



ENCAPSULADOR SERIE A IP TIPO CIC



MANUAL DE USUARIO

V03 - Junio 2018

M0CIC1806EV03

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

Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: ziv@zivautomation.com

www.zivautomation.com

SÍMBOLOS DE SEGURIDAD



ADVERTENCIA O PRECAUCIÓN:

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



NOTA:

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

ÍNDICE

	Pág.
1	INTRODUCCIÓN 5
1.1	GENERALIDADES 5
1.2	INTERCONEXIONES ENTRE PUERTOS 8
1.3	MODELOS DISPONIBLES 11
1.4	ESPECIFICACIONES TÉCNICAS 11
1.4.1	Interfaces del equipo 11
1.4.2	Protocolos de encapsulamiento 12
1.4.3	Gestión del equipo 12
1.4.4	Servicios adicionales 12
1.4.5	Accesorios 12
1.4.6	Certificaciones 13
1.4.7	Características de los puertos de datos serie asíncronos (DCE) 13
1.4.8	Características de los transductores de fibra óptica 13
1.4.9	Características de la interfaz WAN opcional 14
1.4.10	Características mecánicas 14
1.4.11	Condiciones de funcionamiento 14
2	CARACTERÍSTICAS MECÁNICAS Y ELÉCTRICAS 15
3	SEÑALIZACIÓN DE LOS LEDS 22
4	ACCESO AL EQUIPO 25
4.1	CONSOLA 25
4.2	SERVIDOR HTTP 26
5	CONFIGURACIÓN Y GESTIÓN 28
5.1	PARÁMETROS GENERALES 29
5.1.1	Identificación del equipo 30
5.1.2	Control de acceso 30
5.1.3	Otros 31

	Pág.
5.2 ADMINISTRATION	31
5.3 CONFIGURACIÓN LAN	32
5.4 CONFIGURACIÓN PUERTOS SERIE	33
5.5 CONFIGURACIÓN WAN	35
5.6 CONFIGURACIÓN RUTAS ESTÁTICAS	43
5.7 CONFIGURACIÓN FILTERING	45
5.8 CONFIGURACIÓN DHCP SERVER	48
5.9 CONFIGURACIÓN SNMP	49
5.10 CONFIGURACIÓN NTP	51
5.11 CONFIGURACIÓN ACCESS	52
5.12 CONFIGURACIÓN DE LOS FLUJOS DE DATOS	54
5.12.1 Protocolos de encapsulado	54
5.12.2 Connection	62
5.12.3 Policy	65
5.12.4 Other	67
5.13 CONFIGURACIÓN DEL PUERTO SERIE COMO <i>ModemEmulator</i>	68
5.14 REINICIO (REBOOT)	71
5.15 ACTUALIZACIÓN DEL CÓDIGO (REFLASH)	71
6 ESTADÍSTICAS	72
APÉNDICE A	
BIBLIOGRAFÍA Y ABREVIACIONES	77
APÉNDICE B	
ESTRUCTURA DE DATOS EN CLI	82

1 INTRODUCCIÓN

1.1 GENERALIDADES

El CIC es un encapsulador serie a IP con un mayor número de puertos de acceso que el encapsulador serie a IP tipo SIP.

El CIC dispone de dos posibles dotaciones en cuanto a número de puertos serie, un puerto serie base con interfaz RS-232/RS-485 y cuatro u ocho puertos serie RS-232 adicionales. El puerto base siempre opera con conector SUB-D de 9 contactos, mientras que los puertos serie adicionales se ofrecen bien con conectores SUB-D de 9 contactos o transductores de fibra óptica, en grupos de cuatro.

En cuanto a la interfaz de red, el equipo dispone de dos interfaces Ethernet que operan como parte de un switch Ethernet de dos puertos, 10/100Base-Tx ó 100Base-Fx.

El equipo permite habilitar el encaminamiento de tráfico, es decir, puede operar como un router de nivel 3.

Todos los puertos serie están configurados como **DCE** (Data Communications Equipment).

Opcionalmente, el CIC puede equiparse con un dispositivo de red WAN GPRS o UMTS.

CIC

FIGURA 1

Encapsulado serie a IP sobre interfaz cableada

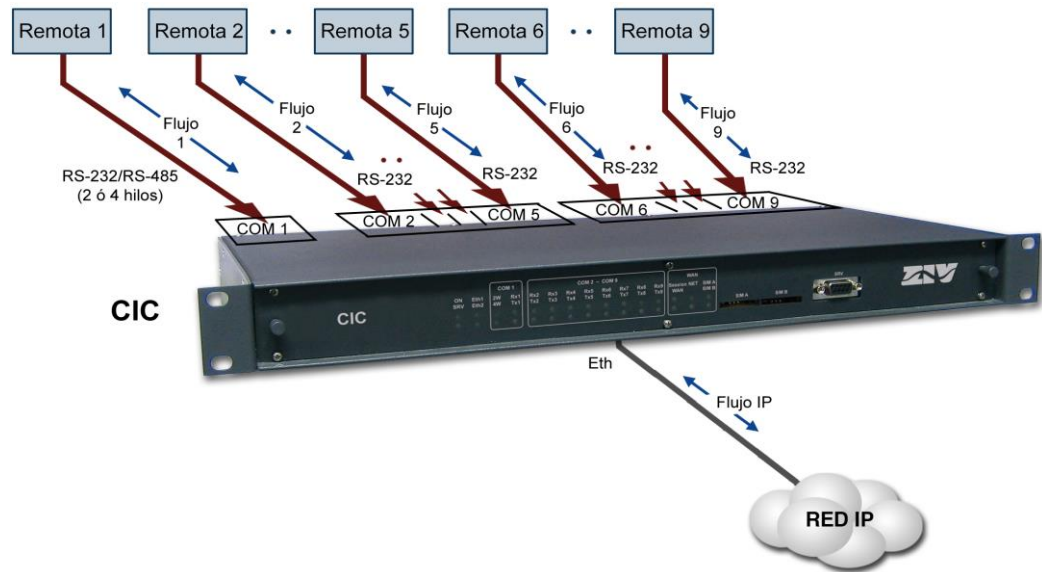


FIGURA 2

Ejemplo de aplicación del CIC

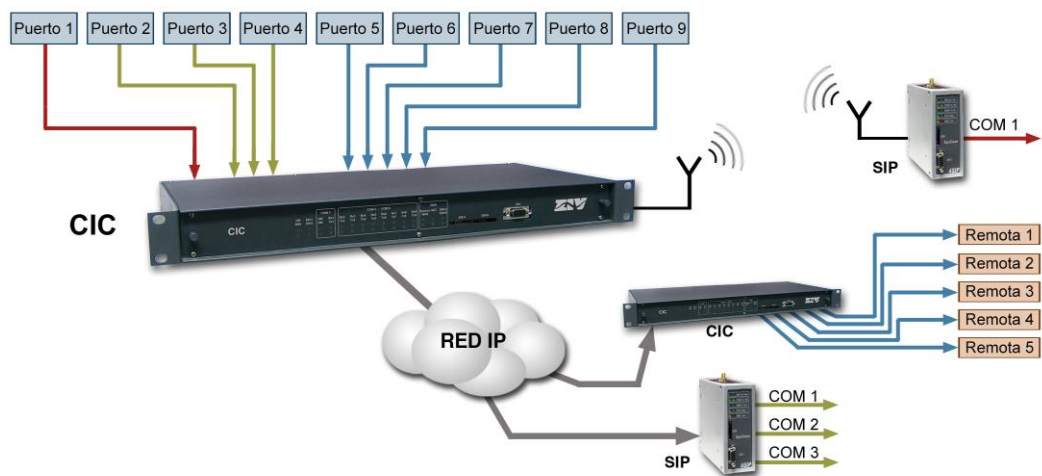


FIGURA 3

Ejemplo de aplicación de encapsulado serie a IP



El CIC es accesible de forma local y remota, bien mediante consola local, servidor Telnet y servidor SSH, o a través de un servidor web incorporado, HTTP.

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

La función básica de encapsulado es la de crear una conexión punto a punto, equivalente a una conexión directa entre dos dispositivos serie, aún cuando realmente el transporte de los datos se realiza sobre una red TCP/IP.

La función de encapsulado garantiza la entrega libre de errores de los datos aceptados en uno de los puertos serie de un extremo, y con el orden inalterado, en el otro extremo de la conexión. A esta funcionalidad normalmente se la denomina como PAD (Packet Assembler-Disassembler).

La función de encapsulado no depende del contenido de los datos de usuario. El equipo admite dos modalidades de procesado con la función PAD: directa o con empaquetado.

A pesar de que la función básica de un encapsulador es la ejecución de los procesos PAD, el equipo CIC dispone de los procedimientos necesarios para realizar un encapsulamiento inteligente de forma que, para una serie de protocolos específicos de Telemedida y Telecontrol, procesa los datos como unidades de transmisión de nivel superior. De este modo, las operaciones sobre los datos no se limitan a su mera transmisión, sino que se identifican posibles errores, o bien el CIC es capaz de identificar distintos flujos de datos en un único canal compartido y transportarlos hacia destinos diferenciados (demultiplexación).

Algunos de los protocolos soportados son IEC 60870-5-101/102/103, DLMS, GESTEL, DNP3.0, PROCOME, SAP20, MODBUS, Pid1, Twc, etc.

Otra característica adicional para cualquiera de los modos de operación del encapsulador, es la capacidad del CIC de ofrecer el comportamiento de un módem HAYES básico hacia el equipo cliente, de modo que el establecimiento de las conexiones punto a punto del encapsulador se realizan bajo demanda y con el destinatario determinado por la aplicación o equipo cliente. La operación en modo HAYES se habilita de forma independiente para cada uno de los puertos serie presentes en el CIC.

1.2 INTERCONEXIONES ENTRE PUERTOS

El equipo, aparte de disponer de los puertos serie, a los que denominamos **puertos físicos**, opera con recursos que son conexiones TCP/UDP y que se emplean para el encapsulado de los datos sobre las redes TCP/IP; a estas conexiones TCP/UDP las denominamos **puertos virtuales**, por contraposición a los puertos tangibles.

La operación básica del equipo consiste en determinar las características de los puertos, tanto los físicos como los virtuales, y establecer a continuación las "conexiones" entre ellos, lo que en la práctica fija los extremos entre los que se realiza el transporte de los datos encapsulados.

Por otro lado, si el equipo dispone de la interfaz WAN opcional, se dispondrá de un puerto virtual adicional asociado a la llamada de datos GSM, pudiéndose establecer una conexión entre dicho puerto virtual y un puerto serie.

A continuación, para una mejor comprensión a la hora de abordar la configuración del CIC accediendo a las páginas HTML del equipo, se describen las operaciones principales que deben llevarse a cabo para realizar **interconexiones entre puertos físicos (COM) y puertos virtuales (TCP/UDP)**. Es aconsejable efectuar las operaciones que se indican y en el orden en que aparecen.

Para información más detallada sobre los menús de configuración y sus parámetros, consúltese el capítulo 5.

1. Configurar los parámetros de los puertos serie. Para ello, acceder al menú **Serial** (véase apartado 5.4 para más información).

El menú **Serial** consta de dos apartados bien diferenciados: **Physical** y **Logical**.

En el apartado **Physical**, configurar los parámetros básicos de funcionamiento de los puertos COM (velocidad, bits de datos, paridad y bits de stop).

En el apartado **Logical**, configurar el protocolo de encapsulado o bien el uso de una política de encapsulado (opción *policybased*) y un identificador para la misma. La configuración de la política (*policy*) propiamente se lleva a cabo desde el submenú **Policy** del menú **Flow**.

La identificación de cada puerto COM, es decir, el nombre, se lleva a cabo en el apartado **Physical Ports** de la pantalla de configuración del menú **Flow**.

2. Crear y configurar los parámetros de los puertos virtuales TCP/UDP. Para ello, acceder a la pantalla de configuración del menú **Flow** (véase apartado 5.12 para información más detallada).

La pantalla de configuración del menú **Flow** consta de dos apartados bien diferenciados: **Physical Ports** y **Virtual ports**.

En el apartado **Physical Ports**, establecer para cada puerto COM un nombre distinto e inequívoco.

Por defecto, todos los puertos tienen configurado el nombre *serial0* y, por tanto, es imprescindible asignarles un nombre específico a cada uno.

Por otro lado, si el equipo dispone de interfaz WAN; para que la conexión serie-llamada de datos (GSM) sea efectiva, en el parámetro *Datacall*, la casilla *Use autocli* debe estar **OFF**, es decir, sin marcar.

En el apartado **Virtual Ports**, definir la configuración de los puertos virtuales. Para ello, tener en cuenta lo siguiente:

- Las conexiones **TCP** pueden tener dos comportamientos, activo y pasivo. El caso activo significa que el equipo será quién tome la iniciativa en cuanto al establecimiento de la conexión TCP. Por el contrario, en el caso pasivo, el equipo estará a la espera de recibir peticiones de conexión externas. Los comportamientos son complementarios entre sí.
- Las conexiones **UDP** no necesitan ningún procedimiento de establecimiento previo, sencillamente se asume que el destinatario está configurado para la aceptación de datos en el puerto indicado. Las conexiones UDP no ofrecen confirmación extremo a extremo ni garantía alguna en cuanto a que la secuencia de entrega sea la original.
- Es usual configurar puertos con valores superiores a 1000 ya que existen puertos preestablecidos para el uso de servicios usuales en redes TCP/IP, con lo que de este modo se evitan posibles colisiones.

- Los puertos virtuales también pueden tener un protocolo o una política de encapsulado asignada, aunque, por regla general, únicamente se acaba asignando un protocolo o una política de encapsulado en un único extremo de cada conexión, entendiendo que la misma ya incluye tanto un puerto físico como otro virtual. De modo que **lo usual es asignar el protocolo de encapsulado al puerto físico, y dejar el puerto virtual sin protocolo, es decir, con la opción de protocolo raw (opción por defecto).**

! El tiempo de inactividad (*inactivity time*) es el periodo de tiempo máximo que se desea que la conexión sea mantenida en el caso de ausencia de datos, sean estos en transmisión o en recepción.

Por defecto, este parámetro está configurado a 0, es decir, no se monitoriza la actividad a nivel de datos, lo que supone que la conexión será permanente con independencia de su actividad. Las unidades del parámetro son segundos.

- Las conexiones TCP activas disponen del parámetro **On Demand**. Dicho parámetro indica si el establecimiento debe iniciarse por el simple hecho de estar configurada la conexión, o únicamente cuando el equipo disponga de datos encapsulados para su transmisión.

