SWITCH GIGABIT/FAST ETHERNET

TIPO SWT

MANUAL DE USUARIO

V09 - Marzo 2019

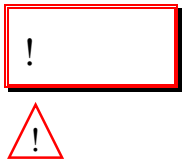
M0SWTA1903Ev09

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.

Pág.

1 INTRODUCCIÓN

1.1 GENERALIDADES

El SWT es un switch Gigabit/Fast Ethernet, especialmente diseñado para el despliegue de LANs escalables cuando las principales necesidades a cubrir son:

- la densidad de puertos,
- el rendimiento de la conmutación, y
- la complejidad lógica.

El SWT cumple con las exigencias para su uso en la automatización de las subestaciones eléctricas conforme al estándar CEI 61850.

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

El SWT también soporta los protocolos SNMPv1, SNMPv2c y SNMPv3, así como otros protocolos y servicios como LLDP, GARP/GMRP, IGMP, NTP/SNTP, TACACS+ y RADIUS.

1.2 CARACTERÍSTICAS PRINCIPALES

A continuación, se indican algunas de las prestaciones más notables del SWT.

- **Agrupación de servicios y arquitecturas.**
  Pueden agruparse y diferenciarse servicios, no siendo accesibles unos con otros, mediante la configuración de diferentes VLAN.
  Cada VLAN se distingue del resto gracias a un identificador específico, denominado VID y que se incluye en el VLAN tag, especificado en el estándar IEEE 802.1q, y permite que varias VLAN puedan compartir recursos, bien sean éstos equipos de conmutación, como el SWT, o enlaces entre equipos de conmutación, con la garantía que los tráficos de cada una de las VLAN permanecerán aislados entre sí.
  La norma 802.1q admite tres tipos de trama, las que no llevan tag (*untagged*), las que sí llevan tag con la identificación de VLAN (VID) y prioridad (*tagged*) y las que únicamente incluyen la prioridad (*priority tagged,* VLAN = 0).
  El SWT puede adaptarse a distintas arquitecturas de red tales como: estrella, doble estrella, anillo, doble anillo y anillos concatenados.

FIGURA 1 Separación del tráfico

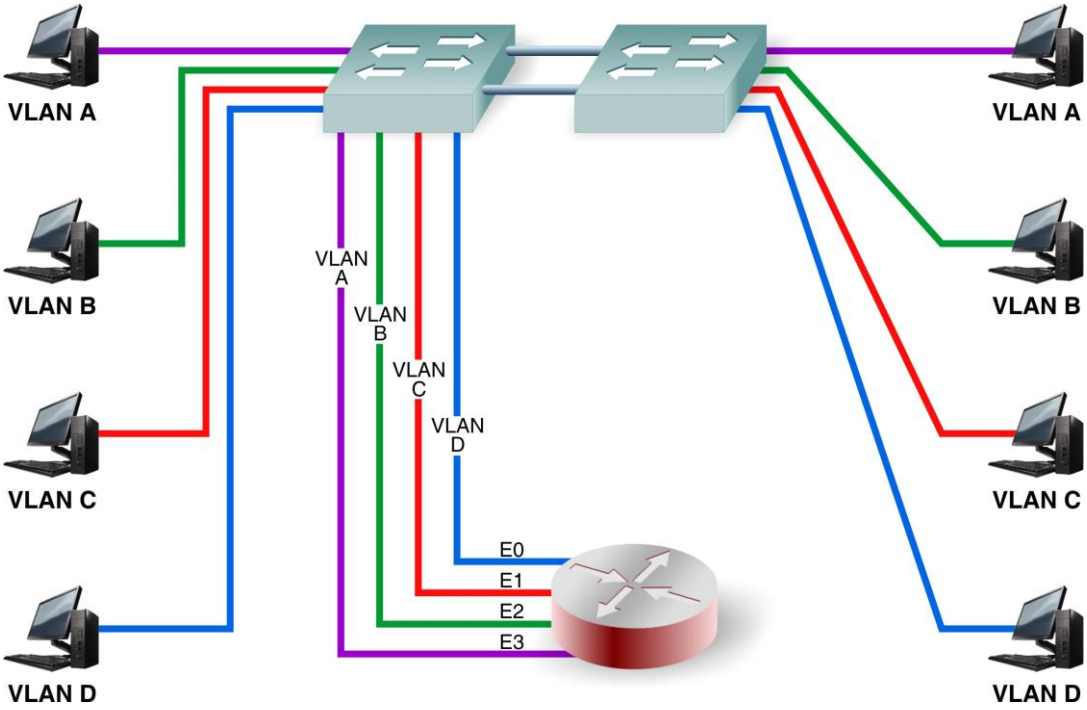


FIGURA 2 Red en estrella

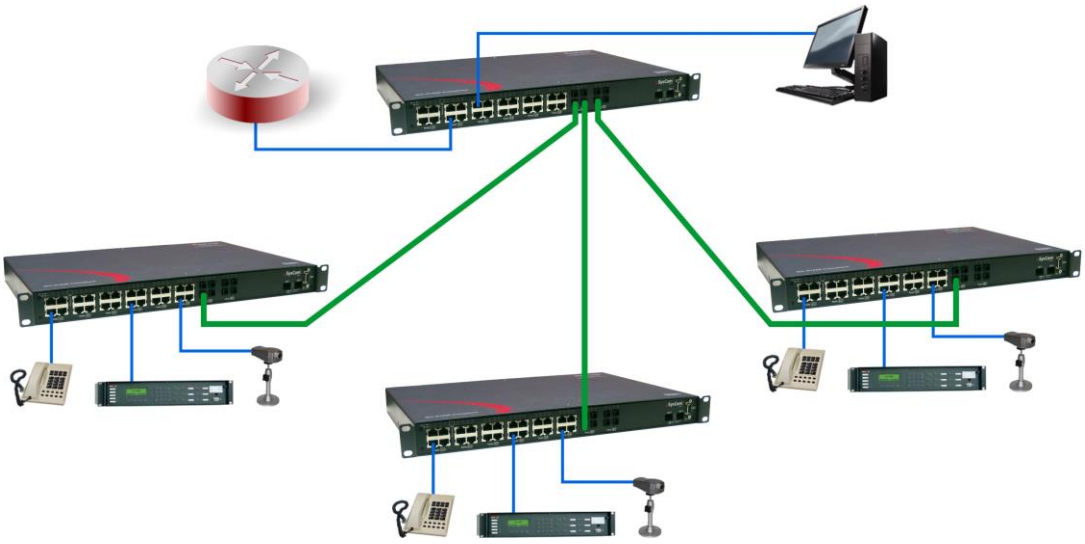
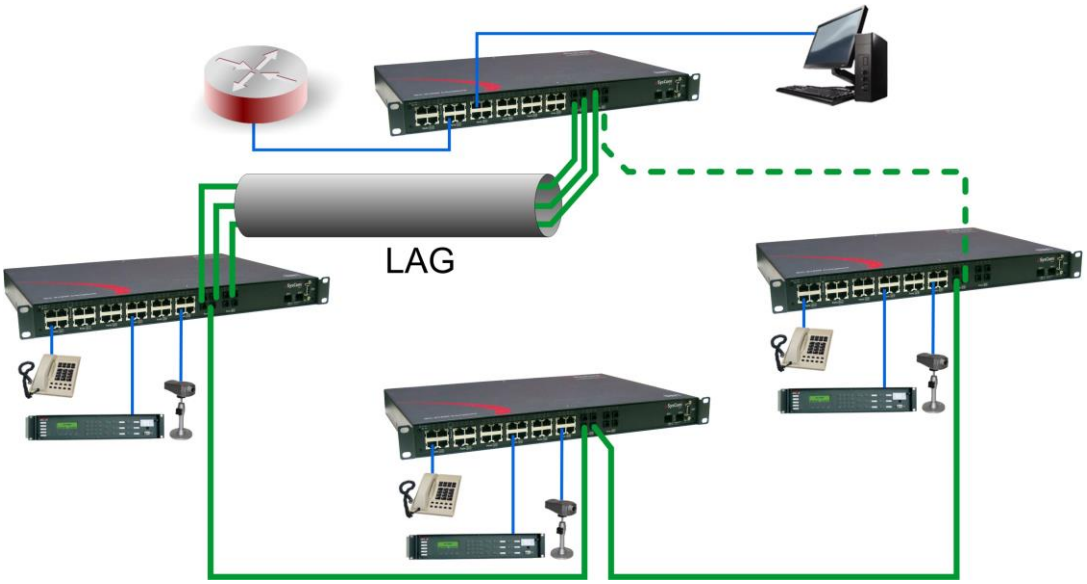


FIGURA 3 Red en anillo



❖ **Agrupación de enlaces mediante función LAG.**

La función LAG (Link Aggregation Group) permite agrupar varios enlaces en un único identificador de enlace agregado. En la Figura 3 puede verse un ejemplo de agrupación. Desde el punto de vista del protocolo STP/RSTP, la entidad de conexión es el identificador del grupo LAG, por lo que los distintos enlaces que lo forman no se manejan a título individual, de este modo no se identifican como bucles, y así se dispone del ancho de banda agregado.

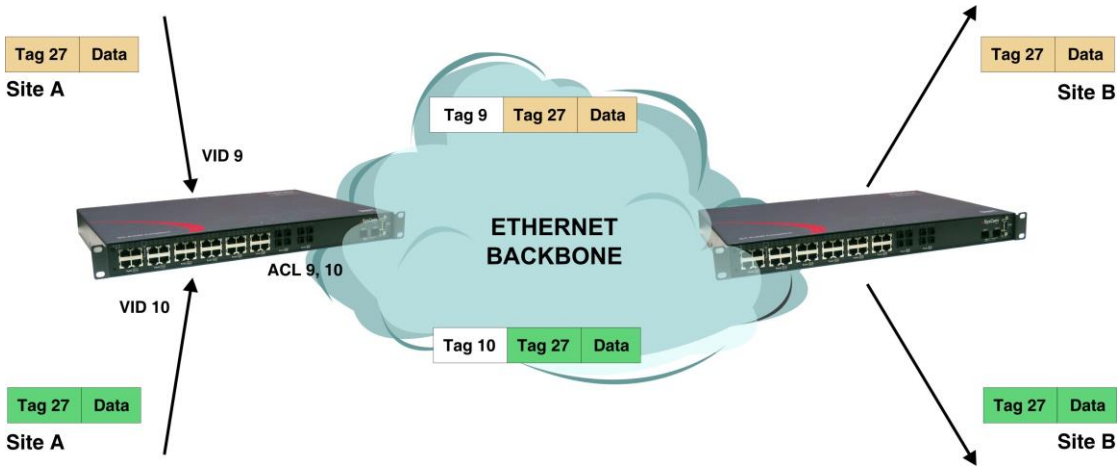
Los grupos de agregación pueden crearse para cualquiera de las funciones de interfaz previstas: usuario (*edge*, *untag*), enlace inter-switch (*trunk* o *native*) y las asociadas a la funcionalidad Q-in-Q (*access* y *core*). Una vez asignado el LAG, el comportamiento del grupo vendrá determinado por los parámetros configurados en la interfaz marcada como *Leader*.

❖ **Operación Q-in-Q.**

El SWT incluye dos funciones para proporcionar operación Q-in-Q (con doble tag). En este modo de operación, las tramas incluyen el tag original (C-TAG), bien sea el generado por el equipo cliente o el asignado por el propio switch en el momento de la recepción, y un segundo tag, el tag del proveedor (S-TAG), que será el tag empleado en la red del proveedor de interconexión.

Los túneles 802.1Q constituyen una herramienta útil a la hora de reutilizar los valores VID de identificación de las VLAN, o de transitar datos sobre redes de terceros.

FIGURA 4 Operación Q-in-Q



❖ **Implementación RSTP avanzada**

El SWT no sólo cumple los protocolos STP y RSTP para la resolución de bucles en la red y funcionamiento en anillos sino que supera los tiempos de recuperación obtenidos mediante dichos protocolos. Así, el SWT garantiza tiempos de recuperación en caso de fallo menores de 4 ms por enlace vía estándar RSTP.

❖ **Servicios críticos y seguridad.**

Los distintos servicios tienen su grado de importancia. Por ejemplo, es más prioritario el envío de órdenes para la apertura de un interruptor que el tráfico derivado de una conexión telefónica. El SWT dispone de prestaciones de Calidad de servicio (QoS) que permiten identificar los servicios críticos asegurando que todo el tráfico sea tratado con la prioridad adecuada.

Por otro lado, el SWT implementa distintas prestaciones de seguridad que evitan el acceso al sistema de tráfico no autorizado tales como: deshabilitación de puertos, restricción de tráfico en función de las direcciones MAC, protocolos de autentificación (TACACS+, RADIUS), etc.

❖ **Limitación de tráfico Broadcast.**

Para evitar la saturación de la red, el SWT permite establecer límites máximos de volumen para distintas combinaciones de mensajes *broadcast*, *multicast* y *flooding*, en cada uno de sus puertos.

- **Tráfico Multicast.**

  El SWT dispone de dos protocolos para la adecuación del tráfico multicast a las interfaces deseadas. Los protocolos son:

  - **GARP/GMRP (IEEE 802.1D 2004).** Los clientes GMRP solicitan al switch la transmisión selectiva del tráfico multicast deseado por cada uno de ellos.
  - **IGMP.** El SWT gestiona el tráfico multicast a partir de los mensajes IGMP intercambiados por los equipos cliente y los routers multicast (IGMP Snooping). Para que sea operativo, es imprescindible que el protocolo GARP/GMRP esté INACTIVO.

  El SWT también permite establecer los flujos multicast de forma explícita y manual.

- **Port mirroring.**

  El SWT permite reenviar copias del tráfico de uno o más puertos hacia otro, el puerto de monitorización, pudiendo establecer las copias de tráfico entrante o saliente en cada puerto monitorizado de forma independiente.

1.3 CONSTITUCIÓN DEL EQUIPO

El SWT se suministra en un chasis de 1U y 19 pulgadas de anchura, preparado para montaje en rack.

Incluye una interfaz serie de mantenimiento (modo DCE) y un conector I/O (véase apartado 2.8), y puede incluir 4 bahías SFP Gigabit Ethernet y hasta 32 puertos, frontales o posteriores.

El SWT presenta una estructura mecánica de cuatro de cuatro bloques para la instalación de los puertos. Véase en el apartado 1.4.2, *Interfaces del equipo,* los tipos de bloques disponibles y sus requisitos.

En lo que respecta a la fuente de alimentación principal, la misma puede ser CC aislada o multirango (Vcc y Vca). También puede incluir una fuente de alimentación redundante CC aislada o multirango (Vcc y Vca) y, en el modelo con puertos frontales, una fuente de alimentación PoE para la conexión directa de dispositivos IP (IEEE 802.3 af) en los cuatro primeros puertos (1 a 4) eléctricos.

1.4 ESPECIFICACIONES TÉCNICAS

1.4.1 Características del switch

- Core de conmutación Full Duplex Wired Speed.
- Detección automática de velocidad del puerto.
- STP y RSTP para resolución de bucles en la red y funcionamiento en anillos.
- Gestión de múltiples VLANs (250 simultáneamente).
- QoS:
  - el SWT puede usar los campos de prioridad incluidos tanto en el tag IEEE 802.1p,
  - como el identificador DSCP incluido en la cabecera IP.
- Limitación de tráficos Broadcast y Multicast (Broadcast Storm Control).
- Listas de control de acceso MAC y autentificación de usuarios 802.1x.
- Operación Q-in-Q (con doble tag).
- Agrupación de enlaces mediante función LAG (Link Aggregation Group), estática, según IEEE 802.1ad.
- Port mirroring.
- Enlaces en modo Native VLAN.
- Interoperación con IEDs (Intelligent Electronic Device) conforme al estándar CEI 61850.

1.4.2 Interfaces del equipo

- Hasta 32 puertos, frontales o posteriores.

  El chasis presenta una estructura mecánica de **hasta cuatro bloques** para la instalación de los puertos. Los tipos de bloque a combinar son los siguientes:

  - Bloque de **8** puertos tipo **10/100Base-Tx** con conector **RJ-45**.
  - Bloque de **8** puertos tipo **10/100Base-Tx** con conector **RJ-45** y **PoE** en los cuatro primeros puertos (siempre frontales). Un bloque de este tipo como máximo.
  - Bloque de **4** u **8** puertos tipo **100Base-Fx multimodo** (1300 nm) con conector **MT-RJ**.
  - Bloque de **2** u **4** puertos tipo **100Base-Fx multimodo** (1300 nm) con conector **ST**.

- Bloque de **4 u 8** puertos tipo **100Base-Fx multimodo** (1300 nm) con conector **LC**.
- Bloque de **4 u 8** puertos tipo **100Base-Lx monomodo** (1300 nm) con conector **LC SM**.
- Bloque de **2 u 4** puertos tipo **100Base-Fx multimodo** (1300 nm) con conector **SC.**

Los bloques deben instalarse de forma consecutiva, de izquierda a derecha, y sin dejar slots vacíos.

De haber puertos eléctricos, éstos deben ir siempre en primer lugar.

De usarse únicamente puertos de fibra óptica, se admiten 24 puertos como máximo. En la primera posición, no deben instalarse bloques de puertos con 4 conectores MT-RJ, con 2 conectores ST, con 2 conectores SC o con 4 conectores LC (LC SM).

- 1 consola de servicio (modo DCE).
- 4 bahías SFP Gigabit Ethernet (véase apartado 1.4.3, *Accesorios*), frontales o posteriores.
- 1 conector I/O con una entrada y una salida digitales, gestionables vía SNMP.
  La salida digital puede configurarse como alarma.

1.4.3 Accesorios

- Módulos SFP Gibabit/Fast Ethernet.
  La lista que sigue a continuación corresponde a módulos verificados, los cuales cumplen los criterios de temperatura.
  - SFP 1000BaseT (4CZ07980001)
    tipo de conector: RJ-45
  - SFP 1000BaseSx (4CZ07980002)
    tipo de conector: LC
    tipo de fibra: multimodo
    longitud de onda: 850 nm
    distancia máxima típica: 550 m
  - SFP 1000BaseZx (4CZ07980004)
    tipo de conector: LC
    tipo de fibra: monomodo
    longitud de onda: 1530 nm
    distancia máxima típica: 80 km
  - SFP 1000BaseLx (4CZ07980005)
    tipo de conector: LC
    tipo de fibra: monomodo
    longitud de onda: 1310 nm
    distancia máxima típica: 10 km

- SFP 100BaseEx (4CZ07980008)
  tipo de conector: LC
  tipo de fibra: monomodo
  longitud de onda: 1310 nm
  distancia máxima típica: 40 km

- SFP 100BaseFx (4CZ07980006)
  tipo de conector: LC
  tipo de fibra: monomodo
  longitud de onda: 1310 nm
  distancia máxima típica: 10 km

- SFP 100BaseFx (4CZ07980007)
  tipo de conector: LC
  tipo de fibra: multimodo
  longitud de onda: 1310 nm
  distancia máxima típica: 2 km

➢ Pigtails fibra óptica y cable.

- Cable plano CAT6 STP RJ45, longitud 3m (4GL03000141).
- Fibra multimodo MTRJ-MTRJ, longitud 2m (4CZ05000010).
- Fibra multimodo MTRJ-SC, longitud 2m (4CZ05000011).
- Fibra multimodo MTRJ-ST, longitud 2m (4CZ05000012).
- Fibra multimodo MTRJ-LC, longitud 2m (4CZ05000013).
- Fibra multimodo LC-LC, longitud 2m (4CZ05000014).
- Fibra monomodo LC-LC, longitud 2m (4CZ05000015).

1.4.4 Gestión del equipo

➢ Acceso local y remoto mediante consola o a través de un servidor web incorporado, HTTP o HTTPS, conexión SSH y Telnet.

1.4.5 Servicios adicionales

➢ Agente SNMP (SNMPv1, SNMPv2c y SNMPv3).

➢ Servidor NTP, y cliente NTP/SNTP.

➢ Cliente TACACS+.

➢ Cliente RADIUS.

➢ GARP/GMRP (IEEE 802.1D 2004).

➢ IGMP snooping.

➢ LLDP (IEEE 802.1AB 2016).

1.4.6 Certificaciones

- CE.
- Diseñado para Aplicaciones Industriales.
- Diseñado para Subestaciones Eléctricas.

1.4.7 Características mecánicas

- Chasis mecánico: panel de 1U y 19 pulgadas de anchura.
- Dimensiones: Altura: 44 mm; Anchura: 445 mm; Profundidad: 283 mm. Véase FIGURA 5
- Peso: 3,4 kg
- Grado de protección IP: IP 2xB
- Material: Hierro galvanizado pintado exteriormente en gris (RAL 7024)

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

1.4.8 Condiciones de funcionamiento

- Alimentación: 36-72 Vcc ó multirango (80-360 Vcc, 80-260 Vca).

  Posibilidad de alimentación redundante y, en el modelo con puertos frontales, opción de alimentación PoE para los cuatro primeros puertos (1 a 4) eléctricos.

  En el modelo para funcionamiento en corriente continua, la fuente está protegida mediante diodo contra inversión de polaridad.
  El modelo multirango soporta inversión de polaridad.

- Consumo: Consumo máximo a 48 Vcc: 40 W.

  Consumo PoE máximo a repartir entre puertos P1 a P4 eléctricos: 12 W.

- Rango de temperatura: -25ºC a +70ºC

- Humedad relativa: No superior al 95%, según CEI 721-3-3 clase 3K5 (climatograma 3K5).

- Seguridad eléctrica: Según la norma EN 60950.

- Emisiones R.F.: Según la norma EN 55022.

- Rigidez dieléctrica: Según la norma EN 60255-5.

- Compatibilidad electromagnética.

  - Inmunidad a las descargas electrostáticas:
    según la norma EN 61000-4-2.
  - Inmunidad a los campos electromagnéticos permanentes de R.F.:
    según la norma EN 61000-4-3.
  - Inmunidad a los transitorios rápidos en ráfagas:
    según la norma EN 61000-4-4.
  - Inmunidad a la onda de choque:
    según la norma EN 61000-4-5.
  - Inmunidad a las perturbaciones conducidas por campos de R. F.:
    según la norma EN 61000-4-6.
  - Inmunidad a los campos electromagnéticos a frecuencia industrial:
    según la norma EN 61000-4-8.
  - Inmunidad a los campos magnéticos oscilatorios amortiguados:
    según la norma EN 61000-4-10.
  - Inmunidad a los armónicos de baja frecuencia:
    según la norma EN 61000-4-13.
  - Inmunidad a la onda oscilatoria amortiguada:
    según la norma EN 61000-4-18.
  - Inmunidad a los huecos, interrupciones y variaciones de tensión en c.a.:
    según la norma EN 61000-4-11.
  - Inmunidad a los huecos, interrupciones y variaciones de tensión en c.c.:
    según la norma EN 61000-4-29.

1.5 ADVERTENCIAS

1.5.1 Advertencias previas

! **1.** La instalación del SWT en una Subestación Eléctrica o Centro de Transformación (CT) está sujeta de modo genérico al cumplimiento de todas las medidas de seguridad y de prevención de riesgos laborales que para este entorno de trabajo tenga establecida la compañía eléctrica usuaria de estos dispositivos y de los estándares de seguridad (EN 50110).

2. De modo específico, para la instalación y manipulación del SWT se deben cumplir los siguientes requisitos:

- Únicamente personal cualificado y designado por la compañía propietaria de la instalación debe llevar a cabo la instalación y manipulación del SWT.
- El entorno de funcionamiento debe ser el apropiado para el SWT, asegurando el cumplimiento de las condiciones indicadas en el apartado 1.4.8.

3. ZIV no se hace responsable de cualquier daño a personas, instalaciones o a terceros derivados del no cumplimiento de los puntos 1 y 2.

1.5.2 Consideraciones de seguridad del equipo

! **1.** El equipo dispone de dos modelos de fuente de alimentación:
- el modelo de 48 Vcc aislada
- el modelo Multirango Vcc/Vca.

Cuando el equipo contenga el modelo de fuente Multirango, debe realizarse la conexión de la toma de tierra antes de conectar cualquier cable de alimentación.

En el modelo 48 Vcc aislada, esta conexión no es obligatoria pero es recomendable llevarla a cabo.

2. ZIV no se hace responsable no se hace responsable de cualquier daño a personas o a terceros derivados del no cumplimiento del punto 1.

! **1.** El equipo contiene componentes sensibles a la electricidad estática, por lo que se deben cumplir los siguientes requisitos:
- El personal designado para llevar a cabo la instalación y mantenimiento del switch SWT debe estar siempre libre de electricidad estática, por lo que siempre debe emplear una pulsera antiestática y/o talonera conectada a tierra.
- El habitáculo del SWT debe estar libre de elementos que faciliten la generación de electricidad estática y, en el caso de los suelos provistos de moqueta, que ésta sea antiestática.

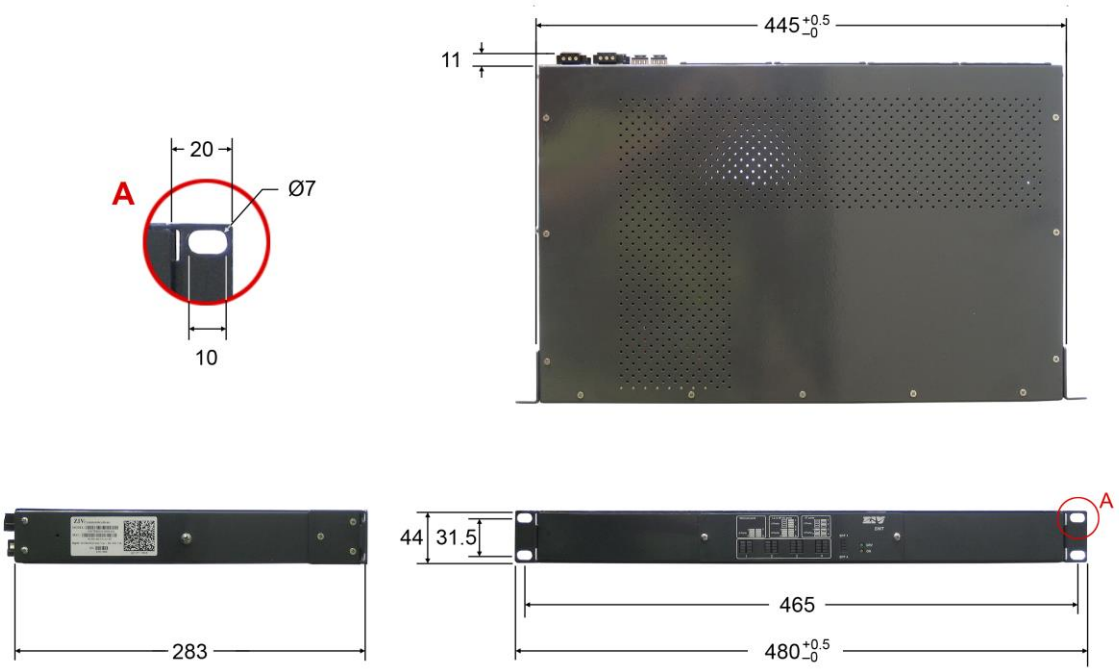
2. ZIV no se hace responsable de cualquier daño que pueda sufrir el equipo derivado del no cumplimiento del punto 1.

2 CARACTERÍSTICAS MECÁNICAS Y ELÉCTRICAS

Los distintos elementos que conforman el switch Gigabit/Fast Ethernet tipo SWT están contenidos en un panel de una unidad normalizada de altura y 19 pulgadas de anchura, preparado para montaje en rack.

En la FIGURA 5 se indican las dimensiones generales en mm, así como la posición de los taladros de sujeción.

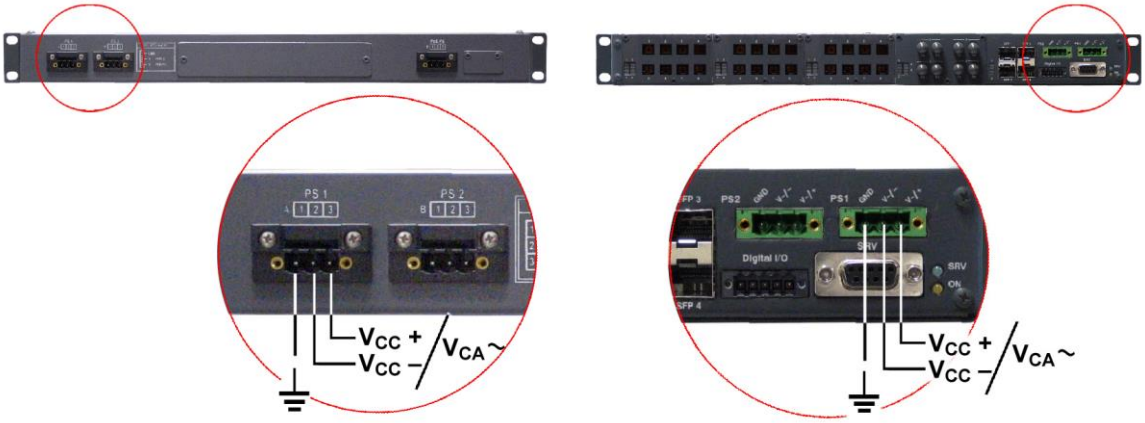
FIGURA 5 Dimensiones generales en mm del SWT



El SWT se alimenta a una tensión nominal de 48 V_{CC} (aislada) o a una tensión continua y alterna (80-360 Vcc, 80-260 Vca), a través del conector que se muestra en la FIGURA 6.

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

FIGURA 6 Disposición del conector de alimentación principal (PS 1) y alternativa (PS 2)



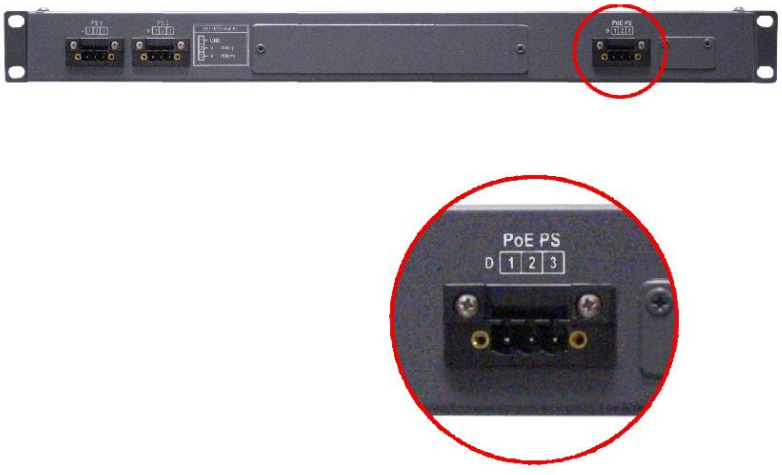
a) Vista posterior panel con puertos frontales

b) Vista posterior panel con puertos posteriores

En el modelo del SWT con puertos frontales, los cuatro primeros puertos 10/100Base-Tx, identificados como puertos 1 a 4, admiten la opción de alimentación PoE, la cual se lleva a cabo a través del conector que se muestra en la FIGURA 7. Las interfaces PoE proporcionan alimentación a los equipos cliente usando el propio cable Ethernet, por ejemplo teléfonos IP (IEEE 802.3 af).

