han sido medidos por el laboratorio TECNALIA (Baracaldo).

Descargas parciales [1]	<10 pC a 15,24 kV_{ef} (1,1$V_{máx}$/ $\sqrt{3}$) según UNE 21333 (CEI 60358) <100 pC a 26,4 kV_{ef} (1,1$V_{máx}$) según UNE 21333 (CEI 60358)

1.3.2 Características de transmisión

Rango de frecuencias nominales	100 kHz ÷ 1 MHz (con pérdidas de inserción < 1 dB para impedancia de línea de 200 Ω) Hasta 10 MHz (con pérdidas de inserción < 2 dB para impedancia de línea de 200 Ω)
Impedancia nominal lado equipo	50 Ω
Impedancia característica de la línea	200 Ω ÷ 400 Ω
Pérdidas de Inserción	< 1 dB (200 Ω). Véase Figura 2

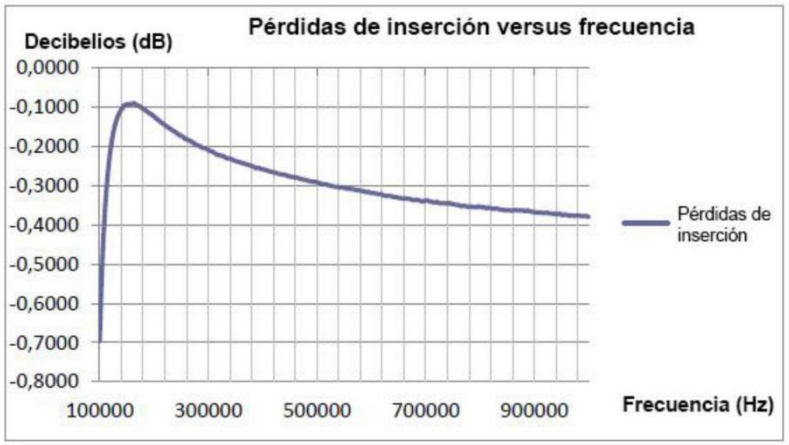


Figura 2 Pérdidas de inserción dB/Hz para impedancia de línea de 200 Ω

1.3.3 Elementos de protección

Drenaje a tierra de la corriente de 50 Hz

Impedancia a 50/60 Hz	< 1Ω
Corriente soportada a 50/60 Hz	1 A_{ef} permanente. 50 A_{ef} durante 0,2 s

Descargador de gas

Cantidad	Dos (uno lado AT y otro lado BT)
Modelo	CG2-350
Tensión nominal	350 V_p
Corriente de descarga CA nominal	20 A (10 x 1 s)
Impulso de corriente de descarga nominal	20 kA (10 impulsos de 8/20 µs)

1.3.4 Características mecánicas

Conexión al equipo de comunicación	Mediante conector BNC y cable RG-58 (Balanceada)
Conexión a la línea	Mediante tornillo M16 x 30 mm, de cabeza hexagonal, de acero inox. A2-70
Conexión a tierra/fijación	Mediante tres espárragos M8 de acero inox. A2-70 (véase plantilla de fijación en Figura 5)

Dimensiones bloque CEMC-10/C	Véase Figura 3
Dimensiones bloque ESMC-10/C	Véase Figura 4
Diámetro de la aleta	172 mm
Longitud total del conjunto	403 mm
Material de encapsulado	Silicona (Pieza CEMC-10/C). Poliamida y fibra de vidrio encapsulada en poliuretano (Pieza ESMC-10/C)
Peso total	7,75 kg
Par de apriete entre bloques	Recomendable de 60 Nm
Par de apriete de la conexión a línea	Recomendable de 80 Nm
Par de apriete de sujeción	Recomendable de 10 Nm

1.3.5 Condiciones de funcionamiento y almacenamiento

Rango de temperatura	-20 ºC a +65 ºC

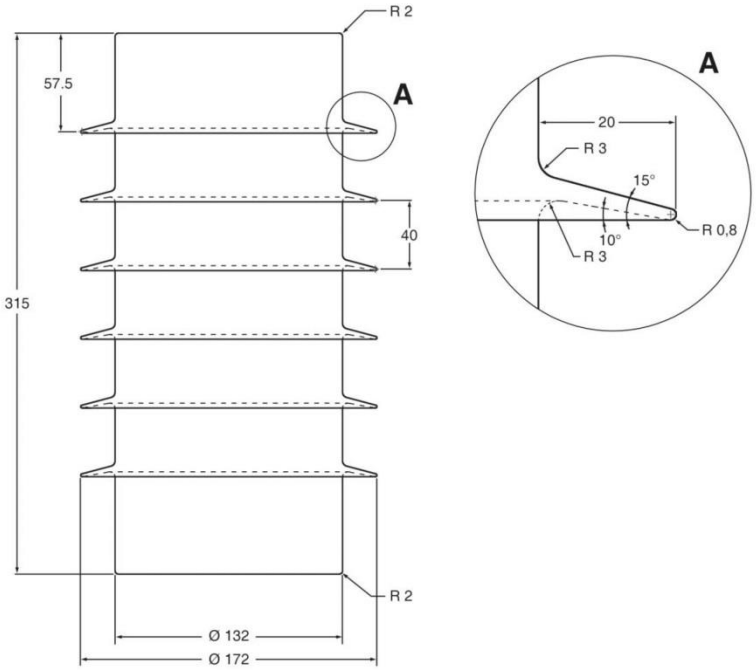


Figura 3 Dimensiones generales del bloque CEMC-10/C

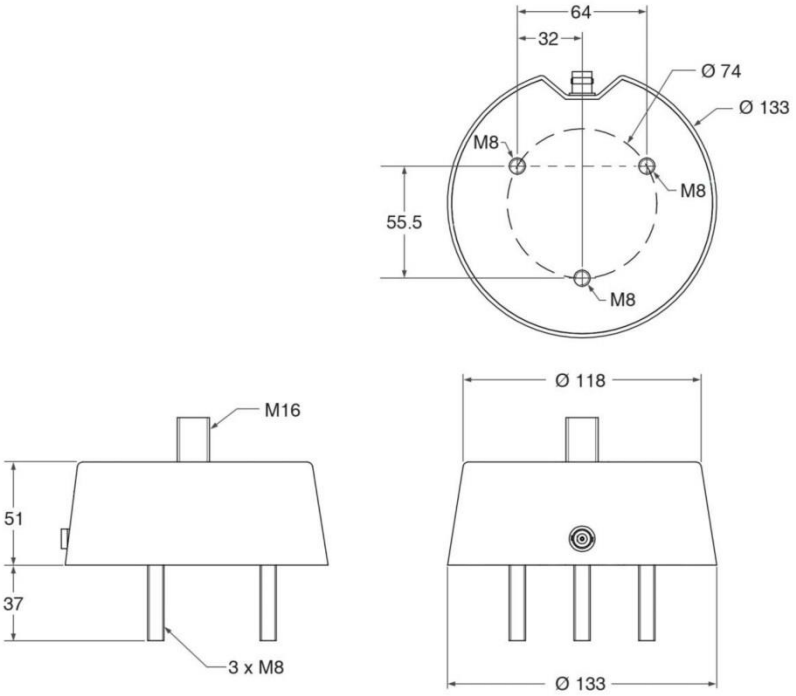


Figura 4 Dimensiones generales del bloque ESMC-10/C

2 INSTALACIÓN DE LA UNIDAD

2.1 ADVERTENCIAS PREVIAS A LA INSTALACIÓN

! 1. La unidad de acoplamiento debe instalarse y manipularse cumpliendo los estándares de seguridad (EN 50110-1 y EN 50110-2).

2. Especial consideración deben tener los puntos siguientes:
   - Únicamente personal cualificado y designado por la compañía propietaria de la instalación debe llevar a cabo la instalación y manipulación de la unidad de acoplamiento.
   - Deben tenerse en consideración 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.
   - Debe suprimirse el voltaje de la línea de Media Tensión y conectar ésta a tierra.
   - El entorno de funcionamiento debe ser el apropiado para la unidad de acoplamiento, asegurando el cumplimiento de las condiciones indicadas en el apartado 1.3, *Características técnicas*.

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.

2.2 INSTALACIÓN

La instalación de la unidad conlleva varias fases, empezando por la fase de sujeción y conexión a tierra para terminar con la fase de conexionado a la línea de Media Tensión y al equipo de comunicación.

⚠ Para realizar un enlace PLC se requieren dos acopladores, uno en cada extremo. En un extremo de la línea se instalará un acoplador, y en el otro extremo y ***en la misma fase*** el otro.

⚠ En instalaciones aéreas, dado que el acoplador puede sufrir cimbreado por efecto del viento, las conexiones deben ser seguras y los distintos cables de conexión estar bien sujetos.

2.2.1 Sujeción y conexión a tierra

El CAMS-10/C puede utilizarse tanto en interior como en exterior. En interior, normalmente se ubica en subestaciones o estaciones transformadoras, dentro de distintos tipos de cabinas o celdas tales como celdas de mampostería y celdas con aislamiento de aire. En exterior, el acoplador se instala en líneas aéreas de distribución de MT (véase ejemplos en Figura 7 y Figura 8).

La ubicación de la unidad debe decidirse teniendo en cuenta la distancia mínima despejada entre el terminal de conexión a la línea y las partes metálicas, paredes y partes no aisladas de la celda o cabina (véase Tabla 1).

Rated Voltage (kV)	Distancia (mm)
3,6	60
7,2	90
12	120
24	220

Tabla 1 Distancias mínimas entre el terminal de conexión a la línea y partes metálicas a tierra

Además, para obtener las máximas prestaciones de transmisión, las conexiones a la línea de MT y a la tierra de protección deben tener la menor longitud posible.

Una vez decidida la posición de instalación:

1. Efectuar en la estructura metálica prefabricada, en los herrajes de la celda o bien en la pared o suelo de la celda metálica, los taladros para la sujeción de la unidad según plantilla (véase Figura 5).

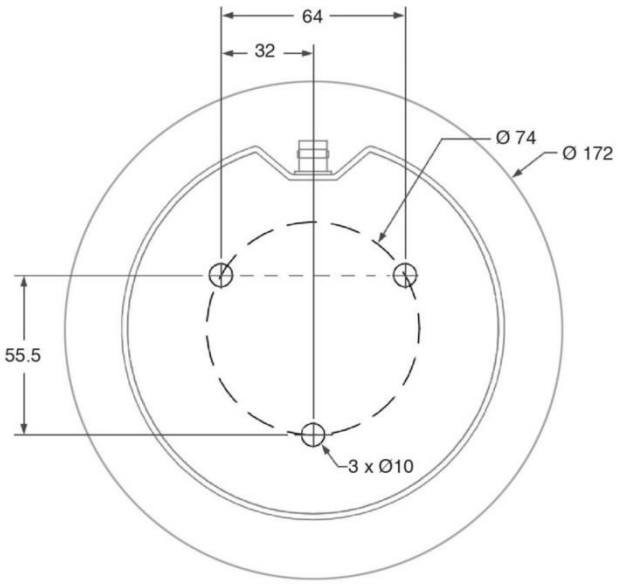


Figura 5 Plantilla de fijación del CAMS-10/C

2. Sujetar la unidad a la base elegida en el punto anterior, mediante los tres espárragos M8 del bloque ESMC-10/C y las tuercas y arandelas M8 suministradas (véase Figura 6). Se recomienda un par de apriete de 10 Nm.
3. Realizar la conexión a tierra. Asegurar la conexión conectando a tierra uno de los espárragos M8 del bloque ESMC-10/C, mediante un cable adicional de al menos 16 mm^2 de sección.

> La sujeción y conexión a tierra de la unidad puede llevarse a cabo de manera más cómoda desensamblando la unidad (véase Figura 1).

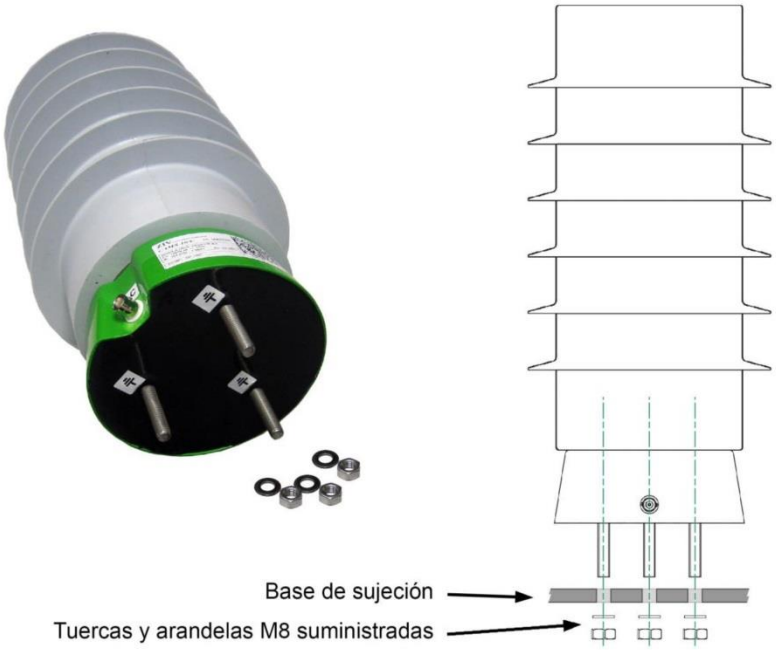


Figura 6 Sujeción del CAMS-10/C

Figura 7 Ejemplo de sujeción mediante un herraje unido a la torre eléctrica

Figura 8 Ejemplo de instalación del CAMS-10/C en línea aérea

2.2.2 Conexión eléctrica a la línea de Media Tensión

La conexión a la línea de MT se efectúa mediante el tornillo de M16 x 30 mm, de cabeza hexagonal, situado en la parte superior del acoplador.

Tal y como se indica en la Figura 9, conectar el cable de MT al tornillo utilizando la arandela Grower y el terminal tubular de pala suministrados.

Se recomienda un par de apriete de 80 Nm.

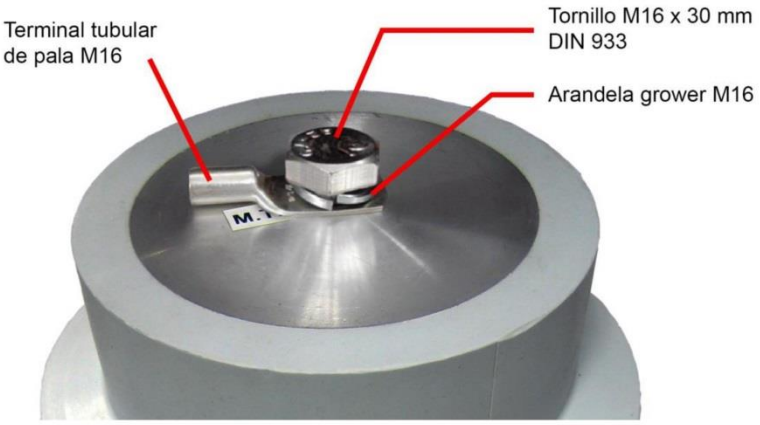


Figura 9 Sujeción del cable flexible de conexión a línea al tornillo M16.

El cable de conexión debe tener la menor longitud posible. La sección mínima recomendada es de 16 mm^2. Por otro lado, debe poder moldearse para que cumpla con las distancias indicadas en la Tabla 1.

2.2.3 Conexión al equipo de comunicación

El cable de conexión entre el equipo de comunicaciones y el acoplador debe ser un cable coaxial de 50 Ω de impedancia característica (tipo RG-58), y se conectará en el conector BNC del bloque ESMC-10/C identificado con la etiqueta "PLC".

El cable puede ser protegido, si es necesario, contra la acción de roedores, insertándolo en un tubo ondulado corrugado de PVC.

Como orientación, para el montaje del conector BNC macho en el cable coaxial, a continuación se incluye una instrucción para conector engarzado a presión o "crimpado".

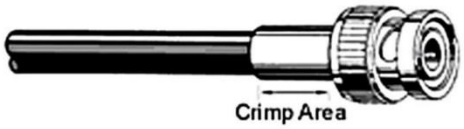
El cable coaxial debe ser comprobado antes de instalarlo, para evitar tener que realizar una nueva descarga de la línea de Media Tensión debido a un defecto en el mismo.

En primer lugar, sin conectar el cable coaxial al acoplador, se debe medir entre el conductor y la parte metálica del conector BNC un circuito abierto en el otro extremo del cable, lado equipo. En segundo lugar, una vez el cable ha sido conectado al acoplador, en el mismo extremo, debe medirse un cortocircuito debido ahora a la presencia del transformador de acoplamiento.

Instrucciones para conector BNC engarzado a presión

Retirar las piezas del conector de la forma mostrada, sin que sufran daño alguno.

Córtese el cable como se muestra, teniendo cuidado de no mellar ni el conductor ni la malla del mismo.



Coloque las piezas suministradas en la posición correcta de forma que no se produzcan cortocircuitos entre la malla y el vivo del conductor. Apriete con la herramienta adecuada.

1.3 Acoblador Inductiu AIMT

ACOPLADOR INDUCTIVO
SOBRE LÍNEAS DE MEDIA TENSIÓN

DESCRIPCIÓN AIMT-2

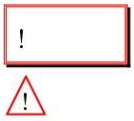
Rev. 6 - Abril 2015

ZIV communications S.A.U.
Antonio Machado,78-80
08840 Viladecans, Barcelona-Spain

Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: communications@ziv.es

www.communications.ziv.es

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

1 INTRODUCCIÓN

1.1 GENERALIDADES

El AIMT-2 es un acoplador inductivo, destinado a sistemas PLC (Powerline Communications), que permite inyectar y transmitir la señal de alta frecuencia en líneas de Media Tensión (MT).

El diseño mecánico del AIMT-2 está concebido para que su instalación se realice de forma fácil y cómoda y, de otro lado, que pueda utilizarse en cables de hasta 50 mm de diámetro.

Puede utilizarse en interior (celdas de mampostería, celdas con aislamiento de aire, celdas con aislamiento de gas, etc.).

El AIMT-2, básicamente, está formado por un núcleo toroidal encapsulado en resina epóxica altamente aislante, el cual permite realizar un acoplamiento inductivo al cable de media tensión. Un descargador de gas protege en modo diferencial contra posibles sobretensiones. Estos elementos, junto con el cierre, borne de conexión a tierra y conector hacia el equipo de comunicación, forman un conjunto compacto.

El aspecto exterior del acoplador inductivo AIMT-2 puede verse en la FIGURA 1.

FIGURA 1 Aspecto exterior del acoplador inductivo AIMT-2

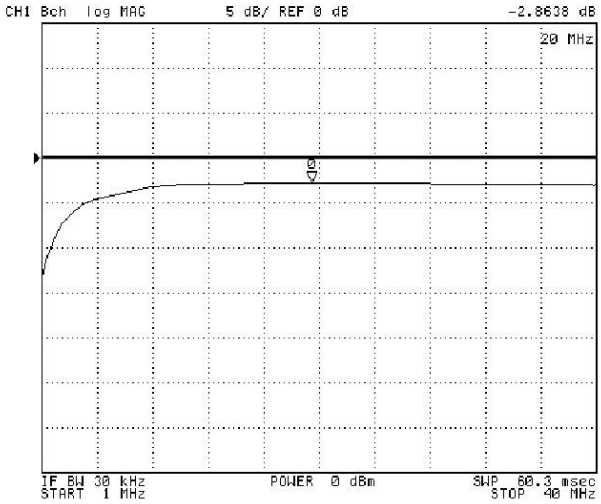
1.2 CARACTERÍSTICAS TÉCNICAS

1.2.1 Características eléctricas

Tipo de acoplador	Inductivo. Fase-tierra
Utilización	Interior
Margen de frecuencias	1 ÷ 40 MHz
Principio de saturación[1]	300 A/50 Hz
Impedancia	50 Ω
Rigidez dieléctrica del AIMT-2	10 kV/1 min
Intensidad Térmica de Cortocircuito (Ith) a 50 Hz [1]	20 kA/1s según EN 60044-1
Intensidad Dinámica (Idyn) a 50 Hz [1]	50 kA según EN 60044-1
Impulso Tipo Rayo (1,2/50 µs) [1]	20 kV según EN 60044-1
Resistencia de aislamiento	>100 MΩ
Protección lado equipo	Descargador de gas 230 V

[1] Los valores han sido certificados en un laboratorio externo (LABEIN).

Pérdidas de inserción	Según frecuencia[2] (Véase FIGURA 2)

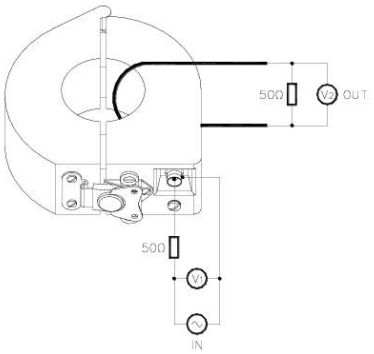


NOTA: El valor medio de las pérdidas para todo el rango de frecuencias es menor de 3,5 dB.

FIGURA 2 Pérdidas de inserción

---

[2] La medida de las pérdidas de inserción viene dada por la expresión:
$H(f) = 20 \log(V_2/V_1) + 6$ (dB)



1.2.2 Condiciones de funcionamiento y almacenamiento

Temperatura y humedad	De -25 a +55 °C y humedad relativa no superior al 95%
Condiciones de almacenamiento	De -40 a +70 °C

1.2.3 Características mecánicas

Dimensiones	Véase FIGURA 3
Diámetro máximo del cable de MT	50 mm
Conexión al equipo de comunicación	Mediante conector BNC (Véase FIGURA 4)
Conexión a tierra	Mediante espárrago M6
Sistema de enclavado	Mediante cierre de tracción giratorio equipado con muelle (Véase FIGURA 4)
Peso	1,4 kg

AIMT-2 es un producto con patente solicitada por ZIVCommunications

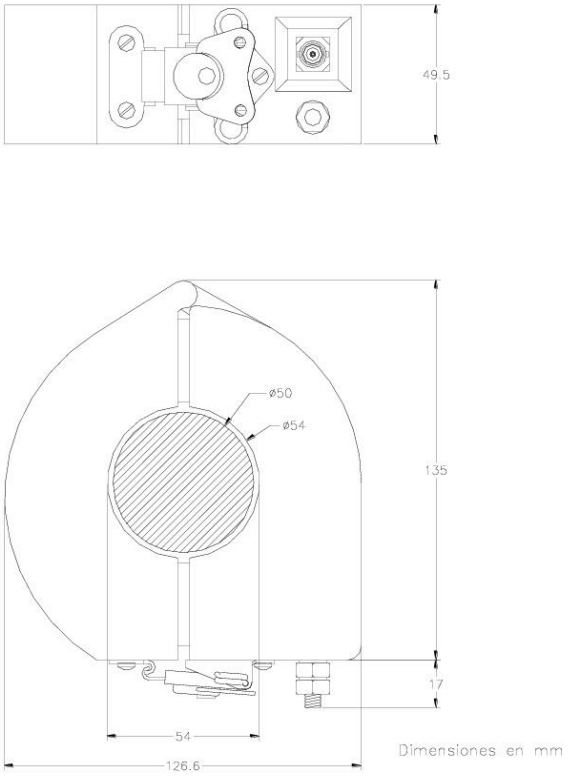


FIGURA 3 Dimensiones generales del acoplador inductivo AIMT-2

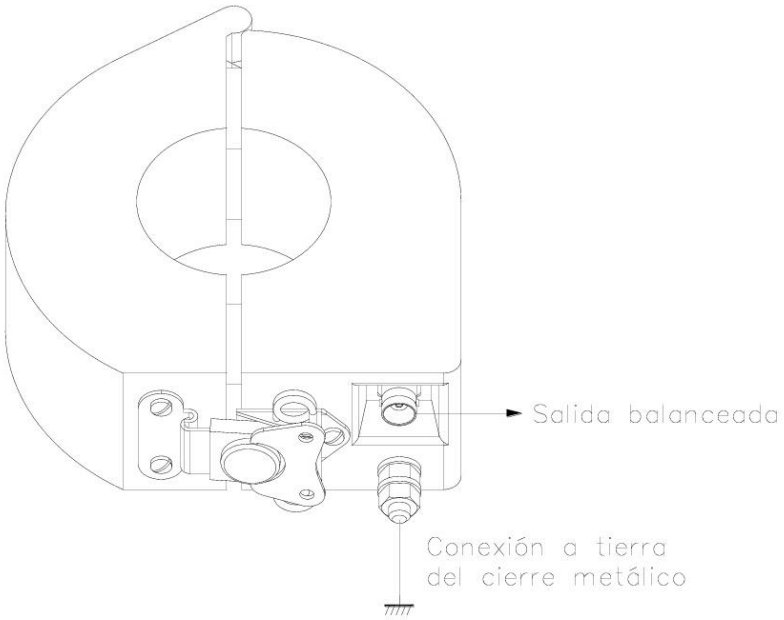


FIGURA 4 Elementos de conexión y enclavado

2 INSTALACIÓN DEL AIMT-2

2.1 ADVERTENCIAS PREVIAS A LA INSTALACIÓN ⚠

! **1.** El acoplador AIMT-2 debe instalarse y manipularse cumpliendo los estándares de seguridad (EN 50110-1 y EN 50110-2).

2. Especial consideración deben tener los puntos siguientes:

- Únicamente personal cualificado y designado por la compañía propietaria de la instalación debe llevar a cabo la instalación y manipulación del AIMT-2.
- Deben tenerse en consideración 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.
- El entorno de funcionamiento debe ser el apropiado para el acoplador, asegurando el cumplimiento de las condiciones indicadas en el apartado 1.2, *Características técnicas*.

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.

2.2 INSTALACIÓN

La instalación del acoplador inductivo AIMT-2 se divide en dos fases bien diferenciadas, conexión a la línea de Media Tensión y conexión al equipo de comunicación.

La conexión a la línea de Media Tensión consiste básicamente en insertar en el interior del acoplador el cable protegido así como la malla de dicho cable la cual, como se indicará más adelante, no deberá estar en contacto con ninguna superficie metálica previamente.

Para poder insertar el cable protegido y la malla de dicho cable en el interior del acoplador, es necesario desensamblar éste. El desensamblaje del acoplador se realiza mediante el cierre.

El procedimiento de apertura del cierre es el siguiente:

1. Desplazar la mariposa del cierre 90°.

2. Girar la mariposa en sentido antihorario hasta liberar el cierre del retén.

3. Tirar del cierre.

4. Separar los dos seminúcleos.

Para ensamblar nuevamente el acoplador, debe realizarse el procedimiento pero a la inversa. Así, una vez se ha insertado el cable protegido y la malla de dicho cable, unir los dos seminúcleos, empujar el cierre y girar la mariposa en sentido horario hasta introducir totalmente el cierre en el retén. Finalmente, desplazar 90° la mariposa hasta dejarla en su posición de reposo, es decir, descansando sobre el muelle.

El cierre está conectado internamente al tornillo de conexión a tierra.

Ejemplo de instalación en interior

La FIGURA 5 muestra un ejemplo de instalación del acoplador en una celda metálica.

FIGURA 5 Ejemplo de instalación del acoplador inductivo AIMT-2 en cable subterráneo

La conexión a tierra de la malla del cable protegido debe efectuarse de la forma indicada en la FIGURA 6.

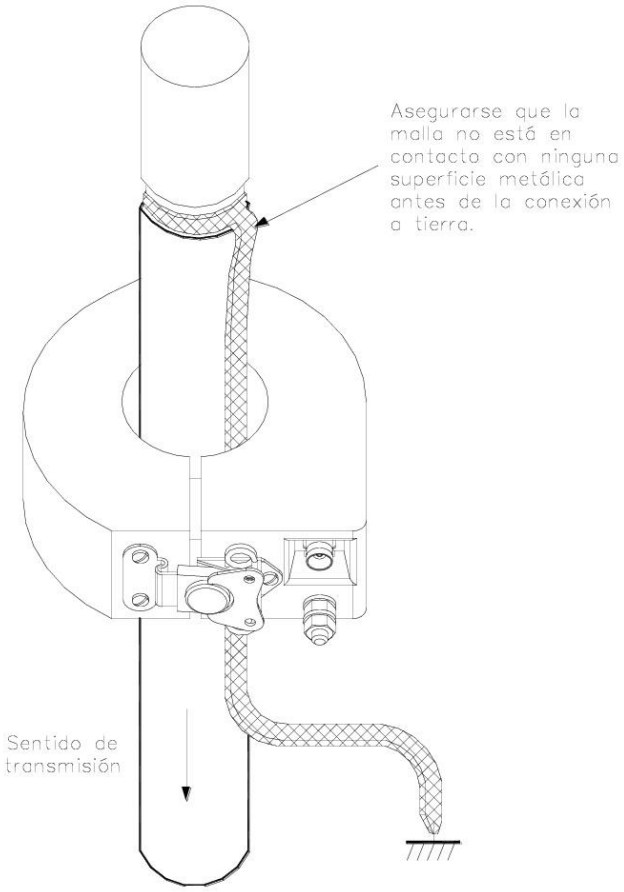


FIGURA 6 Detalle de conexión a tierra de la malla

1.4 Node BPLC DRN

NODO DE COMUNICACIONES UNIVERSAL

DRA-2

MANUAL DE USUARIO

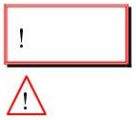
Rev. 1 - Noviembre 2011

ZIV communications S.A.U.
Antonio Machado,78-80
08840 Viladecans,
Barcelona-Spain

Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: communications@ziv.es

www.communications.ziv.es

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

1 INTRODUCCIÓN

1.1 REDES INTELIGENTES

Las redes inteligentes, más conocidas como "smartgrids", están en boca de todos, y no sólo de los especialistas/técnicos del sector eléctrico. Hoy en día, es habitual que los medios de comunicación se hagan eco de los avances en este área. Todo el mundo habla de las distintas aplicaciones que conforman las "smartgrids", desde la gestión de la demanda, gracias a las nuevas familias de contadores inteligentes, pasando por la automatización de la distribución, integración de energías renovables, impacto del coche eléctrico en las redes del futuro, etc.

Para hacer realidad dichas aplicaciones son necesarias distintas tecnologías. Entre ellas, tienen un papel fundamental las telecomunicaciones.