! Por defecto, el parámetro **On Demand** está configurado para que se establezca permanentemente el inicio de la comunicación. En el caso de activar la opción **On Demand**, la duración de la conexión vendrá estipulada por el parámetro de inactividad, con lo que se consigue limitar la conexión a los periodos de actividad.

3. Establecer las conexiones entre los puertos, mediante sus identificadores. Para ello, acceder al submenú **Connection** (véase apartado 5.12.2 para más información) del menú **Flow**.



Para que una conexión sea efectiva es imprescindible introducir correctamente el nombre de los identificadores establecidos en los apartados **Physical ports** y **Virtual ports** de la pantalla de configuración del menú **Flow**. Para evitar posibles errores, en lugar del teclado, es aconsejable utilizar los comandos **Ctrl.+C** (copiar) y **Ctrl.+V** (pegar).

En segundo lugar, para que una conexión esté operativa, el **CheckBox** del parámetro **Enable** debe estar activo, es decir, marcado.

1.3 MODELOS DISPONIBLES

El CIC incluye de base una **interfaz serie de mantenimiento**, **dos interfaces Ethernet** tipo 10/100Base-Tx (con conector RJ-45) ó 100Base-Fx multimodo (con conector MT-RJ), y **1 puerto serie asíncrono** configurable por software con interfaz eléctrica V.24/V.28 ó interfaz RS-485 (2 ó 4 hilos).

El equipo puede completarse con **cuatro** u **ocho puertos serie RS-232 adicionales**, con conector SUB-D de 9 contactos y/o transductores de fibra óptica.

Opcionalmente, puede equiparse con **1 interfaz WAN inalámbrica** (GPRS/UMTS/HSDPA), que a su vez puede estar equipada con **una o dos bahías para tarjetas SIM**.

En cuanto a la fuente de alimentación, existen dos versiones:

- Multirango (85-360 Vcc, 60-260 Vca).
- CC aislada (20-75 Vcc).

En lo que respecta a su instalación, el CIC se suministra en un panel de una unidad normalizada de altura y 19 pulgadas de anchura, preparado para montaje en rack.

1.4 ESPECIFICACIONES TÉCNICAS

1.4.1 Interfaces del equipo

- 2 puertos con interfaces Fast Ethernet, tipo 10/100Base-Tx con conector RJ-45 o tipo 100Base-Fx multimodo (1300 nm) con conector MT-RJ.
- 1 puerto serie asíncrono (COM1), configurable por software para interfaz RS-232 ó interfaz RS-485 (2 ó 4 hilos).
- Bloque 1 opcional: 4 puertos serie asíncronos (COM2 a COM5), configurables por software para interfaz RS-232, todos ellos con conector SUB-D de 9 contactos o transductor de fibra óptica (plástico o vidrio).
- Bloque 2 opcional: 4 puertos serie asíncronos (COM6 a COM9), configurables por software para interfaz RS-232, todos ellos con conector SUB-D de 9 contactos o transductor de fibra óptica (plástico o vidrio).
- 1 consola de servicio.
- Opcionalmente, 1 interfaz WAN inalámbrica (GPRS/UMTS/HSDPA), con una o dos bahías para tarjetas Mini Sim (2FF).

Para más detalles eléctricos, véase capítulo 2, *Características mecánicas y eléctricas*.

1.4.2 Protocolos de encapsulamiento

- IEC 60870-5-101/102/103 (los dos primeros con variantes para soportar direcciones de enlace con un tamaño de 1 o 2 bytes).
- DLMS.
- GESTEL.
- MODBUS.
- DNP 3.0.
- SAP20.
- PROCOME.
- Pid1.
- Twc.

1.4.3 Gestión del equipo

- Acceso local y remoto, bien mediante consola local, servidor Telnet y servidor SSH, o a través de un servidor web incorporado, HTTP.

1.4.4 Servicios adicionales

- Agente SNMP (SNMPv1 y SNMPv2c).
- Servidor y cliente DHCP.
- Servidor y cliente NTP.
- Cliente IPSec ó SSL/TLS (según configuraciones).
- Cliente TACACS+.

1.4.5 Accesorios

- Cables Ethernet.
- Cables serie.
- Pigtailes fibra óptica.
- Cables de antena.
- Antenas.

1.4.6 Certificaciones

- CE.
- Diseñado para Subestaciones Eléctricas.
- Diseñado para aplicaciones industriales.

1.4.7 Características de los puertos de datos serie asíncronos (DCE)

- Bits de datos: 5, 6, 7 u 8.
- Bits de stop: 1 ó 2.
- Paridad: impar, par o ninguna.
- Velocidad: de 600 a 115200 bit/s.
- Control de flujo: ninguno, hardware o software.
- Interfaz: V.24/V.28 de la UIT-T (EIA RS-232C) y, para el COM 1, RS-485 (2 ó 4 hilos).

Véase detalle de utilización del conector COM en capítulo 2, *Características mecánicas y eléctricas*.

1.4.8 Características de los transductores de fibra óptica

- Fibra de vidrio.
 - Tipo de conector: ST
 - Longitud de onda: 820 nm
 - Velocidad de transmisión: 5 MBd
 - Tipo de fibra: 50/125 μm , 62.5/125 μm , 100/140 μm y 200 μm
 - Distancia máxima típica: 2 km con fibra 62.5/125 μm
 - Tipo de emisor: LED
- Fibra de plástico.
 - Tipo de conector: Versatile Link
 - Longitud de onda: 660 nm
 - Velocidad de transmisión: 40 kBd
 - Tipo de fibra: POF (Plastic Optical Fiber) de 1mm diámetro
 - Distancia máxima típica: 120 m
 - Tipo de emisor: LED

Véase detalle de los conectores en capítulo 2, *Características mecánicas y eléctricas*.

1.4.9 Características de la interfaz WAN opcional

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

1.4.10 Características mecánicas

- Panel de 1 U y 19 pulgadas de anchura, preparado para montaje en rack.
Altura: 45 mm; Anchura: 484 mm; Profundidad: 213 mm (con conector).
- Peso: 2 kg

Para más detalles mecánicos, véase capítulo 2, *Características mecánicas y eléctricas*.

1.4.11 Condiciones de funcionamiento

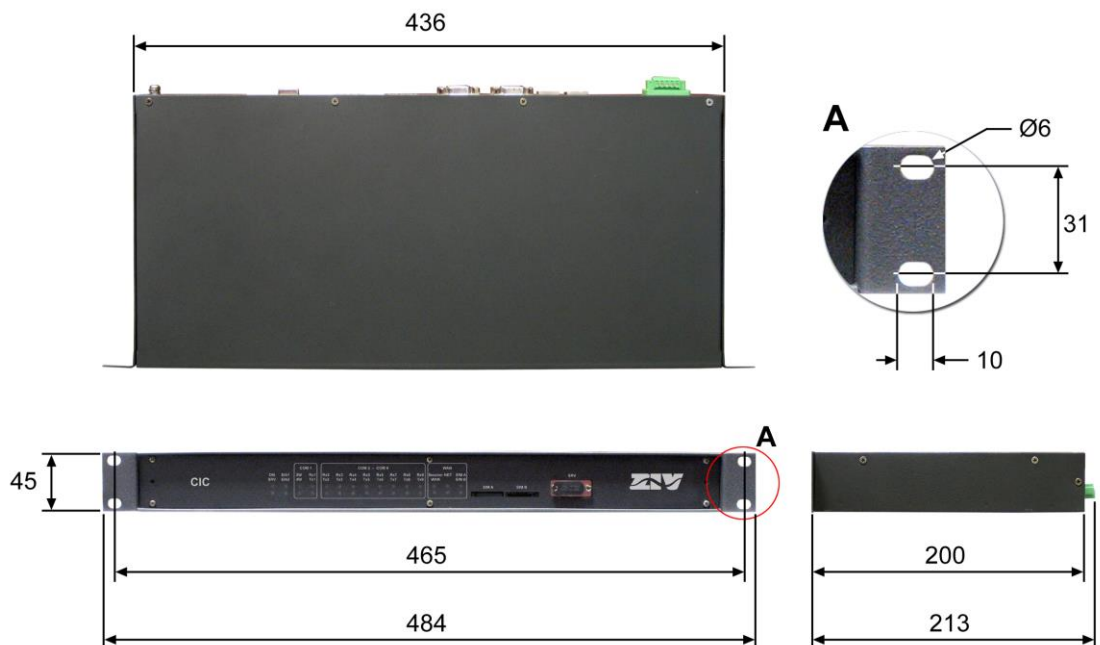
- Alimentación: 20-75 Vcc (aislada) ó multirango (85-360 Vcc, 60-260 Vca).
- Temperatura y humedad: de -20°C a +70°C y humedad relativa no superior al 95%, según CEI 721-3-3 clase 3K5 (climatograma 3K5).
- Consumo de potencia máximo: 20 W.
- Seguridad eléctrica: según la norma EN 60950.
- Emisiones R.F.: 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.

2 CARACTERÍSTICAS MECÁNICAS Y ELÉCTRICAS

Los distintos elementos que conforman el CIC están contenidos en un panel de una unidad normalizada de altura y 19 pulgadas de anchura, preparado para montaje en rack.

Las dimensiones generales en mm del panel, así como la posición de los taladros de sujeción, se muestran en la FIGURA 4.

FIGURA 4 Dimensiones generales en mm del panel CIC



CIC

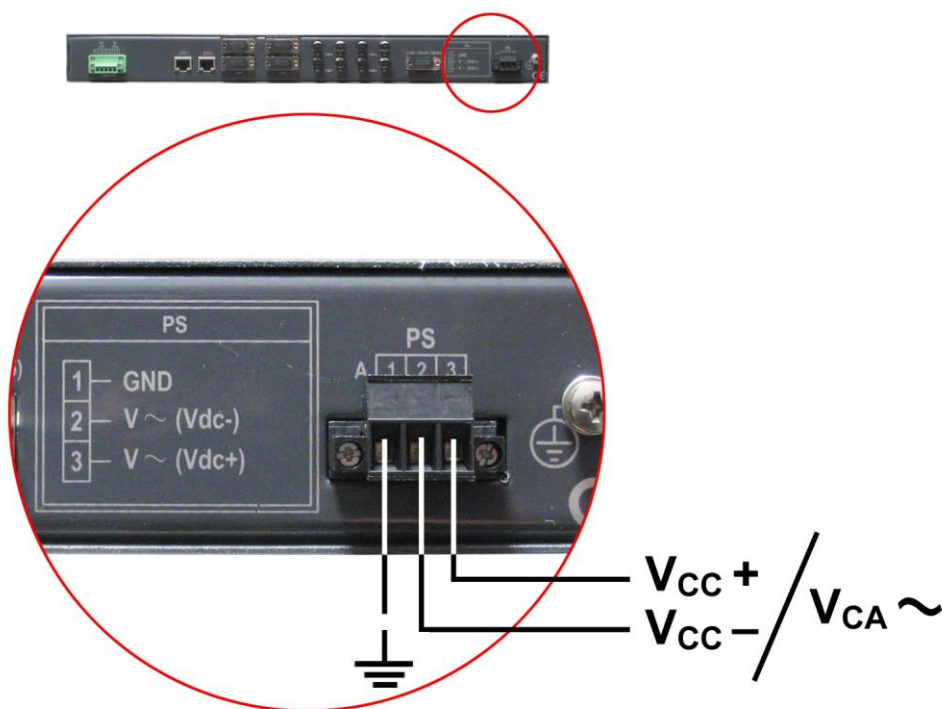
La FIGURA 5 muestra la parte posterior del panel CIC equipado con 8 puertos adicionales, los cuatro primeros con conector SUB-D de 9 contactos y los cuatro restantes para conector de fibra óptica.

FIGURA 5 Vista posterior del panel CIC con 8 puertos adicionales (SUB-D y fibra óptica de vidrio)



El CIC se alimenta a una tensión nominal de 48 V_{CC} (aislada) o a una tensión continua y alterna (85-360 V_{CC}, 60-260 V_{CA}), a través del conector que se muestra en la FIGURA 6.

FIGURA 6 Disposición del conector de alimentación en el panel CIC

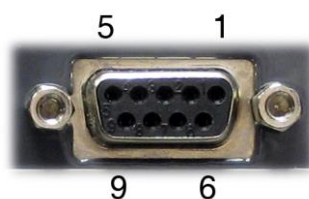


Junto al conector de alimentación, véase FIGURA 7, se encuentra dispuesto el puerto serie asíncrono (COM1), configurable por software para interfaz RS-232 ó interfaz RS-485 (2 ó 4 hilos).

FIGURA 7 Disposición del conector COM1 en el panel CIC



Las características eléctricas del conector se configuran mediante software de entre las indicadas en las características técnicas, véase apartado 1.4.7, *Características de los puertos de datos serie asíncronos (DCE)*. A continuación, se indica su utilización. El conector está provisto de tapón de protección.



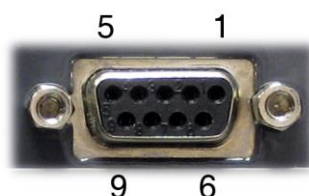
Pin	RS-232	RS-485 (4 hilos)	RS-485 (2 hilos)
1	DCD		
2	RD		
3	TD		
4	DTR		
5	GND		
6	DSR	RX-	
7	RTS	RX+	
8	CTS	TX-	TX/RX-
9	RI	TX+	TX/RX+

En la FIGURA 8, puede apreciarse la disposición de los cuatro conectores adicionales para interfaz RS-232 (COM2 a COM5) con conector SUB-D de 9 contactos.