El SWT puede incluir dos fuentes de alimentación, principal (PS 1) y alternativa (PS 2), y en el modelo con puertos frontales la fuente de alimentación PoE (PoE PS).

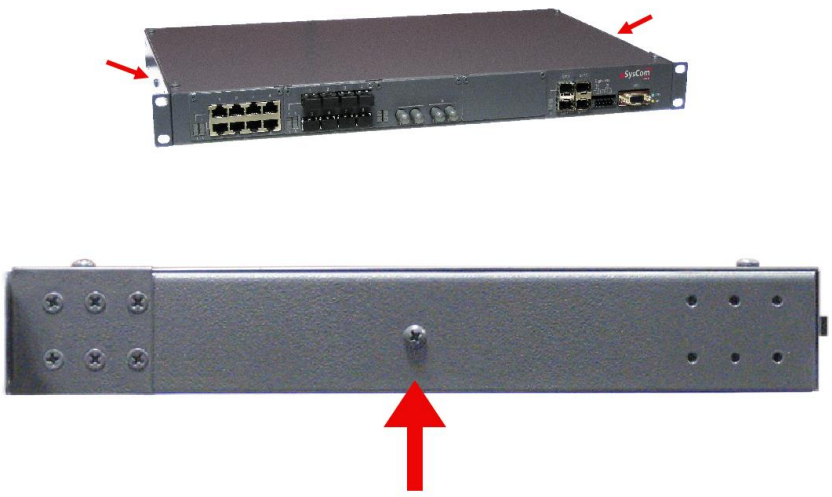
FIGURA 7 Disposición del conector de alimentación PoE (PoE PS) en panel con puertos frontales



Asimismo, se encuentra disponible una conexión a tierra, véase FIGURA 8. Esta conexión debe realizarse en el modelo de fuente multirango, antes de conectar cualquier cable de alimentación.

En el modelo de fuente de 48 Vcc aislada, esta conexión no es obligatoria pero es recomendable llevarla a cabo.

FIGURA 8 Disposición de la conexión a tierra



El SWT puede estar equipado con 4 bahías SFP Gigabit Ethernet y con hasta 32 puertos, frontales o posteriores.

El SWT presenta una estructura mecánica de cuatro bloques para la instalación de los puertos. Véase en el apartado 1.4.2, *Interfaces del equipo*, los tipos de bloques disponibles y sus requisitos.

La FIGURA 9 muestra un ejemplo de vista frontal del SWT equipado con 4 bahías SFP Gigabit Ethernet y con 26 puertos Fast Ethernet ***frontales***, los 16 primeros en configuración 10/100Base-Tx (RJ-45), los 8 siguientes en configuración 100Base-Fx (multimodo, MT-RJ) y los 2 restantes en configuración 100Base-Fx (multimodo, ST).

La FIGURA 10 muestra un ejemplo de vista posterior del SWT equipado con 4 bahías SFP Gigabit Ethernet y con 24 puertos Fast Ethernet ***posteriores***, los 16 primeros en configuración 100Base-Fx (multimodo, MT-RJ) y los 8 restantes en configuración 100Base-Fx (multimodo, ST).

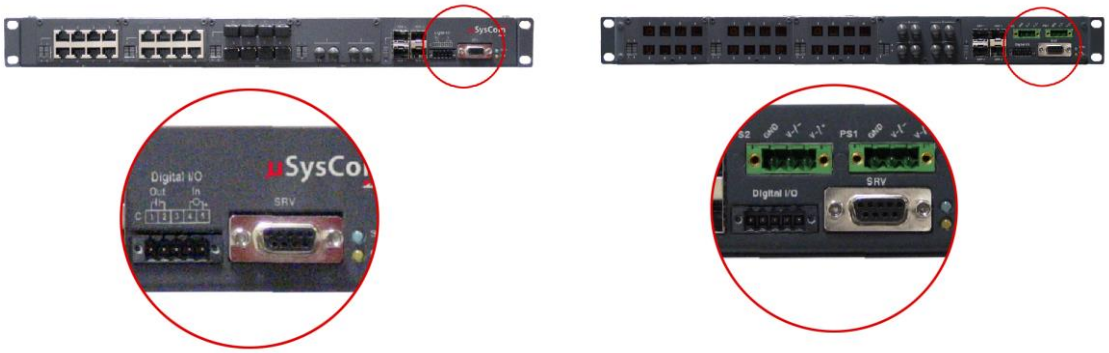
Las características eléctricas de los conectores y su utilización se indican en los apartados 2.1 a 2.8.

FIGURA 9 Vista frontal del panel SWT con 26 puertos Fast Ethernet ***frontales*** y 4 bahías SFP

FIGURA 10 Vista posterior del panel SWT con 24 puertos Fast Ethernet ***posteriores*** y 4 bahías SFP

Como puede verse en la FIGURA 11, en la parte derecha se encuentra un conector de mantenimiento, identificado como SRV, para el acceso al equipo mediante consola, y un conector I/O.

FIGURA 11 Disposición del conector de mantenimiento SRV y del conector I/O



a) Vista frontal panel con puertos frontales

b) Vista posterior panel con puertos posteriores

Las características eléctricas del conector I/O se indican en el apartado 2.8.

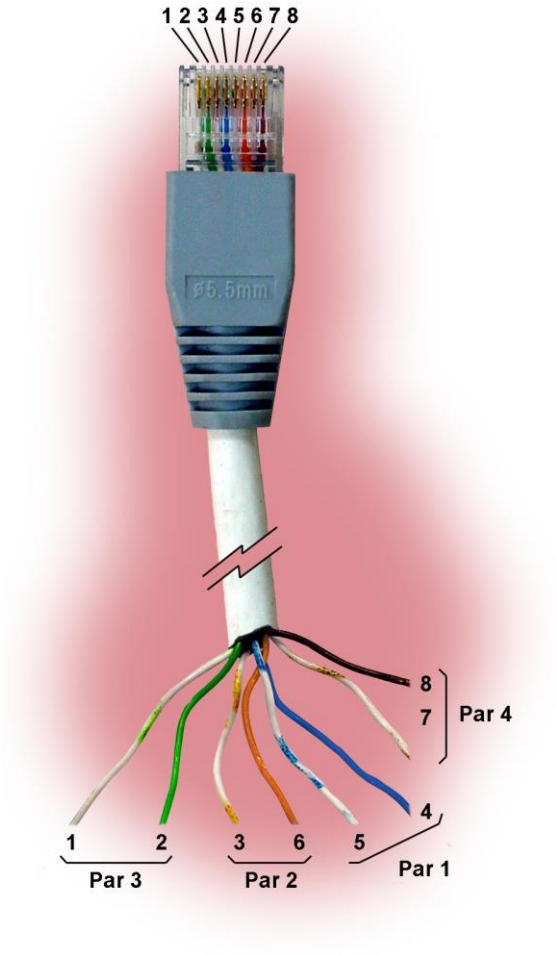
Las características eléctricas del conector de mantenimiento y su utilización se indican en el apartado 2.7, *Puerto SRV*. El conector está provisto de tapón de protección.

2.1 PUERTOS 10/100BASE-TX (RJ-45)

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

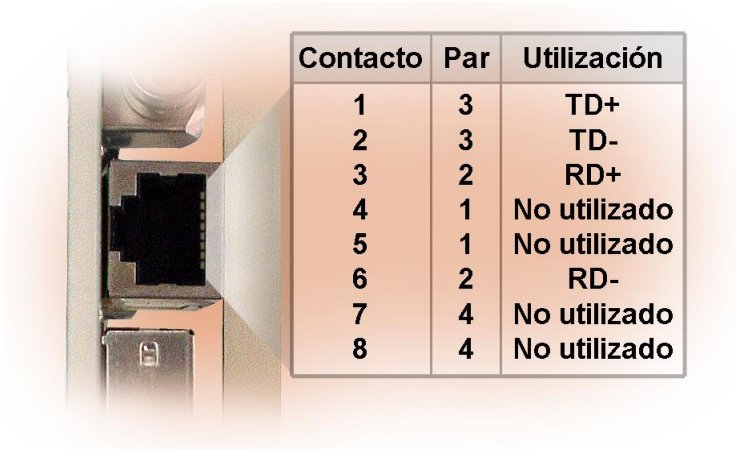
El cable UTP-5 está formado por ocho hilos de cobre, que componen los cuatro pares trenzados, cubiertos por un plástico de aislamiento de diferente color. El color de los hilos que componen cada uno de los pares, según el estándar ANSI/TIA/EIA-568-A, es el que se indica en la FIGURA 12.

FIGURA 12 Cable de pares trenzados no blindados categoría cinco (UTP-5) con conector RJ-45 según el estándar ANSI/TIA/EIA-568-A



En la FIGURA 13 se indica la utilización de cada uno de los contactos del conector RJ-45 además del par al que pertenecen según el estándar ANSI/TIA/EIA-568-A, en la interfaz de red 10/100Base-Tx.

FIGURA 13 Señales del conector RJ-45 en la interfaz 10/100Base-Tx

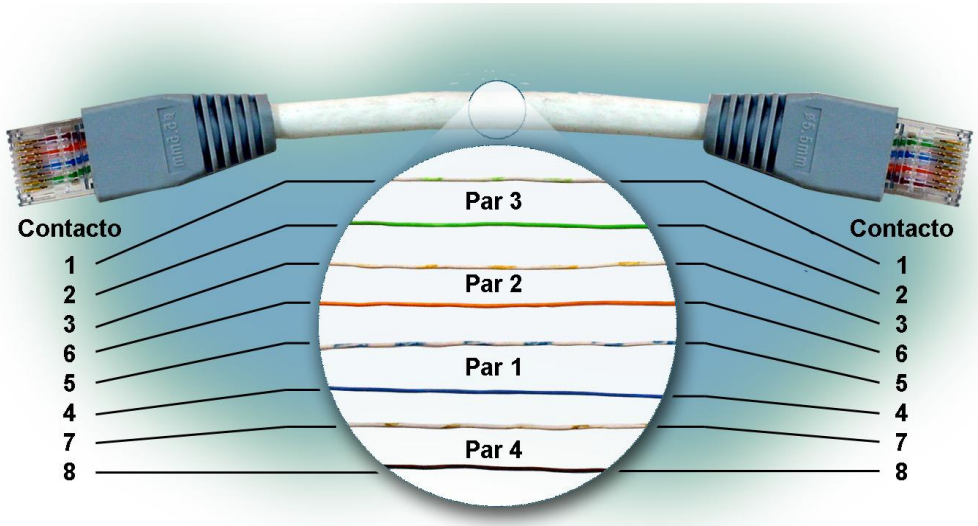


Contacto	Par	Utilización
1	3	TD+
2	3	TD-
3	2	RD+
4	1	No utilizado
5	1	No utilizado
6	2	RD-
7	4	No utilizado
8	4	No utilizado

En los puertos que admiten la opción de alimentación PoE, puertos 1 a 4 eléctricos, el par 1 se utiliza para la conexión VccPoE+ y el par 4 para la conexión VccPoE-.

Los cables utilizados deben ser cables de conexión directa, véase FIGURA 14, en los que los 4 pares se corresponden en ambos extremos del cable.

FIGURA 14 Cable de conexión directa



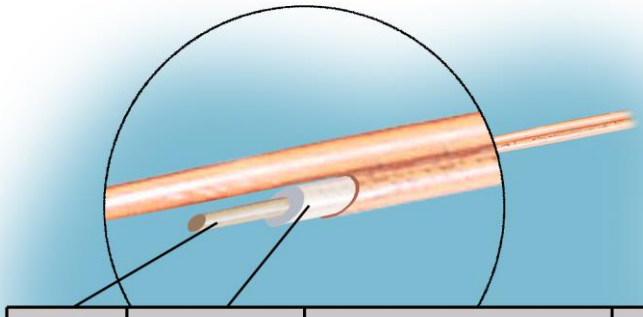
2.2 PUERTOS 100BASE-FX (MULTIMODO, MT-RJ)

En cada puerto 100Base-Fx de este tipo, se encuentra dispuesto un conector tipo MT-RJ. El cable requerido para llevar a cabo la conexión debe ser un cable de fibra óptica compuesto de dos fibras ópticas multimodo, una para transmitir datos y otra para recibir. Cada una de las fibras debe tener un diámetro de 125 µm. En este diámetro están incluidos el núcleo y el revestimiento de la fibra, como se aprecia en la FIGURA 15. El diámetro del núcleo puede ser de 50 µm o 62,5 µm. La longitud de onda utilizada debe ser de 1300 nm (multimodo). La longitud del cable no debe ser superior a 2 km.

En la FIGURA 15, además, se indican las características más importantes de potencia óptica de entrada y salida en función del tipo de fibra multimodo utilizado.

Todos los conectores tipo MT-RJ disponen de un tapón de protección.

FIGURA 15 Fibra óptica multimodo



Núcleo	Revestimiento	Potencia óptica de entrada		Potencia óptica de salida genérica
		Mínima	Máxima	
Ø62,5 µm	Ø125 µm	-33,5 dBm	-11,8 dBm	-15,7 dBm
Ø50 µm	Ø125 µm	-33,5 dBm	-11,8 dBm	-20,3 dBm

2.3 PUERTOS 100BASE-FX (MULTIMODO, ST ó SC)

En cada puerto 100Base-Fx de este tipo, se encuentra dispuesto un conector tipo ST ó SC. El cable requerido para llevar a cabo la conexión debe ser un cable de fibra óptica compuesto de dos fibras ópticas multimodo, una para transmitir datos y otra para recibir. Cada una de las fibras debe tener un diámetro de 125 µm. En este diámetro están incluidos el núcleo y el revestimiento de la fibra, como se aprecia en la FIGURA 15. El diámetro del núcleo puede ser de 50 µm o 62,5 µm. La longitud de onda utilizada debe ser de 1300 nm (multimodo). La longitud del cable no debe ser superior a 2 km.

En la FIGURA 15, además, se indican las características más importantes de potencia óptica de entrada y salida en función del tipo de fibra multimodo utilizado.

Todos los conectores tipo ST ó SC disponen de un tapón de protección.

2.4 PUERTOS 100BASE-FX (MULTIMODO, LC)

En cada puerto 100Base-Fx de este tipo, se encuentra dispuesto un conector tipo LC. El cable requerido para llevar a cabo la conexión debe ser un cable de fibra óptica compuesto de dos fibras ópticas multimodo, una para transmitir datos y otra para recibir. Cada una de las fibras debe tener un diámetro de 125 µm. En este diámetro están incluidos el núcleo y el revestimiento de la fibra, como se aprecia en la FIGURA 15. El diámetro del núcleo puede ser de 50 µm o 62,5 µm. La longitud de onda utilizada debe ser de 1300 nm (multimodo). La longitud del cable no debe ser superior a 2 km.

En la FIGURA 15, además, se indican las características más importantes de potencia óptica de entrada y salida en función del tipo de fibra multimodo utilizado.

Todos los conectores tipo LC disponen de un tapón de protección.

2.5 PUERTOS 100BASE-LX (MONOMODO, LC)

En cada puerto 100Base-Lx de este tipo, se encuentra dispuesto un conector tipo LC monomodo. El cable requerido para llevar a cabo la conexión debe ser un cable de fibra óptica compuesto de dos fibras ópticas monomodo, una para transmitir datos y otra para recibir. Cada una de las fibras debe tener un diámetro de 125 µm. En este diámetro están incluidos el núcleo y el revestimiento de la fibra. El diámetro del núcleo es de 9 µm. La longitud de onda utilizada debe ser de 1300 nm (monomodo). La longitud del cable no debe ser superior a 10 km.

Las características más importantes de potencia óptica de entrada y salida son las siguientes:

Potencia óptica de entrada		**Potencia óptica de salida**	
Mínima	**Máxima**	**Mínima**	**Máxima**
-25 dBm	-8 dBm	-15 dBm	-8 dBm

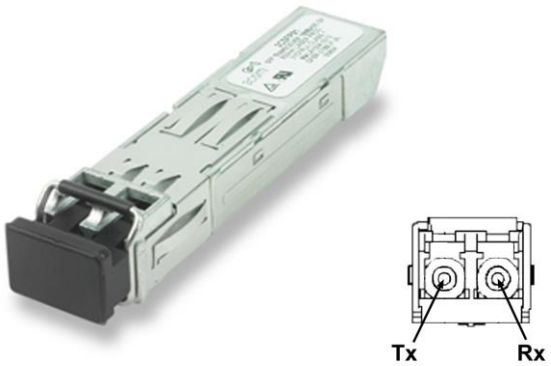
Todos los conectores tipo LC monomodo disponen de un tapón de protección.

2.6 PUERTOS SFP

Las bahías disponibles en el frontal del equipo admiten la instalación de módulos SFP (Small Form Factor Pluggable), que proporcionan al switch interfaces Gigabit Ethernet ópticas; las características de la fibra óptica a emplear así como el tipo de conector dependerá del módulo SFP utilizado. Véanse los módulos disponibles en el apartado 1.4.3, *Accesorios*.

Las bahías disponen de un tapón de protección.

FIGURA 16 Módulos SFP



Procedimiento de inserción de un módulo SFP

El procedimiento de inserción de un módulo SFP es el siguiente:

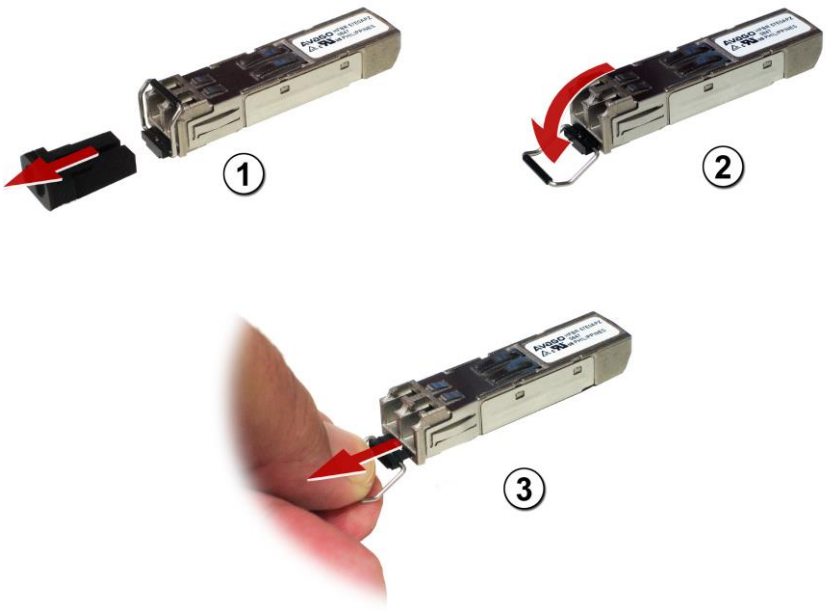
1. Extraer el módulo SFP de su embalaje de protección.
2. Verificar que el módulo SFP es el apropiado para la correcta configuración de la red.
3. Sujetar el módulo entre los dedos pulgar e índice.
4. Insertar el módulo en la ranura SFP correspondiente del frontal del equipo.
5. Retirar los protectores contra suciedad de las bocas ópticas del módulo.
6. Insertar las fibras, en las bocas ópticas del módulo, respetando la dirección de los datos TX y RX (véase FIGURA 16).

Procedimiento de extracción de un módulo SFP

El procedimiento de extracción de un módulo SFP es el siguiente:

1. Desconectar la fibra óptica del conector del módulo SFP.
2. Bajar la palanca de seguridad del módulo.
3. Extraer el módulo del puerto del equipo tirando de la palanca de seguridad (si el SFP no se desliza fácilmente por la ranura del equipo, aplicar un suave movimiento de lado a lado mientras que se tira, firmemente, del SFP hacia el exterior).

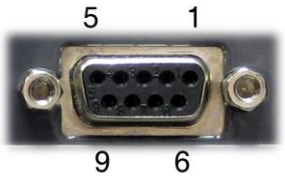
FIGURA 17 Extracción de un módulo SFP



2.7 PUERTO SRV

Las características eléctricas del conector de mantenimiento y su utilización se indican a continuación. El conector está provisto de tapón de protección.

FIGURA 18 Disposición del conector de mantenimiento SRV



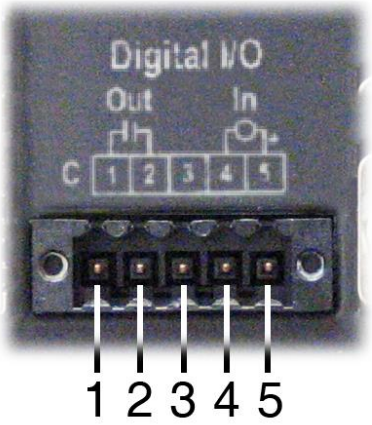
Pin	RS-232
2	RD
3	TD
5	GND

	CONECTOR SRV (en modo DCE)
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)

2.8 CONECTOR I/O

La entrada y la salida del conector I/O, ambas gestionables vía SNMP, están aisladas galvánicamente. El conexionado, así como las características físicas más importantes del conector, se indican a continuación.

FIGURA 19 Disposición del conector I/O



Contacto	Utilización
1	Salida -
2	Salida +
3	No conectado
4	Entrada -
5	Entrada +

ENTRADA (contacto 4 y 5)		SALIDA (Contacto 1 y 2)	
Entrada Inactiva	Tensión Entr < 8 Vcc (entre contactos 4 y 5)	**Salida Activa**	Impedancia <26 Ω (entre contactos 1 y 2)
Entrada Activa	Tensión Entr > 10 Vcc (entre contactos 4 y 5)	**Salida Inactiva**	Impedancia> 500 MΩ (entre contactos 1 y 2)
Tensión máx.	250 Vcc Protegida contra sobretensiones >270 Vcc	**Tensión máx.**	250 Vcc Protegida contra sobretensiones >270 Vcc No puede aplicarse Vca
Drenaje corriente CC máx.	12 mA	**Corriente CC máx.**	150 mA
Polaridad	El contacto 4 es la referencia para ENTRADA- y el contacto 5 para la ENTRADA+ Protegida contra error de polaridad	**Polaridad**	Contacto 1 conectado a SALIDA-- y contacto 2 a SALIDA+
Tiempo conmutación ON/OFF	~1 ms	**Tiempo conmutación ON/OFF**	2 ms

3 SEÑALIZACIÓN DE LOS LEDS

El SWT dispone de dos LEDs de base (SRV y ON) y de varios LEDs específicos asociados a los puertos Fast Ethernet y a los módulos SFP.

En los apartados que siguen a continuación, se indica la disposición e identificación de los LEDs según modelo.

3.1 SWT CON PUERTOS FRONTALES

La FIGURA 20 muestra una vista frontal del SWT con puertos frontales en la que puede verse el detalle de los distintos LEDs. Su descripción se indica a continuación.

FIGURA 20 Detalle de los distintos LEDs en el SWT con puertos ***frontales***

LEDs de base

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 On	Rojo. Se ilumina en permanencia cuando al equipo se le suministra tensión de alimentación externa.

LEDs asociados a PoE (puertos 1 a 4 eléctricos)

LED PoE — Bicolor. Existe un LED por interfaz asociada a cada puerto PoE (sólo puertos 1 a 4 eléctricos). En ausencia de equipos conectados se iluminan los cuatro LEDs ámbar en permanencia, siempre que exista tensión de alimentación PoE (conector PoE PS). Cuando se conecte algún equipo IP que use la alimentación PoE (IEEE 802.3af), se iluminará el LED verde correspondiente en permanencia, permaneciendo los LEDs de los puertos sobre los que no se está consumiendo alimentación PoE apagados.

LEDs asociados a puertos SFP

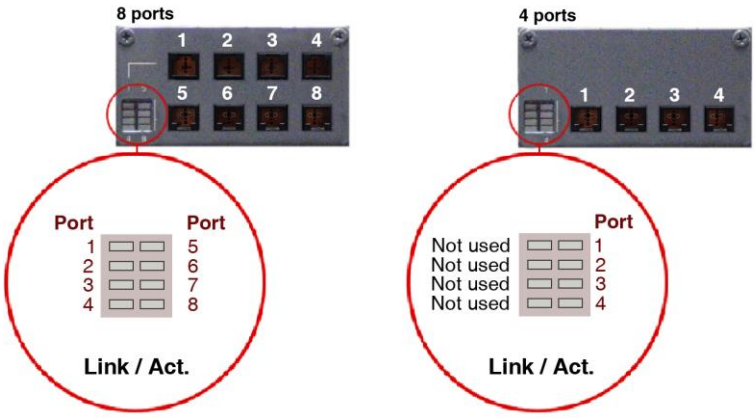
LED Link/Act. — Ámbar. Existe un LED por interfaz SFP. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.

LEDs asociados a puertos 10/100Base-Tx (RJ-45)

LED Sp/Lk/Act — Bicolor. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz. Se ilumina en verde a 100 Mbit/s y en ámbar a 10 Mbit/s.

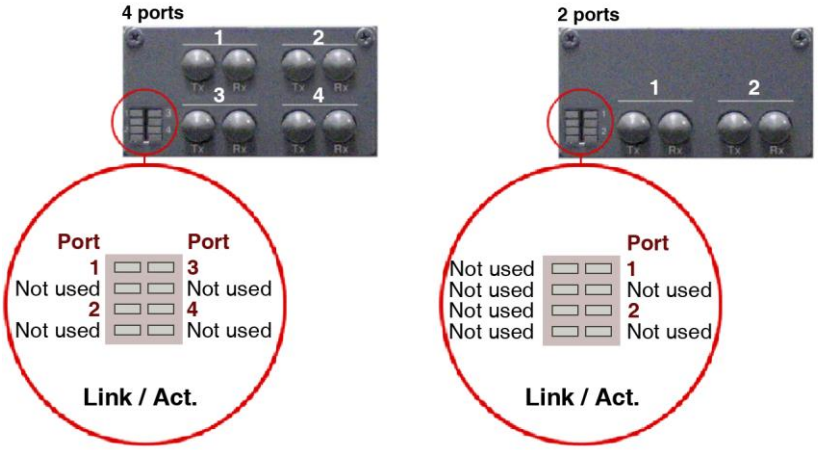
LEDs asociados a puertos 100Base-Fx (multimodo, MT-RJ)

LED Link/Act. — Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



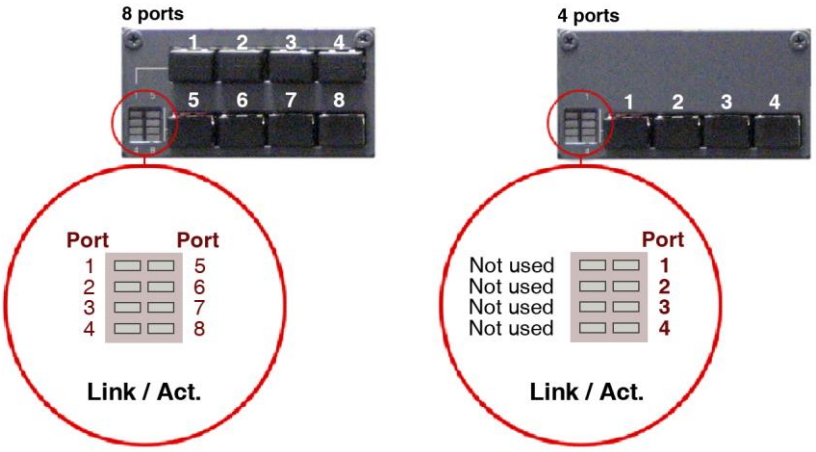
LEDs asociados a puertos 100Base-Fx (multimodo,ST)

LED Link/Act. — Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



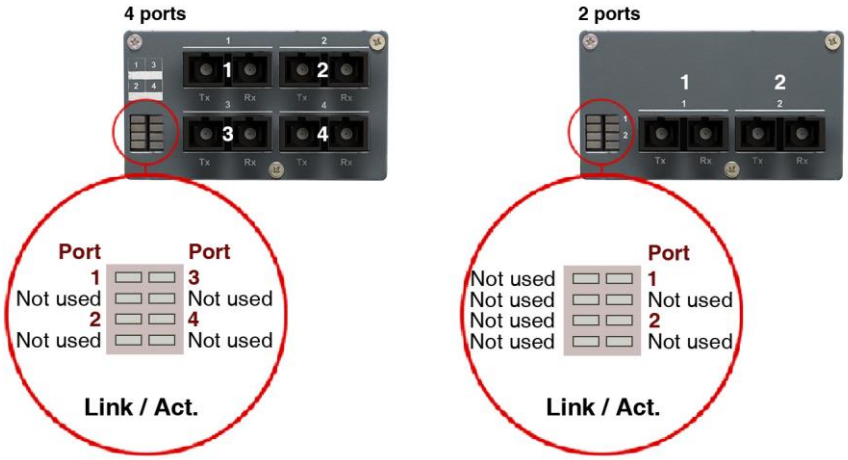
LEDs asociados a puertos 100Base-Fx (multimodo, LC)
ó 100Base-Lx (monomodo, LC)

LED Link/Act — Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



LEDs asociados a puertos 100Base-Fx (multimodo,SC)

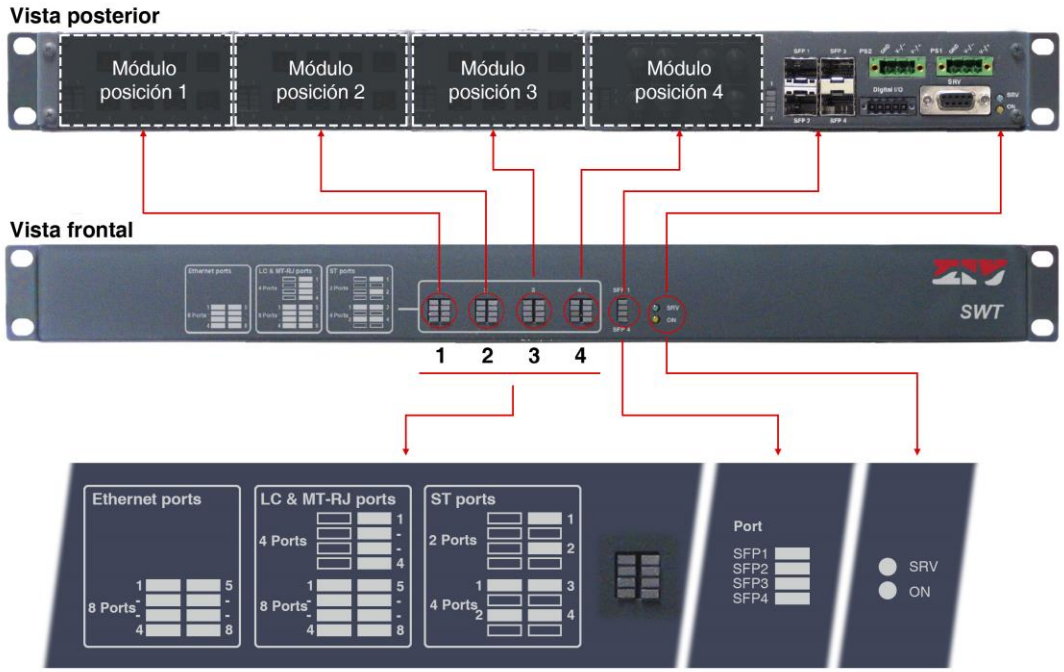
LED Link/Act.	Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



3.2 SWT CON PUERTOS POSTERIORES

La FIGURA 21 muestra una vista frontal del SWT con puertos posteriores en la que puede verse el detalle de los distintos LEDs. Su descripción se indica a continuación.