Las compañías de distribución eléctrica han venido desplegando redes de telecomunicaciones para proporcionar conectividad remota a todas sus subestaciones eléctricas. Las nuevas aplicaciones de "smartgrids" requerirán dotar de conectividad segura a los Centros de Transformación. Este punto es un gran reto para las áreas de telecomunicaciones de las distintas compañías de distribución eléctrica, principalmente debido al gran número de instalaciones y a la conectividad prácticamente nula existente en la actualidad en dichas instalaciones.

La automatización de los centros de transformación, por tanto, es un paso obligado en el camino hacia la "SmartGrid".

1.2 SOLUCIÓN DRA-2

Para hacer realidad las nuevas aplicaciones de "smartgrids", se necesitan más comunicaciones en los Centros de Transformación. Ahora bien, ¿qué tipo de información deberán transportar los nuevos equipos de telecomunicaciones que instalemos?.

ZIV apuesta por un equipo de comunicaciones universal para Centros de Transformación de Media Tensión, denominado DRA-2.

DRA-2

El DRA-2 está diseñado para transportar los servicios presentes en un Centro de Transformación hacia niveles superiores dentro de la red eléctrica, por medio de una amplia gama de interfaces:

- Fibra óptica
- Tecnología Powerline Communications en Media Tensión (interfaces BPLC y SSPLC)
- Tecnologías celulares (GPRS/UMTS)
- Líneas ADSL

El DRA-2 incluye de base una interfaz serie de mantenimiento, 6 puertos Fast Ethernet y 2 bahías SFP Gigabit Ethernet.

Los puertos Fast Ethernet están usualmente dedicados a prestar servicio a los equipos presentes en el Centro de Transformación (CT), tales como concentradores de lectura de contadores PLC, unidades remotas de telecontrol, protecciones, localizadores de paso de falta, cámaras o teléfonos IP.

Las 2 bahías SFP Gigabit Ethernet posibilitan la inclusión del nodo de comunicaciones DRA-2 en topologías tipo anillo de Fibra Óptica o bien su utilización como uplink de alta capacidad.

El cliente debe completar el equipo seleccionado las distintas opciones de interfaz disponibles (véase apartado 1.3).

El DRA-2, además de la función de conmutación (L2), dispone de la capacidad de enrutado IPv4 (L3), lo que hace posible distintos escenarios de funcionamiento:

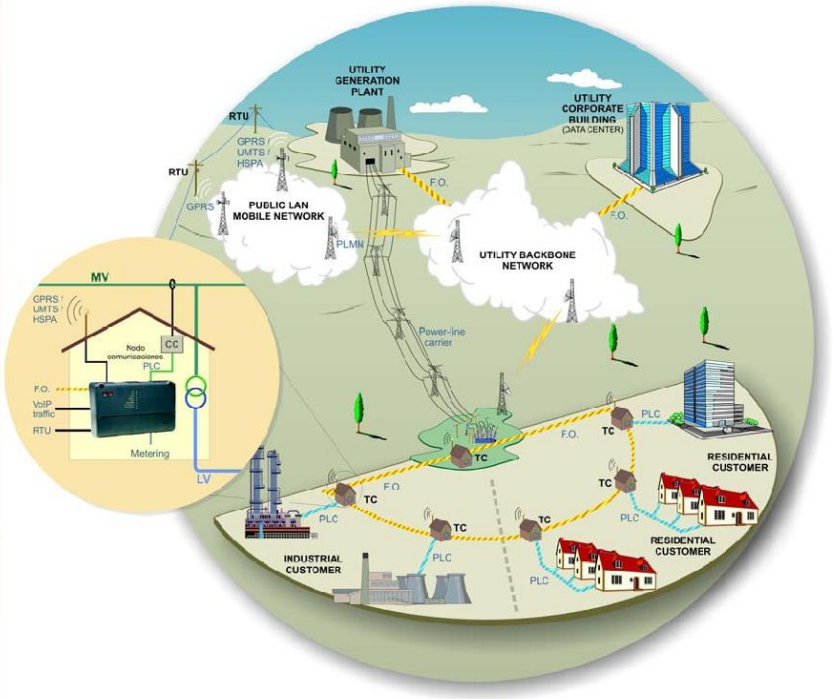
- Posibilidad de operación como conmutador para interfaces Ethernet, Gigabit Ethernet y PLC-MT (BPLC).
- Funcionalidad de enrutado entre dos o más VLANs configuradas, estando constituida cada VLAN por un conjunto de puertos locales (Ethernet / Gigabit Ethernet / BPLC) e interfaces WAN (GPRS / UMTS / ADSL).
- Utilización de interfaces WAN inalámbricas (GPRS / UMTS) como recurso de salvaguarda (backup) para la funcionalidad de enrutado descrita en el punto anterior.

Para las funciones de encaminamiento, el equipo soporta la utilización de información de encaminamiento estática (configurada por el usuario) y dinámica, para lo cual dispone de los protocolos de encaminamiento estándar RIP y OSPF.

El DRA-2 es gestionable de forma local y remota, bien mediante consola o a través de un servidor web incorporado, http o https, conexión SSH y Telnet.

El DRA-2 también soporta el protocolo SNMPv1 y SNMPv2c, así como otros protocolos y servicios como DHCP, NTP y TACACS+.

FIGURA 1 Solución DRA-2



1.3 INTERFACES DEL DRA-2

Un aspecto muy destacable del DRA-2 es su gran variedad de interfaces las cuales permite dar solución a las distintas topologías presentes en los Centros de Transformación. En algunos Centros de Transformación, la tecnología PLC-MT será la única viable, mientras que en otros podrá emplearse la fibra óptica o incluso el ADSL (PSTN). Además, en donde ninguna de las opciones ya mencionadas pueda proporcionar la suficiente comunicación, podrán utilizarse interfaces inalámbricas.

FIGURA 2 Constitución del nodo DRA-2

Las distintas interfaces, de base y opcionales, se integran en tres módulos principales, véase FIGURA 2, siendo éstos:

- **ALIMENTACIÓN, UNIDAD CENTRAL DE PROCESO E INTERFACES LAN DE BASE**.
  Es el módulo de base del DRA-2. Lleva a cabo, como Unidad Central de Proceso así como de adaptación y control de los periféricos, las funciones avanzadas de conmutación ethernet (L2), las funciones de encaminamiento, protocolos de acceso, control de flujo y congestión, y funciones avanzadas de gestión de tráfico.
  Incluye 6 puertos Fast Ethernet en configuración 10/100Base-Tx.
  Incluye también 2 receptáculos para transceptores SFP Gigabit Ethernet.
  La fuente de alimentación es parte del módulo base, existiendo dos versiones: la primera para su uso con tensión continua de 48 V_{CC}, mientras que la segunda admite el uso de tensión alterna y continua aunque, en este último caso, a partir de un rango de tensión superior a los 80 V_{CC}. Ambas versiones generan las tensiones internas de alimentación a partir de la tensión de entrada, y disponen de varios filtros a la entrada para protección. La fuente está protegida contra la inversión de polaridad.

CONSOLA DE SERVICIO Y OPCIÓN INTERFACES WAN (GPRS/UMTS/ADSL)

Este módulo dispone de un conector identificado como SRV, para el acceso al equipo mediante consola. Dicho conector siempre se incluye de base.

Puede incluir, además, interfaces WAN, debiendo seleccionar el usuario una de las opciones siguientes:

- 1 GPRS con 1 SIM y 1 conector SMA para antena
- 1 GPRS con 2 SIMs y 1 conector SMA para antena
- 2 GPRS con 2 SIMs y 2 conectores SMA para antenas
- 1 GPRS con 1 SIM y 1 conector SMA para antena + 1 ADSL (bajo demanda)
- 1 ADSL (bajo demanda)
- 1 GPRS con 1 SIM y 1 conector SMA para antena + 1 UMTS con 1 SIM y 1 conector SMA para antena (bajo demanda)
- 1 UMTS con 1 SIM y 1 conector SMA para antena + 1 ADSL (bajo demanda)
- 1 UMTS con 1 SIM y 1 conector SMA para antena
- 1 UMTS con 2 SIMs y 1 conector SMA para antena

OPCIÓN INTERFACES PLC-MT, LAN ADICIONALES u OTRAS

Este módulo puede estar preparado para distintos tipos de interfaz, debiendo seleccionar el usuario una de las opciones siguientes:

- 1 interfaz BPLC de alta velocidad
- 2 interfaces BPLC de alta velocidad
- 1 interfaz SSPLC de baja velocidad (en desarrollo)
- 2 interfaces SSPLC de baja velocidad (en desarrollo)
- 2 interfaces Fast Ethernet adicionales (100Base-Tx o 100Base-Fx) (en desarrollo)
- 1 interfaz serie RS-232 (en desarrollo) (no válido con 1 ADSL ó 2 PLC)
- 1 interfaz serie RS-485 (en desarrollo) (no válido con 1 ADSL ó 2 PLC)
- 1 interfaz serie óptico (en desarrollo) (no válido con 1 ADSL ó 2 PLC)
- 1 concentrador de lectura de contadores PLC (en desarrollo)

Las interfaces WAN permiten al usuario utilizar los servicios de los operadores públicos y son una alternativa muy interesante dada su cobertura geográfica y su facilidad de puesta en marcha.

El PLC de MT es una opción a la hora de transportar la información de los distintos Centros de Transformación hasta una Subestación Principal. Existen dos tipos de interfaces para las comunicaciones de Powerline Communications a través de la red de Media Tensión:

- Una de alta velocidad, interfaz BPLC, pensada en especial para entornos urbanos, donde se necesitan cubrir distancias de nivel medio ya que los centros de transformación están muy próximos entre ellos.

- Una de baja velocidad, interfaz SSPLC, que permite cubrir distancias mucho más largas y que está pensada para entornos rurales donde la cantidad de información a enviar es mucho más reducida y prima el que se puedan cubrir distancias más largas y acceder a lugares más recónditos.

Para poder insertar la señal de PLC en las redes de Media Tensión se utilizan acopladores de Banda Ancha adaptados a dicha tecnología, y a los diferentes lugares de instalación. La gama disponible se encuentra descrita en el *Apéndice C*.

1.4 ESPECIFICACIONES TÉCNICAS

1.4.1 Características del DRA-2 con funcionalidad de switch

- Detección automática de velocidad del puerto.
- STP y RSTP para resolución de bucles en la red y funcionamiento en anillos.
- Gestión de VLANs por puerto.
- Gestión de QoS por VLAN (802.1p).
- Limitación de tráficos Broadcast y Multicast (Broadcast Storm Control).
- Listas de control de acceso MAC y autentificación de usuarios 802.1x.
- Conmutación de nivel 2 entre el medio Ethernet y el medio PLC-MT en caso de disponer de interfaz BPLC de Media Tensión.

1.4.2 Características del DRA-2 con funcionalidad de router

- Capacidades de rutado, filtrado, NAT, firewall y túneles.
  - Hasta 6 túneles IPSec simultáneos con soporte DMVPN (Dynamic Multipoint VPN) y NHRP (Next Hop Resolution Protocol).
  - Protocolos de rutado RIP y OSPF.
  - Protocolo de redundancia VRRP.
- Asignación de calidades de servicio al tráfico entrante, y gestión de calidades de servicio a nivel de capa 3/4. Los niveles de gestión de prioridades son los siguientes:
  - Calidad por dirección IP origen y/o destino.
  - Calidad por tipo de tráfico (DSCP o TOS) y servicio (protocolo y puerto).
- Los modelos con 2 interfaces inalámbricas soportan el establecimiento de dos enlaces IP simultáneamente, con funcionamiento tanto de backup activo con conmutación rápida como de balanceo de carga.

1.4.3 Gestión del equipo

- Acceso remoto mediante servidor web seguro (https) o conexión SSH, SNMP, http y Telnet.
- En el modelo con interfaz inalámbrica es posible la gestión mediante llamada de datos.

1.4.4 Servicios adicionales

- Servidor y cliente DHCP
- Servidor y cliente NTP
- Cliente TACACS+

1.4.5 Accesorios

- Módulos SFP.
- Cables de antena.
- Antenas.
- Cables Ethernet.
- Pigtails fibra óptica.
- Coaxiales PLC.
- Acopladores PLC de Banda Ancha (véase *Apéndice C*).

1.4.6 Certificaciones

- CE.
- Diseñado para centros de transformación de la red eléctrica.
- Diseñado para aplicaciones industriales.

1.4.7 Interfaces del equipo

- Interfaces de base:
  - 6 puertos fast Ethernet en configuración 10/100BaseTx.
  - 2 puertos SFP Gigabit Ethernet.
  - 1 consola de servicio.
- Las interfaces proporcionadas por las opciones* disponibles:
  - GPRS/UMTS y ADSL (bajo demanda)
  - BPLC
  - SSPLC (en desarrollo)
  - Fast Ethernet (100Base-Tx o 100Base-Fx) (en desarrollo)
  - RS-232, RS-485, serie óptico (en desarrollo)

* *Véase detalle de las combinaciones permitidas en el apartado 1.3,interfaces del dra-2*

1.4.7.1 Características de la interfaz con GPRS

- Cuatribanda: 850/900/1800/1900MHz.
  - Class 4 (+33dBm ±2dB) for EGSM850
  - Class 4 (+33dBm ±2dB) for EGSM900
  - Class 1 (+30dBm ±2dB) for GSM1800
  - Class 1 (+30dBm ±2dB) for GSM1900

1.4.7.2 Características de la interfaz con UMTS

- UMTS/HSDPA: Dual band, 900/2100MHz
- GSM/GPRS/EDGE: Dual band, 900/1800MHz
  - Class 4 (+33dBm ±2dB) for EGSM900
  - Class 1 (+30dBm ±2dB) for GSM1800
  - Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK
  - Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK
  - Class 3 (+24dBm +1/-3dB) for UMTS 2100, WCDMA FDD BdI
  - Class 3 (+24dBm +1/-3dB) for UMTS 900,WCDMA FDD BdVIII

1.4.7.3 Características de la interfaz BPLC de MT (alta velocidad)

- Rango de frecuencias de 2 a 30 MHz.
- Velocidad de canal de 200 Mbit/s*.
- Velocidad máx. de usuario de 150 Mbit/s.
- Encriptación AES de 128 bits.
- Flexibilidad de supresión de determinadas frecuencias para evitar interferencias con otros servicios.
- Modulación OFDM de 1155 portadoras útiles.
- Modulación 1024/256/64/16/8 QAM, QPSK, BPSK, ROBO (Modulación básica/robusta DBPSK) – con aplicación independiente en cada portadora.
- Potencia de salida entre 1 y 10 W
- Alcance de hasta 1 km*.

* *Existe un compromiso entre la velocidad de transmisión, la distancia y la relación S/R necesaria en el receptor*

1.4.7.4 Características de la interfaz SSPLC de MT (alto alcance)

- Rango de frecuencias de 2 a 10 MHz.
- Velocidad de 128 kbit/s*.
- Modulación Direct-Sequence Spread Spectrum (DSSS).
- Potencia de salida entre 1 y 10 W
- Distancias del orden de 5 km*.

1.4.8 Características mecánicas

- Instalación mediante Carril DIN (EN 50022, BS 5584, DIN 46277-3)
- Dimensiones Altura: 140 mm; Anchura: 220 mm; Profundidad: 94 mm.
  Para más detalles mecánicos y eléctricos de los conectores, véase capítulo 2, *Características mecánicas y eléctricas*.
- Peso 1 Kg

1.4.9 Condiciones de funcionamiento

- Alimentación: 16-75 Vcc (48 Vcc nominal) ó multirango (80-360 Vcc, 80-260 Vca).
- Temperatura y humedad: de -20ºC a +70ºC y humedad relativa no superior al 95%, según CEI 721-3-3 clase 3K5 (climatograma 3K5).
- Consumo de potencia: 15 W máx.
- Seguridad eléctrica: según la norma EN 60950.
- Emisiones R.F.: según la norma EN 55022.
- Susceptibilidad a las descargas electrostáticas: según la norma UNE-EN 61000-4-2.
- Susceptibilidad a campos electromagnéticos permanentes de R.F.: según la norma UNE-EN 61000-4-3.

---

* *Existe un compromiso entre la velocidad de transmisión, la distancia y la relación S/R necesaria en el receptor*

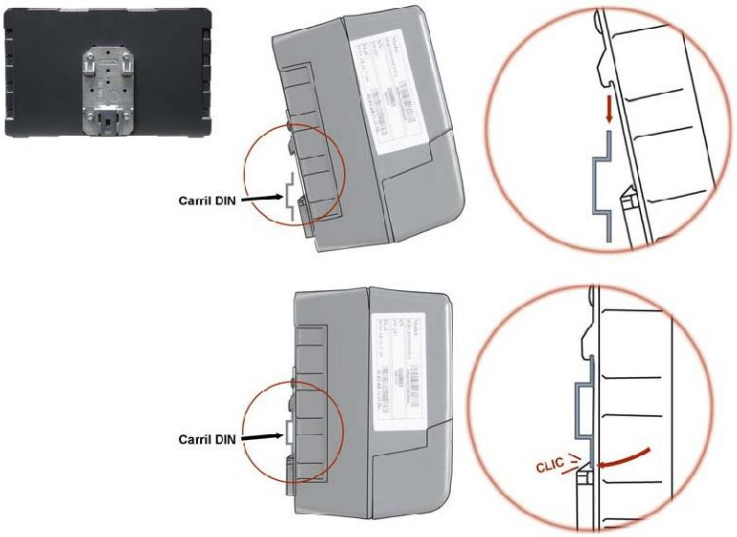
2 CARACTERÍSTICAS MECÁNICAS Y ELÉCTRICAS

Los distintos elementos que constituyen el nodo de comunicaciones DRA-2 están contenidos en una caja de plástico epoxy de alta resistencia, preparada para montaje en carril DIN.

Las dimensiones generales en mm del equipo se muestran en la FIGURA 3. En la parte inferior de la caja, se encuentra el elemento de fijación del equipo en carril DIN, véase FIGURA 4.

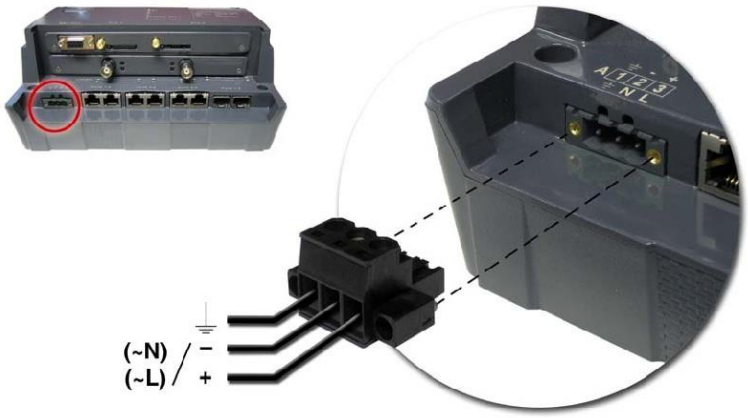
FIGURA 3 Dimensiones generales del equipo DRA-2

FIGURA 4 Detalle del elemento de fijación en carril DIN



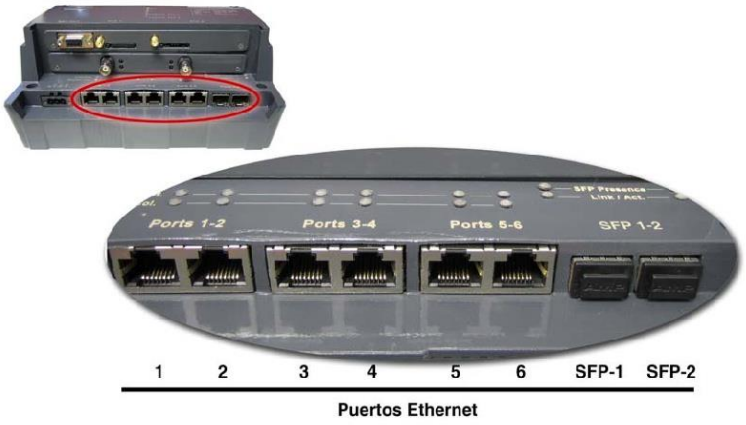
El DRA-2 se alimenta a una tensión nominal de 48 V_{CC} (el rango de tensión admitido es entre 16 y 75 V_{CC}) o a una tensión continua y alterna (80-360 Vcc, 80-260 Vca), a través del conector que se muestra en la FIGURA 5.

FIGURA 5 Conector de alimentación



De base, véase FIGURA 6, el equipo dispone de 6 puertos Fast Ethernet 10/100Base-Tx y de 2 puertos SFP Gigabit Ethernet cuyas bahías disponen de una tapón de protección.

FIGURA 6 Conectores Ethernet de base



El DRA-2 también dispone de un conector de mantenimiento, identificado como SRV, véase FIGURA 7, para el acceso al equipo mediante consola. Dicho conector está provisto de tapón de protección. Las características eléctricas del conector se indican a continuación.

	CONECTOR SRV
Tipo de interfaz	V.24/V.28 de la UIT-T (EIA RS-232)
Conector	DB9 hembra
Datos	Asíncronos
Velocidad	115200 bit/s
Protocolo	CLI (Consola de sistema)

FIGURA 7 Conector de mantenimiento

Conector de gestión del equipo mediante consola

Cuando el equipo está dotado con interfaces WAN (GPRS/UMTS), dispone de hasta dos conectores SMA para antena GSM/GRPS y hasta dos ranuras para alojamiento de tarjetas SIM, véase FIGURA 8. Ambas SIMs pueden estar activas simultáneamente con dos operadores distintos o bien puede utilizarse un funcionamiento *dual SIM*, es decir, una SIM como principal (*primary*) y la otra SIM como secundaria o back-up.

FIGURA 8 Detalle conector SMA para antena y ranura para alojamiento de tarjeta SIM de interfaz WAN (GPRS/UMTS)

Cuando el equipo está dotado con interfaces PLC-MT HPAV, véase FIGURA 9, dispone de hasta dos conectores BNC.

FIGURA 9 Detalle interfaces PLC-MT (BPLC)

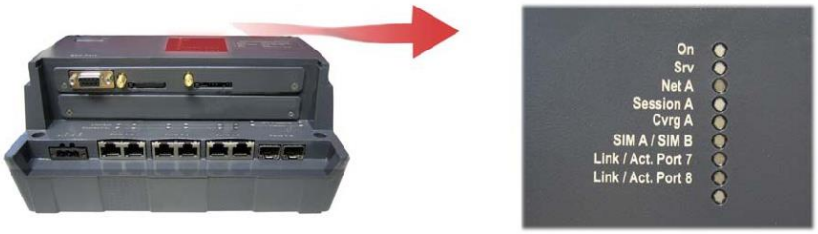
3 SEÑALIZACIÓN DE LOS LEDS

El equipo DRA-2 dispone en su parte frontal de dos LEDs de base y de varios LEDs específicos asociados a las interfaces WAN (GPRS/UMTS) y/o a las interfaces PLC-MT.

La FIGURA 10 muestra una vista del DRA-2 con interfaces WAN (GPRS/UMTS) como opción principal, mientras que la FIGURA 11 corresponde a un equipo DRA-2 con interfaces PLC-MT como opción principal.

El acceso a los LEDs asociados a las interfaces Ethernet de base es posible una vez se levanta la tapa de plástico. La FIGURA 12 muestra el detalle de dichos LEDs.

FIGURA 10 DRA-2 con interfaces WAN (GPRS/UMTS)



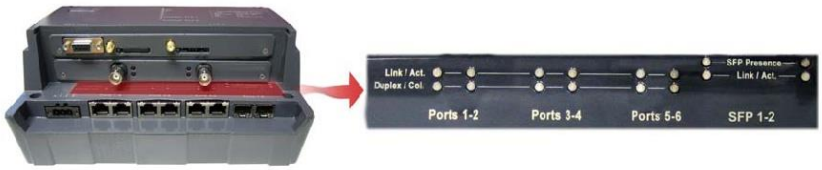
LED ON	Rojo. Se ilumina en permanencia cuando al equipo se le suministra tensión de alimentación externa.
LED Srv	Ámbar. Se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz serie de servicio SRV.

LED Net A	Verde. El comportamiento varía según el tipo de interfaz: **GPRS**: Se ilumina intermitentemente cuando la interfaz inalámbrica se ha registrado en la red del operador. **UMTS**: Se ilumina en permanencia cuando la interfaz inalámbrica se ha registrado en la red del operador.
LED Session A	Ámbar. Se ilumina en permanencia cuando para la interfaz inalámbrica (GPRS/UMTS) designada como 1 se ha establecido la sesión con el operador.
LED Cvrg A	Tricolor. Se ilumina en permanencia indicando el nivel de cobertura. **Verde**: la cobertura de señal es buena. **Ámbar**: la cobertura de señal es media. **Rojo**: la cobertura es insuficiente.
LED SIM A / SIM B	Bicolor. Se ilumina en permanencia indicando cual de las dos SIMs está en uso. **Verde**: la SIM A está en uso. **Rojo**: la SIM B está en uso.
LED Link / Act Port 7	Verde. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz PLC 1.
LED Link / Act Port 8	Verde. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz PLC 2.

FIGURA 11 DRA-2 con interfaces PLC-MT (BPLC)

LED PLC Act.	Verde. Iluminado en permanencia indica que la interfaz PLC opera en modo Maestro. Cuando la interfaz opera en modo esclavo, muestra la actividad sobre la interfaz. Mientras el dispositivo se está inicializando, parpadea al mismo ritmo que el LED PLC State. Si la interfaz se encuentra inhabilitada (dispositivo en power down), permanece apagado.
LED PLC State	Ámbar. Iluminado en permanencia señala que el dispositivo PLC funciona correctamente. Parpadea con una cadencia del 50% cuando el dispositivo se está inicializando, y se ilumina brevemente de forma intermitente cuando la interfaz está inhabilitada (dispositivo en power down).

FIGURA 12 LEDs asociados a las interfaces Ethernet de base



LED Link/Act.	Bicolor. Existe un LED por interfaz. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz. Se ilumina en verde a 100 Mbit/s y en ámbar a 10 Mbit/s.
LED Duplex/Col.	Ámbar. Existe un LED por interfaz 10/100Base-Tx. Se ilumina en permanencia cuando la transmisión es Full-duplex, y permanece apagado cuando la transmisión es Half-duplex. Se ilumina intermitente en caso de colisión.
LED SFP Presence	Ámbar. Existe un LED por interfaz SFP Gigabit Ethernet. Se ilumina en permanencia cuando en el receptáculo físico se encuentra instalado un transceptor SFP.

4 ACCESO AL EQUIPO

El DRA-2 es gestionable de forma local y remota, bien mediante consola o a través de un servidor web incorporado, el servidor opera con protocolo http y/o https.

4.1 CONSOLA

El equipo proporciona una aplicación de consola de usuario, denominada *CLI (*véase *Apéndice B*), accesible a través del conector SRV, un conector DB9 estándar, hembra, en modo DCE, y que opera a 115200 bit/s, con caracteres de 8 bits, sin paridad y con un bit de stop.

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

La consola de usuario, en función de la identidad del mismo, proporciona el acceso completo a la totalidad de los datos de configuración del equipo.

La consola dispone de una pequeña ayuda en relación a los comandos disponibles y que se obtiene ejecutando el comando ***help***.

Los datos se agrupan de forma virtual en directorios y subdirectorios. La navegación en los directorios se lleva a cabo con el comando ***cd*** (***change directory***). El valor de un dato o de un grupo de ellos se obtiene como respuesta a un comando ***get***, al que se le puede indicar el dato de forma concreta, o bien devuelve el valor de todos aquellos datos ubicados en el directorio y subdirectorios actuales. Para establecer un nuevo valor, se debe ejecutar el comando ***set***, indicando el parámetro a modificar y a continuación el valor deseado; en el caso en que no se proporcione el valor a configurar, el sistema lo solicita de forma explícita.

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, si no 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 salvaguardar 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.

También es posible obtener acceso a la consola de forma remota mediante conexión SSH y Telnet.

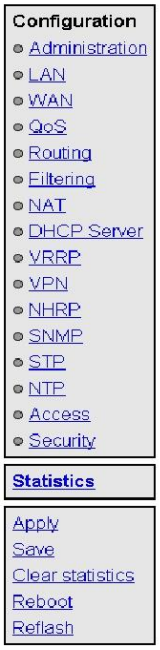
4.2 SERVIDOR HTTP

El servidor HTTP incluido proporciona el acceso a las páginas HTML que ofrecen el acceso a la totalidad de los datos de configuración.

Los procedimientos para la efectiva configuración de los parámetros son idénticos, es decir, es necesario ejecutar el comando ***Apply*** y/o el comando ***Save***, según lo indicado en el caso de uso de la consola, si bien con anterioridad a cualquiera de los mismos es necesario haber indicado al sistema que se han modificado datos, con el comando ***Send*** (botón presente en todas la páginas HTML).

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. En la FIGURA 13 se muestran los comandos indicados.

FIGURA 13 Árbol de menús de páginas HTML



Para el detalle de los comando ***Reboot*** y ***Reflash***, véanse respectivamente los apartados 5.18 y 5.19.

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

En las página HTML, los comandos para la adición y la eliminación de elementos en los datos tabulares se muestran de forma explícita en forma de botones, etiquetados como *Add* y *Delete*, localizados en cada uno de los objetos que los emplean.

> La dirección IP del equipo de fábrica es 192.168.0.1, de modo que es posible el acceso al servidor HTTP para la configuración del mismo desde el instante inicial (véase capítulo 5).
>
> Debe tenerse en cuenta que en caso de modificar la dirección IP será necesario modificar de forma acorde la dirección IP del equipo cliente.

5 CONFIGURACIÓN Y GESTIÓN

La configuración y la gestión del DRA-2 se puede llevar a cabo tanto mediante la consola como mediante al 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.

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.

