Conceptronic

CB100S24S y CB100S48S

Manual de usuario

Índice

ESPAÑOL

Preámbulo

El Manual de usuario del *CB100S24S / CB100S48S* está dividido en apartados que describen el proceso de instalación del sistema y las instrucciones de funcionamiento con ejemplos.

Apartado 1: Introducción
Describe el switch y sus características.

Apartado 2: Instalación
Ayuda a iniciar el proceso de instalación básica del switch y también describe el panel frontal, el panel trasero, los paneles laterales y los indicadores LED del switch.

Apartado 3: Conectar el switch
Describe cómo puede conectarse el switch a su red Ethernet/Fast Ethernet.

Apartado 4: Introducción a la administración del switch
Expone las características básicas de la administración del switch, incluida la protección con contraseña, las opciones SNMP, la asignación de la dirección IP y la conexión de dispositivos al switch.

Apartado 5: Introducción a la administración del switch basada en web
Trata sobre la conexión y el uso de la administración del switch basada en web del dispositivo.

Apartado 6: Administración
Descripción detallada de la configuración de las funciones básicas del switch, incluida la dirección IP, la Configuración de los puertos, las Cuentas de usuario, la Replicación de puertos, los Servicios TFTP, los Servicios de imagen múltiple y los Envíos y filtros.

Apartado 7: Características de Capa 2
Descripción de las características de Capa 2 del switch, incluyendo VLANs, Enlaces troncales, Control IGMP y Árbol de expansión.

Apartado 8: Clase de Servicio (CoS)
Descripción de las características de Clase de Servicio (CoS) del switch, incluyendo Prioridad predeterminada (802.1p) y Prioridad de usuario (802.1p).

Apartado 9: Seguridad
Descripción de las funciones de seguridad del switch, incluyendo SSH, 802.1X.

Apartado 10: Control
Incluye información de control, como la Dirección MAC, el Grupo de Control IGMP, Explorar los puertos del router y Control de acceso a los puertos.

Apartado 11: Mantenimiento
Información sobre utilidades del switch como Restablecer el sistema, Reiniciar el sistema, Guardar los cambios y Cerrar sesión.

Apéndice A: Especificaciones técnicas
Especificaciones técnicas de los sistemas CB100S24S y CB100S48S.

Apéndice B: Entradas de registro del sistema
Información sobre las Entradas de registro del sistema.

Apéndice C: Longitudes de los cables
Información sobre los tipos de cables y las distancias máximas.

Apéndice D: Glosario
Lista de definiciones de los términos utilizados en este manual.

Lectores objetivo

El *Manual de Usuario del CB100S24S / CB100S48S* contiene información acerca de la configuración y la administración del switch. Se utilizará el término "switch" para referirse a ambos dispositivos. Este manual está dirigido a administradores de redes que estén familiarizados con los conceptos y la terminología relacionados con la administración de redes.

Convenciones tipográficas

Convención	Descripción
[ ]	En una línea de comandos, los corchetes indican una entrada opcional. Por ejemplo: [copiar nombre del archivo] significa que de forma opcional puede introducir "copiar" seguido del nombre del archivo. No introduzca los corchetes.
Negrita	Hace referencia a un botón, icono de la barra de herramientas, menú o elemento del menú. Por ejemplo: Abra el menú **Archivo** y seleccione **Cancelar**. La negrita se utiliza para enfatizar. Asimismo, puede emplearse para mensajes del sistema o indicaciones que aparecen en pantalla. Por ejemplo: Tiene un mensaje de correo. La fuente en negrita se utiliza también para indicar nombres de archivos, nombres de programas y comandos. Por ejemplo: Utilice el comando de copia.
Fuente de máquina de escribir en negrita	Indica comandos y respuestas a indicaciones que deben introducirse exactamente como está indicado en el manual.
Inicial en mayúsculas	Indica el nombre de una ventana. El nombre de las teclas del teclado se escribe con la letra inicial en mayúscula. Por ejemplo: Haga clic en Enter.
Cursiva	Indica el nombre de la ventana o de un campo. También se refiere a una variable o parámetro sustituido por una palabra o secuencia adecuadas. Por ejemplo: Introduzca *nombre del archivo* significa que deberá introducir el propio nombre del archivo en lugar de la palabra que aparece en cursiva.
Nombre del menú > Opción del menú	**Nombre del menú > Opción del menú** indica la estructura del menú. **Dispositivo > Puerto > Propiedades del puerto** indica la opción del menú de Propiedades del puerto, en la opción del menú de los puertos, ubicada en el menú del dispositivo.

Notas, avisos y precauciones

Una **NOTA** ofrece información importante que ayuda a hacer un mejor uso del dispositivo.

Un **AVISO** advierte sobre posibles daños en el hardware o pérdida de datos, e indica cómo evitar el problema.

Una **PRECAUCIÓN** advierte sobre posibles daños materiales, lesiones corporales o peligros mortales.

Instrucciones de seguridad

Siga las directrices de seguridad siguientes para garantizar su propia seguridad y ayudar a proteger el sistema contra posibles daños. En todo el documento se utiliza el icono de precaución (⚠) para indicar las precauciones que deben tenerse en cuenta y respetarse.

Precauciones de seguridad

Para reducir el peligro de lesiones, descarga eléctrica, incendio y daños en el equipo, tenga en cuenta las precauciones siguientes:

- Cumpla y siga las indicaciones de mantenimiento.
  - No realice tareas de mantenimiento del producto, salvo cuando lo indique la documentación del sistema.
  - Abrir o retirar tapas que llevan impreso un símbolo triangular con un rayo puede exponerle a una descarga eléctrica.
  - Las tareas de mantenimiento de componentes del producto deben realizarse por parte de un técnico de mantenimiento cualificado.

- En caso de que se produzca alguna de las situaciones siguientes, desenchufe el producto de la toma de corriente eléctrica y sustituya la pieza, o bien póngase en contacto con un técnico de mantenimiento cualificado:
  - El cable de alimentación, el cable de extensión o el enchufe están dañados.
  - Un objeto ha caído en el producto.
  - El producto ha estado expuesto al agua.
  - El producto se ha golpeado o se ha dañado.
  - El producto no funciona correctamente cuando sigue las instrucciones de funcionamiento.

- Mantenga el sistema alejado de radiadores y fuentes de calor. No bloquee las zonas de ventilación.
- Evite el contacto de los componentes del sistema con alimentos o líquidos, y no utilice nunca el producto en entornos húmedos. En caso de que el sistema se moje, consulte el apartado correspondiente de la guía de resolución de problemas o póngase en contacto con un técnico de mantenimiento cualificado.
- No introduzca objetos en las aberturas del sistema, ya que podría provocar que se origine un incendio o se produzca una descarga eléctrica por el cortocircuito de los componentes internos.
- Utilice el producto únicamente con equipos autorizados.
- Deje que el producto se enfríe antes de retirar las tapas o tocar los componentes internos.
- Utilice el producto únicamente con el tipo de fuente de alimentación externa que indica la etiqueta de clasificaciones eléctricas. Si no está seguro del tipo de fuente de alimentación necesaria, consulte a un técnico de mantenimiento o a su compañía eléctrica.

- Asimismo, asegúrese de que los dispositivos conectados pertenecen a la clasificación eléctrica para poder utilizarse con la alimentación disponible en su ubicación.
- Utilice únicamente cables de alimentación autorizados. En caso de que no disponga de un cable de alimentación adecuado para su sistema o para cualquier opción que funcione con corriente AC apta para su sistema, compre un cable de alimentación cuyo uso está autorizado en su país. El cable de alimentación debe ser apto para el producto y para el voltaje y la corriente indicada en la etiqueta de clasificaciones eléctricas del producto. El voltaje y la clasificación de corriente del cable debe ser mayor que la clasificación que indica el producto.
- Para evitar riesgos de descarga eléctrica, enchufe el sistema y los cables de alimentación periféricos en tomas eléctricas de tierra adecuadas. Estos cables tienen enchufes de tres puntas que contribuyen a una correcta conexión a tierra. No utilice enchufes adaptadores ni retire la punta de conexión a tierra del cable. En caso de necesidad de un cable de extensión, utilice un cable trifilar con enchufes con conexión a tierra.
- Tenga en cuenta el amperaje de los cables de extensión y de las toma de corriente múltiple. Asegúrese de que el amperaje total de todos los productos enchufados en los cables de extensión o tomas de corriente múltiple no supera el 80% del amperaje límite de dichos cables de extensión o tomas de corriente múltiple.
- Para proteger su sistema contra subidas y bajadas de tensión repentinas y momentáneas, utilice un regulador de voltaje, un acondicionador de línea o un sistema de alimentación ininterrumpida (SAI).

ESPAÑOL

- Coloque los cables del sistema y de alimentación con cuidado de tal manera que no puedan pisarse ni provoquen caídas. Asegúrese de que no se coloca ningún objeto encima de los cables.
- No altere los cables de alimentación ni los enchufes. Consulte con un electricista cualificado o con su compañía eléctrica en caso de modificaciones del emplazamiento. Respete siempre las normativas local y nacional relativas a instalaciones eléctricas.
- Al conectar y desconectar la corriente de tomas de conexión directa, siga las directrices siguientes en caso de que su sistema lo permita:
    - Instale la fuente de alimentación antes de conectar el cable de alimentación.
    - Desenchufe el cable de alimentación antes de retirar la fuente de alimentación.
    - En caso de que el sistema esté equipado con diversas fuentes de alimentación, desconecte el sistema de la alimentación desenchufando los cables de alimentación de las tomas de corriente.

- Mueva el producto con cuidado y asegúrese de que todas las ruedecitas y/o estabilizadores están acoplados firmemente al sistema. Evite paradas repentinas y superficies que no sean uniformes.

Precauciones generales para productos que pueden montarse en un rack

Tenga en cuenta las precauciones siguientes relativas a la estabilidad y la seguridad del rack. Asimismo, consulte el documento de instalación de racks que incluye el sistema y el rack para conocer los procedimientos y precauciones específicas:

- Los sistemas se consideran componentes de un rack. Por tanto, el término "componente" significa cualquier sistema y los diversos elementos periféricos o de apoyo.
- Antes de operar con el rack, compruebe que los estabilizadores están instalados de forma segura en el rack, y que todo el peso de este último descansa sobre el suelo. Instale los estabilizadores frontal y lateral en un rack individual o los estabilizadores frontales en varios racks acoplados antes de operar en el rack.
- Cargue siempre el rack empezando por la parte de abajo y siguiendo hacia arriba, y cargue en primer lugar el elemento más pesado.
- Compruebe que el rack está nivelado y estable antes de instalar un componente.
- Preste atención cuando presione los pestillos del riel del componente y lo coloque en el rack, ya que podría atraparse los dedos.
- Una vez que haya introducido un componente en el rack, coloque el riel con cuidado en posición de bloqueo.
- No sobrecargue el circuito derivado de corriente AC que alimenta el rack. La resistencia total del rack no debe superar el 80% de la capacidad del circuito derivado.
- Asegúrese de que los componentes instalados en el rack disponen de una ventilación adecuada.
- No camine ni permanezca de pie sobre los componentes durante las tareas de mantenimiento de otros componentes instalados en el rack.

NOTA: Todas las conexiones a tomas de alimentación DC y conexiones a tierra de seguridad deben realizarse por electricistas cualificados. Las instalaciones eléctricas deben cumplir con la normativa y las prácticas aplicables locales, regionales y nacionales.

PRECAUCIÓN: Nunca elimine el conductor a tierra ni trabaje con el equipo en ausencia de un conductor a tierra instalado correctamente. Póngase en contacto con la autoridad de supervisión eléctrica correspondiente o con un electricista en caso de duda sobre la idoneidad de la conexión a tierra.

PRECAUCIÓN: La estructura del sistema debe estar bien fijada a la estructura del rack. No intente conectar el sistema a la fuente de alimentación hasta que los cables conductores a tierra no estén conectados. Un electricista cualificado deberá encargarse de supervisar el cableado a tierra de seguridad. Si se omite o se desconecta el cable a tierra de seguridad podría producirse una situación de riesgo eléctrico.

PRECAUCIÓN: No reponga las pilas con un tipo de pilas diferente. Hay riesgo de explosión si coloca un tipo de pila de litio incorrecto. Deseche las pilas agotadas de acuerdo con las instrucciones.

Protección contra descargas de electricidad estáticas

La electricidad estática puede dañar los componentes delicados de su sistema. Para evitar estos daños, descargue la electricidad estática de su cuerpo antes de tocar cualquier elemento electrónico, como un microprocesador. Para ello, puede tocar la superficie metálica no pintada de la estructura cada cierto tiempo.

Asimismo, siga los pasos siguientes para evitar los daños que puede provocar una descarga de electricidad estática:

1. Cuando desembale un componente sensible a la electricidad estática de su caja de cartón, no retire el envase de material antiestático del componente hasta que vaya a instalar el componente en el sistema. Justo antes de desembalar el envase antiestático, asegúrese de descargar la electricidad estática de su cuerpo.
2. Cuando transporte un componente sensible a la electricidad estática, colóquelo en primer lugar en un envase antiestático.
3. Manipule todos los componentes sensible en zonas seguras libres de electricidad estática. En la medida de lo posible, utilice alfombras, bancos de trabajo y cintas de conexión a tierra antiestáticas.

Apartado 1

Introducción

- *Descripción del switch CB100S24S / CB100S48S*
- *Características*
- *Puertos*
- *Componentes del panel frontal*
- *Descripción del panel lateral*
- *Descripción del panel trasero*

CB100S24S / CB100S48S

Estos switches ofrecen un rendimiento inigualable, tolerancia a fallos, flexibilidad ajustada, seguridad robusta, interoperabilidad conforme a la normativa y una tecnología impresionante para implantar redes adaptables a futuros desarrollos en empresas y departamentos, con una ruta de migración muy sencilla.

El manual siguiente describe la instalación, el mantenimiento y las configuraciones relativas al CB100S24S y al CB100S48S. Estos switches son idénticos en cuanto a configuración y muy similares en el hardware básico y, por tanto, la mayor parte de la información que contiene este manual será universal en ambos switches. Las capturas de pantalla correspondientes al administrador web pueden tomarse de los dos switches, pero la configuración será idéntica, salvo en el caso de los puertos que varíen. En las próximas páginas de este documento, utilizaremos el CB100S48S como el switch en cuestión para ejemplos, capturas de pantalla, configuraciones y explicaciones.

Características

- Tabla de direcciones: compatible con direcciones MAC de hasta 8K por dispositivo.
- Tabla de direcciones: compatible con un máximo de 256 entradas MAC estáticas.
- Jumbo Frame: compatible con Frame con etiqueta: 2048 bytes, Frame sin etiqueta: 2044 bytes (máximo)
- Compatible con Control IGMP
- Control IGMP *Fast Leave*
- Conformidad con IEEE 802.1D STP
- IEEE 802.1w RSTP
- Compatible con enlaces troncales de puertos
- Compatible con Replicación de puertos
- VLANs IEEE 802.1Q
- Compatible con Grupos VLAN
- Colas de prioridad IEEE 802.1p
- Control de acceso basado en MAC y en puertos IEEE 802.1x
- Administración: administración basada en web
- Compatible con cliente BootP/DHCP
- Compatible con Imagen Dual y descripción de puertos
- Nivel de cuentas de usuario: nivel de usuario(lector) y nivel de administración (privilegio)

Puertos

La tabla siguiente enumera los puertos relativos presentes en cada switch, así como las características y la compatibilidad de cada tipo de puerto presente en los dispositivos CB100S24S y CB100S48S:

CB100S24S	**Descripción**
24 puertos 10/100BASE-T	Conformidad con los estándares siguientes: IEEE 802.3 IEEE 802.3u Compatibles con operaciones Half/Full-Duplex Todos los puertos son compatibles con auto MDI-X/MDI-II cruzado Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex, y prevención de bloqueo de cabeza de línea.
2 puertos Combo 1000Base-T/SFP	2 puertos Combo 1000Base-T/SFP Los puertos 1000BASE-T son conformes con los estándares siguientes: IEEE 802.3 IEEE 802.3u IEEE 802.3ab Compatibles con operaciones Full-Duplex Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex, y prevención de bloqueo de cabeza de línea. Transceptores SFP compatibles: 1000BASE-LX 1000BASE-SX Conformidad con los estándares siguientes: IEEE 802.3z IEEE 802.3u
2 puertos 1000Base-T	Puertos 1000BASE-T conformes con los estándares siguientes: IEEE 802.3 IEEE 802.3u IEEE 802.3ab Compatibles con operaciones Full-Duplex Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex, y prevención de bloqueo de cabeza de línea.
1 puerto consola DB-9 hembra DCE RS-232	DCE RS-232 DB-9 para recuperar los valores de fábrica.

CB100S48S	**Descripción**
48 puertos 10/100BASE-T	Conformidad con los estándares siguientes: IEEE 802.3 IEEE 802.3u Compatibles con operaciones Half/Full-Duplex Todos los puertos son compatibles con auto MDI-X/MDI-II cruzado Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex, y prevención de bloqueo de cabeza de línea.
2 puertos Combo 1000Base-T/SFP	2 puertos Combo 1000BASE-T/SFP Los puertos 1000BASE-T son conformes con los estándares siguientes: IEEE 802.3 IEEE 802.3u IEEE 802.3ab Compatibles con operaciones Full-Duplex Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex, y prevención de bloqueo de cabeza de línea. Transceptores SFP compatibles: 1000BASE-LX 1000BASE-SX Conformidad con los estándares siguientes: IEEE 802.3z IEEE 802.3u
2 puertos 1000Base-T	Los puertos 1000BASE-T son conformes con los estándares siguientes: IEEE 802.3 IEEE 802.3u IEEE 802.3ab Compatibles con operaciones Full-Duplex Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex, y prevención de bloqueo de cabeza de línea.
1 puerto consola DB-9 hembra DCE RS-232	DCE RS-232 DB-9 para recuperar los valores de fábrica.

NOTA: Los puertos Combo SFP del switch no pueden utilizarse simultáneamente con los puertos correspondientes 1000BASE-T. Si los dos puertos se están utilizando al mismo tiempo (por ejemplo, el puerto 25 del SFP y el puerto 25 del 1000BASE-T), los puertos SFP tendrán prioridad sobre los puertos Combo y dejarán inoperativos a los puertos 1000BASE-T.

Componentes del panel frontal

CB100S24S

- 24 puertos BASE-T de 10/100Mbps
- 2 puertos Combo 1000BASE-T/SFP, ubicados en la parte derecha
- 2 puertos 1000BASE-T, ubicados en la parte derecha
- 1 puerto consola DB-9 hembra DCE RS-232
- LEDs para encendido y consola Link/Act/Velocidad para cada puerto

Figura 1- 1. Panel frontal del CB100S24S

CB100S48S

- 48 puertos BASE-T de 10/100Mbps
- 2 puertos Combo 1000BASE-T/SFP, ubicados en la parte derecha
- 2 puertos 1000BASE-T, ubicados en la parte derecha
- 1 puerto consola DB-9 hembra DCE RS-232
- LEDs para encendido y consola Link/Act/Velocidad para cada puerto

Figura 1- 2. Panel frontal del CB100S48S

LEDs

En la tabla siguiente se enumeran los LEDs y su descripción correspondiente:

Ubicación	LED indicativo	Color	Estado	Descripción
En cada dispositivo	**Encendido**	Verde	Luz fija	Encendido
			Apagado	Apagado
	Consola	Verde	Luz fija	Consola encendida
			Parpadeo	POST funcionando / error del POST
			Apagado	Consola apagada
LED de cada puerto de 10/100 Mbps	**Link/Act/Velocidad**	Verde/Ámbar	Verde fijo	Cuando hay una conexión segura Fast Ethernet de 100Mbps (o enlace) en alguno de los puertos.
			Parpadeo verde	Cuando hay recepción o transmisión (por ej., Actividad—Act) de datos en un puerto conectado a Fast Ethernet.
			Ámbar fijo	Cuando hay una conexión segura Ethernet de 10Mbps (o enlace) en alguno de los puertos.
			Parpadeo ámbar	Cuando hay recepción o transmisión (por ej., Actividad—Act) de datos en un puerto conectado a Ethernet.
			Apagado	No hay enlace
LED de cada puerto GE	**Modo Link/Act/Velocidad para los puertos 1000BASE-T**	Verde/Ámbar	Verde fijo	Cuando hay una conexión segura de 1000Mbps (o enlace) en alguno de los puertos.
			Parpadeo verde	Cuando hay recepción o transmisión (por ej., Actividad—Act) de datos en un puerto conectado a 1000Mbps.
			Ámbar fijo	Cuando hay una conexión segura Fast Ethernet de 10/100Mbps (o enlace) en alguno de los puertos.
			Parpadeo ámbar	Cuando hay recepción o transmisión (por ej., Actividad—Act) de datos en un puerto conectado a Fast Ethernet.
			Apagado	No hay enlace
	Modo Link/Act/Velocidad para los puertos SFP	Verde/Ámbar	Verde fijo	Cuando hay una conexión segura de 1000Mbps (o enlace) en alguno de los puertos.
			Parpadeo verde	Cuando hay recepción o transmisión (por ej., Actividad—Act) de datos en un puerto conectado a 1000Mbps.
			Ámbar fijo	Cuando hay una conexión segura de 100Mbps (o enlace) en alguno de los puertos.
			Parpadeo ámbar	Cuando hay recepción o transmisión (por ej., Actividad—Act) de datos en los puertos.
			Apagado	No hay enlace

Instalación de los puertos SFP

Estos switches están equipados con puertos SFP (Small Form Factor Portable), que pueden utilizarse con cableado de fibra óptica del transceptor para realizar enlaces ascendentes con otros dispositivos de red y obtener un enlace gigabit capaz de abarcar grandes distancias. Estos puertos SFP son compatibles con transmisiones full-duplex, tienen autonegociación y pueden utilizarse con los transceptores siguientes: INFINEON / V23818-K15-B57((1000BASE-LX) -- 1310nm; INFINEON / V23818-K305-B57(1000BASE-SX) -- 850nm; Finisar / FTRJ-1319-7D

(1000BASE-LX) -- 1310nm; CORETEK OPTO CT-0155TSP-MB5L(modo individual: 100BASE-FX) y CT-0155NSP-MB2L (modo múltiple: 100BASE-FX) -- 1310nm. Consulte la ilustración siguiente para instalar los puertos SFP en el switch:

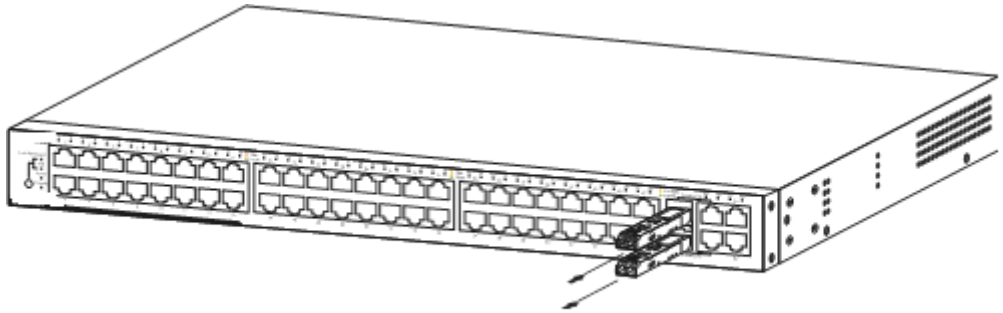


Figura 1- 3. Introducción de los transceptores de fibra óptica en el switch

Apartado 2

Instalación

Contenido del paquete

Abra la caja de cartón del switch y desembale con cuidado su contenido. El paquete debe incluir los elementos siguientes:

- Smart switch de 10/100Mbps y 24/48 puertos de Conceptronic
- Cable de alimentación AC
- Cable de la consola DCE RS-232
- Kit de montaje del switch (2 soportes con tornillos)
- 4 peanas de goma de fijación del producto
- CD-ROM del producto
- Esta guía de instalación rápida

En caso de que falte algún elemento o presente daños, póngase en contacto con el distribuidor más cercano para proceder a su devolución.

Antes de conectar el switch a la red

El lugar donde instale el switch puede afectar en gran medida al rendimiento del dispositivo. Siga las directrices siguientes a la hora de configurar el switch.

- Instale el switch en una superficie horizontal sólida con una resistencia de al menos 4,24 kg (9,35 libras) de peso. No coloque objetos pesados encima del switch.
- La toma de corriente debe estar situada a una distancia de 1,82 metros (6 pies) del switch.
- Examine visualmente el cable de corriente y compruebe que está completamente protegido con un puerto de corriente AC/DC.
- Compruebe que el lugar donde está instalado el switch cuenta con la evacuación de calor y la ventilación adecuadas. Deje al menos un espacio de 10 cm (4 pulgadas) por delante y por detrás del dispositivo para favorecer la ventilación.
- Instale el switch en un lugar fresco y seco dentro del rango de temperatura y humedad aceptables para el funcionamiento del dispositivo.
- Instale el switch en un lugar donde no haya potentes generadores de campos electromagnéticos (como motores), vibraciones, polvo y no expuesto a la luz directa del sol.
- Cuando instale el switch en una superficie horizontal, adhiera las peanas en las cuatro esquinas de la parte inferior del dispositivo. De este modo protegerá la carcasa del switch contra arañazos y evitará que el dispositivo arañe la superficie.

Instalación del switch sin un rack

Cuando instale el switch en un escritorio o en un estante, en primer lugar deberá colocar y adherir las peanas de goma que incluye el producto en la parte inferior de cada esquina del dispositivo. Deje suficiente espacio de ventilación entre el switch y los demás objetos en torno al mismo.

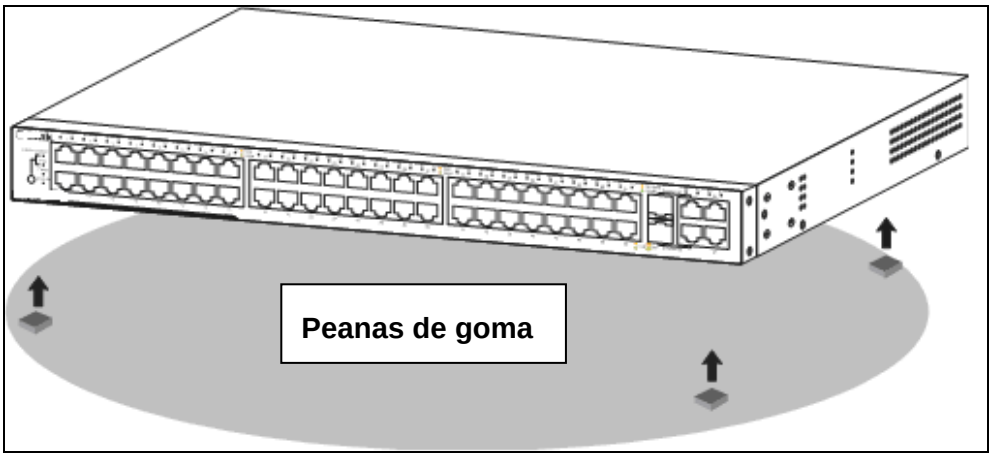


Figura 2 - 1. Preparación del switch para su instalación en un escritorio o en un estante

Instalación del switch en un rack

El switch puede instalarse en un rack estándar de 19". Consulte la ilustración siguiente a modo de orientación.

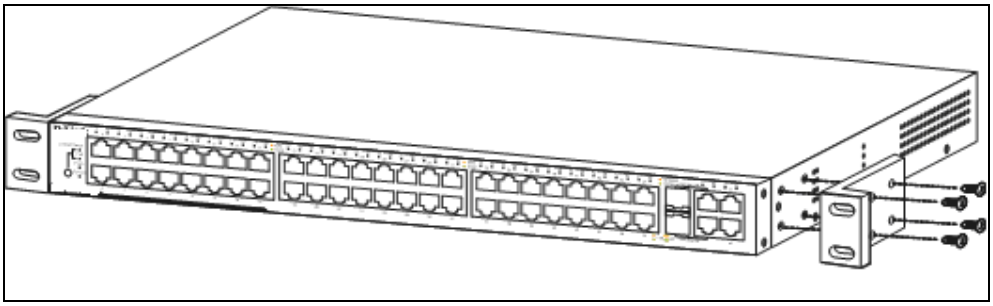


Figura 2 - 2. Ajuste de los soportes de instalación al switch

Ajuste los soportes de fijación al switch utilizando los tornillos que incluye el producto. Una vez fijados los soportes de forma segura, podrá montar el switch en un rack estándar tal y como muestra la ilustración siguiente.

Instalación del switch en un rack estándar de 19"

ATENCIÓN: Instalar sistemas en un rack sin haber montado primero los estabilizadores frontal y lateral podría hacer que el rack volcase y provocar lesiones en determinadas situaciones. Por tanto, monte siempre los estabilizadores antes de instalar componentes en un rack. Una vez instalados los componentes, no saque del rack más de un componente al mismo tiempo por las juntas deslizantes. El peso de varios componentes de grandes dimensiones podría hacer que el rack volcase y provocar lesiones.

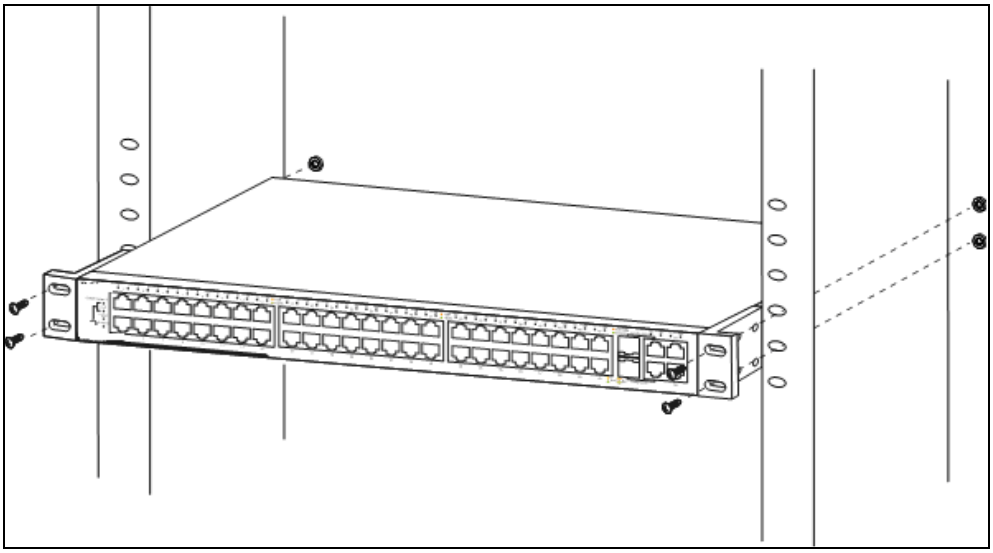


Figura 2 - 3. Instalación del switch en un rack

Encendido mediante alimentación AC

Enchufe un extremo del cable de alimentación AC en un conector de alimentación del switch y el otro extremo, en la toma de alimentación local.