FIGURA 21 Detalle de los distintos LEDs en el SWT con puertos ***posteriores***



LEDs de base

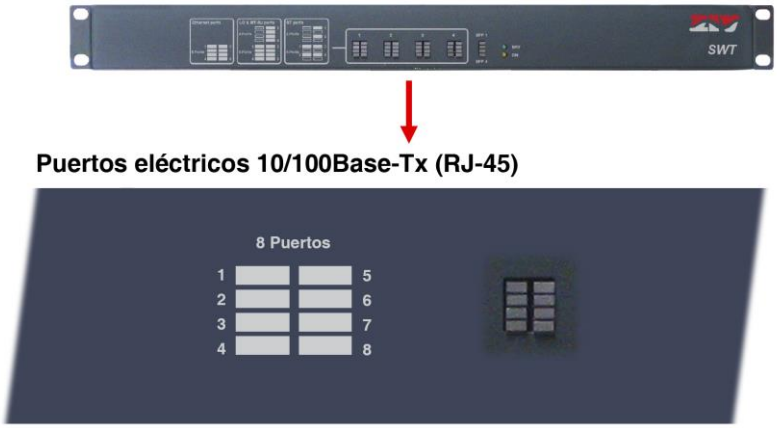
LED SRV	Ámbar. Se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz serie de servicio SRV.
LED ON	Rojo. Se ilumina en permanencia cuando al equipo se le suministra tensión de alimentación externa.

LEDs asociados a puertos SFP

LED SFP (1 a 4)	Ámbar. Existe un LED por interfaz SFP. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.

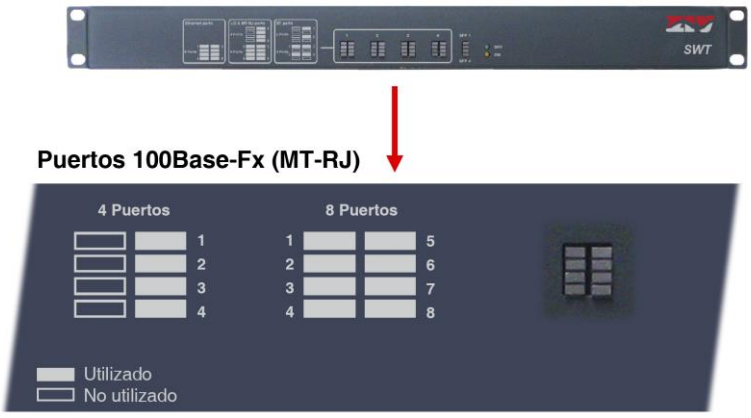
LEDs asociados a puertos 10/100Base-Tx (RJ-45)

LEDs puertos Ethernet	Bicolor. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz. Se ilumina en verde a 100 Mbit/s y en ámbar a 10 Mbit/s.



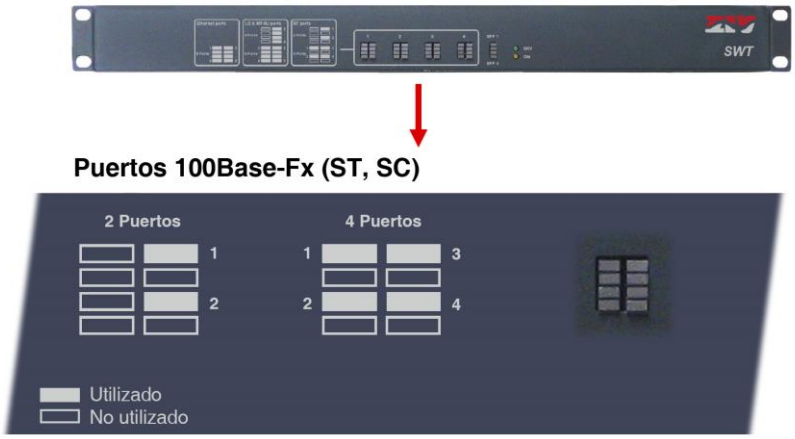
LEDs asociados a puertos 100Base-Fx (multimodo, MT-RJ)

LEDs puertos MT-RJ	Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



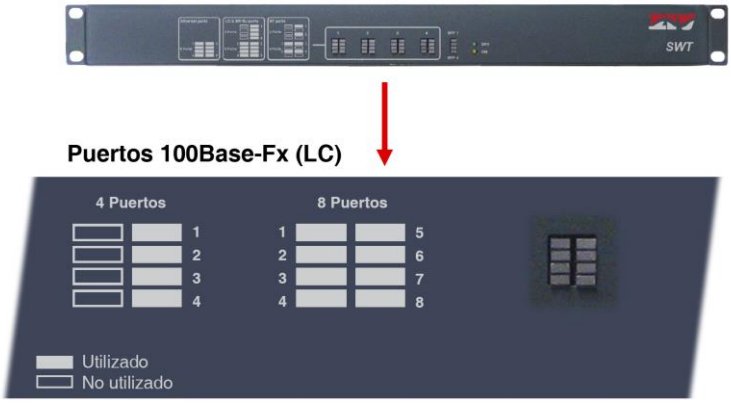
LEDs asociados a puertos 100Base-Fx (multimodo, ST ó SC)

LEDs puertos ST ó SC	Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



LEDs asociados a puertos 100Base-Fx (multimodo, LC)
ó 100Base-Lx (monomodo, LC)

LEDs puertos LC	Verde. Existe un LED por puerto. Se ilumina en permanencia cuando el enlace está establecido de forma correcta, y se ilumina de forma intermitente cuando hay actividad a nivel de emisión o recepción por parte de la interfaz.



4 ACCESO AL EQUIPO

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

4.1 CONSOLA

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

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

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

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

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

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

Los cambios realizados con el comando ***set*** no son operativos por el simple hecho de haber sido ejecutados. El uso efectivo e inmediato de los cambios realizados se consigue mediante la ejecución del comando ***Apply***. Por el contrario, el comando ***Save*** supone el almacenamiento de los cambios realizados con carácter permanente, y no conlleva su uso inmediato, 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 la páginas HTML).

Los comandos ***Apply*** y ***Save*** se hallan en la zona inferior del árbol de menús, y únicamente son visibles cuando el perfil del usuario tiene derecho de administración. En la FIGURA 22 se muestran los comandos indicados.

Para el detalle de los comandos ***Reboot, Reflash, Configuration files*** *y* ***Event files***, véanse respectivamente los apartados 5.17, 5.18, 5.19 y 5.20.

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

FIGURA 22 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 SWT 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.

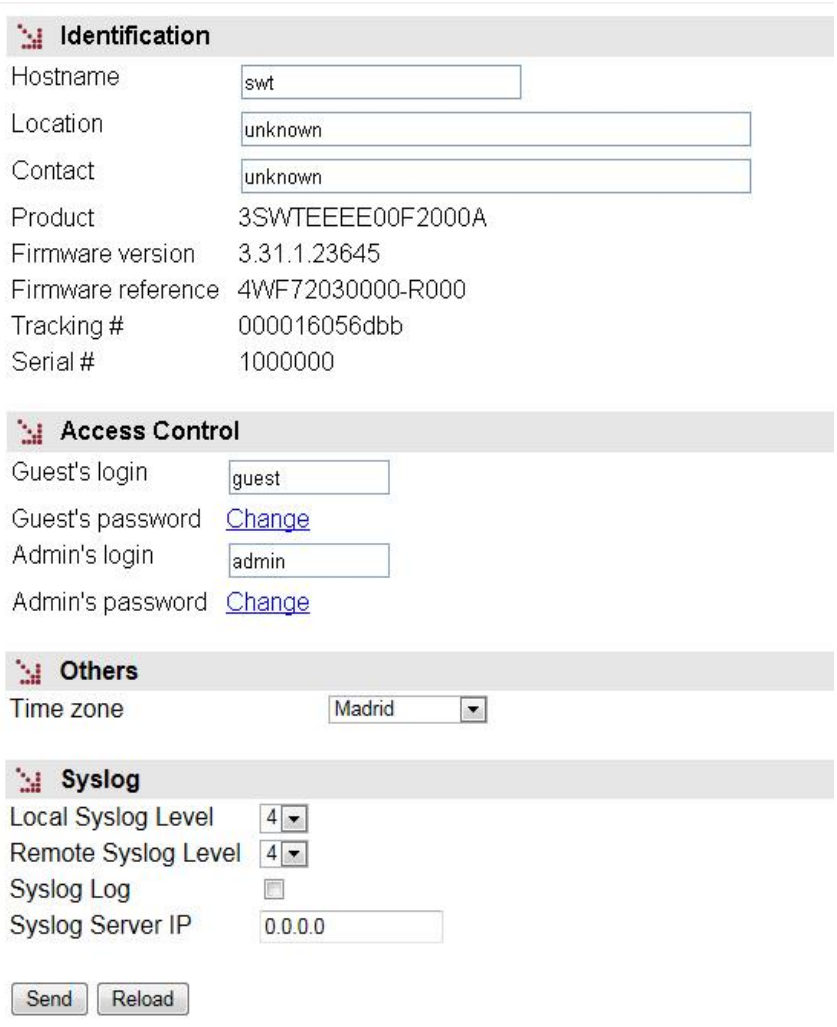
5.1 PARÁMETROS GENERALES

Los parámetros generales se agrupan en la primera página, véase FIGURA 23, que se muestra una vez el SWT 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 23 Pantalla de configuración principal



5.1.1 Identificación del equipo

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

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

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

5.1.2 Control de acceso

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

El perfil de invitado únicamente tiene acceso a operaciones de consulta. Por el contrario, el perfil administrador 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 (*login*)	**Contraseña (*password*)**
Usuario Invitado	guest	passwd01
Usuario Administrador	admin	passwd02

> Es altamente recomendable modificar, como mínimo, la contraseña del perfil administrador en la primera configuración de cada equipo.
>
> Es aconsejable almacenar la nueva contraseña en algún tipo de registro ya que, de olvidarla, no podría accederse al servidor web.

5.1.3 Otros

En esta sección existe un parámetro que establece la zona horaria en relación a UTC.

5.1.4 Syslog

En esta sección existen cuatro parámetros. El primero de ellos, ***Local Syslog Level***, establece el nivel máximo de severidad que se almacena en el Log local. El rango admitido es el comprendido entre 1 y 8. El valor por defecto es 4.

Los niveles suponen el almacenamiento de todas las informaciones etiquetadas con un nivel igual o inferior al configurado.

Los niveles son los siguientes:

Nivel	Descripción
Emergency: Nivel **1**	Múltiples aplicaciones/servidores/sitios. Este nivel no debe ser utilizado por las aplicaciones.
Alert. Nivel **2**	Debe corregirse de inmediato. Un ejemplo podría ser la pérdida de la conexión ISP principal.
Critical. Nivel **3**	Puede utilizarse para indicar un fallo en la aplicación principal del sistema.
Error. Nivel **4**	Una aplicación ha superado su límite de almacenamiento y los intentos de escritura están fallando.
Warning. Nivel **5**	Puede indicar que se producirá un error si no se toman medidas. Por ejemplo, un sistema de archivos *non-root* que sólo dispone de 2GB.
Notice. Nivel **6**	Eventos que son inusuales pero que no son condiciones de error.
Informational. Nivel **7**	Mensajes normales de funcionamiento que no requieren una acción. Por ejemplo que una aplicación ha arrancado, está en pausa o ha terminado con éxito.
Debugging. Nivel **8**	Información útil para los desarrolladores para depurar la aplicación.

El segundo parámetro, ***Remote Syslog Level***, establece el nivel máximo de severidad que se enviará al servidor Syslog Remoto. El rango admitido es el comprendido entre 1 y 8. El valor por defecto es 4. Véase información sobre los niveles en el parámetro anterior.

El tercer parámetro, ***Syslog Log***, es un control *CheckBox.* Por defecto, NO está seleccionado, lo que quiere decir que, estando configurado un servidor remoto, las trazas **NO** se almacenan en el Log local. Cuando se selecciona el control, las trazas **también** se almacenan en el Log local con el nivel de severidad correspondiente, además de enviarse al servidor remoto.

El último parámetro, ***Syslog Server IP***, establece la dirección IP del servidor Syslog Remoto al que se enviará la información.

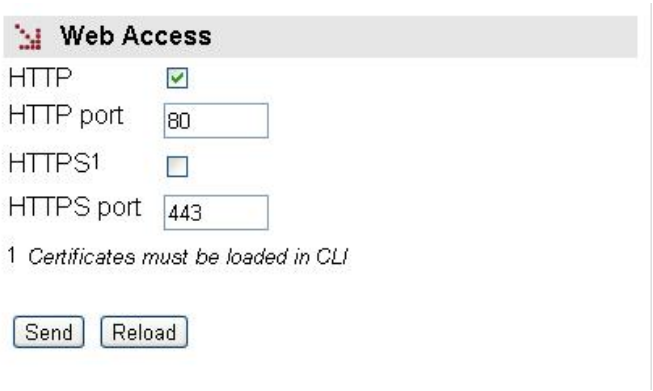
El sistema admite la activación/desactivación selectiva de información de log correspondiente a algunos bloques funcionales (véase el comando **log**).

A través de *CLI* se pueden consultar los ficheros de log locales distintos al actual (véase el comando **show**).

5.2 ADMINISTRATION

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

FIGURA 24 Pantalla de configuración del menú ***Administration***



El procedimiento para instalar los certificados está descrito en el apartado B.4 del Apéndice B, *Estructura de datos en CLI*

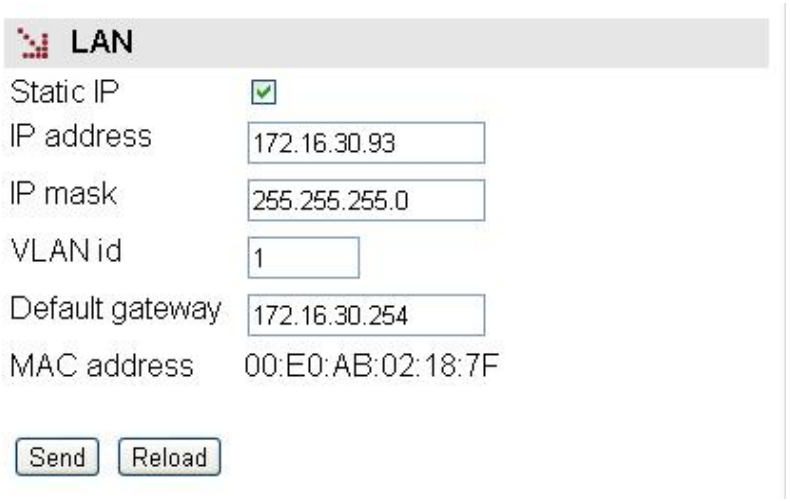
5.3 CONFIGURACIÓN LAN

El menú ***LAN*** contiene los parámetros IP para la administración y gestión del switch.

Los parámetros de configuración son los siguientes:

- **Static IP.** Cuando este control está marcado, el equipo usa los datos proporcionados por el usuario en relación a la dirección IP y su máscara. Si el control no está marcado, la dirección IP principal y su máscara se obtienen de forma automática mediante un servidor DHCP.
- **IP address.** Establece la dirección IP del switch.
- **IP mask.** Establece la máscara asociada a la dirección IP del switch.
- **VLAN id.** Identificador numérico de la VLAN. En el caso de configurar múltiples VLAN, este parámetro especifica en cuál de ellas será accesible la gestión del equipo. Por defecto, está configurado con el valor 1, es decir, la gestión será accesible desde las interfaces asignadas a la **vlan1**.
- **Default gateway.** Establece la dirección IP del router por defecto (Default Gateway).
- **MAC address.** Muestra la dirección MAC Ethernet propia del switch.

FIGURA 25 Pantalla de configuración del menú ***LAN***

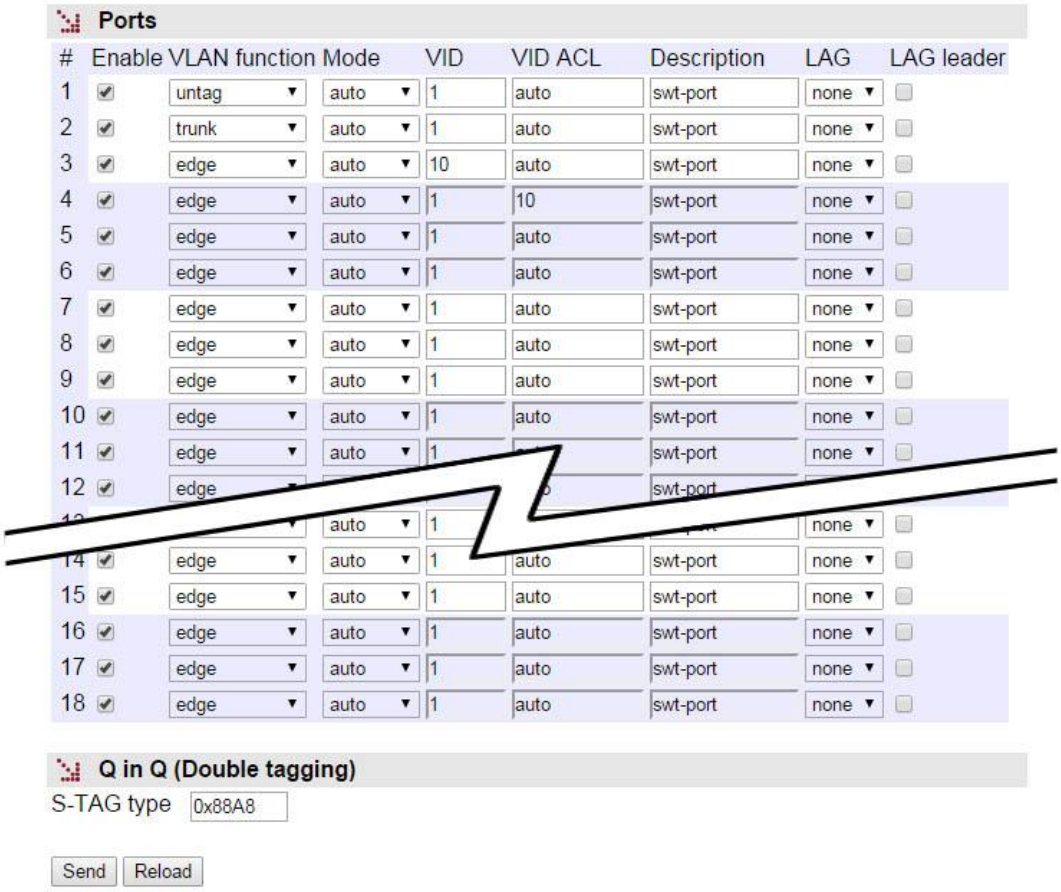


5.4 CONFIGURACIÓN DE LOS PUERTOS ETHERNET

En el menú ***Ports*** se lleva a cabo la configuración de los parámetros de funcionamiento de los puertos Gigabit/Fast Ethernet del equipo, así como la asignación de cada uno de los puertos (*ports*) a las VLAN definidas en el equipo (véase el apartado 5.5).

> Por defecto, la Gestión Web será accesible desde las interfaces asignadas a la **vlan1**. De fábrica, todos los puertos Gigabit/Fast Ethernet tienen asignados una **VID** (VLAN id por defecto) de valor **1**.
>
> Por ello, debe de tenerse en cuenta que, de modificar este valor en un puerto, desde el mismo no será posible llevar a cabo la Gestión Web del equipo.

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



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

Ports:

- **#.** Identifica el número de puerto y coincide con el número del conector del equipo. Los cuatro últimos puertos siempre son los asociados a los puertos SFP.
- **Enable.** Permite habilitar y deshabilitar individualmente cada puerto marcando o desmarcando, respectivamente, la casilla *Enable*.
- **VLAN function.** Especifica el comportamiento del puerto en relación al procesado del tag 802.1q, siendo las opciones *edge*, *trunk, untag, native, QinQ Core o QinQ Access*.

  Edge: Las tramas 802.1 se transmitirán con la misma configuración 802.1q que tenían en el momento de ser recibidas por el switch, es decir, si la trama recibida incluía **tag**, se transmitirá **con tag**, y si la trama recibida **no incluía tag**, será transmitida sin **tag**.

  Trunk: Todas las tramas se transmiten **siempre con tag**. Es el modo específico para la conexión con otros equipos de conmutación, de modo que se preserva la información de VLAN entre switches.

  Untag: Las tramas 802.1 se transmitirán **sin tag**, independientemente de que en el momento de ser recibidas por el equipo tuvieran tag o no.

  Native: El modo native es equivalente al modo **Trunk**, con la salvedad de que las tramas pertenecientes a la VLAN coincidente con la **VID** configurada se transmiten sin tag. Este modo de operación es equivalente a Native VLAN de Cisco, con la consideración de que la VLAN nativa se define puerto a puerto mediante el parámetro **VID.**

  QinQ Core. Todas las tramas se transmiten **siempre con doble tag (Double tagged)**. Es el modo específico para la conexión hacia la red de un tercero, del cual se ha obtenido un tag privativo.

  QinQ Access. Todas las tramas se transmiten **siempre con tag**. Es el modo específico para la interfaz que acepta el tráfico que se cursará hacia una red de terceros usando doble tagging.

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

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

> En **puertos 100Base-Fx,** las interfaces **no admiten negociación ni cambio de velocidad,** es decir, **únicamente pueden operar en modo 100 Mbit/s Full-duplex (100fdx) y 100 Mbit/s Half-duplex (100hdx),** de forma que, cualquier valor del parámetro distinto a 100hdx, es interpretado como 100fdx.
>
> Las interfaces **SFP no admiten cambio de velocidad,** es decir, **pueden operar a la velocidad establecida por el fabricante,** de modo que el valor del campo no afecta a la operación de las interfaces SFP.

- **VID (VLAN id por defecto)**. Identificador numérico de la VLAN en la que está incluido el puerto. También constituye el identificador de VLAN que se asignará a las tramas recibidas en el puerto y que no incluyan tag (*untagged*), o que el tag únicamente tenga información de prioridad (*priority tagged*). La definición de la VLAN se lleva a cabo desde el menú ***VLANs***, véase apartado 5.5, *Configuración de las VLAN*.

> En el caso de las interfaces operando en modo QinQ Access, el valor de este parámetro determina el identificador de VLAN que se incluirá en el tag más externo sobre las interfaces con doble tag, el denominado S-Tag.

- **VID ACL (Access control list).** VLANs de acceso permitidas para cada puerto. Este parámetro actúa como un filtro en cuanto a los paquetes que se aceptarán a nivel de puerto. Únicamente los paquetes con un identificador de VLAN incluida en la lista serán procesados, tanto en transmisión como en recepción. Todos los paquetes disponen de un identificador VLAN, bien porque ya estaba incluido en el momento de ser recibidos (tagged frames) bien porque le fue asignado por el puerto de entrada en el momento de la recepción, siendo en este último caso el parámetro **VID** asignado al puerto. El valor especial **all** significa que el filtro no está activo. El valor por defecto es auto, y supone el equivalente a que únicamente se aceptarán paquetes pertenecientes a la VLAN asignada al puerto, es decir, el filtro está inactivo.

  Un conjunto de vlans discretas se configura con el identificador de cada una de ellas separado por una coma, sin espacios. Si se desea la inclusión de un rango, el identificador de la vlan inicial y de la vlan final se separan con guión. Ejemplo: en un equipo con la **vlan1** a **vlan3** y la **vlan5** definidas, el conjunto de identificadores numéricos sería **1-3,5**.

  En el caso de las interfaces operando en modo QinQ Core, los identificadores de VLAN incluidos en este parámetro determinan cuales de las interfaces QinQ Access se van a servir a través de cada interfaz, aquellas cuyo parámetro VID sea parte del ACL.

- **Description.** Campo descriptivo a disposición del usuario como mnemotécnico.

- **LAG.** Identificador de grupo de enlaces. Establece si la interfaz forma parte de un grupo de interfaces que operarán como interfaz agregada. El valor del parámetro, en caso de que sea distinto de **none**, indicará en cual de los 8 posibles grupos se integrará la interfaz.

  Un grupo de interfaces LAG se considera como una única interfaz, de modo que los enlaces del mismo grupo no se consideran bucles por parte del STP, lo que permite el incremento del ancho de banda entre equipos manteniendo un cierto nivel de redundancia automática. Todas las interfaces de un mismo grupo deben ser interconectadas entre los mismos equipos extremos.

- **LAG leader.** Para la correcta operativa de las interfaces agregadas, todas las interfaces pertenecientes a un mismo grupo deben coincidir en sus parámetros de configuración. La elección de un **Leader** dentro del grupo sirve para determinar qué conjunto de parámetros será el que se empleará para todas las interfaces incluidas en el grupo. En caso de selección múltiple, se tomará como Leader al último que se encuentre, obviando el resto.

> Si se configuran interfaces como miembros de un grupo pero ninguna de ellas está seleccionada como Leader del mismo, el grupo no será efectivo.

Q in Q (Double tagging):

- **S-TAG type.** Este parámetro permite al usuario fijar el campo 'ethertype' que se empleará en el tag de servicio o proveedor, y que permite identificar que una trama incluye doble tag. El valor por defecto es 0X88A8 según normativa.

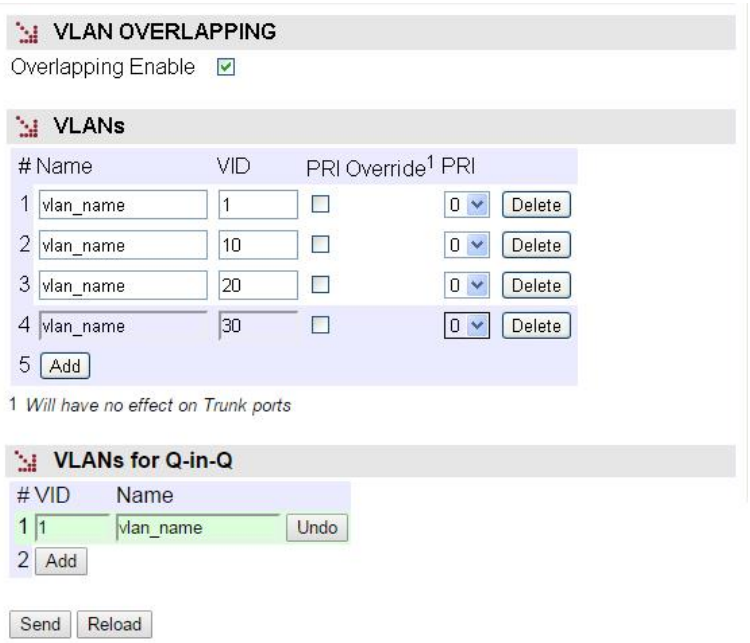
5.5 CONFIGURACIÓN DE LAS VLAN

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

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

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

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

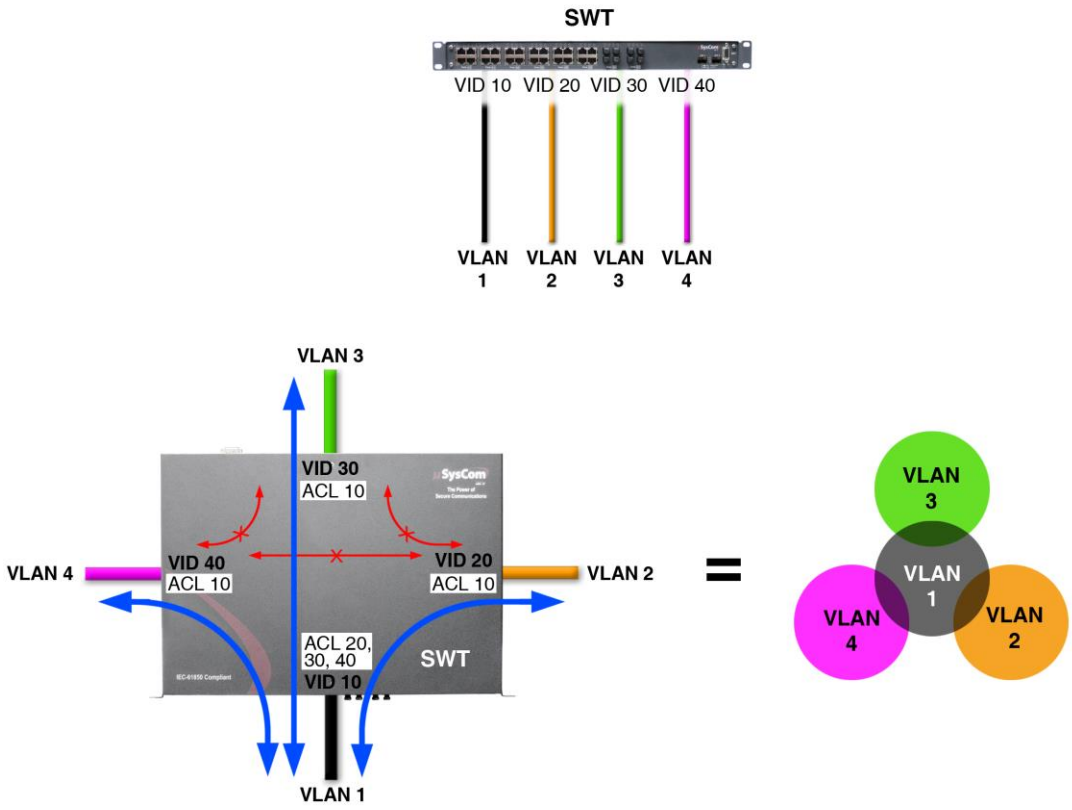


La pantalla asociada al menú ***VLANs*** presenta tres apartados bien diferenciados, los cuales se describen a continuación.

Existe un parámetro global que afecta a todas las VLAN.

- **Overlapping Enable.** Establece el modo de operación interno del switch en cuanto a la gestión de las direcciones MAC de las distintas VLAN. Por defecto, el modo de operación es ***IVL*** (*Independent VLAN Learning*). Con la opción seleccionada, el equipo pasa a operar en modo ***SVL*** (*Shared VLAN Learning*).
  El modo ***SVL*** (**Overlapping Enabled**) es necesario cuando se usen topologías con varias VLAN en las que exista alguna interfaz que tenga acceso a más de una de las VLAN configuradas, es decir, que **las VLAN compartan alguna interfaz** de usuario, y los **clientes** operen con **tramas UNTAGGED**. En estos casos, la exclusión de tráfico se realiza mediante las **listas de control de acceso** determinadas para cada una de las interfaces (véase el parámetro ***VID ACL*** en el apartado 5.4).
  En la FIGURA 28 se muestra un ejemplo de utilización del parámetro **Overlapping Enable**.