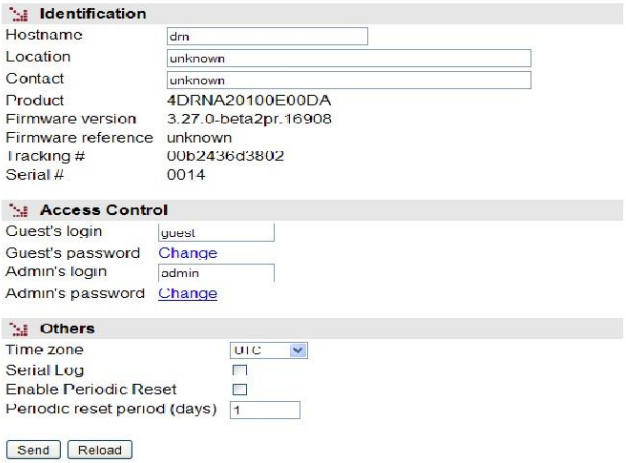
5.1 PARÁMETROS GENERALES

Los parámetros generales se agrupan en la primera página, véase FIGURA 14, que se muestra una vez el DRA-2 valida la identidad del usuario.

Además de los parámetros de configuración, los cuales se detallarán en los apartados siguientes, como puede apreciarse en la figura, el sistema proporciona información sobre el software, es decir, versión en ejecución, y el hardware del equipo, es decir, número de serie y de seguimiento (*tracking*).

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

FIGURA 14 Página HTML principal



5.1.1 Identificación del equipo

La zona de identificación incluye tres parámetros, 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 caracter.

El ***hostname*** se usa de forma automática como valor de prompt en la consola.

Los parámetros de identificación coinciden con los asignados con el mismo nombre en los datos SNMP.

5.1.2 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 tienen acceso a la totalidad de los datos de configuración del sistema.

Tal y como se resume en la TABLA 1, 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 1 Claves de acceso por defecto del sistema

	Nombre de usuario (*login*)	**Contraseña (*password*)**
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.

5.1.3 Otros

En esta sección, existen cuatro parámetros. El primero de ellos 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***.

5.2 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 15 Menú *Administration*

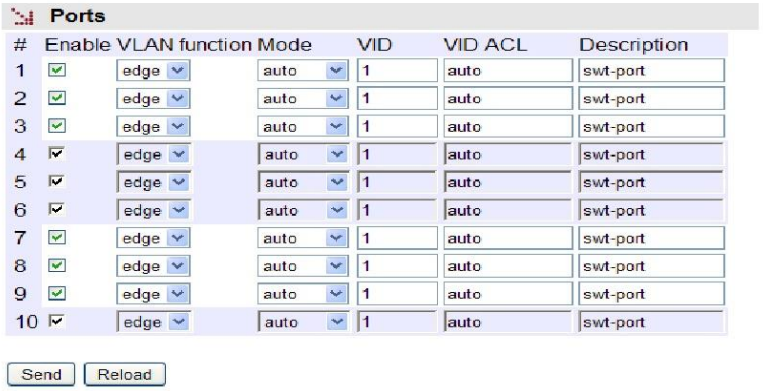
5.3 CONFIGURACIÓN LAN

Este menú contiene tres submenús: *Puertos*, *VLAN* y *PLC,* cuya funcionalidad se describe a continuación.

5.3.1 Puertos

En este submenú se lleva a cabo la configuración de los parámetros de funcionamiento de los puertos Ethernet del equipo, y la de los dos puertos asociados a las interfaces BPLC cuando las mismas están presentes, así como la asignación de cada uno de los puertos a alguna de las VLAN definidas en el equipo (véase previamente apartado 5.3.2).

FIGURA 16 Submenú *Puertos* del menú *LAN*



El número de puertos que muestra el submenú depende del número real de puertos con los que el equipo esté dotado. Con independencia del mismo, los dos últimos puertos siempre son los asociados a las interfaces SFP Gigabit Ethernet, tal y como se verá a continuación en la descripción del parámetro #.

En cuanto a operativa de nivel 2, los puertos BPLC son vistos por el equipo, a todos los efectos, mediante los puertos asociados correspondientes (puertos 7 y 8 en parámetro #).

Los parámetros de configuración son:

- **#.** Relaciona los puertos presentes en el equipo. Para las interfaces 10/100BaseTx, los números coinciden con la identificación de los conectores. Con independencia del número final, los dos últimos puertos siempre son los asociados a los puertos SFP Gigabit Ethernet lo que, dependiendo de la presencia de dispositivos, puede corresponder a los puertos 7 y 8 (sin BPLC) ó a los puertos 9 y 10 (con 2 BPLC), en este último caso, los puertos 7 y 8 están asociados a las dos interfaces BPLC.

- **Enable**. Permite habilitar y deshabilitar individualmente cada puerto marcando o desmarcando, respectivamente, la casilla *Enable* correspondiente.

- **VLAN funtion.** Especifica el formato de datagrama 802.1q (edge o trunk) que se empleará para la transmisión en el puerto.
  Edge: Las tramas 802.1 se transmitirán con el mismo formato que tenían en el momento de ser aceptadas por el equipo, con o sin tag.

Trunk: Todas las tramas se transmiten siempre con tag. Es el modo específico para la conexión con otros equipos de conmutación cuando se desea que la información 802.1Q tenga carácter global.

- **Mode.** Especifica el tipo de funcionamiento del puerto LAN en cuanto a velocidad y modo de operación. Los parámetros de funcionamiento de los puertos PLC se establece en el submenú PLC.
  Auto (autonegociación): Recomendado y valor por defecto.
  10fdx: 10 Mbit/s Full-duplex.
  100fdx: 100 Mbit/s Full-duplex.
  10hdx: 10 Mbit/s Half-duplex.
  100hdx: 100 Mbit/s Half-duplex.

> Si se configura un modo de operación distinto de **Auto**, para el correcto funcionamiento, es imprescindible que ambos extremos del enlace estén configurados de forma idéntica.

- **VID.** Indica la VLAN en la que está incluido el puerto. La asignación se lleva a cabo desde el submenú VLAN.
- **VID ACL (Access control list).** Este parámetro actúa como un filtro en cuanto a los paquetes que se aceptarán a nivel de Puerto. Únicamente los paquetes con un identificador de VLAN incluida en la lista serán procesados, tanto en transmisión como en recepción. Todos los paquetes disponen de un identificador VLAN, bien por que ya estaba incluido en el momento de ser recibidos (tagged frames) bien por que le fue asignado por el puerto de entrada en el momento de la recepción, siendo en este último caso el parámetro **VID** asignado al puerto. El valor especial **any** significa que el filtro no está activo.
- **Description.** Campo descriptivo a disposición del usuario como mnemotécnico.

5.3.2 VLAN

Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión, zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local. Es decir, una VLAN es una red con agrupamientos lógicos independientes del nivel físico.

Cada VLAN se distingue del resto gracias a un identificador específico, denominado usualmente como VLAN tag, y especificado en el estándar IEEE 802.1q. El tag permite que

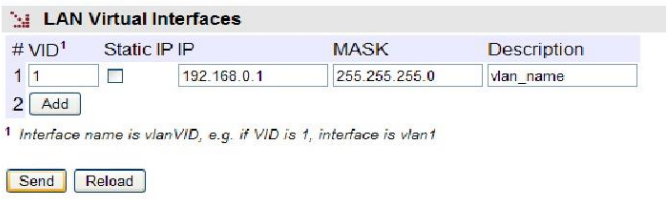
varias VLAN puedan compartir recursos, bien sean éstos equipos de conmutación, como el DRA-2, o enlaces entre equipos de conmutación, con la garantía que los tráficos de cada una de las VLAN llegarán al destino adecuado.

El hecho de que a nivel de equipo la definición de las VLAN, así como la asignación de los puertos a cada una de ellas, se realice por parámetros de configuración, supone una gran flexibilidad, ya que es posible alterar la topología de la(s) VLAN sin necesidad de realizar cambios en la infraestructura.

El intercambio de paquetes entre equipos pertenecientes a distintas VLAN únicamente puede llevarse a cabo a nivel de encaminamiento (L3). El DRA-2 tiene la capacidad para realizar esta función entre las distintas VLAN que se hayan definido en el equipo, con lo que el tráfico entre ellas admite más opciones de control.

La dirección IP principal y su máscara pueden obtenerse de forma automática mediante el cliente DHCP, lo que se denomina configuración dinámica o NO estática. El usuario puede activar esta prestación a través del control tipo *Checkbox* con la etiqueta ***Static IP***. Cuando el control está marcado, el equipo usa los datos proporcionados por el usuario.

FIGURA 17 Submenú *VLAN* del menú *LAN*



5.3.3 PLC

Este submenú se muestra cuando el equipo dispone de interfaces PLC. Permite configurar los parámetros de funcionamiento de los puertos PLC del equipo cuyos conectores están identificados como *PLC 1 y PLC 2*.

El paradigma de operación de las interfaces PLC es del tipo *Maestro-Esclavo*, aunque no por ello la comunicación está restringida a topologías punto a punto, ya que un mismo *Maestro* admite múltiples *Esclavos*. Por otro lado, está contemplada la posibilidad de que varias comunicaciones PLC coexistan, bien por compartición de un mismo medio, o bien por actuar como señales interferentes.

El mecanismo para garantizar la exclusión entre varias comunicaciones PLC es el uso de claves distintas para cada una de ellas, las cuales además se usan para el cifrado de

datos, por lo que se garantiza la privacidad. Está clave identificativa se denomina **Network Management Key (NMK)**, y es compartida por todos los equipos de un mismo grupo. Cada NMK está constituida por una secuencia de 16 bytes.

Cada una de las interfaces PLC debe disponer de una NMK asignada, y en condiciones normales, distinta entre ellas. De todos modos, están previstas configuraciones especiales de las interfaces, con la finalidad de que éstas sean operativas sin necesidad de que el usuario tenga que configurarlas a priori. Por ejemplo, es posible tener una configuración base de los equipos aún desconociendo la ubicación exacta de los mismos.

Estos modos específicos se traducen en la presencia de parámetros de configuración adicionales a la propia NMK y que son el **grupo de NMKs (GNMK)** y el **Modo de operación**.

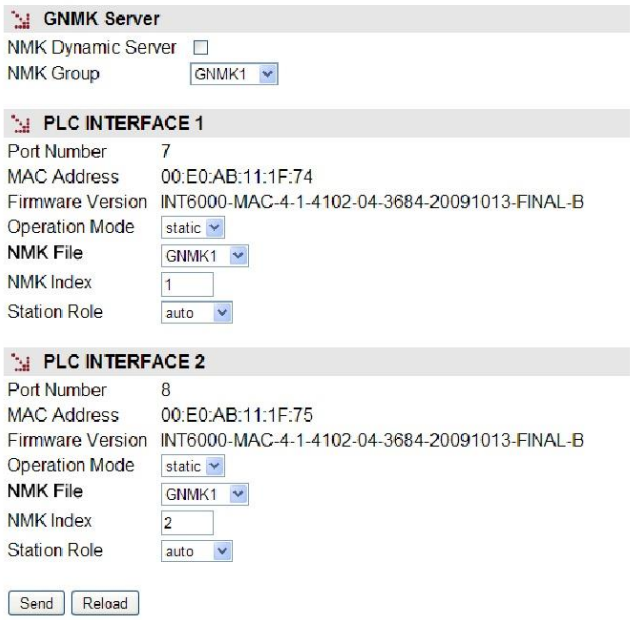
Cada uno de los 10 GNMK disponible incluye múltiples NMKs. El equipo está preparado para recorrer de forma cíclica el GNMK asignado a una interfaz hasta detectar el establecimiento de una conexión exitosa (modo **AUTO**), y también permite actuar como el extremo que acepta las conexiones (modo **ASK**), en cuyo caso, la NMK se obtiene por consulta a un servidor que las gestiona, y que puede ser habilitado en el propio equipo.

Las interfaces PLC en modo **AUTO** intentan siempre establecer la conexión con el último valor de NMK exitoso.

Únicamente debe habilitarse un **servidor GNMK** para la totalidad de los equipos que operen dentro del **mismo grupo GNMK**.

También es posible usar una configuración estática (modo **STATIC**) en el que se fija el NMK de cada interfaz PLC de forma directa, siendo entonces responsabilidad del usuario la correcta configuración del mismo en todos los equipos que se desee interconectar. En este último caso es cuando tiene sentido el parámetro **Station Role**.

FIGURA 18 Submenú *PLC* del menú *LAN*



Los parámetros de configuración son:

- **NMK Dynamic Server**. Habilita el servidor de claves NMK.
- **NMK Group**. Identificador del grupo de NMKs con el que operará la interfaz, seleccionable de la lista desplegable.
- **Operation Mode.** Establece el modo en que el equipo obtendrá la NMK para la interfaz.
  AUTO: El equipo desconoce la NMK asignada al enlace al que está conectado, de modo que ejecuta pruebas automáticas de conexión con cada una de las NMK incluidas en el GNMK configurado. En este modo, el rol de la interfaz PLC es siempre **Station (esclavo)**.
  ASK: La interfaz usa una NMK específica obtenida por consulta al servidor GNMK Server. En este modo, el rol de la interfaz PLC es siempre **CCo (maestro)**.
  STATIC: La NMK en uso es la indicada por el usuario en el cuadro de selección.

- **NMK Index.** Selecciona un NMK dentro del grupo asignado. Se emplea un índice en lugar de la propia clave de modo que, por un lado, se evitan errores en la introducción y, por otro lado, se mantiene su privacidad.
- **Station Role.** Establece el comportamiento de la interfaz en cuanto al paradigma *Maestro-Esclavo*. Los valores admisibles son: **Auto**, **Station (esclavo)** y **CCo (maestro)**. Únicamente tiene sentido cuando el modo de operación (Operation Mode) es **STATIC**.

> En modo **Auto**, la elección del **CCo (maestro)** se realiza de forma automática entre todos los equipos que comparten una misma NMK, inclusive la resolución en caso de que el equipo elegido dejase de ser operativo.
>
> Cuando se fijan los roles, es **IMPRESCINDIBLE** garantizar que existe **UN único equipo configurado con el rol de CCo (maestro) de forma estática**. En caso de que todos los equipos estuviesen configurados de forma estática con rol Station (esclavo) y ninguno como Auto ó CCo (maestro), el medio PLC estaría indisponible.
>
> Pueden coexistir equipos con roles en modo dinámico y estático, **siempre y cuando** se cumpla la condición anterior.

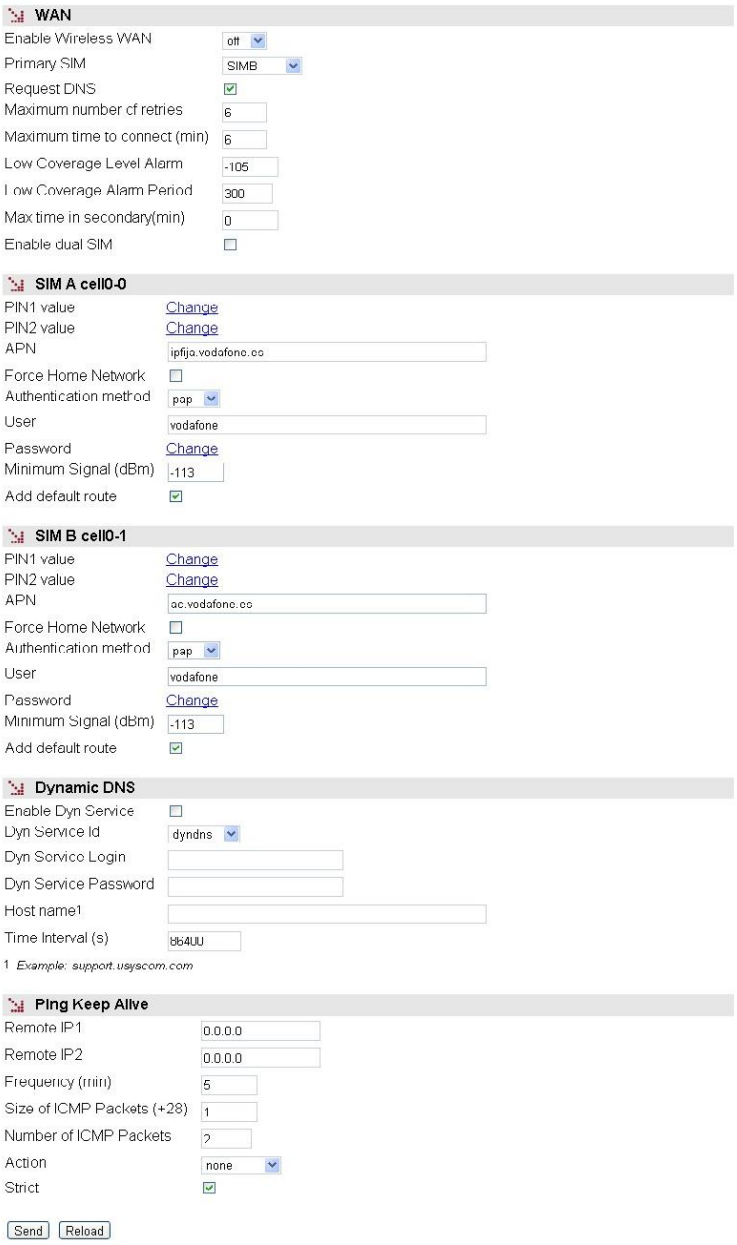
5.4 CONFIGURACIÓN WAN

Este menú se muestra cuando el equipo dispone de interfaces WAN (GPRS/UMTS). Contiene dos submenús: *Cell0* y *Tunnel,* cuya funcionalidad se describe a continuación.

5.4.1 Configuración Cell0

En este submenú se configuran los datos de la interfaz inalámbrica. El submenú presenta cuatro apartados bien diferenciados, los cuales se describen a continuación.

FIGURA 19 Submenú *Cell0* del menú *WAN*



WAN:

- **Enable Wireless WAN.** Permite habilitar y deshabilitar la interfaz o interfaces WAN del equipo seleccionado ON y OFF, respectivamente.
  La selección de la opción **ON** implica que el equipo intente una nueva sesión GPRS/UMTS/HSDPA de acuerdo a los datos de la subscripción (PIN, APN, Authentication method, user, password). En caso de funcionalidad **dual SIM** (doble SIM) los datos de la subscripción serán los correspondientes a la SIM primaria (*primary* SIM).
  La selección de la opción **VRRP** determina que el comportamiento de la interfaz estará condicionado al funcionamiento VRRP, habilitándose por consiguiente una vez el equipo al que pertenece pasa a ser el router maestro.

  La opción **OFF,** deshabilitación de la interfaz WAN, es la opción por defecto. No olvidar, por tanto, habilitar esta opción si se desea el servicio GPRS/UMTS, habiendo configurado PREVIAMENTE los parámetros necesarios para el establecimiento de la sesión con operador.

- **Primary SIM**. En caso de funcionalidad **dual SIM** (doble SIM), permite establecer cual de las dos SIMs disponibles va a actuar como principal: SIMA ó SIMB. En este modo de funcionamiento, la SIM que no se selecciona es, por tanto, la secundaria o de back-up.

- **Request DNS.** Seleccionado esta casilla, el equipo requerirá direcciones para servidores DNS cuando se conecte al servicio GPRS/UMTS.

- **Maximum number of retries.** Especifica el número de intentos (3 a 10) que se podrán llevar a cabo para conseguir establecer la sesión con el operador. Si se agota el número de intentos, el equipo se inicializará.
  En caso de funcionalidad **dual SIM** (doble SIM), especifica el número de intentos de establecimiento de sesión con el operador del servicio GPRS/UMTS de la SIM principal (*primary*). Una vez alcanzado el número de intentos, el equipo intentará la conexión utilizando la SIM secundaria. En caso de que no fuera posible la conexión o la SIM secundaria estuviera deshabilitada, el equipo se inicializaría.

- **Maximum time to connect (minutes)**. Especifica el tiempo en minutos (3 a 20) que el equipo esperará para conseguir la dirección IP WAN del operador. Si, transcurrido el tiempo, no se ha conseguido una IP WAN, el equipo se inicializará.
  En caso de funcionalidad **dual SIM** (doble SIM), especifica el tiempo máximo que el equipo intentará la conexión con el servicio GPRS/UMTS de la SIM principal (*primary*). Una vez alcanzado el tiempo, el equipo intentará la conexión utilizando

la SIM secundaria. En caso de que no fuera posible la conexión o la SIM secundaria estuviera deshabilitada, el equipo se inicializaría.

- **Max time in secondary (minutes)**. Este parámetro está asociado a la funcionalidad **dual SIM** (doble SIM). Permite limitar el tiempo en que el equipo estará conectado a la SIM secundaria. Transcurrido el tiempo, el equipo intentará nuevamente conectarse a la SIM principal (*primary*). El tiempo máximo admitido es de 1440 minutos.
- **Enable dual SIM.** Seleccionando esta casilla se determina si el equipo hará uso del SIM secundario o no.

SIM A cell0-0 y SIM B cell0-1:

- **PIN 1 and PIN 2 values.** Son los códigos de seguridad asociados a la tarjeta SIM. Normalmente es suficiente el PIN1 para el acceso a los servicios generales proporcionados por el operador. Comprobar que el código introducido es correcto. Un código equivocado, bloqueará la tarjeta SIM.
- **Preferred network. Únicamente para interfaz UMTS**. Permite especificar el comportamiento del equipo en caso de falta de cobertura UMTS/HSDPA. Seleccionando **UMTS**, el equipo siempre debe intentar conectarse a una red UMTS/HSDPA. Esta opción, por tanto, implicará la desconexión del equipo a falta de cobertura UMTS/HSDPA. Seleccionando **UMTS/GPRS**, el equipo intentará conectarse a una red UMTS/HSDPA pero, a falta de cobertura UMTS/HSDPA se conectará a una red GPRS. En esta opción, el equipo siempre estará monitorizando la cobertura de la red UMTS/HSDPA y, tan pronto como la red UMTS vuelva a estar disponible, conmutará de una red GPRS a una red UMTS/HSDPA.
- **APN.** Establece la identidad del punto de acceso del operador.
- **Force Home Network.** Seleccionando esta casilla se fuerza la conexión con el operador de red local asociado a la tarjeta SIM (home network). Con esta opción seleccionada, el equipo no podrá conectarse a ningún otro operador que no sea el especificado.
- **Authentication method.** Deberá seleccionarse el método de autentificación a emplear durante el establecimiento de la sesión PPP. Los valores posibles son None, PAP y CHAP.

- **User Name.** Usuario establecido por el operador para la identificación durante el proceso de autentificación (punto anterior).
- **Password.** Contraseña establecida por el operador para validar el usuario del punto anterior. El password no se muestra por razones de seguridad, por lo que cuando se modifica (opción **Change**) debe ser introducido por duplicado.
- **Minimum Signal (dBm).** Este parámetro permite especificar un nivel de cobertura mínimo (en dBm) como parámetro de calidad para la conexión WAN. Cuando el nivel de cobertura esté por debajo de este valor, el equipo no intentará establecer la sesión con el operador y permanecerá desconectado. Los valores por defecto son -113 dBm (0%, no cobertura) y -51 dBm (100%, cobertura).

Dynamic DNS:

Un servicio DNS dinámico permite asignar un nombre DNS a un equipo con una dirección IP no permanente, siendo responsabilidad del cliente Dynamic DNS la actualización de la misma cuando cambia. De este modo, desde el punto de vista del usuario, el equipo siempre es accesible vía un nombre DNS, por lo que no es necesario conocer en cada momento la dirección IP asignada.

El cliente Dynamic DNS se encarga de conectarse al servidor elegido y actualizar la dirección IP.

> Para la utilización del cliente Dynamic DNS es necesario que el usuario haya registrado previamente el nombre DNS del equipo en el proveedor del servicio. El cliente únicamente puede actualizar la dirección IP.

Los parámetros son los siguientes:

- **Enable Dyn Service.** Habilita la ejecución del cliente Dynamic DNS.
- **Dyn Service Id.** Permite seleccionar uno de los proveedores de servicio dinámico DNS soportados.
- **Login y Password.** Establece el nombre de usuario (login) y la contraseña (password) para acceder al proveedor del servicio.
- **Host name.** Nombre del equipo registrado en el proveedor del servicio, es decir, el nombre del equipo que vía DNS identifica al equipo DRA-2.
- **Time interval (seconds).** Tiempo entre accesos para la actualización de la dirección IP por parte del cliente Dynamic DNS.

Ping Keep Alive:
Es una facilidad para verificar el estado de las interfaces WAN.

- **Remote IP1 y Remote IP2.** Establece las direcciones IP de los equipos con los que se comprobará la accesibilidad, mediante el envío de paquetes ICMP (ping). Si los campos están a 0.0.0.0 significa que la función "Ping Test" está deshabilitada. Es suficiente que uno cualquiera de los equipos remotos responda para dar por válido el test de accesibilidad. Un campo con valor 0.0.0.0 significa que la opción no está habilitada.

- **Frequency (minutes).** Permite especificar el tiempo que transcurre entre envío de paquetes ICMP (ping).

- **Size of ICMP packets.** Permite especificar el tamaño del paquete ICMP. La configuración consiste en indicar los bytes extra que se añadirán al paquete ICMP mínimo el cual, por defecto, es de 28 bytes.

- **Number of ICMP packets.** Permite especificar el número de paquetes ICMP que se envían en cada verificación.

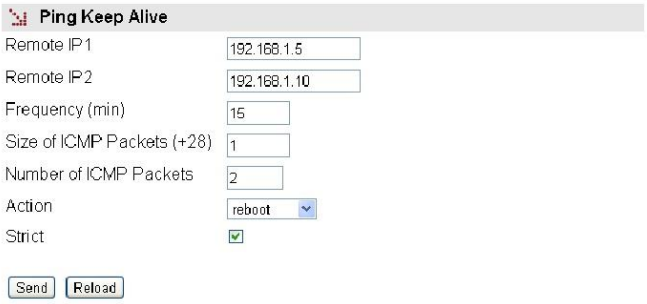
- **Action.** Establece el comportamiento deseado del equipo cuando el test de accesibilidad falla. Las opciones son: **None** (no realizar ninguna acción), **Reconnect** (establecer una nueva sesión GPRS/UMTS) ó **Reboot** (inicializar el equipo).

- **Strict.** Está opción permite inhibir el test de accesibilidad en presencia de tráfico. Cuando la opción no está activada únicamente se ejecutará el test cuando haya transcurrido el periodo de tiempo indicado en **frequency** sin tráfico. Cuando la opción está habilitada, el test se realizará de forma incondicional a la presencia de tráfico.

En la figura de ejemplo de configuración Ping Keep Alive, cada **15** minutos se verifica la conectividad de las direcciones IP 192.168.1.5 y 192.168.1.10 mediante el envío de **2** paquetes ICMP de 29 bytes (28+**1**). De no haber respuesta al "Ping Test", se llevará a cabo la inicialización (**reboot**) del equipo.

> Para evitar que se produzcan fallos de "Ping Test" causados por la recepción simultánea de tráfico, el equipo verificará, durante los 30 segundos previos a la función de "Ping Test", la actividad a través de la interfaz WAN. De detectar la recepción de tráfico, no llevará a cabo la función de "Ping Test".

FIGURA 20 Ejemplo de configuración Ping Keep Alive



5.4.2 Configuración túneles

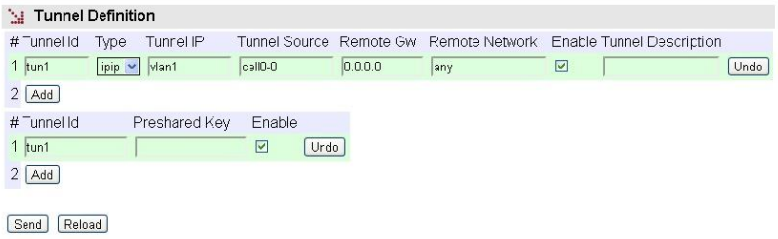
Un túnel puede definirse como una conexión virtual que emula una conexión punto a punto entre dos nodos conectados a través de una red compleja, bien sea pública como Internet, o privada.

Para configurar un túnel, básicamente, es necesario definir los puntos de inicio y fin del túnel, y el tráfico que se va a enviar a través del mismo.

Existen dos tipos de túneles no seguros (sin cifrado): IPIP y GRE. La diferencia entre ellos es que los túneles IPIP únicamente pueden encapsular tráfico IPv4unicast, mientras que los túneles GRE admiten tráfico tipo multicast.

Para brindar privacidad y seguridad, puede llevarse a cabo la encriptación de los datos que circulan sobre el túnel mediante el protocolo de cifrado IPSec. Su configuración es posible desde el menú *VPN*.

FIGURA 21 Submenú *Tunnel* del menú *WAN*



Los parámetros de configuración son:

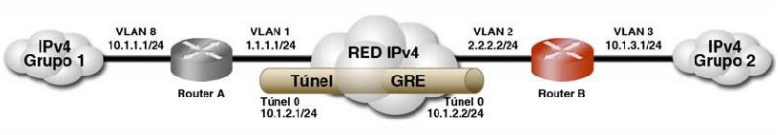
- **Tunnel ID.** Establece el nombre del dispositivo virtual tipo túnel.
- **Type.** Establece el tipo de túnel que se desea, GRE o IPIP.
- **Tunnel IP**. Establece la dirección IP asociada al dispositivo virtual túnel, cuya identidad es el valor del parámetro **Tunnel ID**. La dirección debe ser necesariamente de host, aunque admite también la inclusión de la máscara de red asociada, aunque también admite su configuración de forma indirecta mediante el uso del identificador de un dispositivo del equipo, en cuyo caso se asigna la dirección IP configurada en esta interfaz con una máscara de host.
- **Tunnel Source**. Establece la interfaz local a través de la cual se enviará el tráfico del túnel. En el caso de las interfaces WAN (GPRS/UMTS) puede ser *cell0-0* (identifica a la SIM A) o *cell0-1* (identifica a la SIM B). Sino, será un identificador de interfaz virtual de una de las VLAN existentes en el equipo.
- **Remote GW**. Establece la dirección IP del equipo en el extremo opuesto del túnel, es decir, el terminador.
- **Remote network**. Subred remota conectada al punto de fin del túnel (Remote GW) cuyo tráfico pasa por el túnel. Seleccionando *any* todo el tráfico que no es accesible localmente o por reglas específicas se envía por el túnel.
- **Enable.** Permite habilitar y deshabilitar un túnel marcando y desmarcando, respectivamente, la casilla *Enable* correspondiente.
- **Tunnel description.** Campo descriptivo que permite indicar datos sobre el túnel, como por ejemplo su utilidad.
- **Preshared key.** Clave que se intercambia entre los equipos extremos del túnel para el establecimiento del mismo. Ha de configurarse en ambos terminadores (Tunnel IP y Remote GW). Para que sea efectivo, debe marcarse la casilla *Enable* asociada.