Una vez encendido el switch, los LEDs parpadearán unos segundos, lo cual indica que el sistema se está reiniciando.

Corte de corriente

Como precaución para las fuentes de alimentación AC, desenchufe el switch en caso de que se produzca un corte de corriente. Una vez recuperada la corriente, vuelva a enchufarlo.

ATENCIÓN: Instalar sistemas en un rack sin haber montado primero los estabilizadores frontal y lateral podría hacer que el rack volcase y provocar lesiones en determinadas situaciones. Por tanto, monte siempre los estabilizadores antes de instalar componentes en un rack. Una vez instalados los componentes, no saque del rack más de un componente al mismo tiempo por las juntas deslizantes. El peso de varios componentes de grandes dimensiones podría hacer que el rack volcase y provocar lesiones.

.

Apartado 3

Conectar el switch

- *Conectar el nodo final al switch*
- *Conexión a un hub o a otro switch*
- *Conexión a una red troncal o servidor de la red*

NOTA: Todos los puertos Ethernet N-Way de 10/100/1000Mbps son compatibles con las conexiones MDI-II y MDI-X.

Conexión del nodo final al switch

Entre los nodos finales se incluyen PCs equipados con una tarjeta de interfaz de red (NIC) RJ 45 Ethernet/Fast Ethernet de 10, 100 o 1000 Mbps y la mayoría de routers. Un nodo final puede conectarse al switch mediante un cable UTP/STP de par trenzado de categoría 3, 4 o 5. El nodo final debe conectarse a cualquiera de los puertos del switch.

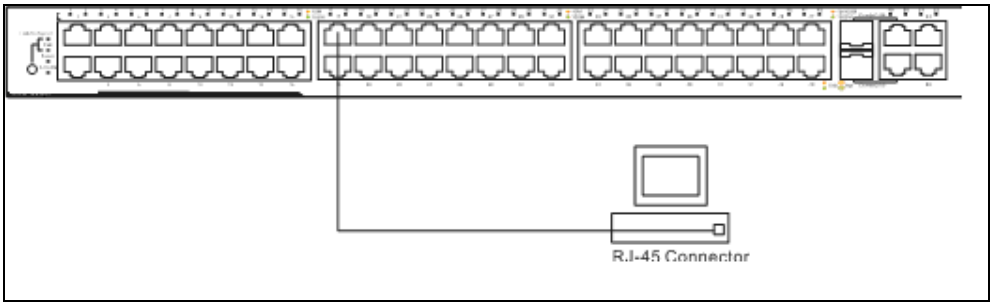


Figura 3- 1. Switch conectado a un nodo final

Los LEDs Link/Act de cada puerto UTP se encenderán de color verde o ámbar cuando el enlace sea válido. Si el LED parpadea indicará que hay actividad en ese puerto.

Conexión a un hub o a otro switch

Pueden llevarse a cabo las conexiones siguientes de diversas maneras utilizando un cable normal.

- Un hub o switch 10BASE-T puede conectarse al switch mediante un cable UTP/STP de par trenzado de categoría 3, 4 o 5.
- Un hub o switch 100BASE-TX puede conectarse al switch mediante un cable UTP/STP de par trenzado de categoría 5.
- Un switch 1000BASE-T puede conectarse al switch mediante un cable UTP/STP de par trenzado de categoría 5e.
- Un switch compatible con enlaces ascendentes de fibra óptica puede conectarse a los puertos SFP del switch mediante cableado de fibra óptica.

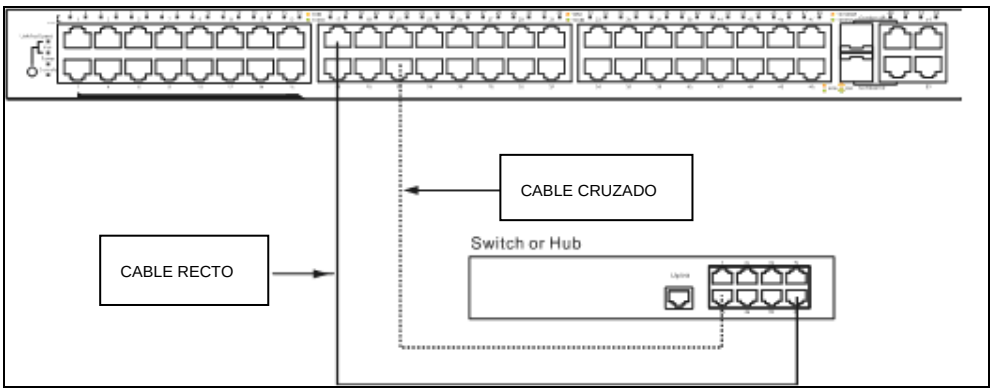


Figura 3- 2. Switch conectado a un puerto normal (de enlace no ascendente) de un hub o switch utilizando un cable recto o cruzado

AVISO: Cuando el transceptor SFP incorpore un enlace, el puerto 10/100/1000BASE-T asociado integrado quedará desactivado.

Apartado 4

Introducción a la administración del switch

- *Opciones de administración*
- *Interfaz de administración basada en web*
- *Administrar las cuentas de usuario*
- *Interfaz de línea de comando a través del puerto en serie*
- *Conectar el puerto de la consola (RS-232 DCE)*
- *Primera conexión al switch*
- *Protección con contraseña*
- *Asignación de la Dirección IP*

Opciones de administración

Este sistema puede gestionarse mediante la administración basada en web, a la que se puede acceder con un navegador web.

Interfaz de administración basada en web

Una vez instalado correctamente el switch, podrá proceder a configurarlo, controlar el panel de LEDs y visualizar datos estadísticos gráficamente mediante un navegador web, como Netscape Navigator (versión 6.2.3 y superior) o Microsoft® Internet Explorer (versión 6.0).

Conectar el puerto de la consola (DCE RS-232 DB-9)

El switch incorpora un puerto en serie RS-232 que permite conectar el dispositivo a un ordenador o a un terminal para recuperar los valores de fábrica. Este puerto es un conector hembra DB-9, instalado como conexión de un equipo terminal de datos.

Para utilizar el puerto de la consola necesitará los elementos siguientes:

- Un terminal o un ordenador con un puerto en serie y capacidad para emular un terminal.
- Un módem nulo o un cable RS-232 cruzado con un conector hembra DB-9 para el puerto de la consola del switch.

Para conectar un terminal al puerto de la consola:

1. Conecte el conector hembra del cable RS-232 directamente al puerto de la consola del switch y apriete los tornillos cautivos de retención.
2. Conecte el otro extremo del cable a un terminal o al conector en serie de un ordenador equipado con software de emulación de terminales. Configure dicho software tal y como se indica a continuación:
3. Seleccione el puerto en serie adecuado (puerto COM 1 o puerto COM 2).
4. Ajuste la velocidad de transferencia de datos a **9600 baudios**.
5. Ajuste el formato de datos a **8 bits de datos**, **1 bits de parada** y **sin paridad**.
6. Ajuste el control de flujo a **ninguno**.
7. En **Propiedades**, seleccione **VT100** para el modo Emulación.
8. Seleccione las teclas de **Terminal** para las teclas de **Función**, **Flechas** y **Ctrl**. Compruebe que selecciona las teclas de Terminal (no teclas de Windows).

NOTA: Cuando utilice HyperTerminal con el sistema operativo Microsoft® Windows® 2000, asegúrese de que tiene instalado Windows 2000 Service Pack 2 o una versión posterior. Windows 2000 Service Pack 2 le permitirá utilizar las teclas de flecha en la emulación VT100 de HyperTerminal. Consulte la página www.microsoft.com para obtener información sobre los service packs de Windows 2000.

9. Una vez configurado el terminal correctamente, enchufe el cable de alimentación en la toma de alimentación de la parte trasera del switch. La secuencia de arranque aparecerá en el terminal.
10. Cuando termine la secuencia de arranque, aparecerá la pantalla de inicio de sesión de la consola.
11. Si ha iniciado sesión en el programa de la Interfaz de Línea de Comando (CLI), pulse la tecla **Enter** que aparece en los mensajes de Nombre de usuario y Contraseña. El switch no tiene nombre de usuario y contraseña predefinidos, sino que el administrador debe crearlos en primer lugar. Si ya ha configurado cuentas de usuario, inicie sesión y continúe configurando el switch.
12. Cuando haya finalizado las tareas que deba realizar, cierre la sesión con el comando correspondiente o cierre el programa de emulación.
13. Asegúrese de que el terminal o PC que está utilizando para realizar esta conexión está configurado de acuerdo con estas opciones.

Si tiene problemas a la hora de realizar esta conexión en su PC, compruebe que la emulación está en VT-100. Para ajustar la emulación, haga clic en el menú **Archivo** de la ventana HyperTerminal, haga clic en **Propiedades** del menú desplegable y finalmente haga clic en la pestaña **Opciones**. Aquí encontrará las opciones de **Emulación**. Si sigue sin ver nada, trate de reiniciar el switch desconectándolo de la fuente de alimentación.

Una vez conectado a la consola, en la pantalla de la consola aparecerá la información siguiente. Aquí es donde el usuario deberá introducir los comandos para utilizar las funciones de administración disponibles. El switch solicitará al usuario que introduzca un nombre de usuario y una contraseña. En la conexión inicial no hay ni nombre de usuario ni contraseña, de manera que sólo deberá pulsar **Enter** dos veces para acceder a la interfaz de línea de comando.

Figura 4- 1. Pantalla inicial tras la primera conexión

Primera conexión al switch

El switch incorpora seguridad basada en el usuario que le permite, si lo desea, impedir que usuarios no autorizados tengan acceso al switch o modifiquen su configuración. Esta sección le explica cómo iniciar sesión en el dispositivo.

NOTA: La contraseña utilizada para acceder al switch distingue entre mayúsculas y minúsculas. Por tanto, "S" no es lo mismo que "s".

La primera vez que se conecte al switch verá la primera pantalla de inicio de sesión.

NOTA: Pulse Ctrl+R para actualizar la pantalla. Este comando puede utilizarse en cualquier momento para hacer que el programa de la consola del switch actualice la pantalla de la consola.

Pulse **Enter** en los campos de Nombre de usuario y Contraseña. A continuación, tendrá acceso al mensaje de comando **CB100S48S:1#** que se muestra a continuación:

No hay un nombre de usuario o contraseña inicial, de manera que deberá dejar en blanco estos campos.

Interfaz de línea de comando del Switch Fast Ethernet CB100S48S

Firmware: Build 1.00-B11

Copyright (C) 2008, 2L International B.V. Reservados todos los derechos.

Nombre de usuario:

Contraseña:

CB100S48S:1#

Figura 4- 2. Mensaje de comando

Apartado 5

Configuración del switch basada en web

Introducción

Todas las funciones de software del switch pueden administrarse, configurarse y controlarse a través de una interfaz incrustada basada en web (HTML). El switch puede administrarse desde estaciones remotas de cualquier punto de la red mediante un navegador estándar, como Opera, Netscape Navigator/Communicator o Microsoft Internet Explorer. El navegador actúa como herramienta de acceso universal y puede comunicarse directamente con el switch mediante el protocolo HTTP.

Acceso al Administrador web

Para empezar a utilizar el switch, sólo tiene que ejecutar el navegador que ha instalado en su ordenador y dirigirlo hacia la dirección IP que ha definido para el dispositivo. La URL de la barra de direcciones será http://123.123.123.123, en la que los números 123 representan la dirección IP del switch.

NOTA: La dirección IP predeterminada del switch es 192.168.0.200

Seguidamente, se abrirá la ventana de autenticación del usuario del módulo de administración, tal y como se indica a continuación.

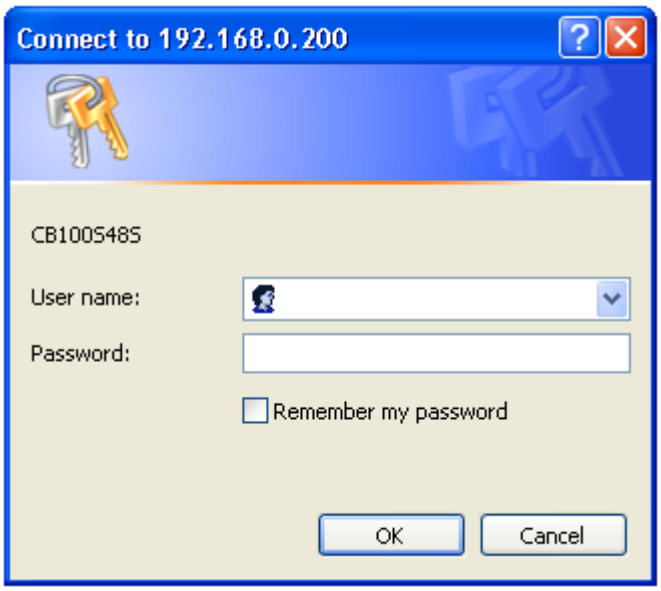


Figura 5- 1. Cuadro de diálogo con contraseña de acceso

ESPAÑOL

Como no hay ni nombre de usuario ni contraseña predeterminados, haga clic en **Aceptar** y accederá a la interfaz de usuario basada en web. A continuación se explican las características de administración del switch que ofrece el administrador basado en web.

Interfaz de usuario basada en web

Mediante la interfaz de usuario se accede a varias ventanas de administración y configuración del switch que le permiten visualizar datos estadísticos de rendimiento y controlar gráficamente el estado del sistema.

Áreas de la interfaz de usuario

La figura siguiente muestra la interfaz de usuario, que está dividida en tres áreas diferentes, tal y como describe la tabla.

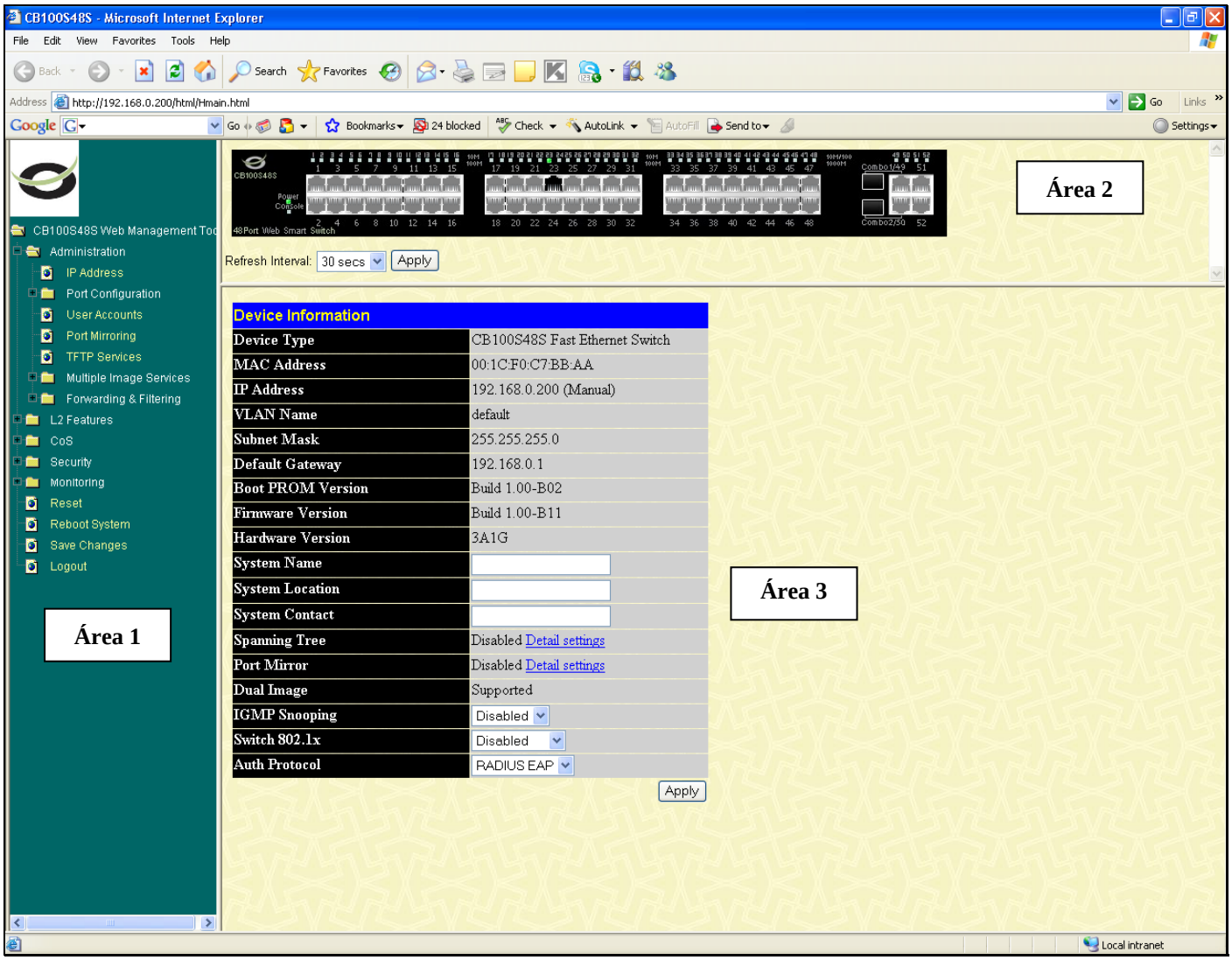


Figura 5- 2. Página principal del Administrador web

Área	Función
Área 1	Seleccione la carpeta o la ventana que desea mostrar. Los iconos de las carpetas pueden abrirse para mostrar los botones y subcarpetas de la ventana enlazada que contienen. Haga clic en el logotipo de 2L International B.V. para ir al sitio web de la empresa.
Área 2	Presenta una imagen gráfica casi en tiempo real del panel frontal del switch. Esta área muestra los puertos y los módulos de expansión del switch, con la actividad de los puertos, el modo duplex o el control de flujo, dependiendo del modo especificado. Pueden seleccionarse diversas áreas del gráfico para las funciones de administración del

	rendimiento, incluida la configuración de los puertos.
Área 3	Presenta información del switch basada en la selección del usuario y en la entrada de los datos de configuración.

AVISO: Los cambios que se realicen en la configuración del switch durante la sesión actual deben guardarse en el menú web **Guardar cambios** (explicado más abajo).

Páginas web

Cuando conecte el modo de administración del switch con un navegador web, aparecerá una ventana de inicio de sesión. Introduzca su nombre de usuario y su contraseña para acceder al modo de administración del switch.

A continuación se enumera una lista y la descripción de las carpetas principales disponibles en la interfaz web:

Administración
Contiene ventanas acerca de la configuración de las funciones básicas del switch, incluida la Dirección IP, la Configuración de los puertos, las Cuentas de usuario, la Replicación de puertos, los Servicios TFTP, los Servicios de imagen múltiple y Envíos y filtros.

Características de Capa 2
Contiene ventanas acerca de las características de Capa 2 del switch, incluyendo VLANs, Enlaces troncales, Control IGMP y Árbol de expansión.

Clase de Servicio (CoS)
Contiene ventanas acerca de la Prioridad predeterminada (802.1p) y la Prioridad de usuario (802.1p).

Seguridad
Contiene ventanas para 802.1x.

Control
Contiene ventanas acerca de la Dirección MAC, el Registro del switch, el Grupo de Control IGMP, Explorar los puertos del router y el Control de acceso a los puertos.

Mantenimiento del switch
Contiene información acerca de Restablecer el sistema, Reiniciar el sistema, Guardar los cambios y Cerrar sesión.

NOTA: Asegúrese de configurar el nombre de usuario y la contraseña en la ventana de Cuentas de usuario antes de conectar el switch a una red más grande.

Apartado 6

Administración

- *Dirección IP*
- *Configuración de los puertos*
- *Cuentas de usuario*
- *Replicación de puertos*
- *Servicios TFTP*
- *Servicios de imagen múltiple*
- *Envíos y filtros*

Información acerca del dispositivo

Esta ventana contiene las opciones principales de las funciones más importantes del switch y aparece automáticamente cuando el usuario inicia sesión. Para volver a la ventana de **Información acerca del dispositivo**, haga clic en la carpeta **Herramienta de administración web del CB 100S48S**. La ventana de **Información acerca del dispositivo** muestra la **Dirección MAC** (asignada de fábrica y sin posibilidad de cambio), el **PROM de arranque**, la **Versión del firmware** y la **Versión del hardware** del switch. Esta información es útil para mantener un registro de las actualizaciones del PROM y del firmware y para obtener la dirección MAC del switch para acceder a la tabla de direcciones de otro dispositivo de red en caso necesario. El usuario, a su discreción, también puede introducir un **Nombre del sistema**, **Ubicación del sistema** y **Contacto del sistema** para añadir más detalles para definir el switch. Asimismo, esta ventana muestra el estado de la funciones del switch para evaluar rápidamente su estado global actual. Algunas funciones están enlazadas con su ventana de configuración para facilitar el acceso desde la ventana de **Información acerca del dispositivo**.

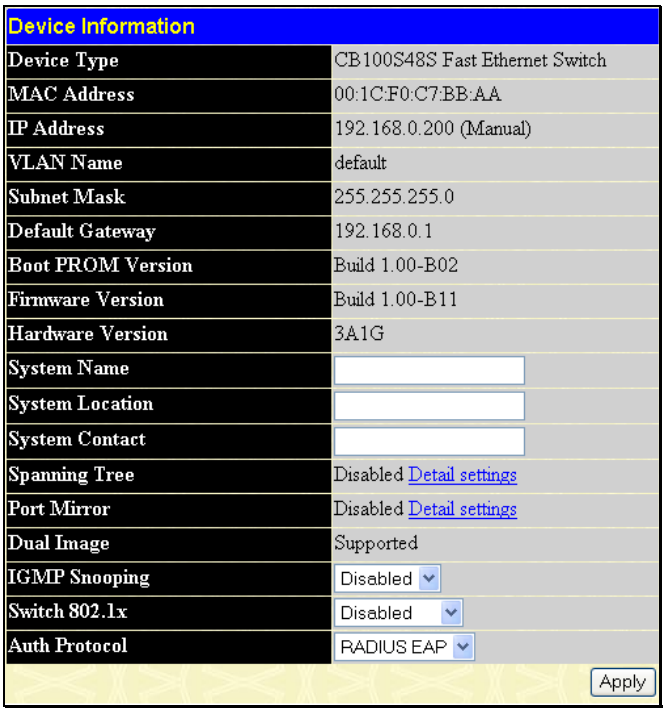


Figura 6- 1. Ventana de Información acerca del dispositivo

A continuación se describen los campos que pueden configurarse:

Parámetro	Descripción
Nombre del sistema	Si lo desea, introduzca un nombre de sistema para el switch. Este nombre lo identificará en la red del switch.

Ubicación del sistema	Si lo desea, introduzca un nombre para la ubicación del switch.
Contacto del sistema	Si lo desea, introduzca un nombre de contacto del switch.
Control IGMP	Para activar la función Control IGMP para todo el sistema, seleccione *Activado*, ya que el Control IGMP está *Desactivado* por defecto. Al activar el Control IGMP, podrá especificar el uso único de un router multicast (véase más abajo). Para configurar el Control IGMP para VLANs individuales, utilice la ventana **Control IGMP**, ubicada en la carpeta **Control IGMP**, que se encuentra en la carpeta **Características de Capa 2**.
802.1x del switch	La Dirección MAC puede activarse por los puertos o por la función 802.1x del switch; por defecto está *desactivada*. Este campo debe activarse para visualizar y configurar determinadas ventanas para 802.1x. Encontrará más información acerca de 802.1x, sus funciones y su implementación más adelante en la carpeta **802.1x** 頁 : 19 situada en la carpeta **Seguridad**. La función 802.1x basada en los puertos especifica que los puertos configurados para 802.1x se inician basándose únicamente en el número de puertos y están sujetos a los parámetros de autorización configurados. La autorización basada en MAC especifica que los puertos configurados para 802.1x se inician basándose en el número de puertos y en la dirección MAC del ordenador que se está autorizando, y están sujetos a los parámetros de autorización configurados.
Protocolo de autorización	頁 : 19 Hay dos opciones en este menú desplegable: RADIUS EAP y Local, lo cual determina qué función de autorización se asignará a 802.1x.

Haga clic en **Aplicar** para aplicar los cambios realizados.

Dirección IP

La dirección IP puede configurarse mediante el administrador web. Para ello, acceda a la ventana de la **Dirección IP** ubicada en la carpeta **Administración**.

Para configurar la dirección IP del switch:

Abra la carpeta **Administración** y haga clic en el enlace de la **Dirección IP**. El administrador web mostrará las opciones IP actuales del switch en la ventana de la **Dirección IP**, tal y como aparece a continuación.

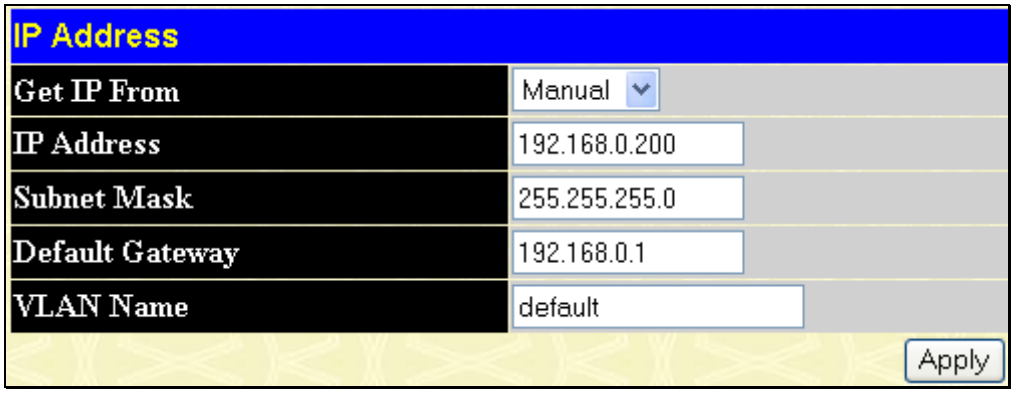


Figura 6- 2. Ventana de configuración de la Dirección IP

Para asignar manualmente al switch la dirección IP, la máscara de subred y la dirección de la puerta de enlace predeterminada:

1. Seleccione *Manual* en el menú desplegable Obtener IP.
2. Introduzca la dirección IP y la máscara de subred correspondientes.

3. Si desea acceder al switch desde una subred diferente a la que tiene instalada, introduzca la dirección IP de la puerta de enlace predeterminada. Si gestiona el switch desde la subred que el switch tiene instalada, puede dejar la dirección predeterminada (0.0.0.0) de este campo.
4. Si no ha configurado ninguna VLAN en el switch, puede utilizar el Nombre de la VLAN *predeterminada*. La *VLAN predeterminada* contiene todos los puertos del switch como miembros. Si ya ha configurado VLANs en el switch, deberá introducir el *Nombre de* la *VLAN* de la que contiene el puerto conectado a la estación de administración que accederá al switch, y éste permitirá el acceso a la administración desde estaciones con el mismo VID.

NOTA: La dirección IP predeterminada del switch es 192.168.0.200, con la máscara de subred 255.255.255.0 y la puerta de enlace predeterminada 192.168.0.1.

Para utilizar los protocolos BOOTP o DHCP para asignar al switch una dirección IP, la máscara de subred y la dirección de la puerta de enlace predeterminada:

Utilice el menú desplegable Obtener IP para elegir entre *BOOTP* o *DHCP*. De este modo seleccionará el modo en que asignará una dirección IP al switch la próxima vez que lo reinicie.

A continuación se enumeran las opciones de configuración de la Dirección IP:

Parámetro	Descripción
BOOTP	El switch enviará una solicitud BOOTP cuando se encienda. El protocolo BOOTP permite asignar direcciones IP, máscaras de subred y puertas de enlace predeterminadas mediante un servidor BOOTP central. Si esta opción está activa, el switch buscará un servidor BOOTP para proporcionarle esta información antes de usar la configuración predeterminada o introducida previamente.
DHCP	El switch enviará una solicitud DHCP cuando se encienda. El protocolo DHCP permite asignar direcciones IP, máscaras de subred y puertas de enlace predeterminadas mediante un servidor DHCP. Si esta opción está activa, el switch buscará un servidor DHCP para proporcionarle esta información antes de usar la configuración predeterminada o introducida previamente.
Manual	Permite introducir una dirección IP, la máscara de subred y una puerta de enlace predeterminada para el switch. Estos campos deben ajustarse al formato siguiente: xxx.xxx.xxx.xxx, donde cada xxx es un número (representado en forma decimal) entre 0 y 255. Esta dirección debe ser única y exclusiva en la red asignada que utilizará el administrador de dicha red.
Máscara de subred	Máscara de bits que determina el alcance de la subred en la que está el switch. Debe ajustarse al formato xxx.xxx.xxx.xxx, donde cada xxx es un número (representado en forma decimal) entre 0 y 255. El valor debe ser 255.0.0.0 para las redes de clase A, 255.255.0.0 para las redes de clase B, y 255.255.255.0 para las redes de clase C, aunque pueden configurarse máscaras de subred personalizadas.
Puerta de enlace predeterminada	Dirección IP que determina a dónde deben enviarse los paquetes con una dirección de destino fuera de la subred actual. Normalmente se trata de la dirección de un router o de un host que actúa como una puerta de enlace IP. Si su red no forma parte de una intranet o no desea que se pueda acceder al switch desde fuera de su red local, puede dejar intacto este campo y no aplicar cambios.
Nombre de la VLAN	Permite asignar un nombre a la VLAN desde el que una estación de administración podrá gestionar el switch mediante TCP/IP (en banda a través del administrador web). En caso de que no se haya configurado ninguna VLAN para el switch, la VLAN predeterminada contiene todos los puertos del switch. Todas las estaciones de administración que pueden conectarse al switch pueden acceder al switch hasta que se especifique una VLAN de administración.

Haga clic en **Aplicar** para que los cambios se hagan efectivos.

Configuración de los puertos

Esta sección contiene información para configurar los diversos atributos y propiedades de los puertos físicos individuales, incluida la velocidad de los puertos y el control de flujo.