FIGURA 28 Ejemplo de utilización del parámetro **Overlapping Enable**



4 VLANs con puertos comunes y clientes UNTAGGED = OVERLAPPING ENABLE ACTIVADO

VLANs:

Los parámetros de configuración individuales para cada VLAN son los siguientes:

- **#.** Indicador de posición en la tabla.
- **Name.** Campo descriptivo a disposición del usuario como mnemotécnico.
- **VID.** Permite establecer el identificador de la VLAN. El rango admitido comprende del **1** al **4095**.
- **PRI Override.** Establece si la prioridad de las tramas recibidas en los puertos asignados a la VLAN VID debe ser sobrescrita en el valor del campo PRI (opción habilitada) o debe mantenerse la prioridad recibida (opción NO habilitada). Este campo **NO** tiene efecto en los puertos en los que el parámetro *VLAN function* esté configurado como *trunk*.
- **PRI.** En caso de que la opción **PRI Override** esté habilitada, la prioridad original de las tramas recibidas **con tag** se modificará con el valor establecido.

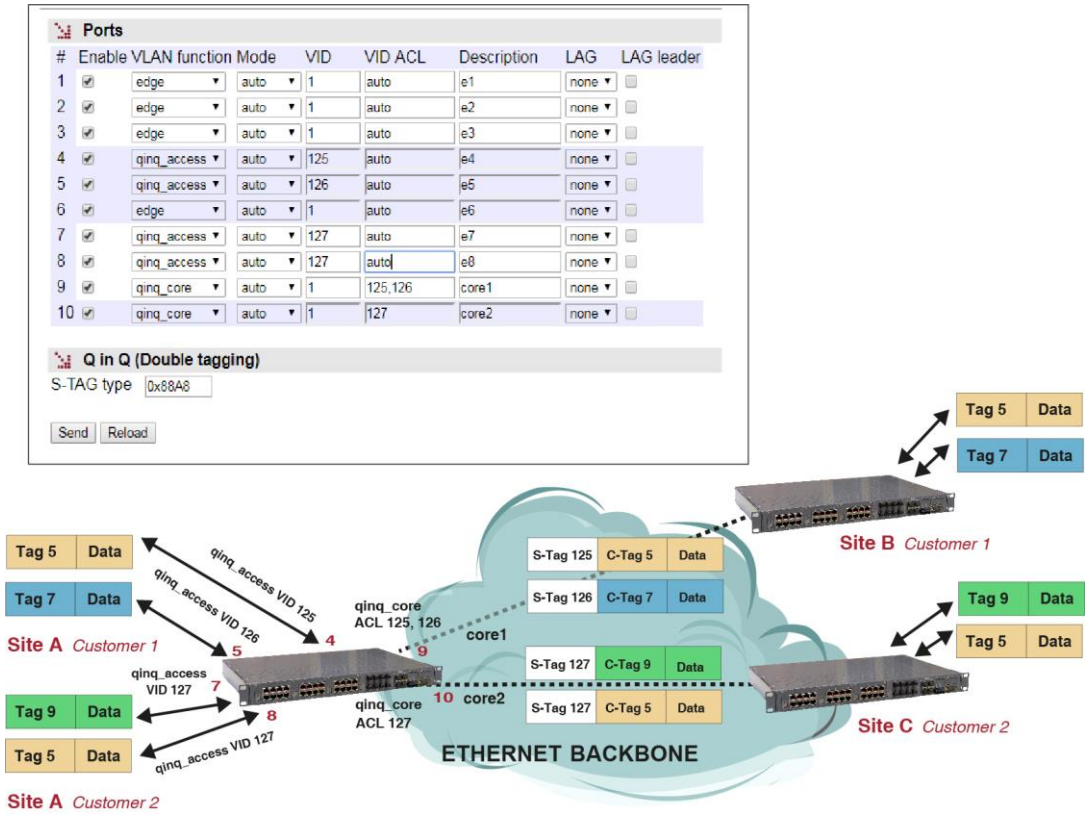
VLANs for Q-in-Q:

En este apartado se indica cuáles de las VLAN van a ser las que se empleen en interfaces QinQ Access, es decir, cuáles de las VLAN que se acepten por parte del equipo se van a cursar sobre otra red mediante el empleo de tags dobles. Véase FIGURA 29 de ejemplo.

- **#.** Indicador de posición en la tabla.
- **VID.** Indica que la VLAN VID se cursará con doble tag.
- **Name.** Campo descriptivo a disposición del usuario como mnemotécnico.

> Los identificadores VID que se configuren para la función Q-in-Q se emplearán en el S-Tag y, por tanto, serán los que indique el proveedor del backbone ethernet (usualmente un tercero).
>
> El sistema no admite que el mismo identificador VID esté en uso de forma simultánea como VLAN local y como VLAN reservada para Q-in-Q. En caso de simultaneidad, la utilización como VLAN local es prioritaria y no se tendría en cuenta para la operación de Q-in-Q.

FIGURA 29 Ejemplo de utilización del parámetro **VLANs for Q-in-Q**



5.6 CONFIGURACIÓN DEL LÍMITE DE ANCHO DE BANDA

El menú ***Rate Control*** permite establecer limitaciones de ancho de banda en cada uno de los puertos, tanto entrante como saliente. El límite de volumen de datos puede establecerse de forma general para todo tipo de tráfico o bien para ciertas combinaciones que tienen en cuenta el tipo de mensajes.

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

- Límite de ancho de banda de entrada al puerto (***Ingress Rate Control***).
- Límite de ancho de banda de salida de datos desde el puerto (***Egress Rate Control***).

Los parámetros de configuración de cada bloque se indican a continuación.

Ingress Rate Control:

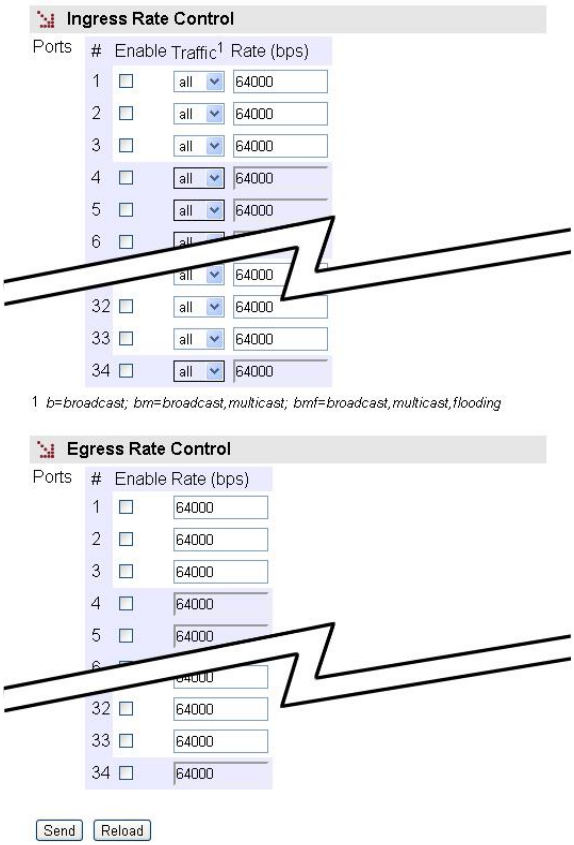
- **#.** Identifica el número de puerto y coincide con el número del conector del equipo. Los cuatro últimos puertos siempre son los asociados a los puertos SFP.
- **Enable.** Permite habilitar y deshabilitar individualmente cada puerto marcando o desmarcando, respectivamente, la casilla *Enable*.
- **Traffic.** Permite especificar el tipo de tráfico: todo (***all***), *broadcast* (***b***), *broadcast* y *multicast* (***bm***) ó *broadcast*, *multicast* y *flooding* (***bmf***).
  Broadcast se refiere a los mensajes de difusión, es decir, al modo de transmisión de información donde un nodo emisor envía información a todos los receptores de manera simultánea.
  Multicast se refiere a los mensajes de multidifusión, los cuales están dirigidos a los integrantes de un grupo de multidifusión.
  Flooding se refiere a la situación en que se produce una avalancha (*flood*) en un corto espacio de tiempo, típicamente debido a una topología incorrecta, una configuración inadecuada o una acción voluntaria por parte de algún equipo cliente.
- **Rate (bps).** Establece el ancho de banda de entrada límite en el puerto: **64000** bps (64 kbps) a **250000000** bps (250 Mbps). La velocidad máxima sólo tiene sentido para los puertos Gigabit Ethernet.

Egress Rate Control:

- **#.** Identifica el número de puerto y coincide con el número del conector del equipo. Los cuatro últimos puertos siempre son los asociados a los puertos SFP.

- **Enable.** Permite habilitar y deshabilitar individualmente cada puerto marcando o desmarcando, respectivamente, la casilla *Enable*.
- **Rate (bps).** Establece el ancho de banda de salida límite en el puerto: **64000** bps (64 kbps) a **250000000** bps (250 Mbps). La velocidad máxima sólo tiene sentido para los puertos Gigabit Ethernet.

FIGURA 30 Pantalla de configuración del menú Rate Control



5.7 CONFIGURACIÓN QoS

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

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

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

La política de servicio es única para el servicio de nivel 2. Los parámetros son la prioridad 802.1q o en el campo DSCP de la cabecera IP (nivel 3).

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

Los apartados y sus parámetros de configuración son los siguientes:

Weight Fair Scheduling:

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

Priority:

En este apartado se fijan las condiciones de clasificación de las tramas a cada una de las tres colas existentes en función del valor de la prioridad 802.1q, con independencia del mecanismo de asignación o procesado de la misma.

- **#.** Identifica el valor de la prioridad asociada a la trama 802.1 (cubre todo el rango de valores permitidos por la norma).

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

> ! La prioridad **Mgmt**, aunque está disponible para el usuario, la recomendación es que se reserve para la prioridad 7 en exclusiva, y que se evite el uso de dicha prioridad por parte del tráfico de usuario.

DSCP:

En este apartado se fijan las condiciones de clasificación de las tramas a cada una de las tres colas existentes en función del valor del campo DSCP de la cabecera IP. Se admite un rango discreto de valores para el campo DSCP.

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

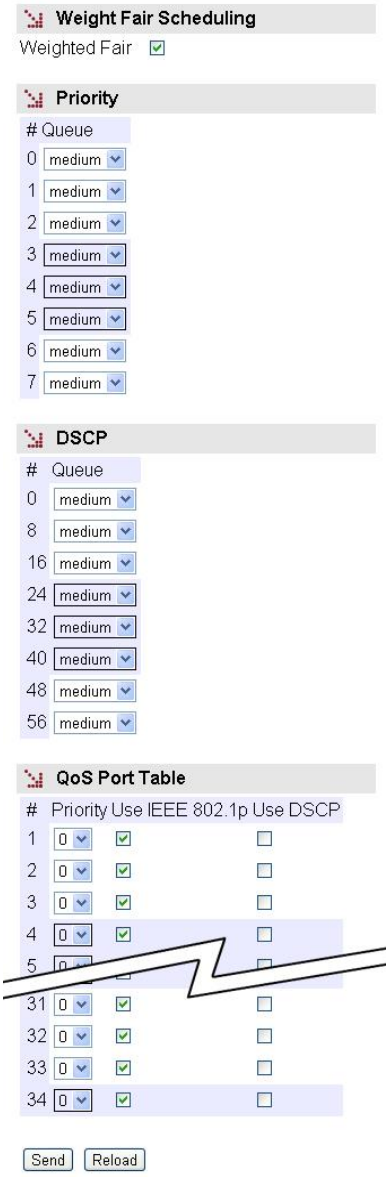
QoS Port Table:

En este apartado se fijan las condiciones de obtención o asignación de la prioridad para cada uno de los puertos.

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

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

FIGURA 31 Pantalla de configuración del menú ***QoS***

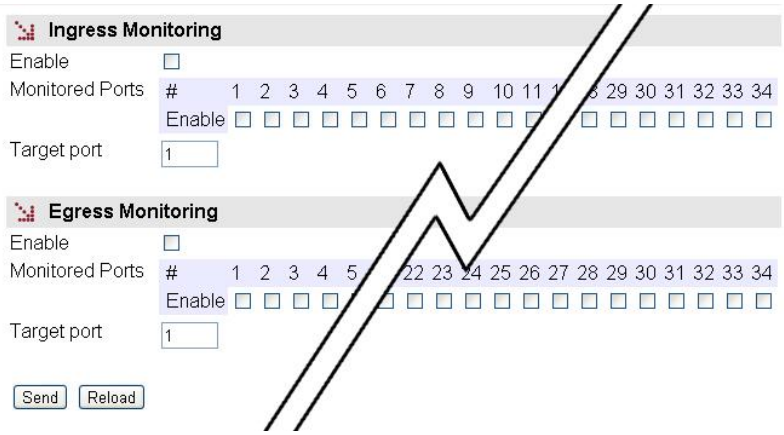


5.8 CONFIGURACIÓN DE LA MONITORIZACIÓN DE LOS PUERTOS

Este menú permite llevar a cabo funciones de ***Port mirroring*** en los puertos, con el fin de poder monitorizar su comportamiento.

El tráfico **entrante y/o saliente** de un puerto específico (*Monitored port*) se replica en un puerto destino (*Target port*) para su monitorización mediante, por ejemplo, un analizador de protocolos.

FIGURA 32 Pantalla de configuración del menú ***Monitor***



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

- Monitorización del tráfico de entrada (***Ingress Monitoring***).
- Monitorización del tráfico de salida (***Egress Monitoring***).

Los parámetros de configuración de cada bloque se indican a continuación.

Ingress Monitoring:

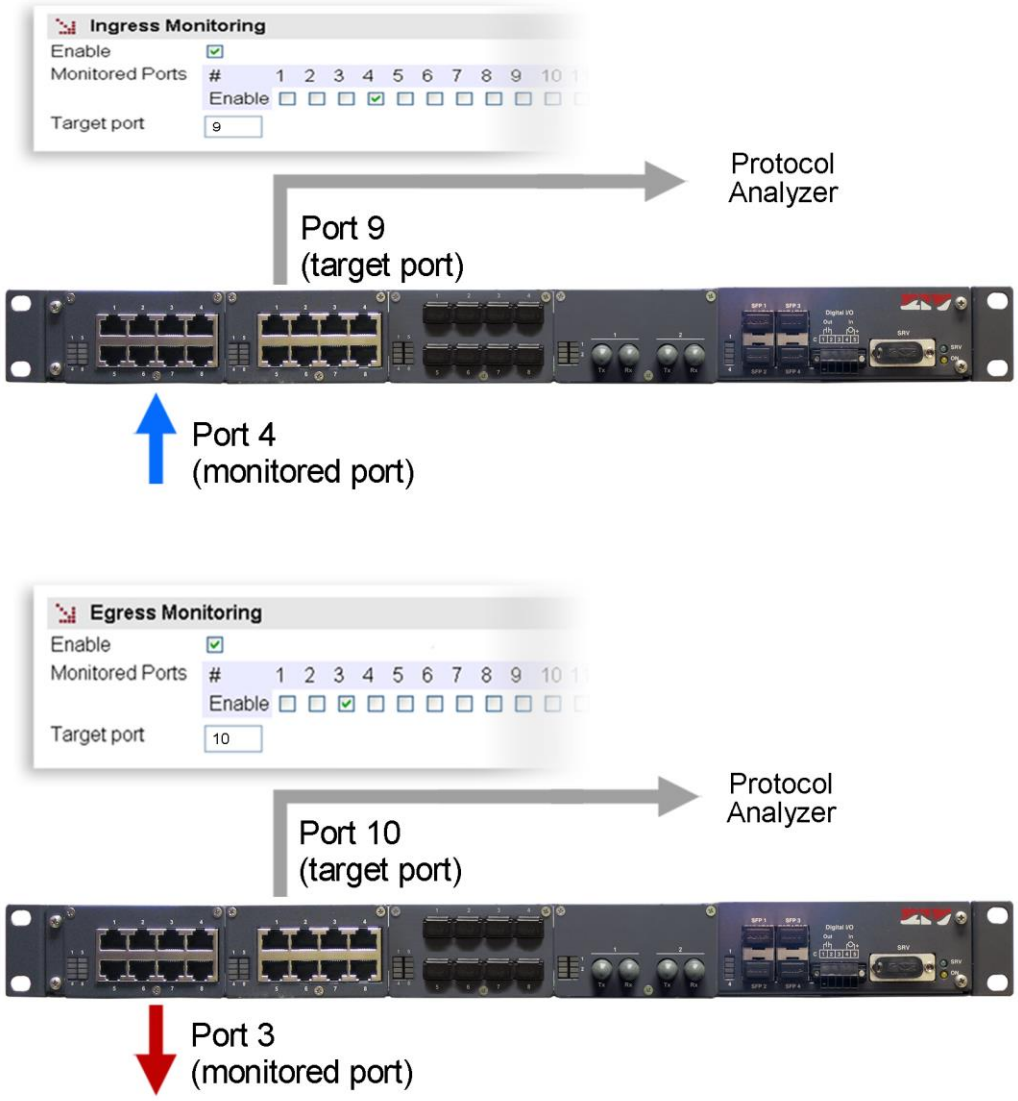
- **Enable.** Permite habilitar y deshabilitar la monitorización del tráfico entrante marcando o desmarcando, respectivamente, la casilla.
- **Monitored Ports.** Establece el puerto o puertos objeto de monitorización. El tráfico de entrada en cada uno de los puertos seleccionados se replicará en el puerto destino (*Target port*).
- **Target port.** Establece el puerto sobre el que se enviará los paquetes replicados para la monitorización.

Egress Monitoring:

- **Enable.** Permite habilitar y deshabilitar la monitorización del tráfico saliente marcando o desmarcando, respectivamente, la casilla.
- **Monitored Ports.** Establece el puerto o puertos objeto de monitorización. El tráfico de salida en cada uno de los puertos seleccionados se replicará en el puerto destino (*Target port*).

- **Target port.** Establece el puerto sobre el que se enviará los paquetes replicados para la monitorización.

FIGURA 33 Ejemplo de configuración del menú ***Monitor***



5.9 CONFIGURACIÓN LLDP

LLDP es un protocolo estándar de la capa de enlace que se emplea para anunciar la identidad y capacidades a los equipos vecinos en redes de área local.

Tanto la información comunicada como la recibida es accesible mediante el protocolo SNMP, mediante las MIBs definidas en el propio estándar LLDP, y usualmente se emplea para determinar la topología de las redes.

El estándar establece unos campos de información que deben ser incluidos de forma obligatoria. Otros campos tienen carácter opcional y el usuario puede seleccionar la información de cada uno de ellos.

El acceso a la información mediante SNMP implica necesariamente que el agente SNMP esté habilitado.

El equipo controla la ejecución del protocolo LLDP mediante un parámetro *CheckBox*, y ofrece parámetros adicionales, individuales para cada uno de los puertos, que son los siguientes:

- **Admin Status.** Establece el modo de operación del agente LLDP de la interfaz. Los valores admitidos son *TxRx*, *TxOnly*, *RxOnly* y *disabled*. El valor por defecto es *TxRx*.

- **Tx Interval.** Establece el tiempo entre la emisión de mensajes, en operación normal. Las unidades son segundos, siendo 30 el valor por defecto y recomendado. El rango admitido es el comprendido entre 1 y 3600.

- **Hold.** El valor de este parámetro se emplea como multiplicador de *Tx Interval* y sirve para determinar el valor de *txTTL* que se incluye en los mensajes LLDP enviados por el agente. El valor por defecto y recomendado es 4. El rango admitido es el comprendido entre 1 y 100.

- **Reinit.** Establece el periodo de tiempo que debe transcurrir desde que el *Admin Status* se fija como *disabled* hasta que se intenta la reinicialización. Las unidades son segundos, siendo 2 el valor por defecto y recomendado. El rango admitido es el comprendido entre 1 y 10.

- **Credit Max.** Establece el número máximo de mensajes LLDP consecutivos que pueden ser transmitidos en cualquier momento. El valor por defecto y recomendado es 5. El rango admitido es el comprendido entre 1 y 10.

- **Tx Interval Fast.** Este parámetro establece el periodo de envío de mensajes LLDP en el periodo de transmisión rápida, que se activa de forma automática cuando se detecta a un equipo vecino. El valor por defecto y recomendado es 1. El rango admitido es el comprendido entre 1 y 3600.

- **Mess num Fast.** Con este parámetro se determina el número de mensajes LLDP que se enviarán durante un periodo de transmisión rápida. El valor por defecto y recomendado es 4. El rango admitido es el comprendido entre 1 y 8.

- **Tx Notif. Enable.** Indica al agente LLDP si debe enviar notificaciones SNMP (traps) cuando se producen cambios en la información remota recibida en la interfaz.

> Para que las notificaciones SNMP sean efectivamente enviadas, debe permitirse su envío de forma explícita en el menú SNMP.

- **PortDesc.** Indica al agente LLDP si debe incluir o no el campo opcional con la información descriptiva de la interfaz en los mensajes LLDP enviados. El valor del campo es el texto del parámetro *Description* del menú *Port* (véase 5.4).

- **SysName.** Indica al agente LLDP si debe incluir o no el campo opcional con el nombre del equipo en los mensajes LLDP enviados. El valor del campo es el texto del parámetro *Hostname* del menú principal (véase 5.1.1).

- **SysDesc.** Indica al agente LLDP si debe incluir o no el campo opcional con la descripción del equipo en los mensajes LLDP enviados**.** El valor del parámetro se obtiene de forma automática del firmware en ejecución, por lo que no está sujeto a cambios por parte del usuario.

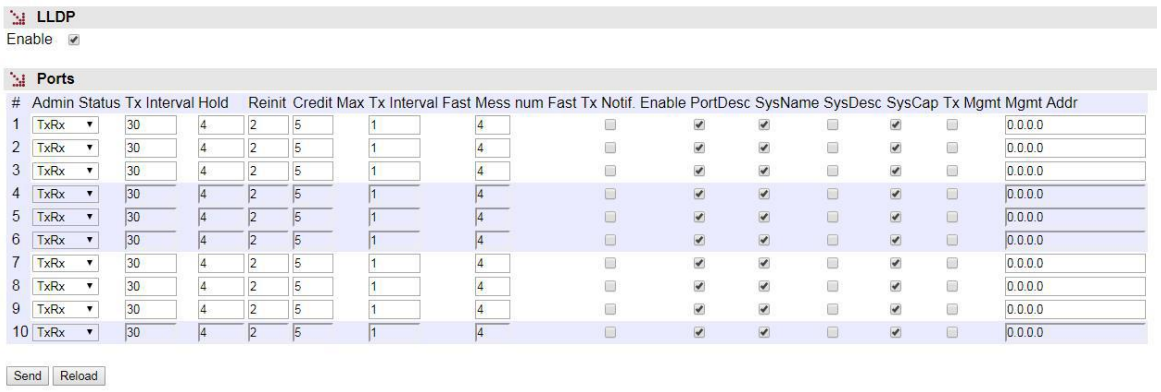
- **SysCap.** Indica al agente LLDP si debe incluir o no el campo opcional con las capacidades del equipo en los mensajes LLDP enviados. La codificación del campo se fija en la norma y está formada por flags. El valor se inserta automáticamente.

- **Tx Mgmt.** Indica al agente LLDP si debe incluir o no el campo opcional con la dirección de gestión del equipo en los mensajes LLDP enviados. El valor a enviar es determinado por el parámetro *Mgmt Address*.

- **Mgmt Address.** Permite al usuario establecer el valor del campo opcional que comunica la dirección de gestión del equipo.

El protocolo dispone de estadísticas propias que muestran los datos propios de la ejecución del protocolo en cada interfaz como parte de la información recibida.

FIGURA 34 Ejemplo de configuración del menú ***LLDP***



5.10 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], SNMPv2c [2] y SNMPv3, así como la elección del tipo de mensajes, *trap* e *inform*.

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

Los parámetros de configuración son:

SNMP:

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

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

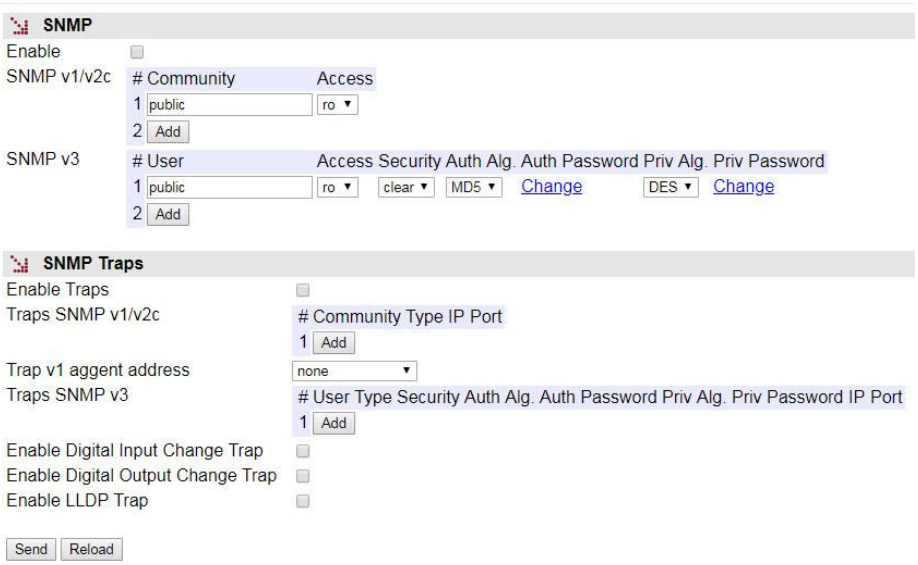
  En caso de transmisión autentificada (*auth*), es necesario seleccionar el tipo de algoritmo (*Auth Alg*.), MD5 o SHA, y establecer la contraseña de autentificación (*Auth Password*). La contraseña establece la palabra que se empleará para la generación de la información de autentificación. La palabra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

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

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

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

FIGURA 35 Pantalla de configuración del menú ***SNMP***



SNMP Traps:

- **Enable Traps:** Habilita/inhabilita la generación y transmisión de mensajes espontáneos por parte del agente SNMP. El agente enviará mensajes de los distintos eventos cuando la opción está seleccionada.

- **Traps SNMPv1/v2c:** Dato tabular que permite definir varios equipos destinatarios de los *traps*.
  Para cada uno de los destinatarios de los mensajes espontáneos SNMP, es necesario proporcionar el perfil que se incluirá en el mensaje espontáneo, la versión del protocolo SNMP con el que se codificará, la dirección IP del destinatario y el puerto UDP al que se enviarán los mensajes. El valor por defecto establecido en el estándar es el puerto 162. Admite su modificación para adaptarse a los datos de operación de cada destinatario.
  La transmisión de los mensajes de forma confirmada (*inform*) sólo es admitida por las versiones v2c y v3 del protocolo.

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

- **Traps SNMPv3:** Dato tabular que permite definir varios equipos destinatarios de las notificaciones.
  Los destinatarios se identifican mediante su dirección IP y el puerto UDP al que se enviarán las notificaciones. El puerto UDP estándar para las notificaciones SNMP es el 162, que es el valor por defecto.
  El control *Type* establece si la transmisión de las notificaciones se realizará de forma no confirmada (*trap*) o confirmada (*inform*).

- **Enable Digital Input Change Trap.** Habilita/inhabilita la emisión de mensajes espontáneos SNMP indicando los cambios de estado de la entrada digital.
  La entrada digital corresponde a los contactos 4 y 5 del conector I/O.

- **Enable Digital Output Change Trap.** Habilita/inhabilita la emisión de mensajes espontáneos SNMP indicando los cambios de estado de la salida digital.
  La salida digital corresponde a los contactos 1 y 2 del conector I/O.

  Si la salida digital está configurada como Alarma, no se envían mensajes SNMP asociados a los cambios de la misma, aunque la configuración así lo indique.

- **Enable LLDP Trap.** Indica al agente SNMP si las notificaciones creadas por el agente LLDP están permitidas o no.

5.11 CONFIGURACIÓN DEL PROTOCOLO STP

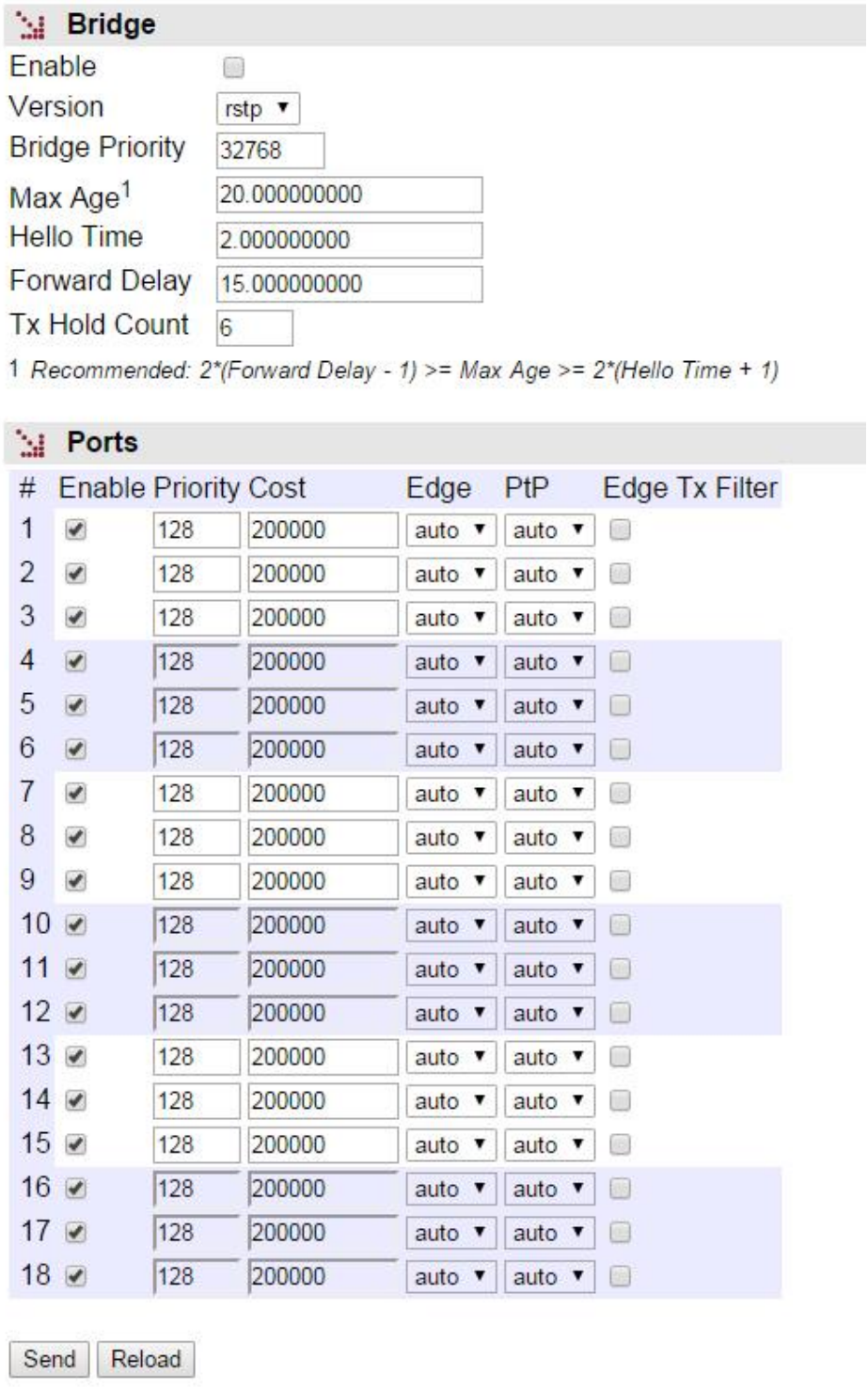
El protocolo Spanning Tree, tanto en su variante original (STP) como en la versión mejorada (RSTP) tiene como objetivo la identificación de los posibles bucles en redes de nivel 2, de modo que los equipos dialogan entre sí y establecen si las distintas interfaces de cada uno de ellos será activa en cuanto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

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

Los parámetros de configuración específicos del equipo son:

- **Enable.** Un parámetro *CheckBox* simple para indicar si el protocolo STP debe ejecutarse o no.
- **Version.** Establece cual de las posibles versiones del protocolo se ejecutará. STP o RSTP (Rapid STP).
- **Bridge Priority.** Fija la prioridad del equipo que éste comunicará al equipo raíz.
- **Max Age.** Tiempo máximo que el equipo considera válido el último mensaje BPDU recibido. En el caso de expirar el tiempo estipulado, el equipo asume que ha habido un cambio topológico, e iniciará el proceso de comunicación de cambio topológico. El valor por defecto es de 20 segundos, mientras que el rango admitido está entre 6 y 40 segundos.
- **Hello Time.** Este parámetro establece el tiempo entre envíos de mensajes BPDUs (los mensajes propios del protocolo STP). El valor por defecto y a la vez máximo es de 2 segundos.
- **Forward Delay.** Este parámetro es el periodo de tiempo máximo que una interfaz estará en los estados *listening* y *learning*. El valor por defecto de este periodo es de 15 segundos, y el rango admitido está entre 4 y 30 segundos.
- **Tx Hold Count.** Establece el número máximo de paquetes BPDU que se pueden transmitir en un segundo. El valor por defecto es 6, y el rango admitido es entre 1 y 10.