Ejemplo:

A continuación se muestra un ejemplo que permite identificar los distintos parámetros mencionado con valores concretos. El túnel GRE se establece entre los routers denominados Router A y Router B, conectados a través de una red IPv4, pudiendo ser perfectamente que la conexión sea Internet.

Los routers A y B encaminan el tráfico entre los equipos pertenecientes al Grupo 1 y al Grupo 2 como si ambos routers tuvieran conexión directa entre ellos, ya que los dos tienen una dirección de red IP en el mismo segmento, 10.1.2.1 y 10.1.2.2 respectivamente, que son las direcciones IP asignadas localmente en cada extremo del túnel, y lo hacen de forma transparente sobre la red IPv4.

FIGURA 22 Ejemplo de configuración de túnel



En el router A, la configuración sería:

- **Tunnel ID.** Tunnel0.
- **Type.** GRE
- **Tunnel IP**. 10.1.2.1/24 (dirección IP del dispositivo virtual Tunnel0).
- **Tunnel Source**. vlan1 (Interfaz local en el que esté configurada la dirección local 1.1.1.1/24).
- **Remote GW**. 2.2.2.2/24 (dirección del terminador del túnel).
- **Remote network**. 10.1.3.0/24 (red IP ubicada en el extremo remoto del túnel).

En el router B, la configuración sería:

- **Tunnel ID.** Tunnel0.
- **Type.** GRE
- **Tunnel IP**. 10.1.2.2/24 (dirección IP del dispositivo virtual Tunnel0).
- **Tunnel Source**. vlan2 (Interfaz local en el que esté configurada la dirección local 2.2.2.2/24).
- **Remote GW**. 1.1.1.1/24 (dirección del terminador del túnel).
- **Remote network**. 10.1.1.0/24 (red IP ubicada en el extremo remoto del túnel).

5.5 CONFIGURACIÓN QoS

La calidad de servicio (QoS) permite la clasificación y política de servicio para el tráfico, estableciendo las condiciones en que será tratado por parte del equipo.

El equipo proporciona QoS tanto a nivel 2 (conmutación) como a nivel 3 (encaminamiento). Las prestaciones QoS de los dos niveles son independientes entre sí, aunque el hecho de que comparten la posibilidad de usar el parámetro DSCP, permite obtener comportamientos coherentes en ambos niveles.

5.5.1 QoS Layer 2

La QoS de nivel 2 se ejecuta sobre el tráfico conmutado, y se ajusta al procesado de parámetros y comportamiento de IEEE 802.1p, con tres niveles de prioridad interna. Esta prioridad se toma en consideración para establecer el orden de procesado y transmisión en cada una de las interfaces de salida del switch.

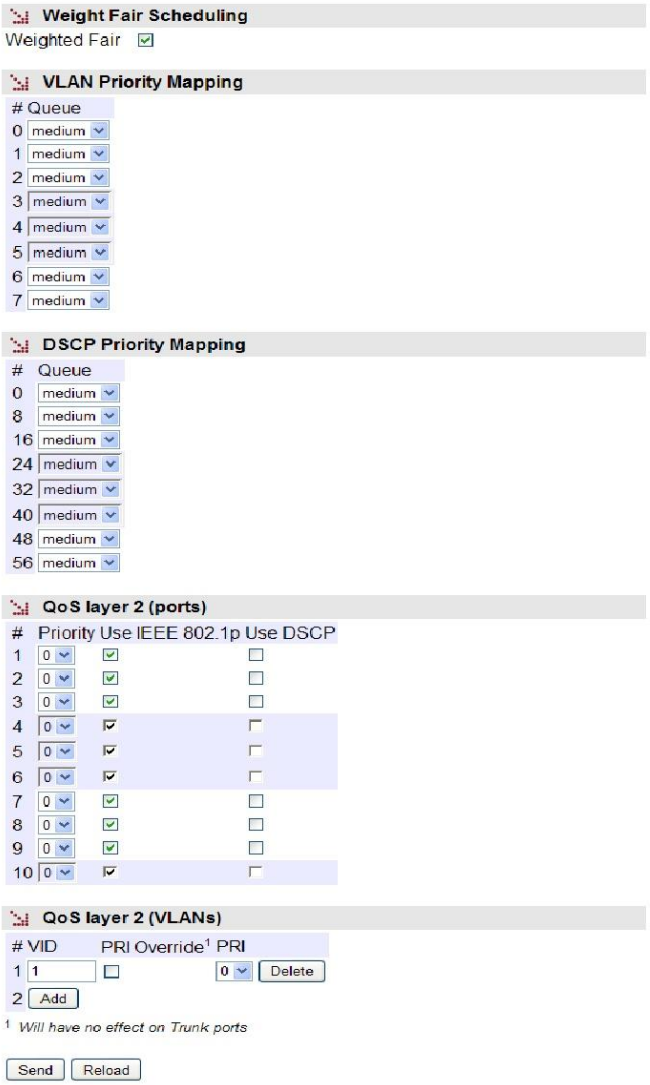
Se admiten dos posibles políticas de servicio en el procesado de las colas de cada una de las prioridades: ***Priority*** o ***Weight Fair Scheduling*** **(WFQ)**. La política ***Priority*** sólo sirve una cola de menor prioridad cuando las colas de prioridad superior están vacías. La política **WFQ** garantiza un servicio ponderado a todas las prioridades, aunque dando preeminencia a las colas de mayor prioridad.

La política de servicio es única para el servicio de nivel 2. Los parámetros son la VLAN y la prioridad 802.1p (incluidas en el tag o asignadas en función del puerto de entrada) o el campo DSCP de nivel 3.

La prioridad soportada por la norma 802.1p admite valores en el rango 0 a 7. Las tramas recibidas sin tag (untagged) reciben una prioridad en dicho rango en función de la interfaz por la que han sido recibidas, según el apartado **QoS Layer 2 (ports)**. Las tramas que sí tienen tag, puede ser que incluyan tanto el identificador de la VLAN como la prioridad (tagged) como únicamente la prioridad (priority tagged, VLAN = 0). En caso de incluir el identificador de VLAN, se procesan según las reglas del apartado **QoS Layer 2 (VLANs)**. Si, por el contrario, únicamente incluyen la prioridad, se procesan según el apartado **QoS Layer 2 (ports).**

En todo caso, con excepción de la asignación por DSCP que es directa a las colas internas, la prioridad asignada se emplea para la clasificación final según el apartado **VLAN Priority Mapping.**

FIGURA 23 Submenú *Layer 2* del menú *QoS*



Los apartados y sus parámetros de configuración son los siguientes:

Weight Fair Scheduling:

- **Weighted Fair.** Establece la política de servicio de prioridad a nivel 2. Con la opción NO habilitada la política es ***Priority***. Con la opción Sí habilitada la política es ***WFQ***.

VLAN Priority Mapping:

- **#.** Identifica el valor de la prioridad asociada a la trama 802.1 (cubre todo el rango de valores permitidos por la norma).
- **Queue.** Establece la prioridad de la cola en la que se insertará el tráfico coincidente con el valor de la prioridad indicado por el campo #. Los valores admisibles identifican las tres prioridades internas: **High**, **Medium** o **Low.**

DSCP Priority Mapping:

- **#.** Identifica el valor del campo DSCP que se procesa.
- **Queue.** Establece la prioridad de la cola en la que se insertará el tráfico coincidente con el valor del DSCP indicado por el campo #. Los valores admisibles identifican las tres prioridades internas: **High**, **Medium** o **Low.**

QoS layer 2 (ports):

- **#.** Identificador de interfaz física.
- **Priority.** Valor de la prioridad asignado a las tramas 802.1 recibidas en la interfaz indicada por #. Esta prioridad se asigna siempre que las tramas recibidas no incluyan un tag 802.1p. La asignación a las prioridades internas se lleva a cabo según los valores establecidos en el apartado **VLAN Priority Mapping**.
- **Use IEEE 802.1p.** La opción habilitada indica que deberá usarse el campo de prioridad presente en las tramas cuando éstas incluyan tag 802.1p. La asignación a las prioridades internas se lleva a cabo según los valores establecidos en el apartado **VLAN Priority Mapping.**

- **Use DSCP.** La opción habilitada indica que deberá procesarse el campo DSCP de las tramas recibidas para asignar la prioridad interna de la trama, según los valores establecidos en el apartado **DSCP Priority Mapping.**

> Las opciones **Use IEEE 802.1p** y **Use DSCP** pueden estar activadas de forma simultánea. La jerarquía en cuanto a la prioridad final asignada a la trama es la siguiente: **DSCP**, **IEEE 802.1p** y **Priority** (usuario); de este modo:
>
> - A una trama sin tag se le asociará la prioridad establecida por el usuario.
>
> - A una trama con tag se le mantendrá la prioridad presente en la propia trama siempre que el campo DSCP o bien no esté presente (tráfico no IP) o no coincida con ninguno de los valores especificados.

QoS layer 2 (VLANs):
Este apartado incluye una tabla que admite la adición y eliminación de conjuntos de parámetros.

- **#.** Indicador de posición en la tabla.
- **VID.** Valor del identificador de VLAN incluido en el tag 802.1.
- **PRI Override**. Establece si la prioridad de las tramas perteneciente a la VLAN coincidente con el campo VID debe ser sobrescrita (opción habilitada) o debe mantenerse la prioridad recibida (opción NO habilitada).
- **PRI**. Establece la prioridad asignada a las tramas perteneciente a la VLAN coincidente con el campo VID si la opción **PRI Override** está habilitada.

5.5.2 QoS Layer 3

La QoS de nivel 3 permite la clasificación del tráfico encaminado en base a un conjunto de parámetros de nivel superior como son: la dirección IP origen y/o destino, el tipo de servicio y a su vez el campo DSCP.

También dispone de políticas de servicio, aunque a nivel 3 pueden configurarse para cada interfaz. Las políticas disponibles son: ***FIFO***, ***Priority***, ***HTB*** y ***HTB-Shared***.

Por defecto, la política de servicio es ***Priority***. No obstante, como en ausencia de reglas específicas todo el tráfico se clasifica con la misma prioridad, en la práctica, la política en estas condiciones es ***FIFO***.

Las reglas de clasificación de QoS de nivel 3 contemplan como parámetros elegibles la dirección IP origen, la dirección IP destino, ambas admiten redes utilizando la máscara para ello, el tipo de servicio y el campo específico de nivel 3 DSCP, que identifica clases de tráfico.

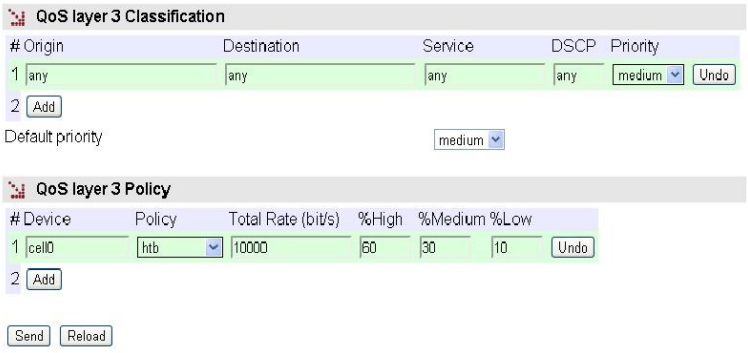
En cuanto existan reglas de clasificación, la política Priority pasa a ser efectiva de forma automática.

Como alternativa, se dispone de la opción de especificar la política HTB o HTB-Shared de forma individual por dispositivo. HTB es el acrónimo de *Hierarchical Token Bucket*. La política de servicio permite un reparto ponderado del ancho de banda a los flujos de datos generados por las reglas de clasificación, y que siempre son tres, high, medium y low.

La ponderación se configura con un porcentaje del ancho de banda disponible, el cual es a su vez un parámetro que el usuario debe especificar.

La diferencia entre HTB y HTB-Shared es que, en el primer caso, el ancho de banda se asigna de forma estricta según los valores de la ponderación, incluso en el caso de que una de las clases no use el ancho de banda asignado, las otras clases nunca podrán superar el valor porcentual configurado, es decir, siempre los valores porcentuales son límites máximos que nunca se van a sobrepasar. Por el contrario, la política HTB-Shared permite la utilización del ancho de banda no ocupado por las otras clases cuando alguna de ellas excede el límite propio, en este caso, los valores porcentuales se comportan como límites mínimos garantizados en caso de plena ocupación, a la vez que admite puntas de tráfico que exceden el valor garantizado cuando la ocupación no es plena.

FIGURA 24 Submenú *Layer 3* del menú *QoS*



Los apartados y sus parámetros de configuración son los siguientes:

QoS Layer 3 Classification:

En este apartado se crean las reglas de clasificación, con una estructura tabular. Los parámetros para cada una de las reglas son:

- **Origin.** Establece la dirección IP origen del paquete asociado con esta regla de clasificación. 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. El valor any es un valor válido, e implica que no se analizará la dirección IP origen.
- **Destination.** Este campo es equivalente al anterior, pero analizando ahora el campo de dirección IP destino.
- **Service**. 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**, y supone que no se analiza el servicio como parte de la condición.
- **DSCP**. El campo analizado es la información de clase de servicio de nivel 3, DSCP (*Differentiated Services Code Point*). El usuario configura de forma directa el valor para el cumplimiento de la condición. Es un valor numérico comprendido entre 0 y 31 (valor estricto del campo DSCP completo). Admite el valor **any** como comodín para obviar esta parte de la condición.
- **Priority.** Establece la prioridad del paquete en caso de que cumpla todos los requisitos fijados por la regla. Los valores son High, Medium y Low.

El campo **Default priority** fija la prioridad en todos aquellos casos en que el paquete no cumpla con ninguna de las reglas establecidas o bien no existan reglas configuradas. Los valores son los mismos que el campo **Priority.**

QoS Layer 3 Classification:

En este apartado el usuario puede asignar las políticas HTB o HTB-Shared de forma específica a un dispositivo. En caso de no hacerlo, la política de servicio es **Priority** para todos ellos (véase el apartado introductorio).

La configuración también es tabular, y los parámetros para cada una de las asignaciones son los siguientes:

- **Device.** Identificador del dispositivo al que se aplicará la política especificada por los parámetros siguientes.
- **Policy.** Fija la política de servicio de las colas de cada una de las tres prioridades. Los valores son **htb** y **htb-shared**.
- **Total rate**. Indica el ancho de banda asociado al dispositivo. Las unidades son bits por segundo (bps).
- **%High, % Medium y % Low**. Estos tres campos indican el porcentaje del ancho de banda que se asignará a cada una de las prioridades.

5.6 CONFIGURACIÓN ROUTING

El equipo opera como router para el protocolo IPv4. El servicio de router está siempre activo. Los datos para la función de encaminamiento pueden tener dos orígenes, datos estáticos con carácter permanente establecidos por el usuario, y datos dinámicos, obtenidos por el propio equipo a partir de la ejecución de protocolos de encaminamiento estándar: RIP y OSPF.

5.6.1 Static routes

Mediante el submenú *Static routes* del menú *Routing*, el usuario puede proporcionar al sistema datos estáticos y permanentes al servicio de encaminamiento.

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 caso en que el servicio no disponga de datos concretos para alcanzar un destino, en el apartado *Default Static Routes*.

> En caso de que el equipo disponga de interfaces inalámbricas operativas, el operador no únicamente proporcionará la dirección IP de la interfaz, sino que también establecerá un router por defecto asociado a dicha interfaz, teniendo ésta precedencia sobre cualquier configuración establecido por el usuario.

FIGURA 25 Submenú *Static routes* del menú *Routing*

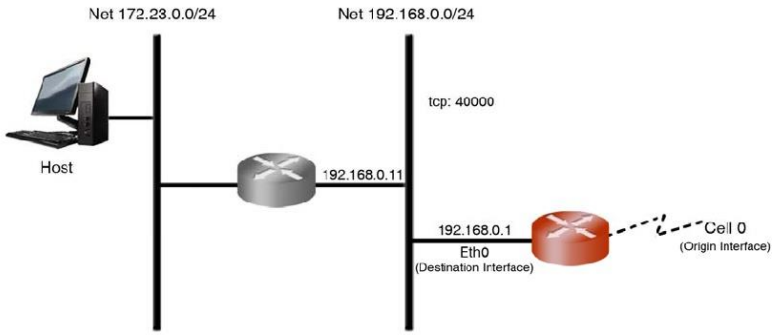
Los parámetros de configuración de una ruta estática son:

- **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.
- **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, p.e. cell0 para la interfaz WAN, 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:

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 26 Ejemplo de configuración de ruta estática



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

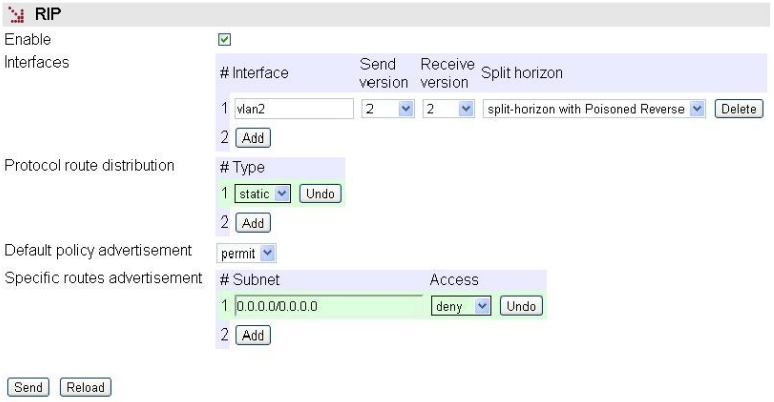
- **Gateway.** Permite especificar la dirección IP del siguiente router para el enrutamiento del tráfico cuyo destino no coincida con ninguna ruta conocida.
- **Dest I/F (Destination interface)**. Permite especificar la interfaz a través de la cual se enviará el tráfico encaminado hacia el router indicado en el campo anterior. Las interfaces se identifican por el dispositivo asociado, bien sea real, p.e. cell0 para la interfaz WAN, 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.

5.6.2 Protocolo RIP

El equipo incorpora el protocolo de encaminamiento estándar RIPv1 [1] y RIPv2 [2].

El protocolo RIP puede ser habilitado o inhabilitado por parte del usuario, mediante el control tipo *Checkbox Enable* . En caso de que el usuario habilite el protocolo, también deberá establecer las interfaces en las que se desea que se halle operativo.

FIGURA 27 Submenú *Protocolo RIP* del menú *Routing*



Los parámetros de configuración propios de cada interfaz son:

- **Interface.** Identificador del dispositivo, real o virtual, en el que se quiere habilitar la ejecución del protocolo.
- **Send version.** Establece la versión de protocolo que el equipo empleará para transmitir los datos de encaminamiento sobre la interfaz especificada. Las opciones son: *none* (no se transmite información), *1* (versión 1), *2* (versión 2) y *1-2* (la información se transmite con las dos versiones).
- **Receive version.** Establece la versión de protocolo que el equipo aceptará en los mensajes recibidos en la interfaz especificada. Las opciones son: *none* (no se acepta ningún mensaje RIP), *1* (únicamente se procesarán mensajes con la versión 1), *2* (únicamente se procesarán mensajes con la versión 2) y *1-2* (se aceptarán mensajes de cualquiera de las dos versiones).

- **Split-horizon:** Establece el criterio que se empleará en el procesado de los datos de encaminamiento con la finalidad de evitar el problema de "counting to infinity". Las opciones son: *no split-horizon*, *split-horizon* y *split-horizon with poisoned reverse* (Véase apartado 3.4.3 de [2]).

Los parámetros de configuración comunes a todas las interfaces son:

- **Protocol Route Distribution.** Permite indicar si el protocolo deberá incluir, no únicamente la información de encaminamiento adquirida mediante los mensajes propios del protocolo y los datos IP de las interfaces locales, sino también los datos de encaminamiento especificados en el apartado de rutas estáticas o bien de otros protocolos.

- **Default policy advertisement y Specific routes advertisement.** Estos dos parámetros permiten establecer opciones de filtrado de la información de encaminamiento. El primero de ellos establece el criterio general del filtro, permitir o denegar, y afecta a la totalidad de las rutas. El segundo de ellos, permite indicar las excepciones deseadas al criterio general, de ahí que cada una de las entradas específicas incluya también la opción de permitir o denegar.

Las opciones del criterio general, combinadas con las posibles excepciones, permiten disponer de dos comportamientos de filtro:

- **Envío todo con excepciones.** Opción del criterio general *permitir*, que es el valor por defecto, con las exclusiones establecidas en el apartado correspondiente, que en este caso tendrían habilitada la opción *denegar*.

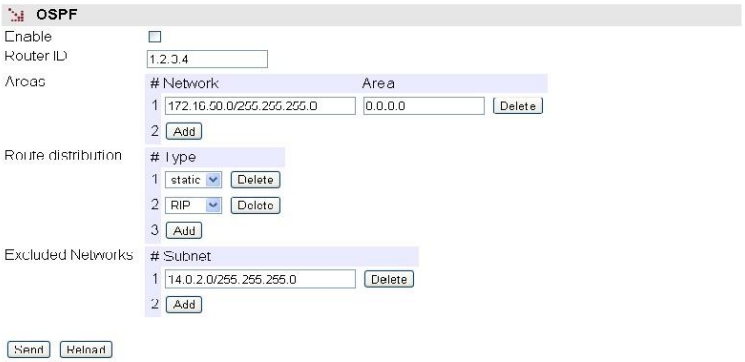
- **Sólo se envían las excepciones.** Opción del criterio general *denegar*, con las excepciones establecidas en el apartado correspondiente, que en este caso tendrían habilitada la opción *permitir*.

5.6.3 Protocolo OSPF

El equipo incorpora el protocolo de encaminamiento estándar OSPFv4.

El protocolo OSPF puede ser habilitado o inhabilitado por parte del usuario, mediante el control tipo Checkbox *Enable*.

FIGURA 28 Submenú *Protocolo OSPF* del menú *Routing*



El conjunto de parámetros necesarios para la ejecución del protocolo y las condiciones del mismo se detallan a continuación:

- **Router ID:** Identificador del equipo. Aunque el formato coincide con el usualmente empleado para una dirección IP, realmente es un dígito para distinguir a los routers que ejecutan el protocolo OSPF entre sí. Normalmente se suele hacer coincidir con una de las direcciones IP asignadas al router.

- **Areas:** Consta de dos valores, el primero es una dirección o rango de direcciones IP, y que supone que la interfaz o interfaces cuyas direcciones IP estén incluidas en el rango mencionado ejecutarán el protocolo OSPF, y su área será la indicada por el parámetro **Area**, este último, a pesar de representarse normalmente como si fuera una dirección IP es el identificativo del Área a la que están conectadas las interfaces incluidas por el primer valor. Todos los routers con interfaces operando en una misma área comparte dicho identificativo. El área con identificador 0.0.0.0 es válida y actúa como troncal (backbone), ya que todas las áreas deben estar conectadas a ella.

- **Protocol Route Distribution:** Permite indicar si el protocolo deberá incluir, no únicamente la información de encaminamiento adquirida mediante los mensajes propios del protocolo y los datos IP de las interfaces locales, sino también los datos de encaminamiento especificados en el apartado de rutas estáticas o bien de otros protocolos.

- **Excluded Networks:** El usuario puede aquí indicar que redes IP no deben ser incluidas en los mensajes de rutas OSPF.

5.7 CONFIGURACIÓN FILTERING

El menú *Filtering* permite funcionalidades de firewall, definiendo qué tráfico se permite y qué tráfico será rechazado, así como la aplicación de condiciones adicionales al tráfico procesado por la función de rutado.

Los parámetros del menú se dividen en tres bloques bien diferenciados, siendo éstos:

- Filtrado de paquetes para los servicios locales (http, Telnet ó ***any***)
- Filtrado de paquetes por servicio entrante/saliente para las interfaces WAN.
- Filtrado de paquetes por servicio entrante/saliente para las interfaces virtuales asociadas a cada VLAN definida.

FIGURA 29 Menú *Filtering*

Los parámetros de configuración en cada bloque son los siguientes:

- **Vlan.** Identificador del dispositivo, real o virtual, sobre el que tiene aplicación la regla. Sólo presente en el apartado correspondiente a las interfaces LAN.
- **Origin.** Permite especificar la procedencia IP del tráfico, es decir, de una dirección IP en concreto o de cualquier dirección IP (**any**). El valor por defecto es **any.** La especificación de una dirección IP en concreto requiere que los valores se introduzcan en el formato del direccionamiento IP. Ejemplo: Subred (192.168.50.0/255.255.255.0 ó 192.168.50.0/24) o Host (192.168.50.5/255.255.255.255 ó 192.168.50.5/32 ó 192.168.50.5). Sólo presente en los apartados en los que tiene sentido.

- **Destination.** Permite especificar el destino IP del tráfico, es decir, hacia una dirección IP en concreto o hacia cualquier dirección IP (**any**). El valor por defecto es **any.** La especificación de una dirección IP en concreto requiere que los valores se introduzcan en el formato del direccionamiento IP. Ejemplo: Subred (192.168.50.0/255.255.255.0 ó 192.168.50.0/24) o Host (192.168.50.5/255.255.255.255 ó 192.168.50.5/32 ó 192.168.50.5).

- **Service**. Permite especificar cualquier tipo de tráfico (**any**) o bien un tráfico en concreto (**tcp**/**udp**/**icmp)**. El valor por defecto es **any**. Si se especifica un tráfico en concreto, si se desea, junto con el servicio puede indicarse el número de puerto (1÷65535) o un rango. Ejemplo: tcp ó tcp:23 ó udp:5001-5005.

- **Dir**. Permite especificar la dirección del tráfico, es decir, si es entrante (**in**) o saliente (**out**).

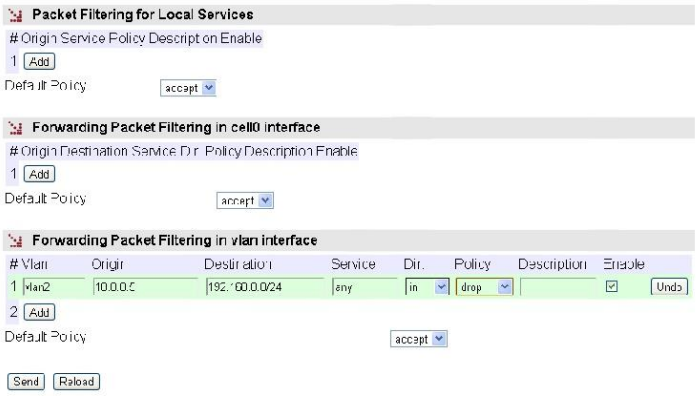
- **Policy**. Permite especificar la política del filtrado (**accept**, **drop** ó **reject**). Cuando la política de filtrado es **accept**, se aceptan sólo los paquetes que cumplen la regla establecida. Cuando la política de filtrado es **drop**, en cambio, se descartan los paquetes que cumplen la regla establecida. La política de filtrado **reject** también implica el descarte de los paquetes que cumplen la regla establecida pero, a diferencia de drop, cuando se descarta el paquete, se envía a la dirección de origen del paquete el mensaje ICMP adecuado.

- **Description.** Permite especificar una descripción de hasta 15 caracteres alfanuméricos.

- **Default Policy**. Permite determinar el comportamiento del filtrado del equipo respecto al que no se incluye en ninguna regla específica del apartado correspondiente.

Ejemplo:

Se desea establecer una política de filtrado para eliminar el tráfico presente en la VLAN2 procedente del host 10.0.0.5 cuyo destino esté en el rango IP 192.168.0.0/24. La configuración del bloque VLAN sería la mostrada en la figura.



5.8 CONFIGURACIÓN NAT

NAT es el servicio de traducción de direcciones IP que nos permite mezclar la utilización de direcciones IP privadas sin que ello nos impida acceder a recursos con dirección IP pública, o bien preservar esquemas de direccionamiento entre distintas áreas de redes interconectadas.

El menú NAT define las reglas que permiten traducir de forma selectiva las direcciones IP, así como modificar los puertos del servicio de transporte.

> ! Debe tenerse en cuenta que el servicio NAT tiene una **regla por defecto.**
> La correcta operación de servicios que basan su operativa en el análisis de los datos que las reglas NAT tienen capacidad para modificar, puede verse alterada por la presencia de la regla por defecto, ya que los servicios tienen un cierto orden de ejecución.
> **Si no se va a usar NAT es imprescindible eliminar la regla por defecto.**

FIGURA 30 Menú *NAT*

Los parámetros de configuración son:

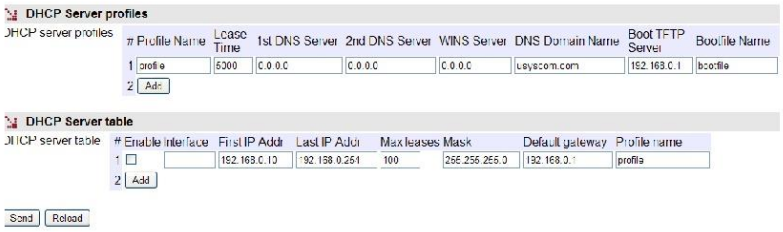
- **Origin**. Establece un rango de direcciones IP. Admite como valor **any**, en caso de que la dirección IP **origen** no sea relevante.
- **Destination**. Establece un rango de direcciones IP. Admite como valor **any**, en caso de que la dirección IP **destino** no sea relevante.
- **Service**. Establece condiciones en cuanto al servicio, entendido como protocolo (**tcp/udp/icmp)** y puerto (1 a 65535 o un rango). Admite como valor **any,** en caso de que el servicio no sea relevante. Ejemplo: tcp ó tcp:23 ó udp:5001-5005.
- **Transl**. **Origin**. Establece la dirección IP que debe reemplazar a la dirección IP **origen**. Puede especificarse una dirección IP o bien el identificador de la interfaz correspondiente. En caso de que no se desee alterar la dirección original, el valor debe ser **original.**
- **Transl. Dest.** Establece la dirección IP que debe reemplazar a la dirección IP **destino**. Puede especificarse una dirección IP o bien el identificador de la interfaz correspondiente. En caso de que no se desee alterar la dirección original, el valor debe ser **original.**
- **T. Orig. Port.** Establece el identificador de puerto que debe reemplazar al puerto **origen** contenido en el paquete. Admite la configuración de un rango. En caso de que no se desee alterar el puerto origen, el valor debe ser **original.**
- **T. Dest. Port.** Establece el identificador de puerto que debe reemplazar al puerto **destino** contenido en el paquete. Admite la configuración de un rango. En caso de que no se desee alterar el puerto destino, el valor debe ser **original.**
- **Description.** Permite especificar una descripción de hasta 15 caracteres alfanuméricos.