FIGURA 8 Ejemplo de disposición de conectores RS-232 adicionales (SUB-D) en el panel CIC



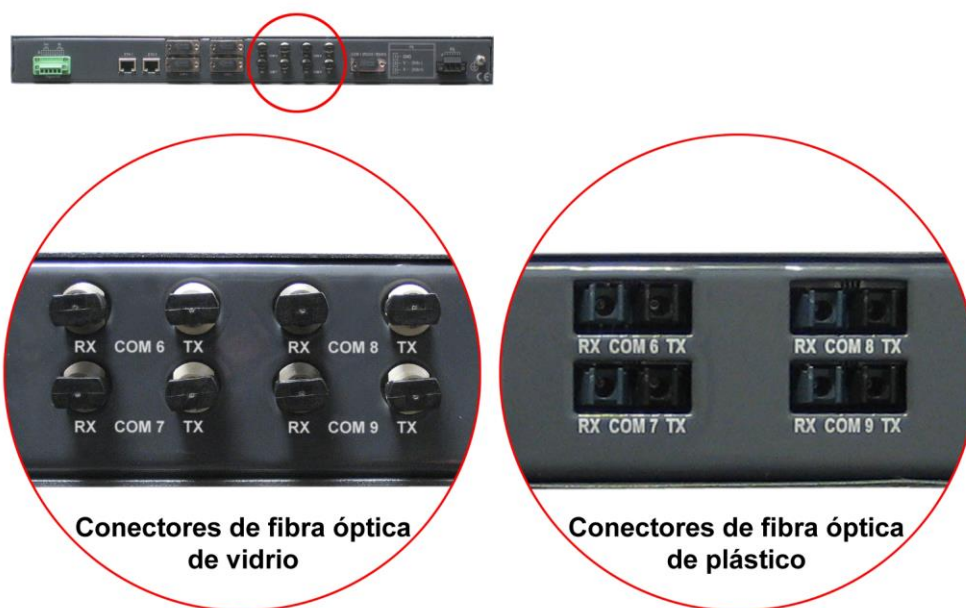
Cada conector está provisto de tapón de protección. A continuación, se indica la utilización del conector.



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

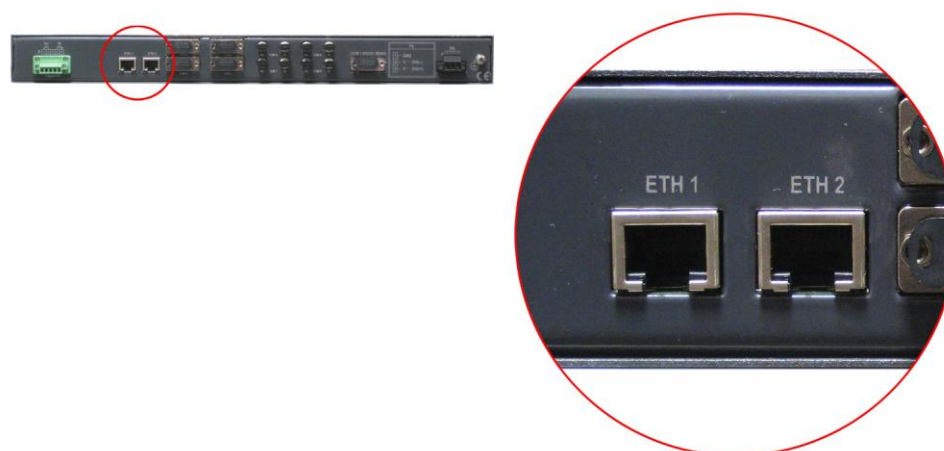
En la FIGURA 9, puede apreciarse la disposición de los cuatro conectores adicionales para fibra óptica de plástico o vidrio (COM6 a COM9). Las características de los conectores están indicadas en las características técnicas, véase apartado 1.4.8, *Características de los transductores de fibra óptica*.

FIGURA 9 Ejemplo de disposición de conectores adicionales (COM) en el panel CIC

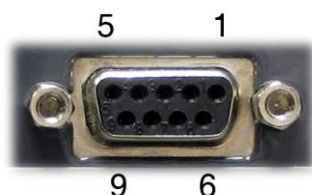


En cuanto a las interfaces de red, puede estar provisto de interfaces Fast Ethernet 10/100Base-Tx con conector RJ-45, como puede apreciarse en la FIGURA 10, o bien con interfaces 100Base-Fx multimodo (1300 nm) con conector óptico tipo MT-RJ.

FIGURA 10 Disposición de puertos Ethernet en el panel CIC



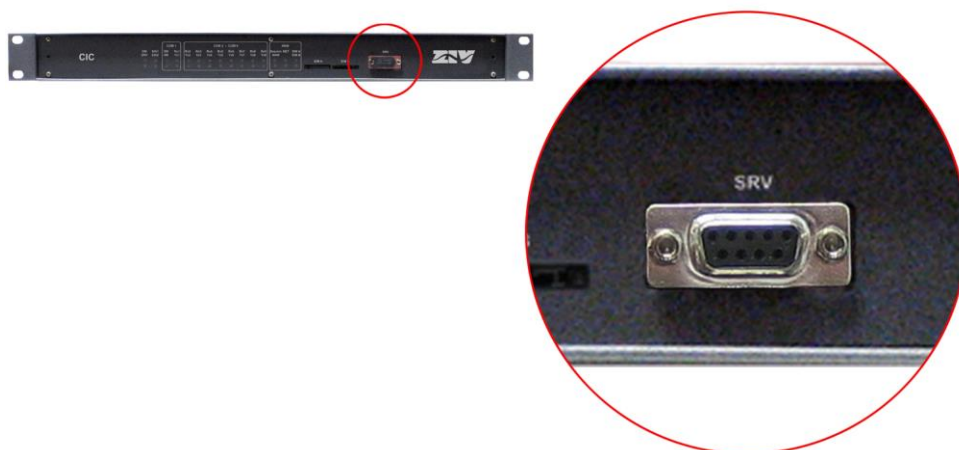
En el frontal del panel, véase FIGURA 11, se encuentra dispuesto un conector de mantenimiento, identificado como SRV, para el acceso al equipo mediante consola. Las características eléctricas del conector y su utilización se indican a continuación. El conector está provisto de tapón de protección.



Pin	RS-232
2	RD
3	TD
5	GND

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 11 Disposición del conector de mantenimiento en el frontal del panel CIC



Opcionalmente, el CIC puede equiparse con un dispositivo de red WAN GPRS o UMTS. En ese caso, junto a los conectores Ethernet, se encuentra dispuesto un conector SMA hembra para antena GSM/GPRS y, en el frontal del equipo, se encuentran dispuestas dos ranuras para alojamiento de tarjetas Mini Sim (2FF).

Ambas SIMs **NO pueden** estar activas simultáneamente. Se utiliza un funcionamiento *dual SIM*, es decir, una SIM actúa como principal (*primary*) y la otra SIM actúa como secundaria o back-up.

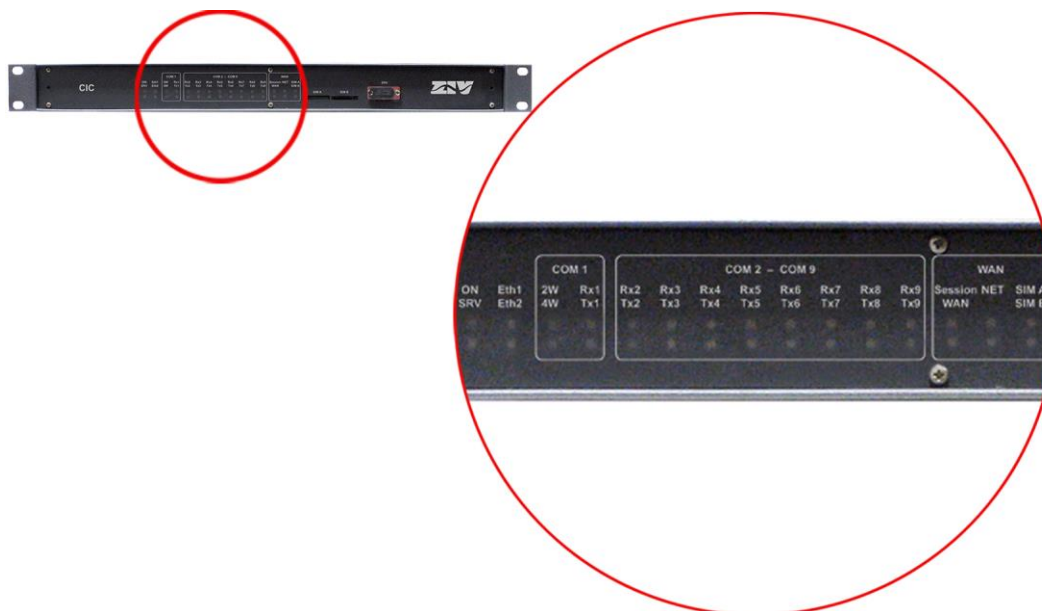
3 SEÑALIZACIÓN DE LOS LEDS

El CIC dispone en su parte frontal de dos LEDs de base (ON y SRV), de dos LEDs asociados a los puertos Ethernet (Eth1 y Eth2), de cuatro LEDs asociados al puerto de base COM1, de hasta dieciséis LEDs asociados a los ocho puertos adicionales (COM2 a COM9), dos por puerto, y de varios LEDs asociados a la interfaz WAN opcional.

FIGURA 12 Vista frontal del panel CIC



FIGURA 13 Detalle frontal de los LEDs asociados a las interfaces



La descripción de los distintos LEDs se indica a continuación.

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 Eth1	Ámbar. Se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz LAN.
LED Eth2	Ámbar. Se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz LAN.
LED 2w (COM1)	Verde. Se ilumina en permanencia cuando el puerto COM 1 se ha configurado con una interfaz RS-485 a 2 hilos.
LED 4w (COM1)	Verde. Se ilumina en permanencia cuando el puerto COM 1 se ha configurado con una interfaz RS-485 a 4 hilos.
LED Rx1 (COM 1)	Ámbar. Se ilumina intermitente cuando se reciben datos del puerto COM1.
LED Tx1 (COM 1)	Ámbar. Se ilumina intermitente cuando se transmiten datos por el puerto COM1.
LED RxX (COM X)	Ámbar. Se ilumina intermitente cuando se reciben datos del puerto COM X (<i>siendo X: 2 a 9</i>).
LED TxX (COM X)	Ámbar. Se ilumina intermitente cuando se transmiten datos por el puerto COM X (<i>siendo X: 2 a 9</i>).

LED WAN	Verde. Se ilumina en permanencia cuando para la interfaz inalámbrica se ha establecido la sesión con el operador.
LED NET	Verde. Se ilumina intermitente cuando la interfaz inalámbrica se ha registrado en la red del operador.
LED SIM X	<p>Verde. Se ilumina en permanencia indicando que la SIM X está en uso.</p> <p>Ambas SIMs NO pueden estar activas simultáneamente. Se utiliza un funcionamiento <i>dual SIM</i>, es decir, una SIM actúa como principal (<i>primary</i>) y la otra SIM actúa como secundaria o back-up.</p>

4 ACCESO AL EQUIPO

El CIC es gestionable de forma local y remota, bien mediante consola o a través de un servidor web incorporado, el servidor opera con protocolo HTTP.

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, sino que serán aplicados en el caso de producirse una inicialización.

De este modo, como procedimiento operativo, los cambios se ponen en operación con el comando **Apply**, y una vez verificado que el comportamiento es el deseado, se procede a 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.

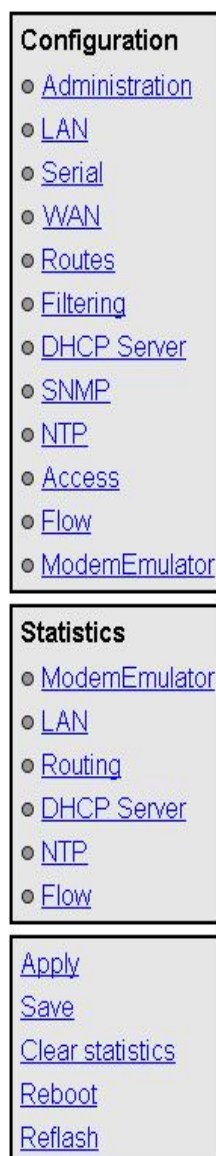
Los procedimientos para la efectiva configuración de los parámetros son idénticos, es decir, es necesario ejecutar el comando **Apply** y/o el comando **Save**, según lo indicado en el caso de uso de la consola, si bien con anterioridad a cualquiera de los mismos es necesario haber indicado al sistema que se han modificado datos, con el comando **Send** (botón presente en todas las 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 14 se muestran los comandos indicados.

Para el detalle de los comandos **Reboot** y **Reflash**, véanse respectivamente los apartados 5.14 y 5.15.

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

FIGURA 14 Árbol de menús de páginas HTML



En la 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 CIC se puede llevar a cabo tanto mediante la consola como mediante el acceso a las páginas HTML del equipo.

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

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 15, que se muestra una vez el CIC 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 15 Página HTML principal

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

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

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

5.1.1 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 carácter.

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

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

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

5.1.3 Otros

En esta sección, existen cuatro parámetros. El primero de ellos establece la zona horaria en relación a UTC.

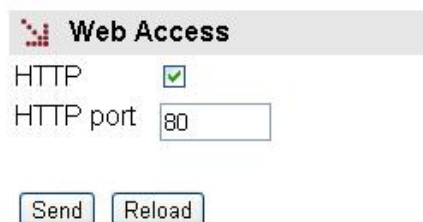
El segundo parámetro, **Serial log**, indica si el equipo activa la transmisión de los datos de log sobre el puerto serie de servicio desde el momento inicial de arranque (control *Checkbox* seleccionado) o no.

El tercer parámetro, **Enable periodic reset**, permite al usuario indicar si desea que el equipo se reinicie 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.

FIGURA 16 Pantalla de configuración **Administration**



Web Access

HTTP

HTTP port

5.3 CONFIGURACIÓN LAN

El menú **LAN** contiene los datos de configuración de la conexión de red.

La pantalla asociada al submenú **eth0** presenta dos apartados bien diferenciados, los cuales se describen a continuación.

FIGURA 17 Página de configuración asociada al submenú **eth0**

LAN

Static IP

IP Address

Mask

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

IP Alias

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

LAN:

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.

IP Alias:

El equipo es capaz de responder a direcciones IP diferentes de la principal si, previamente, han sido agregadas mediante el *CommandButton Add*.

5.4 CONFIGURACIÓN PUERTOS SERIE

El menú **Serial** da acceso a la pantalla de configuración de los puertos serie (COM) del equipo.

De base, el equipo dispone de 1 puerto serie asíncrono, COM 1, configurable por software para interfaz RS-232 ó interfaz RS-485 (2 ó 4 hilos). Además del anterior, el equipo puede completarse con cuatro (COM2 a COM5) u ocho (COM6 a COM9) puertos serie RS-232 adicionales, con conector SUB-D de 9 contactos y/o transductores de fibra óptica.

La pantalla asociada al menú **Serial** presenta dos apartados bien diferenciados, los cuales se describen a continuación. Para obtener una información general sobre la interconexión de puertos, véase el apartado 1.2.