FIGURA 36 Pantalla de configuración del menú ***STP***



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

- **Enable.** Establece si se ejecuta o no el protocolo STP configurado en la interfaz. Únicamente tiene sentido cuando el *CheckBox* Enable de ejecución general está activo.

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

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

- **Edge.** Este parámetro indica el modo administrativo de la interfaz en cuanto al STP. Las interfaces conectadas a equipos cliente, es decir, equipos que no son de conmutación de nivel 2 y por tanto no ejecutan STP ni pueden dar lugar a la creación de bucles, pueden ser arrancadas directamente en situación de cursar tráfico (modo **on**). Por el contrario, aquellas que están directamente conectadas a equipos de conmutación de nivel 2, y por tanto susceptibles de cerrar lazos, deben ser arrancadas en modo de aceptar tráfico de usuario (modo **off**).
  Existe un tercer modo, **auto**, en que es el equipo el que determinará la presencia o no de equipos de conmutación de nivel 2 conectados a la interfaz, útil en el caso en que se desconoce qué tipo de equipos acabarán siendo conectados.
  El último y cuarto modo, **redundant**, está diseñado especifícamente para pares de switches con enlaces múltiples debidos a cadenas de equipos multi-homed. El modo **redundant** permite la conexión de equipos cliente con más de una interfaz de red en uso conectada a distintos switches y que sean transparentes a STP, de modo que los switches interconectados puedan identificarse entre sí a la vez que den acceso a los equipos cliente. Los puertos **redundant** actúan como enlaces redundantes para el acceso a los equipos cliente, pero no como enlaces redundantes en cuanto a la topología de la red. La FIGURA 37 muestra un ejemplo del modo **redundant**.
  Incluso cuando el parámetro **Edge** es **on**, el switch mantiene activada la detección de una posible conexión de un switch a la interfaz, lo que supondría que el estado operativo acabase siendo **off**.
  El modo operativo de la interfaz, **on** u **off**, puede verse en el apartado estadísticas de STP.

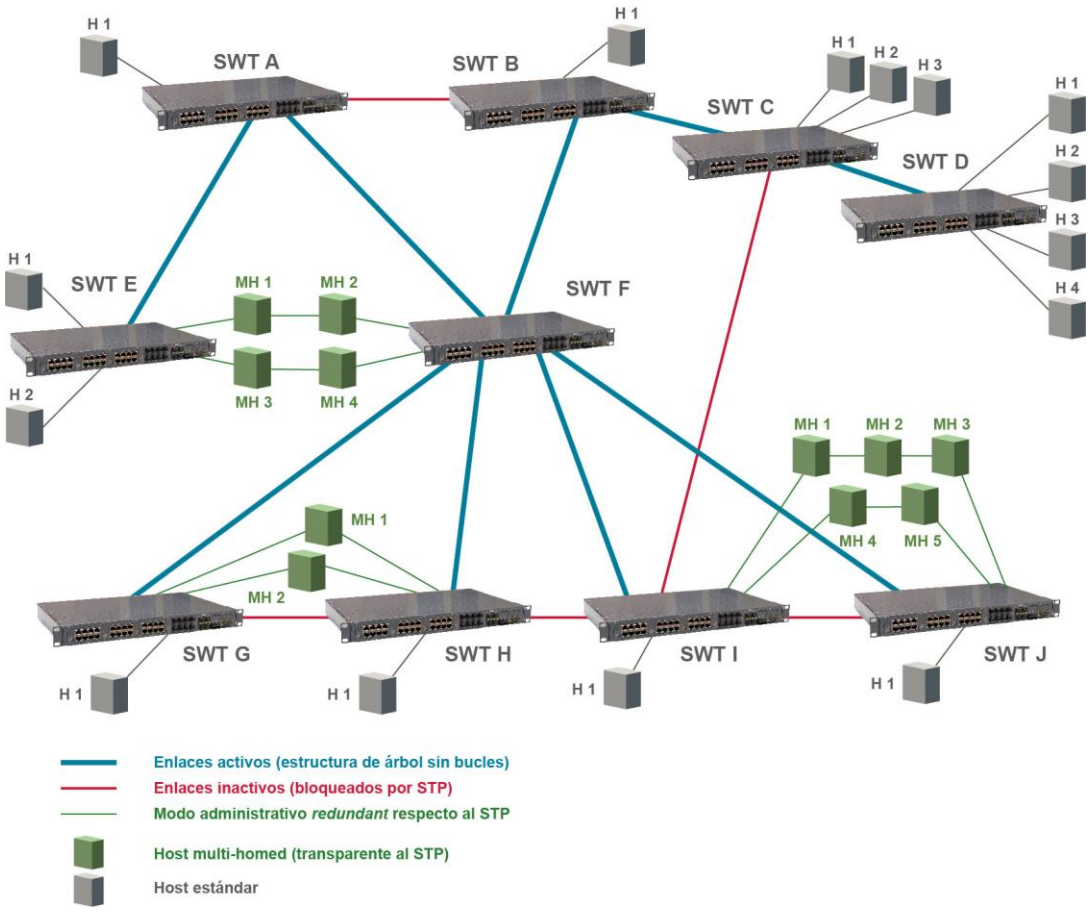
- **PtP.** El parámetro PtP establece si la interfaz está directamente conectada a otro equipo de conmutación de nivel 2 sobre un enlace punto a punto (valor **on**) o no (valor **off**), aunque el equipo también es capaz de detectar dicha situación (valor

auto). El hecho de indicar al equipo que un enlace es PtP permite una mayor velocidad de convergencia del protocolo, se acelera el proceso de acuerdo sobre el paso de estado de un enlace de *designated* a *non-discarding (*operativo en cuanto a tráfico de usuario).

- **Edge Tx Filter.** Este parámetro permite al usuario habilitar un filtro que evita la emisión de los paquetes BPDU del protocolo STP en las interfaces operando en modo **edge** cuando se está ejecutando el protocolo RSTP. El parámetro únicamente es efectivo cuando el estado operativo de la interfaz es **edge**, y esta situación sólo es alcanzable cuando el parámetro **Edge** está configurado con valores **on** o **auto**.

> ! Si la conexión entre dos switch se realiza **mediante interfaces con la opción Edge a ON y el filtro Edge_Tx_filter activo,** los equipos **no tienen la capacidad para determinar** que la conexión forma parte de un bucle.

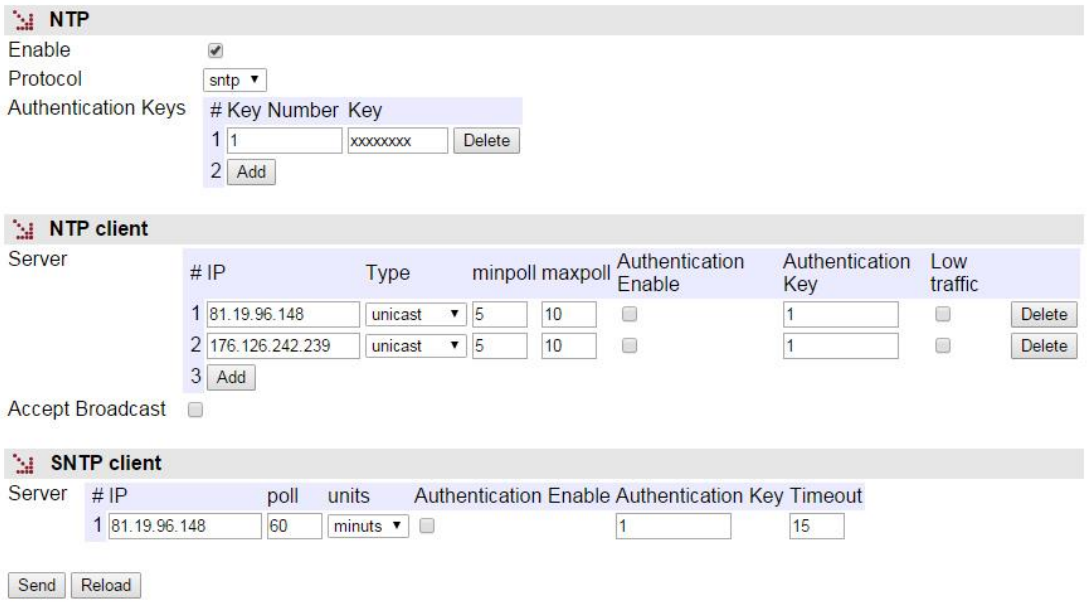
FIGURA 37 Ejemplo del modo **redundant** de la interfaz en cuanto al STP



5.12 CONFIGURACIÓN NTP/SNTP

El equipo dispone de un cliente NTP/SNTP, 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 autentificación. La variante SNTP supone una sincronización más rápida pero a la vez menos precisa y, por otro lado, es necesario ejecutar la misma de forma periódica.

FIGURA 38 Pantalla de configuración del menú ***NTP/SNTP***



Los parámetros de uso generales son:

- **Enable:** Habilita/inhabilita la ejecución del cliente NTP. El cliente está operativo cuando la opción está seleccionada.
- **Protocol.** Permite seleccionar si se usará el cliente NTP o SNTP.
- **Authentication keys:** Dato tabular que permite definir varias claves de autentificación a emplear posteriormente con la comunicación con los distintos servidores NTP.

El cliente NTP admite la configuración de múltiples servidores NTP para realizar la sincronización. Cada uno de ellos dispone de un conjunto de parámetros individualizados que determinan el procedimiento de acceso:

- **IP.** Dirección IP del servidor NTP.
- **Type.** Establece la tipología de los mensajes que se enviarán al servidor NTP, pudiendo ser individuales (*unicast*) o colectivos (*manycast*).
- **Minpoll.** Tiempo mínimo entre solicitudes. El parámetro es el exponente de la potencia de 2 que corresponde al periodo mínimo.
- **Maxpoll.** Tiempo máximo entre solicitudes. El parámetro es el exponente de la potencia de 2 que corresponde al periodo máximo.
- **Authentication Enable.** Indica si los mensajes deben ser enviados con información de autentificación.
- **Authentication Key.** Determina cual de las claves de autentificación definidas en el bloque anterior se usará para autentificar el mensaje, en el caso en que la opción esté habilitada.
- **Low Traffic.** Minimiza el consumo del ancho de banda empleado por los mensajes de sincronización.

Hay un parámetro adicional no dependiente de la configuración de los servidores NTP que establece si se aceptarán los mensajes NTP tipo broadcast.

- **Accept broadcast.** Habilita la aceptación de los mensajes NTP recibidos con dirección broadcast.

El cliente SNTP admite únicamente la configuración de un servidor, y los parámetros necesarios son los siguientes:

- **IP.** Dirección IP del servidor NTP.
- **Poll.** Establece el periodo de generación de los mensajes de sincronismo. Los valores admisibles están en el rango 1 a 60.

- **Units.** Unidad de tiempo para el periodo de generación de los mensajes de sincronismo, puede ser minutos u horas.
- **Authentication Enable.** Indica si los mensajes deben ser enviados con información de autentificación.
- **Authentication Key.** Determina cual de las claves de autentificación definidas en el bloque anterior se usará para autentificar el mensaje, en el caso en que la opción esté habilitada.
- **Timeout.** Periodo máximo de espera para la recepción de respuesta a los mensajes de sincronismo transmitidos. Se admiten los valores en el rango 1 a 15 segundos.

5.13 CONFIGURACIÓN MULTICAST

En condiciones normales, el tráfico multicast se propaga, de forma automática, en todas las interfaces pertenecientes a cada una de las VLAN, siendo los equipos cliente los que de forma selectiva habilitan la recepción de las direcciones multicast concretas en las que están interesados.

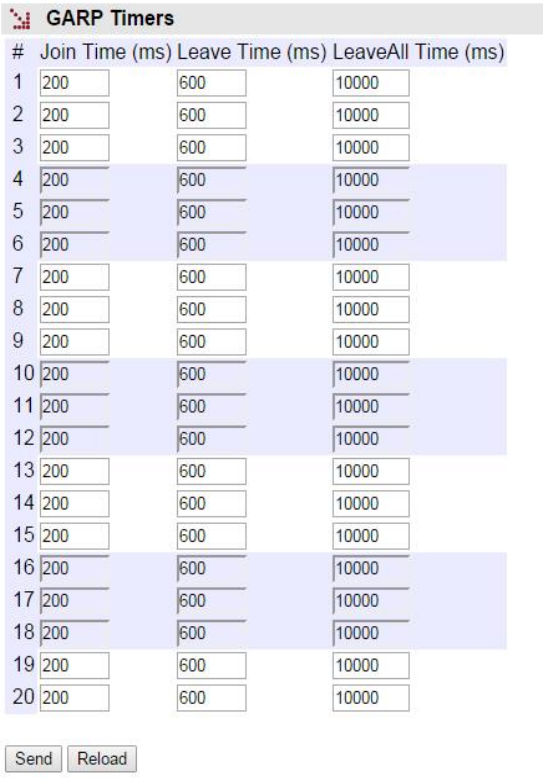
El switch dispone de mecanismos para controlar la propagación del tráfico multicast, de modo que no se propague en todos los puertos. Uno de los mecanismos es por configuración explícita y manual, es decir, configurando entradas estáticas en las que se detalla la dirección multicast de interés y los puertos a los que debe ser transmitido el tráfico correspondiente.

Hay otros mecanismos que evitan la configuración manual, empleando protocolos estándares para conseguir la identificación de los puertos que desean cada uno de los flujos multicast que puedan existir. Los protocolos son GARP/GMRP e IGMP.

El protocolo GARP/GMRP es de capa 2, y funciona por registro explícito de los equipos cliente a los switches de la red.

GARP es un protocolo base sobre el que opera GMRP, y necesita del establecimiento de configuración para temporizadores que le son propios, de modo que su configuración es accesible de forma independiente (véase FIGURA 39).

FIGURA 39 Pantalla de configuración de ***GARP Timers***

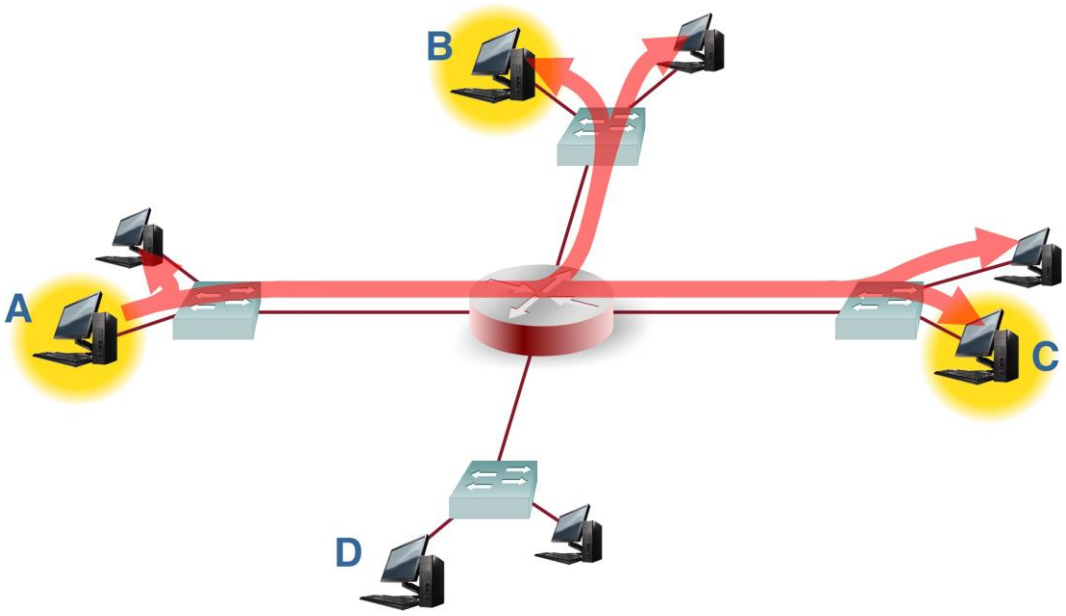


El protocolo IGMP es de capa 3 y el intercambio de mensajes para las solicitudes de recepción de flujos multicast se lleva a cabo entre los equipos cliente y los routers IGMP. En este caso, el switch espía los mensajes para adecuar la configuración de cada puerto (IGMP Snooping). Para que el IGMP Snooping sea operativo, es obligado que el protocolo GARP/GMRP esté inactivo.

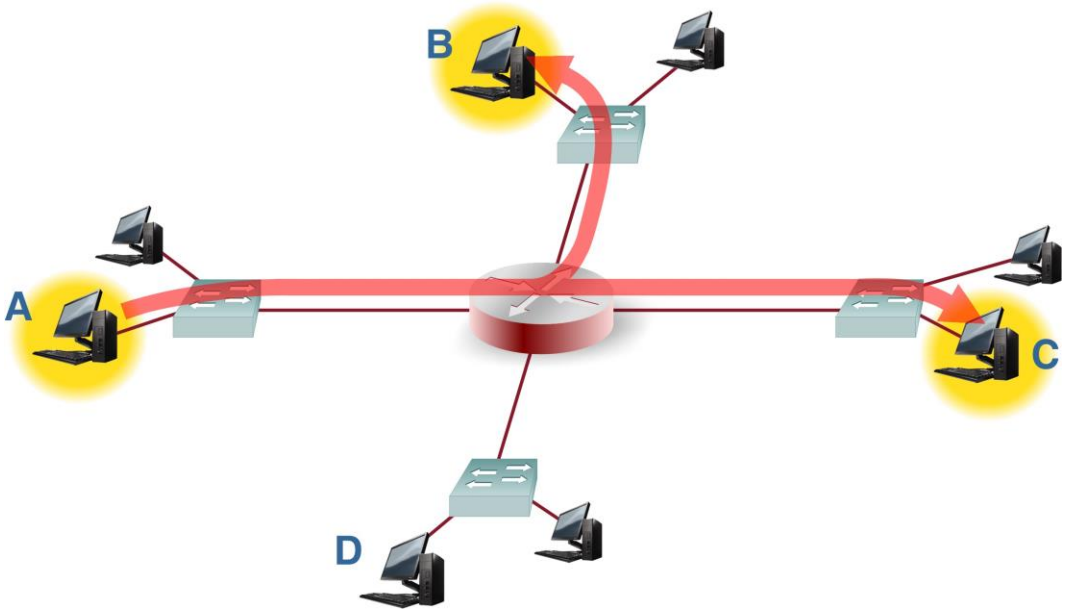
La activación de cualquiera de los mecanismos mencionados implica necesariamente que el switch únicamente cursará el tráfico multicast incluido en la configuración manual o solicitado por los equipos cliente. Cualquier otro tráfico multicast será descartado.

A título de ejemplo, la FIGURA 40 muestra las ventajas de utilizar GARP/GMRP ó IGMP Snooping. En la Figura 40a) se muestra una red compuesta por cuatro switches de nivel 2 los cuales a su vez están conectados a un router. El Host A es un emisor de mensajes multicast y los Hosts B y C son receptores multicast pertenecientes al mismo grupo que el Host A. El router encaminará el tráfico multicast sólo hacía los segmentos de la red en los que se encuentren los Hosts B y C, mientras que los switches de nivel 2 transmitirán en avalancha (flood) el tráfico hacía todos los hosts conectados a sus interfaces. En la Figura 40b) se muestra una red que utiliza el mecanismo de análisis GARP/GMRP ó IGMP (IGMP Snooping) en sus dispositivos de nivel 2. Como puede apreciarse en la figura, en este caso, sólo los hosts que pertenecen al grupo de difusión reciben el tráfico multicast.

FIGURA 40 Ejemplo de utilización de GARP/GMRP ó IGMP Snooping



a) Red que NO utiliza protocolos de configuración Multicast



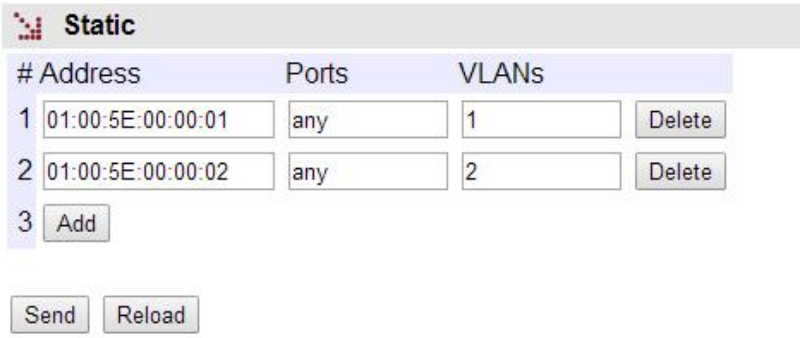
b) Red que utiliza GARP/GMRP ó IGMP Snooping en sus dispositivos de nivel 2

5.13.1 Static

El usuario puede configurar aquí manualmente las interfaces que propagarán cada una de las direcciones MAC multicast indicadas.

En redes con múltiples switch, la configuración debe realizarse en cada uno de ellos.

FIGURA 41 Pantalla de configuración ***Static*** del menú ***Multicast***



Los parámetros para la creación de la lista de MACs multicast son los siguientes:

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

La presencia de identificadores en el parámetro **Ports** y el apartado **VLANs** no son excluyentes. Si se especifican valores en ambos parámetros, la configuración se aplicará en los puertos señalados que también cumplan el requisito de pertenencia a las VLAN configuradas.

Los puertos tipo **trunk** se consideran pertenecientes a todas las vlan, por lo que únicamente deberán ser incluidos cuando el parámetro **Ports** tenga valores distintos a **any**.

5.13.2 GMRP

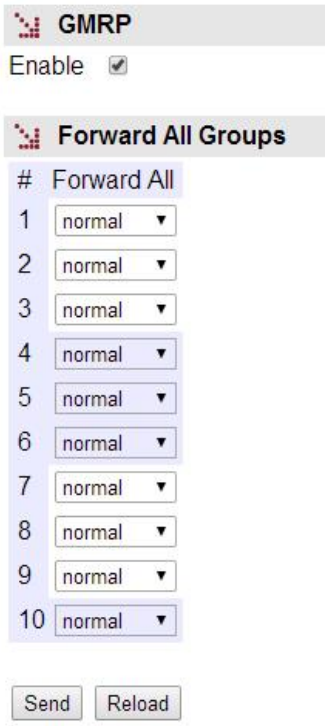
El protocolo GMRP está diseñado para que los switch adapten la transmisión de los datos multicast en función de las solicitudes emitidas por los clientes en cada una de las interfaces.

De todos modos, el protocolo tiene previsto la posibilidad de fijar manualmente la transmisión de direcciones multicast, de modo que equipos cliente que no ejecuten el protocolo puedan operar adecuadamente. Esta opción se materializa configurando los registros de la zona *Static.*

A diferencia de la operación puramente manual, la ejecución del protocolo supone la propagación automática de la demanda configurada manualmente al resto de los switches de la red, por lo que únicamente es necesario configurar la dirección multicast en el equipo en el que está la interfaz afectada.

Adicionalmente, el protocolo GMRP tiene previsto este tipo de configuración manual para una dirección de grupo abstracta, denominada ***Forward All***, y que implica que una interfaz desea recibir la totalidad del tráfico multicast. Esta opción se configura individualmente para cada interfaz local del equipo.

FIGURA 42 Pantalla de configuración ***GMRP*** del menú ***Multicast***



Los parámetros son los siguientes:

GMRP:

Un solo parámetro para indicar la ejecución del protocolo GMRP:

- **Enable.** Un parámetro *CheckBox* simple, que controla la ejecución del protocolo.

Forward All Groups:

El equipo permite la configuración manual de esta dirección especial de forma individual para cada interfaz.

- #. Identifica el número de puerto físico del equipo.
- **Forward All.** Indica el estado de la dirección de grupo especial para la interfaz correspondiente. Los valores admitidos son ***Normal***, ***Fixed*** y ***Forbidden***. La opción ***Normal***, que a su vez es la opción por defecto, indica que la propagación o no de todo el tráfico multicast estará sujeta a que exista algún equipo cliente que haya solicitado el registro para la dirección de grupo. La opción ***Fixed*** supone que la interfaz propagará la totalidad del tráfico multicast, y se obviarán los mensajes GMRP relativos a la dirección de grupo. La opción ***Forbidden*** supone que no se aceptarán solicitudes por parte de los equipos cliente para la dirección de grupo, y que únicamente se cursará el tráfico multicast registrado en la interfaz.

5.13.3 IGMP

El IGMP Snooping es una optimización a utilizar en equipos de nivel 2 como el SWT. El protocolo IGMP es de nivel 3 por lo que la operación del IGMP Snooping por parte del switch se halla condicionada a la presencia de un router Multicast en la red.

El SWT incluye una prestación especial en caso de que NO exista un router multicast en la red, y se desee que la operación IGMP Snooping esté activa. La mencionada prestación supone que es el propio switch el que emula la presencia de un router multicast realizando las peticiones periódicas de consulta a los clientes sobre la pertenencia a los distintos grupos de difusión multicast.

Los parámetros son los siguientes:

IGMP:

Hay un único parámetro que establece si la emulación como router IGMP está activa o no:

- **Enable.** Un parámetro *CheckBox* simple para indicar si el servicio de consultas periódicas IGMP está activo o no.

IGMP Snooping:

Es una prestación que permite al switch analizar el tráfico multicast entre equipos y routers con la finalidad de identificar los puertos en los que existen equipos participando activamente en grupos multicast; el objetivo es limitar la transmisión selectiva de datos en función de la información obtenida.

- **Enable.** Un parámetro *CheckBox* simple para indicar si el mecanismo de análisis IGMP (IGMP *Snooping*) debe estar activo o no.
- #. Identifica el número de puerto físico del equipo.
- **IGMP forward.** Establece el tratamiento en el puerto correspondiente de los mensajes multicast. Configurado en ***on*** el puerto transmite todos los mensajes multicast, mientras que en ***off*** no transmite ninguno. Configurado en ***auto*** el puerto transmitirá selectivamente los mensajes multicast en función de que haya equipos cliente que se hayan registrado en el grupo correspondiente.

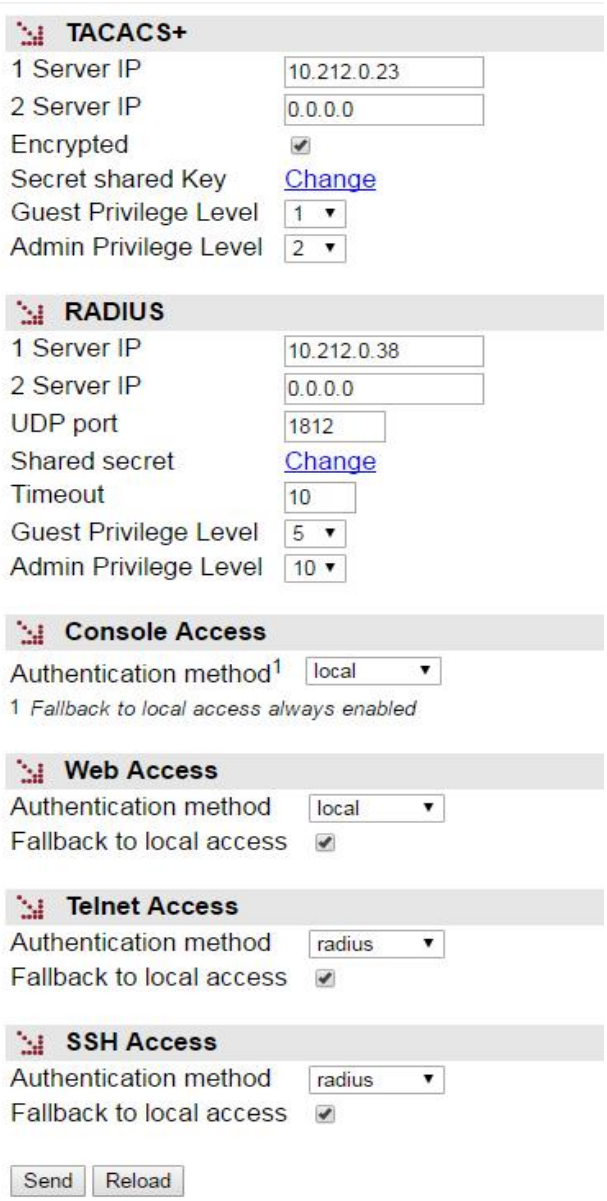
FIGURA 43 Pantalla de configuración ***IGMP*** del menú ***Multicast***

5.14 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+ y un cliente RADIUS.