5.9 CONFIGURACIÓN DHCP SERVER

El DRA-2 tiene integrado un servidor DHCP que permite asignar direcciones IP de forma automática a los equipos que lo soliciten.

El servidor está diseñado para operar de forma selectiva en cada una de las posibles interfaces VLAN virtuales del equipo.

FIGURA 31 Menú *DHCP server*



5.9.1 DHCP Server Profiles

La creación de perfiles permite crear conjuntos de parámetros comunes a varias instancias del servidor DHCP, operando en distintas interfaces.

Los parámetros de configuración de un perfil son:

- **Lease time.** Permite especificar en segundos el tiempo que una dirección IP se asignará en base a un petición de un cliente DHCP. Transcurrido el tiempo indicado, si el cliente DHCP no solicita una renovación, la dirección IP se considerará disponible para atender nuevas peticiones.
- **1st DNS server.** Permite especificar la dirección IP del servidor DNS primario que el servidor DHCP proporcionará al cliente DHCP. Si se deja en blanco (0.0.0.0) no se enviará información de servidores DNS al cliente.
- **2nd DNS server**. Permite especificar la dirección IP de un servidor DNS secundario al cliente DHCP. Si se deja en blanco (0.0.0.0) significa que no se enviará información alguna al cliente en este concepto.
- **WINS server**. Permite establecer la dirección IP del servidor WINS que se comunicará al cliente DHCP. WINS es un sistema de resolución de nombres propietario de Microsoft para equipos que ejecutan el sistema operativo Windows.

- **DNS Domain Name**. Establece el dominio DNS que el cliente usará para construir su nombre DNS completo.
- **Boot TFTP Server**. Establece la dirección IP del servidor TFTP que almacena el fichero de arranque remoto, lo que permitirá al cliente ejecutar una petición de descarga del fichero.
- **Bootfile Name**. Establece el nombre del fichero de arranque remoto que el cliente solicitará al servidor TFTP configurado en el punto anterior.

5.9.2 DHCP Server Table

Los parámetros de configuración para cada interfaz son:

- **Enable.** Permite activar el servicio DHCP. Debe marcarse si se quiere utilizar un servidor DHCP.
- **Interface.** Establece la interfaz en la que se atenderán las peticiones de los clientes, según los parámetros que se definen a continuación.
- **First IP Addr.** Permite especificar la **primera** dirección IP del pool de direcciones IP gestionadas por el servidor DHCP en esta interfaz.
- **Last IP Addr.** Permite especificar la **última** dirección IP del pool de direcciones IP gestionadas por el servidor DHCP en esta interfaz.
- **Max leases.** Permite especificar el número máximo de direcciones IP asignadas de forma simultánea en uso.
- **Mask.** Establece la máscara de red que se comunicará a los clientes DHCP.
- **Default Gateway.** Establece la dirección del router por defecto (Default Gateway) que se comunicará a los clientes DHCP.
- **Profile name.** Establece cual de los perfiles definidos en el apartado anterior debe aplicarse a las peticiones servidas en esta interfaz.

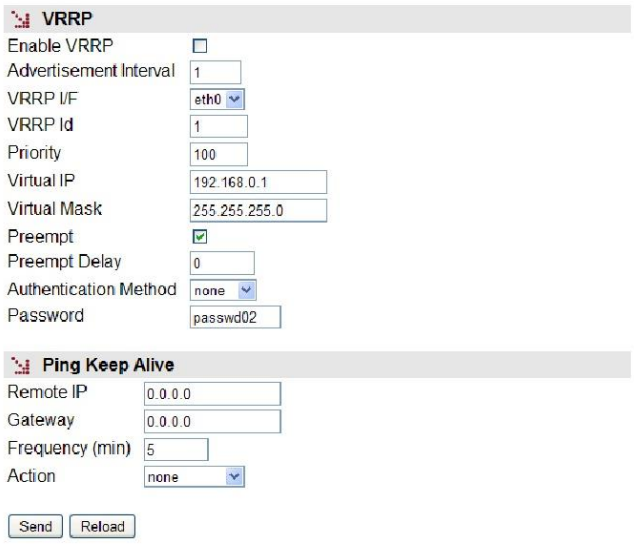
5.10 CONFIGURACIÓN VRRP

En algunos entornos, las redes se conectan entre sí vía un único router. Este único router es, por tanto, un punto potencial de fallo que podría desconectar una red entera del resto.

El protocolo VRRP permite que varios routers se presenten a los clientes con una dirección IP virtual común única, gestionando los routers incluidos en el router virtual quién es en cada momento el que presta el servicio efectivo, de modo que ofrece redundancia a los clientes de un modo transparente. Entre todos los routers, se elige un maestro, mientras que los otros routers actuarán como respaldo en caso de fallo del mismo.

El router maestro envía de forma periódica paquetes de anuncio VRRP a los routers de respaldo. Cuando los routers de respaldo no reciben los paquetes de anuncio VRRP durante un tiempo superior en tres veces el periodo establecido, asumen que el router maestro ha caído e inician un proceso de elección de un nuevo maestro.

FIGURA 32 Menú VRRP



Los parámetros de configuración se agrupan en dos grandes bloques, los cuales se describen a continuación:

VRRP:

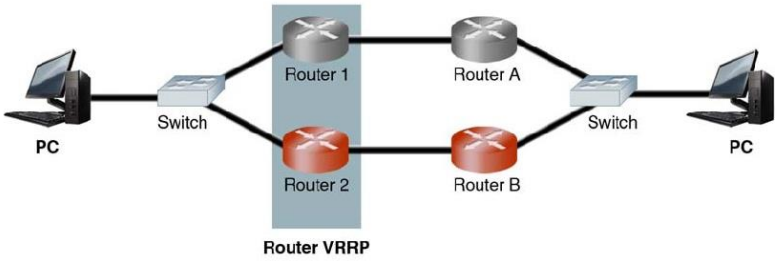
- **Enable VRRP.** Habilita la ejecución del protocolo.
- **Advertisement Interval.** Establece el periodo de tiempo en segundos que se usará, bien para la transmisión de los paquetes de anuncio VRRP cuando actúe como maestro, bien como base de tiempo para la supervisión del router maestro cuando actúe como router de respaldo. El valor por defecto es de 1 segundo.
- **VRRP I/F.** Establece la interfaz en la que se ejecutará el protocolo VRRP.
- **VRRP Id.** El router maestro usa la dirección MAC 00:00:5E:00:01:XX, tal como establece el protocolo estándar, siendo XX el Virtual Router IDentifier (VRID). El VRID permite la distinción de los distintos routers virtuales VRRP que estén operando en la red. El parámetro establece el valor del VRID. Si se especifica, por ejemplo, el VRID a 3, la dirección MAC virtual sería 00:00:5E:00:01:03.
- **Priority.** Este parámetro establece la prioridad que presentará el router durante el proceso de elección del router maestro. El rango admitido es el comprendido entre **1** y **254**. El router maestro se identifica por usar la prioridad 255, una vez finalizado el proceso de elección.
- **Virtual IP.** Establece la dirección IP virtual que usarán los cliente para el acceso al servicio de encaminamiento. Es común a todos los routers incluidos en el router virtual.
- **Virtual Mask.** Establece la máscara de red asociada a la dirección IP del parámetro anterior.
- **Preempt.** Esta opción supone que, si un router de respaldo tiene una prioridad mayor que la otorgada al router maestro elegido, el equipo pasará a forzar el cambio y se declarará como nuevo router maestro en cuanto sea incluido en el router virtual. Puede programarse un retardo para esta acción mediante el parámetro Preempt Delay.
- **Preempt Delay.** Permite especificar el tiempo, en segundos, en que el router de respaldo con más prioridad pasará a ser el router maestro.

- **Authentication Method.** Permite seleccionar el mecanismo de autentificación entre los routers físicos incluidos en el router virtual VRRP. Las opciones son **PASS** (Password) y **AH** (Authentication Header), aunque también es posible trabajar sin autentificación, seleccionando la opción **none.**

- **Password.** Establece la contraseña que se usará en caso de haber seleccionado el uso de autentificación.

Ping Keep Alive:

Es una opción que permite que un router físico de respaldo se erija como router maestro del router virtual VRRP en función de condiciones de accesibilidad a terceros routers por trayectos disjuntos (véase Figura).



- **Remote IP.** Establece la dirección del equipo externo que será objeto de supervisión. Si el campo tiene el valor 0.0.0.0 significa que la función está deshabilitada.

- **Gateway.** Dirección IP del siguiente router en caso de que el equipo remoto bajo supervisión no se halle en la misma red IP.

- **Frequency (minutes).** Establece la frecuencia con la que se transmitirán los mensajes de supervisión.

- **Action.** Selecciona el comportamiento que se desea que tenga el equipo cuando la función de supervisión falle. Las acciones disponibles son: **None** (no realizar ninguna acción) ó **vrrp2master** (forzando su prioridad a 255).

5.11 CONFIGURACIÓN VPN

Como ya se ha comentado en el apartado de los túneles WAN, éstos constituyen la forma de establecimiento de enlaces tipo punto a punto entre equipos. A diferencia de los túneles GRE y IPIP, los túneles IPSec se caracterizan por ser seguros, entendiendo por ello que la información es transportada de modo que su contenido no es accesible a terceros, lo que es especialmente necesario cuando la red IP sobre la que se establece el túnel no está bajo el control del usuario, o incluso ni siquiera es pública.

Para establecer un túnel IPSec es necesario establecer una asociación de seguridad en cada uno de los terminadores: Tunnel IP (inicio) y Remote GW (destino).

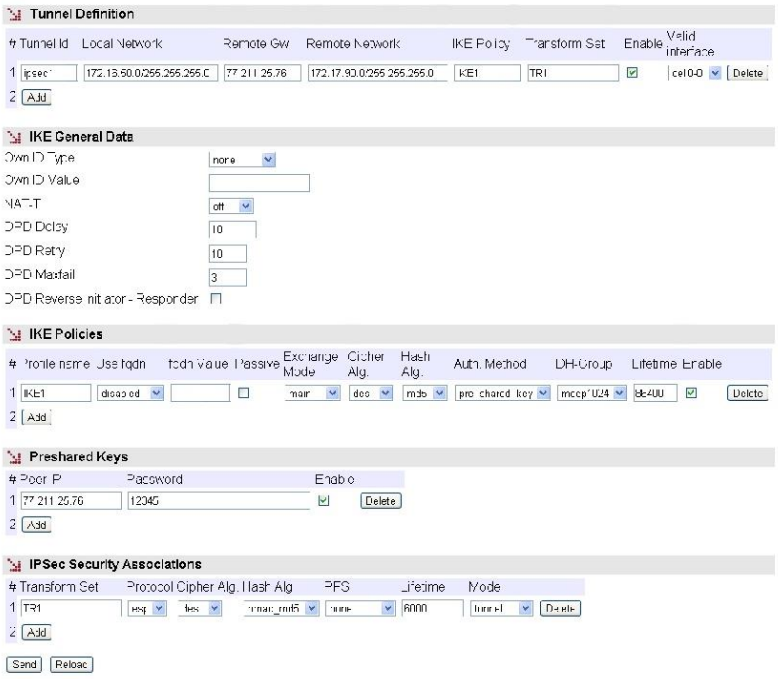
Una conexión IPSec entre dos extremos requiere de tres pasos:

- Establecimiento de un IKE Security association (IKE Policy).
- Establecimiento de un IPSec Security association (IPSec Association).
- Envío de datos protegidos a través de la conexión IPSec.

Los parámetros que se emplean en cada uno de estos tres pasos se configuran como bloques independientes, lo que permite su utilización en más de un túnel de forma simultánea, reduciendo así la necesidad de duplicar información de configuración.

La función DPD (Dead Peer Detection) es un mecanismo de supervisión de la operatividad de los túneles IPSec establecidos.

FIGURA 33 Menú *VPN*



Los apartados y sus parámetros de configuración son los siguientes:

Tunnel Definition:

- **Tunnel ID.** El identificador del dispositivo virtual tipo túnel que se desea establecer.
- **Local Network.** Establece el rango de direcciones IP origen que se transportarán en el túnel. Proporciona un filtro a nivel de dirección IP origen. El valor **any** es aceptado, así como direcciones IP de red, mediante el formato IP/Mask.
- **Remote GW.** Dirección IP del equipo remoto terminador del túnel IPSec.
- **Remote Network.** Rango de direcciones IP alcanzables en el extremo remoto del túnel. Es el equivalente a una ruta estática, en el sentido que se cursarán dentro del túnel todos aquellos datos que coincidan con el rango especificado. También se acepta el valor especial **any**.

- **IKE Policy.** Selecciona el conjunto de parámetros, previamente definidos, que se empleará para el establecimiento de la *IKE Security association*.
- **Transform Set.** Selecciona el conjunto de parámetros, previamente definidos, que se empleará para el establecimiento de la *IPSec Security association*.
- **Enable.** Habilita el túnel configurado. Permite disponer de túneles configurados operativos o no según decisión del usuario.
- **Valid Interface.** Indica el identificador de dispositivo válido sobre el que se permite el establecimiento del túnel. Actúa como un filtro adicional. El valor **any** es aceptado.

IKE General Data:

- **Own ID Type.** Indica el tipo de identificación que se usará por los equipos. Las opciones son **none**, **address** lo que implica la utilización de la dirección IP, **fqdn**, que supone el uso de un dominio (p.e. foo.domain.com), o bien **user_fqdn**, lo que supone el uso de una dirección de correo electrónico (p.e. foo@domain.com).
- **Own ID Value.** El valor de la identidad propia en el caso de haber seleccionado una opción distinta de **none** en el parámetro previo.
- **NAT-T.** Habilita el uso de la opción **NAT-T**, lo que permite que el protocolo IPSec funcione adecuadamente cuando se atraviesan servicios NAT. Las opciones son **off**, cuando no se desea que esté habilitada ni se aceptará en caso de que sea propuesta por el extremo remoto, siendo además el valor por defecto, **on** significa que la opción se usará cuando se detecte la presencia de servicios NAT entre los extremos, y **force** supone que su utilización con independencia de que se detecte o no la presencia de servicios NAT.
- **DPD Delay.** Este parámetro fija el tiempo entre los mensajes Hello transmitidos para la función de supervisión del túnel. El rango de valores válidos es de 0 a 1200, siendo las unidades segundos. El valor 0 supone que la supervisión no se realiza.
- **DPD Retry.** Establece el tiempo de espera de la respuesta a un mensaje Hello transmitido, en segundos. En caso de no recibir la respuesta del extremo remoto en este plazo, el equipo considera que se ha producido un fallo de supervisión.

- **DPD Maxfail.** El valor de este parámetro es el límite máximo de fallos de respuesta a mensajes Hello admitido. En caso de llegar al mismo, se considera que el túnel no está disponible y se intenta su restablecimiento.
- **DPD Reverse Initiator-Responder.** Está opción permite el uso del servicio de supervisión DPD con túneles terminados por equipos Cisco que ejecutan una variante no estándar.

IKE Policies:

- **Profile name.** Identifica el conjunto de parámetros que se está configurando para el establecimiento de una *IKE Security association*, de modo que pueda ser utilizada por uno o más de los túneles configurados.
- **Use fqdn (Full Qualified Domain Name**). Indica el tipo de identificación que se usará por los equipos. Las opciones son **disabled**, lo que implica la utilización de la dirección IP, **fqdn**, que supone el uso de un dominio (p.e. foo.domain.com), o bien **user_fqdn**, lo que supone el uso de una dirección de correo electrónico (p.e. foo@domain.com.
- **fqdn value.** Este parámetro determina bien el dominio o la dirección de correo electrónico a emplear cuando se ha seleccionado una de las dos opciones indicadas en el punto anterior.
- **Passive.** Cuando está opción está activada, el equipo no tomará la iniciativa para el establecimiento del túnel, quedando a la espera de recibir la petición proveniente del extremo remoto.
- **Exchange Mode.** Fija el modo en que se realiza el intercambio de claves. El modo debe ser el mismo en ambos extremos para que el intercambio pueda ser exitoso. Las opciones son **main**, **agressive** y **base.**
- **Cipher alg. Cipher alg.** Determina el algoritmo de cifrado que se empleará para el intercambio de claves. Los algoritmos disponibles don **DES**, **3DES** y **AES**.
- **Hash Alg.** Determina el algoritmo hash empleado para la autentificación durante el intercambio de claves. Las opciones disponible son **MD5** (Message Digest 5) y **SHA1** (Secure Hash Algorithm).
- **Auth. Method.** Establece el mecanismo de generación de claves. Únicamente está disponible como método el intercambio de claves previamente establecidas.

- **DH Group.** Selección del grupo Diffie-Hellman (DH) Modular Exponential (MODP) para la creación de claves. Están disponibles los grupos 1 (768 bits, opción **modp768**), el grupo 2 (1024 bits, opción **modp1024**) y el grupo 5 (1536 bits, opción **modp1536**).
- **Lifetime.** Periodo de vigencia de la asociación de seguridad del intercambio de claves. Cuando expira el tiempo establecido, se renegocia una nueva asociación. El valor establece el tiempo en segundos.
- **Enable.** Indica que el conjunto de parámetros especificado puede ser utilizado (opción activa) o no (opción no activa).

Preshared Keys:

- **Peer IP.** Establece la dirección IP del equipo remoto del túnel (**Remote GW**) para el cual se define la contraseña del parámetro siguiente.
- **Password**. En este parámetro se almacena la contraseña.
- **Enable.** Indica si la contraseña configurada puede ser empleada (opción activa) o no (opción no activa).

IPSec Security Associations:

- **Transform set.** Identifica el conjunto de parámetros que se está configurando para el establecimiento de una *IPSec Security association*, de modo que pueda ser utilizada por uno o más de los túneles configurados.
- **Protocol.** El protocolo establece cuál de los dos tipos de encapsulado se usará. **ESP** (Encapsulating Security Payload) proporciona cifrado y autentificación para cada uno de paquetes, o **AH** (Autentificación Header), únicamente proporciona servicio de autentificación.
- **Cipher alg.** Determina el algoritmo de cifrado que se empleará para encriptar los datos de usuario. Los algoritmos disponibles don **DES**, **3DES** y **AES**.
- **Hash alg.** Determina el algoritmo hash empleado para la autentificación. Las opciones disponible son **MD5** (Message Digest 5) y **SHA1** (Secure Hash Algorithm). Hay una tercera opción, **non-auth** que implica que no se incluye la autentificación.

Las opciones de autentificación y cifrado pueden combinarse de distintos modos. Si se selecciona como protocolo **AH**, únicamente se toma en consideración la elección del algoritmo de hash, por el contrario, cuando se selecciona como protocolo **ESP**, la encriptación está siempre presente, con el algoritmo de cifrado seleccionado, y la autentificación puede ser incluida, bien sea con **MD5** o **SHA1,** o puede no estar incluida seleccionando el valor **non-auth**.

- **PFS (Perfect Forward Secret).** Si la opción está habilitada, supone que cada nueva clave renegociada debe ser completamente desvinculada de la anterior. El extremo remoto debe aceptar la opción **PFS** necesariamente para que el establecimiento sea exitoso. Esta opción proporciona seguridad adicional a costa de una mayor carga de procesado.

- **Lifetime.** Periodo de tiempo máximo de vigencia de una asociación de seguridad. Cuando expira el tiempo establecido, se renegocia una nueva asociación. El valor establece el tiempo en segundos.

- **Mode**. El servicio IPSec proporciona dos modos de operación, la primera es **tunnel**, que supone que el paquete original es completamente encapsulado en una cabecera IP adicional, la segunda es **transport**, lo que significa que se emplea la cabecera original sin añadir ninguna extra.

- **Enable.** Indica que el conjunto de parámetros especificado puede ser utilizado (opción activa) o no (opción no activa).

5.12 CONFIGURACIÓN NHRP

En entornos de redes malladas que emplean interfaces sin capacidad de propagación broadcast, usualmente denominadas interfaces NBMA (Non-Broadcast Medium Acces), no es inusual que un paquete que las atraviese sea procesado por varios routers intermedios hasta que llegue bien a su destino, bien al router de salida.

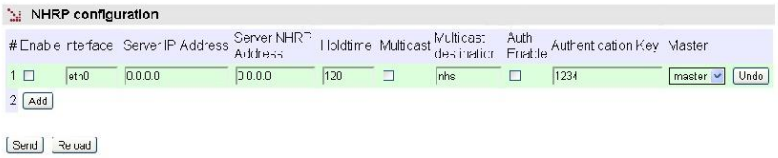
Las redes en las que se crean en base a túneles IP, con independencia del tipo de los mismos, acaban siendo colecciones de enlaces punto a punto, lo que supone que la red es del tipo NBMA.

El protocolo NHRP permite que los equipos cliente se registren de forma dinámica en un recurso común, el servidor NHRP, de modo que cada cliente descubre de la presencia del resto de los clientes sin necesidad de reconfiguración, que sería necesaria cada vez que un cliente se diese de alta, o de baja. Adicionalmente, el servidor NHRP actúa como protocolo de resolución de direcciones equivalente al ARP, ya que éste último no puede

ser empleado por el hecho de que los medios son NBMA, lo que en la práctica facilita intercambios más directos de tráfico entre los clientes NHRP.

El servicio NHRP tiene sentido cuando se emplean túneles IP, siendo éstos los que detectarán la dirección local NHRP que se registrará en el servidor NHRP.

FIGURA 34 Menú *NHRP*



Los distintos parámetros de configuración son los siguientes:

- **Enable.** Habilita o no la ejecución del protocolo NHRP según los parámetros incluidos en el registro (a continuación se detallan).
- **Interface.** Identificador de la interfaz sobre la que ejecutará el protocolo.
- **Server IP Address.** Dirección IP del equipo que presta los servicios como Servidor NHRP.
- **Server NHRP Address.** Dirección IP del servidor NHRP, siendo ésta la dirección accesible por el cliente local a través del túnel correspondiente.
- **Hold time.** Tiempo durante el cual es válido el registro en NHRP.
- **Multicast.** Establece si el tráfico multicast también se resolverá mediante el protocolo NHRP.
- **Multicast destination.** La dirección IP del equipo al que hay que enviar el tráfico multicast para su resolución. El valor por defecto es **nhs**, y equivale a la dirección especificada en el parámetro **Server NHRP Address**, es decir, que es el mismo que resuelve las direcciones unicast.
- **Auth. Enable.** Establece si la comunicación entre cliente y servidor debe incluir autentificación.

- **Authentication key.** Establece la clave que se usará para la autentificación del protocolo NHRP.

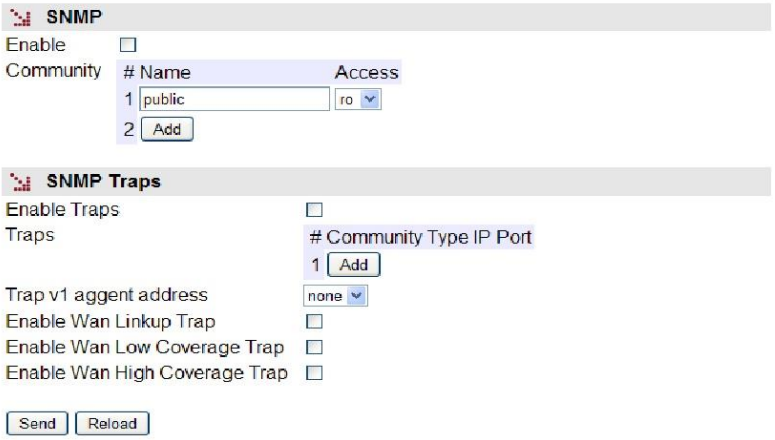
- **Master.** Cuando se establece el protocolo NHRP con más de un servidor NHRP de forma simultánea, este parámetro controla la prioridad para determinar a cual de los servidores NHRP se le envía el tráfico multicast. Típicamente el protocolo multicast suele ser un protocolo de encaminamiento dinámico, por lo que esta opción permite garantizar que sólo se anuncia la presencia del equipo hacia un único servidor NHRP en cada momento.

5.13 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 [3] y SNMPv2c [4], así como la elección del tipo de mensajes, *trap* e *inform*.

FIGURA 35 Menú *SNMP*



Los parámetros de configuración son:

- **Enable:** Habilita/inhabilita la ejecución del agente SNMP. El agente está operativo cuando la opción está seleccionada.

- **Community:** Dato tabular que permite definir varios perfiles de operación, incluidos los derechos de acceso asociados a cada uno, derechos de únicamente lectura (*ro*) o lectura/escritura (*rw*). Los perfiles se denominan *communities*.
- **Enable Traps:** Habilita/inhabilita la generación y transmisión de mensajes espontáneos por parte del agente SNMP. El agente enviará mensajes cuando la opción está seleccionada.
- **Traps:** Dato tabular que permite definir varios equipos destinatarios de los *traps*.
- **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.

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.

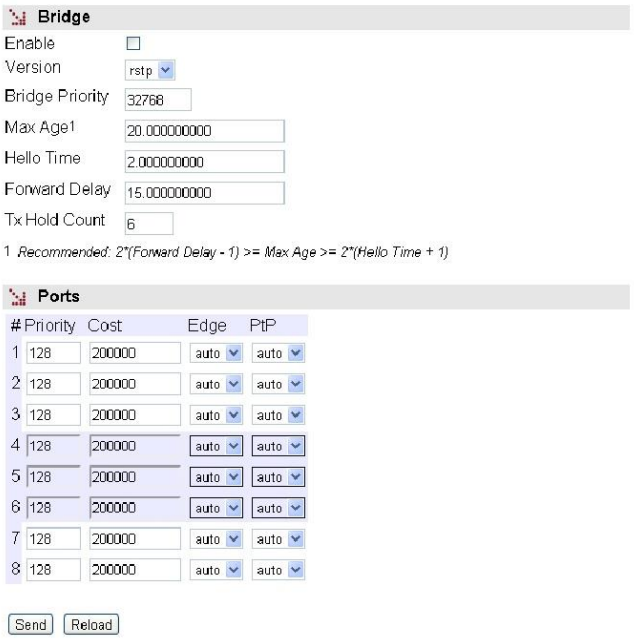
Cualquier cambio efectuado en la configuración del agente SNMP **únicamente** será activo después de realizar un **RESET** al equipo. El comando ***Apply*** no es suficiente, por lo que el cambio debe necesariamente almacenarse con el comando ***Save*** antes de solicitar la reinicialización.

5.14 STP

El protocolo Spanning Tree, tanto en su variante original (STP) como en la versión mejorada (RSTP) tiene como objetivo la identificación de los posibles bucles en redes de nivel 2, de modo que los equipos dialogan entre sí y establecen si las distintas interfaces de cada uno de ellos será activa en cuanto a la conmutación de tráfico de cliente, o por el contrario, quedará en reserva como respaldo en caso de posibles cambios topológicos. El resultado final es que los interfaces de cada equipo activos acaban conformando una estructura en árbol libre de bucles a partir del equipo raíz.

Si el equipo va a ser incluido en una red de nivel 2 interconectado con otros equipos de conmutación y existe la posibilidad de que se creen bucles (según la topología de conexión), es IMPRESCINDIBLE activar el protocolo Spanning Tree.

FIGURA 36 Menú *STP*



Los parámetros de configuración específicos del equipo son:

- **Enable.** Un parámetro checkbox simple para indicar si el protocolo STP debe ejecutarse o no.
- **Version.** Establece cual de las posibles versiones del protocolo se ejecutará. STP o RSTP (Rapid STP).
- **Bridge Priority.** Fija la prioridad del equipo que éste comunicará al equipo raíz.
- **Max Age.** Tiempo máximo que el equipo considera válido el último mensaje BPDU recibido. En el caso de expirar el tiempo estipulado, el equipo asume que ha habido un cambio topológico, e iniciará el proceso de comunicación de cambio topológico. El valor por defecto es de 20 segundos, mientras que el rango admitido está entre 6 y 40 segundos.
- **Hello Time.** Este parámetro establece el tiempo entre envíos de mensajes BPDUs (los mensajes propios del protocolo STP). El valor por defecto y a la vez máximo es de 2 segundos.

- **Forward Delay.** Este parámetro es el periodo de tiempo máximo que una interfaz estára en los estados listening y learning. El valor por defecto de este periodo es de 15 segundos, y el rango admitido está entre 4 y 30 segundos.

- **Tx Hold Count.** Establece el número máximo de paquetes BPDU que se pueden transmitir en un segundo. El valor por defecto es 6, y el rango admitido es entre 1 y 10.

Los parámetros de configuración propios de cada puerto son los siguientes:

- **Priority.** Establece la prioridad del puerto. En caso de que existan dos o más puertos con un mismo coste, la prioridad permite la elección del puerto raíz del equipo.

- **Cost.** Establece el coste asociado al puerto. La elección del puerto raíz de un equipo está directamente relacionada con el menor coste de los distintos puertos en relación al equipo raíz.