Physical:

- **#.** Establece el número de puerto físico del equipo. Puerto 1 para el puerto COM1, Puertos 2 a 5 para el bloque COM2 a COM5, y Puertos 6 a 9 para el bloque COM6 a COM9.
- **Interface.** Establece el tipo de interfaz. Por defecto, RS-232. El puerto 1 es el único que admite también interfaz RS-485 a 2 ó 4 hilos.
- **Baudrate.** Establece la velocidad del puerto serie. Los valores disponibles son: 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 y 115200 bit/s.
- **Databits.** Establece la longitud de carácter. Los valores disponibles son: 5, 6, 7 y 8.
- **Parity.** Establece la paridad. Los valores disponibles son: impar (*odd*), par (*even*) o ninguna.
- **Stopbits.** Establece el número de bits de paro. Los valores disponibles son: 1 y 2.
- **Flow control.** Establece el mecanismo de control de flujo. Los valores disponibles son: ninguno (*none*), hardware (señales de control) y software (Xon e Xoff).

FIGURA 18 Página de configuración de los **puertos serie (COM)**

Physical

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

1 Just first port can be configured in 485 modes

Logical

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

Logical:

- **#.** Establece el número de puerto físico del equipo. Puerto 1 para el puerto COM1, Puertos 2 a 5 para el bloque COM2 a COM5, y Puertos 6 a 9 para el bloque COM6 a COM9.
- **Mode.** Establece el modo de funcionamiento del puerto: **flow** o **emulator**. Por defecto, **flow**, es decir, modo puerto serie. El modo **emulator** supone la activación de la característica adicional de emulación de módem HAYES, y sólo deberá seleccionarse cuando se desee definir para el puerto un comportamiento *ModemEmulator*, el cual es similar al de un modem HAYES. En este último caso, existen opciones adicionales en el menú *ModemEmulator*.

- **Protocol.** Establece el protocolo de los datos que se encapsularán, siendo los valores posibles: **raw** (sin procesado, es transparente a la información), **packed**, (se agrupan los datos en paquetes según los parámetros asociados, siendo también transparente en cuando a la información encapsulada), uno de los identificadores de los **protocolos de telecontrol soportados** (iec101_1, iec101, iec102_1, iec102, pid1, dlms, gestel, sap20, twc, dnp3, procome, iec103, modbusrtu, modbusrtu_cc) o el modo basado en una política (**policybased**).
- **Policy.** Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo **policybased**. Establece un identificador cuya política (*policy*) deberá configurarse en el submenú *Policy* del menú *Flow*.
- **Packed time (ms).** Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo **packed**. Establece el tiempo máximo de espera después de la recepción del último carácter, en ms, antes de enviar un paquete con los datos recibidos hasta el momento. Fuerza el envío de datos por tiempo de inactividad para los casos en los que no se haya llegado al número de datos establecido como tamaño deseado de paquete (ver siguiente parámetro).
- **Packed size.** Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo **packed**. Establece el número de caracteres máximo que se transmitirán en un paquete sobre la red.

5.5 CONFIGURACIÓN WAN

Este menú sólo aparece en caso de que el equipo CIC esté equipado con la opción de interfaz WAN inalámbrica (GPRS/UMTS/HSDPA).

FIGURA 19 Página de configuración de la interfaz **WAN**

WAN

Enable Wireless WAN

Primary SIM alternated ▾

Request DNS

Maximum number of retries

Maximum time to connect (min)

Low Coverage Level Alarm

Low Coverage Alarm Period

Max time in secondary(min)

Enable dual SIM

Enable inactivity time for datacalls

Inactivity time for datacalls (s)

SIM A

PIN1 value [Change](#)

PIN2 value [Change](#)

APN

Force Home Network

Authentication method pap ▾

User

Password [Change](#)

Minimum Signal (dBm)

SIM B

PIN1 value [Change](#)

PIN2 value [Change](#)

APN

Force Home Network

Authentication method pap ▾

User

Password [Change](#)

Minimum Signal (dBm)

Dynamic DNS

Enable Dyn Service

Dyn Service Id dydns ▾

Dyn Service Login

Dyn Service Password

Host name1

Time Interval (s)

1 Example: support.usyscom.com

Ping Keep Alive

Remote IP1

Remote IP2

Frequency (min)

Size of ICMP Packets (+28)

Number of ICMP Packets

Action none ▾

Strict

El menú presenta cuatro apartados bien diferenciados, los cuales se describen a continuación.

WAN:

- **Enable Wireless WAN.** Permite habilitar y deshabilitar la interfaz WAN del equipo seleccionando 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 opción **OFF**, inhabilitación 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 las direcciones de los servidores DNS al operador cuando esté disponible la conexión con el mismo.
- **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), el número de intentos es para cada una de las SIMs. Así, una vez alcanzado el número de intentos con la SIM principal (*primary*), el equipo intentará la conexión utilizando la SIM secundaria. En caso de que no fuera posible la conexión con la SIM secundaria una vez alcanzado el número de intentos o bien 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), debe tenerse en cuenta que el contador **Maximum time to connect** entrará en funcionamiento al mismo tiempo que el contador **Maximum number of retries**. Así, el equipo se reiniciaría cuando

uno de los dos contadores llegue a cero, es decir, por falta de conexión tras agotar los reintentos con ambas SIMs (ver contador Maximum number of retries) o tras agotar el tiempo configurado en el contador Maximum time to connect.

- **Low Coverage Level Alarm.** Especifica el nivel de cobertura por debajo del cual debe activarse la alarma de baja cobertura.
- **Low Coverage Alarm Period.** Especifica el tiempo que debe permanecer el nivel de cobertura por debajo del nivel indicado en el punto anterior antes de que se active la alarma de baja cobertura.
- **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.
- **Enable inactivity time for datacalls.** Seleccionando esta casilla se determina si el equipo hará uso del parámetro siguiente.
- **Inactivity time for datacalls (s).** Establece el tiempo en segundos de inactividad que supondrá el cierre voluntario y controlado de la conexión de llamada de datos GSM.

SIM:

- **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.

Una vez introducidos los valores **PIN 1** y **PIN 2** desde la opción **Change**, ejecutar el comando **send** de dicha opción y, a continuación, si dichos valores se desean aplicar y salvar en el equipo, **NO olvidar** ejecutar los comandos **apply** y **save** del árbol de menús principal.

- **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 autenticación 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 autenticación (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.

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

- **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).

La TABLA 2 relaciona el comando AT para medida de cobertura (AT+CSQ), el valor en dBm de dicha cobertura, y el nivel de cobertura que está captando el equipo, el cual se muestra en la barra de cobertura que aparece en la franja superior de cualquiera de las páginas de la interfaz de usuario.

TABLA 2

Comando AT para medida de cobertura (AT+CSQ)

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

Dynamic DNS:

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 CIC.
- **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 la interfaz 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.

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

- **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".

5.6 CONFIGURACIÓN RUTAS ESTÁTICAS

El menú **Routes** da acceso a la pantalla de configuración que permite al usuario proporcionar al sistema datos estáticos y permanentes al servicio de encaminamiento.

La pantalla asociada al menú **Routes** contiene dos apartados bien diferenciados. En el apartado **Static Routes** se configuran rutas estáticas explícitas. En el apartado **Default Static Routes** se configura 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 caso de que el equipo disponga de la interfaz inalámbrica opcional, 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 21 Página de configuración de rutas estáticas

Static Routes

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

2

Default Static Routes

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

2

Los parámetros de configuración de una ruta estática son:

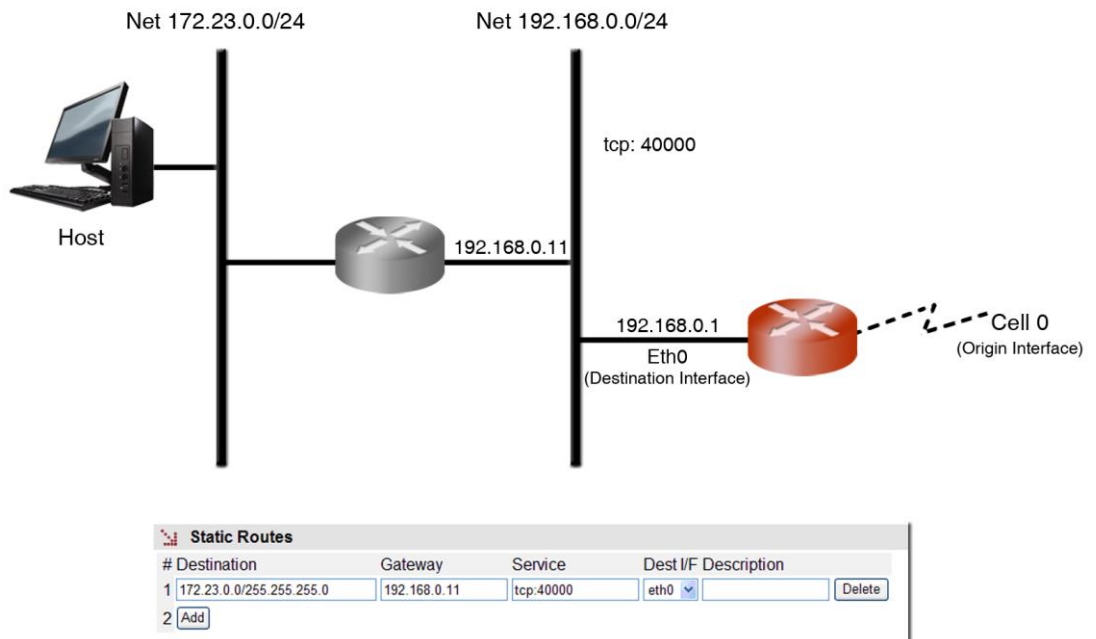
- **Destination.** Permite especificar la dirección IP y máscara de subred de la red remota o destino. El campo requiere que los valores se introduzcan en el formato del direccionamiento IP. Ejemplo: 192.168.0.0/255.255.255.0 ó 192.168.0.0/24.

- **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.
- **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 22 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.
- **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.

5.7 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 la interfaz GPRS/UMTS (cell0), si el equipo dispone de la interfaz WAN opcional.
- Filtrado de paquetes por servicio entrante/saliente para la interfaz Ethernet (eth0).

Packet Filtering for Local Services

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

Default Policy: accept

Forwarding Packet Filtering in cell0 interface

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

Default Policy: accept

Forwarding Packet Filtering in eth0 interface

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

Default Policy: accept

Send
Reload

Los parámetros de configuración en cada bloque son los siguientes:

- **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 interfaz ethernet (eth0) procedente del host 10.0.0.5 cuyo destino esté en el rango IP 192.168.0.0/24. La configuración del bloque **eth0** sería la mostrada en la siguiente figura.

FIGURA 24 Ejemplo de configuración de filtrado

The screenshot shows a configuration interface with three sections for packet filtering:

- Packet Filtering for Local Services:** Shows a table with one row (ID 1) and a default policy of 'accept'.
- Forwarding Packet Filtering in cell0 interface:** Shows a table with one row (ID 1) and a default policy of 'accept'.
- Forwarding Packet Filtering in eth0 interface:** Shows a table with one row (ID 1) and a default policy of 'accept'. The table has columns for #, Origin, Destination, Service, Dir., Policy, Description, and Enable.

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

5.8 CONFIGURACIÓN DHCP SERVER

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

Este servicio únicamente está disponible para la interfaz **eth0** (ETH1 física).

FIGURA 25 Pantalla de configuración del **DHCP server**

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

Los parámetros de configuración son:

- **Enable DHCP server.** Permite activar el servicio DHCP. Debe marcarse si se quiere utilizar un servidor DHCP.

! Por defecto, este parámetro está activado.

- **First IP Addr.** Permite especificar la **primera** dirección IP del pool de direcciones IP gestionadas por el servidor DHCP.
- **Last IP Addr.** Permite especificar la **última** dirección IP del pool de direcciones IP gestionadas por el servidor DHCP.
- **Maximum number of 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.
- **Lease time.** Permite especificar en segundos el tiempo que una dirección IP se asignará en base a una 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 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 [1] y SNMPv2c [2], así como la elección del tipo de mensajes, *trap* e *inform*.

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

FIGURA 26 Pantalla de configuración del menú **SNMP**

SNMP

Enable

Community

#	Name	Access
1	public	ro
2	<input type="text"/>	<input type="text"/>

SNMP Traps

Enable Traps

Traps

#	Community	Type	IP	Port	
1	public	v1	172.17.201.88	162	<input type="button" value="Delete"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Trap v1 agent address

Enable Wan Linkup Trap

Enable Wan Low Coverage Trap

Enable Wan High Coverage Trap

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.

5.10 CONFIGURACIÓN NTP

El equipo dispone de un cliente NTP, de modo que pueda sincronizar la información horaria accediendo a servidores NTP. El protocolo NTP [3] 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 autenticación.

FIGURA 27 Pantalla de configuración del menú **NTP**

NTP

Enable

Authentication Keys

# Key Number	Key
1	xxxxxxxx <input type="button" value="Delete"/>
2	<input type="button" value="Add"/>

NTP client

Server	# IP	Type	minpoll	maxpoll	Authentication Enable	Authentication Key	Low traffic
1	192.168.0.1	unicast	5	10	<input type="checkbox"/>	1	<input type="checkbox"/>
2	<input type="button" value="Add"/>						

Accept Broadcast

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 autenticación 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 (*multicast*), 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 autenticación, en cuyo caso se debe indicar cuál de las claves previamente definidas usará el cliente con el servidor en cuestión.

5.11 CONFIGURACIÓN ACCESS

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

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

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

TACACS+

1 Server IP

2 Server IP

Encrypted

Secret shared Key [Change](#)

Console Access

Authentication method1

1 *Fallback to local access always enabled*

Web Access

Authentication method

Fallback to local access

Telnet Access

Authentication method

Fallback to local 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 encuentran 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.

5.12 CONFIGURACIÓN DE LOS FLUJOS DE DATOS

El menú **Flow** permite, básicamente, establecer los parámetros de configuración de los puertos virtuales (TCP/UDP), así como definir las conexiones y/o flujos entre cualquiera de las interfaces disponibles. Para obtener una información general sobre la interconexión de puertos, véase el apartado 1.2.

El protocolo **UDP** es un protocolo **no orientado a conexión**. Los datos se transmiten como bloques (paquetes) independientes.

El protocolo **TCP** es un protocolo **orientado a conexión**, de modo que es necesaria una fase previa de establecimiento, y en el que los datos se transmiten como un flujo continuo de caracteres.

5.12.1 Protocolos de encapsulado

Cada uno de los puertos debe ser configurado para la operación con un protocolo específico, bien sea para operar de **modo transparente** (*raw* y *packed*), con uno de los **protocolos de telecontrol soportados** o con una **política** definida por el usuario.