FIGURA 44 Pantalla de configuración del menú ***Access***



TACACS+:

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

Los parámetros generales de configuración son los siguientes:

- **1 Server IP.** Establece la dirección IP del servidor TACACS+ primario.
- **2 Server IP.** Establece la dirección IP del servidor TACACS+ secundario.
- **Encrypted.** Permite seleccionar si la comunicación del equipo con los servidores TACACS+ debe realizarse en modo cifrado o no.
- **Secret Shared Key.** Establece la clave a emplear para el cifrado de la comunicación cuando la opción **encrypted** está activa.
- **Guest Privilege Level.** Permite seleccionar el nivel de privilegio (0 a 15) que el equipo solicitará en la petición al servidor TACACS+ para acceder como usuario *Invitado (guest)*. El nivel de privilegio debe ser consistente con el configurado en el servidor TACACS+ consultado.
- **Admin Privilege Level.** Permite seleccionar el nivel de privilegio (0 a 15) que el equipo solicitará en la petición al servidor TACACS+ para acceder como usuario *Administrador (admin)*. El nivel de privilegio debe ser consistente con el configurado en el servidor TACACS+ consultado.

RADIUS:

Los parámetros para el cliente RADIUS son los siguientes:

- **1 Server IP.** Establece la dirección IP del servidor RADIUS primario.
- **2 Server IP.** Establece la dirección IP del servidor RADIUS secundario.
- **UDP Port.** Permite fijar el puerto UDP en el que operan los servidores RADIUS. El valor por defecto establece el puerto UDP reservado para dicho protocolo.
- **Shared Secret.** Establece la clave secreta compartida. Al ser un dato necesario, el equipo usa *ziv12345* como valor por defecto.
- **Timeout.** Fija el tiempo máximo de espera para la obtención de respuesta por parte del servidor. Este parámetro es necesario debido al uso del protocolo sin conexión UDP.
- **Guest Privilege Level.** Establece el nivel de privilegio (0 a 15) del perfil invitado (***guest***). Si el nivel de privilegio recibido para el usuario solicitante en la respuesta afirmativa del servidor RADIUS es igual o mayor que este parámetro, y a la vez inferior al nivel de *Admin*, el usuario obtendrá acceso de invitado (sólo lectura).

- **Admin Privilege Level.** Establece el nivel de privilegio (0 a 15) del perfil administrador (***admin***). Si el nivel de privilegio recibido para el usuario solicitante en la respuesta afirmativa del servidor RADIUS es igual o mayor que este parámetro, el usuario obtendrá acceso de administrador (acceso lectura y escritura).

A continuación, se hallan los parámetros asociados a cada opción de acceso (**consola**, **web, telnet** y **SSH**), 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 o radius configurados.

- **Fallback to local access.** Cuando esta opción está habilitada, en caso de NO accesibilidad de los servidores TACACS+ o RADIUS configurados, se permitirá a los usuarios validarse con los usuarios locales. En caso de que la opción esté inhabilitada, si los servidores TACACS+ o RADIUS 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.

5.15 CONFIGURACIÓN SECURITY

Este menú permite establecer restricciones de tráfico en función de las direcciones MAC de los clientes. El equipo admite dos modalidades para el control de las direcciones MAC de cliente admitidas: maclist o 802.1x.

En la operación con listas, maclist, el equipo únicamente cursará el tráfico cuando la dirección MAC esté incluida en la lista de autorizadas. Tanto la activación de la restricción como la lista se configuran para cada puerto.

Para la modalidad 802.1x, la autentificación de direcciones MAC se realiza mediante consulta a un servidor RADIUS. **RADIUS** (acrónimo de **Remote Authentication Dial-In User Server**) es un protocolo de autentificación remota que se usa para gestionar el acceso a servidores y dispositivos de comunicaciones, y proporciona servicios separados de autentificación, autorización y registro.

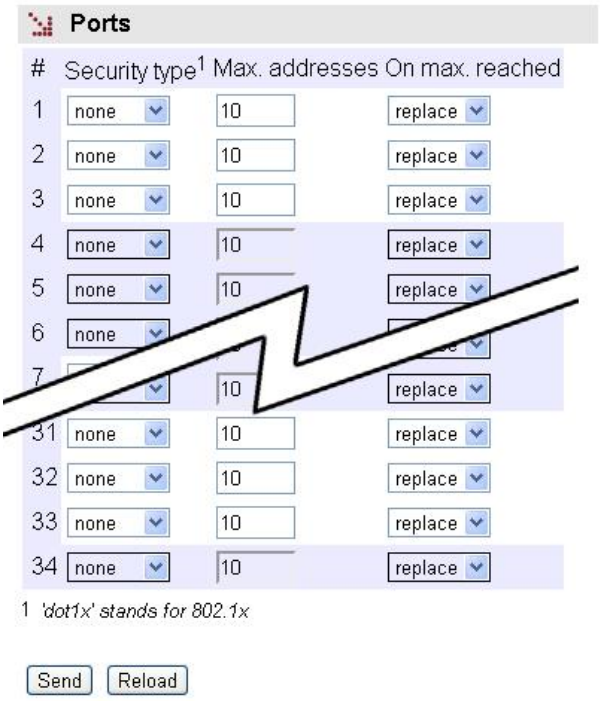
Los parámetros generales de configuración de los puertos son los siguientes:

- **#.** Identificador de interfaz física.

- **Security Type.** Establece si el servicio de filtrado por dirección MAC está activo en el puerto indicado (opción **maclist**), o se emplea la autorización 802.1x (opción **dot1x**) o no se activa ningún filtro (opción **none**).

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

FIGURA 45 Pantalla de configuración principal del menú ***Security***



5.15.1 802.1x

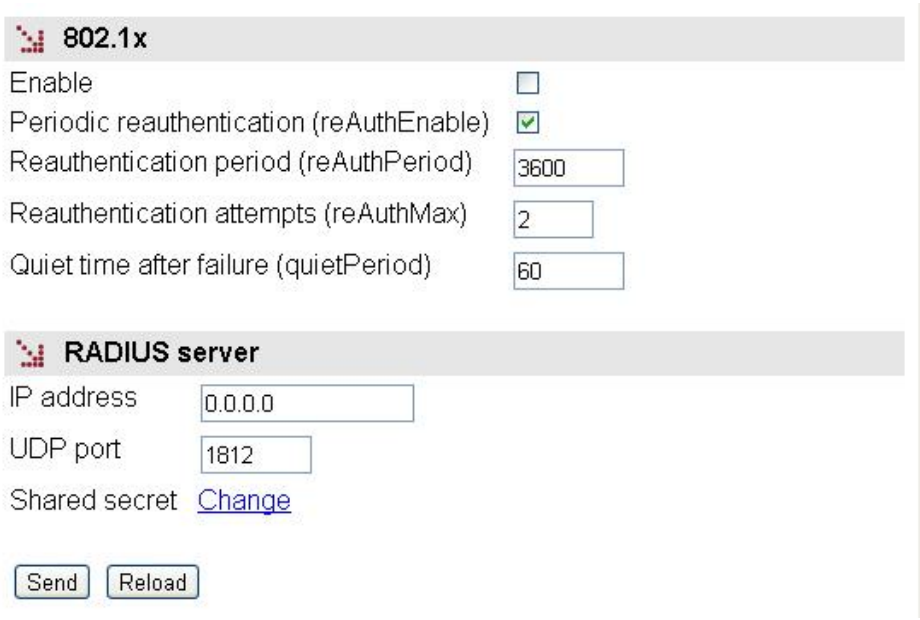
Este submenú permite especificar la autentificación de usuarios 802.1x mediante el acceso a un servidor RADIUS.

Los parámetros generales de configuración son los siguientes:

- **Enable.** Un parámetro *CheckBox* simple para indicar si el cliente RADIUS está activo o no y, por tanto, la autentificación 802.1x.
- **Periodic reauthentication (reAuthEnable).** Si el servidor RADIUS limita el tiempo de sesión, esta opción indica al equipo que debe solicitar la re-autentificación de forma periódica.
- **Reauthentication period (reAuthPeriod).** Establece el tiempo entre una re-autentificación y la siguiente. El parámetro se expresa en segundos, y el rango de valores aceptado está entre 1 y 86400 (1 día), siendo el valor por defecto 3600 (1 hora).

- **Reauthentication attempts (reAuthMax).** Establece el número máximo de intentos que el equipo enviará para solicitar la re-autenticación. El valor debe estar entre 1 y 10.
- **Quiet time after failure (quietPeriod).** Indica el periodo de tiempo en que, una vez superados el número máximo de reintentos configurados, el equipo no solicitará nuevos reintentos. El rango de valores es de 1 a 65535, y sus unidades son segundos.
- **IP address.** Establece la dirección IP del servidor RADIUS.
- **UDP port.** Establece el puerto UDP sobre el que el cliente RADIUS enviará las peticiones al servidor. El valor por defecto establecido en el estándar es el puerto 1812.
- **Shared secret.** Establece la clave a emplear para el cifrado de la comunicación con el servidor RADIUS.

FIGURA 46 Pantalla de configuración del submenú ***802.1x***



5.15.2 MAC list

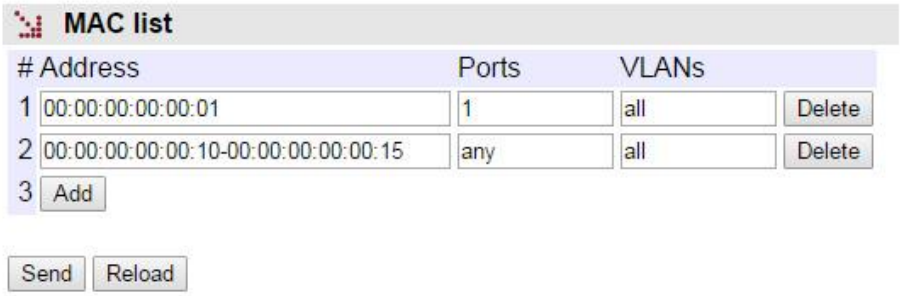
Este submenú permite especificar la lista de direcciones MAC autorizadas de clientes. La lista podrá activarse o no en cada puerto mediante el parámetro ***Security type*.**

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

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

> La presencia de identificadores en el parámetro **Ports** y el apartado **VLANs** no son excluyentes. Si se especifican valores en ambos parámetros, la configuración se aplicará en los puertos señalados que también cumplan el requisito de pertenencia a las VLAN configuradas.

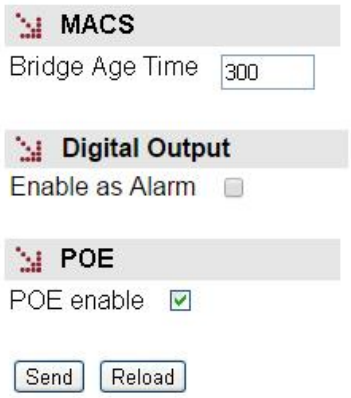
FIGURA 47 Pantalla de configuración del submenú ***MAC list***



5.16 CONFIGURACIÓN OTHERS

El menú ***Others*** permite habilitar/deshabilitar la utilización de la alimentación PoE, configurar el tiempo que el switch almacena las direcciones MAC sin actividad, así como configurar la salida digital como alarma.

FIGURA 48 Pantalla de configuración del menú ***Others***



Los apartados y sus parámetros de configuración son los siguientes:

MACS:

- **Bridge Age Time.** Establece el tiempo máximo que una dirección MAC aprendida y sin actividad permanecerá en la tabla de direcciones MAC del switch. El valor a configurar, en segundos, está comprendido entre 15 y 3600. Por defecto, el valor establecido es 300.

Digital Output:

- **Enable as Alarm.** Un parámetro *CheckBox* simple para indicar si la salida digital, contactos 1 y 2 del conector I/O, va a utilizarse como alarma.

POE:

- **POE enable.** Esta opción se visualiza en el equipo con puertos frontales y fuente de alimentación PoE. Marcando esta casilla se habilita el suministro de alimentación Power over Ethernet (IEEE 802.3af). Dicha alimentación ofrece la posibilidad de alimentar directamente dispositivos IP a través de los cuatro primeros puertos (1 a 4) eléctricos del equipo.

5.17 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.

5.18 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.

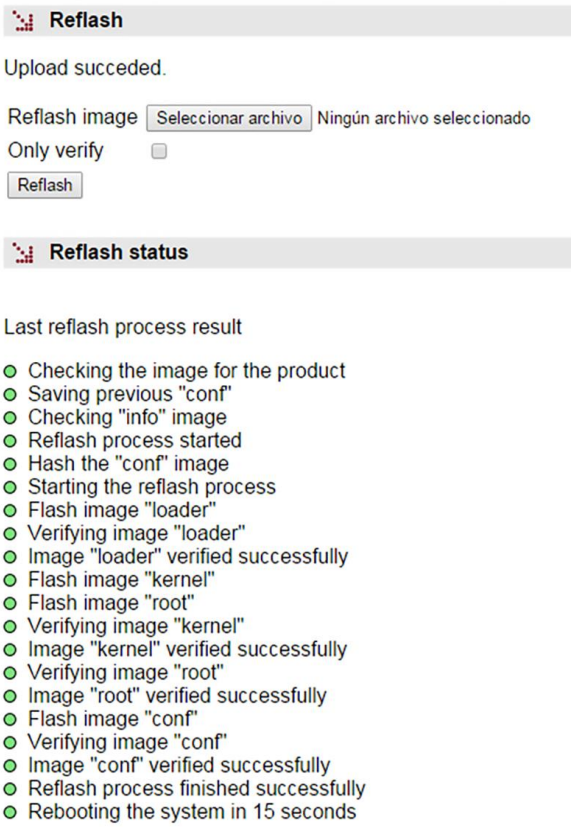
> El proceso de actualización de código no altera los datos de configuración, a no ser que se indique de forma expresa. No obstante, una vez ha finalizado, supone la pérdida momentánea de servicio, por el reinicio automático del equipo.

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

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

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

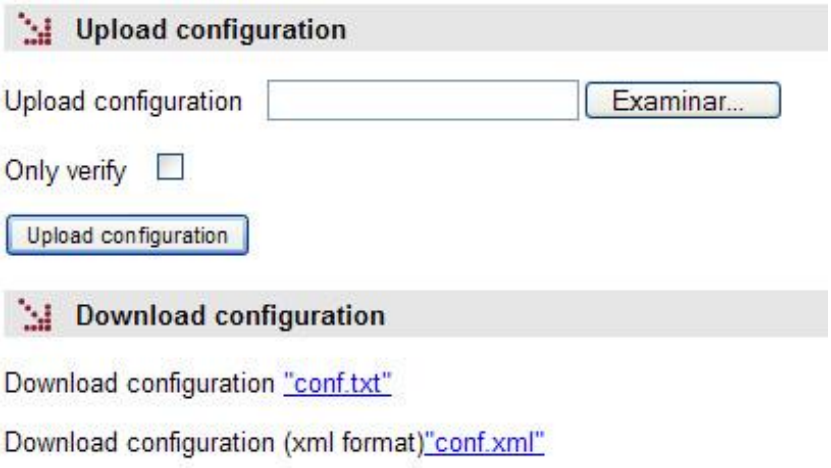
FIGURA 49 Página de configuración *Reflash*



5.19 FICHERO DE CONFIGURACIÓN

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

FIGURA 50 Opciones para el volcado (***Upload***) y obtención (***Download***) del fichero de configuración



5.19.1 Upload (del PC al equipo)

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

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

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

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

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

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

5.19.2 Download (del equipo al PC)

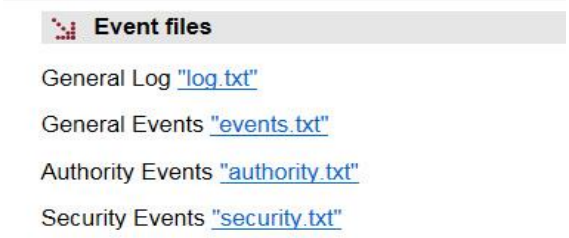
Mediante esta opción, el usuario obtiene una copia local de la configuración del equipo en un fichero tipo texto (con extensión .**txt**) o tipo XML (con extensión.**xml**).

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

5.20 EVENT FILES

Mediante esta opción, el usuario puede descargarse diferentes archivos de log en formato txt.

FIGURA 51 Página de configuración Event Files



Están disponibles el log de eventos total (General Log “log.txt”), el log de eventos más relevantes (General Events “events.txt”), el log de eventos de autenticación (Authority Events “authority.txt”) y el log de eventos de seguridad (Security Events “security.txt”). Este último sólo es accesible para usuarios tipo Admin.

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

6 ESTADÍSTICAS

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

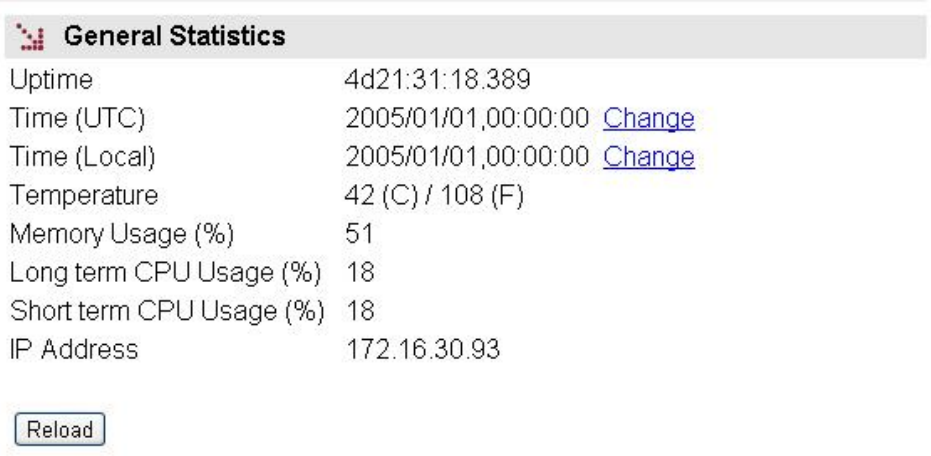
El primer bloque muestra datos generales relativos al equipo, y se muestra de forma automática cuando se selecciona el objeto estadísticas (*Statistics*).

El resto de las estadísticas se agrupan en torno a los datos pertenecientes al estado de los puertos Ethernet (*Ports*), las direcciones MAC identificadas por el switch, protocolo STP, protocolo LLDP, y cliente de sincronización (*NTP*), accediendo a cada uno de ellos mediante la selección de la etiqueta correspondiente localizada bajo el epígrafe *Statistics*.

Cada una de las tablas de datos estadísticos se 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 52 Ejemplo de estadística relativa a Datos Generales

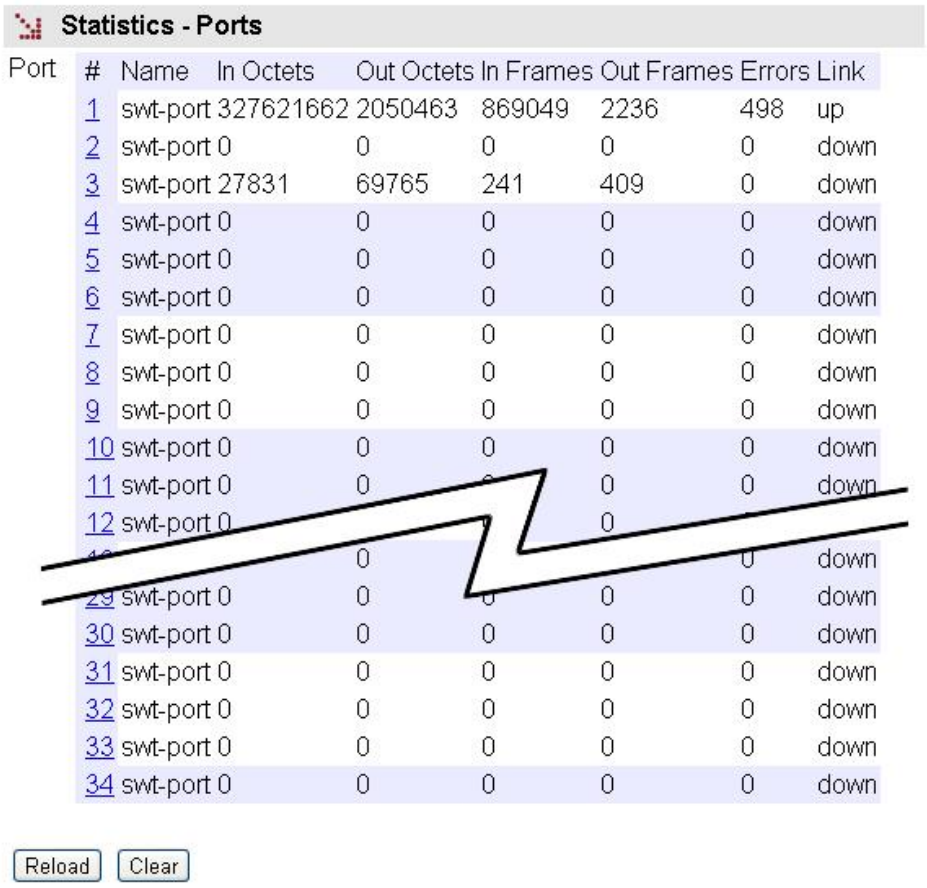


General Statistics

Uptime	4d21:31:18.389
Time (UTC)	2005/01/01,00:00:00 Change
Time (Local)	2005/01/01,00:00:00 Change
Temperature	42 (C) / 108 (F)
Memory Usage (%)	51
Long term CPU Usage (%)	18
Short term CPU Usage (%)	18
IP Address	172.16.30.93

Reload

FIGURA 53 Ejemplo de estadística relativa al estado de los puertos Ethernet



Statistics - Ports

Port

#	Name	In Octets	Out Octets	In Frames	Out Frames	Errors	Link
1	swt-port	327621662	2050463	869049	2236	498	up
2	swt-port	0	0	0	0	0	down
3	swt-port	27831	69765	241	409	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
9	swt-port	0	0	0	0	0	down
10	swt-port	0	0	0	0	0	down
11	swt-port	0	0	0	0	0	down
12	swt-port	0	0	0	0	0	down
29	swt-port	0	0	0	0	0	down
30	swt-port	0	0	0	0	0	down
31	swt-port	0	0	0	0	0	down
32	swt-port	0	0	0	0	0	down
33	swt-port	0	0	0	0	0	down
34	swt-port	0	0	0	0	0	down

Reload Clear

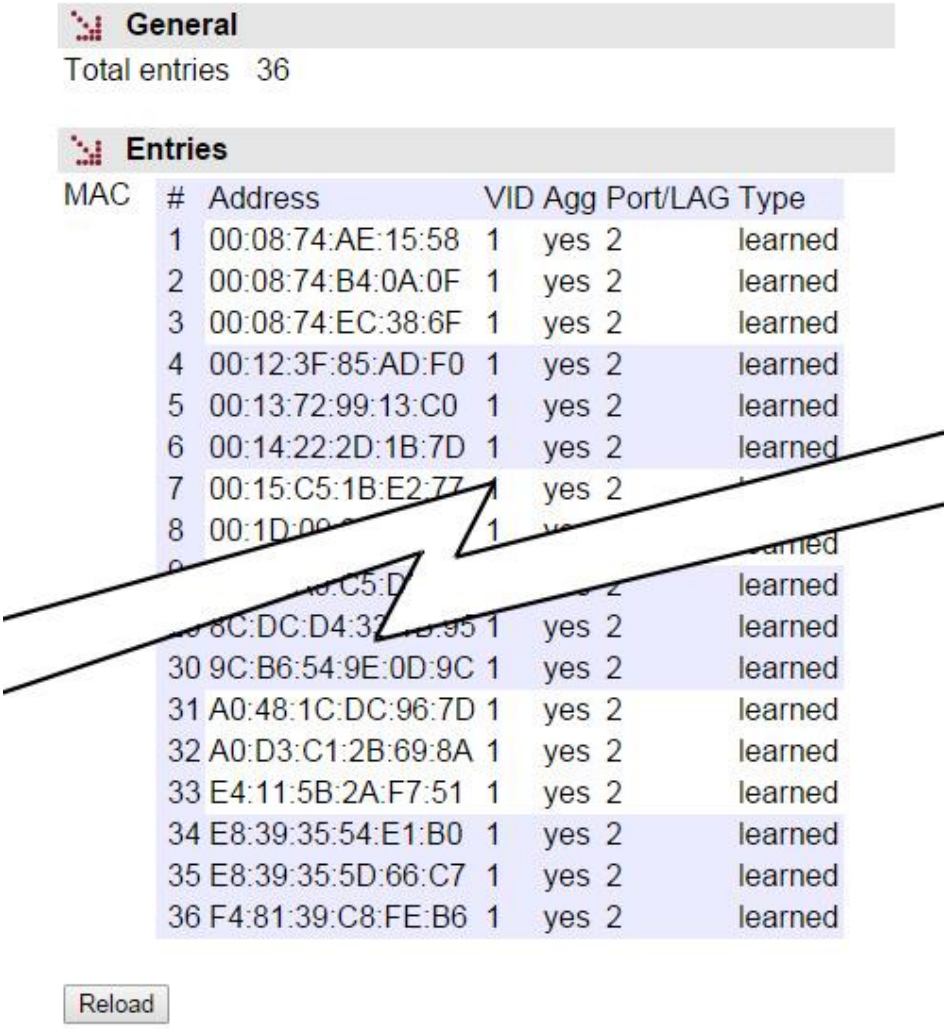
FIGURA 54 Ejemplo de detalle de estadística de un puerto específico (selección del parámetro #)

Statistics - Ports

Port	3
Name	swt-port
Description	STP
Physical Address	00:E0:AB:02:53:82
In Octets	27831
Out Octets	69765
Total Octets	8919104248
In Frames	241
Out Frames	409
Total Frames	14298285
In Errors	0
Out Errors	0
Errors	0
In Unicasts	6514270
Out Unicasts	4083911
Total Unicasts	10598181
In Broadcasts	1913205
Out Broadcasts	19415
Total Broadcasts	1932620
In Multicasts	1761996
Out Multicasts	5488
Total Multicasts	1767484
CRC align errors	0
Fragments	0
Oversize frames	0
Jabbers	0
Collisions	0
Late collision	0
Frames 64 octets	1946027
Frames 65 to 127 octets	2221521
Frames 128 to 255 octets	486092
Frames 256 to 511 octets	102819
Frames 512 to 1023 octets	57591
Frames 1024 to 1536 octets	5375421
Ready	on
Link	down
Speed	100000000
Duplex	fullduplex
Tx Power	unknown
Rx Power	unknown

Reload Clear

FIGURA 55 Ejemplo de estadística relativa a direcciones MAC identificadas por el switch



General

Total entries 36

Entries

MAC

#	Address	VID	Agg	Port/LAG	Type
1	00:08:74:AE:15:58	1	yes	2	learned
2	00:08:74:B4:0A:0F	1	yes	2	learned
3	00:08:74:EC:38:6F	1	yes	2	learned
4	00:12:3F:85:AD:F0	1	yes	2	learned
5	00:13:72:99:13:C0	1	yes	2	learned
6	00:14:22:2D:1B:7D	1	yes	2	learned
7	00:15:C5:1B:E2:77	1	yes	2	
8	00:1D:09	1			
					learned
					learned
	8C:DC:D4:32	1	yes	2	learned
30	9C:B6:54:9E:0D:9C	1	yes	2	learned
31	A0:48:1C:DC:96:7D	1	yes	2	learned
32	A0:D3:C1:2B:69:8A	1	yes	2	learned
33	E4:11:5B:2A:F7:51	1	yes	2	learned
34	E8:39:35:54:E1:B0	1	yes	2	learned
35	E8:39:35:5D:66:C7	1	yes	2	learned
36	F4:81:39:C8:FE:B6	1	yes	2	learned

Reload

FIGURA 56 Ejemplo de estadística relativa al protocolo STP

Bridge

Bridge Id	80:00:00:e0:ab:11:55:ea
Topology Changes	0
Time TC	0.000000000
Designated Root	80:00:00:e0:ab:11:55:ea
Designated Cost	0
Designated Port	none
Max Age	20.000000000
Hello Time	2.000000000
Forward Delay	15.000000000

Ports

Port #	Role	Status	Cost	Bridge	Edge	PtP	LAG
1	designated	forwarding	0	80:00:00:e0:ab:11:55:ea	on	on	none
2	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
3	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
4	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
5	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
6	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
7	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
14	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
15	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
16	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
17	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
18	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none

Reload

FIGURA 57 Ejemplo de estadística del protocolo LLDP

General

Remote Tables Last Changed	3d21:09:37.245
Remote Tables Inserts	9
Remote Tables Deletes	5
Remote Tables Drops	0
Remote Tables Ageouts	0

Port counters

Port #	Txmtd	Len. Err	Disc. Rx Error	Rx Rcvd	Disc. TVLs	Unrec. TLVs	Port Ageouts
1	898	0	0	0	1028	0	0	0
2	0	0	0	0	0	0	0	0
3	11039	0	0	0	11847	0	0	0
4	0	0	0	0	0	0	0	0
5	11031	0	0	0	12047	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	11029	0	0	0	6090	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Remote data

Entry #	L. Port	R. Chassis	R. Port	R. Port Desc	R. Sys Name	R. Sys Desc	R. Caps	R. Caps En
1	1	00:15:C5:27:2A:C3	e5					
2	5	02:E0:AB:14:0E:CA	p1	e1	l2-0.5-3.36		0x4	0x4
3	3	02:E0:AB:14:BA:CA	p1	e1	l3-1.206-3.37		0x14	0x14
4	8	4C:5E:0C:75:32:C0	ether2-master		MikroTik	MikroTik RouterOS 6.38.1 (stable) RB750	0x14	0x10

Reload

FIGURA 58 Ejemplo de estadística relativa a NTP

NTP

Offset	0.000000000
Frequency offset	17.471
Jitter	0.010059728
Allan	0.000000

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.

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

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 local y remoto, mediante Telnet.