Opciones de los puertos

Haga clic en **Administración** > **Configuración de los puertos > Opciones de los puertos** para mostrar la ventana siguiente:

Para configurar los puertos del switch:

1. Elija el puerto o el rango secuencial de los puertos utilizando los menús desplegables de los puertos De… A….

Utilice los menús desplegables restantes para configurar los parámetros descritos a continuación:

Port Configuration

From	To	State	Speed/Duplex	Flow Control	Medium Type	Apply
Port 1	Port 1	Enabled	Auto	Disabled	Copper	Apply

The Port Information Table

Port	State	Speed/Duplex	Flow Control	Connection/Duplex/FlowCtrl	Learning
1	Enabled	Auto	Disabled	LinkDown	Enabled
2	Enabled	Auto	Disabled	LinkDown	Enabled
3	Enabled	Auto	Disabled	LinkDown	Enabled
4	Enabled	Auto	Disabled	LinkDown	Enabled
5	Enabled	Auto	Disabled	LinkDown	Enabled
6	Enabled	Auto	Disabled	LinkDown	Enabled
7	Enabled	Auto	Disabled	LinkDown	Enabled
8	Enabled	Auto	Disabled	LinkDown	Enabled
9	Enabled	Auto	Disabled	LinkDown	Enabled
10	Enabled	Auto	Disabled	LinkDown	Enabled
11	Enabled	Auto	Disabled	LinkDown	Enabled
12	Enabled	Auto	Disabled	LinkDown	Enabled
13	Enabled	Auto	Disabled	LinkDown	Enabled
14	Enabled	Auto	Disabled	LinkDown	Enabled
15	Enabled	Auto	Disabled	LinkDown	Enabled
16	Enabled	Auto	Disabled	LinkDown	Enabled
17	Enabled	Auto	Disabled	LinkDown	Enabled
18	Enabled	Auto	Disabled	LinkDown	Enabled
19	Enabled	Auto	Disabled	LinkDown	Enabled
20	Enabled	Auto	Disabled	LinkDown	Enabled
21	Enabled	Auto	Disabled	LinkDown	Enabled
22	Enabled	Auto	Disabled	LinkDown	Enabled
23	Enabled	Auto	Disabled	100M/Full/None	Enabled
24	Enabled	Auto	Disabled	LinkDown	Enabled
25	Enabled	Auto	Disabled	LinkDown	Enabled
26	Enabled	Auto	Disabled	LinkDown	Enabled
27	Enabled	Auto	Disabled	LinkDown	Enabled
28	Enabled	Auto	Disabled	LinkDown	Enabled
29	Enabled	Auto	Disabled	LinkDown	Enabled
30	Enabled	Auto	Disabled	LinkDown	Enabled
31	Enabled	Auto	Disabled	LinkDown	Enabled
32	Enabled	Auto	Disabled	LinkDown	Enabled
33	Enabled	Auto	Disabled	LinkDown	Enabled
34	Enabled	Auto	Disabled	LinkDown	Enabled
35	Enabled	Auto	Disabled	LinkDown	Enabled
36	Enabled	Auto	Disabled	LinkDown	Enabled
37	Enabled	Auto	Disabled	LinkDown	Enabled
38	Enabled	Auto	Disabled	LinkDown	Enabled
39	Enabled	Auto	Disabled	LinkDown	Enabled
40	Enabled	Auto	Disabled	LinkDown	Enabled
41	Enabled	Auto	Disabled	LinkDown	Enabled
42	Enabled	Auto	Disabled	LinkDown	Enabled
43	Enabled	Auto	Disabled	LinkDown	Enabled
44	Enabled	Auto	Disabled	LinkDown	Enabled
45	Enabled	Auto	Disabled	LinkDown	Enabled
46	Enabled	Auto	Disabled	LinkDown	Enabled
47	Enabled	Auto	Disabled	LinkDown	Enabled
48	Enabled	Auto	Disabled	LinkDown	Enabled
49(C)	Enabled	Auto	Disabled	LinkDown	Enabled
49(F)	Enabled	Auto	Disabled	LinkDown	Enabled
50(C)	Enabled	Auto	Disabled	LinkDown	Enabled
50(F)	Enabled	Auto	Disabled	LinkDown	Enabled
51	Enabled	Auto	Disabled	LinkDown	Enabled
52	Enabled	Auto	Disabled	LinkDown	Enabled

Figura 6- 3. Ventana de Configuración de los puertos

Pueden configurarse los parámetros siguientes:

Parámetro	Descripción
De… A…	Utilice los menús desplegables para seleccionar el puerto o el rango de puertos que desea configurar.
Estado	Utilice este campo para activar o desactivar un puerto determinado o grupo de puertos.
Velocidad/Duplex	Utilice el campo **Velocidad/Duplex** para seleccionar la velocidad y el estado duplex/half-duplex del puerto. *Auto* indica autonegociación entre dispositivos de 10 y 100 Mbps, en full-duplex o half-duplex. La opción *Auto* permite que el puerto determine automáticamente las opciones más rápidas que puede soportar el dispositivo al que el puerto está conectado, y que utilice dichas opciones. Las demás opciones son *Auto*, *10M/Half*, *10M/Full, 100M/Half* y *100M/Full*, *1000M/Full_M* y *1000M/Full_S*. No hay un ajuste automático de la configuración de los puertos con opciones que no sean *Auto*. El switch permite al usuario configurar dos tipos de conexiones gigabit: *1000M/Full_M* y *1000M/Full_S*. Las conexiones gigabit sólo son compatibles con conexiones full duplex y pueden adoptar algunas características diferentes de otras elecciones enumeradas. Los parámetros *1000M/Full_M* (maestro) y *1000M/Full_S* (esclavo) se refieren a las conexiones con un cable 1000BASE-T para conectar a un puerto del switch otro dispositivo que pueda albergar una conexión gigabit. La opción de maestro (*1000M/Full_M)* permitirá al puerto tener capacidades relacionadas con el duplex, la velocidad y el tipo de capa física. Asimismo, la opción de maestro determinará la relación maestro-esclavo entre las dos capas físicas conectadas. Esta relación es necesaria para establecer el control de tiempo entre las dos capas físicas. El control de tiempo se ajusta en una capa física maestro mediante una fuente local. La opción de esclavo (*1000M/Full_S)* utiliza intervalos de bucles, en los que los intervalos proceden de una transmisión de datos procedentes del maestro. Si una conexión está configurada para *1000M/Full_M*, el otro extremo de la conexión debe estar configurado para *1000M/Full_S*. Cualquier otra configuración dará como resultado un estado de enlace descendente para ambos puertos.
Control de flujo	Muestra el estado del control de flujo utilizado para las configuraciones de los diversos puertos. Los puertos configurados para full-duplex utilizan el control de flujo 802.3x; los puertos half-duplex utilizan el control de flujo de contrapresión, y los puertos *Auto* emplean una selección automática de ambos. El estado por defecto es *Desactivado*.
Tipo de medio	Este parámetro es aplicable únicamente a los puertos Combo. En caso de configurar los puertos Combo, este parámetro define el tipo de medio de transporte utilizado. Los puertos SFP deben configurarse como *Fibra*, mientras que los puertos Combo 1000BASE-T deben configurarse como *Cobre*.

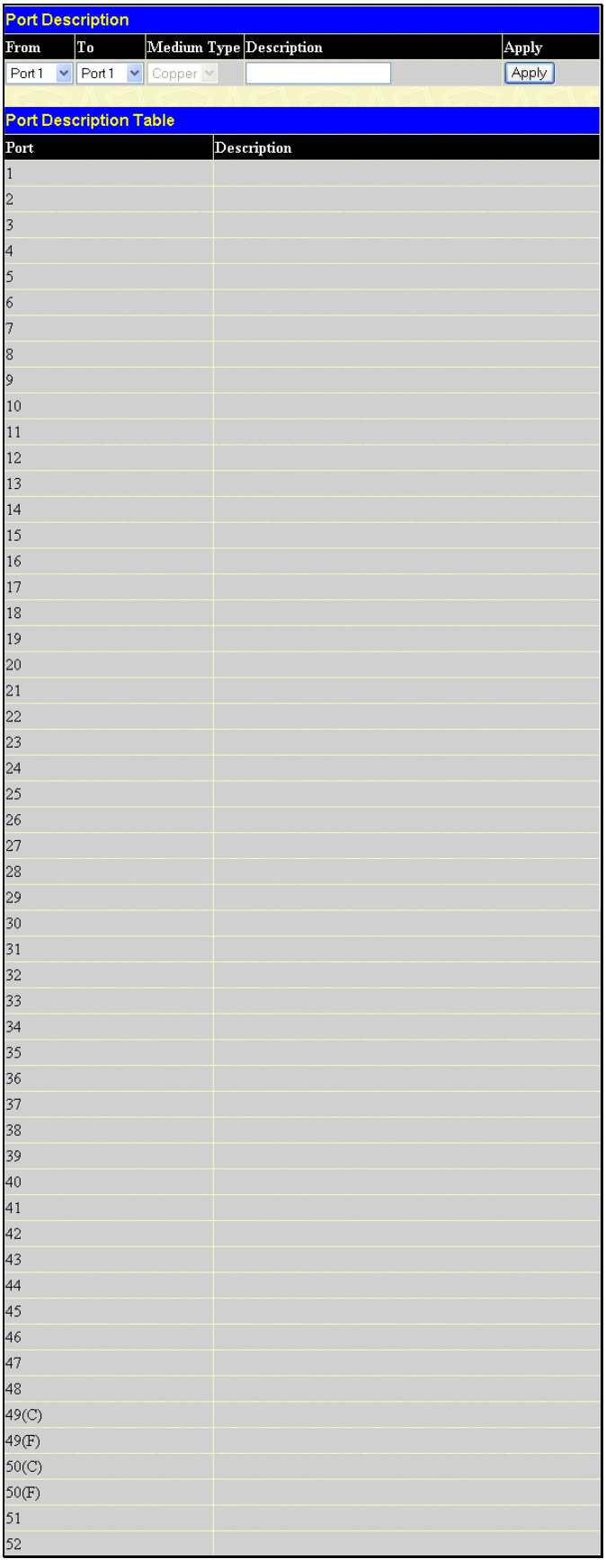
Haga clic en **Aplicar** para aplicar las nuevas opciones de configuración del switch.

Descripción de los puertos

El switch es compatible con una función de descripción de puertos con la que el usuario puede asignar un nombre a los diversos puertos del switch. Para ello, haga clic en **Administración** > **Configuración de los puertos** > **Descripción de los puertos** para visualizar la ventana siguiente:

Utilice los menús desplegables **De…** y **A…** para elegir el puerto o el rango de puertos que describirá, y a continuación, introduzca una descripción del puerto o puertos. Haga clic en **Aplicar** para configurar las descripciones en la **Tabla de descripción de los puertos**.

El **Tipo de medio** es aplicable únicamente a los puertos Combo. En caso de configurar los puertos Combo, este parámetro define el tipo de medio de transporte utilizado. Los puertos SFP deben configurarse como *Fibra*, mientras que los puertos Combo 1000BASE-T deben configurarse como *Cobre*. El resultado aparecerá en la ranura correspondiente del puerto del switch (**C** para los puertos Cobre y **F** para los puertos Fibra).



Port Description

From	To	Medium Type	Description	Apply
Port 1	Port 1	Copper		Apply

Port Description Table

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49(C)	
49(F)	
50(C)	
50(F)	
51	
52	

Figura 6- 4. Ventana de Descripción de los puertos

Cuentas de usuario

Utilice la ventana de **Administración de Cuentas de usuario** para controlar los privilegios del usuario. Para visualizar las Cuentas de usuario existentes, abra la carpeta **Administración** y haga clic en el enlace **Cuentas de usuario**. De este modo abrirá la ventana de **Administración de Cuentas de usuario**, tal y como aparece a continuación.

Figura 6- 5. Ventana de Cuentas de usuario

Para añadir un nuevo usuario, haga clic en el botón **Añadir**.

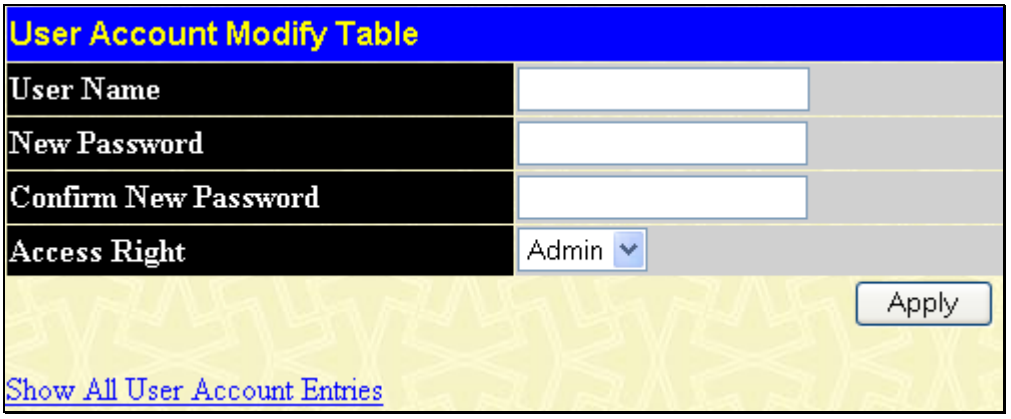


Figura 6- 6. Ventana de la Tabla para modificar las cuentas de usuario

Añada un nuevo usuario introduciendo un Nombre de usuario y una nueva Contraseña, y vuelva a introducir la misma contraseña en el campo Confirmar nueva contraseña. Elija el nivel de privilegio (*Administrador* o *Usuario)* en el menú desplegable Derecho de acceso.

Para modificar o eliminar un usuario existente, haga clic en el botón **Modificar** de ese usuario.

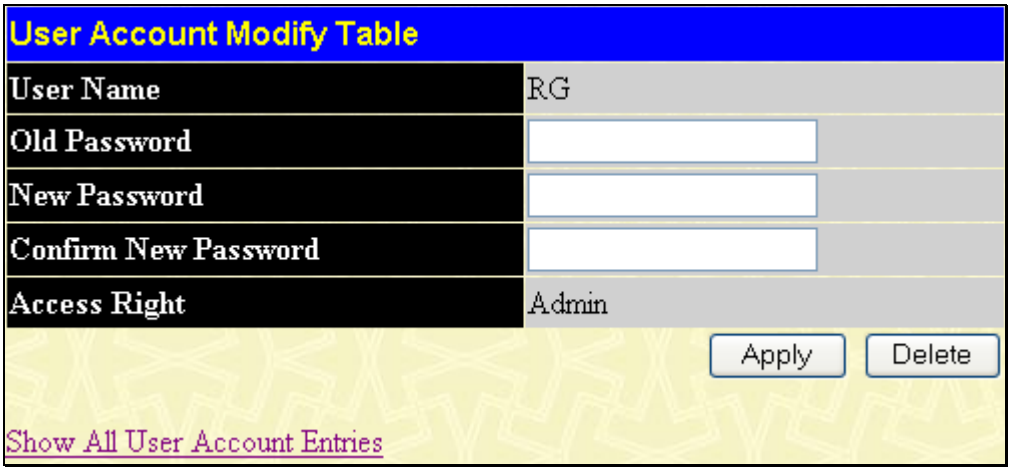


Figura 6- 7. Ventana de la Tabla para modificar las cuentas de usuario

Modifique o elimine una cuenta de usuario existente en la **Tabla para modificar las cuentas de usuario**. Para eliminar la cuenta de usuario, haga clic en el botón **Eliminar**. Para cambiar la contraseña, introduzca la nueva clave en el campo *Nueva contraseña* y vuelva a introducirla en el campo *Confirmar nueva contraseña*. El nivel de privilegio (*Administrador* o *Usuario*) puede verse en el campo **Derecho de acceso**.

Replicación de puertos

El switch le permite copiar frames transmitidos y recibidos en un puerto y redireccionar las copias a otro puerto. Puede conectar un dispositivo de control al puerto de replicación, como un sniffer o una sonda RMON, para ver los detalles sobre los paquetes que pasan por el primer puerto, útil para el control de redes y para la resolución de problemas. Para visualizar la ventana de **Replicación de puertos**, haga clic en **Replicación de puertos** en la carpeta **Administración**.

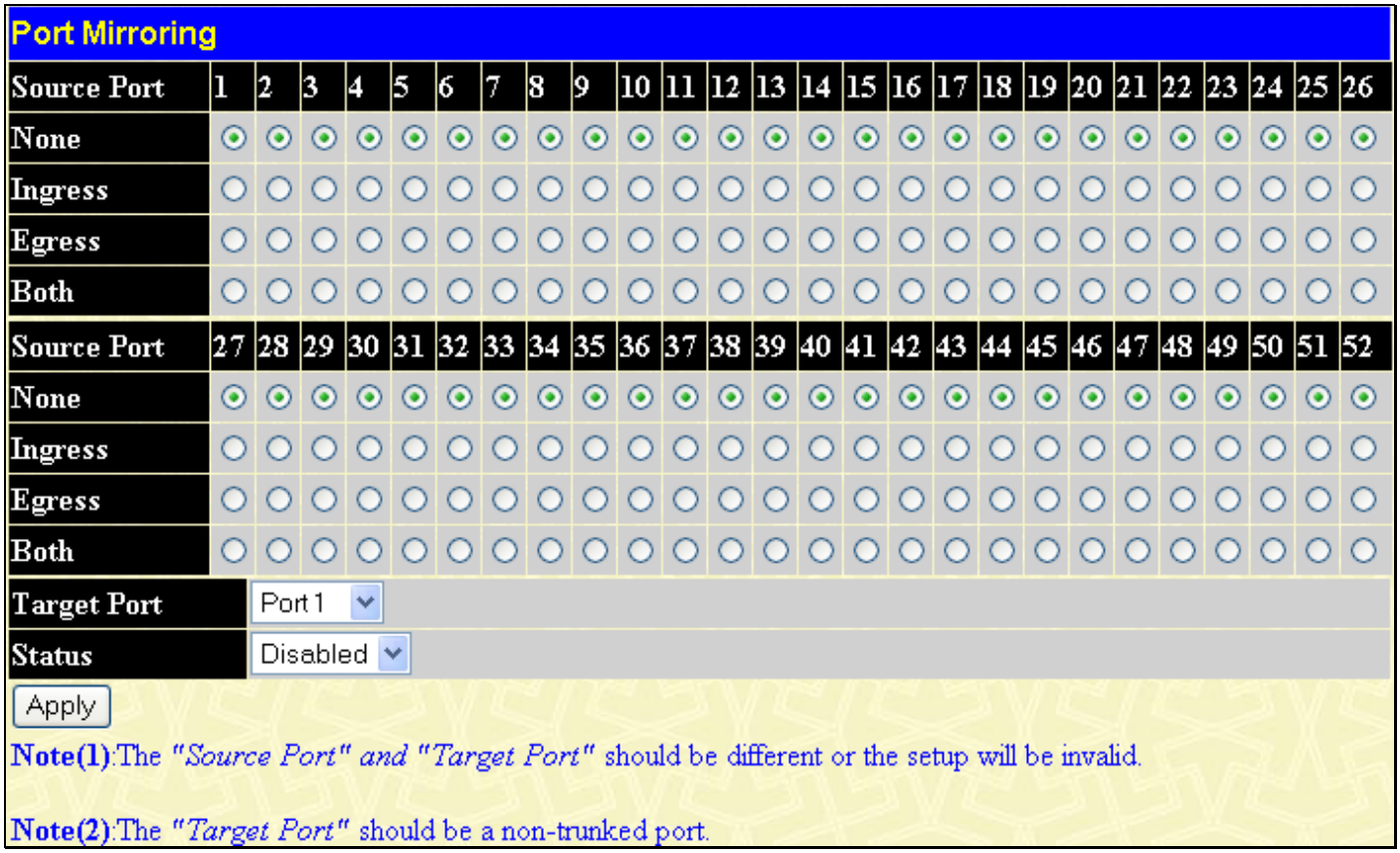


Figura 6- 8. Ventana de Replicación de puertos

Para configurar un puerto de replicación:

1. Seleccione el Puerto de origen del que desea copiar los frames y el Puerto de destino, es decir, el que recibe las copias del puerto de origen.
2. Seleccione la Dirección de origen, Entrada, Salida o Ambos, y ajuste el Estado en el menú desplegable a *Activado*.
3. Haga clic en **Aplicar** para que los cambios se hagan efectivos.

NOTA: Un puerto rápido no puede replicarse en un puerto más lento. Por ejemplo, si intenta replicar el tráfico de un puerto de 100 Mbps en un puerto de 10 Mbps, podrían producirse problemas de procesamiento. El puerto del que está copiando los frames siempre debe poder soportar una velocidad igual o inferior que el puerto al que está enviando las copias. Por otro lado, el puerto de destino de la replicación no puede ser miembro de un grupo de enlaces troncales. Recuerde que el puerto de destino y el puerto de origen no pueden ser el mismo puerto.

Servicios TFTP

Los servicios del Protocolo de Transferencia de Archivos Trivial (TFTP) permiten que el firmware del switch se actualice mediante la transferencia al switch de un nuevo archivo de firmware de un servidor TFTP. Asimismo, también puede cargarse un archivo de configuración de un servidor TFTP al switch. Las opciones de configuración del switch pueden guardarse en el servidor TFTP y puede cargarse un registro histórico del switch al servidor TFTP. El servidor TFTP debe estar equipado con un software de servidor TFTP para poder realizar la transferencia de archivos.

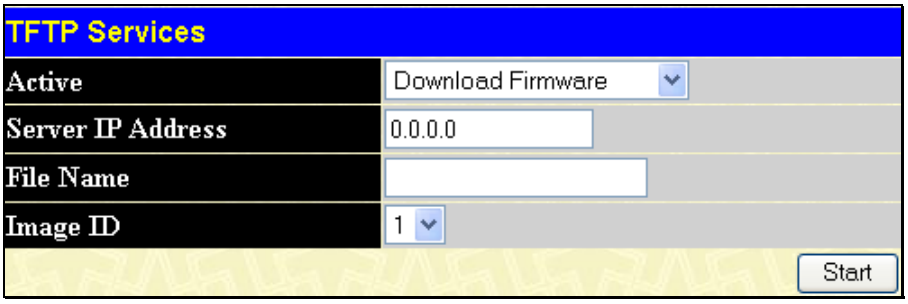


Figura 6- 9. Ventana de Servicios TFTP

El usuario también tiene la opción de transferir los archivos de firmware o de configuración a o desde una unidad flash interna ubicada en el switch. Utilizando esta ventana, el usuario puede añadir un archivo de firmware o de configuración de un servidor TFTP a una memoria flash, o transferir ese archivo de firmware o de configuración a un servidor TFTP. En el apartado siguiente (**Servicios de Archivos Flash**) encontrará más información acerca de la configuración de la unidad flash interna.

El software del servidor TFTP es una parte de los diversos paquetes de software de administración de red, como NetSight, y puede obtenerse por separado. Para actualizar el archivo de firmware o de configuración del switch, abra el hipervínculo **Servicios TFTP** ubicado en la carpeta **Administración**.

Pueden configurarse los parámetros siguientes:

Parámetro	Descripción
Activo	Seleccione un servicio para el servidor TFTP del menú desplegable: • *Descargar firmware*: Introduzca la dirección IP del servidor TFTP y especifique la ubicación del nuevo firmware en el servidor TFTP. Haga clic en **Inicio** para registrar la dirección IP del servidor TFTP e iniciar la transferencia del archivo. • *Descargar configuración*: Introduzca la dirección IP del servidor TFTP y la ruta y el nombre del archivo de configuración en el servidor TFTP. Haga clic en **Inicio** para registrar la dirección IP del servidor TFTP e iniciar la transferencia del archivo. • *Cargar configuración:* Introduzca la dirección IP del servidor TFTP y la ruta y el nombre del archivo de las opciones de configuración del switch en el servidor TFTP. Haga clic en **Inicio** para registrar la dirección IP del servidor TFTP e iniciar la transferencia del archivo.
Dirección IP del servidor	Introduzca la dirección IP del servidor desde el que desea descargar los archivos de firmware o de configuración.
Nombre del archivo	Introduzca la ruta y el nombre del archivo de firmware o de configuración que desea cargar o descargar, ubicado en el servidor TFTP.
ID de la imagen	Seleccione un archivo de firmware de una unidad flash interna a la que el archivo de firmware se transferirá.

Haga clic en **Inicio** para iniciar la transferencia de archivos.

Servicios de imagen múltiple

Para configurar los archivos ubicados en la memoria flash, utilice las ventanas siguientes a modo de orientación.

Información acerca del firmware

Esta ventana se utiliza para visualizar el arranque del firmware.

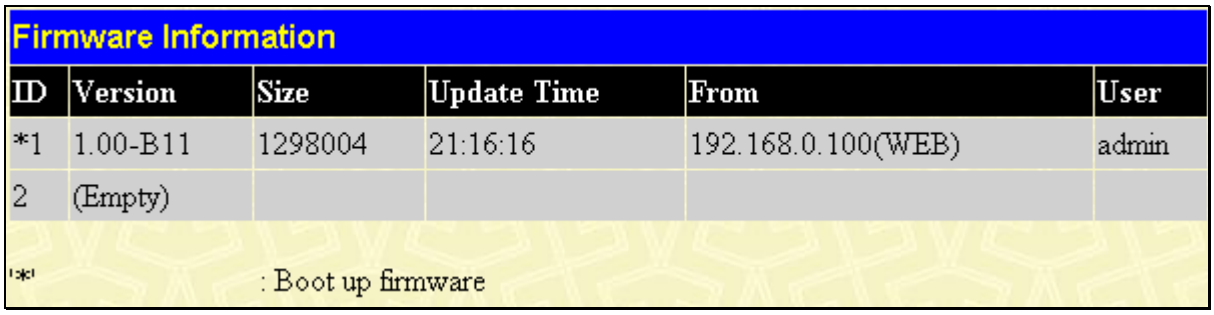


Figura 6- 10. Ventana de Información acerca del firmware

Configuración de la imagen del firmware

La ventana siguiente se utiliza para determinar cuál de las dos imágenes del firmware se empleará como archivo de arranque predeterminado. Asimismo, puede eliminar cualquiera de las dos imágenes.

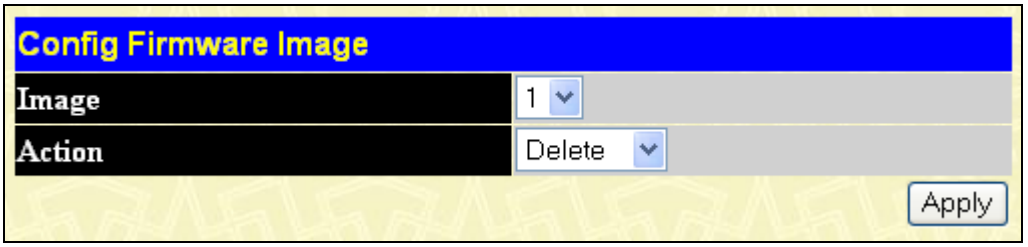


Figura 6- 11. Ventana de la Configuración de la imagen del firmware

Envíos y filtros

Envíos unicast

Abra la carpeta **Envíos y filtros** en el menú **Configuración** y haga clic en el enlace **Envíos unicast**. A continuación se abrirá la ventana siguiente:

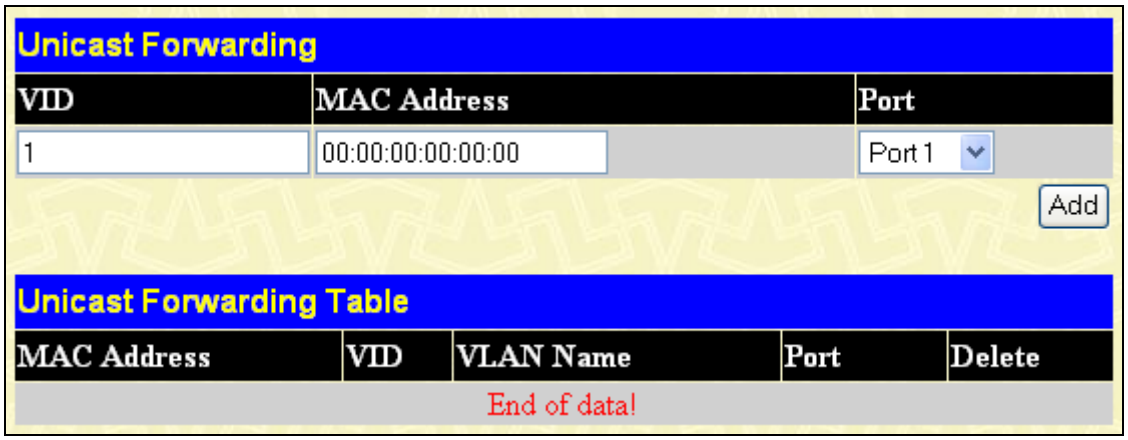


Figura 6- 12. Ventana de Envíos unicast

ESPAÑOL

Para añadir o editar una entrada, defina los parámetros siguientes y, a continuación, haga clic en **Añadir/Modificar**:

Parámetro	Descripción
VID	Número de identificación de la VLAN en el que radica la dirección MAC unicast expresada arriba.
Dirección MAC	Dirección MAC a la que los paquetes se enviarán de forma estática. Ésta debe ser una dirección MAC unicast.
Puerto	Permite seleccionar el número de puertos en el que radica la dirección MAC introducida arriba.

Haga clic en **Aplicar** para aplicar los cambios realizados. Para eliminar una entrada de la Tabla de Envíos unicast estáticos, haga clic en la *X* correspondiente debajo del título Eliminar.