Algunos de los protocolos disponen de identificadores múltiples, ya que con ello se indica no únicamente el protocolo en sí mismo, sino también el **tamaño de la dirección de enlace**, en los casos en que la norma obliga a que sea una opción de usuario.

Los protocolos sin identificadores múltiples son los siguientes:

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

Los protocolos con identificadores múltiples y los valores asociados a los mismos se detallan a continuación:

- **iec101_1.** IEC 60870-5 101, con trama FT1.2 y un tamaño de dirección de enlace de **1** byte.
- **iec101.** IEC 60870-5 101, con trama FT1.2 y un tamaño de dirección de enlace de **2** byte.
- **iec102_1.** IEC 60870-5 102, con trama FT1.2 y un tamaño de dirección de enlace de **1** byte.
- **iec102.** IEC 60870-5 102, con trama FT1.2 y un tamaño de dirección de enlace de **2** byte.

- **modbusrtu**. Protocolo Modbus en modo RTU para su operación en el encapsulador conectado al equipo remoto.
- **modbusrtu_cc**. Protocolo Modbus en modo RTU para su operación en el encapsulador conectado al equipo controlador (centro de control).

Los parámetros siguientes, aunque presentes siempre en los registros de configuración, únicamente tienen sentido cuando el protocolo seleccionado es **packed**.

- **Packed time (ms)**. Establece el tiempo máximo de espera después de la recepción del último carácter, en ms, antes de enviar un paquete con los datos recibidos hasta el momento. Fuerza el envío de datos por tiempo de inactividad para los casos en los que no se haya llegado al número de datos establecido como tamaño deseado de paquete (ver siguiente parámetro).
- **Packed size**. Establece el número de caracteres máximo que se transmitirán en un paquete sobre la red.

La pantalla de configuración asociada al menú **Flow** presenta tres apartados bien diferenciados, los cuales se describen a continuación. El primero, **Physical Ports**, permite establecer la identificación de los puertos serie y, si el equipo está configurado con la interfaz WAN opcional, configurar una conexión serie-llamada de datos (GSM). El segundo, **Virtual Ports**, permite definir la configuración de los puertos virtuales (TCP/UDP). El tercero, **Spy**, permite definir la configuración de un puerto espía.

FIGURA 29 Pantalla de configuración **Flow**

Physical Ports

Serial	# Identifier
1	Serial1
2	Serial2
3	Serial3
4	Serial4
5	serial0
6	serial0
7	serial0
8	serial0
9	serial0

Virtual Ports

TCP

# Identifier	Port	Destination	Retry Time (s)	Inactivity Time (s)	On Demand	Protocol	Policy	Packed time (ms)	Packed size	TLS Password	Enable
1	tcp0	255.255.255.255	1.000000000	0.000000000	<input type="checkbox"/>	raw		10	16	<input type="checkbox"/>	Change Delete
2 Add											

Passive TCP

# Identifier	Interface	Port	Origin	Inactivity Time (s)	Protocol	Policy	Packed time (ms)	Packed size	TLS Password	RFC2217	Enable
1	passivetcpTodos	all	1030	any	0.000000000	raw	50	262	<input type="checkbox"/>	Change	<input type="checkbox"/>
2	passivetcpPto1	all	1021	any	0.000000000	raw	50	262	<input type="checkbox"/>	Change	<input type="checkbox"/>
3	passivetcpPto4	all	1024	any	0.0000				<input type="checkbox"/>	Change	<input type="checkbox"/>
4	passivetcpPto2	all	1022	any	0.000000000	raw	50	262	<input type="checkbox"/>	Change	<input type="checkbox"/>
5	passivetcpPto3	all	1023	any	0.000000000	raw	50	262	<input type="checkbox"/>	Change	<input type="checkbox"/>
6 Add											

RX UDP

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

TX UDP

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

Full UDP

# Identifier	Interface	Local Port	Group-ID	Remote Port	Remote Address	Protocol	Policy	Packed time (ms)	Packed size	Multicast	Enable
1	Ethernet1	all	2011	0.0.0.0	2011	10.250.8.71	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
2	Ethernet1	all	2012	0.0.0.0	2012	10.250.8.70	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
3	Ethernet1	all	2013	0.0.0.0	2013	10.250.8.01	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
4	Ethernet4	all	2043	0.0.0.0	2043	10.250.8.93	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
5	Ethernet4	all	2044	0.0.0.0	2044	10.250.8.94	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
6	Ethernet2	all	2021	0.0.0.0	2021	10.250.8.98	iec101	50	262	<input type="checkbox"/>	<input type="checkbox"/>
7	Ethernet1	all	2014	0.0.0.0	2014	10.250.8.17	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
8	Ethernet3	all	2031	0.0.0.0	2031	10.250.8.68	pid1	50	262	<input type="checkbox"/>	<input type="checkbox"/>
9 Add											

Spy

# Identifier ¹	Header	Mode	Enable
1	spyserialTodos	Serial->	hex <input type="checkbox"/> Delete
2	spyudpTodos	RTUS<-	hex <input type="checkbox"/> Delete
3	spyserialSerial1	SERIAL(1)->	hex <input type="checkbox"/> Delete
4	spyudpEthernet1	RTUS(1)<-	hex <input type="checkbox"/> Delete
5	spyserialSerial4	SERIAL(4)->	hex <input type="checkbox"/> Delete
6	spyudpEthernet4	RTUS(4)<-	hex <input type="checkbox"/> Delete
7	spyserialSerial2	SERIAL(2)->	hex <input type="checkbox"/> Delete
8	spyudpEthernet2	RTUS(2)<-	hex <input type="checkbox"/> Delete
9	spyserialSerial3	SERIAL(3)->	hex <input type="checkbox"/> Delete
10	spyudpEthernet3	RTUS(3)<-	hex <input type="checkbox"/> Delete
11 Add			

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

Send Reload

Physical Ports:

- **Serial #.** Identifica el número de puerto físico del equipo. Puerto 1 para el puerto COM1. Puertos 2 a 5 para el bloque COM2 a COM5, y Puertos 6 a 9 para el bloque COM6 a COM9.
- **Identifier.** Establece un nombre distinto e inequívoco para cada uno de los puertos serie configurados en el menú *Serial*. Por defecto, todos los puertos tienen configurado el nombre *serial0* y, por tanto, es imprescindible asignarles un nombre específico a cada uno.

Si el CIC está equipado con la interfaz WAN opcional, aparecen los parámetros que permiten configurar una conexión serie-llamada de datos (GSM).

- **Datacall #.** Es un identificador de secuencia que proporciona el propio equipo.
- **Identifier.** Establece el identificador asociado a la llamada de datos GSM, por defecto el valor es *datacall0*.
- **Use autocli.** Si esta opción está activada (casilla marcada), cuando el equipo recibe una llamada de datos conecta la llamada al servicio de gestión **cli**, de modo que es equivalente a un acceso remoto a la consola de servicio. Si la opción NO está activada (casilla sin marcar), la llamada de datos se redirigirá al puerto físico configurado por el usuario en el bloque *Connection* (véase apartado 5.12.2).
- **Escape sequence.** En el caso en que la llamada de datos no tenga acceso directo al servicio de gestión sino a un puerto determinado (parámetro autocli NO activado), sigue siendo posible acceder al servicio de gestión **cli** insertando la cadena de escape que se defina en este parámetro. En el caso de acceder al servicio de gestión **cli** mediante la secuencia de escape, para recuperar el flujo inicial de datos, es necesario finalizar la llamada y establecerla de nuevo.

Virtual Ports:

- **TCP (conexiones en modo activo):**
 - #.** Es un identificador de secuencia que proporciona el propio equipo.
 - Identifier.** Establece un nombre distinto e inequívoco para cada uno de los puertos virtuales TCP activos. Por defecto, todas las conexiones al ser añadidas tienen configurado el nombre *tcp0* y, por tanto, es imprescindible cambiar dicho identificador para cada una de las nuevas conexiones.
 - Port.** Establece el puerto TCP destino.
 - Destination.** Establece la dirección IP destino.
 - Retry Time (s).** En caso de caída de la conexión, establece el tiempo en segundos de espera antes de llevar a cabo un reintento en la conexión.
 - Inactivity Time (s).** Establece el tiempo en segundos de inactividad que supondrá el cierre voluntario y controlado de la conexión.
 - On Demand.** Indica si la conexión debe intentar establecerse de forma permanente (parámetro *inactivo*) o únicamente cuando sea necesario a tenor de la existencia de datos (parámetro *activo*).
 - Protocol.** Establece el protocolo de los datos que se encapsularán, siendo los valores posibles los indicados en el inicio del apartado 5.12.1. Es usual que los puertos virtuales operen en modo *raw*, estando el correspondiente puerto físico configurado con el protocolo deseado.

Policy. Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo ***policybased***. Establece un identificador cuya política (*policy*) deberá configurarse en el submenú *Policy* del menú *Flow*.

Packed time (ms). Véase descripción en el inicio del apartado 5.12.1.

Packed size. Véase descripción en el inicio del apartado 5.12.1.

TLS. Establece si la conexión TCP empleará comunicaciones cifradas mediante Transport Layer Secure (TLS).

Password. Asociado a la utilización de TLS, establece la contraseña básica común.

Enable. Establece que la conexión TCP sea activa o no. Con la casilla marcada, la conexión TCP está habilitada. Deseleccionando la casilla, la conexión TCP está deshabilitada y no se intentará su establecimiento.

- **Passive TCP (conexiones en modo pasivo).**

#. Es un identificador de secuencia que proporciona el propio equipo.

Identifier. Establece un nombre distinto e inequívoco para cada uno de los puertos virtuales TCP (conexiones TCP) que estarán a la espera de peticiones de conexión provenientes de otros equipos. Por defecto, todas las conexiones al ser añadidas tienen configurado el nombre *passivetcp0* y, por tanto, es imprescindible cambiar dicho identificador para cada una de las nuevas conexiones.

Interface. Establece las posibles interfaces sobre las que se aceptarán peticiones y, por tanto, restringe los puntos posibles de entrada de las peticiones de conexión. Los valores posibles son: todas (*all*), *eth0* ó *cello* si el equipo está equipado con la interfaz WAN opcional.

Port. Establece el puerto TCP en el que se esperarán las peticiones de conexión.

Origin. Establece el rango de direcciones IP origen de las que se aceptarán las peticiones de conexión. Actúa como filtro de equipos origen autorizados. La dirección puede ser una dirección de host o de red, por lo que es necesario explicitar la máscara de red IP.

Inactivity Time (s). Establece el tiempo en segundos de inactividad que supondrá el cierre voluntario y controlado de la conexión.

Protocol. Establece el protocolo de los datos que se encapsularán, siendo los valores posibles los indicados en el inicio del apartado 5.12.1. Es usual que los puertos virtuales operen en modo *raw*, estando el correspondiente puerto físico configurado con el protocolo deseado.

Policy. Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo ***policybased***. Establece un identificador cuya política (*policy*) deberá configurarse en el submenú *Policy* del menú *Flow*.

Packed time (ms). Véase descripción en el inicio del apartado 5.12.1.

Packed size. Véase descripción en el inicio del apartado 5.12.1.

TLS. Establece si la conexión TCP empleará comunicaciones cifradas mediante Transport Layer Secure (TLS).

Password. Asociado a la utilización de TLS, establece la contraseña básica común.

RFC2217. Establece si se desea que la conexión TCP opere con las extensiones de control de la interfaz serie establecidas en la RFC2217 o no.

Enable. Establece que la conexión TCP sea activa o no. Con la casilla marcada, la aceptación de peticiones de conexión TCP está habilitada. Deseleccionando la casilla, las peticiones de conexión TCP serán rechazadas.

- **RX UDP (puertos UDP que aceptarán datos).**

#. Es un identificador de secuencia que proporciona el propio equipo.

Identifier. Establece un nombre distinto e inequívoco para cada uno de los puertos virtuales UDP sobre los que se aceptarán paquetes de datos. Por defecto, todos los puertos al ser añadidos tienen configurado el nombre *rxudp0* y, por tanto, es imprescindible asignarles un nombre específico a cada uno.

Interface. Establece las posibles interfaces sobre las que se aceptarán datos y, por tanto, restringe los puntos posibles de entrada de los paquetes. Los valores posibles son: todas (*all*), *eth0* ó *cell0* si el equipo está equipado con la interfaz WAN opcional.

Port. Establece el puerto UDP que va a ser empleado para la recepción de paquetes.

Group-ID. Dirección IP *multicast* en la que se aceptarán datos en recepción, siempre y cuando el valor del parámetro sea una dirección válida y la opción *multicast* esté activa. El valor por defecto *0.0.0.0* no es una dirección IP válida.

Source Address. Establece el rango de direcciones IP origen de las que se aceptarán las peticiones de conexión. Actúa como filtro de equipos origen autorizados. La dirección puede ser una dirección de host o de red, por lo que es necesario explicitar la máscara de red IP.

Protocol. Establece el protocolo de los datos que se encapsularán, siendo los valores posibles los indicados en el inicio del apartado 5.12.1. Es usual que los puertos virtuales operen en modo *raw*, estando el correspondiente puerto físico configurado con el protocolo deseado.

Policy. Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo *policybased*. Establece un identificador cuya política (*policy*) deberá configurarse en el submenú *Policy* del menú *Flow*.

Packed time (ms). Véase descripción en el inicio del apartado 5.12.1.

Packed size. Véase descripción en el inicio del apartado 5.12.1.

Multicast. Establece si se aceptarán datos con la dirección *multicast* establecida

en Group-ID. Cuando la opción no está activa, la dirección IP para la recepción es la dirección IP *unicast* propia del equipo.

Enable. Establece que el puerto RX UDP esté activo o no. Con la casilla marcada, el puerto RX UDP está habilitado y aceptará paquetes de entrada. Deseleccionando la casilla, el puerto RX UDP no aceptará datos.

- **TX UDP (puertos UDP sobre los que se transmitirán datos).**

#. Es un identificador de secuencia que proporciona el propio equipo.

Identifier. Establece un nombre distinto e inequívoco para cada uno de los puertos virtuales UDP sobre los que se transmitirán paquetes de datos. Por defecto, todos los puertos al ser añadidos tienen configurado el nombre *txudp0* y, por tanto, es imprescindible asignarles un nombre específico a cada uno.

Port. Establece el puerto UDP destino.

Group-ID/Destination. Dirección IP, *unicast* o *multicast* que se empleará para la transmisión de los datos. El valor por defecto *0.0.0.0* no es una dirección IP válida.