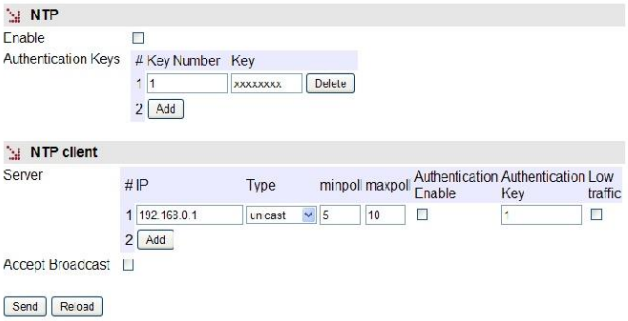
- **Edge.** Este parámetro indica el modo operativo de la interfaz en cuanto al STP. Las interfaces conectadas a equipos cliente, es decir, equipos que no son de conmutación de nivel 2 y por tanto no ejecutan STP ni pueden dar lugar a la creación de bucles, pueden ser arrancadas directamente en situación de cursar tráfico (modo **on**), por el contrario, aquellas que están directamente conectadas a equipos de conmutación de nivel 2, y por tanto susceptibles de cerrar lazos, deben ser arrancadas en modo de aceptar tráfico de usuario (modo **off**). Existe un tercer modo disponible, **auto**, en que es el equipo el que determinará la presencia o no de equipos de conmutación de nivel 2 conectados a la interfaz, útil en el caso en que se desconoce qué tipo de equipos acabarán siendo conectados, aunque el procesado de tráfico se ve ralentizado.

- **PtP.** El parámetro PtP establece si la interfaz está directamente conectada a otro equipo de conmutación de nivel 2 sobre un enlace punto a punto (valor **on**) o no (valor **off**), aunque el equipo también es capaz de detectar dicha situación (valor **auto**). El hecho de indicar al equipo que un enlace es PtP permite una mayor velocidad de convergencia del protocolo, se acelera el proceso de acuerdo sobre el paso de estado de un enlace de *designated* a *non-discarding (*operativo en cuanto a tráfico de usuario).

5.15 CONFIGURACIÓN NTP

El equipo dispone de un cliente NTP, de modo que pueda sincronizar la información horaria accediendo a servidores NTP. El protocolo NTP [5] es un estándar ampliamente usado en las redes basadas en TCP/IP, y admite el uso de varios servidores NTP de forma simultánea, así como la opción de emplear autentificación.

FIGURA 37 Menú *NTP*



Los parámetros de uso son:

- **Enable:** Habilita/inhabilita la ejecución del cliente NTP. El cliente está operativo cuando la opción está seleccionada.
- **Authentication keys:** Dato tabular que permite definir varias claves de autentificación a emplear posteriormente con la comunicación con los distintos servidores NTP.
- **Server:** Dato tabular que incluye los datos de acceso a los servidores NTP. Cada fila contiene los datos relativos a un único servidor NTP.
- **Accept broadcast:** Establece si el cliente NTP aceptará los mensajes transmitidos con mensajes NTP tipo broadcast.

Para cada uno de los servidores NTP configurados, es necesario proporcionar su dirección IP, el tipo de mensaje IP que empleará para acceder al servidor, individual (*unicast*) o colectiva (*manycast*), el tiempo mínimo entre solicitudes, estableciendo el parámetro el exponente de la potencia de 2, en segundos; el tiempo máximo entre solicitudes, también como el exponente de una potencia de 2, en segundos, y una opción de selección que determina si se debe usar la autentificación, en cuyo caso se debe indicar cuál de las claves previamente definidas usará el cliente con el servidor en cuestión.

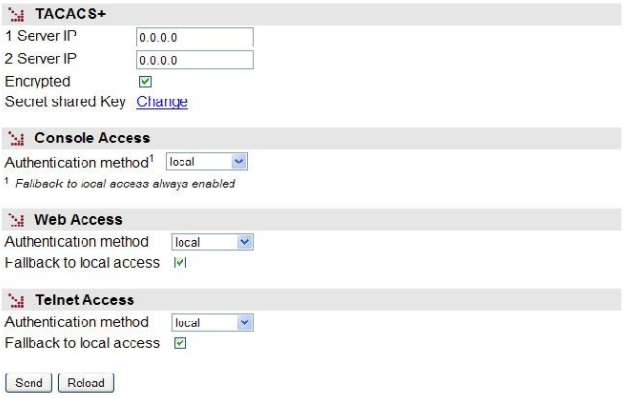
5.16 CONFIGURACIÓN ACCESS

El quipo ofrece varios medios de acceso al usuario: consola de servicio, acceso vía servidor http (web) y telnet.

Los usuario 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 autentificación remota que se usa para gestionar el acceso a servidores y dispositivos de comunicaciones, y proporciona servicios separados de autentificación, autorización y registro.

FIGURA 38 Menú *Access*



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.

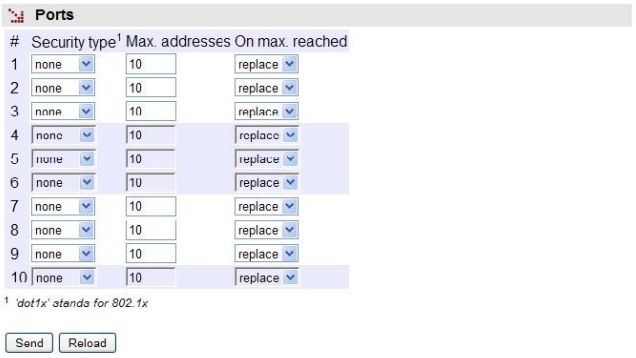
A continuación se hallan los parámetros asociados a cada opción de acceso (**consola**, **web access** y **telnet**), y que son los siguientes:

- **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.

5.17 CONFIGURACIÓN SECURITY

Este menú permite establecer restricciones de tráfico en función de las direcciones MAC de los clientes. El equipo únicamente cursará el tráfico cuando la dirección MAC esté incluida en la lista de autorizadas. Tanto la activación de la restricción como la lista se configura para cada puerto.

FIGURA 39 Menú *Security*

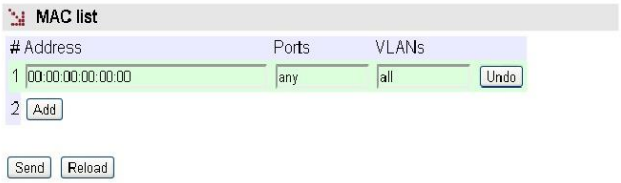


Los parámetros generales de configuración de los puertos son los siguientes:

- **#.** Identificador de interfaz física.
- **Security Type.** Establece si el servicio de filtrado por dirección MAC está activo en el puerto indicado (opción **maclist**) o no (opción **none**).

- **Max. Addresses.** Fija el número máximo de direcciones MAC permitidas de forma simultánea en el puerto indicado.
- **On max. reached.** Establece cual debe ser el comportamiento del equipo en caso de que se alcance el máximo número de direcciones MAC establecido en el parámetro anterior. Las opciones disponibles son **replace** o **restrict.**

FIGURA 40 Submenú *MAC list* del menú *Security*



Los parámetros para la creación de la lista de MACS son los siguientes:

- **#.** Identificador de elemento tabular. No es significativo.
- **Address.** La dirección MAC de cliente que se introduce en la lista.
- **Ports.** Puerto o puertos en que la dirección MAC será aceptada. Un conjunto de puertos discretos se configura con el identificador de cada uno de ellos separado por una coma, sin espacios. Si se desea la inclusión de un rango, el identificador del puerto inicial y del puerto final se separan con guión. El valor **any** significa que el puerto no es relevante.
- **VLANs.** Identificador numérico de las VLAN definidas en el equipo en las que la dirección MAC será aceptada (campos VID del menú VLAN). Un conjunto de vlans discretas se configura con el identificador de cada uno de ellas separado por una coma, sin espacios. Si se desea la inclusión de un rango, el identificador de la vlan inicial y de la vlan final se separan con guión. El valor **all** significa que la vlan no es relevante. (Ejemplo, en un equipo con la **vlan1**, **vlan3** y **vlan4** definidas, el conjunto de identificadores numéricos VID sería **1,3,4**).

La presencia de identificadores en el parámetro **Ports** y el apartado **VLANs** no son excluyentes.

5.18 REINICIO (*REBOOT*)

El equipo puede ser reiniciado mediante la ejecución del comando ***Reboot***, tanto mediante la consola como mediante las páginas HTML. El comando está disponible únicamente para el perfil administrador.

5.19 ACTUALIZACIÓN DEL CÓDIGO (*REFLASH*)

El equipo admite la actualización del software de aplicación mediante la ejecución del comando ***Reflash***, disponible únicamente mediante las páginas HTML y 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 como resultado de acceder al árbol de directorios de la máquina local 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.

6 ESTADÍSTICAS

El sistema proporciona estadísticas estructuradas en diez 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*).

El resto de las estadísticas se agrupan en torno a los datos perteneciente a las interfaces ethernet (*LAN*), VLANs, interfaces PLC si procede, interfaces WAN si procede, el encaminamiento (*Routing*), DHCP server, VRRP, VPN y el cliente de sincronización (*NTP*), accediendo a cada uno de ellos mediante la selección de la etiqueta correspondiente localizada bajo el epígrafe *Statistics*.

Cada una de las tablas de datos estadísticos se pueden 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, bien desde la consola, mediante la ejecución del comando ***clear*** en el prompt, bien mediante la opción de menú ***Clear Statistics***.

Ejemplo de estadística relativa a Datos Generales

General Statistics

Uptime	0d00:19:50.089
Time (UTC)	2005/01/01,00:00:00 Change
Time (Local)	2005/01/01,00:00:00 Change
Temperature	82 (C) / 180 (F)
Memory Usage (%)	13
Long term CPU Usage (%)	44
Short term CPU Usage (%)	46

Reload

Ejemplo de estadística relativa a VLAN

VLANs IP

#	Name	IP Address
1	vlan1	172.16.50.60

Reload

Ejemplo de estadística relativa a PLC

PLC interfaces

#	Port	MAC	Version	State
1	7	00:E0:AB:11:1F:98	INT6000-MAC-4-1-4102-04-3684-20091013-FINAL-B	connected
2	8	00:E0:AB:11:1F:99	INT6000-MAC-4-1-4102-04-3684-20091013-FINAL-B	connected

Reload

Ejemplo de estadística relativa a WAN

General Data

IMEI	356613020004370
IMSI	214016003227233
CID	893456011 1C0053565
PIN Status	READY
Active SIM	SIM B
Operator	"vodafone ES"
Roaming	H-PLMN
Network	GPRS
Local Area Code	69B5
Cell Identifier	583F
Signal Strength	-71 dBm
Total TX KBytes	0
Total RX KBytes	0
Number of Session failures	4
SIMA Tx Bytes	118
SIMA Rx Bytes	70
SIMB Tx Bytes	162
SIMB Rx Bytes	162

Current Data Session

Status	Inactive
IP Address	0.0.0.0
Connection Date	unknown
TX Bytes	0
RX Bytes	0
TX Rate (bps)	0
RX Rate (bps)	0

Previous Data Session

Disconnection Date	Thu Jul 21 12:12:20 UTC 2011
Up Time (s)	47
TX Bytes	0
RX Bytes	0

Reload

Ejemplo de estadística relativa a *Routing*

Routing Rules

#	Network	Gateway	I/F	Metric
1	default	172.16.50.254	vlan1	0

Reload

Ejemplo de estadística relativa a DHCP server

DNS Servers assigned by Network Carrier

DNS1 Server IP 0.0.0.0
DNS2 Server IP 0.0.0.0

Assigned leases

#	MAC Addr	IP Addr	Expiration time

Reload

Ejemplo de estadística relativa a VRRP

VRRP

VRRP virtual MAC	00:00:5E:00:00:xx
VRRP role	unknown
VRRP role Date	unknown
VRRP forced priority	original
VRRP forced priority Date	unknown

Reload

Ejemplo de estadística relativa a VPN

IP/GRE Tunnels

#	Remote router	Type	Tx Bytes	Rx Bytes

IPSEC Tunnels - ISAKMP Phase 1

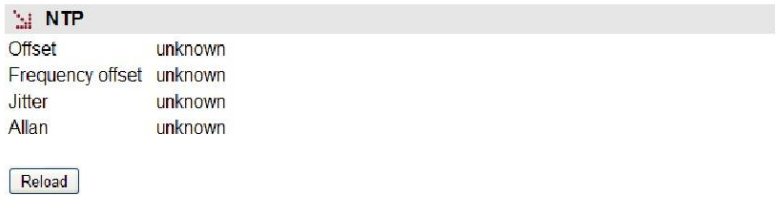
#	Remote router	Status	Status time

IPSEC Tunnels - Security Associations

#	Orig	Dest	Status	Status time	Bytes	Mode	Ciphering	Authentication

Reload

Ejemplo de estadística relativa a NTP



.

APÉNDICE A

BIBLIOGRAFÍA Y ABREVIACIONES

APÉNDICE A

BIBLIOGRAFÍA Y ABREVIACIONES

A.1 BIBLIOGRAFÍA

[1] IEEE RFC 1058. June 1988. Routing Information Protocol.
[2] STD 56. IEEE RFC 2453. November 1998. RIP Version 2 (Obsoletes RFC 1723, RFC 1388).
[3] STD 15. IEEE RFC 1157. May 1990. A Simple Network Management Protocol (SNMP).
[4] STD 62. IEEE RFC 3416. December 2002. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (Obsoletes RFC 1905).
[5] IEEE RFC 1305, March 1992. Network Time Protocol (Version 3) Specification, Implementation and Analysis.

A.2 ABREVIACIONES

ADSL	Asymmetric Digital Subscriber Line
APN	Access Point Name
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name Server
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HTB	Hierarchical Token Bucket
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol (Protocolo Internet)
IP Multicast	Extensión del Protocolo Internet para dar soporte a comunicaciones multidifusión
IPBX	Internet Protocol Private Branch Exchange (Centralita Privada basada en IP)
IPS	Intrusion Prevention System
IPSec	IP Security (Protocolo de Seguridad IP)
ISDN	Integrated Services Data Network (Red Digital de Servicios Integrados, RDSI)
ISP	Internet Service Provider (Proveedor de Servicios Internet, PSI)
ITSP	Internet Telephony Service Provider (Proveedor de Servicios de Telefonía Internet, PSTI)
LAN	Local Area Network
NAT	Netwok Address Translation

NHRP	Next Hop Resolution Protocol
NBMA	Non-Broadcast Medium Access
NMK	Network Management Key
NTP	Network Time Protocol
PPP	Point-to-Point Protocol (Protocolo Punto a Punto)
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network (Red de Telefonía Conmutada Pública)
QoS	Quality of Service (Calidad de Servicio)
RAS	Registration, Authentication and Status
RSVP	Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weight Fair Scheduling
WINS	Windows Internet Naming Service

.

APÉNDICE B

ESTRUCTURA DE DATOS EN *CLI*

APÉNDICE B

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***

B.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 puerto serie (puerto SRV).
- en modo remoto, mediante Telnet.

Acceso en modo local

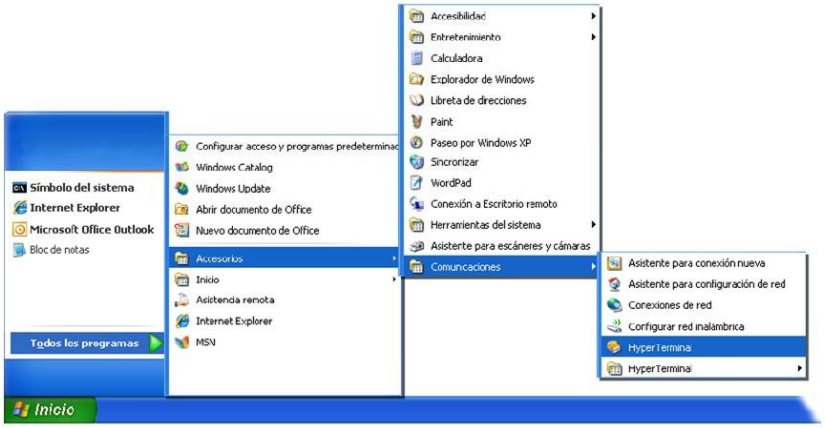
El acceso en modo local se realiza mediante un cable serie plano, conectando el puerto serie del ordenador al puerto serie del equipo (SRV).

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

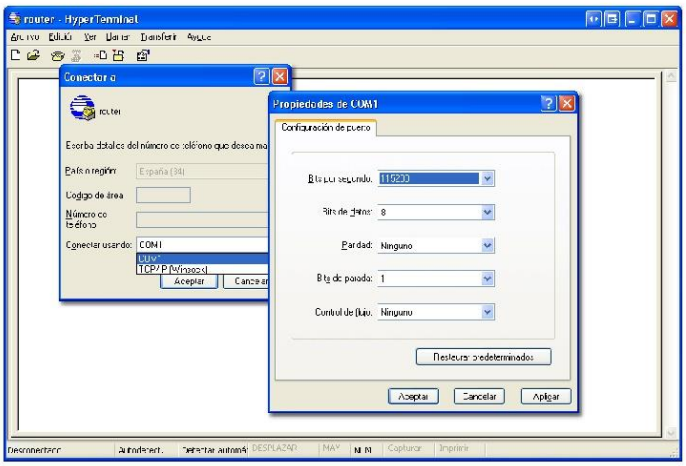
En Windows XP© se puede ejecutar *Hyperterminal* desde *Inicio* → *Todos los Programas* → *Accesorios* → *Comunicaciones* → *HyperTeminal* (véase FIGURA 41).

FIGURA 41 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 42).

FIGURA 42 Configuración de la conexión por puerto serie con *HyperTerminal*



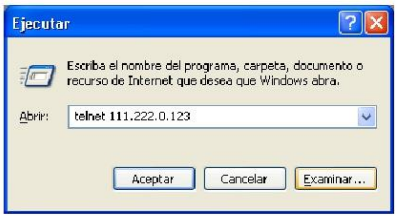
Acceso en modo remoto

El acceso en modo 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.

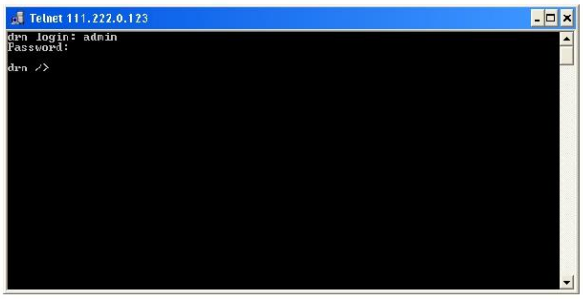
En Windows XP© se puede ejecutar Telnet desde el botón de inicio: Inicio → Ejecutar y, en la ventana de dialogo que aparece, escribir: telnet + espacio + Dirección_IP_del_equipo, pulsando, seguidamente, sobre el botón Aceptar (véase FIGURA 43).

FIGURA 43 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 con el programa Telnet conectado al equipo (véase FIGURA 44).

FIGURA 44 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*.

Sea cual sea el método elegido para establecer la conexión con el equipo, aparecerá el prompt ***equipo login:*** (donde *equipo* serán las 3 letras que lo identifican. *Ej.* ***dnr login:***) esperando a que introduzcamos el *login* de usuario y, posteriormente, la clave de inicio de sesión (los usuarios y sus respectivos passwords son los mismos que en la interfaz web).

B.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 2 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	✓	✗
download	Genera un fichero de comandos de configuración	✓	✓
Exit	Interrumpe la conexión con el equipo	✓	✓
get	Muestra los valores de los parámetros	✓	✓
help	Muestra la lista de comandos disponibles	✓	✓
Log / **Log all**	Muestran el listado de eventos	✓	✓
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	✓	✗
stats	Muestra el estado del equipo	✓	✓
telnet	Cierra la sesión de CLI sin interrumpir la conexión con el equipo	✓	✓

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

TABLA 3 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		

Comandos de configuración

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

Sintaxis: drn /> **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:
drn /> **add nat**
drn /wan> **add tunnel/túnel**
drn /admin> **add ../nat**

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

Sintaxis: drn /> **apply**

Argumentos: -

Observaciones: El uso de este comando es independiente del directorio en que nos encontremos.
Este comando NO guarda los cambios realizados.

Ejemplo: drn /> **apply**

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

Sintaxis: drn /> **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: drn /> **downdload**

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

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

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

Sintaxis: drn /> **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: drn /> **remove nat[2]**
drn /> **remove nat**
drn /admin> **remove ../nat**

restore Aplica la configuración de fábrica.

Sintaxis: drn /> **restore**

Argumentos: -

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

Ejemplo: drn /> **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: drn /> **save**

Argumentos: -

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

Ejemplo: drn /> **save**

set Modifica el valor almacenado en los parámetros de configuración o en los atributos de un ítem de un parámetro matricial.

Sintaxis: drn /> **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:
drn /main> **set hostname**
drn /> **set main/hostname**
drn /admin> **set ../main/hostname**
drn /> **set nat[2]/origin**

Comandos de Control

cd Cambia el directorio activo.

Sintaxis: drn /> **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: ***drn /main>***.

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

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

Sintaxis: drn /> **exit**

Argumentos: -

Observaciones: -

Ejemplo: drn /> **exit**

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

Sintaxis: drn /> **quit**

Argumentos: -

Observaciones: -

Ejemplo: drn /> **quit**

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

Sintaxis: drn /> **reboot**

Argumentos: -

Observaciones: -.

Ejemplo: drn /> **reboot**

reload Vuelve a cargar la configuración guardada en el equipo.

Sintaxis: drn /> **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: drn /> **reload**

telnet Cierra la sesión del programa CLI manteniendo abierta la conexión establecida entre el ordenador y el equipo.

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

Argumentos:

Host	Nombre del host de destino.
Port	*(opcional)* Número de puerto de destino.

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: drn /> **telnet drn**
drn /> **telnet 172.16.50.38 23**

Comandos de Estado y Diagnóstico

clear Borra las estadísticas.

Sintaxis: drn /> **clear**

Argumentos: -

Observaciones: -

Ejemplo: drn /> **clear**

date Muestra la fecha y hora registrada en el equipo.

Sintaxis: drn /> **date**

Argumentos: -

Observaciones: -

Ejemplo: drn /> **date**

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

Sintaxis: drn /> **help**

Argumentos: -

Observaciones: -

Ejemplo: drn /> **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: drn /> **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.

Ejemplo: drn /> **log**
drn /> **log all**

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: drn /> **ls**

Argumentos: -

Observaciones: -

Ejemplo: drn /> **ls**

ping Envía paquetes ICPM ECHO_REQUEST a un host determinado.

Sintaxis: drn /> **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:
drn /> **ping 172.16.50.38**
drn /> **ping emr**

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: drn /> **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:
drn /> **stats**
drn /> **stats main**
drn main/> **stats temperature**
drn main/> **stats ../lan/eth0/txbytes**

B.3 OBTENCIÓN DE INFORMACIÓN DEL ESTADO Y LA CONFIGURACIÓN DE UN EQUIPO

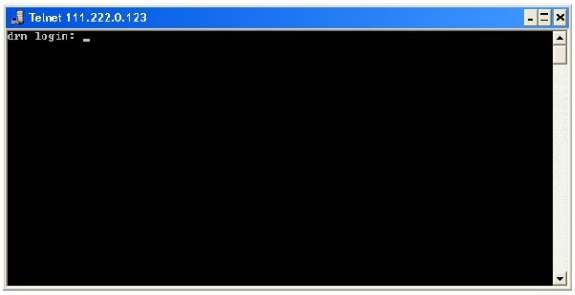
Para la obtención de información sobre el estado y la configuración de un equipo se deberán seguir los siguientes pasos:

1- Conexión con el equipo

Como se ha explicado en el capítulo **B.1**, la conexión con el equipo difiere ligeramente según el método de elegido. En este ejemplo se supone que el equipo es un ***DRA-2***, que está conectado a una red y que tiene una dirección IP configurada que, para este ejemplo, será 111.222.0.123. Así mismo, el ordenador utilizado para realizar la conexión también está conectado a dicha red y el S.O. utilizado es *Windows XP©*.

Para establecer la conexión mediante ***Telnet***, haremos clic sobre el botón de ***Inicio*** de *Windows XP©* y, una vez abierto el menú, sobre el comando ***Ejecutar***. En la ventana que aparece escribiremos "***telnet 111.222.0.123***" (sin las comillas) y pulsaremos sobre el botón ***Aceptar***.

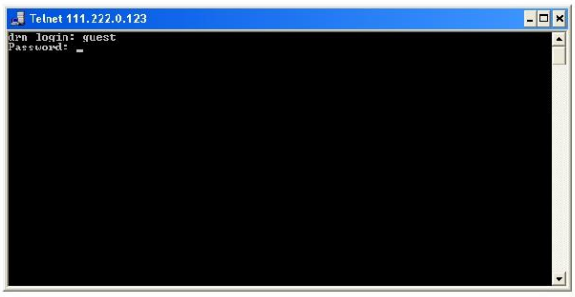
Si todo ha funcionado correctamente se abrirá una ventana de símbolo del sistema que será la interfaz de nuestra conexión.



2- Identificación del usuario

Al establecer la conexión con el equipo, el prompt ***drn login:*** indica que el sistema está esperado un nombre de usuario para la conexión con el quipo ***drn***.

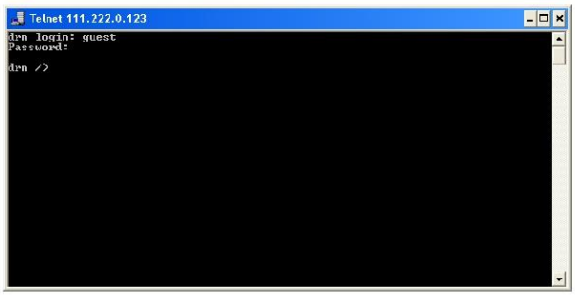
Como tan sólo deseamos obtener información, da lo mismo con que usuario se entre (***admin*** o ***guest***). Así, escribiremos ***guest*** y pulsaremos ***enter***



Ahora el sistema espera a que introduzcamos el password correspondiente. Así pues, escribiremos ***passwd01*** que es el asociado al usuario *guest* y pulsaremos ***enter***.

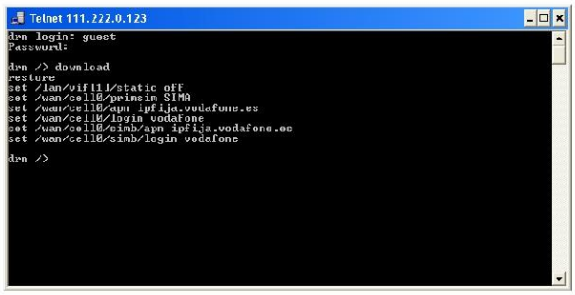
Hay que tener en cuenta que en la ventana de *Telnet* no aparece texto alguno mientras se introduce el password.

Si el usuario y password introducidos son correctos aparecerá el prompt ***drn />*** indicando que el equipo está a la espera de que se entre algún comando.



3- Obtención de la configuración del equipo

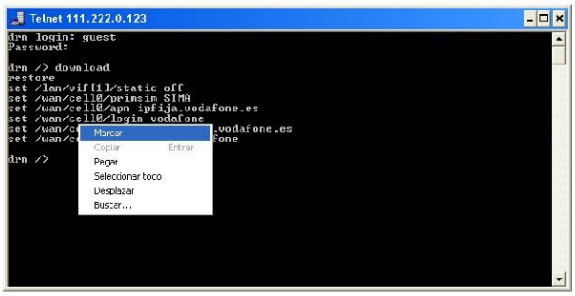
La configuración del equipo se obtiene mediante el comando ***download***. Al pulsar ***enter*** después de escribir este comando se mostrará la configuración completa del equipo.



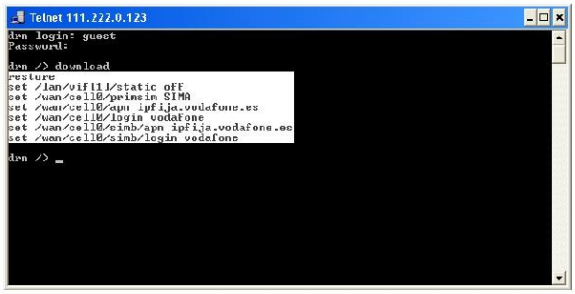
En el caso de que la información mostrada exceda de los límites de la ventana, el sistema sólo mostrará la información del principio y será necesario pulsar ***enter*** una o más veces hasta que se haya mostrado toda la información. Sabremos que el sistema a finalizado de mostrar toda la información cuando aparezca de nuevo el prompt del equipo: ***drn />***.

Es importante guardar la información obtenida mediante el comando *download* en un fichero *.txt* para poder utilizarla cuando se necesite.

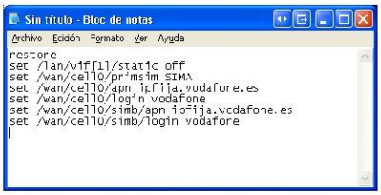
Para copiar texto desde la ventana de comandos de Windows XP© se deberá pulsar el botón derecho del ratón y del menú que aparece seleccionar ***Marcar***.



Seguidamente, colocaremos el cursor al inicio del texto que vamos a copiar, pulsaremos el botón izquierdo del ratón y, sin soltarlo, arrastraremos el cursor hasta que quede seleccionado todo el texto. Tras soltar el botón izquierdo pulsaremos la tecla ***enter***. De este modo, habremos copiado el texto seleccionado en el portapapeles de Windows.

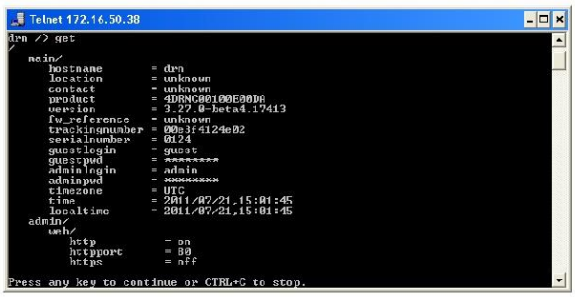


Ahora podremos abrir el *Bloc de notas* de Windows y pegar el texto (***Ctrl*** + ***V***) en un archivo *.txt* para guardarlo.



4- Obtención del estado del equipo

El comando ***get*** muestra el estado completo del equipo. Dado que la información a mostrar es muy extensa, cada vez que se llene la ventana, esperará a que el usuario pulse una tecla para continuar mostrando información.

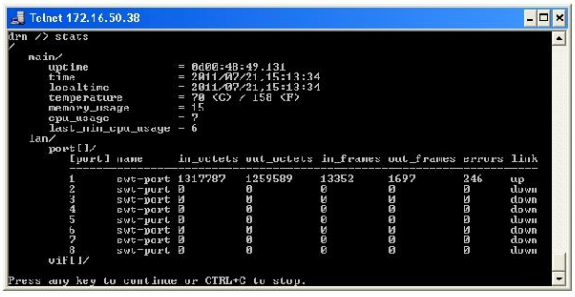


Sabremos que el sistema ha finalizado de mostrar toda la información cuando aparezca de nuevo el prompt del equipo: ***drn />***.