Envíos multicast

La figura y la tabla siguientes describen cómo se configuran los **Envíos multicast** del switch. Abra la carpeta **Envíos y filtros** y haga clic en el enlace **Envíos multicast** para visualizar la ventana de entradas siguiente:

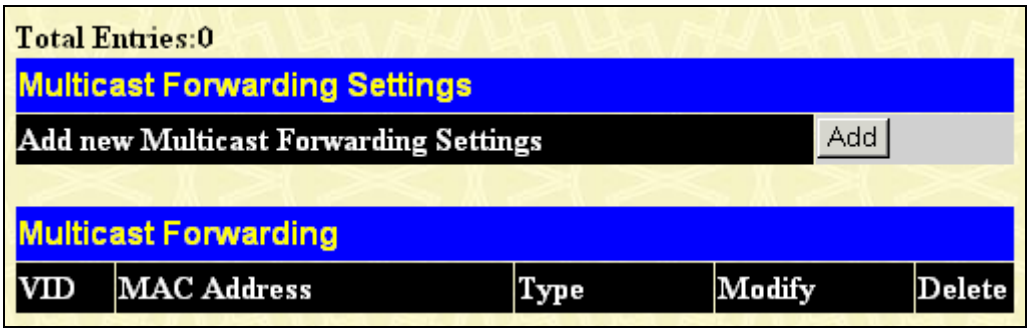


Figura 6- 13. Ventana de configuración de Envíos multicast

La ventana de **Configuración de envíos multicast estáticos** muestra todas las entradas realizadas en dicha tabla del switch. Haga clic en el botón Añadir para abrir la ventana de la **Tabla de configuración de envíos multicast estáticos**, tal y como se muestra a continuación:

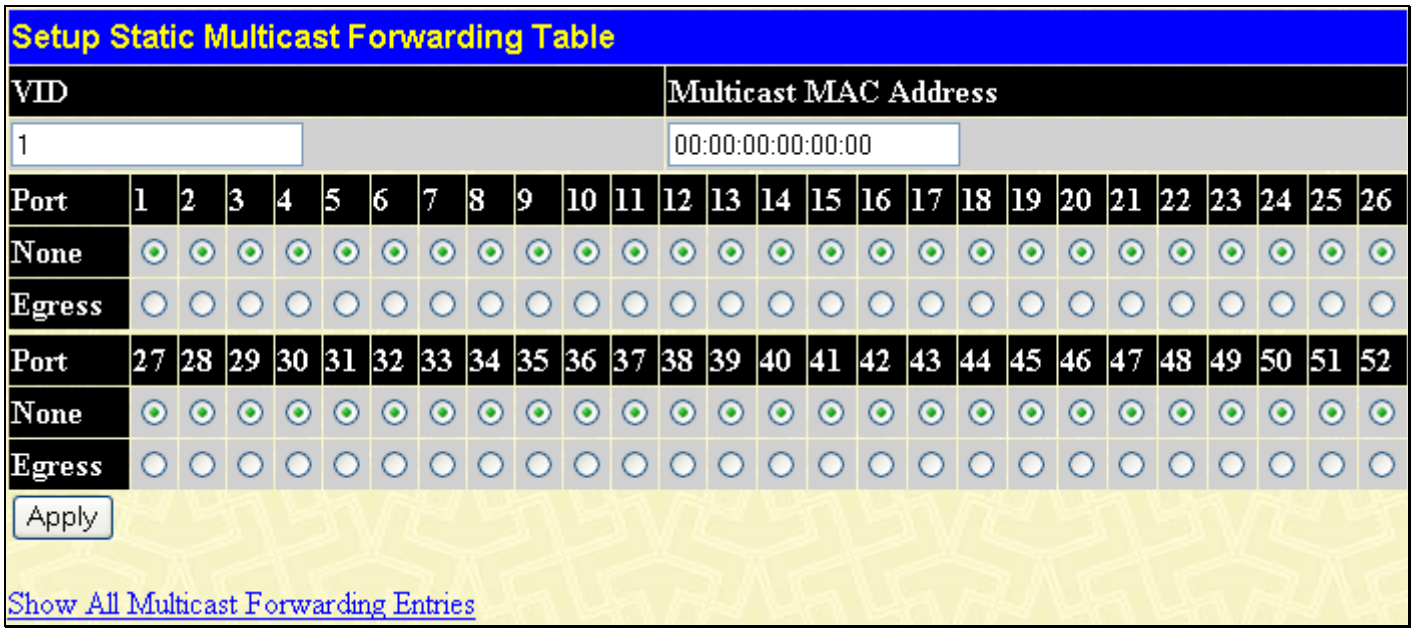


Figura 6- 14. Ventana de la Tabla de configuración de envíos multicast estáticos

Pueden configurarse los parámetros siguientes:

Parámetro	Descripción
VID	Identificación de la VLAN a la que pertenece la dirección MAC correspondiente.
Dirección MAC multicast	Dirección MAC de la fuente estática de paquetes multicast. Ésta debe ser una dirección MAC multicast.
Opciones de los puertos	Permite seleccionar puertos que serán miembros del Grupo Multicast Estático. Las opciones disponibles son las siguientes: *Ninguno* – Cuando se selecciona *Ninguno*, el puerto no será miembro del Grupo Multicast Estático. *Salida* – El puerto es un miembro estático del grupo multicast.

Haga clic en **Aplicar** para aplicar los cambios realizados. Para eliminar una entrada de la Tabla de Envíos multicast estáticos, haga clic en la *X* correspondiente debajo del título Eliminar. Haga clic en el enlace de **Mostrar todas las entradas de envíos multicast** para volver a la ventana de **Configuración de envíos multicast estáticos.**

Modo de filtro multicast

La figura y la tabla siguientes describen cómo se configura el **Modo de filtro multicast** del switch. Abra la carpeta de **Envíos y filtros** y haga clic en el enlace **Configuración del Modo de filtro multicast** para visualizar la ventana de entradas siguiente:

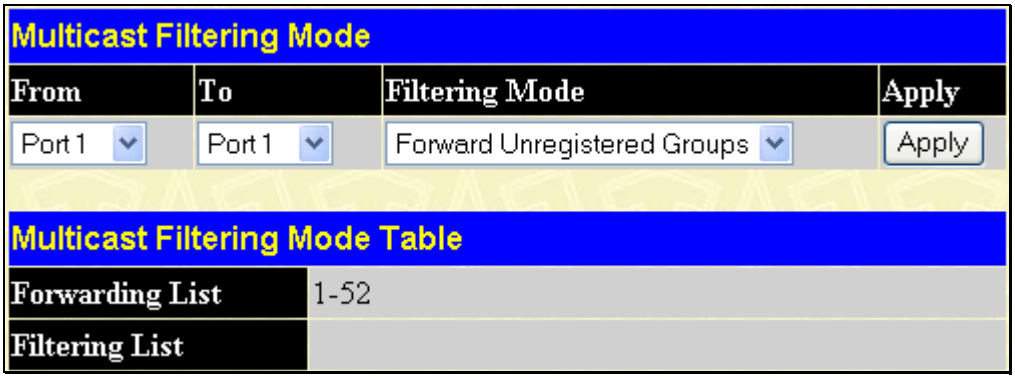


Figura 6- 15. Ventana del Modo de filtro multicast

Pueden configurarse los parámetros siguientes:

Parámetro	Descripción
De/A	Estos menús desplegables le permiten seleccionar un rango de puertos a los que se aplicarán las opciones de configuración del filtro.
Modo	Este menú desplegable le permite seleccionar la acción que realizará el switch cuando reciba un paquete multicast que debe enviarse a uno de los puertos del rango especificado arriba. • *Enviar grupos no registrados* – Indicará al switch que envíe un paquete multicast cuyo destino sea un grupo multicast no registrado que radique en el rango de puertos especificado arriba. • *Filtrar grupos no registrados* - Indicará al switch que filtre cualquier paquete multicast cuyo destino sea un grupo multicast no registrado que radique en el rango de puertos especificado arriba.

Haga clic en **Aplicar** para aplicar los cambios realizados.

Apartado 7

Características de Capa 2

- *VLAN*
- *Enlaces troncales*
- *Control IGMP*
- *Árbol de expansión*

VLANs

Una Red de Área Local Virtual (VLAN) es un tipo de red configurada de acuerdo con un esquema lógico, no con un diseño físico. Las VLANs pueden utilizarse para combinar cualquier conjunto de segmentos LAN con un grupo de usuarios autónomos que aparecer como LAN simple. Las VLANs también segmentan la red de forma lógica en diferentes dominios de difusión para que los paquetes se envíen únicamente entre puertos dentro de la VLAN. Normalmente una VLAN corresponde a una subred en concreto, aunque no necesariamente.

Las VLANs pueden mejorar el rendimiento conservando el ancho de banda y reforzar la seguridad limitando el tráfico en dominios específicos.

Una VLAN es un conjunto de nodos finales agrupados por ubicación lógica en lugar de física. Los nodos finales que con frecuencia se comunican entre sí se asignan a la misma VLAN, independientemente del lugar físico en el que se encuentran en la red. Una VLAN puede identificarse de forma lógica con un dominio de difusión, porque los paquetes de difusión se envían únicamente a miembros de la VLAN en la que se haya iniciado la difusión.

Notas acerca de las VLANs del switch

Al margen de la base que se utilice para identificar de forma exclusiva los nodos finales y hacer que éstos formen parte de la VLAN, los paquetes no pueden pasar por las VLANs sin un dispositivo de red con función de direccionamiento entre las VLANs.

El switch es compatible con VLANs IEEE 802.1Q. La función de desetiquetado de puertos puede utilizarse para retirar la etiqueta 802.1Q de los encabezamientos del paquete para mantener la compatibilidad con los dispositivos sin etiquetas.

El switch asigna de forma predeterminada todos los puertos a una VLAN simple 802.1Q denominada "predeterminada".

La VLAN "predeterminada" tiene un VID = 1.

Si lo desea, los puertos miembros de las VLANs basadas en puertos pueden estar superpuestos.

VLANs IEEE 802.1Q

Términos relevantes:

- **Etiquetar** Acto de colocar información de una VLAN 802.1Q en el encabezamiento de un paquete.
- **Desetiquetar** Acto de retirar información de una VLAN 802.1Q del encabezamiento del paquete.
- **Puerto de entrada** Puerto del switch en el que los paquetes fluyen hacia el switch y deben tomarse decisiones respecto a la VLAN.
- **Puerto de salida** Puerto del switch en el que los paquetes fluyen fuera del switch, ya sea a otro switch o a una estación final, y deben tomarse decisiones respecto al desetiquetado.

Las VLANs IEEE 802.1Q (etiquetado) se implementan en el switch. Las VLANs 802.1Q necesitan etiquetado, que les permite abarcar la red en su totalidad (dando por hecho que todos los switches de la red son conformes a IEEE 802.1Q).

Las VLANs permiten que una red se segmente para reducir el tamaño de los dominios de difusión. Todos los paquetes que se introducen en una VLAN se enviarán únicamente a las estaciones (sobre switches con IEEE 802.1Q activado) que sean miembros de esa VLAN, y ello incluye los paquetes de difusión, multicast y unicast de orígenes desconocidos.

ESPAÑOL

Las VLANs también pueden aportar un nivel de seguridad a la red del usuario. Las VLANs IEEE 802.1Q sólo enviarán paquetes entre estaciones que son miembros de la VLAN.

Cualquier puerto puede configurarse como de etiquetado o desetiquetado. La función de desetiquetado de las VLANs IEEE 802.1Q permite a estas redes trabajar con switches de legado que no reconocen las etiquetas de las VLANs en los encabezamientos del paquete. La función de etiquetado permite a las VLANs abarcar diversos switches conforme a 802.1Q mediante una sencilla conexión física y permite que el Árbol de expansión se active en todos los puertos y funcione con normalidad.

El estándar IEEE 802.1Q restringe el envío de paquetes desetiquetados a la VLAN de la que el puerto receptor es miembro.

Las características principales de IEEE 802.1Q son las siguientes:

- Asigna paquetes a las VLANs mediante filtrado.
- Asume la presencia de un árbol de expansión global simple.
- Utiliza un esquema de etiquetado explícito con etiquetado de un nivel.
- Envía paquetes de VLANs 802.1Q.
- Las decisiones respecto al envío de paquetes se toman basándose en los tres tipos de reglas siguientes:
- Reglas de entrada: relativas a la clasificación de los frames recibidos que pertenecen a una VLAN.
- Reglas de envío entre puertos: decide entre filtrar o enviar el paquete.
- Reglas de salida: determina si el paquete debe enviarse etiquetado o desetiquetado.

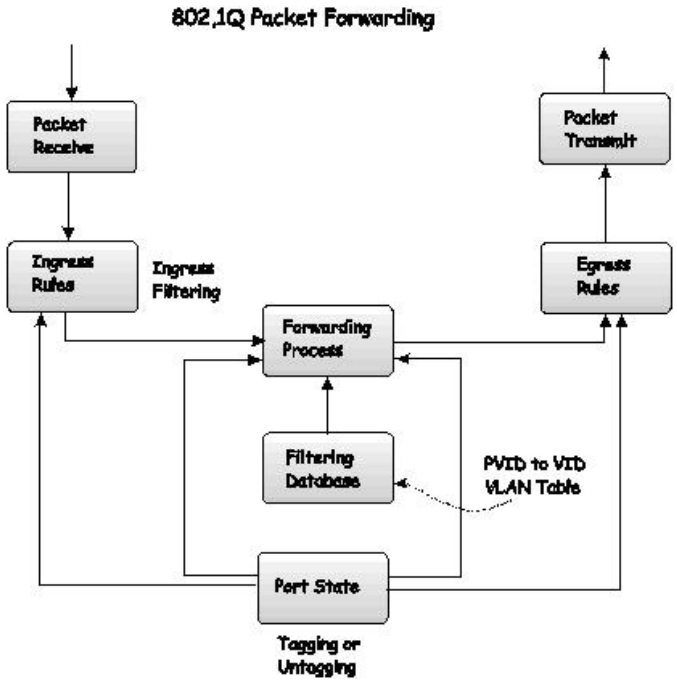


Figura 7- 1. Envío de paquetes IEEE 802.1Q

Etiquetas de VLANs 802.1Q

La figura siguiente muestra la etiqueta de VLANs 802.1Q. Hay cuatro octetos adicionales insertados tras la dirección MAC de origen. Su presencia está indicada por un valor de 0x8100 en el campo EtherType. Cuando el campo EtherType de un paquete es equivalente a 0x8100, el paquete lleva la etiqueta IEEE 802.1Q/802.1p. La etiqueta está en los dos octetos siguientes y está formada por 3 bits de prioridad de usuario, 1 bit de Identificador de formato canónico (CFI, utilizado para encapsular paquetes de anillo de testigo de modo que puedan llevarse por las redes troncales Ethernet) y 12 bits de VLAN ID (VID). 802.1p utiliza los 3 bits de prioridad de usuario. El VID es el identificador de la VLAN, utilizado por el estándar 802.1Q. Como el VID tiene una longitud de 12 bits, pueden identificarse 4094 VLANs únicas.

La etiqueta se introduce en el encabezamiento del paquete, con lo cual éste último aumenta en 4 octetos, y la información que contenía inicialmente se conserva.

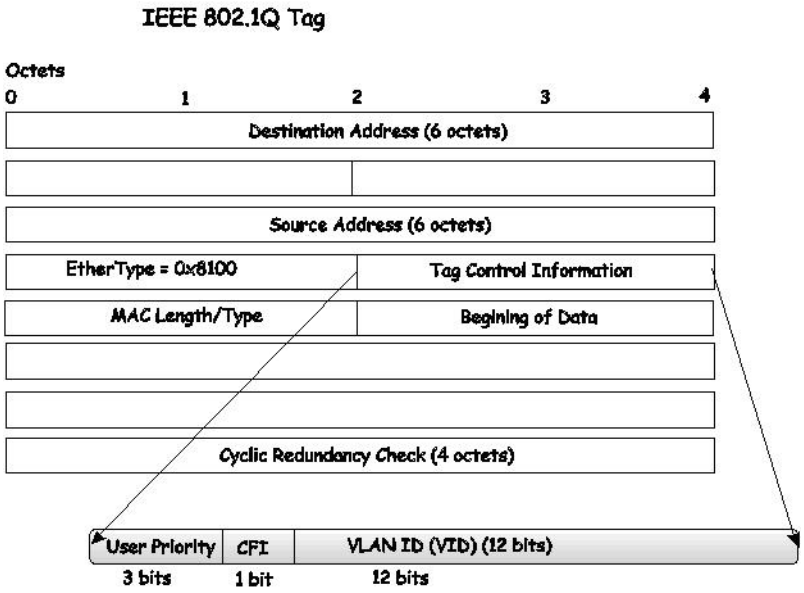


Figura 7- 2.Etiqueta IEEE 802.1Q

El EtherType y el VLAN ID se introducen tras la dirección MAC de origen, pero antes del EtherType/Longitud original o Control de Enlace Lógico. Debido a que el paquete es ahora un poco más largo de lo que era inicialmente, será necesario volver a calcular la Comprobación de Redundancia Cíclica (CRC).

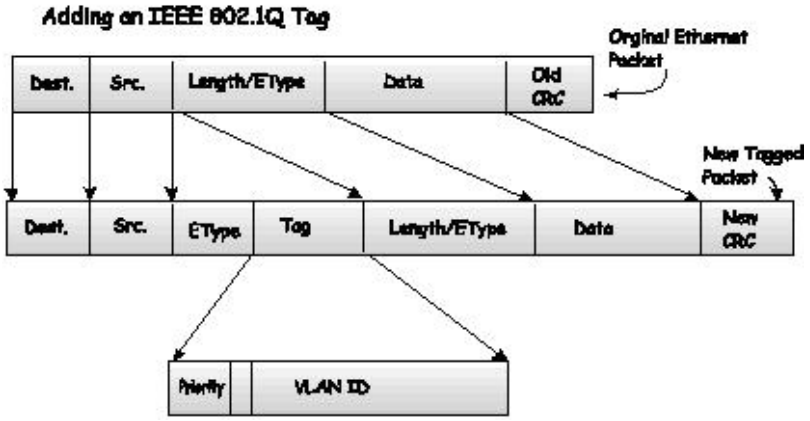


Figura 7- 3. Proceso para añadir una etiqueta IEEE 802.1Q

Etiquetado y desetiquetado

Todos los puertos de un switch conforme a 802.1Q pueden configurarse como de etiquetado o desetiquetado.

Los puertos con la función de etiquetado activada colocan el número VID, la prioridad y demás información sobre la VLAN en el encabezamiento de todos los paquetes que fluyen hacia y fuera de esos puertos. Si un paquete ha sido etiquetado anteriormente, el puerto no alterará el paquete, y por tanto mantendrá intacta la información de la VLAN. Esta información que contiene la etiqueta la pueden utilizar otros dispositivos conformes a 802.1Q de la red para tomar decisiones sobre envíos de paquetes.

Los puertos con la función de desetiquetado activada retiran la etiqueta 802.1Q de todos los paquetes que fluyen hacia y fuera de esos puertos. Si el paquete no tiene una etiqueta de la VLAN 802.1Q, el puerto no alterará el paquete. Por tanto, todos los paquetes recibidos y enviados por un puerto de desetiquetado no contendrán información de la VLAN 802.1Q (recuerde que el PVID sólo se utiliza internamente dentro del switch). El desetiquetado se utiliza para enviar paquetes de un dispositivo de red conforme a 802.1Q a un dispositivo de red no conforme.

Filtrado de entrada

El puerto de un switch en el que los paquetes fluyen hacia el dispositivo y deben tomarse decisiones respecto a la VLAN se denomina “puerto de entrada”. Si el filtrado de entrada está activo en un puerto, el switch examinará la información de la VLAN que figura en el encabezamiento del paquete (en caso de estar presente) y decidirá si envía o no el paquete.

Si el paquete está etiquetado con información de la VLAN, el puerto de entrada determinará en primer lugar si el propio puerto es miembro de la VLAN etiquetada. En caso contrario, el paquete se omite. Si el puerto de entrada es miembro de la VLAN 802.1Q, el switch determinará si el puerto de destino es miembro de la VLAN 802.1Q. En caso contrario, el paquete se omite. Si el puerto de destino es miembro de la VLAN 802.1Q, el paquete se enviará y el puerto de destino lo transmitirá a su segmento de red adjunto.

Si el paquete no está etiquetado con información de la VLAN, el puerto de entrada etiquetará el paquete con su propio PVID como VID (si el puerto es un puerto de etiquetado). Así, el switch determina si el puerto de destino es miembro de la misma VLAN (tiene el mismo VID) como puerto de entrada. En caso contrario, el paquete se omite. Si tiene el mismo VID, el paquete se enviará y el puerto de destino lo transmitirá a su segmento de red adjunto.

Este proceso se denomina “filtrado de entrada” y se utiliza para conservar el ancho de banda dentro del switch omitiendo paquetes que no están en la misma VLAN que el puerto de entrada en el punto de recepción. Con ello se elimina el procesamiento posterior de paquetes que el puerto de destino omitirá.

VLANs predeterminadas

Inicialmente el switch configura una VLAN, VID = 1, llamada "predeterminada". Las opciones de configuración de fábrica asignan a todos los puertos del switch el estado de "predeterminado".

Los paquetes no pueden cruzar las VLANs. Si un miembro de una VLAN quiere conectarse a otra VLAN, el enlace debe realizarse a través de un router externo.

NOTA: Si el switch no tiene VLANs configuradas, todos los paquetes se enviarán a cualquier puerto de destino y los paquetes con direcciones de origen desconocido llegarán a todos los puertos, así como los paquetes de difusión y multicast.

A continuación presentamos un ejemplo:

Nombre de la VLAN	VID	Puertos del switch
Sistema (predeterminado)	1	5, 6, 7, 8, 21, 22, 23, 24
Ingeniería	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finanzas	4	17, 18, 19, 20
Ventas	5	1, 2, 3, 4

Tabla 7- 1. Ejemplo de VLAN: puertos asignados

Segmentación de VLAN

Tomemos, por ejemplo, un paquete transmitido por un equipo en el puerto 1, que es miembro de la VLAN 2. Si el destino radica en otro puerto (encontrado mediante una consulta en la tabla de envíos), el switch buscará si el otro puerto (puerto 10) es miembro de la VLAN 2 (y por tanto, puede recibir paquetes de la VLAN 2). Si el puerto 10 no es miembro de la VLAN 2, el switch omitirá el paquete y éste no llegará a su destino. Si el puerto 10 es miembro de la VLAN 2, el paquete pasará. Esta característica de envío selectivo basada en criterios de la VLAN es el modo de transmisión de segmentos de la VLANs y el punto clave está en que el puerto 1 sólo transmitirá a la VLAN 2.

Sin embargo, los recursos de red, como las impresoras y los servidores, pueden compartirse en las VLANs. Para ello, deben configurarse VLANs superpuestas, es decir, que los puertos pueden pertenecer a más de un grupo VLAN. Por ejemplo, configurar los miembros de la VLAN 1 a los puertos 1, 2, 3 y 4, y los miembros de la VLAN 2, a los puertos 1, 5, 6 y 7. El puerto 1 pertenece a dos grupos VLAN. Los puertos 8, 9 y 10 no están configurados con ningún grupo VLAN, lo cual significa que los puertos 8, 9 y 10 son independientes y no pertenecen a ninguna VLAN, ya que no están en el mismo dominio.

VLAN y grupos de enlaces troncales

Los miembros de un grupo de enlaces troncales tienen la misma configuración VLAN. Cualquier configuración VLAN de los miembros de un grupo de enlaces troncales se aplicará a los demás puertos miembros.

Entrada de VLANs estáticas

En la carpeta **Características de Capa 2**, abra la carpeta **VLAN** y haga clic en el enlace **Entradas de VLANs estáticas** para abrir la ventana siguiente:

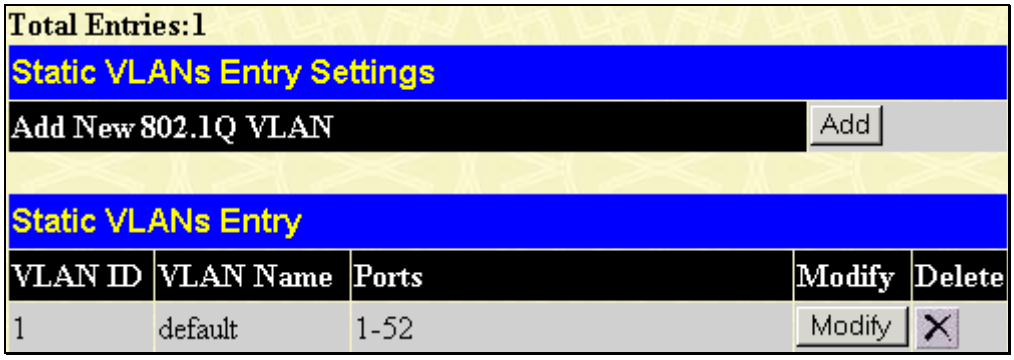


Figura 7- 4. Ventana de configuración de Entradas de VLANs estáticas

La ventana de **VLANs estáticas 802.1Q** enumera todas las VLANs que ya se han configurado anteriormente por **VLAN ID** y por **Nombre de la VLAN**. Para eliminar una VLAN 802.1Q, haga clic en el botón correspondiente debajo del encabezamiento **Eliminar**.

Para crear una nueva VLAN 802.1Q, haga clic en el botón **Añadir** de la ventana **VLANs 802.1Q estáticas**. A continuación aparecerá una nueva ventana, tal y como se muestra abajo, para configurar las opciones de los puertos y para asignar un nombre y un número únicos a la nueva VLAN. Consulte la tabla siguiente para obtener una descripción de los parámetros de la nueva ventana.

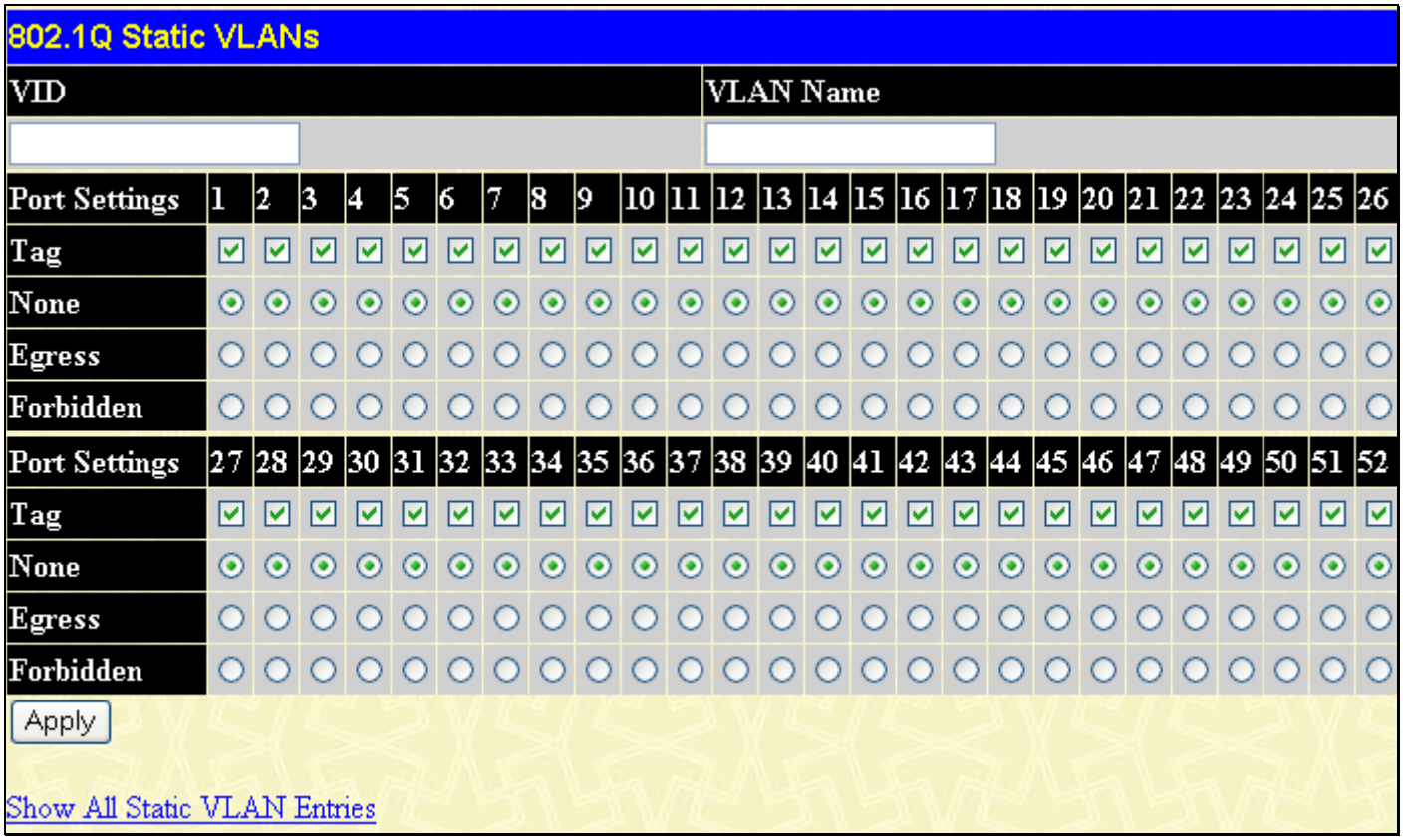


Figura 7- 5. Ventana de VLANs 802.1Q estáticas: Añadir

Para volver a la ventana de **Entradas actuales de VLANs 802.1Q estáticas**, haga clic en el enlace Mostrar todas las entradas de VLAN estáticas. Para cambiar una entrada de VLAN 802.1Q existente, haga clic en el botón **Modificar** de la entrada correspondiente que desea modificar. A continuación aparecerá una nueva ventana para configurar las opciones de los puertos. Consulte la tabla siguiente para obtener una descripción de los parámetros de la nueva ventana.