Protocol. Establece el protocolo de los datos que se encapsularán, siendo los valores posibles los indicados en el inicio del apartado 5.12.1. Es usual que los puertos virtuales operen en modo *raw*, estando el correspondiente puerto físico configurado con el protocolo deseado.

Policy. Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo *policybased*. Establece un identificador cuya política (*policy*) deberá configurarse en el submenú *Policy* del menú *Flow*.

Packed time (ms). Véase descripción en el inicio del apartado 5.12.1.

Packed size. Véase descripción en el inicio del apartado 5.12.1.

Enable. Establece que el puerto TX UDP esté activo o no. Con la casilla marcada, el puerto virtual TX UDP puede ser empleado para la transmisión de paquetes.

- **Full UDP.**

#. Es un identificador de secuencia que proporciona el propio equipo.

Identifier. Establece un nombre distinto e inequívoco para cada uno de los puertos virtuales UDP bidireccionales. Por defecto, todos los puertos al ser añadidos tienen configurado el nombre *fulludp0* y, por tanto, es imprescindible asignarles un nombre específico a cada uno.

Interface. Establece las posibles interfaces sobre las que se aceptarán datos y, por tanto, restringe los puntos posibles de entrada de los paquetes. Los valores posibles son: todas (*all*), *eth0* ó *cell0* si el equipo está equipado con la interfaz WAN opcional.

Local Port. Establece el puerto UDP que va a ser empleado para la recepción de

paquetes.

Group-ID. Dirección IP *multicast* en la que se aceptarán datos en recepción, siempre y cuando el valor del parámetro sea una dirección válida y la opción *multicast* esté activa. El valor por defecto *0.0.0.0* no es una dirección IP válida.

Remote Port. Establece el puerto UDP destino.

Remote Address. Dirección IP, unicast o multicast que se empleará para la transmisión de los datos. El valor por defecto *0.0.0.0* no es una dirección IP válida.

Protocol. Establece el protocolo de los datos que se encapsularán, siendo los valores posibles los indicados en el inicio del apartado 5.12.1. Es usual que los puertos virtuales operen en modo *raw*, estando el correspondiente puerto físico configurado con el protocolo deseado.

Policy. Este campo debe configurarse cuando en el parámetro *Protocol* se ha establecido el modo *policybased*. Establece un identificador cuya política (*policy*) deberá configurarse en el submenú *Policy* del menú *Flow*.

Packed time (ms). Véase descripción en el inicio del apartado 5.12.1.

Packed size. Véase descripción en el inicio del apartado 5.12.1.

Multicast. Establece si se aceptarán datos con la dirección *multicast* establecida en Group-ID. Cuando la opción no está activa, la dirección IP para la recepción es la dirección IP *unicast* propia del equipo.

Enable. Establece que el puerto Full UDP esté activo o no. Con la casilla marcada, el puerto virtual Full UDP está habilitado y acepta paquetes en recepción, así como permite la transmisión de los mismos.

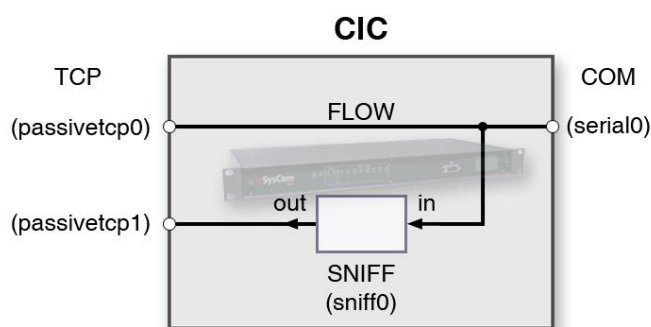
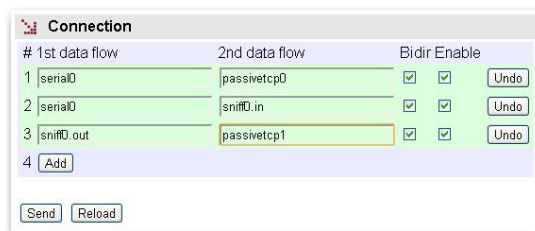
Spy:

- **#.** Es un identificador de secuencia que proporciona el propio equipo.
- **Identifier.** Establece un nombre distinto e inequívoco para cada uno de los puertos espía. Por defecto, todos los puertos al ser añadidos tienen configurado el nombre *sniff0* y, por tanto, es imprescindible asignarles un nombre específico a cada uno.
- **Header.** Establece un texto que precederá cada uno de los mensajes proporcionados por esta instancia, con el fin de facilitar su procedencia en el caso de tener espías múltiples.
- **Mode.** Establece el formato de representación de los datos disponibles en la conexión espía. Los valores admisibles son *raw* (formato original de los datos) o *hex* (representación hexadecimal).
- **Enable.** Establece que el puerto espía esté activo o no. Con la casilla marcada, el puerto espía está habilitado.

Ejemplo:

La figura muestra un ejemplo de definición de un puerto espía para verificar la conexión entre un puerto *serial0* y un puerto *passivetcp0*. Además de definir el puerto espía (*sniff0*), será necesario definir un puerto (*passivetcp1*) que nos permita obtener de él la información que estamos espiando.

FIGURA 30 Ejemplo de configuración de puerto espía



5.12.2 Connection

El submenú **Connection** del menú **Flow** permite definir las conexiones que determinan los puertos, físicos y/o virtuales, entre los que se intercambiará el tráfico de usuario.

Para obtener una información general sobre la interconexión de puertos, véase el apartado 1.2.

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

Send Reload

Los parámetros de configuración son los siguientes:

- **#.** Es un identificador de secuencia que proporciona el propio equipo.
- **1st data flow.** Determina el **primer puerto** incluido en esta conexión, mediante su identificador.

- **2nd data flow.** Determina el **segundo puerto** incluido en esta conexión, mediante su identificador.

Es imprescindible introducir correctamente el nombre del identificador en los dos campos anteriores, de modo que sea uno de los establecidos en los apartados *Physical ports* y *Virtual ports* de la pantalla de configuración del menú *Flow*. Para evitar posibles errores, en lugar del teclado, es aconsejable utilizar los comandos *Ctrl. + C* (copiar) y *Ctrl. + V* (pegar).

- **Bidir.** Determina si la conexión opera en ambos sentidos, es decir, si se comporta de modo **bidireccional**.

En el caso de las conexiones **unidireccionales**, el flujo de tráfico es únicamente desde el puerto con el identificador especificado en *1st data flow* hacia el puerto con el identificador especificado en *2nd data flow*.

- **Enable.** Establece que la conexión esté activa. Con la casilla marcada, la conexión o flujo está habilitado.

Tal y como puede verse en la FIGURA 32, los identificadores admiten la inclusión de un **sufijo numérico**, separado del identificador configurado en apartados previos, y que se interpreta como el flujo de los mensajes del protocolo cuya dirección de enlace coincide con el valor establecido; es decir, para algunos de los protocolos encapsulados, el equipo dispone de la capacidad de extraer conversaciones específicas de modo que puedan ser demultiplexadas hacia destinos diferenciados.

El tamaño de la dirección de enlace queda especificada en el momento en que se selecciona el protocolo encapsulado o se define la política de encapsulado (en este último caso solamente para iec101/102).

FIGURA 32 Ejemplo de inclusión de un sufijo numérico

Connection

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

5.12.3 Policy

El submenú **Policy** del menú **Flow** permite crear variantes de algunos protocolos de modo que se amplían las funciones del encapsulador (véase referencia bibliográfica [4]).

Los protocolos que admiten dichas variantes son: iec101/iec102, pid1, gestel y sap20.

Las funciones adicionales implementadas están diseñadas para la utilización de los protocolos en modo no balanceado para, al mismo tiempo, minimizar el tráfico entre los equipos encapsuladores.

FIGURA 33 Pantalla de configuración **Policy** del menú **Flow**

Policy

iec101/iec102

#	Identifier	DelayControl Mode	QuickCheck Mode	QuickCheck Period (secs)	QuickCheck Timeout	Link Address Size	
1	<input type="text" value="policy0"/>	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="15"/>	<input type="text" value="0.500000000"/>	<input type="text" value="2"/>	<input type="button" value="Undo"/>
2	<input type="button" value="Add"/>						

pid1

#	Identifier	DelayControl Mode	QuickCheck Mode	QuickCheck Period (secs)	QuickCheck Timeout	
1	<input type="text" value="policy0"/>	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="15"/>	<input type="text" value="0.500000000"/>	<input type="button" value="Undo"/>
2	<input type="button" value="Add"/>					

gestel

#	Identifier	DelayControl Mode	QuickCheck Mode	QuickCheck Period (secs)	QuickCheck Timeout	
1	<input type="text" value="policy0"/>	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="15"/>	<input type="text" value="0.500000000"/>	<input type="button" value="Undo"/>
2	<input type="button" value="Add"/>					

sap20

#	Identifier	DelayControl Mode	
1	<input type="text" value="policy0"/>	<input type="text" value="none"/>	<input type="button" value="Undo"/>
2	<input type="button" value="Add"/>		

En modo no balanceado, los equipos remotos únicamente pueden enviar información a los equipos controladores como respuesta a peticiones explícitas (mecanismo de *polling*). De modo que para tener un tiempo de respuesta a posibles situaciones acaecidas y detectadas por las entidades remotas, el centro de control debe transmitir mensajes de consulta de forma cíclica y con una frecuencia lo suficientemente elevada. Por tanto, esos mensajes transitan por la red TCP/IP. A los mensajes cíclicos que conforman el mecanismo de *polling* los denominamos mensajes **Quick Check (QC)**.

Las funciones ampliadas suponen que las consultas cíclicas del mecanismo de *polling* se crearán y enviarán por parte del equipo encapsulador directamente conectado al equipo remoto. Únicamente cuando la remota responde a los **mensajes QC**, el equipo encapsulador del lado remoto los hará llegar al equipo encapsulador del lado controlador para su entrega al centro de control. De este modo, se descarga al centro de control de la misión de consulta cíclica, y a la vez se evita el consumo de ancho de banda asociado.

La función de **Quick Check** se regula con los siguientes parámetros:

- **#**. Es un identificador de secuencia que proporciona el propio equipo.
- **Identifier**. Establece un nombre distinto e inequívoco para cada uno de las políticas (*policy*). Por defecto, todas las políticas al ser añadidas tienen configurado el nombre *policy0* y, por tanto, es imprescindible asignarlas un nombre específico a cada una.
- **Delay Control Mode**. La opción **none** supone que no se ejecutarán las funciones de control de tiempo ampliadas de Quick Check. Cualquier otra opción, habilita la opción y a la vez determina si el equipo está conectado al centro de control (**system**) o al equipo remoto (**rtu**).
- **Quick Check Mode**. La opción **none** supone que no se ejecutarán las funciones ampliadas de Quick Check. Cualquier otra opción, habilita la opción Quick Check y a la vez determina si el equipo está conectado al centro de control (**system**) o al equipo remoto (**rtu**).
- **Quick Check Period (secs)**. Establece el periodo de tiempo para la generación local de los mensajes de QC hacia el equipo remoto.
- **Quick Check Timeout**. Establece el tiempo máximo de espera de una respuesta desde el equipo remoto a la transmisión de un mensaje de QC por parte del encapsulador.
- **Link Address Size**. Únicamente para las políticas **iec101/102**. Establece el tamaño de la dirección de enlace empleada en este perfil, ya que estos protocolos permiten dos opciones en cuanto al tamaño.

5.12.4 Other

El submenú **Other** del menú **Flow** permite activar algunas prestaciones adicionales, orientadas fundamentalmente a la obtención de información para facilitar la resolución de posibles errores de configuración o incidencias.

La pantalla asociada al submenú **Other** presenta tres apartados bien diferenciados, los cuales se describen a continuación.

Device:

- **Identifier.** Este parámetro especifica la identidad del Centro de Control asociado cuando se emplean políticas **Quick Check**. Únicamente aplica al equipo que opera con el perfil system, es decir, el equipo al que está conectado el Centro de Control.

Socket:

- **Maximum time with sockets down (min).** Fija el tiempo máximo admisible, en minutos, en el que no hay conexión entre equipos ejecutando **Quick Check**.

Debug:

- **#.** Es un identificador de secuencia que proporciona el propio equipo.
- **Identifier.** Establece el identificador del puerto, físico o virtual, del que se desea que genere información adicional en los ficheros de log.

FIGURA 34 Pantalla de configuración **Other** del menú **Flow**

Device
Identifier

Socket
Maximum time with sockets down (min)

Debug
Identifier
1 Undo
2

5.13 CONFIGURACIÓN DEL PUERTO SERIE COMO *ModemEmulator*

El menú *ModemEmulator* conlleva que el equipo se presenta como un módem HAYES hacia el equipo cliente, por lo que el establecimiento de las conexiones se realiza de forma automática en base a los parámetros proporcionados por el equipo cliente, mediante los comandos de discado.

La emulación HAYES ofrece, en función del comando recibido, los siguientes comportamientos:

ATDT. Lanza una conexión TCP cuyo destinatario y puerto resulta a partir del número incluido en el propio comando. El número admite dos interpretaciones:

- **Número directo** que corresponde a la dirección IP y puerto destino deseado. Es un número de 17 dígitos: 12 corresponden a la dirección IP y 5 al puerto destino. Tanto la dirección IP como el puerto deben incluir de forma explícita los dígitos cuyo valor sea nulo. Es decir, el destinatario con la *dirección IP 10.89.1.123* y el *puerto 348* supondría que el comando a enviar sería **ATDT 010 089 001 123 00348** (en la cadena de ejemplo se han dejado de forma intencionada espacios en blanco para mostrar el modo de presentación, pero en el comando real no deben existir).
- Por consulta en la **tabla de discado** configurada (**Dialling Table**). La tabla permite la traducción de un plan de numeración arbitrario a direcciones IP y puertos de forma explícita.

ATD*. El puerto serie actúa como un servidor PPP, solicitando al equipo cliente las credenciales (usuario y contraseña) y proporcionando al mismo una dirección IP. Los parámetros indicados se establecen en los registros incluidos en la tabla Modem Emulator.

ATD. Lanza una llamada de datos GSM al número destino incluido en el propio comando.

Otros comandos aceptados por el dispositivo en modo emulación relativos a la gestión de llamadas son:

ATA: Acepta una llamada de datos GSM.

ATH: Supone la finalización de la llamada en curso.