Al igual que con el comando *download*, resulta útil guardar la información, en un fichero *.txt*, con el método indicado anteriormente.

5- Obtención de las estadísticas del equipo

El listado de las estadísticas del equipo se muestra mediante el comando ***stats***.

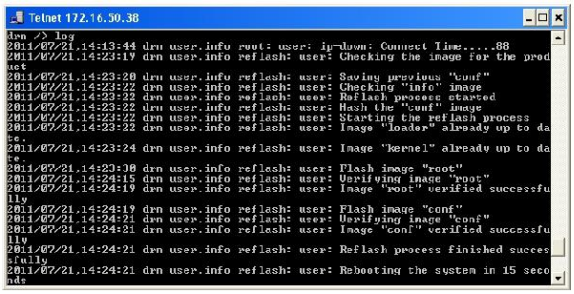


Al igual que los comandos anteriores, si la información a mostrar excede del tamaño de la ventana, se detendrá y esperará a que el usuario pulse una tecla para continuar.

Recuerde guardar la información, en un fichero *.txt*, tal como se ha indicado anteriormente.

6- Obtención de los eventos registrados en el equipo

El comando ***log*** permite consultar los eventos ocurridos en el equipo que, dada su importancia, han sido registrados en la memoria no volátil.



Recuerde guardar la información, en un fichero *.txt*, tal como se ha indicado anteriormente.

7- Obtención, en tiempo real, de los eventos ocurridos en el equipo

El comando ***log all*** permite consultar los eventos ocurridos en el equipo en tiempo real.

El listado de eventos se irá actualizando continuamente mientras el usuario no pulse la tecla ***enter***.

Recuerde guardar la información, en un fichero *.txt*, tal como se ha indicado anteriormente.

8- Listado de ejemplo del estado de un equipo obtenido mediante el comando get y guardado en un fichero .txt

```
drn login: guest
Password:

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

```
            maxretries              = 6
            maxtoconnect            = 6
            alarm_lowcov_level      = -105
            alarm_lowcov_period     = 300
            maxinsec                = 0
            dualsimenable           = off
            pin1                    = ********
            pin2                    = ********
            apn                     = ipfija.vodafone.es
            force_home              = off
            auth                    = pap
            login                   = vodafone
            passwd                  = ********
            minrxpower              = -113
            defroute                = on
            simb/
                pin1        = ********
                pin2        = ********
                apn         = ac.vodafone.es
                force_home  = off
                auth        = pap
                login       = vodafone
                passwd      = ********
                minrxpower  = -113
                defroute    = on
            dyn/
                enable    = off
                service   = dyndns
                host      =
                login     =
                passwd    =
                interval  = 86400
            pingkeep/
                remoteip   = 0.0.0.0
                remoteip2  = 0.0.0.0
                freq       = 5
                bytes      = 1
                count      = 2
                action     = none
                strict     = on
        tunnel/
            tunnel[]/
                [tunnel] iface description type ip     source remote_gw
remote_net
 enable
                ------------------------------------------------------------------
---
-------
                1          tun1                 gre   vlan1 vlan1   172.16.50.43 any
 on
    qos/
        qos2/
            weightfair_enable = on
            priority[]/
                [priority] queue
                ----------------
                0          medium
                1          medium
                2          medium
                3          medium
                4          medium
                5          medium
                6          medium
                7          medium
            dscp[]/
                [dscp] queue
                -------------
                0      medium
                8      medium
                16     medium
                24     medium
                32     medium
                40     medium
                48     medium
                56     medium
            port[]/
                [port] priority use_ieee8021p use_dscp
                ---------------------------------------
                1      0        on             off
                2      0        on             off
                3      0        on             off
                4      0        on             off
```

```
            5       0         on              off
            6       0         on              off
            7       0         on              off
            8       0         on              off
      qos3/
         classify/
            def_priority = medium
   routing/
      static/
         st_rules[]/
            [st_rules] dest                        gateway        service if
descr
            ------------------------------------------------------------------
---
            1           128.127.0.0/255.255.0.0 172.16.50.254 any      vlan1

      rip/
         enable             = on
         advertised_policy = permit
   filter/
      local/
         policy = accept
      cell0/
         policy = accept
      vlan/
         policy = accept
   dhcps/
      profiles[]/
         [profiles] name    lease dns1    dns2    wins    domain      tftp
  bootfile
         ------------------------------------------------------------------
---
----------
         1          profile 5000  0.0.0.0 0.0.0.0 0.0.0.0 usyscom.com
192.168.0.
1 bootfile
      servers[]/
         [servers] enable interface firstip      lastip         max_leases
mask
        gateway     profile
         ------------------------------------------------------------------
---
---------------------------
         1          off               192.168.0.10 192.168.0.254 100
255.25
5.255.0 192.168.0.1 profile
   vrrp/
      enable         = off
      advert_int     = 1
      if             = vlan1
      vid            = 1
      priority       = 100
      vip            = 192.168.0.1
      vmask          = 255.255.255.0
      preempt        = on
      preempt_delay  = 0
      auth_method    = none
      auth_passwd    = passwd02
      pingkeep/
         remoteip = 0.0.0.0
         gateway  = 0.0.0.0
         freq     = 5
         action   = none
   vpn/
      traffic/
         rules[]/
            [rules] tunnel_id local_net                  remote_gw
remote_net
               iskamp saname enable valid_in
            ------------------------------------------------------------------
---
-------------------------------------------
            1       ipsec1     172.16.50.0/255.255.255.0 77.211.25.76
172.17.90.0
/255.255.255.0 IKE1    TR1     on      cell0-0
         ike/
            ownidtype       = none
            ownidvalue      =
            nat_t           = off
            dpd_delay       = 10
```

```
          dpd_retry       = 10
          dpd_maxfail     = 3
          dpd_invcookies = off
          policy[]/
             [policy] name use_fqdn fqdn_value passive exchange cipher_alg
hash_a
lg auth_method    dh_group lifetime descr enable
             ------------------------------------------------------------------
---
-----------------------------------------------
             1        IKE1 disabled            off      main     des         md5
   pre_shared_key modp1024 86400    IKE1  on
          pshkeys/
             peer_keys[]/
                [peer_keys] peer_ip      key   enable
                ------------------------------------
                1           77.211.25.76 12345 on
          ipsec/
             sa[]/
                [sa] tunnel_id protocol cipher_alg hash_alg pfs  lifetime mode
                ------------------------------------------------------------
                1    TR1        esp       des         hmac_md5 none 6000     tunnel
   ntp/
          enable = off
          authkeys[]/
             [authkeys] keynumber key
             ----------------------------
             1          1         xxxxxxxx
          client/
             broadcastenable = off
             server[]/
                [server] ip           type    minpoll  maxpoll  authenable authkey
lowt
raffic
             ------------------------------------------------------------------
---
------
             1         192.168.0.1 unicast 5        10       off         1
off

   snmp/
          enable               = off
          trapenable           = off
          trap_v1_aggent_addr = none
          community[]/
             [community] name   access
             -------------------------
             1           public ro
          traps/
             cell_linkup  = off
             cell_covlow  = off
             cell_covhigh = off
   access/
          tacacsplus/
             server1_ip = 0.0.0.0
             server2_ip = 0.0.0.0
             encrypted  = on
             shared_key = ********
          console/
             method = local
          web/
             method = local
             local  = on
          telnet/
             method = local
             local  = on
   security/
          port[]/
             [port] type max_addresses max_action
             ------------------------------------
             1      none 10            replace
             2      none 10            replace
             3      none 10            replace
             4      none 10            replace
             5      none 10            replace
             6      none 10            replace
             7      none 10            replace
             8      none 10            replace