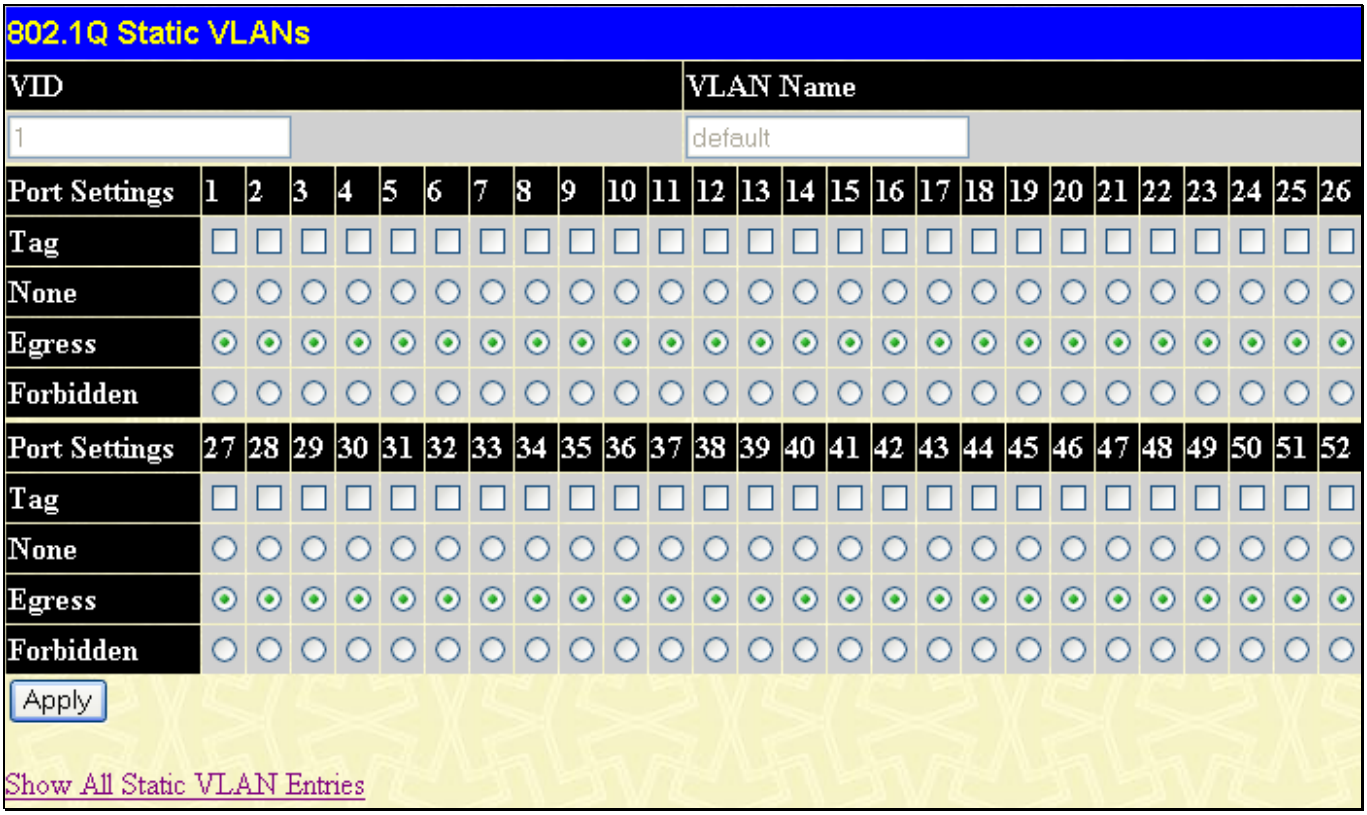


Figura 7- 6. Ventana de VLANs 802.1Q estáticas: Modificar

Los campos siguientes pueden configurarse en la ventana de **Añadir** o **Modificar VLANs 802.1Q estáticas**:

Parámetro	Descripción
VID	Permite la entrada de un VLAN ID en el cuadro de diálogo Añadir, o muestra el VLAN ID de una VLAN existente en el cuadro de diálogo Modificar. Las VLANs pueden identificarse por el VID o por el nombre de la VLAN.
Nombre de la VLAN	Muestra el nombre de la VLAN.
Opciones del puerto	Permite que se especifique un puerto individual como miembro de una VLAN.
Etiqueta	Especifica el puerto como etiquetado 802.1Q o desetiquetado 802.1Q. Si se marca la casilla configurará el puerto como Etiquetado.
Ninguna	Permite que se especifique un puerto individual como no miembro de una VLAN.
Salida	Seleccione este parámetro para especificar el puerto como miembro estático de la VLAN. Los puertos miembro de salida son puertos que transmitirán tráfico para la VLAN y pueden ser etiquetados o desetiquetados.

Haga clic en **Aplicar** para aplicar los cambios realizados. Haga clic en el enlace Mostrar todas las entradas de VLAN estáticas para volver a la ventana de **VLANs 802.1Q estáticas**.

Enlaces troncales

Los grupos de enlaces troncales de puertos se utilizan para combinar un número de puertos para obtener un único flujo de datos de banda ancha de gran calidad.

El switch puede albergar hasta seis grupos de enlaces troncales de puertos con 2 a 8 puertos en cada grupo. Puede alcanzarse una velocidad de transferencia de 800 Mbps.

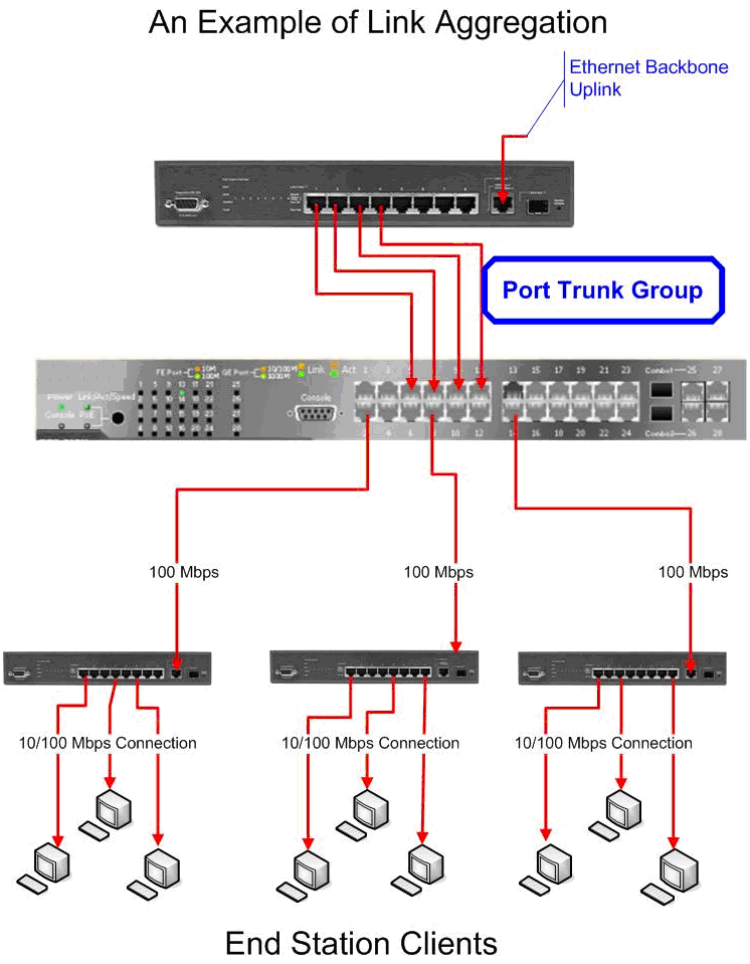


Figura 7- 7. Ejemplo de un grupo de enlaces troncales de puertos

El switch trata a todos los puertos de un grupo de enlaces troncales como si fuera un único puerto. Los datos transmitidos a un host específico (dirección de destino) siempre se transmitirán por el mismo puerto de un grupo de enlaces troncales, lo cual permite que los paquetes del flujo de datos lleguen en el mismo orden que se enviaron.

NOTA: En caso de que algún puerto del grupo de enlaces troncales se desconectase, los paquetes dirigidos al puerto desconectado se cargarán de forma compartida entre los puertos con enlaces ascendentes del grupo de incorporación de enlaces.

La incorporación de enlaces permite agrupar diversos puertos y actuar como un único enlace, lo cual posibilita un ancho de banda múltiple del ancho de banda de un único enlace.

La incorporación de enlaces se usa más habitualmente para enlazar uno o varios dispositivos de red de mayor ancho de banda, como un servidor, con la red troncal de una red.

El switch permite crear hasta seis grupos de incorporación de enlaces, formado cada grupo por 2 a 8 enlaces (puertos). Todos los puertos del grupo deben ser miembros de la misma VLAN, y su estado STP, multicast estático, control y segmentación de tráfico y las configuraciones de prioridad predeterminada (802.1p) deben ser idénticos. El bloqueo y la replicación de puertos y 802.1X no deben estar activados en el grupo de enlaces troncales. Además, los enlaces agregados deben tener la misma velocidad y deben estar configurados como full-duplex.

El Puerto Maestro del grupo debe configurarlo el usuario, y todas las opciones de configuración, incluida la configuración de la VLAN que puede aplicarse al Puerto Maestro, se aplican a todo el grupo de incorporación de enlaces.

El equilibrio de carga se aplica automáticamente a los puertos en el grupo agregado, y en caso de que se produzca un fallo en los enlaces dentro del grupo, el tráfico de la red se direcciona a los enlaces restantes del grupo.

El Protocolo del Árbol de expansión tratará a un grupo de incorporación de enlaces como a un único enlace a nivel del switch. En cuanto a los puertos, el STP utilizará los parámetros de los puertos del Puerto Maestro para calcular el coste de los mismos y determinar el estado del grupo de incorporación de enlaces. Si se configuran dos grupos de incorporación de enlaces redundantes en el switch, el STP bloqueará el grupo completo, del mismo modo que el STP bloqueará un único puerto que tenga un enlace redundante.

Incorporación de enlaces

Para configurar enlaces troncales de puertos, haga clic en **Características de Capa 2 > Enlaces troncales > Incorporación de enlaces** y a continuación aparecerá la ventana siguiente:

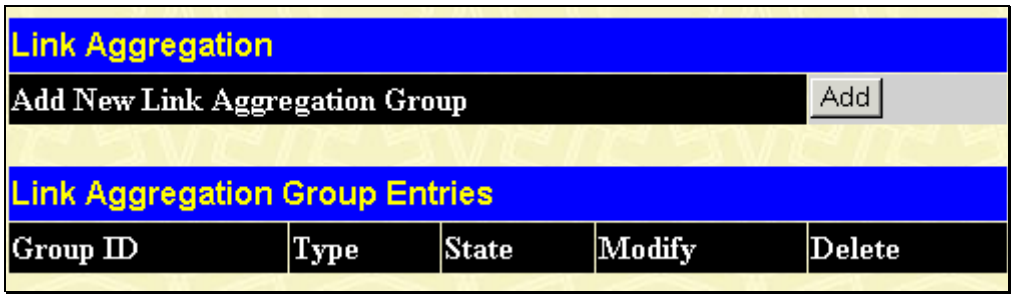


Figura 7- 8. Ventana de Incorporación de enlaces

Para configurar grupos de enlaces troncales, haga clic en el botón **Añadir** para añadir un nuevo grupo y utilice el menú de **Opciones de incorporación de enlaces** (consulte el ejemplo siguiente) para configurar grupos de enlaces troncales. Para modificar un grupo de enlaces troncales, haga clic en el número del grupo enlazado correspondiente a la entrada que desea modificar. Para eliminar un grupo de enlaces troncales, haga clic en la correspondiente bajo el encabezamiento **Eliminar** en la tabla de **Entradas del grupo de incorporación de enlaces** (en la parte inferior de la ventana de **Incorporación de enlaces**).

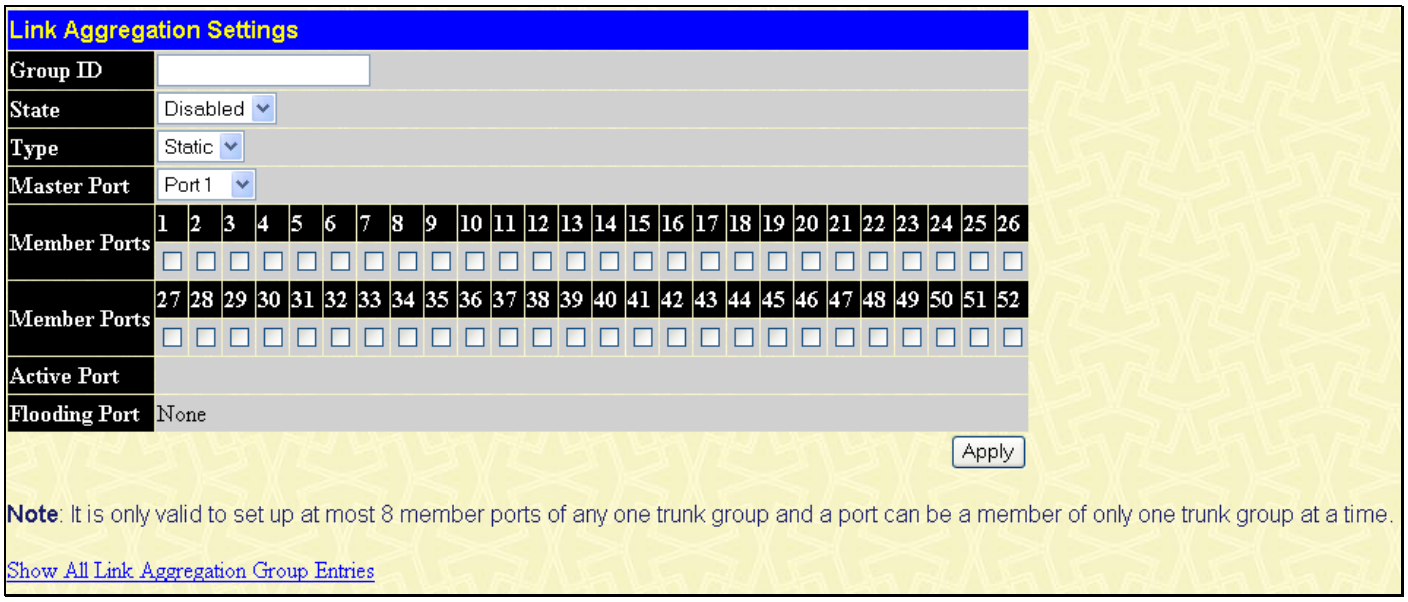


Figura 7- 9. Ventana de Opciones de incorporación de enlaces: Añadir

Control IGMP

El control del **Protocolo de Gestión de Grupos de Internet (IGMP)** permite al switch reconocer consultas e informes IGMP enviados entre estaciones o dispositivos de red y un host IGMP. Cuando tiene activada la función de control IGMP, el switch puede abrir o cerrar un puerto a un dispositivo específico basado en mensajes IGMP que pasan por el switch.

Para utilizar la función de Control IGMP ésta debe estar activada para el switch al completo (consulte la **Información del dispositivo**). Posteriormente, deberá ajustar las opciones de configuración de cada VLAN mediante el enlace de **Control IGMP** situado en la carpeta **Características de Capa 2**. Una vez activadas para el Control IGMP, el switch podrá abrir o cerrar un puerto a un miembro del grupo multicast específico basado en mensajes IGMP enviados desde el dispositivo al host IGMP o viceversa. El switch controla los mensajes IGMP e interrumpe el envío de paquetes multicast cuando ya no hay hosts que soliciten su continuación. Utilice la ventana de **Control IGMP** para visualizar el estado del Control IGMP. Para modificar las opciones, haga clic en el botón **Modificar** de la entrada del Nombre de la VLAN que desea cambiar.

Utilice la ventana **Control IGMP** para visualizar las opciones de configuración de control IGMP. Para modificar dichas opciones, haga clic en el botón **Modificar** del VLAN ID.

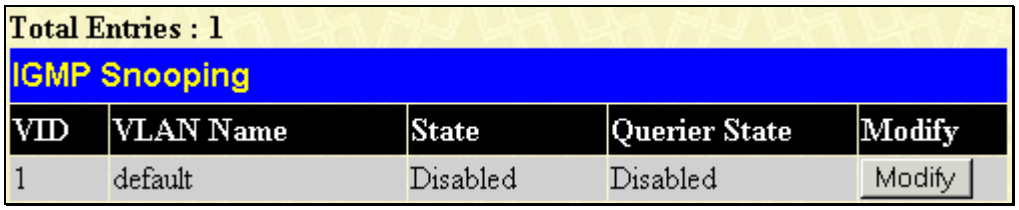


Figura 7- 10. Ventana de Control IGMP

Haga clic en el botón **Modificar** para abrir el menú **Opciones de Control IGMP**, como se indica a continuación:

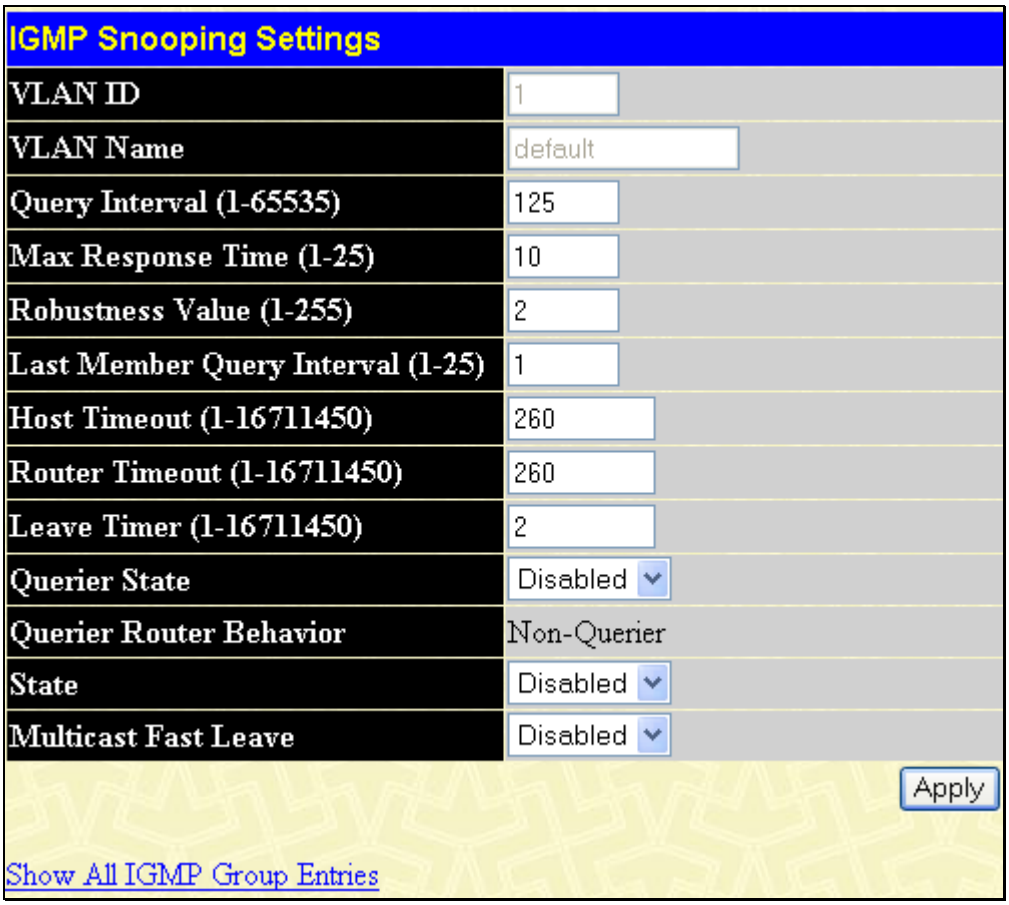


Figura 7- 11. Ventana de Opciones de Control IGMP

ESPAÑOL

Pueden visualizarse o modificarse los parámetros siguientes:

Parámetro	Descripción
VLAN ID	Éste es el VLAN ID que, junto con el Nombre de la VLAN, identifica la VLAN para la que se modifican las Opciones de Control IGMP.
Nombre de la VLAN	Éste es el Nombre de la VLAN que, junto con el VLAN ID, identifica la VLAN para la que se modifican las Opciones de Control IGMP.
Intervalo de consulta	Este campo se utiliza para ajustar el tiempo (en segundos) entre la transferencia de consultas IGMP. Se permiten entradas entre *1* y *65535* segundos. Valor predeterminado: *125*.
Tiempo de respuesta máximo	Determina el tiempo máximo en segundos permitido para enviar un informe de respuesta IGMP. Este campo permite entradas entre *1* y *25* (segundos). Valor predeterminado = *10*.
Valor de solidez	Ajuste esta variable en función de la pérdida de paquetes prevista. Si se espera que la pérdida de paquetes de la VLAN sea alta, el Valor de solidez deberá aumentarse para que se adapte a esa mayor pérdida de paquetes. Este campo permite entradas entre *1* a *255*. Valor predeterminado: *2.*
Intervalo de consulta del último miembro	Este campo especifica el tiempo máximo en segundos entre los mensajes de consulta de un grupo específico, incluidos los enviados en respuesta a mensajes de un grupo que abandona. Valor predeterminado: *1*.
Tiempo de espera del host	Es el tiempo máximo en segundos permitido para que un host siga siendo miembro de un grupo multicast sin que el switch reciba un informe de miembros del host. Valor predeterminado: *260*.
Tiempo de espera del router	Es el tiempo máximo en segundos que el cronómetro de los puertos dinámicos del router se mantiene en el estado “Explorar los puertos del router” cuando el puerto del router recibe una Consulta general. Valor predeterminado: *260*.
Tiempo de espera de cese	Especifica el tiempo máximo en segundos entre el momento en que el switch recibe un mensaje de un grupo que abandona de un host, y el momento en que el switch emite una consulta de miembros de un grupo. En caso de que no se reciba respuesta a dicha consulta antes de que el Temporizador de cese caduque, la entrada del envío (multicast) para ese host se elimina.
Estado de consulta	Elija *Activado* para activar la transmisión de paquetes de Consulta IGMP o *Desactivado* para desactivarla. Este parámetro está *Desactivado* por defecto.
Comportamiento del router (consultas)	Este campo de sólo lectura describe el comportamiento del router durante el envío de paquetes de consulta. *Consultas* indica que el router está enviando paquetes de consultas IGMP, mientras que *Sin consultas* indica que el router no está enviando paquetes de consultas IGMP. Este campo sólo leerá *Consultas* cuando se hayan activado los campos Estado de consulta y Estado.
Estado	Seleccione *Activado* para implementar el Control IGMP. Este campo está *Desactivado* por defecto.
Fast Leave multicast	Este parámetro permite al usuario activar la función Fast Leave. Cuando está *Activada*, esta función permite a los miembros de un grupo multicast abandonar el grupo inmediatamente (sin la aplicación del Cronómetro de consulta del último miembro) cuando el switch recibe un Paquete de informe de abandono IGMP. Este parámetro está *Desactivado* por defecto.

Haga clic en **Aplicar** para aplicar las nuevas opciones de configuración. Haga clic en el enlace Mostrar todas las entradas de Control IGMP para volver a la ventana de **Entradas actuales del Grupo de IGMP**.

NOTA: La función Fast Leave está pensada para usuarios IGMPv2 con intención de abandonar un grupo multicast y se implementa con mejores resultados en VLANs que tienen sólo un host conectado en cada puerto. Cuando un host de un grupo de hosts utiliza la función Fast Leave, es posible que otros hosts del grupo la utilicen también de forma involuntaria.

Opciones de los puertos del router estático

El puerto de un router estático es un puerto que tiene conectado un router multicast. En general este router está conectado a una red WAN o a internet. Establecer el puerto de un router permitirá que los paquetes multicast procedentes del router se difundan por la red y que los mensajes multicast (IGMP) procedentes de la red se dirijan al router.

El puerto de un router debe tener el comportamiento siguiente:

- Todos los paquetes del Informe IGMP se enviarán al puerto del router.
- Las consultas IGMP (procedentes del puerto del router) se enviarán a todos los puertos.
- Todos los paquetes multicast UDP se enviarán al puerto del router. Como los routers no envían informes IGMP ni aplican control IGMP, un router multicast conectado al puerto del router de un switch de Capa 3 no podrá recibir flujos de datos UDP a menos que todos los paquetes multicast UDP se envíen al puerto del router.

El puerto de un router estará configurado de forma dinámica cuando se detecten paquetes de consultas IGMP, paquetes multicast RIPv2, multicast DVMRP o PIM-DM que fluyen hacia un puerto.

Abra la carpeta **Control IGMP** y haga clic en el enlace de **Opciones de los puertos del router estático** para abrir la ventana del mismo nombre, tal y como se muestra a continuación.

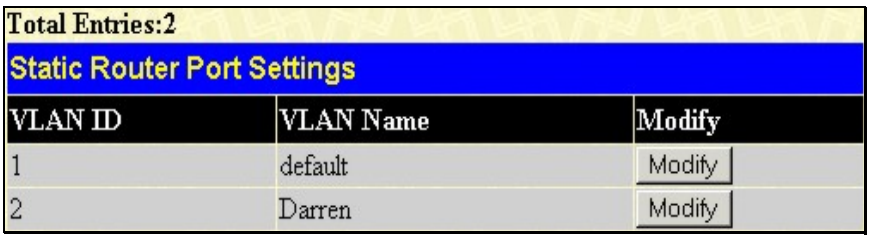


Figura 7- 12. Ventana de Opciones de los puertos del router estático

La página de **Opciones de los puertos del router estático** (que aparece arriba) muestra todas las entradas actuales de los puertos del router estático del switch. Para modificar una entrada, haga clic en el botón **Modificar** y se abrirá la ventana siguiente:

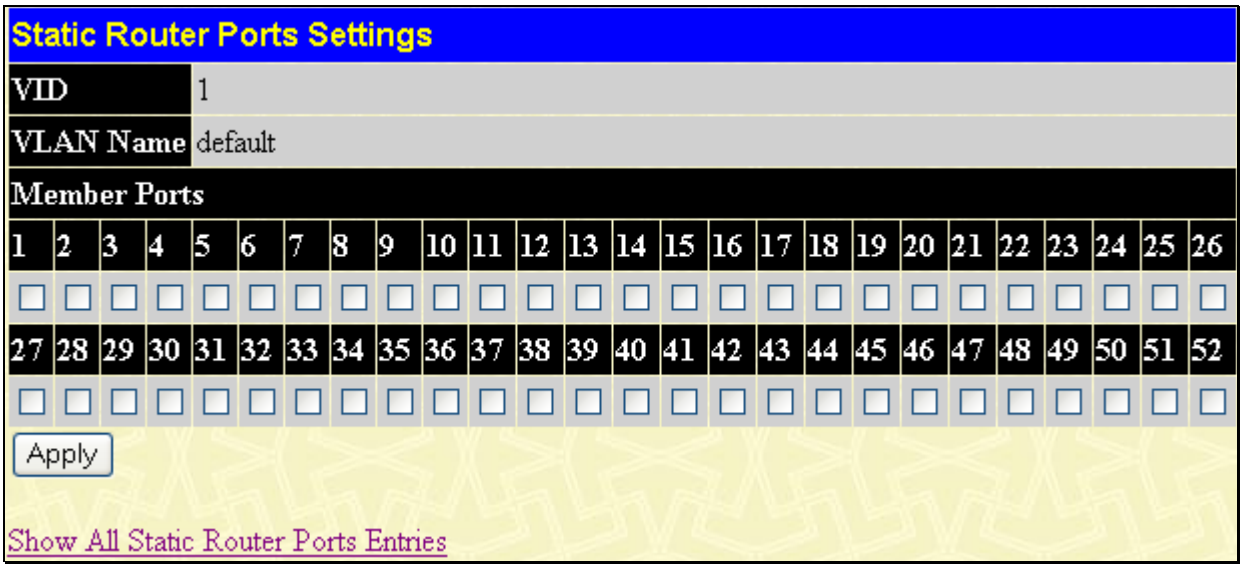


Figura 7- 13. Ventana de Opciones de los puertos del router estático: Editar

Pueden configurarse los parámetros siguientes:

Parámetro	Descripción
VID (VLAN ID)	Éste es el VLAN ID que, junto con el Nombre de la VLAN, identifica la VLAN a la que el router multicast está conectado.
Nombre de la VLAN	Es el nombre de la VLAN a la que el router multicast está conectado.
Puertos miembros	Son los puertos del switch que tendrán un router multicast conectado.

Haga clic en **Aplicar** para implementar las nuevas opciones de configuración. Haga clic en el enlace Mostrar todas las entradas de los puertos del router estático para volver a la ventana **Entrada actuales de los puertos del router estático**.

Árbol de expansión

Árbol de expansión rápida 802.1w

El switch aplica el Protocolo del Árbol de Expansión Rápida (RSTP), tal y como define la especificación IEEE 802.1w, y una versión compatible con IEEE 802.1d STP. El RSTP puede funcionar con equipamiento de legado que aplique IEEE 802.1d, aunque las ventajas de utilizar el RSTP se perderán.

El Protocolo del Árbol de Expansión Rápida (RSTP) IEEE 802.1w evolucionó a partir de la norma 802.1d STP. El RSTP se desarrolló con el objetivo de mejorar limitaciones del STP que impedían que funcionaran determinadas innovaciones de conmutación recientes; en concreto, algunas funciones de Capa 3 que cada vez más forman parte de los switches Ethernet. La función básica y gran parte de la terminología es la misma que la de STP. La mayoría de las opciones configuradas para STP también se usan para RSTP. Esta sección introduce algunos de los nuevos conceptos del Árbol de expansión e ilustra las diferencias principales entre los dos protocolos.

Estados de transición de los puertos

Una diferencia esencial entre los tres protocolos reside en el modo en que los puertos realizan la transición a un estado de envío y en la manera con la que esta transición está relacionada con la función del puerto (de envío o no) en la topología. El RSTP combina los estados de transición desactivado, de bloqueo y de escucha que se utilizan en 802.1d y crea un estado único de Descarte. En cualquiera de esos casos, los puertos no envían paquetes. En los estados de transición de los puertos STP desactivado, de bloqueo o de escucha o en el estado del puerto RSTP de descarte, no hay diferencias funcionales: el puerto no está activo en la topología de la red. La Tabla 7-2 siguiente compara cómo los dos protocolos difieren en relación con el estado de transición de los puertos.

Los tres protocolos calculan una topología estable del mismo modo. Todos los segmentos tendrán una única ruta hacia el puente raíz. Todos los puentes están en escucha de los paquetes BPDU. Sin embargo, los paquetes BPDU se envían más a menudo, con todos los paquetes se saludo (Hello). Los paquetes BPDU se envían incluso si uno de esos paquetes no se ha recibido. Por tanto, cada enlace entre puentes es sensible al estado del enlace. En última instancia, esta diferencia da como resultado una detección más rápida de los enlaces fallidos, y por tanto, un ajuste más rápido de la topología. Un inconveniente de 802.1d es esta ausencia de feedback inmediato de los puentes adyacentes.

802.1w RSTP	802.1d STP	Envío	Aprendizaje
Descarte	Desactivado	No	No
Descarte	Bloqueo	No	No
Descarte	Escucha	No	No
Aprendizaje	Aprendizaje	No	Sí
Envío	Envío	Sí	Sí

Tabla 7- 2. Comparación de Estados de los puertos

El RSTP es capaz de lograr una transición más rápida a un estado de envío (ya no confía en configuraciones de tiempo de espera). Los puentes conformes a RSTP son sensibles al feedback procedente de otros enlaces a puentes conformes a RSTP. Los puertos no necesitan esperar a que la topología se estabilice para realizar la transición a un estado de envío. Para permitir esta rápida transición, el protocolo introduce dos nuevas variables: el puerto de borde y el puerto punto a punto (P2P).

Puerto de borde

El puerto de borde es una designación configurable que se utiliza para un puerto conectado directamente a un segmento en el que no puede crearse un bucle. Un buen ejemplo sería un puerto conectado directamente a una estación de trabajo simple. Los puertos designados como puertos de borde efectúan una transición a un estado de envío inmediatamente sin pasar por los estados de escucha y aprendizaje. Un puerto de borde pierde su estatus si recibe un paquete BPDU, e inmediatamente pasa a ser un puerto normal del árbol de expansión.

Puerto P2P

Un puerto P2P también es capaz de lograr una transición rápida. Los puertos P2P pueden utilizarse para conectarse a otros puentes. Con el RSTP, todos los puertos que funcionan en modo full-duplex se consideran puertos P2P, a menos que se cancelen manualmente al configurarlos.