Adicionalmente, en cuanto a la gestión del comportamiento como MODEM, el equipo dispone el registro S2, admite la configuración de los parámetros de ECHO (E), gestión de la señal DCD (&C) y gestión de la señal DTR (&D), y soporta los siguientes comandos estándar: **ATA**, **ATO**, **ATI**, **AT&F**, **AT&W** y **AT&V**.

FIGURA 35 Pantalla de configuración **ModemEmulator**

Modem Emulator

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

Dialling Table

Enable

Telephone Entries	#	Telephone Number	Destination IP	TCP Port	
1		100001	10.0.0.1	1001	Delete
2		100002	10.0.0.2	1002	Delete
3		100003	10.0.0.3	1003	Delete
4		100004	10.0.0.4	1004	Delete
5		100005	10.0.0.5	1005	Delete
6		100006	10.0.0.6	1006	Delete
7		100007	10.0.0.7	1007	Delete
8		100008	10.0.0.8	1008	Delete
9		100009	10.0.0.9	1009	Delete
10		100010	10.0.0.10	1010	Delete
11		100011	10.0.0.11	1011	Delete
12		100012	10.0.0.12	1012	Delete
13		100013	10.0.0.13	1013	Delete
14		100014	10.0.0.14	1014	Delete
15		100015	10.0.0.15	1015	Delete
16		100016	10.0.0.16	1016	Delete
17		100017	10.0.0.17	1017	Delete
18		100018	10.0.0.18	1018	Delete
19		100019	10.0.0.19	1019	Delete
20		100020	10.0.0.20	1020	Delete
21		100021	10.0.0.21	1021	Delete
22		100022	10.0.0.22	1022	Delete
23		100023	10.0.0.23	1023	Delete
24		100024	10.0.0.24	1024	Delete
25		100025	10.0.0.25	1025	Delete
26		100026	10.0.0.26	1026	Delete
27		100027	10.0.0.27	1027	Delete
28		100028	10.0.0.28	1028	Delete
29		100029	10.0.0.29	1029	Delete
30		100030	10.0.0.30	1030	Delete
31		100031	10.0.0.31	1031	Delete
32		100032	10.0.0.32	1032	Delete
33		100033	10.0.0.33	1033	Delete
34		100034	10.0.0.34	1034	Delete
35		100035	10.0.0.35	1035	Delete
36		100036	10.0.0.36	1036	Delete
37		100037	10.0.0.37	1037	Delete
38		100038	10.0.0.38	1038	Delete
39		100039	10.0.0.39	1039	Delete
40		100040	10.0.0.40	1040	Delete
41		100041	10.0.0.41	1041	Delete
42		100042	10.0.0.42	1042	Delete
43		100043	10.0.0.43	1043	Delete
44		100044	10.0.0.44	1044	Delete
45		100045	10.0.0.45	1045	Delete
46		100046	10.0.0.46	1046	Delete
47		100047	10.0.0.47	1047	Delete
48		100048	10.0.0.48	1048	Delete
49		100049	10.0.0.49	1049	Delete
50		100050	10.0.0.50	1050	Delete
51		100051	10.0.0.51	1051	Delete
52		100052	10.0.0.52	1052	Delete
53		100053	10.0.0.53	1053	Delete
54		100054	10.0.0.54	1054	Delete
55		100055	10.0.0.55	1055	Delete
56		100056	10.0.0.56	1056	Delete
57		100057	10.0.0.57	1057	Delete
58		100058	10.0.0.58	1058	Delete
59		100059	10.0.0.59	1059	Delete
60		100060	10.0.0.60	1060	Delete
61		100061	10.0.0.61	1061	Delete
62		100062	10.0.0.62	1062	Delete
63		100063	10.0.0.63	1063	Delete
64		100064	10.0.0.64	1064	Delete
65		100065	10.0.0.65	1065	Delete
66		100066	10.0.0.66	1066	Delete
67		100067	10.0.0.67	1067	Delete
68		100068	10.0.0.68	1068	Delete
69		100069	10.0.0.69	1069	Delete
70		100070	10.0.0.70	1070	Delete
71		100071	10.0.0.71	1071	Delete
72		100072	10.0.0.72	1072	Delete
73		100073	10.0.0.73	1073	Delete
74		100074	10.0.0.74	1074	Delete
75		100075	10.0.0.75	1075	Delete
76		100076	10.0.0.76	1076	Delete
77		100077	10.0.0.77	1077	Delete
78		100078	10.0.0.78	1078	Delete
79		100079	10.0.0.79	1079	Delete
80		100080	10.0.0.80	1080	Delete
81		100081	10.0.0.81	1081	Delete
82		100082	10.0.0.82	1082	Delete
83		100083	10.0.0.83	1083	Delete
84		100084	10.0.0.84	1084	Delete
85		100085	10.0.0.85	1085	Delete
86		100086	10.0.0.86	1086	Delete
87		100087	10.0.0.87	1087	Delete
88		100088	10.0.0.88	1088	Delete
89		100089	10.0.0.89	1089	Delete
90		100090	10.0.0.90	1090	Delete
91		100091	10.0.0.91	1091	Delete
92		100092	10.0.0.92	1092	Delete
93		100093	10.0.0.93	1093	Delete
94		100094	10.0.0.94	1094	Delete
95		100095	10.0.0.95	1095	Delete
96		100096	10.0.0.96	1096	Delete
97		100097	10.0.0.97	1097	Delete
98		100098	10.0.0.98	1098	Delete
99		100099	10.0.0.99	1099	Delete
100		100100	10.0.0.100	1100	Delete
249		100249	10.0.0.249	1249	Delete
250		100250	10.0.0.250	1250	Delete
251		Add			

La pantalla asociada al menú **ModemEmulator** presenta dos apartados bien diferenciados, los cuales se describen a continuación.

Modem Emulator:

- **#.** Es un identificador de correspondencia con el puerto físico (puerto serie) asociado a la función de emulación a la que corresponde el registro de configuración.
- **Identifier.** Establece un nombre distinto e inequívoco para cada uno de las configuraciones. Por defecto, todas tienen configurado el nombre *emulator0* y, por tanto, es imprescindible asignarles un nombre específico a cada una.
- **User.** Establece el usuario admitido cuando el equipo se comporta como un servidor PPP.
- **Password.** Establece la contraseña asociada al usuario PPP del campo anterior.
- **Authentication method.** Establece el protocolo estándar empleado para el intercambio de credenciales con el equipo externo, los valores son **none** (sin autenticación), **pap** (Password Authentication Protocol) y **chap** (Challenge Handshake Authentication Protocol).
- **Own IP.** La dirección IP asociada a la interfaz serie del equipo cuando opera como servidor PPP.
- **Peer IP.** La dirección IP que se proporcionará al equipo cliente.

Dialling Table:

- **Enable.** Establece si la tabla debe ser empleada para la traducción del plan de numeración de las llamadas realizadas con el comando ATDT o no.
- **#.** Es un identificador de secuencia que proporciona el propio equipo.
- **Telephone Number.** El número del plan de numeración asociado al registro.
- **Destination IP.** La dirección IP destino para el número especificado en el parámetro anterior.
- **TCP Port.** El puerto TCP destino para el número especificado en el parámetro de número telefónico.

5.14 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.

5.15 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 ocho 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 pertenecientes a la funcionalidad *ModemEmulator*, a la interfaz Ethernet (*LAN*), interfaz WAN opcional, reglas de rutado (*Routing*), DHCP server, cliente de sincronización (*NTP*) y a la interconexión entre puertos (*Flow*), 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 puede actualizar mediante el botón *Reload* sin tener que volver a seleccionar la opción correspondiente en el árbol de menús.

Las estadísticas pueden ser **INICIALIZADAS** por el usuario a voluntad, bien desde la consola, mediante la ejecución del comando **clear** en el prompt, bien mediante la opción de menú **Clear Statistics**.

FIGURA 36 Ejemplo de estadística con los Datos Generales

General Statistics

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

FIGURA 37 Ejemplo de estadística de la funcionalidad *ModemEmulator*

Modem Emulator

#	Num TCP	Num PPP	Num Datacalls	State	In Octets	Out Octets
10	0	0		0	0	0
20	0	0		0	0	0
30	0	0		0	0	0
40	0	0		0	0	0
50	0	0		0	0	0
60	0	0		0	0	0
70	0	0		0	0	0
80	0	0		0	0	0
90	0	0		0	0	0

FIGURA 38 Ejemplo de estadística de LAN

General Data

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

FIGURA 39 Ejemplo de estadística de WAN

General Data	
IMEI	353229023794959
IMSI	unknown
CID	unknown
PIN Status	NO SIM
Operator	unknown
Roaming	unknown
Network	unknown
Local Area Code	unknown
Cell Identifier	unknown
Signal Strength	unknown
Total TX KBytes	0
Total RX KBytes	0
Number of Session failures	0
SIMA Tx Bytes	0
SIMA Rx Bytes	0

Current Data Session	
Status	Inactive
IP Address	unknown
Connection Date	unknown
TX Bytes	0
RX Bytes	0
TX Rate (bps)	0
RX Rate (bps)	0

Previous Data Session	
Disconnection Date	unknown
Up Time (s)	unknown
TX Bytes	unknown
RX Bytes	unknown

FIGURA 40 Ejemplo de estadística de Routing

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

Reload

FIGURA 41 Ejemplo de estadística del servidor DHCP

DNS Servers assigned by Network Carrier	
DNS1 Server IP	0.0.0.0
DNS2 Server IP	0.0.0.0

Assigned Leases			
#	MAC	Addr	Expiration time

Reload

FIGURA 42 Ejemplo de estadística del cliente NTP

NTP	
Offset	unknown
Frequency offset	unknown
Jitter	unknown
Allan	unknown

Reload

FIGURA 43

Ejemplo de estadística de la interconexión entre puertos (*Flow*)

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

Virtual Ports						
TCP	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
1	tcp0	0	0	NA	NA	Connecting

Passive TCP	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
1	passivetcpTodos	0	84	NA	NA	Connecting
2	passivetcpPto1	0	54	NA	NA	Connecting
3	passivetcpPto4	0	122	NA	NA	Connecting
4	passivetcpPto2	0	54	NA	NA	Connecting
5	passivetcpPto3	0	54	NA	NA	Connecting

TX UDP	# Identifier	Out Octets	Out Frames	Status

RX UDP	# Identifier	In Octets	In Frames	Status

Full UDP	# Identifier	In Octets	Out Octets	In Frames	Out Frames	Status
1	Ethernet1	0	0	NA	NA	Connected
2	Ethernet1	0	0	NA	NA	Connected
3	Ethernet1	0	0	NA	NA	Connected
4	Ethernet4	0	0	NA	NA	Connected
5	Ethernet4	0	0	NA	NA	Connected
6	Ethernet2	0	0	NA	NA	Connected
7	Ethernet1	0	0	NA	NA	Connected
8	Ethernet3	0	0	NA	NA	Connected

Reload

APÉNDICE A

BIBLIOGRAFÍA Y ABREVIACIONES

APÉNDICE A**BIBLIOGRAFÍA Y ABREVIACIONES****A.1 BIBLIOGRAFÍA**

- | |
|--|
| [1] STD 15. IEEE RFC 1157. May 1990. A Simple Network Management Protocol (SNMP). |
| [2] STD 62. IEEE RFC 3416. December 2002. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (Obsoletes RFC 1905). |
| [3] IEEE RFC 1305, March 1992. Network Time Protocol (Version 3) Specification, Implementation and Analysis. |
| [4] Especificación de desarrollo de los equipos utilizados para la creación de un canal punto-multipunto via GPRS_Rev.06 (14/4/2008) de IBD referencia GPF070302CVG. |

A.2 ABREVIACIONES

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
API	Application Programming Interface
APN	Access Point Name
ASDU	Application Service Data Units
BPDU	Bridge Protocol Data Units
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name Server
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IOA	Information Object Address
IP	Internet Protocol (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	Network Address Translation
NHRP	Next Hop Resolution Protocol
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)
RADIUS	Remote Authentication Dial-In User Server
RAS	Registration, Authentication and Status
RSVP	Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator

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

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

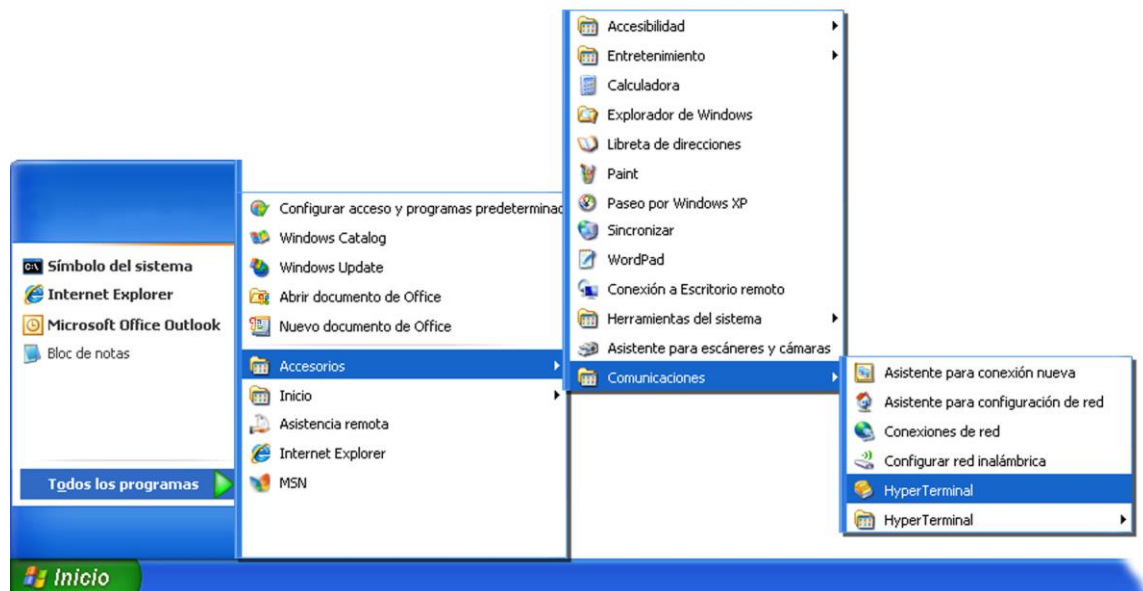
El acceso en modo local se realiza mediante un cable serie plano, conectando el puerto serie del ordenador al puerto serie del equipo (SRV).