drn />
```

APÉNDICE C

ACOPLADORES PLC DE BANDA ANCHA

APÉNDICE C

ACOPLADORES PLC DE BANDA ANCHA

ZIV dispone de acopladores, capacitivos e inductivos, que permiten inyectar las señales de alta frecuencia moduladas por las interfaces BPLC/SSPLC del nodo DRA-2, que utilizan tecnología Powerline Communications (PLC), entre una fase de las líneas de Media Tensión y tierra.

La correcta adaptación de los Acoplamientos a las impedancias presentadas por los equipos de comunicaciones y por los cables de Media Tensión, en el rango de frecuencias utilizado por la Banda Ancha, es uno de los factores indicativos de las características de transmisión punto a punto entre subestaciones secundarias.

Los acoplamientos PLC de Banda Ancha están diseñados para cumplir los estándares eléctricos y permitir el acceso de las interfaces de comunicaciones a la red de Media Tensión con la seguridad requerida.

Se dispone de modelos que se adaptan a cada uno de los diferentes tipos de celda, siendo éstos:

ACA-500
Acoplador PLC de Banda Ancha capacitivo, para conector en T, apto para celdas de gas

CAMT-1
Acoplador PLC de Banda Ancha capacitivo, condensador de 2 nF, apto para celdas de aire y mampostería

CAMT-5

Acoplador PLC de Banda Ancha capacitivo, condensador de 500 pF, apto para celdas de aire y mampostería

AIMT-2

Acoplador PLC de Banda Ancha inductivo, sobre conductor, apto para celdas de gas, aire y mampostería

MVSD-2

Acoplador PLC de Banda Ancha inductivo, intrusivo, apto para celdas de gas, aire y mampostería

1.5 Generador de funcions 4087

Data Sheet

Programmable DDS Function Generator Series
Models 4084, 4085, 4086 & 4087

B&K Precision® models 4084, 4085, 4086 and 4087 are high performance laboratory grade synthesized function generators with a wide frequency range of up to 120 MHz. Direct digital synthesis (DDS) techniques are used to create stable, accurate output signals for all 27 built-in standard and complex (arbitrary) waveforms. The generators produce high purity, low distortion sine waves, square waves up to 40 MHz and provide a stable output of very small signals down to the 1mV - 10mV range. The instrument also provides a built-in 100 MHz universal counter with frequency measurement and totalize function.

The versatility and capabilities of this series make it an ideal tool for many general-purpose test and bench applications or for use in training and education.

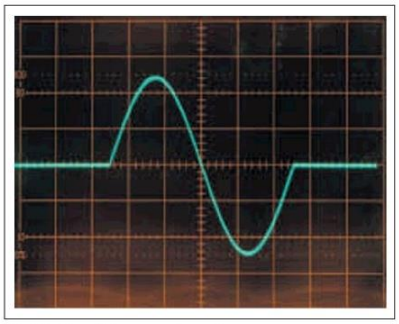


Fig.1 Single cycle burst, start phase=0°

Versatile modulation and trigger capabilities

The generators provide extensive modulation capabilities including AM, FM, FSK, PSK, pulse modulation and linear/logarithmic sweep. Internal and external modulation sources, as well as internal, external and gated trigger sources are supported. Modulation parameters can be set precisely and are adjustable over a wide range. For instance burst count is programmable in 1 burst increments up to 10000 bursts and burst phase is adjustable in 0.1° increments.

Convenient user interface and operation

You can adjust parameters via knob or numeric keypad. Enter amplitude values directly in Vpp, mVpp, Vrms, mVrms or dBm and display the correct voltage by entering the actual output configuration used (terminated with 50 Ohm or open circuit). You can enter frequency in terms of frequency or seconds using time values s, ms, Hz, kHz or MHz. Submenus are used for modulation modes and other complex functions. The generators are fully programmable via the standard RS232 interface, using SCPI commands. The instrument also provides 10 memories to store and recall instrument settings. Additionally the current state is saved at power off and can be restored at power up.

www.bkprecision.com

B&K PRECISION
ELECTRONIC TEST INSTRUMENTS

Specifications

Models	4084	4085	4086	4087
Frequency Characteristics				
Sine	1μHz ~ 20MHz	1μHz ~ 40MHz	1μHz ~ 80MHz	1μHz ~120MHz
Square	1μHz ~ 20MHz	1μHz ~ 40MHz	1μHz ~ 40MHz	1μHz ~40MHz
All Other waveforms	1μHz ~ 100kHz			
Frequency Stability	±1x10⁻⁶ (22°C ±5°C)			
Resolution	1μHz			
Accuracy	≤ ± 5x10⁻⁶ (22°C ±5°C)			
Data entry Units	s, ms, Hz, kHz, MHz			
Waveform Characteristics				
Main Waveforms (Sine, Square)				
Amplitude resolution	12 bits			
Sample Rate	200MSa/s			300MSa/s
Sine				
Harmonic Distortion of Sine Wave*	≤ - 50dBc (frequency ≤ 5MHz) ≤ - 45dBc (frequency ≤ 10MHz) ≤ - 40dBc (frequency ≤ 20MHz) ≤ - 35dBc (frequency ≤ 40MHz) ≤ - 30dBc (frequency > 40MHz)			
THD *	0.1% (20Hz ~ 100kHz)			
Square				
Rise and fall time*	≤ 15ns			
* = Note: Test conditions for harmonic distortion, sine distortion, rise/fall time Output Amplitude 2Vp-p, Environmental temperature: 25°C±5°C				
Others built-in waveforms				
27 build-in standard and complex waveforms	Sine, Square, Triangle, Positive Ramp, Falling Ramp, Noise, Pulse, Positive Pulse, Negative Pulse, Positive DC, Negative DC, Stair wave, Coded Pulse, Full wave rectified, Half-wave rectified, Sine transverse cut, Sine vertical cut, Sine phase modulation, Logarithmic, Exponential, Half-round, Sinx/x, Square root, Tangent, Cardiac, Earthquake, Combination			
Waveform Length	4096 dots			
Amplitude Resolution	10 bits			
Pulse				
Duty Cycle	0.1% ~ 99.9% (below 10kHz), 1% ~ 99% (10kHz ~ 100kHz)			
Rise/Fall Time	≤ 100ns (Duty Cycle 20%)			
DC signal characteristics				
DC range	≤ 10mV ~ 10V (high impedance)			
DC Accuracy	≤ ±5% of setting +10mV (high impedance)			
Arbitrary				
Non volatile memory	8 waveforms			
Waveform length	8~16000 points			
Amplitude resolution	10 bits			
Frequency range	1μHz~100kHz			
Sample rate	200MSa/s			
Amplitude Characteristics				
Amplitude Range				
For all models	Freq.≤ 40MHz: 2mV ~ 20Vpp (open circuit) , 1mV ~ 10Vpp (50Ω)			
4084, 4085, 4086	Freq. > 40MHz: 2mV ~ 4Vp-p (open circuit), 1mV ~ 2Vpp (50Ω)			
4087	Freq. > 40MHz: 0.1mV ~ 3Vpp (50Ω)			
Resolution	2μVpp (open circuit), 1μVpp (50Ω)			
Accuracy	± 1%+0.2mV (sine wave relative to 1kHz)			
Stability	±0.5 % /3 hours			
Flatness				
For amplitude ≤ 2Vpp	±3% (freq≤ 5MHz), ±10% (5MHz<freq≤ 40MHz)			
For amplitude >2Vpp:	±5% (freq≤ 5MHz), ±10% (5MHz<freq≤ 20MHz) ±20% (frequency>20MHz) ±1dBm (frequency>40MHz)			
Output Impedance	50Ω			
Output Units	Vpp, mVpp, Vrms, mVrms, dBm			
DC Offset Characteristics				
Offset Range (open circuit)	Freq.≤ 40MHz: ±10Vpk ac+dc (Offset ≤ 2 x pk - pk amplitude) Freq. > 40MHz: ±2Vpk ac+dc (Offset ≤ 2 x pk - pk amplitude)			
Offset Resolution	2μV (open circuit), 1μV (50Ω)			
Offset Error	±5% of setting +10mV (Ampl. ≤ 2Vpp into open circuit) ±5% of setting +20mV (Ampl. > 2Vpp into open circuit)			

Modulation	
AM Characteristics	
Carrier Waveforms	Sine or Square
Modulation Source	Internal or external
Internal Modulating Waveform	Sine, Square, Triangle, Rising/Falling Ramp
Frequency of modulating signal	100μHz ~ 20kHz
Distortion	≤ 2%
Modulation Depth	1% ~ 120%, 1% ~ 80% (frequency>40MHz, Ampl > 2Vpp into open circuit)
Modulation Error	± 5%+0.2% (100μHz < frequency ≤ 10kHz) ±10%+2% (10kHz < frequency ≤ 20kHz)
Max. Amplitude of ext. input signal	3Vp-p (-1.5V~ +1.5V)
FM Characteristics	
Carrier Waveforms	Sine or Square
Modulation Source	Internal or external
Internal Modulating Waveform	Sine, Square, Triangle, Rising/Falling Ramp
Frequency of modulating signal	100μHz ~ 10kHz
Deviation	Max. 50% of carrier frequency for internal FM Max 100kHz (carrier frequency≥ 5MHz) for external FM, with input signal voltage 3Vp-p (-1.5V~+1.5V)
FSK Characteristics	
Carrier Waveform	Sine or Square
Control Model	Internal or external trigger (external: TTL level, low level F1, high level F2)
FSK Rate	0.1ms ~ 800s
PSK Characteristics	
Carrier Waveform	Sine or Square
PSK	Phase1 (P1) and Phase 2 (P2), range: 0.0 ~ 360.0°
Resolution	0.1°
PSK rate	0.1ms ~ 800s
Control Mode	Internal or external trigger (external: TTL level, low level P1, high level P2)
Burst Characteristics	
Waveform	Sine or Square
Burst Counts	1 ~ 10000 cycles
Time interval between bursts	0.1ms ~ 800s
Control Mode	Internal, single or external gated trigger
Frequency Sweep Characteristics	
Waveform	Sine or Square
Sweep Time	1ms ~ 800s (linear), 100ms ~ 800s (log)
Sweep Mode	Linear or Logarithmic
Start/ Stop Frequency	Same as frequency range of Sine & Square
External trigger signal frequency DC	~ 1kHz (linear) DC~10Hz (log)
Control Mode	Internal or external trigger
Inputs/ Outputs	
Main Output	
Impedance	50Ω
Protection	Short circuit and overload protected
Output MOD OUT	
Frequency	100Hz ~ 20kHz
Waveform	Sine, Square, Triangle, Rising/Falling Ramp
Amplitude	5Vp-p ± 5%
Output Impedance	600Ω
Modulation IN	3Vpp = 100% Modulation
External Input Trig/FSK/Burst	Level - TTL
Universal Counter, Key Specs*	
Frequency Range	
Frequency Measurement	1Hz ~ 100MHz
Totalize mode	50MHz max
* For full specification of the counter section, refer to online manual at www.bkprecision.com	
General	
Power Supply	198~242V or 99~121V, Frequency: 47~ 63Hz
Power Consumption	<35VA
State Storage Memory	
Storage Parameters	frequency, amplitude, waveform, DC offset values, modulation parameters
Storage Capacity	10 user configurable stored states
Dimensions (W x H x D)	10" x 3.93" x 14.56" (255 x 100 x 370) mm
Weight	6.6 lbs (3 kg)
Remote Interface	RS232
Safety designed according to	EN61010
EMC tested according to	EN55022, EN55024, EN61326, EN601000

Three Year Warranty

Included Accessories: BNC to alligator cable, BNC to BNC cable, RS232 communication cable, power line cord, test report, spare fuse

1.6 Analitzador PERSEUS

PERSEUS RECEIVER
USER MANUAL

Microtelecom s.r.l. – Pavia di Udine, Italy

- Document version EN13 -

INDEX

1. RECEIVER DESCRIPTION

PERSEUS is a software defined VLF-LF-MF-HF, 10 kHz – 30 MHz, communication receiver based on an outstanding direct sampling digital architecture and with the capability of recording up to 800kHz of RF spectrum.

It features a 14 bit 80 MS/s analogue-to-digital converter, a high-performance FPGA-based digital down-converter and a high-speed 480 Mbit/s USB2.0 PC interface.

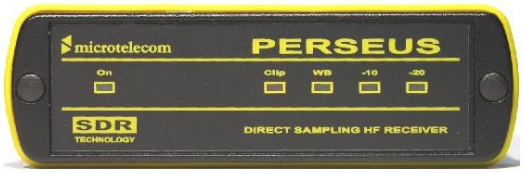
The PERSEUS receiver analogue front-end has been carefully designed for the most demanding users and includes a 0-30 dB attenuator, in 10 dB steps, a ten bands preselection filters bank, and a high dynamic preamplifier with a top-class input third-order intercept point of more than 30 dBm.

The receiver is designed to operate on a PC under Microsoft Windows 2000, XP, or Vista operating systems.

The antenna connection is a BNC female socket. The power source is an universal 100/240 Vac 50/60 Hz wall socket adapter which provides the required +5Vdc (+/-5%) power supply to the receiver.

Audio source is via the PC soundcard/ on board audio. Best results are heard by feeding the PC audio through a good amplifier and speakers systems, rather than the standard speakers bundled along with most PCs.

1.1 FRONT PANEL



On - Receiver status.
The receiver detects the connection to the PC USB Host Controller. When the PC is turned off or if the receiver is not connected to a USB port, an internal circuit disables the receiver and put it in an OFF state.

Clip - ADC Clip.
The ADC clip indicator signals that the input signal level is exceeding the capability of the receiver.

WB - Wide Band Mode.
It indicates that the receiver is operating in wide band mode (no RF preselection filter inserted in the signal path)

-10 - 10 dB RF attenuator status.
The indicator activates when the 10 dB attenuator is inserted.

-20 - 20 dB RF attenuator status.
The indicator activates when the 20 dB attenuator is inserted.

1.2 REAR PANEL

RF input
BNC type 50 Ohm antenna input socket. For best performance connect the receiver to a suitable 50 Ohm external antenna system.

+5V – 1A
Regulated receiver power supply socket. Use the receiver only with the wall adapter provided with the receiver. Improper voltage power supplies may seriously damage the receiver.

USB 2.0
USB 2.0 Cable socket. Connect the receiver to a PC USB 2.0 port with the cable provided with the receiver.

2. USB DRIVERS INSTALLATION

To install the Perseus USB Drivers on your system:

1) Insert the CD which came with the Perseus, into the CD/ DVD ROM drive on the PC,

2) Connect the Perseus receiver to the wall power adapter,

3) Connect the USB cable to a spare USB2.0 socket of the PC and then to the Perseus receiver.

Please note that the Perseus receiver detects the connection to the PC, and its power supply is internally disabled when the receiver is not connected to a PC, or when the PC is powered off.

Windows XP detects the new hardware and begins the installation procedure. NB. These messages may differ slightly, depending on which version of the Windows operating system is used.

This screen may be seen, depending on the version of Windows used. The software "asks" to log on to the Windows update site. Tick "No not at this time" and click "next".

By default the above screen has the "Install Software automatically" box ticked. Click next.

Windows XP informs the user about the status of the Windows Logo testing of the USB drivers provided with the software. Click "Continue Anyway".

Allow the software driver installation to set up automatically

The USB drivers are now installed.

3. SYSTEM REQUIREMENTS

- 2 GHz Pentium IV CPU with 512 MB RAM (for 125 KS/s, 250 KS/s and 500 KS/s)
- 2.5 GHz Dual Core CPU with 1 GB RAM (for 1 MS/s and 2 MS/s operations)
- USB2.0 High-Speed (480 Mbit/s) port
- 16 bit AC-97 compatible audio board
- 1024 x 768 minimum resolution video board and monitor
- 2 Button mouse with wheel
- 10 GB or more internal hard-disk
- Supported OS: Windows 2000 SP4, Windows XP SP2, Windows Vista

NB: The above is a guide only. The Perseus receiver may operate on machines with a lower specification, but performance can not be guaranteed.

4. OPERATING THE RECEIVER SAFELY

WARNING! Failure to observe the following instructions could seriously damage the receiver:

- USE ONLY THE POWER SUPPLY PROVIDED WITH THE RECEIVER

- DO NOT CONNECT THE ANTENNA CONNECTOR OF THE RECEIVER TO THE ANTENNA CONNECTOR OF A TRANSCEIVER/TRANSMITTER

- DO NOT CONNECT THE RECEIVER TO AN ANTENNA WHICH IS NEAR AN ANTENNA SYSTEM CONNECTED TO A HIGH POWER TRANSCEIVER/TRANSMITTER, I.E. A HIGH RF FIELD

5. LATEST SOFTWARE RELEASE

The latest software release is available for download on the internet at the address:

http://microtelecom.it/perseus/software

Release notes are provided at the same address or in the distributed software.

6. OPERATING THE PERSEUS SOFTWARE

Copy the folder with the latest release of the PERSEUS software from the installation CD (or from the latest download, see below) to the PC hard drive. Any user preferred location is fine, e.g. simply onto the desktop, or "out of the way" in for example "My Documents" or on a storage partition.

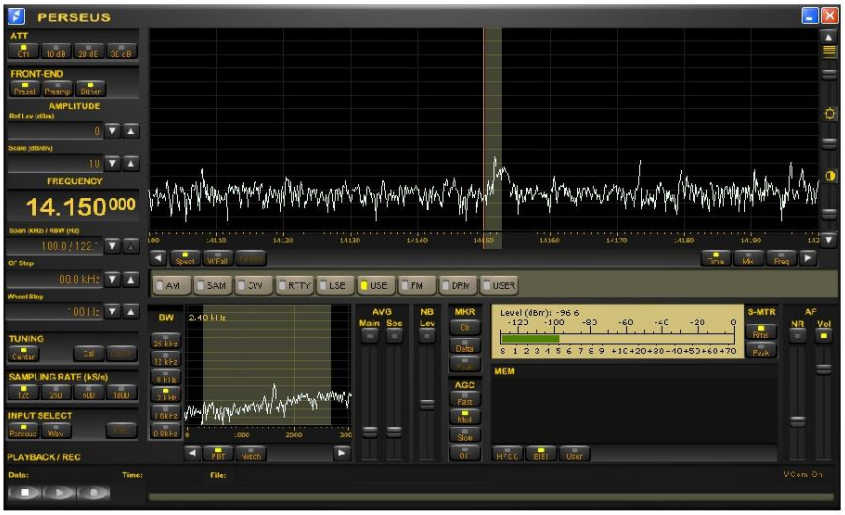
To activate the PERSEUS receiver, "run" the receiver operating software, "perseus.exe" file. (Double click, or right click - open to run.)

SHORTCUT: To create a single click shortcut for the PC desktop, right click "Perseus.exe" and click on create shortcut. "Right click" the shortcut, and "cut". Then right click on the desktop, and "paste" the shortcut. (This is only one way to create a shortcut. The user may also use for example, the quick launch toolbar)

The operating software is free standing, and does not install any files to the hard drive, once the drivers are installed. User settings are stored in the windows registry.

Connect a suitable antenna and click on the new shortcut. Audio heard from the PC speakers should now be from the PERSEUS SDR receiver.

NB: If recording a wideband piece of spectrum, remember that a tuned antenna will not work, eg using an ATU or a MW loop, which peaks on a single frequency.



Perseus operating software default screenshot

6.1 TUNING THE RECEIVER

Tuning is probably the most important function in any receiver. There are many ways to tune the Perseus SDR:

1) Frequency Pane - "mouse over"
2) Frequency Pane - "direct entry"
3) CF step
4) Frequency bar - "dragging" or "mouse over"
5) Secondary BW window and the many adjustments within
6) Main Spect / WFall screen - "mouse over" and "mouse click"

6.1.1 MOUSE OVER FREQUENCY PANE

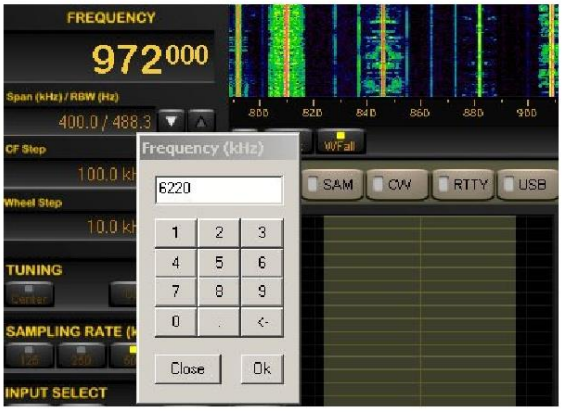
Hovering the mouse over any of the digits (except 10 MHz) on the "frequency pane", and turning the mouse scroll wheel changes frequency. This is perhaps the most convenient way of tuning the PERSEUS SDR quickly over a large area of the spectrum.

NB: Frequency changes depend on which digit the user hovers over. In the image below, "1" in 1530 represents 1MHz. Therefore hovering over "1" and turning the wheel changes frequency by 1MHz at a single wheel click. Mouse over "5" changes frequency by 100kHz per click etc. The frequency will count upwards continuously (or downwards for that matter). If the mouse is hovered over "3" (30kHz) below, and clicked upwards past 9, the next digit will clock up to "6", ie 600kHz.

The Frequency Pane

6.1.2 DIRECT ENTRY ON THE FREQUENCY PANE

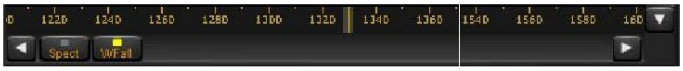
Double clicking on the "frequency pane" brings up a frequency input window, allowing the user to manually enter a desired frequency. This may be typed directly in to the space at the top, or "mouse clicked" via the numbered buttons below.



The direct frequency entry box pops up just below the main frequency box.

6.1.3 CF STEP

White horizontal arrows either side of the "Spect / WFall" select bar (below the frequency bar), tune the receiver up/ down by user selected step, eg 500kHz or 1MHz at a time.



The frequency bar. Below are white arrows either side for CF step

CF Step choices are 1MHz, 500, 400, 200, 100, 50, 25, 20, 10, 5, 2 and 1kHz. The buttons to set the CF step are two panes below the frequency. (See above images)

Span, CF step, and Wheel Step

Different steps will be useful to different users. One example could be that a MW dxer is recording a bandwidth of 400kHz just before the top of the hour, to find station ids. He (or she) may wish to move up or down the band by 400kHz to try and capture a completely different set of station ids. (Possibly at the end of the news at 5 minutes past the hour) The dxer could stop the initial recording, and in only one click, move 400kHz down the band to begin recording again quickly.

6.1.4 FREQUENCY BAR DRAGGING OR MOUSE OVER

Dragging: Frequency can be tuned by dragging the frequency bar (see above) located below the main spec / waterfall window. Hold the left mouse button down and drag.

Mouse over: If the mouse wheel is turned while the pointer is over the frequency bar, the receiver will tune in "wheel steps" in the same fashion as "mouse over" the main spect/ waterfall window. This step is set in the "wheel step" pane.

6.1.5 FILTER BANDWIDTH PANE

The Filter bandwidth Pane close up

The function buttons within the BW pane are "PBT", "NOTCH", and "BW" buttons.

When the "PBT" (Pass Band Tune) mode is selected there are many functions within the Bandwidth pane:

a - Double left click to centre the signal carrier
b - Left drag to fine tune the signal
c - Rotate the wheel to adjust the selectivity filter bandwidth
d - Drag the two filter edges independently
e - Tune via the "wheel step" arrows
f - Right drag to emulate passband tuning

a) DOUBLE LEFT CLICK: Double click on the waveform in the BW pane, to centre the carrier.

b) LEFT MOUSE CLICK AND DRAG: Left click, hold and drag within this window, to drag the frequency around, in a "fine tuning" mode.

c) BANDWIDTH: The bandwidth is continually variable from 25kHz to virtually zero on the PERSEUS. The buttons may give the impression of fixed bandwidth, with settings of 25, 12, 6, 3, 1.6 and 0.8kHz. This is not so however. Hover the mouse over the shaded area within the BW pane, and turn the mouse wheel. The selected area which is shaded will be seen to be continually variable. If very narrow bandwidth is required, choose a lower selection, like 1.6, or 0.8, and it is possible to reduce the bandwidth to virtually zero. Using a lower setting not only "magnifies" the screen, but also switches in different filters.

d) DRAG THE FILTER EDGES INDEPENDENTLY: Left mouse click, hold and drag to "grab" the edges of the shaded area independently of each other, to manually increase or decrease the bandwidth. A small arrow appears on the red line when this adjustment is being made. This can be useful for example if there is an interfering signal on one of the sidebands only.

e) TUNE VIA "WHEEL STEP ARROWS": The white arrows either side of the tune notch and PBT buttons act as a tuner up and down in the steps assigned by the "wheel step" function.

f) PASSBAND TUNING: PERSEUS has a right click function within the BW pane, which moves the whole selected part of the window around. Right click and hold the shaded area, to drag left or right. This is the SDR emulation of Passband Tuning, as there is no real PBT in a zero IF single conversion receiver like Perseus.

In the example below, PERSEUS is tuned to 1070kHz, Canadian MW station CBC Moncton. There is QRM from 1071kHz from UK Talk Sport. If the emulated Pass Band Tuning is used, the shaded filter area is right clicked, held and dragged to the left, away from the carrier of Talk Sport. CBC is then heard free of interference.

The freq centred on 1070 (left), but using PBT the QRM vanishes (right)

6.1.6 NOTCH FILTER

This function can "notch" out a selected carrier, or area of spectrum close by the desired signal. The above PBT example worked well with CBC 1070, and the Euros on 1070. An excellent example of the notch filter's use is as follows. Again a MW example. Until early 2008, many dxers noticed an unidentified carrier on around 1181kHz. If a European Dxer wishes to listen to WHAM 1180 from Rochester, NY, the PBT as per the example above could be used to drag the filter hf to get rid of the Euros on 1179. But what of the unidentified carrier hf of the desired signal. The notch filter can completely eliminate this unwanted menace.

Notch functions are activated selecting the "Notch" button in the Bandwidth pane or, performing the following action holding the Ctrl-key when in "PBT" mode:

ACTION	EFFECT
Double left mouse click	Place notch at the selected frequency
Drag with mouse left btn clicked	Tune notch filter to desired frequency
Mouse wheel	Adjust notch filter width
Right click	Disable notch filter

6.2 MAIN SPECTRUM/WATERFALL WINDOW

The main Waterfall / Spect window allows operation of many functions associated with direct tuning.

6.2.1 MOUSE OVER & WHEEL STEP

The centre of the SDR Receiver is the Spectrum / Waterfall screen (which ever mode the user chooses). Hover the mouse over anywhere within the main Spect / WFall window, and turn the mouse wheel. This will step the receiver up or down by the amount defined in the "wheel step" pane. The options are 25, 12.5, 10, 9 and 5kHz, as well as 100hz and 1hz!

Common examples for dxers include 9kHz steps for dxing European MW stations, or 10kHz for The Americas. The 5kHz step is ideal for SW/ HF broadcast band dxing.

NB: This is a very convenient method of zipping up and down the band for both MW dxers (steps of 9 or 10kHz), and SW dxers (in 5kHz steps).

6.2.2 DIRECT CLICK

Double click directly onto a wave or waterfall line and the receiver will jump straight to the frequency selected, to the nearest full 1kHz (no decimal places).

6.2.3 DIAL POINTER

The receiver has a dial pointer which spans the main Spect/ Waterfall window vertically on the frequency to which the receiver is tuned. The user can left click, hold and drag the "dial pointer" to change frequency, but only as long as the "CENTER" button in inactive. This is another way to move up and down the frequency spectrum quickly.

Dial pointer in spectrum mode in conjunction with the settings in BW pane

The pointer is present on the Spectrum view, and on "mouse over the tuned frequency" in the waterfall mode. The pointer changes in conjunction with adjustments made in the BW pane, and is physically as wide as the selected bandwidth, as seen within the BW PANE.

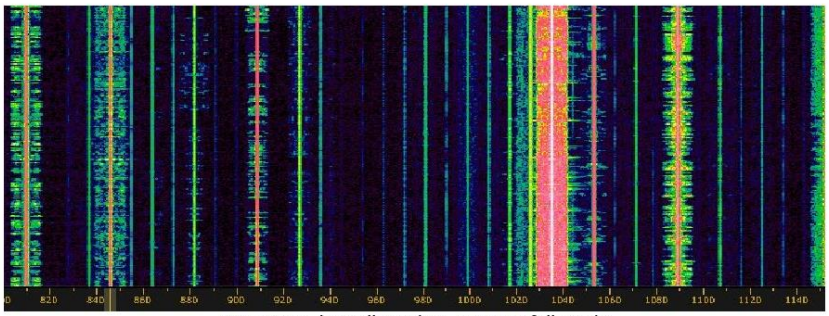
6.2.4 TUNING: Center button – active

This button keeps the tuning dial pointer in the centre of the frequency scale. If a waterfall line is double clicked when the Center button is active, the frequency scale moves along, and the whole waterfall will move along. (The user may lose track of which waterfall line is which, till the screen catches up) If the "center" function is activated, the "tuning pointer" will not move from the centre of the screen.

"Center" button inactive

6.2.5 TUNING: Center button – inactive
The user can click anywhere on the waterfall, or spectral screen, and the receiver jumps to the new frequency without moving the whole waveform/ waterfall. The pointer will also move, and can be dragged across the frequency spectrum.

There are various functions related to the main window other than direct tuning, see above.



Main Spect/ WFall window in Waterfall mode

6.2.6 SPAN
This is the bandwidth displayed within the main waterfall/ spectral pane.
The selections available are 800kHz, 400kHz, 200kHz, 100kHz, 50kHz, 25kHz, 12.5kHz & 6.3kHz, 3.1kHz.
A 1.6kHz span is available only when the receiver sampling rate is set to 500kHz or less.
A 0.8kHz span is available only when the receiver sampling rate is set to 250kHz or less.
A 0.4kHz span is available only when the receiver sampling rate is set to 125kHz.

"Span" box

SPAN could also be described as increasing the magnification on the Spec/ Waterfall screen. This function can be used on playback as well as live listening. SPAN is directly related to the sampling rate setting. The waterfall can not show 400kHz if for example the receiver is only sampling 250kHz at the time. (Or is playing back a recording of 200kHz of spectrum)

6.2.7 WATERFALL CONTROLS

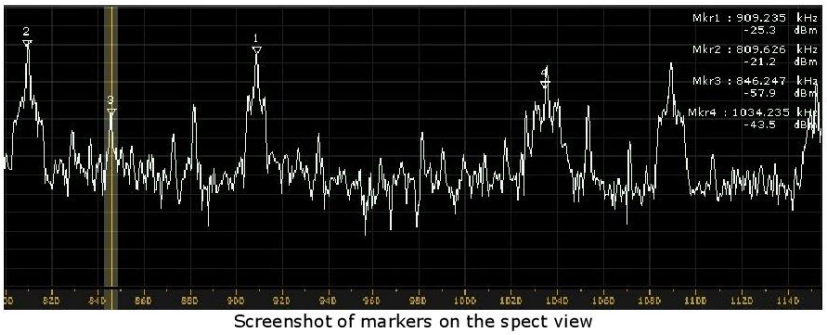
Speed/Contrast/Brightness: The three scroll bar to the right of the waterfall pane slows/speeds up the waterfall, and allow changes waterfall brightness and contrast.

Colour palette: The waterfall colour palette can be selected in the palette dialog which is activated pressing the Palette button in the main spectrum window control bar.

All the waterfall controls are disabled when in Spectrum mode.

6.3 MARKERS

A right mouse click feature is available within the spect/ waterfall pane. Right click on up to four frequencies, and a small arrow appears. In waterfall mode, the arrow is situated where the signal waveform would be on the spect view. On the spect view, the arrows are situated where the mouse was right clicked. The screenshot below shows the numbered arrows, relating to Mkr1-Mkr4 in small text on the top right. The frequency and signal in dBm is also given.

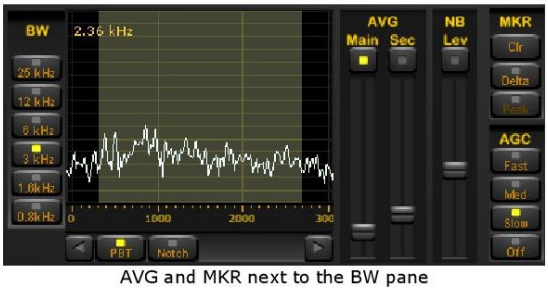


Screenshot of markers on the spect view

Clr. This button clears the Mkr arrows from the spect/waterfall display.
Delta. This button changes the values from the markers 2, 3 and 4 to delta values (Different to MRK 1)
Peak. This function is not enabled on the current software version.

6.4 SPECTRUM AVERAGE

AVG Main. Stabilizes the spectrum waveform in the main spect/waterfall display. Will also stabilize the waterfall mode**.** The main spectrum average function and its slider control are active only when the the enable button above the slider is enabled.
AVG Sec. Stabilizes the spect waveform in the secondary "bandwidth" display/ pane. The secondary spectrum average function and its slider control are active only when the the enable button above the slider is enabled.



AVG and MKR next to the BW pane

6.5 RECORDING / PLAYBACK

The biggest attraction to PERSEUS is the record feature. Technology has advanced enough to enable the PERSEUS SDR to record a massive 800kHz of the RF spectrum, and play back the file at a convenient time, with all the desired features of the receiver still available to optimise reception, eg bandwidth, mode, passband tuning, etc. This spectrum record function has particular interest to DXers whose main focus is MW or Tropical Bands, though not of course exclusively.
Perseus can record a spectrum bandwidth of 800, 400, 200, or 100 kHz. This is selected from the SAMPLING RATE buttons. The SAMPLING RATE buttons actually select the sampling rate at the output of the receiver digital down converter, accordingly to the following table:

Sampling Rate	REC/PLAY Bandwidth
(Ksample/s)	(KHz)
125	100
250	200
500	400
1000	800

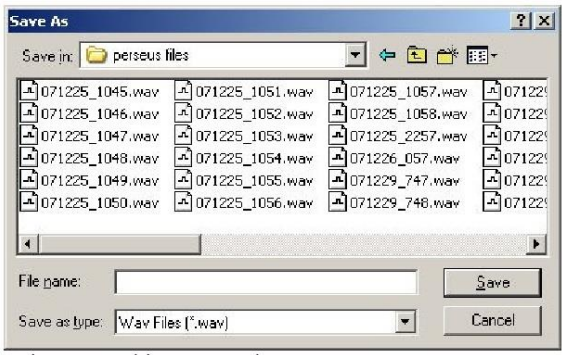
Sampling rate pane

The PERSEUS will record up to a maximum of 10 minutes (5 minutes when the selected sampling rate is 1000 KS/s), before automatically creating a new (.wav) file. After 10m (5 m @ 1MS/s) a new file is created with the same name "plus 1". 080117_2308.wav file is the example below. The next file becomes 080117_2309.wav. The file size of an automatic 10m recording is around 1.757GB at 400kHz, 878MB at 200kHz, and 439MB at 100kHz of spectrum recorded.

STOP, PLAY and RECORD buttons, and PROGRESS BAR at the bottom

6.5.1 RECORDING

To record from the PERSEUS, select the chosen frequency limits required in the main window, by dragging the frequency bar. Click on the record button, which is third from the left at the bottom of the screen. A new window pops up asking for a user defined file name and folder location to store the file (see below). As seen in the example above, the file may be named to include the date and time, for ease of finding. The example above is called 080117_2308, meaning the file was recorded on January 17th 2008, at 2308UTC. The Perseus software takes the file time from the computer clock, so it is a must that the PC clock be kept accurate. The software also displays how much free space is left on the hard drive. In the case above, 371.14 GBytes are free.



File name and location window pops up on pressing RECORD

Note: While recording, it is NOT possible to tune around beyond the frequency limits of the spectrum being recorded, eg the user can not check a SW frequency while recording say 560 - 960kHz. The same of course stands for playback. It is not possible to tune beyond the recorded frequencies.

6.5.2 PLAYBACK

To play back a file which has been recorded at an earlier time, click on the "Wav" button, within the "INPUT SELECT" pane. The PERSEUS stops receiving live signals and the "Wav" and "File" buttons are now activated. Click "File" and browse on the PC to the location of the pre recorded file(s). Then simply press the PLAY button. These buttons are similar to those found on most domestic DVD players and video recorders.

If the receiver has created numerous automatically named files, PERSEUS will playback the whole series of files if required. This playback should be continuous and flawless, even during track/ file change. The PERSEUS software will playback .wav files which have been copied to a DVD equally as flawlessly.

The input select pane

During playback, the Perseus software will display date and time in the same format as during recording. Therefore so long as the PC clock has been kept accurate during recording, so too will the playback time.

A PC clock sometimes becomes wildly out of time, especially in the mid winter cold of a radio shack. This also means that windows automated file date of creation will be wrong. A replacement back up battery on the PC motherboard may be required if the clock goes off time frequently.

NB: Playback is restricted to the PERSEUS hardware being connected and running on the PC. The software will not activate if the PERSEUS is not connected to the PC.

6.5.3 MOVING FORWARD AND BACK DURING PLAYBACK

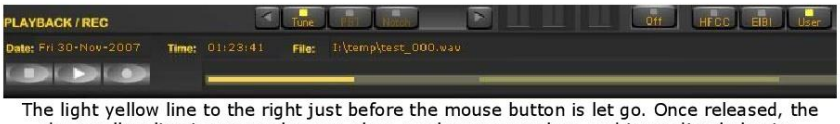
Since version 1.0, single left click anywhere on the progress bar to advance to a chosen point of the recording.

To loop the playback over a smaller selection, simply left click and hold at the desired spot on the progress bar. Drag the mouse pointer along to the right to create a new line, which will be a much paler shade of yellow, almost see through. Let the mouse button go, and playback immediately begins from the new desired spot. This should be flawless and instant. The player will repeat the new selected section only over and over until stopped. This may be useful if the user wishes to repeat a possible station ID over and over again.

A left click on the line cancels the new selection, and returns the playback to the beginning of the file.

NB: The progress bar differs slightly in operation from common progress bars in WINAMP, or WINDOWS MEDIA PLAYER for example.

Troubleshooting: If the user fails to create a new line, but only "clicks" to attempt to advance playback by a few minutes, the software may seem to "stick". The player is probably only playing back a very small selected area over and over again, and hence the impression of "stuttering and jamming".



The light yellow line to the right just before the mouse button is let go. Once released, the deep yellow line jumps to the new place on the progress bar, and immediately begins playback from the new point.

6.6 OTHER CONTROLS

A detailed description of the other controls on the software control panel, beginning at the top left of the screen:

6.6.1 Attenuator (ATT)

Like on a conventional receiver, the attenuator reduces signal input. This may be useful if a user has problems with strong local signals appearing on frequencies other than their own, eg from a local radio ham, or local MW station.

6.6.2 Preselection filters (Presel)

This control inserts the receiver preselection filters. It is very useful when very strong out of band interfering signals may saturate the A/D converter. Eg, if the user is tuned to MW, while a radio amateur very close by is active on 160 or 80metres, and breaking through. Switch in the Preselector in this instance to prevent or reduce overloading.

6.6.3 ADC Preamplifier (Preamp)
This control enables the preamplifier built in the A/D converter. When activated, the ADC improves the receiver sensitivity by about 2 dB at the expense of a slightly inferior blocking dynamic range. It may be difficult to notice any real difference when broadcast listening signals are very strong, and atmospheric noise is far beyond the receiver's own noise level.

6.6.4 ADC DITHERING (Dither)
This control enables the A/D converter dither generator and the reduces the amplitude of its spurious signals. Spurious responses are improved at the expense of the receiver sensitivity (about 2 dB). Users may have this function "always on" unless tuned for example to a very quiet 10m band.

ATT and FRONT-END controls

6.6.5 AMPLITUDE (Reference level and Scale)
Both "ref level" and "scale" alter the height and position of the spectrum waveform displayed when the Spectrum mode on the main panel is selected as well as the spectrum waveform in the secondary "bandwidth" window.

6.6.6 MODE BAR
The reception mode buttons (AM, SYNC AM, CW, RTTY, USB, LSB, FM, DRM, USER) are placed along the centre of the screen.

DRM demodulator. The demodulation of DRM signals requires a Virtual Audio Cable (VAC) software interface, and an external DRM decoder like i.e. the Dream software application.

USER demodulator. When the user demodulator is selected the receiver VAC (Virtual Audio Cable) output is fed with zero-IF IQ samples, filtered with the selected bandwidth and normalized in amplitude with the selected AGC setting. This mode is useful when a third party application wishes to process the zero-IF data stream at the selected frequency.

The MODE bar

6.6.7 VOLUME AND MUTE (AF Vol)

Volume control is on the bottom right of the software, though many users prefer to use the volume on their external amplifiers. The button above the Volume slider enables the audio output and mutes it when disabled.

6.6.8 NOISE REDUCTION (AF NR)

The NR control reduces background noise and is activated by the button above its slider control. The NR slider controls the amount of noise reduction. The noise reduction can be activated in all modes except with DRM and USER demodulators.

6.6.9 NOISE BLANKER (NB)

The NB control reduces impulsive noise and is activated by the button above its slider control. The NB slider sets the threshold of the noise blanker. Care should be exercised when strong signals are present in the band where the receiver is tuned. A too low NB threshold (NB slider at or near its maximum position) may affect the quality of the tuned signal and introduce intermodulation distortions.

6.6.10 SIGNAL STRENGTH METER

The signal strength meter (S meter) is marked in both S points and dBm (S9=-73 dBm input). The S meter response is very linear thorough all its scale and accurate to within less than 1 dB across the range.

LOCK indication. When operating in Sync AM mode (SAM), a small "LOCK" display appears in the top right of the meter, when the demodulator locks on to the AM carrier.

ADC CLIP indication. A red ADC clip mark appears in the S meter when the input signal strength is higher than the receiver input clipping level. When this happens the receiver A/D converter operates in a non linear mode and may introduce high intermodulation distortions. In this case it is necessary to switch on the attenuator until the ADC CLIP mark disappears.

The S meter can be operated in RMS mode (input signal RMS power displayed) or in Peak mode (input signal peak power displayed) clicking the "RMS" or "Peak" at the right of the S meter.

6.6.11 AUTOMATIC GAIN CONTROL (AGC)

The Automatic Gain Control keeps the audio output at a constant output level, disregarding the input signal power. Three time decay constants can be selected with the buttons "Fast", "Med", and "Low" in the AGC control bar.
The AGC can be excluded with the "Off" button. In this case the audio output level is controlled by the Volume slider. When the AGC is off large input signals can cause the saturation of the audio output. Better DRM signals reception is achieved with the AGC in the "slow" position.

6.6.12 FREQUENCY CALIBRATION

To calibrate the frequency scale of the Perseus receiver the following procedure should be performed:

- **a.** Tune to a WWV signal at 10 MHz or 5 MHz,
- **b.** Select "Center" in the "Tuning" control window,
- **c.** Select the 0.8kHz filter in the "BW" window,

d. Double click the WWV carrier in the Secondary Spectrum Window to exactly center it at a 0 Hz offset (before double clicking it will appear at some offset from the center due to the finite precision of the Perseus reference oscillator),
e. Click "Cal" on the "Tuning" control panel.

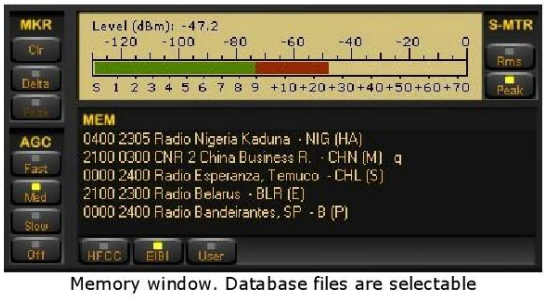
In the case the calibration has to be repeated, click CalClr and repeat the above procedure. With some experience you can calibrate the clock with a precision which is much higher than the clock stability itself.

The Cal button is active only when in "Center" tuning mode.

6.6.13 Memory window (MEM)

In the memory window the receiver software can display three lists of active broadcasting stations at the selected frequency. The lists contents are based on the data contained in the HFCC, in the EIBI and in an optional USER database. The memory window shows only the broadcast stations which are active, according to the records contained in these databases, at the UTC time they are transmitting.

There are three function buttons associated with the memory window: "HFCC" "EIBI" and "USER". The receiver software displays information from the "HFCC" and "EIBI" on line frequency databases. The user can produce his own personal USER database. The USER database file should be named "userlist.txt", have the same format of the EIBI database, and kept within the Peseus software folder.



Memory window. Database files are selectable

As seen in the example above, when a frequency listed in the database is tuned, the entries are displayed in the MEM window. Station names appear if the tuning frequency is within +/- 500 Hz of the frequency listed in the database. Stations scheduled at 1200UTC for example, do not show in the MEM window at 2100UTC. Time and day of the week of stations appearing in the window match time and date displayed by the PC clock (day of the week is not checked in the EIBI database).

HFCC (High Frequency Co-Ordination Conference) database.

Perseus software requires 3 files:

1) hfcc.txt
2) broadcas.txt (not a misprint, this is the file name, kept to 8 characters)
3) site.txt

The main HFCC database is available on the internet at the address:
http://www.hfcc.org/data/index.html
The databases names have a prefix formed by a letter and two digits which code the seasons and the year of the edition validity. The "A" letter marks Spring/Summer editions, the "B" letter marks Fall/Winter editions. I.e. the archive A08ALL00.ZIP is the 2008 Spring/Summer edition. To update the HFCC database used by the Perseus software, download the new archive, unzip the archive in a separate folder, rename the file XNNALL00.TXT (X=A or B, NN=Year) to hfcc.txt, and copy the new hfcc.txt, broadcas.txt and site.txt files in the Perseus software folder overwriting their older version.

The EIBI database file is available on the internet at the address:
http://www.eibi.de.vu/

To update the EIBI database used by the Perseus software download the frequency sorted version from the above address. The EIBI file is named with the same convention used by the HFCC (freq-XNN.txt, where X=A or B and NN=Year). The file should be renamed "eibi.txt" and copied into the Perseus software folder.

Text files within the PERSEUS folder:

1) hfcc.txt
2) broadcas.txt
3) site.txt
4) eibi.txt
5) userlist.txt (only if a user file is required)

NB: Names of any updated text files should be changed and copied into the Perseus software folder, where the operating software is stored. Allow the old files to be overwritten. If the file names are left as original, the operating software will not recognise them.

If the user tries to rename the database file to "eibi.txt" without knowing if his file extensions within Windows are hidden, the real file name may end up as "eibi.txt.txt" and the file will not be recognized by the Perseus software.

6.7 FACTORY DEFAULT SETTINGS

The Perseus software stores all the user settings in the Windows registry.

To reset the Perseus software to its factory default, you need to delete the key stored in the Windows registry by the Perseus software as follows:

1) Close the Perseus software

2) Type "regedit" in the Windows Start/Run menu and browse the registry tree for the key:

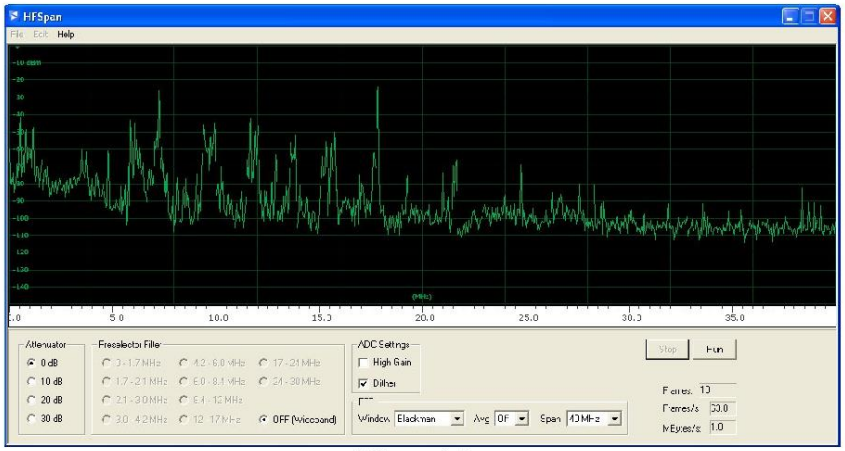
   HKEY_CURRENT_USER/Software/Microtelecom s.r.l./perseus

3) Delete the folder "v1.0f" to reset the software version v1.0f settings to its factory default (or the appropriate version if newer. If preferred, the full "microtelecom s.r.l." can be deleted)
4) Restart the Perseus software.

7. HFSPAN UTILITY

HFSpan is a stand alone spectrum analyser, which is included along with the PERSEUS operating software. HFSpan will display 10, 20 or the maximum 40MHz spectrum.
The frequency bar can be dragged when the bandwidth is set at 10 and 20MHz.

To start HFSpan double click (or right click and open) "HFSpan.exe". The PERSEUS operating software does not run in conjunction with the HFSpan software.



HFSpan window

8. TECHNICAL SPECIFICATIONS

Frequency Coverage	10 kHz – 30 MHz
Modes	SSB, CW, AM, S-AM, FMNB, etc. (Software Defined)
Sensitivity	0.49 uV (SSB, S+N/N= 10 dB, Preamp ON, Dither OFF)
Selectivity	Software Defined (>100 dB Stop Band Attenuation)
Image Rejection	90 dB
Input IP3	31 dBm
Dynamic Range (IMD3) (CW)	102 dB @ 7.050 MHz, 2 kHz Spacing
	100 dB @ 14.150 MHz, 2 KHz Spacing
Blocking Dynamic Range (CW)	124 dB (CW, Dither OFF)
Blocking Dynamic Range (SSB)	117 dB (SSB, Dither OFF)
Minimum Detectable Signal (CW)	-125 dBm
	-129 dBm (Preamp ON, Dither OFF)
	-131 dBm (Presel OFF, Preamp ON, Dither OFF)
Minimum Detectable Signal (SSB)	-118 dBm
	-122 dBm (Preamp ON, Dither OFF)
	-124 dBm (Presel OFF, Preamp ON, Dither OFF)
Input Clipping Level	-3 dBm (Preamp OFF), -6 dBm (Preamp ON)
Attenuators	0, 10, 20, 30 dB
RF Preselection Filters Bank	LPF Filter: 0-1.7 MHz. BPF filters (1.7-30 MHz):
	0-1.7, 1.7-2.1, 2.1-3.0, 3.0-4.2, 4.2-6.0,
	6.0-8.4, 8.4-12.0, 12-17, 17-24, 24-32,
	OFF (0-40 MHz Wide-Band Mode)
PC Interface	High-speed 480 Mbit/s USB2.0 port
DDC Output Sampling Rate	125 Ks/s, 250 Ks/s, 500 Ks/s, 1 MS/s, 2 MS/s 24 bit/sample IQ
DDC Output Bandwidth	100/200/400/800 kHz (>120 dB Alias Rejection) 1600 kHz (> 110 dB Alias Rejection)
Power Supply Requirements	+5Vdc +/-5% - 700 mA
Cabinet: Aluminium Enclosure	110 x 36 x 185 mm (W x H x L)
Operating Temperature Range	0-40 °C
Frequency Accuracy	+/-1 ppm after calibration
Weight	380 g

All specification are measured at 14.15 MHz, with Preselector ON, Preamp OFF, and Dither ON, unless otherwise indicated, CW bandwidth = 500 Hz, SSB bandwidth = 2400 Hz.

9. EUROPEAN COMMUNITY CE CONFORMITY

Microtelecom s.r.l. declares that the Perseus receiver complies with the European Community EMC standards:

ETSI EN 300 330-1
ETSI EN 300 489-1
ETSI EN 300 489-15

Compliance reports are available upon written request to Microtelecom s.r.l.

10. FCC PART 15 COMPLIANCE

The Perseus receiver is labelled with the identifier:

FCC ID V75-RC8014V11

11. INFORMATION TO THE USER (FCC Part 15 - §15.21 and §15.105)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

Caution! Modifications to this device not expressly approved by Microtelecom s.r.l. could void the user's authority to operate the equipment.

The Perseus receiver is made in Italy

12. DISPOSAL OF YOUR OLD APPLIANCE

DIRECTIVE 2002/96/EC (WEEE)

1. When this crossed-out bin symbol is attached to a product it means that the product is covered by the European Community directive 2002/96/EC.

2. All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or by the local authorities.
3. The correct disposal of your old appliance will help prevent potential negative consequences for the environment and the human health.
4. For more detailed information about the disposal of your old appliance, please consult your city office, waste disposal service or the shop where you purchased the product.

Microtelecom s.r.l. – S.S. n.352 Km. 3,600 – 33050 Pavia di Udine – Italy