Compatibilidad entre 802.1d y 802.1w

El RSTP puede funcionar con equipamiento de legado y es capaz de ajustar automáticamente paquetes BPDU al formato 802.1d cuando es necesario. Sin embargo, los segmentos que utilizan 802.1d STP no se beneficiarán de la detección de cambios de rápida transición y topología de RSTP. El protocolo también ofrece una variable utilizada para la migración en caso de que el equipamiento de legado de un segmento se actualice para usar el RSTP.

El Protocolo del Árbol de Expansión (STP) funciona a dos niveles:

1. A nivel del switch, las opciones de configuración se implementan de forma global.
2. A nivel del puerto, las opciones de configuración se aplican de acuerdo con un grupo de puertos definidos por el usuario.

Configuración global del puente STP

Para abrir la ventana siguiente, abra el **Árbol de expansión** en la carpeta **Características de Capa 2** y haga clic en el enlace **Opciones globales del puente STP**.

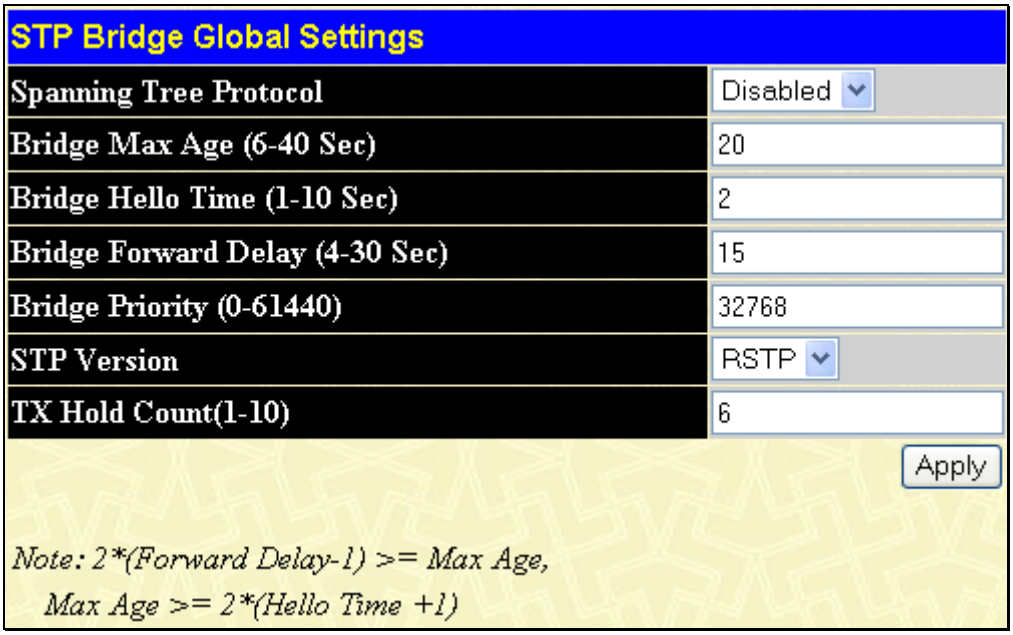


Figura 7- 14. Ventana de Opciones globales del puente STP

Pueden configurarse los parámetros siguientes:

Parámetro	Descripción
Protocolo del Árbol de Expansión	Utilice el menú desplegable para activar o desactivar el STP del switch globalmente. El estado predeterminado es *Desactivado*.
Puente de tiempo máximo (6 - 40 segundos)	El tiempo máximo puede ajustarse para asegurarse de que la información antigua no circule eternamente por rutas redundantes en la red, lo cual evita la propagación efectiva de nueva información. Este valor, configurado por el Puente Raíz, ayudará a determinar que el switch tiene valores de configuración del árbol de expansión coherentes con otros dispositivos del LAN enlazado. Si el valor caduca sin que se ha haya recibido aún ningún BPDU procedente del Puente Raíz, el switch empezará a enviar su propio BPDU a los demás switches para obtener la autorización para convertirse en Puente Raíz. Si su switch tiene el Identificador de Puente más bajo, se convertirá en Puente Raíz. El usuario puede elegir una duración de entre *6* y *40* segundos. El valor predeterminado es *20*.
Puente de tiempo de saludo (1 - 10 segundos)	El Tiempo de saludo puede ajustarse de *1* a *10* segundos. Se trata del intervalo entre dos transmisiones de paquetes BPDU enviados por el Puente Raíz para indicar a los demás switches que efectivamente es el Puente Raíz.
Puente de retraso de envío (4 - 30 segundos)	El Retraso de envío puede oscilar entre *4* y *30* segundos. Los puertos del switch permanecen este tiempo en estado de escucha mientras pasa del estado de bloqueo al de envío.
Puente de prioridad (0-6144)	Se utiliza para especificar el nivel de prioridad del Puente STP. La prioridad del puente puede ajustarse de 0 a 6144.

Versión STP	Utilice el menú desplegable para elegir la versión STP que desea implementar en el switch. Existen tres opciones: *Compatibilidad de STP* – Seleccione este parámetro para configurar el Protocolo del Árbol de Expansión (STP) en el switch de forma global. *RSTP* - Seleccione este parámetro para configurar el Protocolo del Árbol de expansión rápida (RSTP) en el switch de forma global. *MSTP* – Seleccione este parámetro para configurar el Protocolo del Árbol de expansión múltiple (MSTP) en el switch de forma global.
Recuento TX Hold (1-10)	Se utiliza para configurar el número máximo de paquetes Hello que se transmiten por intervalo. El recuento puede especificarse de *1* a *10*. El valor predeterminado es *3.*

Haga clic en **Aplicar** para aplicar los cambios realizados.

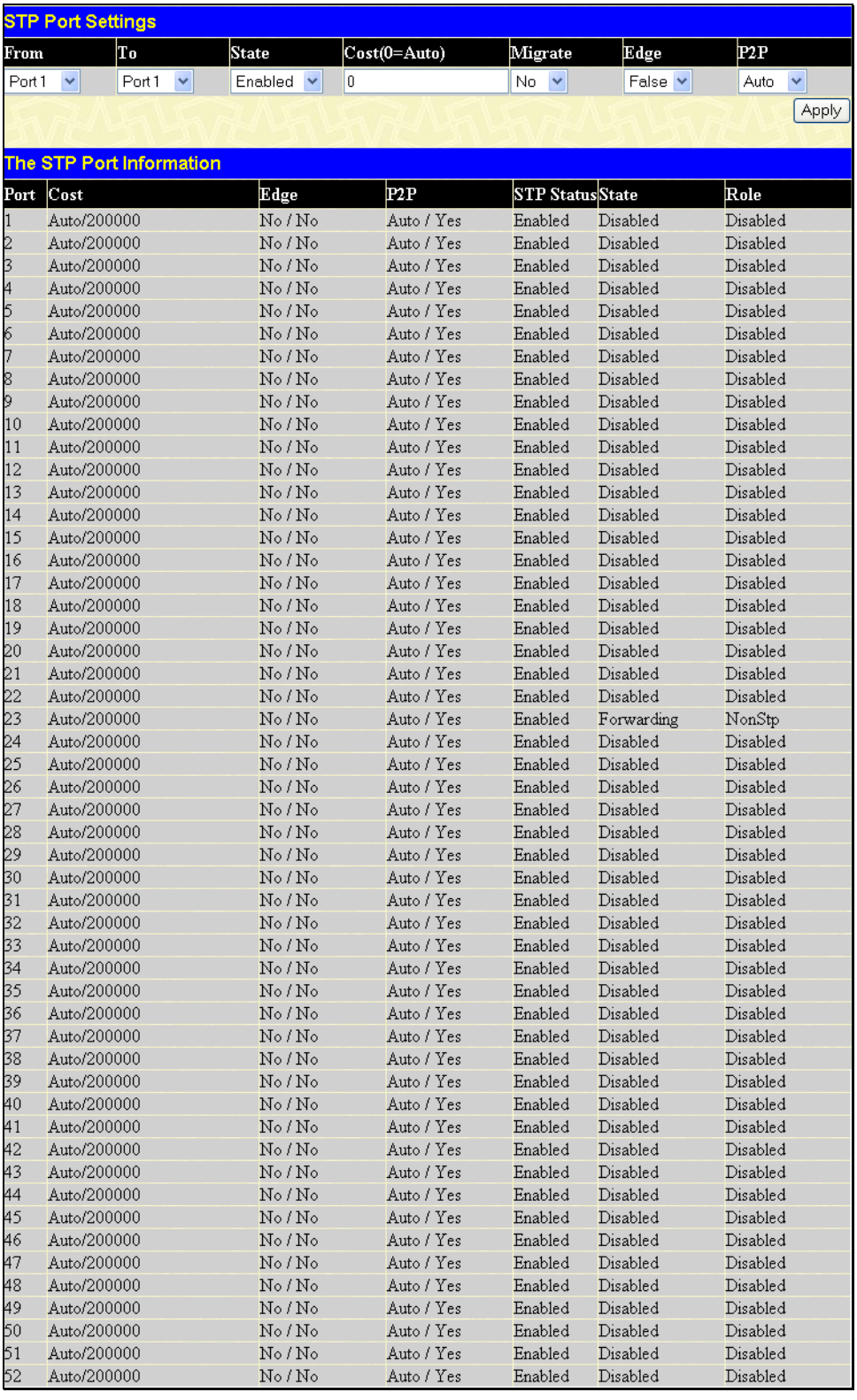
NOTA: El Tiempo de saludo no puede superar el Tiempo máximo. De lo contrario, se produciría un error de configuración. Observe las fórmulas siguientes a la hora de configurar los parámetros anteriores:

Tiempo máx. ≤ 2 x (Retraso de envío - 1 segundo)

Tiempo máx.≥ 2 x (Tiempo de saludo + 1 segundo)

Configuración de los puertos STP

El STP puede configurarse puerto por puerto. Para visualizar la ventana siguiente haga clic en **Características de Capa 2 > Árbol de expansión > Configuración de los puertos STP**:



STP Port Settings

From	To	State	Cost(0=Auto)	Migrate	Edge	P2P
Port 1	Port 1	Enabled	0	No	False	Auto

Apply

The STP Port Information

Port	Cost	Edge	P2P	STP Status	State	Role
1	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
2	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
3	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
4	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
5	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
6	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
7	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
8	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
9	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
10	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
11	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
12	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
13	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
14	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
15	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
16	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
17	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
18	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
19	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
20	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
21	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
22	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
23	Auto/200000	No / No	Auto / Yes	Enabled	Forwarding	NonStp
24	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
25	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
26	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
27	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
28	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
29	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
30	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
31	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
32	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
33	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
34	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
35	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
36	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
37	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
38	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
39	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
40	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
41	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
42	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
43	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
44	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
45	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
46	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
47	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
48	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
49	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
50	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
51	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled
52	Auto/200000	No / No	Auto / Yes	Enabled	Disabled	Disabled

Figura 7- 15. Ventana de Configuración de los puertos STP

Además de configurar los parámetros del Árbol de expansión para utilizarlo a nivel del switch, el dispositivo permite configurar grupos de puertos. Cada uno de estos grupos de puertos tendrá su propio Árbol de expansión y necesitará algunas de sus propias opciones de configuración. Un grupo de STP utilizará los parámetros a nivel de switch introducidos arriba, añadiendo la **Prioridad de los puertos** y **Coste de los puertos**.

ESPAÑOL

El Árbol de expansión de un Grupo STP funciona del mismo modo que el Árbol de expansión a nivel de switch, pero el concepto de puente raíz se sustituye por el concepto de puerto raíz. Un puerto raíz es un puerto del grupo elegido de acuerdo con la prioridad y el coste de los puertos para ser la conexión con la red del grupo. Los enlaces redundantes quedarán bloqueados, al igual que los enlaces redundantes estarán bloqueados a nivel de switch.

El STP a nivel del switch bloquea los enlaces redundantes entre switches (y dispositivos de red similares). El STP a nivel de puertos bloqueará los enlaces redundantes dentro de un Grupo STP.

Es recomendable definir un Grupo STP para que corresponda con un grupo VLAN de puertos.

Pueden configurarse los campos siguientes:

Parámetro	Descripción
De/A	Un grupo de puertos consecutivos puede configurarse empezando por el puerto seleccionado.
Estado	Varíe entre *Desactivado* y *Activado* para aplicar el envío de paquetes BPDU.
Coste (*0 = Auto)*	**Coste externo** – Define un sistema métrico que indica el coste relativo del envío de paquetes a la lista de puertos especificados. El coste de los puertos puede configurarse automáticamente o como valor métrico. El valor predeterminado es *0* (auto). • *0 (auto)*: Ajustar *0* como coste externo configurará automáticamente la velocidad para el envío de paquetes al puerto o puertos especificados de la lista de eficiencia óptima. Coste del puerto predeterminado: puerto de 100Mbps = *200000*. Puerto gigabit = *20000*. • *valor 1-2000000* – Defina un valor entre *1* y *2000000* para determinar el coste externo. Cuanto más bajo sea el número, mayor será la probabilidad de que el puerto sea elegido para enviar los paquetes.
Tiempo de saludo	Puede ajustarse entre *1* y *10* segundos. Se trata del intervalo entre dos transmisiones de paquetes BPDU enviadas por el Puente Raíz para indicar a los demás switches que es efectivamente el Puente Raíz.
Migrar	Configurar este parámetro como *Sí* hará que todos los puertos envíen paquetes BPDU a otros puentes, solicitando información en su configuración STP. Si el switch está configurado para RSTP, el puerto podrá migrar de 802.1d STP a 802.1w RSTP. La migración debería configurarse como Sí en los puertos conectados a las estaciones o segmentos de red capaces de actualizarse a 802.1w RSTP en la totalidad o en parte del segmento.
Borde	La selección del parámetro *Verdadero* designa el puerto como puerto de borde. Los puertos de borde no pueden crear bucles, aunque un puerto de borde puede perder ese estatus si un cambio de la topología crea un entorno potencial para un bucle. Un puerto de borde normalmente no debe recibir paquetes BPD. Y en caso de que se reciba un paquete BPDU, el puerto de borde perderá automáticamente su estatus. La selección del parámetro *Falso* indica que el puerto no tiene el estatus de puerto de borde.
P2P	La selección del parámetro *Verdadero* indica un enlace compartido de punto a punto (P2P). Los puertos P2P son similares a los puertos de borde, aunque tienen la limitación de que un puerto P2P debe funcionar en full-duplex. Al igual que los puertos de borde, los puertos P2P realizan la transición al estado de envío rápidamente, por lo que se benefician del RSTP. Un valor p2p *Falso* indica que el puerto no puede tener un estatus p2p. El valor *Auto* permite que el puerto tenga el estatus p2p siempre que sea posible y funcione como si el estatus p2p fuese verdadero. En caso de que el puerto no pueda mantener ese estatus (por ejemplo, si el puerto debe funcionar en half-duplex), el estado p2p cambiará para funcionar como si el valor p2p fuera *Falso*. La configuración predeterminada para este parámetro es *Verdadero*.

Haga clic en **Aplicar** para aplicar los cambios realizados.

Apartado 8

CoS

- *Prioridad predeterminada (802.1p)*
- *Prioridad de usuario (802.1p)*

El switch es compatible con la Calidad de Servicio de cola de prioridad 802.1p. La sección siguiente expone la aplicación de CoS (Calidad de Servicio) y las ventajas de utilizar la cola de prioridad 802.1p.

Comprender la prioridad IEEE 802.1p

El etiquetado de prioridad es una función definida por el estándar IEEE 802.1p pensada para ofrecer los medios para gestionar el tráfico de una red en la que se pueden transmitir muchos tipos diferentes de datos simultáneamente. Su objetivo consiste en aliviar los problemas asociados a la entrega de datos en momentos críticos en redes sobrecargadas. La calidad de las aplicaciones que dependen de dichos datos, como las videoconferencias, pueden sufrir graves efectos a causa de pequeños retrasos en la transmisión.

Los dispositivos de red que cumplen con el estándar IEEE 802.1p tienen la capacidad de reconocer el nivel de prioridad de los paquetes de datos. Estos dispositivos también pueden asignar una etiqueta de prioridad a los paquetes, o bien retirarlas. Esta etiqueta de prioridad determina la rapidez del paquete y la cola a la que se ha asignado.

Las etiquetas de prioridad tienen valores del 0 al 7, en las que el 0 es el nivel de prioridad más bajo y 7, el más alto. La etiqueta de prioridad más alta (7) se suele utilizar únicamente para datos asociados a aplicaciones de vídeo o audio, que son sensibles a los más mínimos retrasos, o para datos de usuarios específicos cuyas transmisiones de datos requieren una consideración especial.

El switch permite un nivel superior de personalización de cómo los paquetes de datos con etiquetas de prioridad se tratan en su red. El uso de colas para gestionar los datos con etiquetas de prioridad le permitirá especificar su prioridad relativa para satisfacer las necesidades de su red. Pueden darse situaciones en las que resulte positivo agrupar dos o más paquetes con etiquetas diferentes en la misma cola. No obstante, generalmente es recomendable que la cola de prioridad más alta, la Cola 3, se reserve para paquetes de datos con un valor de prioridad de 7. Los paquetes a los que no se les ha asignado ningún valor de prioridad se colocan en la Cola 0, de modo que se les adjudica el nivel más bajo de prioridad para la entrega.

En el switch se emplea un sistema de turno rotativo ponderado para determinar la velocidad a la que las colas se vacían de paquetes. La velocidad utilizada para vaciar las colas es de 4:1, lo cual significa que la cola de prioridad más alta, la Cola 3, vaciará 4 paquetes por cada paquete vaciado de la Cola 0.

Recuerde que las opciones de configuración de las colas de prioridad del switch son para todos los puertos, y todos los dispositivos conectados al switch se verán afectados. Este sistema de colas de prioridad será especialmente ventajoso si su red emplea switches con capacidad de asignar etiquetas de prioridad.

Ventajas de CoS

CoS es una aplicación de la norma IEEE 802.1p que ofrece a los administradores de redes un método para reservar ancho de banda para funciones importantes que requieren un gran ancho de banda o tener una gran prioridad, como los servicios de VoIP (protocolo de telefonía por internet), aplicaciones de navegación web, aplicaciones de servidores de archivos o videoconferencias. No sólo puede crearse un ancho de banda mayor, sino que también puede limitarse otro tipo de tráfico menos importante de manera que el ancho de banda que sobra puede ahorrarse. El switch tiene colas de hardware independientes en cada puerto físico para las que se pueden distribuir, y a su vez priorizar, paquetes de diversas aplicaciones. Consulte la distribución siguiente para comprobar cómo el switch aplica las colas de prioridad básicas de 802.1P.

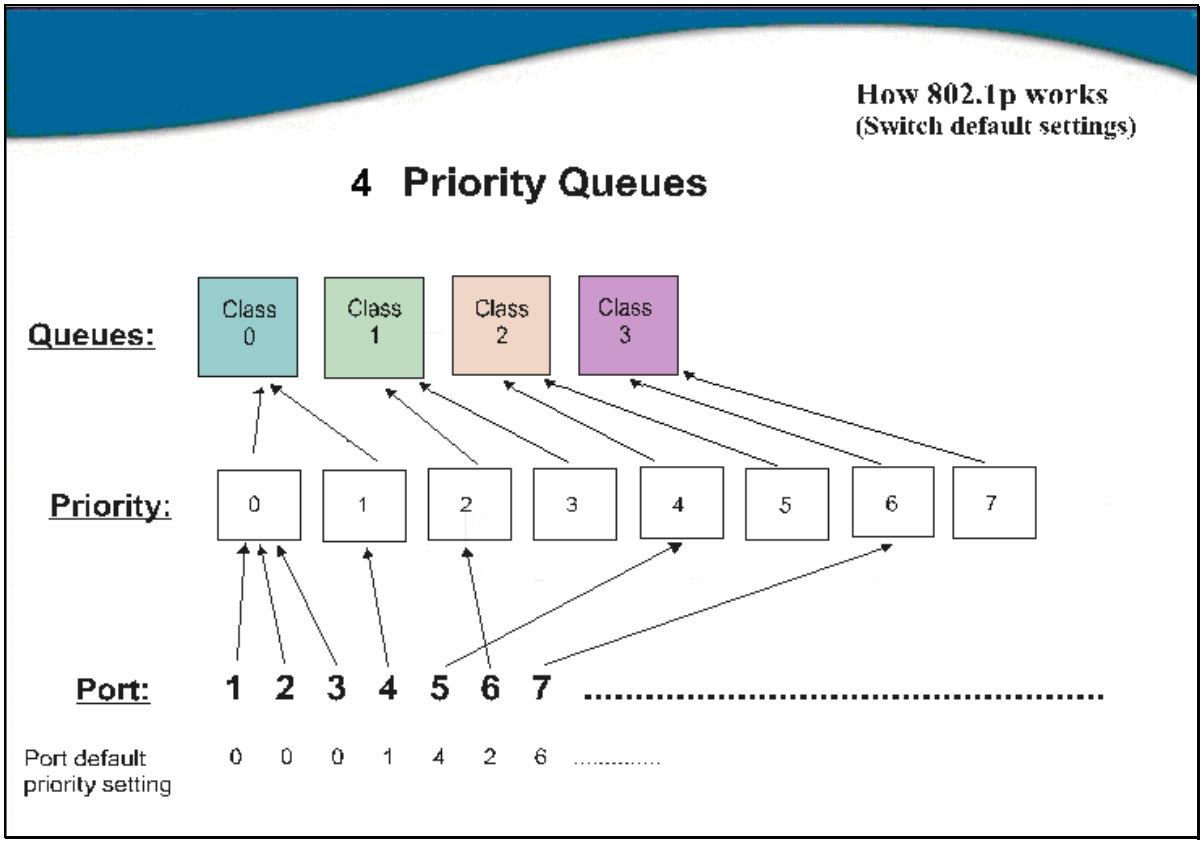


Figura 8- 1. Un ejemplo de la distribución de prioridad predeterminada de CoS en el switch

La imagen anterior muestra la distribución de prioridad predeterminada del switch. La Clase 3 tiene la prioridad más alta de las cuatro clases de servicio de prioridad del switch. Para aplicar la CoS, el usuario deberá ordenar al switch que examine el encabezamiento de un paquete para ver si contiene la etiqueta de identificación adecuada. A continuación, el usuario deberá enviar esos paquetes etiquetados a clases de servicio determinadas del switch, donde serán vaciadas en función de la prioridad.

Por ejemplo, imaginemos que un usuario desea celebrar una videoconferencia entre dos ordenadores en ubicaciones remotas. El administrador puede añadir etiquetas de prioridad a los paquetes de vídeo que se envían utilizando los comandos de Perfil de Acceso. A continuación, en el extremo de recepción, el administrador ordena al switch que examine los paquetes para esta etiqueta, adquiere los paquetes etiquetados y los distribuye a una cola de clase del switch. A su vez, el administrador configura una prioridad para esa cola de modo que se vacíe antes de que se envíe otro paquete. El resultado es que el usuario final recibe todos los paquetes enviados lo más rápidamente posible, y por tanto, la cola se prioriza y se favorece un flujo de paquetes ininterrumpido, lo cual optimiza el uso de un ancho de banda disponible para videoconferencias.

Comprender las CoS

El switch tiene cuatro clases de servicio de prioridad y éstas se clasifican como 3 para la clase alta y como 0 para la más baja. Las ocho etiquetas de prioridad, especificadas en IEEE 802.1p, corresponden a las siguientes clases de servicio de prioridad del switch:

- Se asigna la prioridad 0 a la clase Q1 del switch.
- Se asigna la prioridad 1 a la clase Q0 del switch.
- Se asigna la prioridad 2 a la clase Q0 del switch.
- Se asigna la prioridad 3 a la clase Q1 del switch.
- Se asigna la prioridad 4 a la clase Q2 del switch.
- Se asigna la prioridad 5 a la clase Q2 del switch.
- Se asigna la prioridad 6 a la clase Q3 del switch.
- Se asigna la prioridad 7 a la clase Q3 del switch.

Para una programación estricta basada en la prioridad, se transmiten primero los paquetes que pertenecen a las clases de servicio de prioridad más alta. Las múltiples clases de servicio de prioridad estricta se vacían en función de las etiquetas de prioridad. Sólo cuando estas clases están vacías se transmiten los paquetes de prioridad más baja.

Para las colas de turno rotativo ponderado, el número de paquetes enviados desde cada cola de prioridad depende de la ponderación asignada. Para la configuración de ocho colas CoS, A~H con su respectivo valor de ponderación (8~1), los paquetes se envían en la secuencia siguiente: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

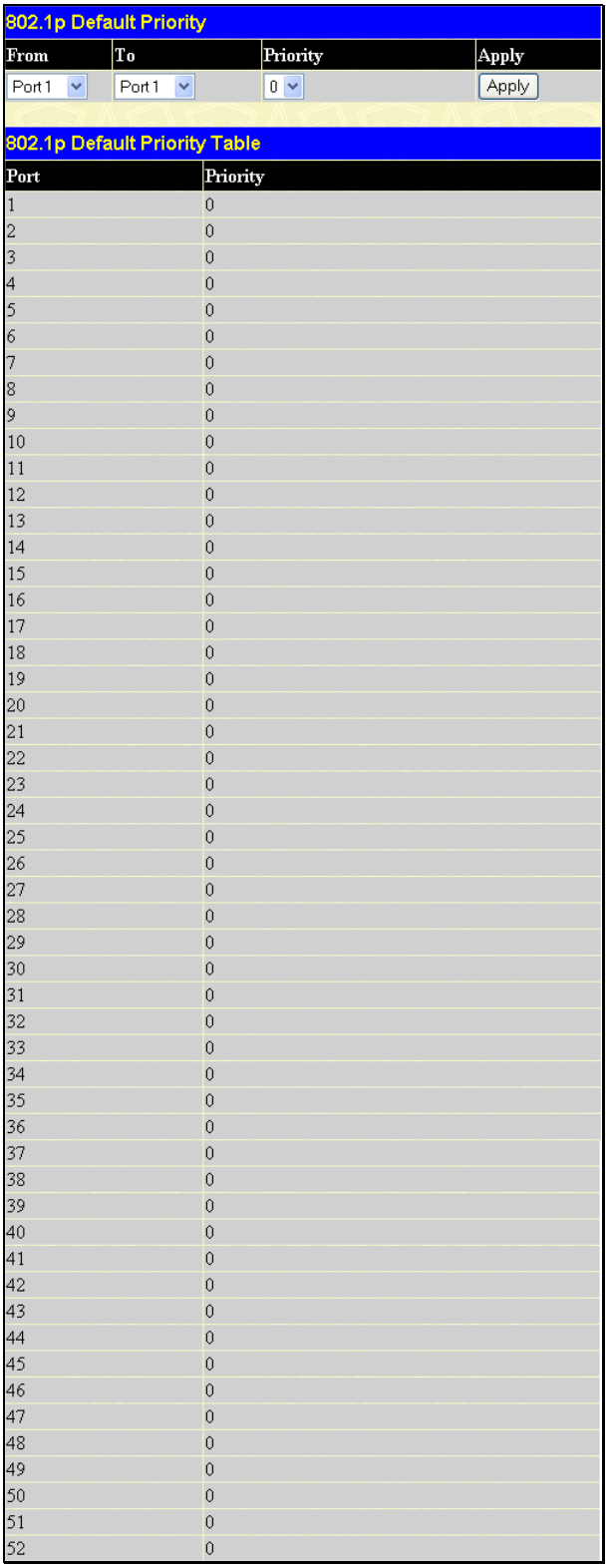
Para las colas de turno rotativo ponderado, si cada cola CoS tiene el mismo valor de ponderación, cada cola CoS tendrá la misma oportunidad para enviar paquetes, igual que las colas de turno rotativo.

Para las colas de turno rotativo ponderado, si la ponderación para una CoS se configura en 0, continuarán procesando los paquetes desde esta CoS hasta que no haya más paquetes para ella. Las demás colas CoS a las que se les ha asignado un valor diferente de cero, y dependiendo de la ponderación, seguirán un esquema de turno rotativo ponderado.

Recuerde que el switch tiene cuatro colas de prioridad configurable (y cuatro Clases de Servicio) por cada puerto del switch.

Prioridad predeterminada (802.1p)

El switch permite asignar una prioridad 802.1p predeterminada a cada puerto del dispositivo. En la carpeta **CoS**, haga clic en **Prioridad predeterminada (802.1p)** para visualizar la ventana siguiente.



802.1p Default Priority

From	To	Priority	Apply
Port 1	Port 1	0	Apply

802.1p Default Priority Table

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
29	0
30	0
31	0
32	0
33	0
34	0
35	0
36	0
37	0
38	0
39	0
40	0
41	0
42	0
43	0
44	0
45	0
46	0
47	0
48	0
49	0
50	0
51	0
52	0

Figura 8- 2. Ventana de Prioridad predeterminada (802.1p)

Esta ventana permite asignar una prioridad 802.1p predeterminada a cualquier puerto del switch. Las etiquetas de prioridad están numeradas de *0*, que tiene la prioridad más baja, a *7*, con la prioridad más alta. Para aplicar una nueva prioridad predeterminada, elija un rango de puertos utilizando los menús desplegables **De** y **A** y, después, introduzca un valor de prioridad de *0* a *7* en el campo **Prioridad**. A continuación, haga clic en **Aplicar** para aplicar la configuración.

Prioridad de usuario (802.1p)

Cuando se utiliza un mecanismo de prioridad 802.1p, se examina el paquete para encontrar la presencia de una etiqueta de prioridad 802.1p válida. Si dicha etiqueta está presente, el paquete se asigna a una cola de salida programable basada en el valor de la prioridad etiquetada. La prioridad etiquetada puede asignarse a cualquiera de las colas disponibles.

El switch permite asignar una clase de servicio a cada una de las prioridades 802.1p. En la carpeta **CoS**, haga clic en **Prioridad de usuario (802.1p)** para visualizar la ventana siguiente.