Acceso a través del puerto SRV

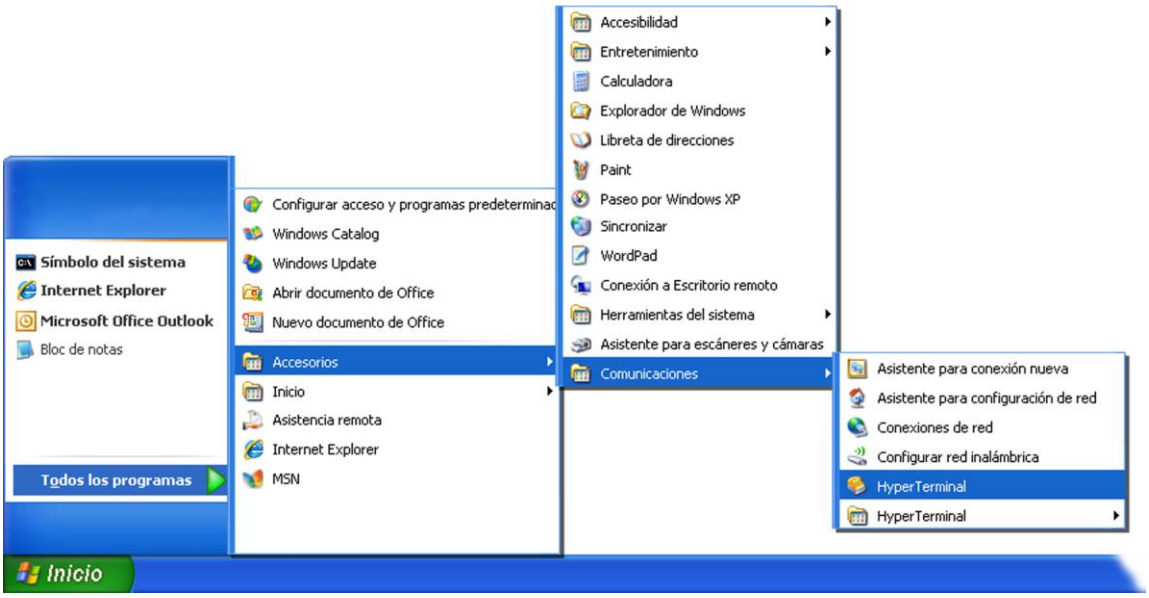
El acceso en modo local se realiza mediante un cable serie plano, conectando el puerto serie del ordenador al puerto serie del equipo (SRV).

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

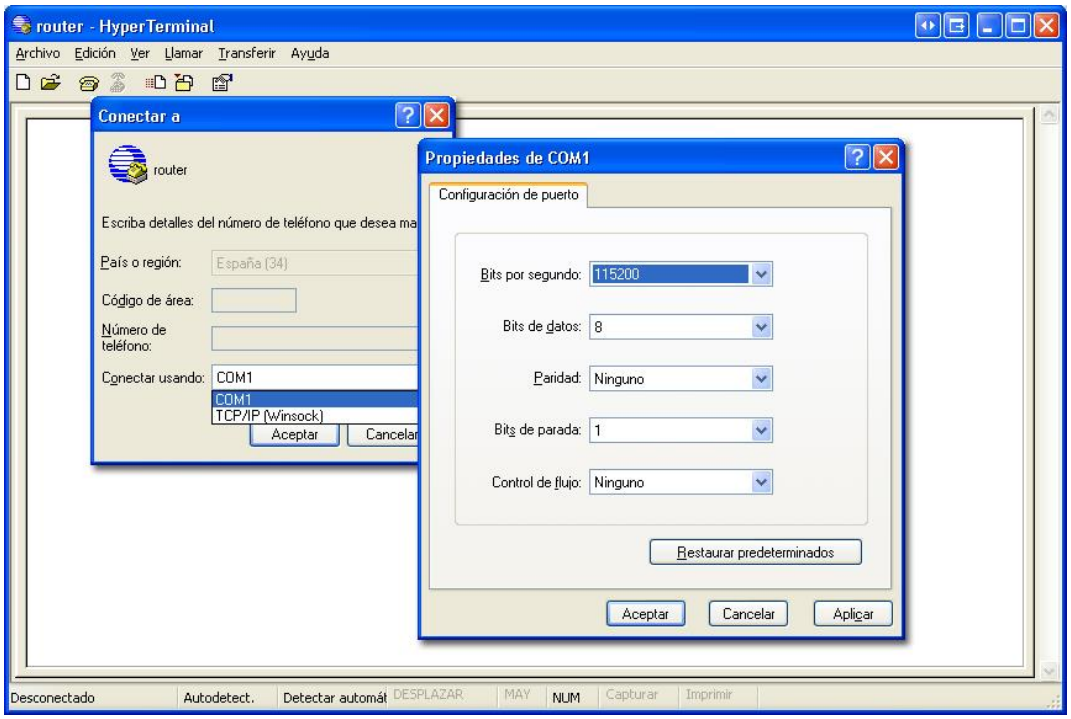
En Windows XP© se puede ejecutar *HyperTerminal* desde *Inicio* → *Todos los Programas* → *Accesorios* → *Comunicaciones* → *HyperTerminal* (véase FIGURA 59).

FIGURA 59 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 60).

FIGURA 60 Configuración de la conexión por puerto serie con *HyperTerminal*



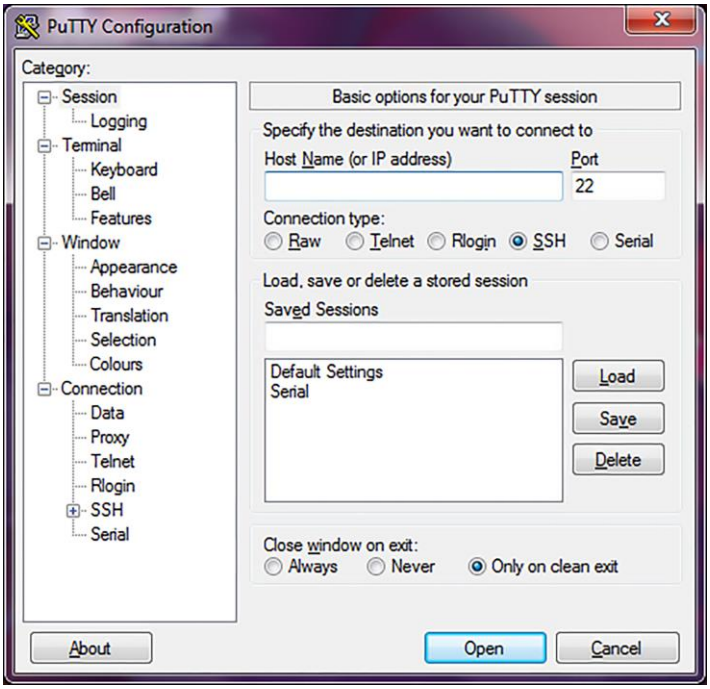
Ejecutar la opción *Llamar* del menú *Llamar*. Pulsando return, se mostrará una ventana en la que aparecerá el prompt ***swt login:*** esperando a que introduzcamos el *login* de usuario y, posteriormente, la clave de inicio de sesión (los usuarios y sus respectivos passwords son los mismos que en la interfaz web).

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

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

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

FIGURA 61 Ventana principal de *Putty*



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

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

FIGURA 62 Ventana del administrador de dispositivos

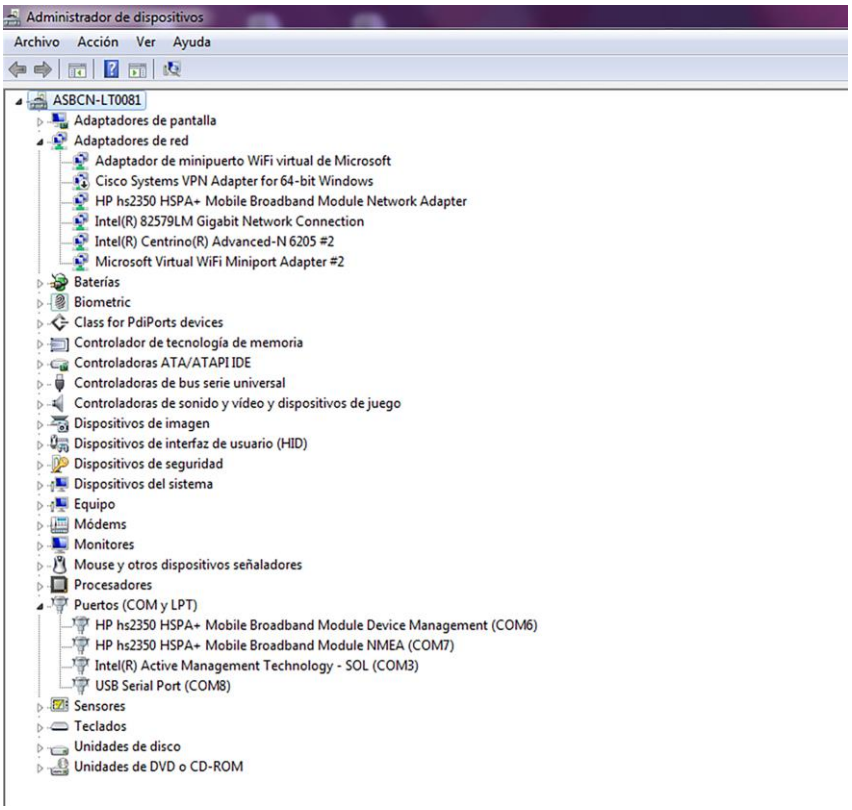
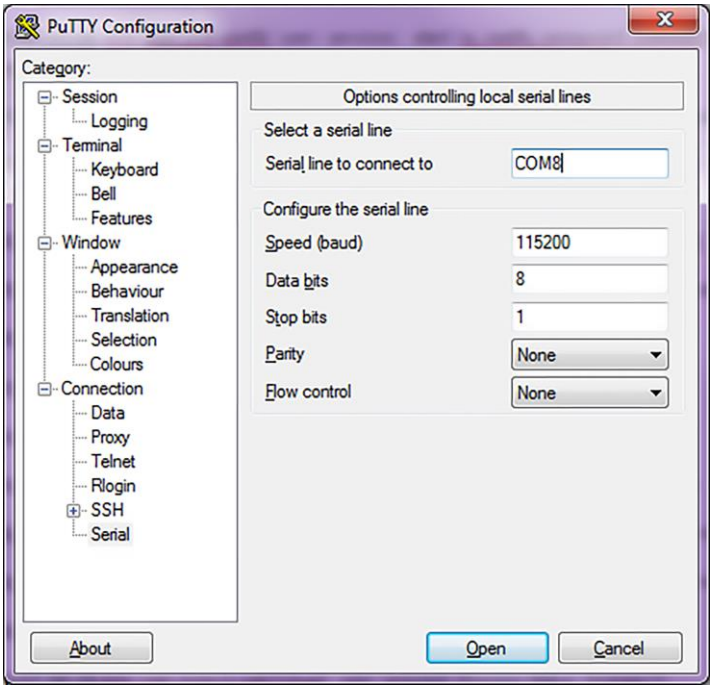


FIGURA 63 Configuración de la conexión por puerto serie con *Putty*



Pulsado el botón *Open*, y si es necesario return, se mostrará una ventana en la que aparecerá el prompt ***swt 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).

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

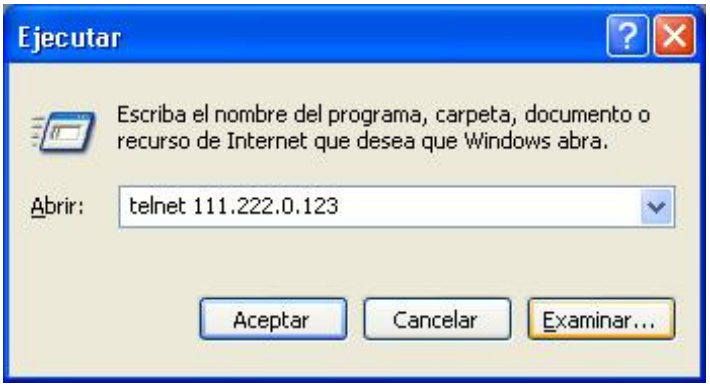
Acceso mediante Telnet

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

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

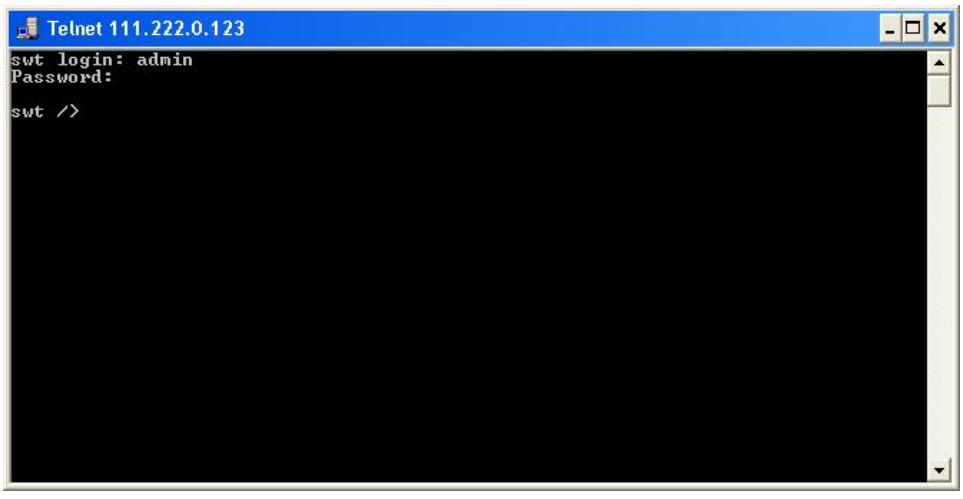
En Windows XP© se puede ejecutar Telnet desde el botón de inicio: Inicio → Ejecutar y, en la ventana de dialogo que aparece, escribir: telnet + espacio + Dirección_IP_del_equipo (en el ejemplo 111.222.0.123), pulsando, seguidamente, sobre el botón Aceptar (véase FIGURA 64).

FIGURA 64 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 65).

FIGURA 65 Ventana de *Telnet*



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

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

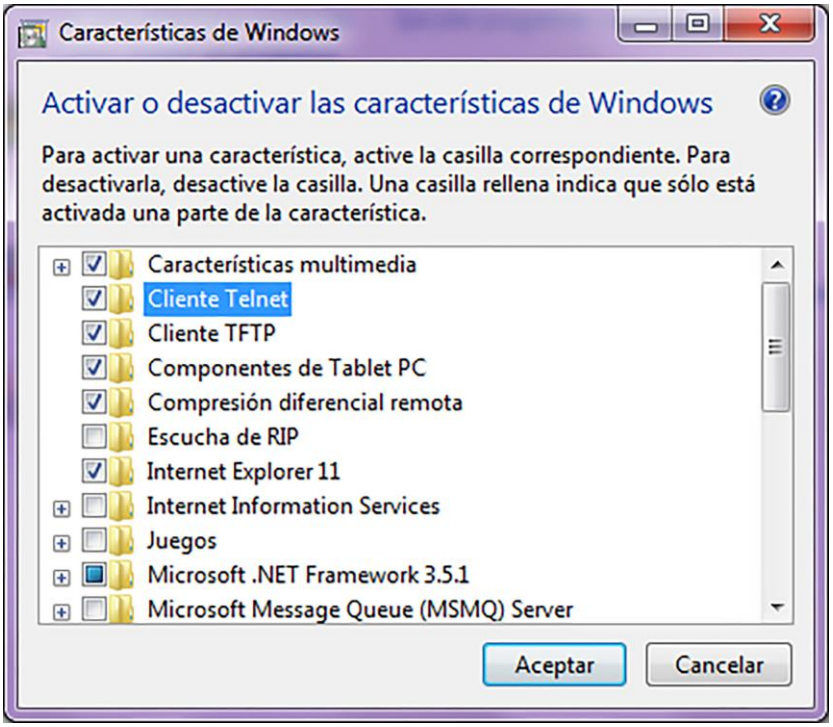
Sea cual sea el método elegido para establecer la conexión con el equipo, aparecerá el prompt ***swt login:*** esperando a que introduzcamos el *login* de usuario y, posteriormente, la clave de inicio de sesión (los usuarios y sus respectivos passwords son los mismos que en la interfaz web).

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

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

A continuación, en la ventana de *Características de Windows*, seleccionar *Cliente Telnet*, véase FIGURA 66. Pulsando *Aceptar*, ya se podrá utilizar el cliente Telnet de Windows.

FIGURA 66 Ventana de Características de Windows



B.2 COMANDOS DE LA CONSOLA DE USUARIO

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

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

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

TABLA 2 Listado completo de comandos de la consola de usuario CLI

Comando	Descripción	Usuario	
		admin	guest
add	Añade un nuevo ítem a un parámetro de tipo matricial	✓	✗
apply	Aplica la nueva configuración	✓	✗
cd	Cambia de directorio en el árbol de parámetros	✓	✓
clear	Borra las estadísticas	✓	✗
date	Muestra la fecha almacenada en el equipo	✓	✗
download	Genera un fichero de comandos de configuración	✓	✓
exit	Interrumpe la conexión con el equipo	✓	✓
get	Muestra los valores de los parámetros	✓	✓
help	Muestra la lista de comandos disponibles	✓	✓
log	Muestra el fichero de log en uso	✓	✓
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	✓	✗
show	Equivale al comando log, pero permite la consulta de los ficheros de log de más antigüedad especificando el nombre del fichero como parámetro	✓	✓
stats	Muestra el estado del equipo	✓	✓
tail	Muestra el listado de eventos almacenados en el fichero de log y se mantiene para mostrar los eventos a medida que se producen. Se finaliza el comando con Ctrl+C	✓	✓
telnet	Abre una sesión telnet sin interrumpir la conexión con el equipo	✓	✓

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

TABLA 3 Clasificación de los comandos según su función

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

Información incluida en el log

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

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

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

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

Comandos de configuración

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

Sintaxis: 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 Permite obtener una copia (back up) de los parámetros configurados en el equipo, los cuales tendrán un valor distinto al de defecto (fábrica). Por ello, este comando es útil 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 Muestra el listado de eventos del fichero de log en uso (actual).

Sintaxis: drn /> **log**

Argumentos:

- Sin argumentos, este comando muestra los eventos registrados en el fichero de log actual.

Observaciones: Todos los eventos producidos en el equipo se almacenan en ficheros con carácter permanente. El número máximo de ficheros es 5. Los ficheros se usan de forma rotativa si bien se mantiene siempre una denominación que establece la secuencia temporal, usando para ello un sufijo. Cuanto mayor es el sufijo, más antiguo es el contenido del fichero. Para ver los ficheros más antiguos, se emplea el comando **show.**

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

Ejemplo: drn /> **log**
drn /> **log crit**
drn /> **log debug**

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

Sintaxis: 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**

show Muestra en pantalla el contenido del fichero de log especificado.

Sintaxis: drn /> **show** *fichero*

Argumentos:

fichero Nombre del fichero a mostrar. El fichero de log en uso (actual) se denomina *messages*. Los ficheros log de más antigüedad incluyen un sufijo, p.e. *messages.1*.

Observaciones: Pueden mostrarse cinco ficheros de log como máximo: *messages* (log en uso), *messages.0*, *messages.1*, *messages.2* y *messages.3*. Los ficheros almacenan los datos con continuidad temporal. En el caso de los log de más antigüedad, cuanto mayor es el sufijo, mas antiguo es el contenido del fichero.
El fichero de configuración por defecto de cliente está almacenado como *customer.txt.*

Ejemplo: drn /> **show messages**
drn /> **show messages.0**
drn /> **show messages.1**
drn /> **show messages.2**
drn /> **show messages.3**

drn /> **show customer.txt**

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.

La ejecución del comando ***stats*** estando en drn/mac> muestra las direcciones MAC identificadas por el switch.

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

tail Este comando es útil para monitorizar el equipo y detectar posibles errores durante su funcionamiento. Muestra el listado de eventos almacenados en el fichero de log en uso (actual) y se mantiene para mostrar los eventos a medida que se producen. Se finaliza el comando con ***Ctrl.+C***.

Sintaxis: drn /> **tail**

Argumentos:

- Sin argumentos, este comando muestra los eventos registrados en la memoria no volátil del equipo.

Observaciones: Al ejecutar este comando, el equipo se mantiene para mostrar los eventos a medida que se producen hasta que el usuario pulse la combinación de teclas ***Ctrl.***+***C***.

Ejemplo: drn /> **tail**

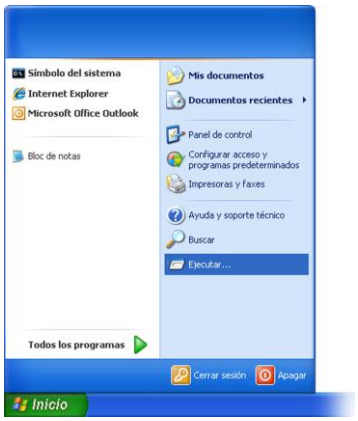
B.3 OBTENCIÓN DE INFORMACIÓN DEL ESTADO Y LA CONFIGURACIÓN DE UN EQUIPO

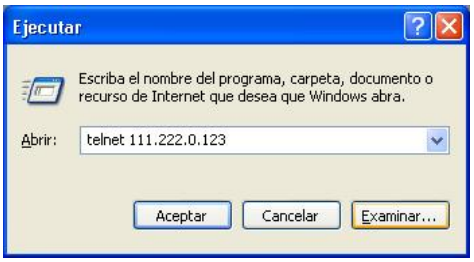
Para la obtención de información sobre el estado y la configuración de un equipo se deberán seguir los siguientes pasos:

1- Conexión con el equipo

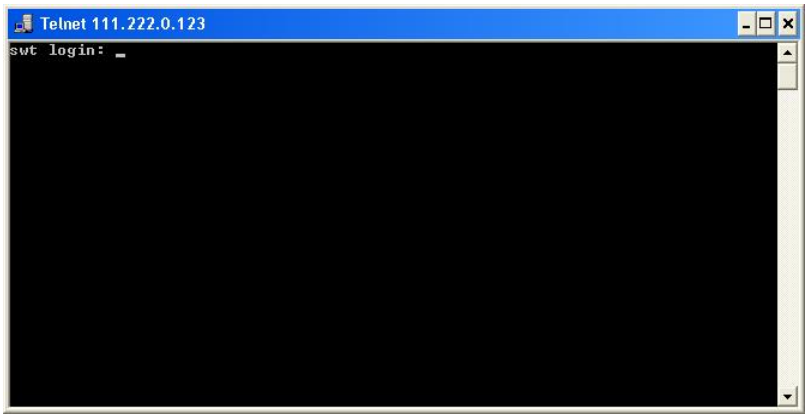
Como se ha explicado en el capítulo **B.1**, la conexión con el equipo difiere ligeramente según el método de elegido. En este ejemplo se supone que el equipo está conectado a una red y que tiene una dirección IP configurada que, para este ejemplo, será 111.222.0.123. Así mismo, el ordenador utilizado 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***.





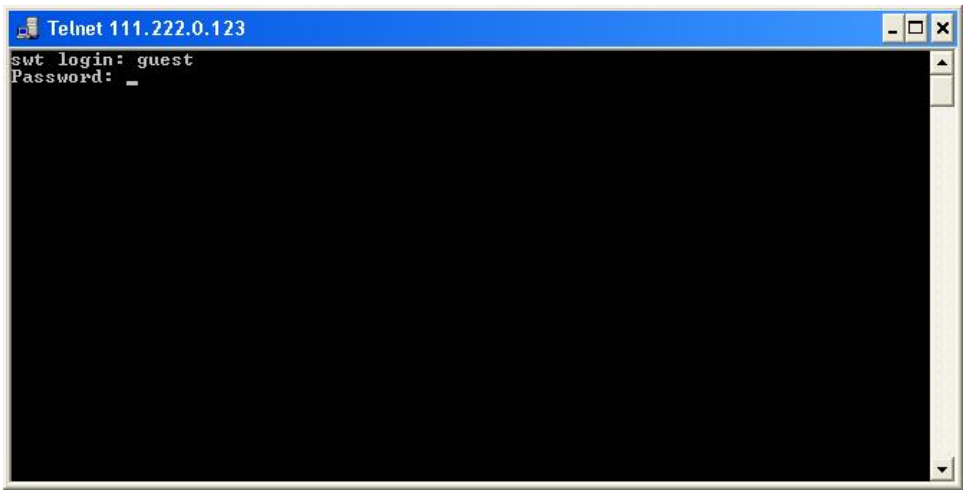
Si todo ha funcionado correctamente se abrirá una ventana de símbolo del sistema que será la interfaz de nuestra conexión.



2- Identificación del usuario

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

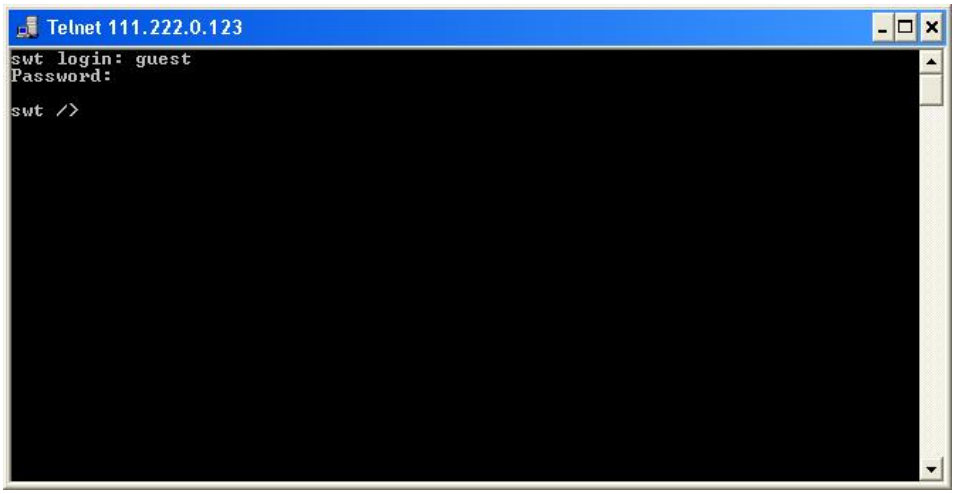
Como tan sólo deseamos obtener información, da lo mismo con que usuario se entre (***admin*** o ***guest***). Así, escribiremos ***guest*** y pulsaremos ***enter.***



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

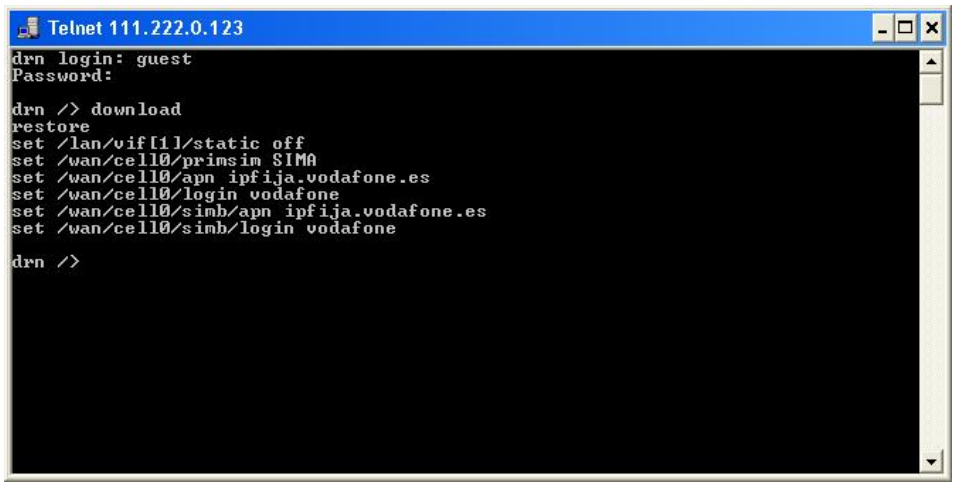
> Hay que tener en cuenta que en la ventana de *Telnet* no aparece texto alguno mientras se introduce el password.

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



3- Obtención de la configuración del equipo

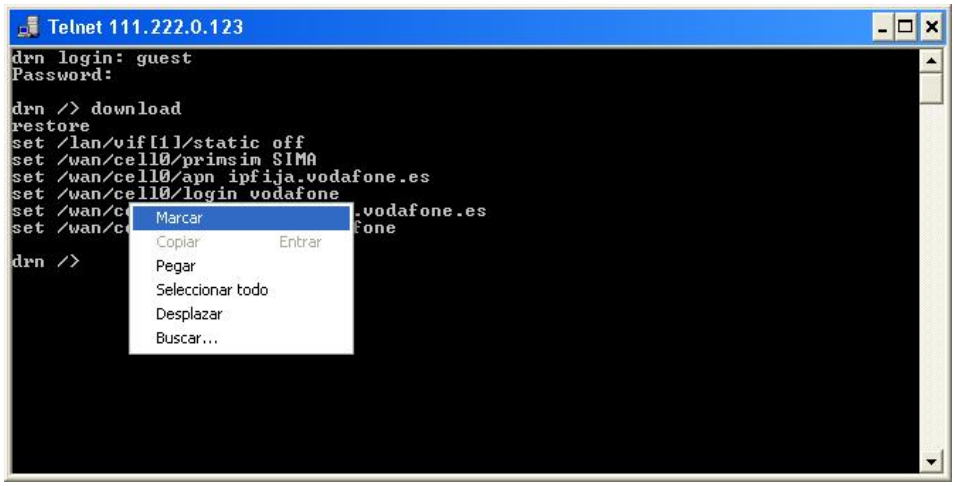
La configuración del equipo se obtiene mediante el comando ***download***. Al pulsar ***enter*** después de escribir este comando se mostrará la configuración completa del equipo. En la figura de ejemplo el equipo corresponde a un ***DRA-2***.



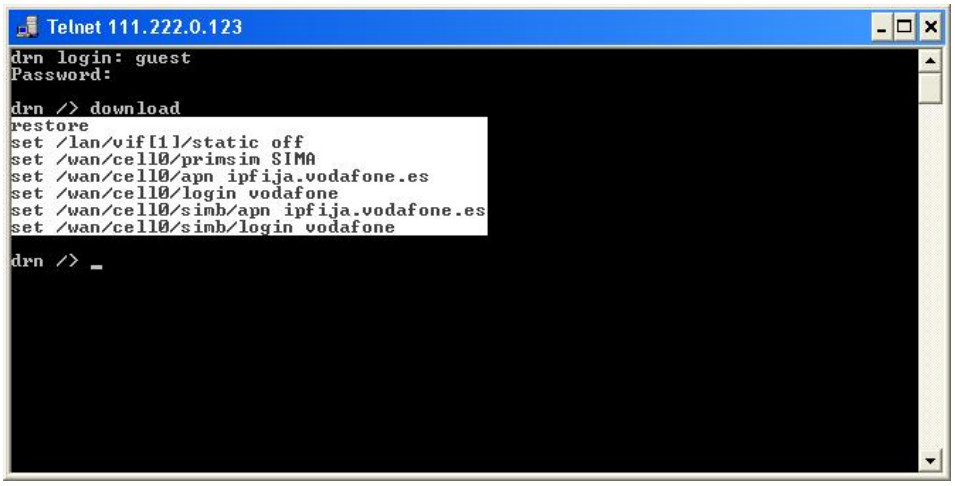
En caso de que la información mostrada exceda los límites de la ventana, el sistema sólo mostrará la información del principio y será necesario pulsar ***enter*** una o más veces hasta que se haya mostrado toda la información. Sabremos que el sistema ha mostrado toda la información cuando aparezca de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

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

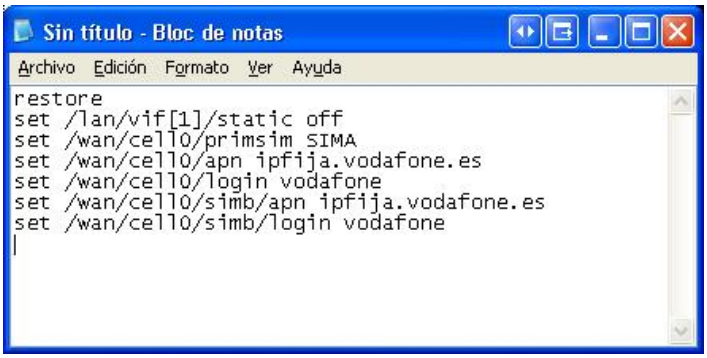
Para copiar texto desde la ventana de comandos de Windows XP© se deberá pulsar el botón derecho del ratón y del menú que aparece seleccionar ***Marcar***.