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

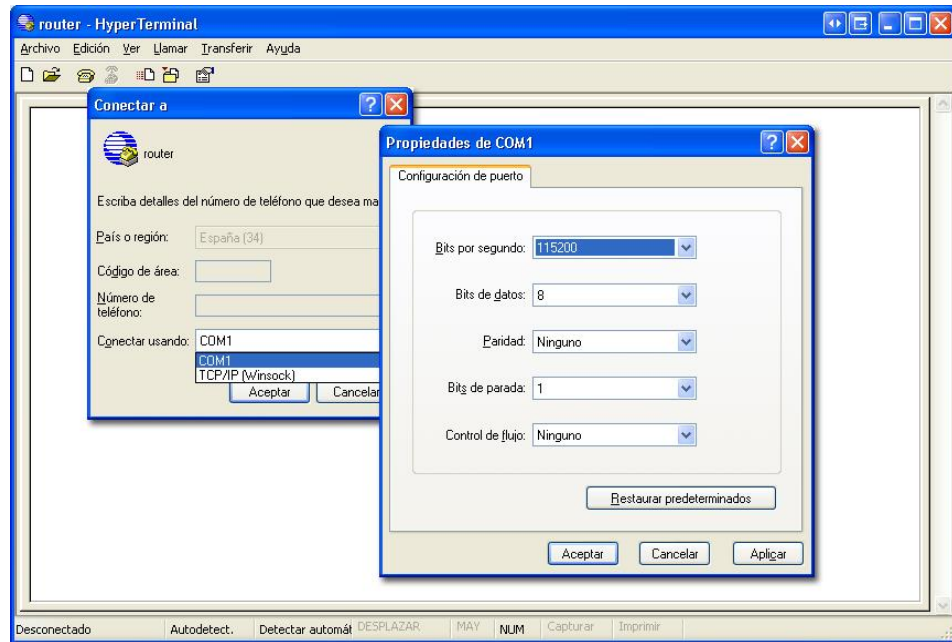
En Windows XP® se puede ejecutar *HyperTerminal* desde *Inicio* → *Todos los Programas* → *Accesorios* → *Comunicaciones* → *HyperTerminal* (véase FIGURA 44).

FIGURA 44 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 45).

FIGURA 45 Configuración de la conexión por puerto serie con *HyperTerminal*



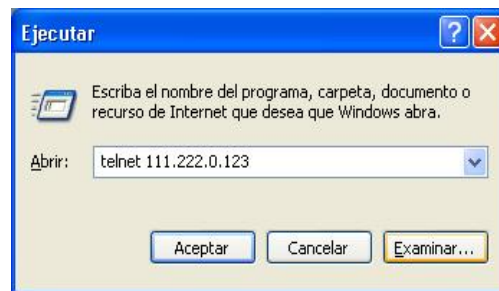
Acceso en modo remoto

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

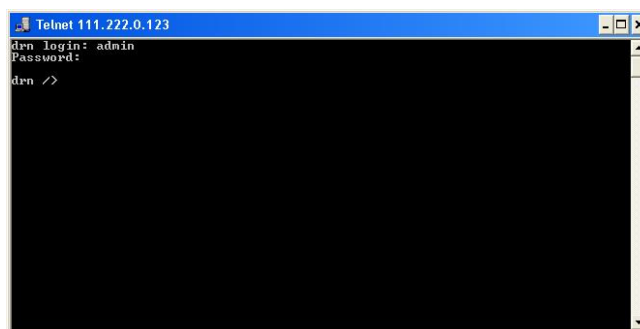
! Para emplear este modo de acceso, el equipo debe tener configurada su dirección IP y estar conectado a la red en la que se encuentra el ordenador de gestión.

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 46).

FIGURA 46 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 47).



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 3

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	Abre una sesión telenet sin interrumpir la conexión con el equipo	✓	✓

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

TABLA 4

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 /> **download**

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

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

Argumentos:

Host Nombre del host de destino de la sesión telnet.

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

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

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

Ejemplo: `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
```

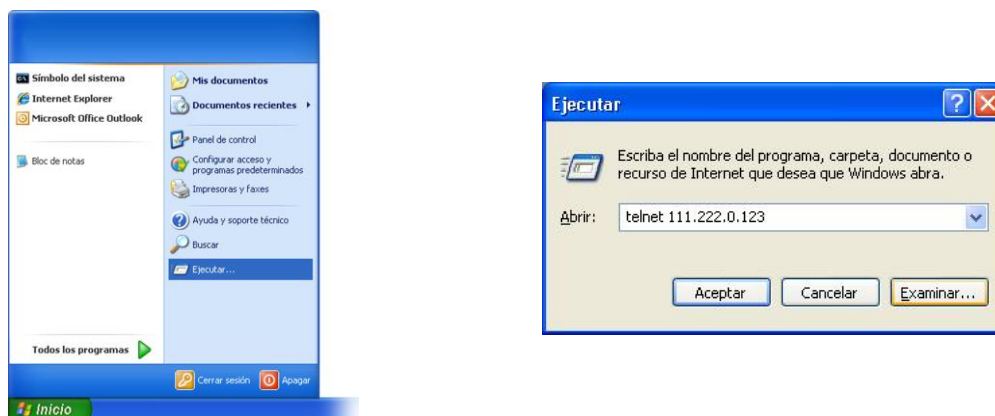
B.3 OBTENCIÓN DE INFORMACIÓN DEL ESTADO Y LA CONFIGURACIÓN DE UN EQUIPO

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

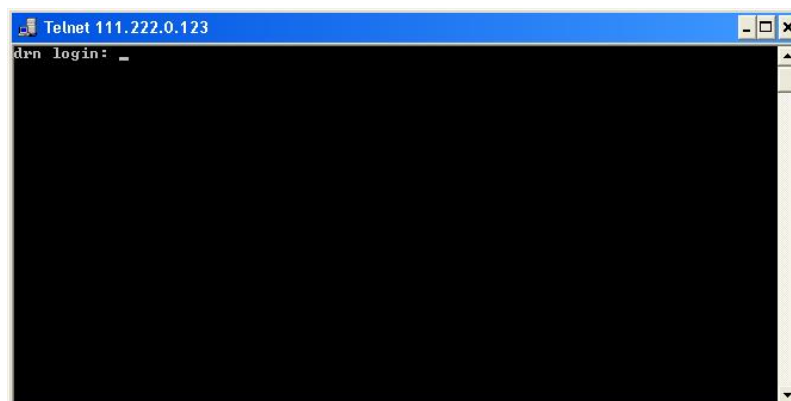
1- Conexión con el equipo

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**.



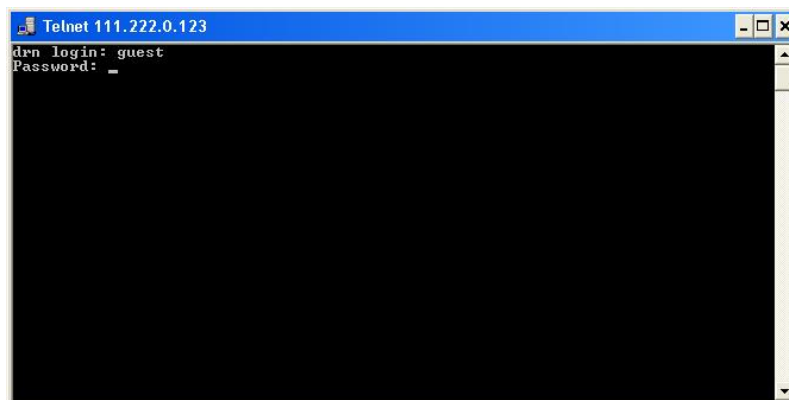
Si todo ha funcionado correctamente se abrirá una ventana de símbolo del sistema que será la interfaz de nuestra conexión.



2- Identificación del usuario

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

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

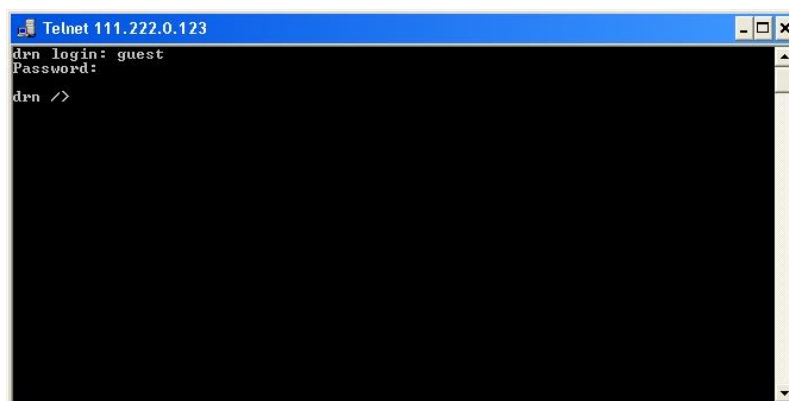


```
Telnet 111.222.0.123
drn login: guest
Password: _
```

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.

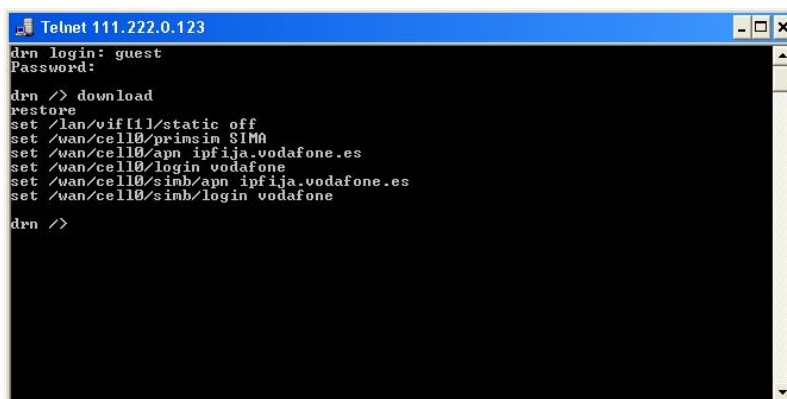
Si el usuario y password introducidos son correctos aparecerá el prompt **drn />** indicando que el equipo está a la espera de que se entre algún comando.



```
Telnet 111.222.0.123
drn login: guest
Password:
drn />
```

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.

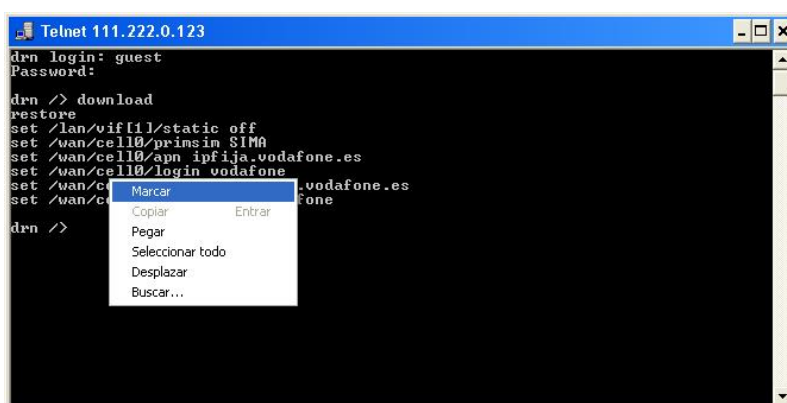


```
Telnet 111.222.0.123
drn login: guest
Password:
drn >> download
restore
set /lan/vif111/static off
set /wan/cell0/prinsin SIM0
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/sinh/apn ipfija.vodafone.es
set /wan/cell0/sinh/login vodafone
drn >>
```

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 />**.

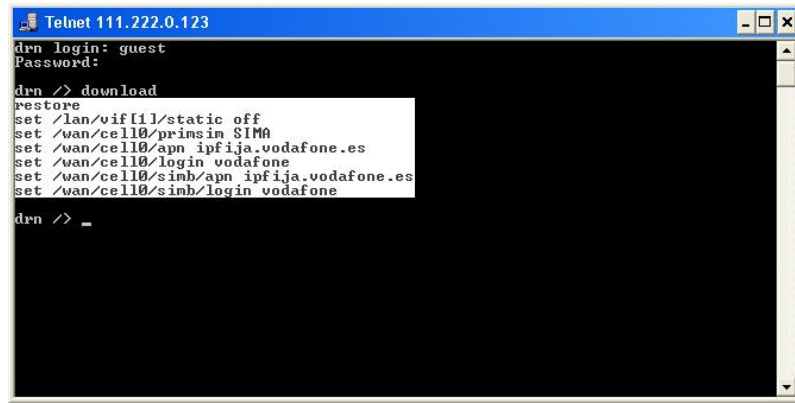
Es importante guardar la información obtenida mediante el comando **download** en un fichero **.txt** para poder utilizarla cuando se necesite.

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**.



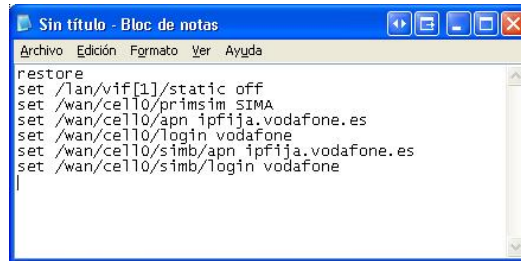
```
Telnet 111.222.0.123
drn login: guest
Password:
drn >> download
restore
set /lan/vif111/static off
set /wan/cell0/prinsin SIM0
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/c
set /wan/c
drn >>
```

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.



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

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



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

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.

```

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

Sabremos que el sistema habrá mostrado 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**.

```

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

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.

```

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

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     = SIMB
      dns_req     = on
      maxretries  = 6
      maxtoconnect = 6
      alarm_lowcov_level = -105

```



```

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

```



```

static/
st_rules[]/
[st_rules] dest gateway service if
descr
-----
1 128.127.0.0/255.255.0.0 172.16.50.254 any vlan1
rip/
enable = on
advertised_policy = permit
filter/
local/
policy = accept
cello/
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
255.255.0.192.168.0.1 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 cello-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
-----
off          1          192.168.0.1 unicast 5          10          off          1

snmp/
enable          = off
trapenable      = off
trap_v1_agent_addr = none
community[]/
[community] name  access
-----
1          public ro
traps/
cell_linkup    = off
cell_covlow    = off
cell_covhigh   = off
access/
tacacsplus/
server1_ip     = 0.0.0.0
server2_ip     = 0.0.0.0
encrypted      = on
shared_key     = *****
console/
method = local
web/
method = local
local  = on
telnet/
method = local
local  = on
security/
port[]/
[port] type max_addresses max_action
-----
1      none 10          replace
2      none 10          replace
3      none 10          replace
4      none 10          replace
5      none 10          replace
6      none 10          replace
7      none 10          replace
8      none 10          replace
drn />

```