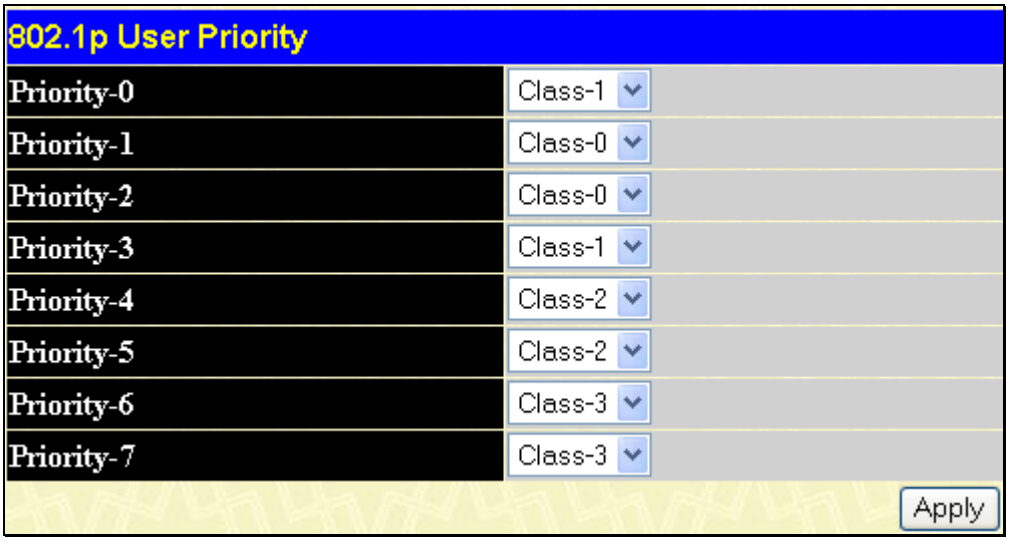


Figura 8- 3. Ventana de Prioridad de usuario (802.1p)

Una vez asignada una prioridad a los grupos de puertos del switch, ya puede asignar esta Clase a cada uno de los cuatro niveles de prioridades 802.1p. Haga clic en **Aplicar** para guardar los cambios.

Apartado 9

Seguridad

- *802.1X*

802.1X

Control de acceso basado en puertos 802.1x / MAC

La norma IEEE 802.1x es una medida de seguridad para autorizar y autenticar a los usuarios para que accedan a los diversos dispositivos con o sin cables en una Red de Área Local determinada utilizando un modelo de control de acceso basado en Cliente y Servidor. Esto se consigue utilizando un servidor RADIUS para autenticar a los usuarios que tratan de acceder a una red mediante la transmisión entre el Cliente y el Servidor del Protocolo de Autenticación Extensible por paquetes LAN (EAPOL). La figura siguiente representa un paquete EAPOL básico:

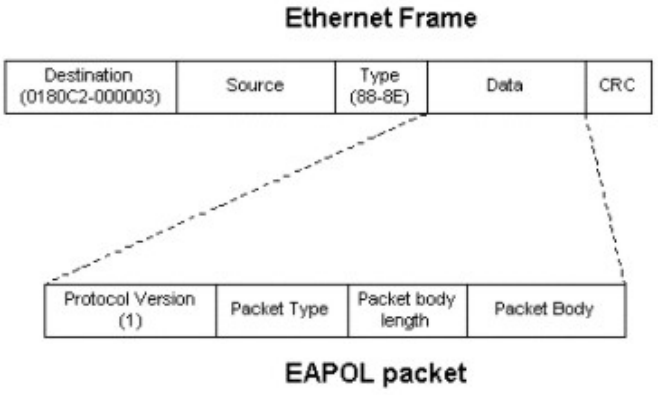


Figura 9- 1. Paquete EAPOL

Utilizando este método, los dispositivos no autorizados no pueden conectarse a una LAN a través de un puerto al que el usuario está conectado. Los paquetes EAPOL son el único tráfico que puede transmitirse a través del puerto específico hasta que se otorgue la autorización. El método de Control de acceso 802.1x tiene tres funciones, y cada una de ellas es vital a la hora de crear y mantener un método de seguridad de control de acceso estable y apropiado.

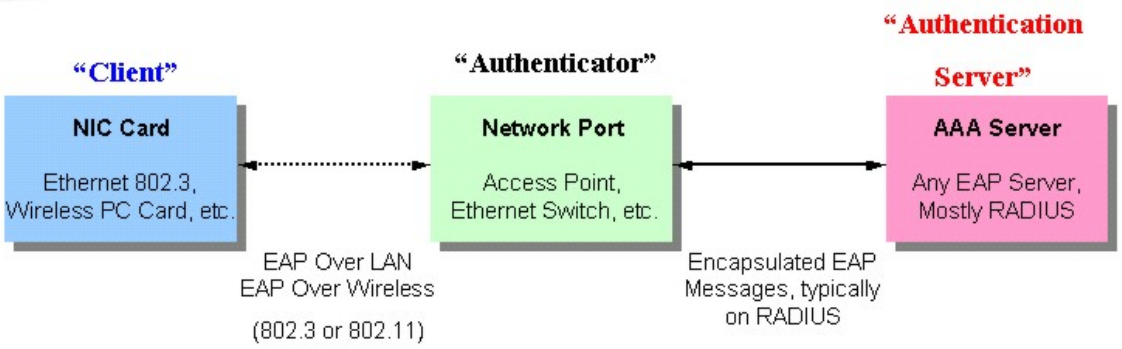


Figura 9- 2. Las tres funciones de 802.1x

La sección siguiente expone detalladamente las tres funciones del Cliente, del Autenticador y del Servidor de Autenticación.

Servidor de Autenticación

El Servidor de Autenticación es un dispositivo remoto conectado a la misma red que el Cliente y el Autenticador, debe tener instalado el programa de un Servidor RADIUS y debe estar configurado correctamente en el Autenticador (switch). El Servidor de Autenticación (RADIUS) debe autenticar a los Clientes conectados a un puerto del switch antes de obtener los servicios que el switch ofrece en la red LAN. La función del Servidor de Autenticación consiste en certificar la identidad del Cliente que intenta acceder a la red intercambiando información de seguridad entre el servidor RADIUS y el Cliente mediante paquetes EAPOL y, a su vez, informa al switch sobre si al Cliente se le concede o no acceso a la red LAN y/o a los servicios del switch.

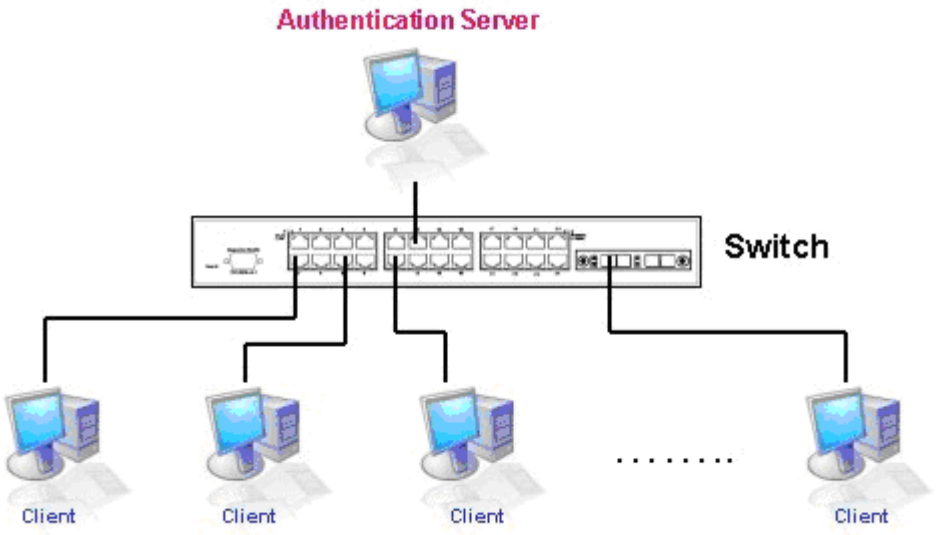


Figura 9- 3. El Servidor de Autenticación

Autenticador

El Autenticador (el switch) es un intermediario entre el Servidor de Autenticación y el Cliente. El Autenticador tiene dos funciones cuando se utiliza 802.1x. La primera consiste en solicitar información de certificación del Cliente mediante paquetes EAPOL, que es la única información que se permite que pase por el Autenticador antes de que se conceda el acceso al Cliente. La segunda función del Autenticador es la de verificar la información recogida del Cliente con el Servidor de Autenticación y transmitirla de vuelta al Cliente.

Para configurar el Autenticador correctamente deben seguirse los tres pasos siguientes:

1. El Estado 802.1x debe estar *Activado* (**Herramienta de administración web**)
2. Las opciones de configuración 802.1x deben implementarse por puertos (**Seguridad** / **802.1x** / **Configurar Opciones del Autenticador 802.1X y Opciones de capacidad 802.1X**)
3. El switch debe tener configurado un servidor RADIUS (**Seguridad** / **802.1x** / **Servidor RADIUS**)

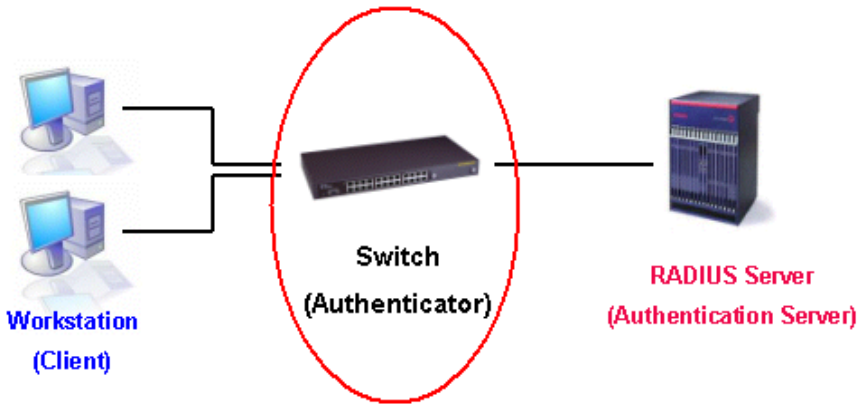


Figura 9- 4. El Autenticador

Cliente

El Cliente no es más que la estación final que desea acceder a la red LAN o a los servicios del switch. Todas las estaciones finales deben tener instalado el software compatible con el protocolo 802.1x. Para los usuarios de Windows XP, ese software está incluido en el sistema operativo. Los demás usuarios deberán obtener el software cliente 802.1x de fuentes externas. El Cliente solicitará acceso a la red LAN y/o al switch mediante paquetes EAPOL y a su vez responderá a las solicitudes del switch.

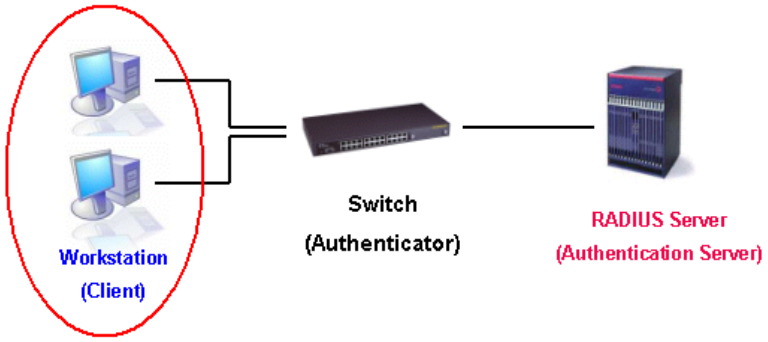


Figura 9- 5. El Cliente

Proceso de autenticación

Utilizando las tres funciones expuestas arriba, el protocolo 802.1x ofrece un método estable y seguro de autorizar y autenticar a los usuarios que tratan de acceder a la red. Sólo se permite el paso del tráfico EAPOL por el puerto especificado antes de que se realice una autenticación satisfactoriamente. Este puerto queda "bloqueado" hasta el momento en que al Cliente con el nombre de usuario y la contraseña correctos (y la dirección MAC si el 802.1x está activado por dicha dirección) se le concede el acceso y, por tanto, "desbloquea" el puerto. Una vez desbloqueado, se permite el tráfico habitual por ese puerto. La figura siguiente ofrece una explicación más detallada sobre cómo se desarrolla el proceso de autenticación entre las tres funciones expuestas arriba.

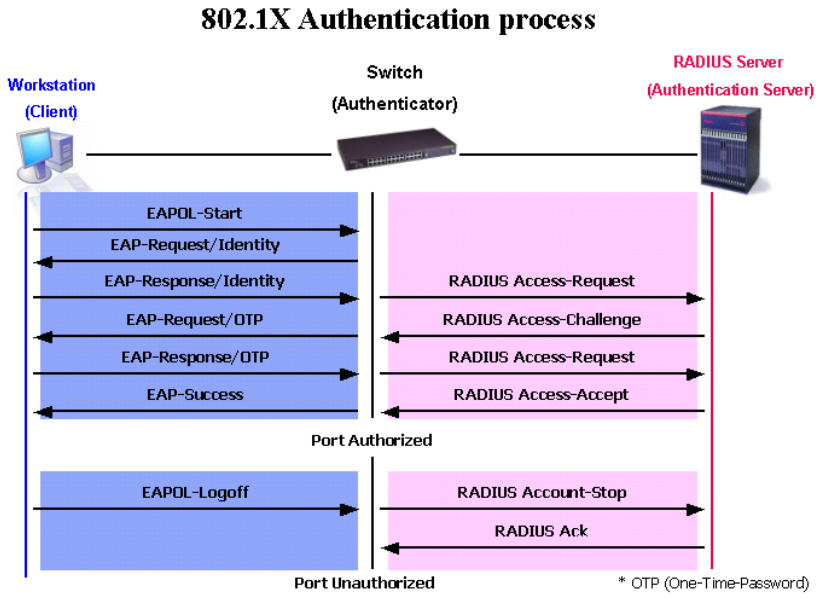


Figura 9- 6. Proceso de autenticación 802.1x

La implementación del 802.1x permite a los administradores de la red elegir entre dos tipos de Control de acceso utilizados en el switch:

1. Control de acceso basado en puertos: este método requiere autenticar sólo un usuario por puerto por parte de un servidor RADIUS remoto para permitir el acceso a la red a los usuarios restantes del mismo puerto.
2. Control de acceso basado en MAC: mediante este método, el switch memorizará automáticamente hasta dieciséis direcciones MAC por puerto y las configurará en la lista. Cada dirección MAC deberá ser autenticada por el switch mediante un servidor RADIUS remoto antes de permitirle el acceso a la red.

Comprender el Control de acceso a la red basado en puertos 802.1x y en MAC

La intención original del desarrollo del 802.1x era potenciar la característica de punto a punto de las redes LAN. Como cualquier segmento LAN individual de dichas infraestructuras no tiene más de dos dispositivos conectados, uno de ellos es un Puerto Puente. Este tipo de puerto detecta los casos que indican la conexión a un dispositivo activo en el extremo remoto del enlace, o un dispositivo activo que pasa a estar inactivo. Estos casos pueden utilizarse para controlar el estado de autorización del puerto e iniciar el proceso de autenticación del dispositivo conectado si el puerto no dispone de la autorización. Éste es el Control de acceso a la red basado en puertos.

Control de acceso a la red basado en puertos

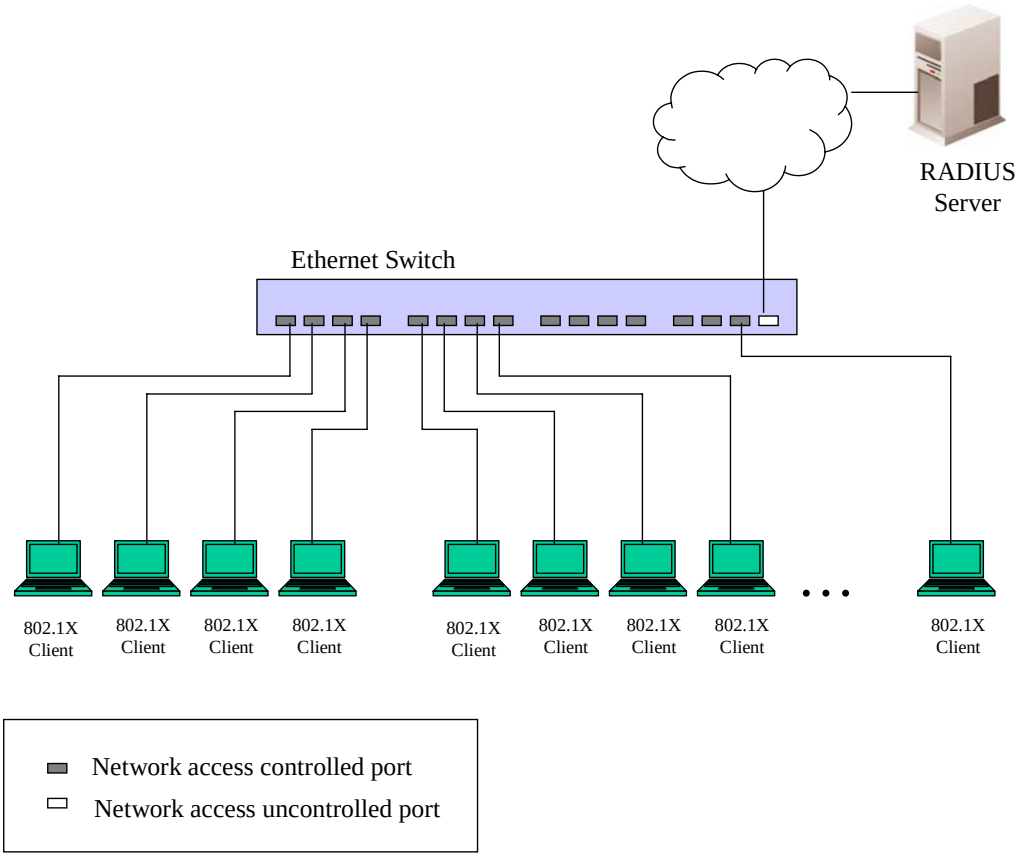


Figura 9- 7. Ejemplo de la Configuración habitual basada en puertos

Una vez que el dispositivo conectado se ha autenticado correctamente, el puerto adquiere el estatus de Autorizado, de modo que el tráfico posterior que pase por el puerto no estará sujeto a la restricción de control de acceso hasta que se produzca una situación que despoje al puerto de autorización. Por tanto, si el puerto está conectado a un segmento LAN compartido con más de un dispositivo conectado, la autenticación correcta de uno de los dispositivos conectados concederá el acceso a la LAN a todos los dispositivos del segmento compartido. Naturalmente, la seguridad que hay en este tipo de situaciones puede ser objeto de ataques.

Control de acceso a la red basado en MAC

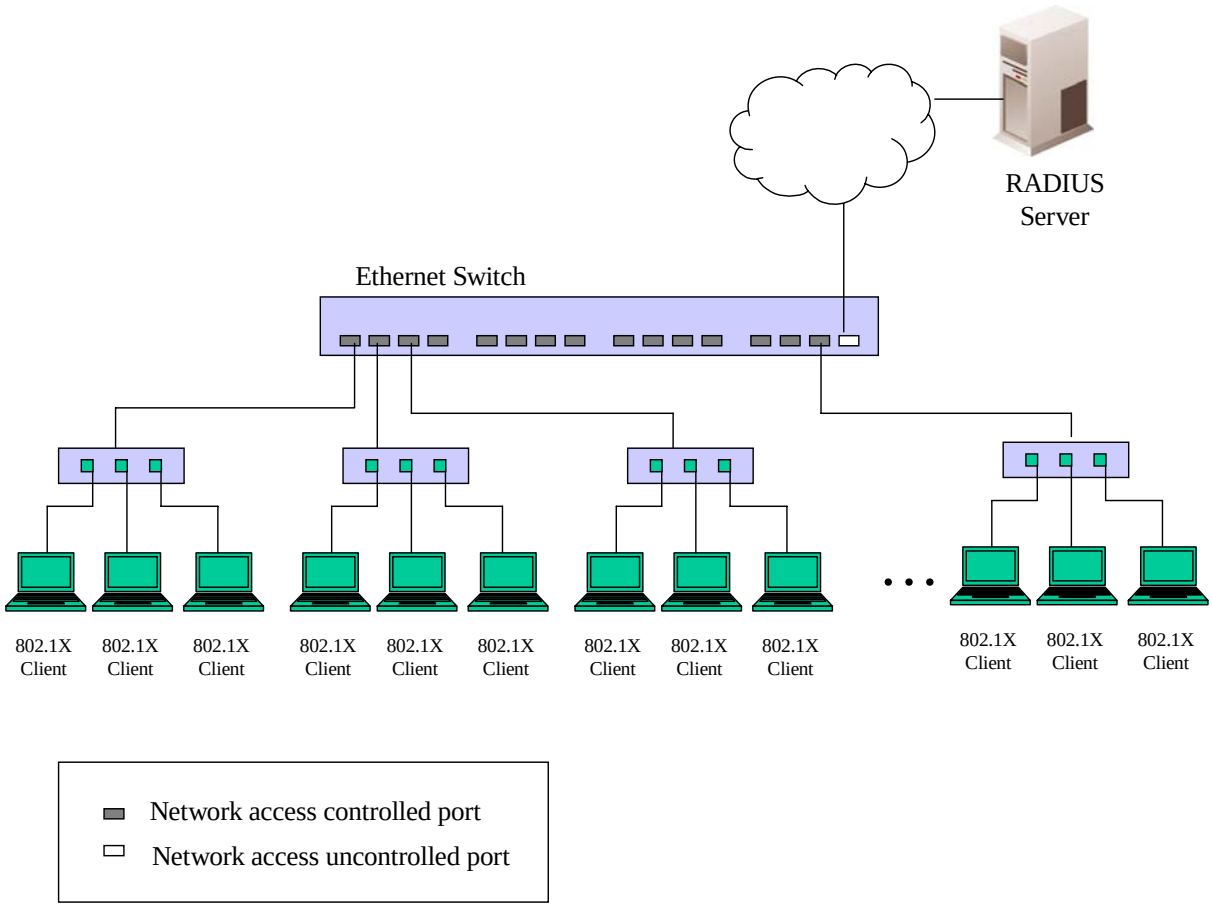


Figura 9- 8. Ejemplo de la Configuración habitual basada en MAC

Para utilizar correctamente el 802.1x en un segmento LAN compartido, es necesario crear puertos “lógicos”, uno para cada dispositivo conectado que requiera acceso a la red LAN. El switch considerará que el puerto físico simple conectado al segmento compartido está formado por un conjunto de puertos lógicos distintos, y cada uno de ellos controlado de forma independiente del punto de vista de los intercambios EAPOL y el estado de autorización. El switch memoriza las direcciones MAC individuales de cada dispositivo conectado y crea un puerto lógico que el dispositivo conectado puede utilizar después para comunicarse con la red LAN a través del switch.

Opciones del Autenticador 802.1x

Para configurar las Opciones del Autenticador 802.1X, haga clic en **Seguridad > 802.1X > Opciones del Autenticador 802.1X**:

802.1X Authenticator Settings

Port	AdmDir	Ctrl Stat	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	auto	30	60	30	30	2	3600	no
2	both	auto	30	60	30	30	2	3600	no
3	both	auto	30	60	30	30	2	3600	no
4	both	auto	30	60	30	30	2	3600	no
5	both	auto	30	60	30	30	2	3600	no
6	both	auto	30	60	30	30	2	3600	no
7	both	auto	30	60	30	30	2	3600	no
8	both	auto	30	60	30	30	2	3600	no
9	both	auto	30	60	30	30	2	3600	no
10	both	auto	30	60	30	30	2	3600	no
11	both	auto	30	60	30	30	2	3600	no
12	both	auto	30	60	30	30	2	3600	no
13	both	auto	30	60	30	30	2	3600	no
14	both	auto	30	60	30	30	2	3600	no
15	both	auto	30	60	30	30	2	3600	no
16	both	auto	30	60	30	30	2	3600	no
17	both	auto	30	60	30	30	2	3600	no
18	both	auto	30	60	30	30	2	3600	no
19	both	auto	30	60	30	30	2	3600	no
20	both	auto	30	60	30	30	2	3600	no
21	both	auto	30	60	30	30	2	3600	no
22	both	auto	30	60	30	30	2	3600	no
23	both	auto	30	60	30	30	2	3600	no
24	both	auto	30	60	30	30	2	3600	no
25	both	auto	30	60	30	30	2	3600	no
26	both	auto	30	60	30	30	2	3600	no
27	both	auto	30	60	30	30	2	3600	no
28	both	auto	30	60	30	30	2	3600	no
29	both	auto	30	60	30	30	2	3600	no
30	both	auto	30	60	30	30	2	3600	no
31	both	auto	30	60	30	30	2	3600	no
32	both	auto	30	60	30	30	2	3600	no
33	both	auto	30	60	30	30	2	3600	no
34	both	auto	30	60	30	30	2	3600	no
35	both	auto	30	60	30	30	2	3600	no
36	both	auto	30	60	30	30	2	3600	no
37	both	auto	30	60	30	30	2	3600	no
38	both	auto	30	60	30	30	2	3600	no
39	both	auto	30	60	30	30	2	3600	no
40	both	auto	30	60	30	30	2	3600	no
41	both	auto	30	60	30	30	2	3600	no
42	both	auto	30	60	30	30	2	3600	no
43	both	auto	30	60	30	30	2	3600	no
44	both	auto	30	60	30	30	2	3600	no
45	both	auto	30	60	30	30	2	3600	no
46	both	auto	30	60	30	30	2	3600	no
47	both	auto	30	60	30	30	2	3600	no
48	both	auto	30	60	30	30	2	3600	no
49	both	auto	30	60	30	30	2	3600	no
50	both	auto	30	60	30	30	2	3600	no
51	both	auto	30	60	30	30	2	3600	no
52	both	auto	30	60	30	30	2	3600	no

Figura 9- 9. Ventana de Opciones del Autenticador 802.1x

ESPAÑOL

Para configurar las opciones por puertos, haga clic en el enlace **Puertos** correspondiente, que mostrará la tabla de configuración siguiente:

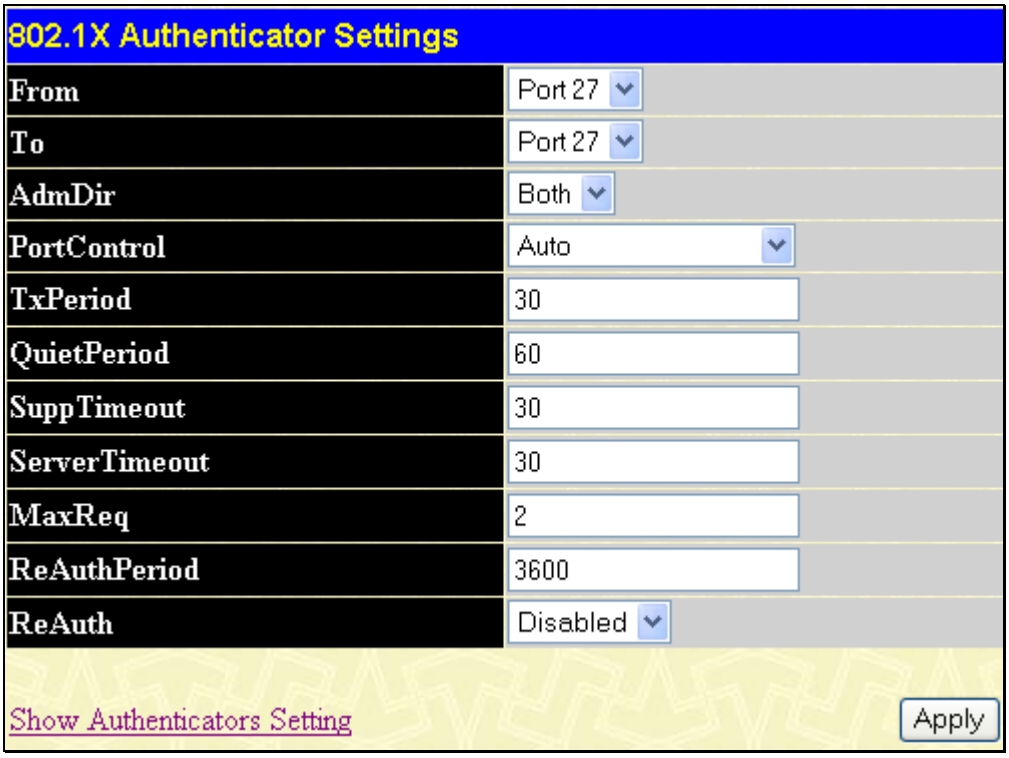


Figura 9- 10. Ventana de Opciones del Autenticador 802.1X (Modificar)

Esta ventana permite a los usuarios configurar las características siguientes:

Parámetro	Descripción
[De/A]	Introduzca el puerto o puertos que desea configurar.
Dirección administrativa (AdmDir)	Configura la dirección controlada de forma administrativa en posición *En* o *Ambas*. Si se selecciona *En*, el control sólo se ejerce sobre el tráfico entrante por el puerto seleccionado en el primer campo. Si se selecciona *Ambas*, el control se ejerce sobre el tráfico entrante y saliente del puerto controlado que ha seleccionado en el primer campo.
Control de puertos (PortControl)	Permite controlar el estado de autorización de los puertos. Seleccione *Fuerza autorizada* para desactivar el 802.1X y hacer que el puerto pase a un estado autorizado sin necesidad de intercambio de autenticación. Esto significa que el puerto transmite y recibe tráfico normal sin autenticación basada en 802.1X- del cliente. Si se selecciona *Fuerza no autorizada*, el puerto permanecerá en un estado no autorizado e ignorará todos los intentos de autenticación del cliente. El switch no ofrece servicio de autenticación al cliente a través de la interfaz. Si se selecciona *Auto*, activará el 802.1X y hará que el puerto empiece en el estado no autorizado, lo cual sólo permite que se envíen y reciban frames EAPOL a través del puerto. El proceso de autenticación empieza cuando el estado del enlace del puerto va de abajo a arriba, o cuando se recibe un frame EAPOL de inicio. Entonces, el switch solicita la identidad del cliente y empieza a transmitir mensajes de autenticación entre el cliente y el servidor de autenticación. La opción predeterminada es *Auto*.
PeríodoTx (TxPeriod)	Configura el PeríodoTx de tiempo para la máquina de estados PAE del autenticador. Este valor determina el período de una Solicitud EAP/Paquete de identidad transmitido al cliente. El valor predeterminado es *30* segundos.

Período en espera (QuietPeriod)	Permite configurar los segundos que el switch permanece en estado de "Espera" después de un error en el intercambio de autenticación con el cliente. El valor predeterminado es *60* segundos.
Tiempo de espera supp. (SuppTimeout)	Este valor determina las condiciones de tiempo de espera en los intercambios entre el Autenticador y el cliente. El valor predeterminado es *30* segundos.
Tiempo de espera del servidor (ServerTimeout)	Este valor determina las condiciones de tiempo de espera en los intercambios entre el Autenticador y el servidor de autenticación. El valor predeterminado es *30* segundos.
Solicitud máxima (MaxReq)	El número de veces máximo que el switch retransmitirá una Solicitud EAP al cliente antes de que caduque la sesión de autenticación. El valor predeterminado es *2*.
Período de reautenticación (ReAuthPeriod)	Constante que define un numero de segundos distinto de cero entre la reautenticación periódica del cliente. El valor predeterminado es *3600* segundos.
Reautenticación (ReAuth)	Determina si la reautenticación normal tendrá lugar en este puerto. La opción predeterminada es *Desactivado*.