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

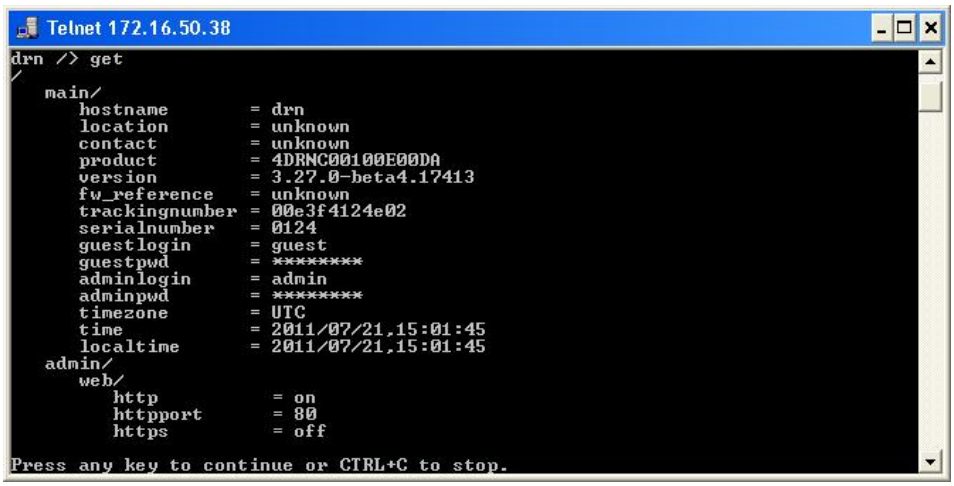


Ahora podremos abrir el *Bloc de notas* de Windows y pegar el texto (***Ctrl.*** + ***V***) en un archivo *.txt* para guardarlo.



4- Obtención del estado del equipo

El comando ***get*** muestra el estado completo del equipo. Dado que la información a mostrar es muy extensa, cada vez que se llene la ventana, esperará a que el usuario pulse una tecla para continuar mostrando información. En la figura de ejemplo el equipo corresponde a un ***DRA-2***.

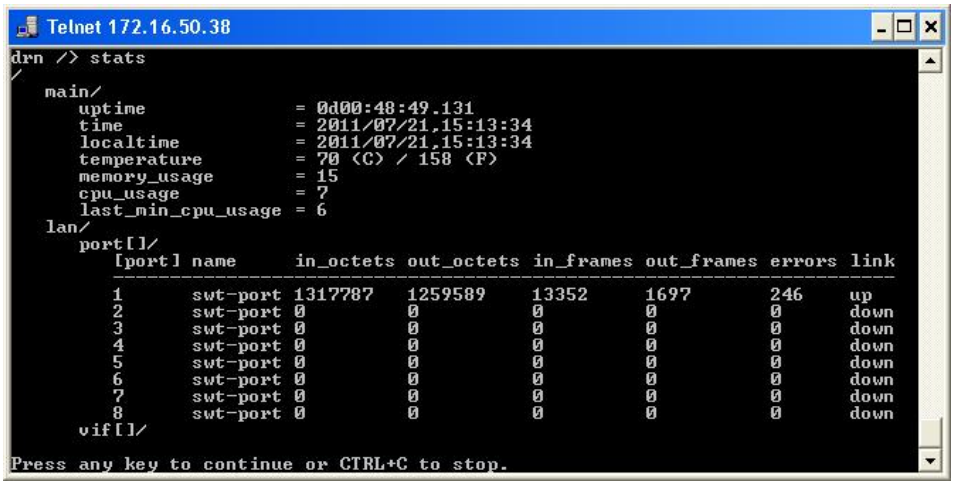


Sabremos que el sistema habrá mostrado toda la información cuando aparezca de nuevo el prompt del equipo.

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***. En la figura de ejemplo el equipo corresponde a un ***DRA-2***.



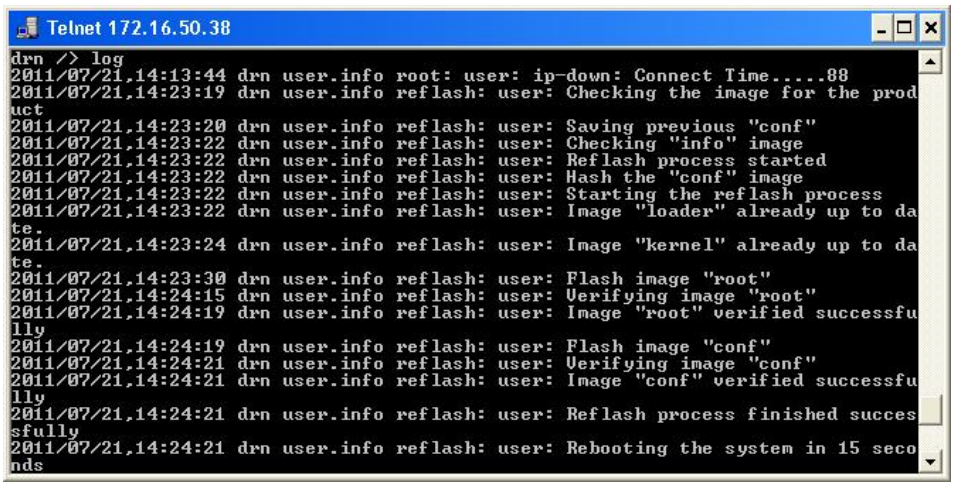
Al igual que los comandos anteriores, si la información a mostrar excede del tamaño de la ventana, se detendrá y esperará a que el usuario pulse una tecla para continuar.

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 obtener el listado de eventos del fichero de log en uso (actual).

Para la consulta de los ficheros de log de más antigüedad, debe utilizarse el comando ***show.*** En la figura de ejemplo el equipo corresponde a un ***DRA-2.***



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 ***tail*** permite consultar los eventos ocurridos en el equipo en tiempo real. Al ejecutar este comando, el equipo se mantiene para mostrar los eventos a medida que se producen hasta que el usuario pulse la combinación de teclas ***Ctrl.+C***.

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

```
swt login: guest
Password:

swt /> get
/
main/
      hostname       = l2-0.20-3.31-lite2
      location       = unknown
      contact        = unknown
      product        = 3SWTES001NM300AM
      version        = 3.31.14.42186
      fw_reference   = 4WF72030000-R013
      trackingnumber = 00001888b5d9
      serialnumber   = 1000000
      guestlogin     = guest
      guestpwd       =
tH4sIADaCD1wCAzM0AAPtgsTi4vIUA0MAkoosAhAAAAA5M2NlNmFiN2I0MzA2UZDkOZTE3YzM3YjU0ZjQ3Y2UwZgo=
      adminlogin     = admin
      adminpwd       =
tH4sIADaCD1wCAzM0AAPtgsTi4vIUAyMAKNslmxAAAABlMjRiMWM4NmNkMWI3UZDhlMWQyNDY5OWZiMWE3NWUyMAo=
      timezone       = Madrid
      time           = 2018/12/11,09:24:06
      localtime      = 2018/12/11,10:24:06
   admin/
      web/
         http          = on
         httpport      = 80
         https         = off


Press any key to continue or CTRL+C to stop. [A
 [J         httpsport     = 443
         cert          = empty
         privatekey    = empty
         privatekeypwd = tH4sIADaCD1wCAzM0AANtAHFEx4YIAAAANDI5OTM3YzMyN2VmYjU4MTc2NjM3MMmY1OWJlMWNiOGQK
      cli/
         syslog_level        = 8
         syslog_level_remote = 4
         syslog              = off
         syslog_server       = 0.0.0.0
   eth0/
      static         = off
      ip             = 10.212.0.36
      mask           = 255.255.254.0
      vlanid         = 1
      dgw            = 10.212.1.254
      mac            = 02:E0:AB:01:33:40
      swt_int_mode   = Interrupt_mode
      swt_int_devnum = 0
   qinq/
      stag = 0x88A8
   vlanoverlapping/
      enable = off


Press any key to continue or CTRL+C to stop. [A
 [J   vlan[]/
      [vlan] name      vid priover priority
      ------------------------------------
      1      vlan_name 1   off     0
      2      vlan_name 10  off     0
   port[]/
      [port] name     enable vlan_function mode vid vid_acl lag  lag_config
      ------------------------------------------------------------------------
      1      e1       on     edge          auto 1   auto    none off
      2      e2       on     edge          auto 1   auto    none off
      3      e3       on     edge          auto 1   auto    none off
      4      e4       on     edge          auto 1   auto    none off
      5      e5       on     edge          auto 1   auto    none off
      6      e6       on     edge          auto 1   auto    none off
      7      e7       on     edge          auto 1   auto    4    on
      8      e8       on     edge          auto 1   auto    4    off
      9      swt-port on     edge          auto 1   auto    none off
      10     swt-port on     edge          auto 1   auto    none off
      11     swt-port on     edge          auto 1   auto    none off
      12     swt-port on     edge          auto 1   auto    none off
      13     swt-port on     edge          auto 1   auto    none off
      14     swt-port on     edge          auto 1   auto    none off


Press any key to continue or CTRL+C to stop. [A
 [J      15     swt-port on     edge          auto 1   auto    none off
      16     swt-port on     edge          auto 1   auto    none off
      17     swt-port on     edge          auto 1   auto    none off
      18     swt-port on     edge          auto 1   auto    none off
      19     swt-port on     edge          auto 1   auto    none off
      20     swt-port on     edge          auto 1   auto    none off
      21     swt-port on     untag         auto 1   auto    none off
      22     swt-port on     edge          auto 1   auto    none off
      23     swt-port on     edge          auto 1   auto    none off
      24     swt-port on     edge          auto 1   auto    none off
   qos/
      weightfair_enable = on
      priority[]/
         [priority] queue
         ----------------
         0          medium
         1          medium
         2          medium
         3          medium
         4          medium
         5          medium
         6          medium
```

```
Press any key to continue or CTRL+C to stop. [A
 [J         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


Press any key to continue or CTRL+C to stop. [A
 [J         8      0        on             off
         9      0        on             off
         10     0        on             off
         11     0        on             off
         12     0        on             off
         13     0        on             off
         14     0        on             off
         15     0        on             off
         16     0        on             off
         17     0        on             off
         18     0        on             off
         19     0        on             off
         20     0        on             off
         21     0        on             off
         22     0        on             off
         23     0        on             off
         24     0        on             off
   rate_control/
      ingress[]/
         [ingress] enable traffic rate
         ---------------------------------
         1         off    all     90000000


Press any key to continue or CTRL+C to stop. [A
 [J         2          off    all     60000000
         3         off    all     40000000
         4         off    all     20000000
         5         off    all     64000
         6         off    all     64000
         7         off    all     64000
         8         off    all     64000
         9         off    all     64000
         10        off    all     64000
         11        off    all     64000
         12        off    all     64000
         13        off    all     64000
         14        off    all     64000
         15        off    all     64000
         16        off    all     64000
         17        off    all     64000
         18        off    all     64000
         19        off    all     64000
         20        off    all     64000
         21        off    all     64000
         22        off    all     64000
         23        off    all     64000


Press any key to continue or CTRL+C to stop. [A
 [J         24        off    all     64000
      egress[]/
         [egress] enable rate
         --------------------
         1        off    64000
         2        off    64000
         3        off    64000
         4        off    64000
         5        off    64000
         6        off    64000
         7        off    64000
         8        off    64000
         9        off    64000
         10       off    64000
         11       off    64000
         12       off    64000
         13       off    64000
         14       off    64000
         15       off    64000
         16       off    64000
         17       off    64000
         18       off    64000


Press any key to continue or CTRL+C to stop. [A
 [J         19       off    64000
         20       off    64000
         21       off    64000
         22       off    64000
         23       off    64000
         24       off    64000
   monitor/
      ingress_enable    = on
      ingress_dest_port = 4
      egress_enable     = off
      egress_dest_port  = 4
      port[]/
         [port] ingress egress
         ---------------------
         1      off     off
```

```
         2      off     off
         3      off     off
         4      off     off
         5      off     off
         6      off     off
         7      off     off
         8      off     off


Press any key to continue or CTRL+C to stop. [A
 [J         9      off     off
         10     off     off
         11     off     off
         12     off     off
         13     off     off
         14     off     off
         15     off     off
         16     off     off
         17     off     off
         18     off     off
         19     off     off
         20     off     off
         21     on      on
         22     off     off
         23     off     off
         24     off     off
   mac/
      age_time = 300
   stp/
      enable        = on
      version       = rstp
      priority      = 32768


Press any key to continue or CTRL+C to stop. [A
 [J      max_age       = 20.000000000
      hello_time    = 2.000000000
      forward_delay = 15.000000000
      tx_hold_count = 6
      port[]/
         [port] enable priority cost   edge ptp  edge_tx_filter
         ------------------------------------------------------
         1      on      128      200000 auto auto off
         2      on      128      200000 auto auto off
         3      on      128      200000 auto auto off
         4      on      128      200000 auto auto off
         5      on      128      200000 auto auto off
         6      on      128      200000 auto auto off
         7      on      128      200000 auto auto off
         8      on      128      200000 auto auto off
         9      on      128      200000 auto auto off
         10     on      128      200000 auto auto off
         11     on      128      200000 auto auto off
         12     on      128      200000 auto auto off
         13     on      128      200000 auto auto off
         14     on      128      200000 auto auto off
         15     on      128      200000 auto auto off


Press any key to continue or CTRL+C to stop. [A
 [J         16     on      128      200000 auto auto off
         17     on      128      200000 auto auto off
         18     on      128      200000 auto auto off
         19     on      128      200000 auto auto off
         20     on      128      200000 auto auto off
         21     on      128      20000  auto auto off
         22     on      128      20000  auto auto off
         23     on      128      20000  auto auto off
         24     on      128      20000  auto auto off
   lldp/
      enable = on
      port[]/
         [port] admin_status transmit_interval hold_multiplier reinit_delay credit_max
trans_interval_fast number_message_fast_tx notification_enable tx_portdesc tx_sysname tx_sysdesc
tx_syscap tx_management management_address
         ------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------
--------------------
         1      TxRx            30                 4               2               5               1
4                       off                 on              on              off             off             off
0.0.0.0
         2      TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         3      TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         4      disabled        30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         5      TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         6      TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         7      TxRx            30                 4               2               5               1
4                       off                 on              on              off             off             off
0.0.0.0
         8      TxRx            30                 4               2               5               1
4                       off                 on              on              off             off             off
0.0.0.0


Press any key to continue or CTRL+C to stop. [A
 [J         9      TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         10     TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         11     TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
0.0.0.0
         12     TxRx            30                 4               2               5               1
4                       off                 off             off             off             off             off
```

```
0.0.0.0
         13     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         14     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         15     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         16     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         17     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         18     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         19     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         20     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         21     disabled    30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         22     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         23     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
         24     TxRx        30                4           2           5          1
4                     off                off         off         off        off         off
0.0.0.0
   igmp_snooping/
      enable = off
      port[]/
         [port] igmp_forward
         -------------------
         1      auto


Press any key to continue or CTRL+C to stop. [A
 [J         2      auto
         3      auto
         4      auto
         5      auto
         6      auto
         7      auto
         8      auto
         9      auto
         10     auto
         11     auto
         12     auto
         13     auto
         14     auto
         15     auto
         16     auto
         17     auto
         18     auto
         19     auto
         20     auto
         21     auto
         22     auto
         23     auto


Press any key to continue or CTRL+C to stop. [A
 [J         24     auto
   garp_timers/
      port[]/
         [port] join_time leave_time leaveall_time
         -----------------------------------------
         1      200       600        10000
         2      200       600        10000
         3      200       600        10000
         4      200       600        10000
         5      200       600        10000
         6      200       600        10000
         7      200       600        10000
         8      200       600        10000
         9      200       600        10000
         10     200       600        10000
         11     200       600        10000
         12     200       600        10000
         13     200       600        10000
         14     200       600        10000
         15     200       600        10000
         16     200       600        10000
         17     200       600        10000


Press any key to continue or CTRL+C to stop. [A
 [J         18     200       600        10000
         19     200       600        10000
         20     200       600        10000
         21     200       600        10000
         22     200       600        10000
         23     200       600        10000
         24     200       600        10000
   ntp/
      enable   = on
      protocol = ntp
      authkeys[]/
         [authkeys] keynumber key
         ----------------------------
         1          1         xxxxxxxx
      client/
         broadcastenable = off
         server[]/
            [server] ip           type    minpoll maxpoll authenable authkey lowtraffic
            ------------------------------------------------------------------------
            1        10.212.1.205 unicast 5       10      off        1       off
```

```
      sntp/
         client[]/


Press any key to continue or CTRL+C to stop. [A
 [J           [client] ip           poll units   authenable authkey timeout
             ------------------------------------------------------------------
             1        10.212.1.205 1    minutes off        1       5
   igmp/
      enable = off
   gmrp/
      enable = off
      port[]/
         [port] forward_all
         ------------------
         1      normal
         2      normal
         3      normal
         4      normal
         5      normal
         6      normal
         7      normal
         8      normal
         9      normal
         10     normal
         11     normal
         12     normal


Press any key to continue or CTRL+C to stop. [A
 [J         13     normal
         14     normal
         15     normal
         16     normal
         17     normal
         18     normal
         19     normal
         20     normal
         21     normal
         22     normal
         23     normal
         24     normal
   snmp/
      enable              = on
      trapenable          = off
      trap_v1_aggent_addr = none
      community[]/
         [community] name   access
         ------------------------
         1          public ro
      user[]/
         [user] name   access security auth_alg auth_passwd
priv_alg priv_passwd


Press any key to continue or CTRL+C to stop. [A
 [J         ------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------
         1      public ro     clear    MD5
tH4sIADiCD1wCAzM0AAPtOuLUnMTSkoyCxOLi8vyiFADVIuggGAAAADcwODc2cY2FmZGE1OGUwNDUwNTcyMTU2M2EyMzlmOTJhCg==
DES
tH4sIADiCD1wCAzM0AAPtOuLUnIKizLKCxOLi8vyiFAB+BTwoGAAAAGNlZTc1cMjlmOWVmOTUxOGMzMDU1MjRlZmZhNDgxYjBhCg==
      traps/
         dig_in_change  = off
         dig_out_change = off
   access/
      tacacsplus/
         server1_ip = 0.0.0.0
         server2_ip = 0.0.0.0
         encrypted  = on
         shared_key = tH4sIADiCD1wCAzM0AANtAHFEx4YIAAAANDI5OTM3YzMyN2VmYjU4MTc2NjM3MMmY1OWJlMWNiOGQK
         guest_lvl  = 1
         admin_lvl  = 2
      radius/
         server1_ip = 0.0.0.0
         server2_ip = 0.0.0.0
         udp_port   = 1812
         secret     =
tH4sIADiCD1wCAzM0AAPtqswyQyNjE1MAgNPFdBAAAABiZTJlODhjYjNkNDJhUNjZhNWYxMDZkMGM1OTUyYjViZAo=
         timeout    = 10
         guest_lvl  = 1
         admin_lvl  = 2
      console/


Press any key to continue or CTRL+C to stop. [A
 [J         method = local
      web/
         method = local
         local  = on
      telnet/
         method = local
         local  = on
      ssh/
         method = local
         local  = on
      ftp/
         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      dot1x 10            replace
         5      none  10            replace


Press any key to continue or CTRL+C to stop. [A
 [J      6      none  10            replace
         7      none  10            replace
         8      none  10            replace
         9      none  10            replace
```

```
          10     none  10            replace
          11     none  10            replace
          12     none  10            replace
          13     none  10            replace
          14     dot1x 10            replace
          15     none  10            replace
          16     none  10            replace
          17     none  10            replace
          18     none  10            replace
          19     none  10            replace
          20     none  10            replace
          21     none  10            replace
          22     none  10            replace
          23     none  10            replace
          24     none  10            replace
       dot1x/
          enable        = on
          reauth_enable = on


Press any key to continue or CTRL+C to stop. [A
 [J         reauth_period = 3600
          reauth_max    = 2
          quiet_period  = 60
          radius_server/
             ip       = 10.212.4.5
             udp_port = 1812
             secret   =
tH4sIADiCD1wCAzM0AANtIyMDMwNzYwNDcwAgTwtvEgAAADE2ZDY3NDRiNjljWZmExZTZlYWFhY2Y0NzAxMTIxYjNkCg==
   digital_out/
      enable_alarm = off

swt />
```

B.4 INSTALACIÓN DE CERTIFICADOS PARA GESTIÓN HTTPS

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

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

1- Acceder al apartado de configuración de la interfaz web a través del puerto SRV ("**cd /admin/web**")

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

3- Cargar una **clave privada** válida en "**privatekey**" con el comando "**upload privatekey raw**".
El procedimiento es idéntico al indicado para la carga del certificado.

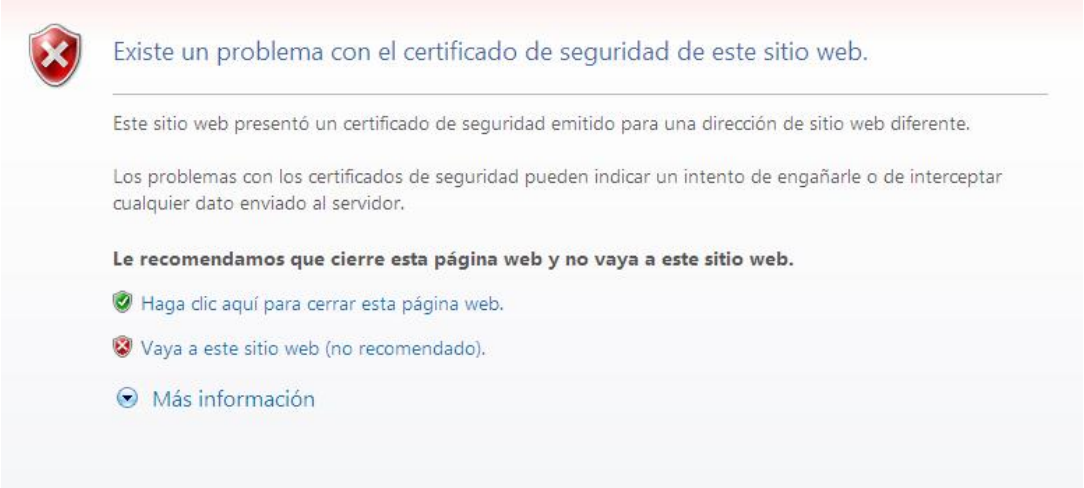
4- Introducir la **contraseña de la clave privada** en "**privatekeypwd**" con el comando "**set privatekeypwd**".
Se pedirá confirmación de la misma dos veces.

5- Activar en el equipo el acceso mediante HTTPS ("**set https on**")

6- Solicitar la activación de los cambios ("**apply**")

7- Almacenar los nuevos datos (opcional) ("**save**")

8- **Cargar** la página web de configuración del equipo en un navegador (Microsoft Internet Explorer, Mozilla Firefox, etc. Google Chrome no está soportado) [1] usando el prefijo "**https://**", en lugar de http://".
Aparecerá el mensaje siguiente:



Dicho mensaje es una advertencia porque el certificado no ha sido validado por una entidad de confianza, pero el certificado funciona correctamente.
Seleccionar "**Vaya a este sitio web (no recomendado)**".
El control de acceso al equipo pide la introducción del nombre de usuario (***login***) y la contraseña asociada (***password***).

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

[1] La operación se ha comprobado satisfactoriamente con Microsoft Internet Explorer y Mozilla Firefox. Google Chrome no acepta los certificados autofirmados.

Ejemplo de download en un equipo que ya opere con HTTPS:

```
emr2 /> download
restore
set /main/hostname emr2
set /main/timezone Madrid
set /admin/web/https on
set       /admin/web/cert       "-----BEGIN       CERTIFICATE-----
\nMIICWzCCAcQCCQCcL+NbBdYynDANBgkqhkiG9w0BAQUFADByMQswCQYDVQQGEwJF\
nUzESMBAGA1UECBMJQmFyY2Vsb25hMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNV\n
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWDmouc2FsYXRA\ne
ml2LmVzMB4XDTEzMDMyNzE1NTAzOVoXDTE0MDMyNzE1NTAzOVowcjELMAkGA1UE\nBh
MCRVMxEjAQBgNVBAgTCUJhcmNlbG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww\nCgY
DVQQKEwNaSVYxDjAMBgNVBAMTBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh\nbGF0
QHppdi5lczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt49IfdfD/xVO\nGsqL2
17s6aumdFWr9NYoJw68LbrHY0VZ9OGwen+alXAjBcl2lqLZjf1lOh250aWE\neZLH31
lD5bxS9c+w8YrwXoWEnYOxUQpK49YGvH7DnqLAyI5ptyQbdyMoTkMcxBOZ\njNoToVi
oGiZ9GRBg6nKCDC4+PxN3/90CAwEAATANBgkqhkiG9w0BAQUFAAOBgQAT\n7QtOOJT6
lLcGciF4R5aooiRoZEiTJQBFm6PoTZ21apGGhF1Bz0FPn3LRxC1Mb6PI\nkNatYteCq
5FJNjGunF8hDIQVc1x7O2ju2vmGOiyVfSz1eqiy+Tx0dMYsgpBeY3K+\n8fb+J1jmLP
NzPhgMlzPK6VGNA70/QhfCG9l5xK1oWQ==\n-----END CERTIFICATE-----"
set   /admin/web/privatekey   "-----BEGIN   RSA   PRIVATE   KEY-----
\nMIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6z0Vav01ignDrwtusdjRVn04bB6\
nf5qVcCMFyXaWotmN/WU6HbnRpYR5ksffWUPlvFL1z7DxivBehYSdg7FRCkrj1ga8\n
fsOeosDIjmm3JBt3IyhOQxzEE5mM2hOhWKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB\nA
oGAOvDzYhVKhjodHlUzm3lbsZzAklKAKNorgn8kxbpYE/RM8mkV9f/Lb3jWhiEu\nxy
f7m7BmNMcex8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S\nApu
oZFYmh34uBl6SJkUdihCs4jM1ocQBQMHQ7mXe7Sk1sgECQQDgpSDx45vm8Yk+\nGoX4
UzcRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcNOpU8bFtQbWfxjkThHthQBN\nrUeER
Ej9AkEA0S4ernXQGVJGm7b6JhJXFKkILVYo5vP0C3jx7ByRIMt4lkll4l7Q\ntzNepK
jlcmimzLWuHJAiyTBtvzfVcnU4YQJAaXOaX3HkwSgosIpq0QLfGp7yJNQu\nqt5h+vZ
O6FTuSFPm3tOD4G0K6MlN0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7Wp\ns/lpJEDj
Pg/p+lkeHqvBLwdQZXldbM442rjnlAZBNzq01ZuWTEvUWcLG3fMt9iBN\nVq6G4cg+x
ZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1XSt5nxH8U2Zk1u7ZWZZhOTcw\nezG/TDLBWk
ROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==\n-----END RSA PRIVATE KEY------"
set /admin/web/privatekeypwd testhttps
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn gnftsg.com
set /wan/cell0/login pruebas_ziv1
set /wan/cell0/passwd pruebas_ziv1
set /snmp/enable on
set /access/tacacsplus/server1_ip 10.132.2.148
set /access/tacacsplus/server2_ip 10.132.2.168
set /access/tacacsplus/shared_key Sm4rt3Sy13
set /access/tacacsplus/admin_lvl 15
set /access/web/method tacacsplus
```

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

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

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

Ejemplo de **certificado** válido:

```
-----BEGIN CERTIFICATE-----
MIICWzCCAcQCCQCcL+NbBdYynDANBgkqhkiG9w0BAQUFADByMQswCQYDVQQGEwJF
UzESMBAGA1UECBMJQmFyY2Vsb25hMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNV
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWDmouc2FsYXRA
eml2LmVzMB4XDTEzMDMyNzE1NTAzOVoXDTE0MDMyNzE1NTAzOVowcjELMAkGA1UE
BhMCRVMxEjAQBgNVBAgTCUJhcmNlbG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww
CgYDVQQKEwNaSVYxDjAMBgNVBAMTBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh
bGF0QHppdi5lczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt49IfdfD/xVO
GsqL217s6aumdFWr9NYoJw68LbrHY0VZ9OGwen+alXAjBcl2lqLZjf1lOh250aWE
eZLH31lD5bxS9c+w8YrwXoWEnYOxUQpK49YGvH7DnqLAyI5ptyQbdyMoTkMcxBOZ
jNoToVioGiZ9GRBg6nKCDC4+PxN3/90CAwEAATANBgkqhkiG9w0BAQUFAAOBgQAT
7QtOOJT6lLcGciF4R5aooiRoZEiTJQBFm6PoTZ21apGGhF1Bz0FPn3LRxC1Mb6PI
kNatYteCq5FJNjGunF8hDIQVc1x7O2ju2vmGOiyVfSz1eqiy+Tx0dMYsgpBeY3K+
8fb+J1jmLPNzPhgMlzPK6VGNA70/QhfCG9l5xK1oWQ==
-----END CERTIFICATE-----
```

Ejemplo de **clave privada** válida:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6Z0Vav01ignDrwtusdjRVn04bB6
f5qVcCMFyXaWotmN/WU6HbnRpYR5ksffWUPlvFL1z7DxivBehYSdg7FRCkrj1ga8
fsOeosDIjmm3JBt3IyhOQxzEE5mM2hOhWKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB
AoGAOvDzYhVKhjodHlUzm3lbsZzAklKAKNorgn8kxbpYE/RM8mkV9f/Lb3jWhiEu
xyf7m7BmNMcex8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S
ApuoZFYmh34uBl6SJkUdihCs4jM1ocQBQMHQ7mXe7Sk1sgECQQDgpSDx45vm8Yk+
GoX4UzcRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcNOpU8bFtQbWfxjkThHthQBN
rUeEREj9AkEA0S4ernXQGVJGm7b6JhJXFKkILVYo5vP0C3jx7ByRIMt4lkll4l7Q
tzNepKjlcmimzLWuHJAiyTBtvzfVcnU4YQJAaXOaX3HkwSgosIpq0QLfGp7yJNQu
qt5h+vZ06FTuSFPm3t0D4G0K6MlN0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7Wp
s/lpJEDjPg/p+lkeHqvBLwdQZXldbM442rjnlAZBNzq01ZuWTEvUWcLG3fMt9iBN
Vq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1XSt5nxH8U2Zk1u7ZWZZhOTcw
ezG/TDLBWkROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==
-----END RSA PRIVATE KEY-----
```