Haga clic en **Aplicar** para aplicar los cambios de la configuración.

Usuarios locales

En la carpeta **Seguridad**, abra la carpeta **802.1x** y haga clic en **Usuario 802.1X** para abrir la ventana **Usuario 802.1x**. Esta ventana le permitirá configurar diferentes usuarios locales en el switch.

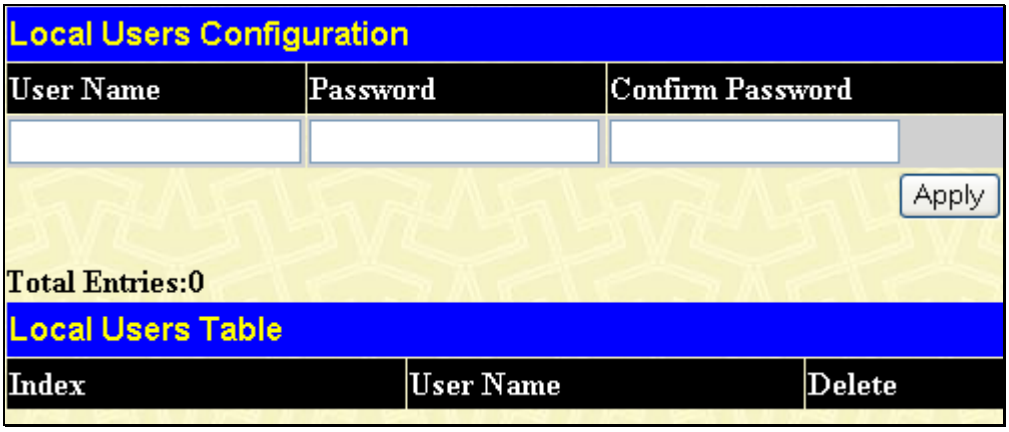
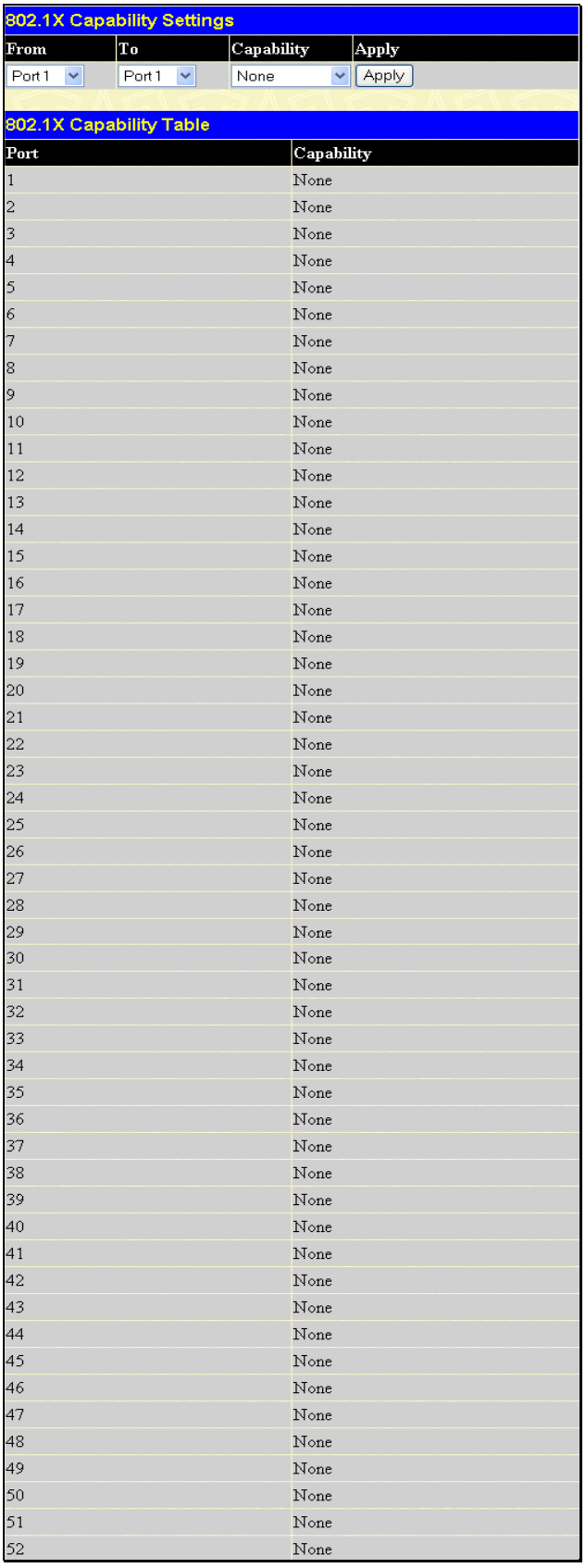


Figura 9- 11. Ventana de Configuración de usuarios locales

Introduzca un **Nombre de usuario**, una **Contraseña** y la confirmación de dicha contraseña. Los usuarios locales configurados correctamente aparecerán en la **Tabla de usuarios locales**, situada en la parte inferior de la misma ventana.

Opciones de capacidad 802.1X

En la carpeta **Seguridad**, abra la carpeta **802.1x** y haga clic en **Opciones de capacidad 802.1X** para abrir la ventana **Opciones de capacidad 802.1x**. Esta ventana le permitirá configurar las opciones de capacidad para cada uno de los puertos del switch.



802.1X Capability Settings

From	To	Capability	Apply
Port 1	Port 1	None	Apply

802.1X Capability Table

Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None
16	None
17	None
18	None
19	None
20	None
21	None
22	None
23	None
24	None
25	None
26	None
27	None
28	None
29	None
30	None
31	None
32	None
33	None
34	None
35	None
36	None
37	None
38	None
39	None
40	None
41	None
42	None
43	None
44	None
45	None
46	None
47	None
48	None
49	None
50	None
51	None
52	None

Figura 9- 12. Ventana de Opciones de capacidad 802.1x

ESPAÑOL

Esta ventana muestra la información siguiente:

Parámetro	Descripción
De y A	Seleccione el puerto o el rango de puertos que desea configurar.
Capacidad	Permite aplicar las opciones del Autenticador 802.1x puerto por puerto. Seleccione *Autenticador* para aplicar las opciones al puerto. Cuando la opción está activada un usuario deberá pasar el proceso de autenticación para poder acceder a la red. Seleccione *Ninguno* para las funciones 802.1x desactivadas del puerto.

Servidor RADIUS

La característica RADIUS del switch facilita la administración centralizada de usuarios y le ofrece protección contra piratas activos curiosos. El Administrador web ofrece tres ventanas.

Haga clic en **Seguridad** > **802.1x** > **Servidor RADIUS** para abrir la ventana del **Servidor RADIUS** que se muestra a continuación:

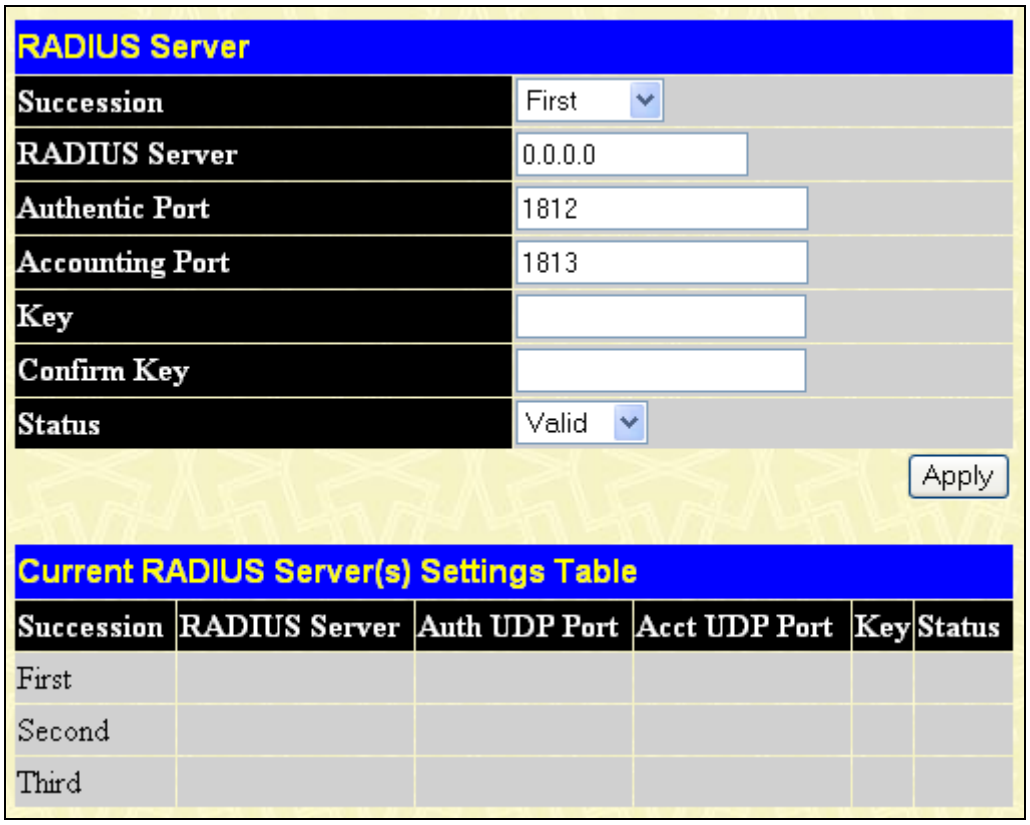


Figura 9- 13.Ventana del Servidor RADIUS

Esta ventana muestra la información siguiente:

Parámetro	Descripción
Sucesión	Elija el Servidor RADIUS deseado para configurar: *Primero, Segundo* o *Tercero*.
Servidor RADIUS	Configure la dirección IP del Servidor RADIUS.
Puerto auténtico	Configure el puerto UDP auténtico de los servidores RADIUS. El puerto predeterminado es *1812*.
Puerto de cuentas	Configure el puerto UDP de las cuentas de los servidores RADIUS. El puerto predeterminado es *1813*.
Clave	Configure la clave con la misma que la del Servidor RADIUS.
Confirmar clave	Confirme que la clave compartida es la misma que la del Servidor RADIUS.
Estatus	Permite a los usuarios configurar el Servidor RADIUS como *Válido* (Activado) o *No válido* (Desactivado).

Apartado 10

Control

- *Dirección MAC*
- *Grupo de Control IGMP*
- *Explorar los puertos del router*
- *Control de acceso a los puertos*

Dirección MAC

Esta función permite visualizar la tabla de envíos de la Dirección MAC dinámica del switch. Cuando el dispositivo memoriza una asociación entre una dirección MAC y un número de puerto, crea una entrada en su tabla de envíos. Estas entradas se utilizan para enviar paquetes a través del switch.

Para visualizar la tabla de envíos de la Dirección MAC desde el menú **Control**, haga clic en el enlace **Dirección MAC**:

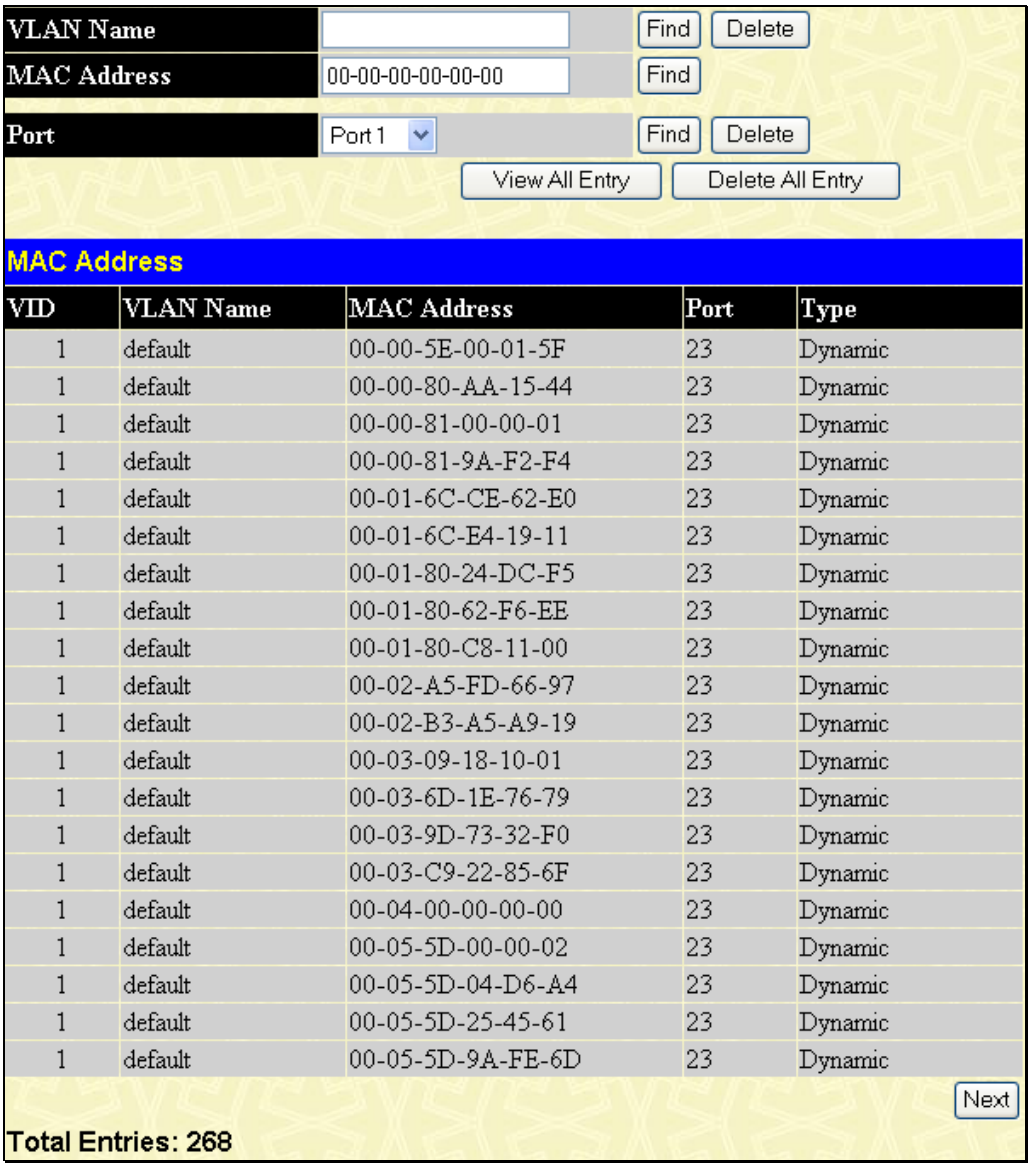


Figura 10- 1. Ventana de la Dirección MAC

Se pueden visualizar o configurar los campos siguientes:

Parámetro	Descripción
Nombre de la VLAN	Introduzca un nombre para la VLAN con el que explorar en la tabla de envíos.
Dirección MAC	Introduzca una dirección MAC con la que explorar en la tabla de envíos.
Puerto	Seleccione el puerto utilizando el menú desplegable correspondiente.
Buscar	Permite al usuario pasar a un sector de la base de datos correspondiente a un puerto definido por el usuario, VLAN o dirección MAC.
VID	El VLAN ID de la VLAN a la que pertenece el puerto.
Dirección MAC	La dirección MAC introducida en la tabla de direcciones.
Puerto	El puerto al que corresponde la dirección MAC anterior.
Tipo	Describe el método con el que el switch detectó la dirección MAC. Las entradas posibles son Dinámico, Propio y Estático.
Siguiente	Haga clic en este botón para visualizar la página siguiente de la tabla de direcciones.
Ver todas las entradas	Haga clic en este botón para visualizar todas las entradas de la tabla de direcciones.

Grupo de Control IGMP

Esta ventana permite visualizar la Tabla del Grupo de Control IGMP del switch. El Control IGMP permite al switch leer la dirección IP del grupo multicast y la dirección MAC correspondiente de los paquetes IGMP que pasan por el switch. El número de informes IGMP controlados se muestra en el campo **Informes**.

Para visualizar la ventana del **Grupo de Control IGMP**, haga clic en **Grupo de Control IGMP** en el menú **Control**:

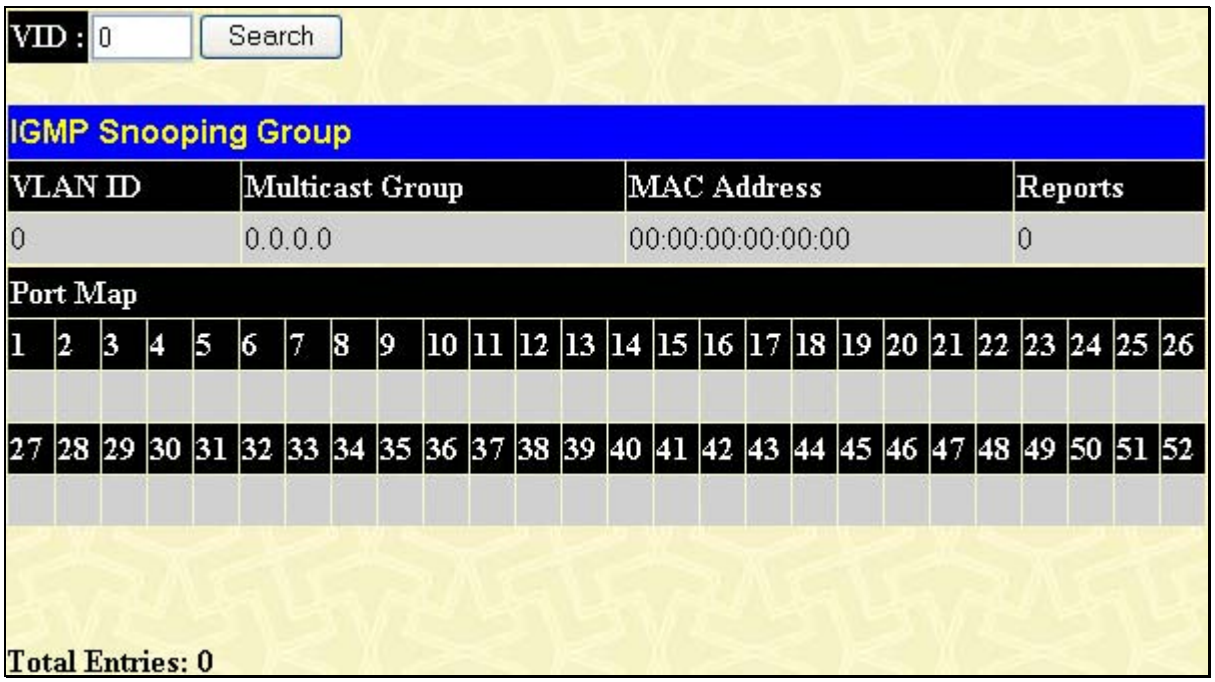


Figura 10- 2. Ventana del Grupo de Control IGMP

El usuario deberá buscar en la **Tabla del Grupo de Control IGMP** introduciendo el VID en la parte superior izquierda y haciendo clic en **Buscar**.

Se pueden visualizar los campos siguientes:

Parámetro	Descripción
VLAN ID	Nombre de la VLAN del grupo multicast.
Grupo Multicast	Dirección IP del grupo multicast.
Dirección MAC	Dirección MAC del grupo multicast.
Informes	Número total de informes recibidos para este grupo.
Distribución de puertos	Puertos en los que se muestran los paquetes IGMP controlados.

NOTA: Para configurar el Control IGMP para el switch, vaya a la carpeta **Características de Capa 2** y seleccione **Control IGMP**. La información sobre la configuración y otros aspectos relacionados con el Control IGMP se encuentran en el Apartado 7 de este manual, en el epígrafe **Control IGMP**.

Explorar los puertos del router

Esta ventana muestra qué puertos del switch están configurados en cada momento como puertos del router. Los puertos del router configurados por el usuario (empleando las interfaces de administración basada en web) se muestran como puertos del router estático, designado como **S**. Los puertos del router configurados de forma dinámica por el switch se designan como **D**.

Total Entries: 1

Browse Router Port

VLAN ID	VLAN Name
1	default

Dynamic Router Port

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

Figura 10- 3. Ventana de Explorar puertos del router

Control de acceso a los puertos

Las ventanas siguientes se utilizan para controlar los datos estadísticos 802.1x del switch puerto por puerto. Para visualizar la ventana **Control de acceso a los puertos**, abra la carpeta **Control** y haga clic en la carpeta **Control de acceso a los puertos**.

NOTA: Las ventanas del **Estado del Autenticador**, de las **Estadísticas del Autenticador**, de las **Estadísticas de la sesión del Autenticador** y de los **Diagnósticos del Autenticador** de esta sección no pueden visualizarse en el switch a menos que el 802.1x se active por puertos o por dirección MAC. Para activar el 802.1x, vaya a la entrada **Switch 802.1x** de la **Herramienta de administración web**.

Autenticación RADIUS

Esta tabla contiene información acerca de la actividad del cliente de autenticación RADIUS en la parte de cliente del protocolo de autenticación RADIUS. Dispone de una fila para cada servidor de autenticación RADIUS que el cliente comparte de forma confidencial. Para visualizar la **Autenticación RADIUS**, haga clic en **Control > Control de acceso a los puertos > Autenticación RADIUS**.

Clear

RADIUS Authentication Time Interval 1s

ServerIndex	InvalidServer	Identifier	ServerIPAddr	UDP Port	Timeouts	Requests	Challenges	Accepts	Rej
1	0	CB100S48S	0.0.0.0	0	0	0	0	0	
2	0	CB100S48S	0.0.0.0	0	0	0	0	0	
3	0	CB100S48S	0.0.0.0	0	0	0	0	0	

Figura 10- 4. Ventana de Autenticación RADIUS

ESPAÑOL

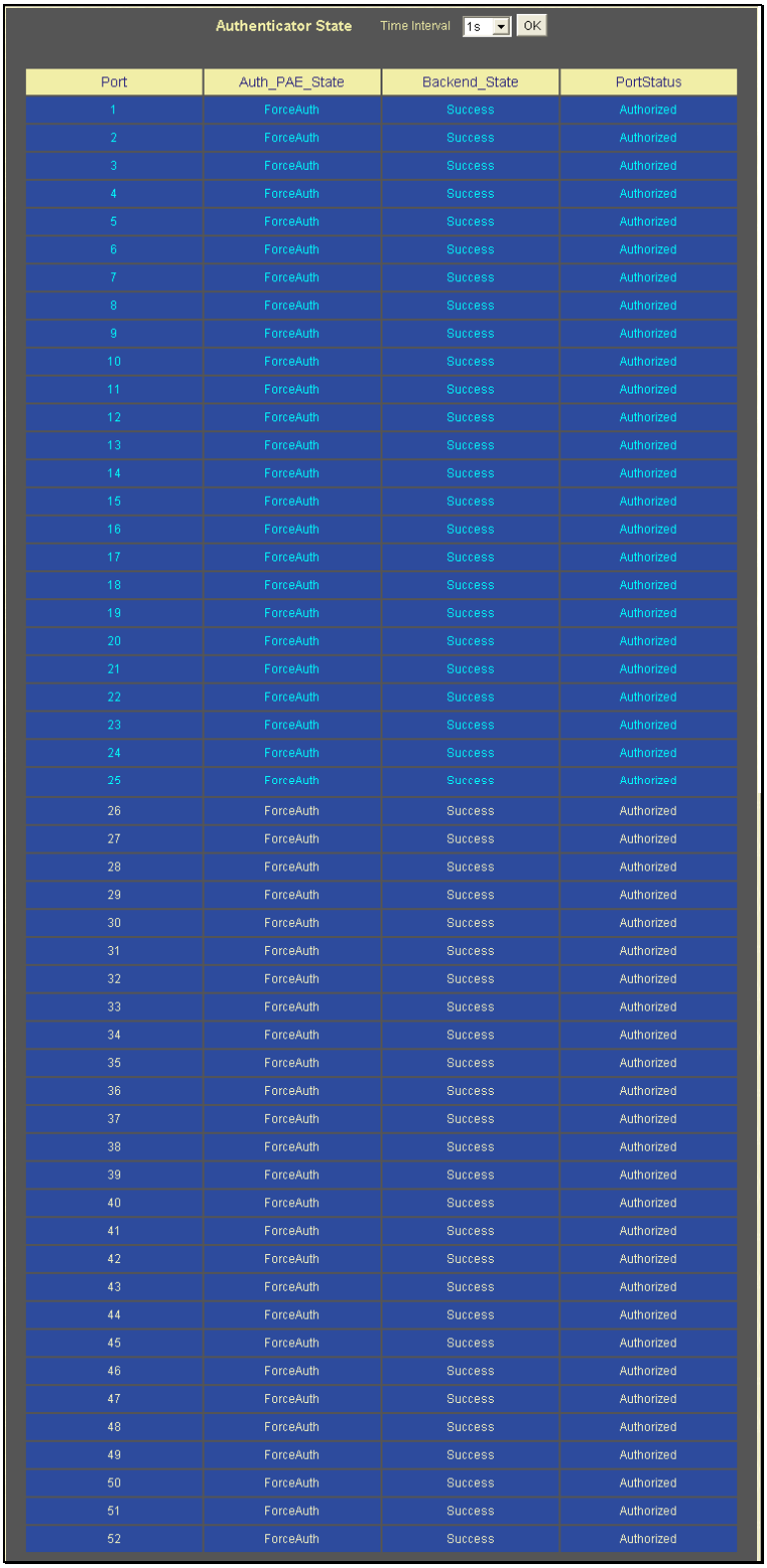
El usuario también debe seleccionar el intervalo de tiempo deseado para actualizar las estadísticas, entre *1s* y *60s*, donde "s" significa segundos. El valor predeterminado es un segundo. Para borrar las estadísticas actuales que muestra la tabla, haga clic en el botón **Borrar**, situado en el parte superior izquierda.

Se pueden visualizar los campos siguientes:

Parámetro	Descripción
Índice del servidor	Número de identificación asignado a cada servidor de autenticación RADIUS que el cliente comparte de forma confidencial.
Dirección IP del servidor	Dirección IP de identificación del servidor.
Puerto UDP	Puerto UDP que el cliente está utilizando para enviar solicitudes a este servidor.
Tiempos de espera	Número de tiempos de espera de autenticación en este servidor. Tras un tiempo de espera el cliente debe volver a intentar el envío al mismo servidor, a un servidor diferente o abandonar. Un nuevo intento de envío al mismo servidor computa como retransmisión, al igual que un tiempo de espera. El envío a un servidor diferente computa como una solicitud, al igual que un tiempo de espera.
Solicitudes	Número de paquetes RADIUS de solicitud de acceso enviados a este servidor. No incluye retransmisiones.
Intentos	Número de paquetes RADIUS de intento de acceso (válidos o no válidos) recibidos procedentes de este servidor.
Aceptaciones	Número de paquetes RADIUS de aceptación de acceso (válidos o no válidos) recibidos procedentes de este servidor.
Rechazos de acceso	Número de paquetes RADIUS de rechazo de acceso (válidos o no válidos) recibidos procedentes de este servidor.
Tiempo de ida y vuelta	Intervalo de tiempo (en centésimas de segundo) entre el intento/respuesta de acceso y la solicitud de acceso coincidente desde el servidor RADIUS de autenticación.
Retransmisiones de acceso	Número de paquetes RADIUS de solicitud de acceso retransmitidos a este servidor RADIUS de autenticación.
Solicitudes pendientes	Número de paquetes RADIUS de solicitud de acceso destinados a este servidor que todavía no han caducado o no han recibido respuesta. Esta variable aumenta cuando se envía una solicitud de acceso y se reduce debido a la recepción de una aceptación, un rechazo, un intento de acceso, un tiempo de espera o una retransmisión.
Respuestas de acceso	Número de paquetes RADIUS mal formados de respuesta de acceso recibidos procedentes de este servidor. Entre los paquetes mal formados se incluyen aquéllos con una longitud no válida. En las respuesta de acceso mal formadas no se incluyen los autenticadores deficientes, los atributos de firma o los tipos conocidos.
Autenticadores deficientes	Número de paquetes RADIUS de respuesta de acceso que contienen autenticadores no válidos o los atributos de firma recibidos procedentes de este servidor.
Tipos desconocidos	Número de paquetes RADIUS de tipos desconocidos que se han recibido procedentes de este servidor en el puerto de autenticación.
Paquetes omitidos	Número de paquetes RADIUS recibidos procedentes de este servidor en el puerto de autenticación y omitidos por algún motivo.

Estado del Autenticador

El Estado del Autenticador no puede visualizarse a menos que el switch esté configurado basado en puerto o en MAC para la función 802.1X. Esta tabla muestra el Estado del Autenticador de cada puerto. Para visualizar el Estado del Autenticador, haga clic en **Control > Control de acceso a los puertos > Estado de Autenticador.**



Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
21	ForceAuth	Success	Authorized
22	ForceAuth	Success	Authorized
23	ForceAuth	Success	Authorized
24	ForceAuth	Success	Authorized
25	ForceAuth	Success	Authorized
26	ForceAuth	Success	Authorized
27	ForceAuth	Success	Authorized
28	ForceAuth	Success	Authorized
29	ForceAuth	Success	Authorized
30	ForceAuth	Success	Authorized
31	ForceAuth	Success	Authorized
32	ForceAuth	Success	Authorized
33	ForceAuth	Success	Authorized
34	ForceAuth	Success	Authorized
35	ForceAuth	Success	Authorized
36	ForceAuth	Success	Authorized
37	ForceAuth	Success	Authorized
38	ForceAuth	Success	Authorized
39	ForceAuth	Success	Authorized
40	ForceAuth	Success	Authorized
41	ForceAuth	Success	Authorized
42	ForceAuth	Success	Authorized
43	ForceAuth	Success	Authorized
44	ForceAuth	Success	Authorized
45	ForceAuth	Success	Authorized
46	ForceAuth	Success	Authorized
47	ForceAuth	Success	Authorized
48	ForceAuth	Success	Authorized
49	ForceAuth	Success	Authorized
50	ForceAuth	Success	Authorized
51	ForceAuth	Success	Authorized
52	ForceAuth	Success	Authorized

Figura 10- 5. Ventana del Estado del Autenticador

El usuario debe seleccionar el intervalo de tiempo deseado para actualizar las estadísticas, entre *1s* y *60s*, donde “s” significa segundos. El valor predeterminado es un segundo.

Restablecer el sistema

La función **Restablecer** tiene muchas opciones a la hora de restablecer el switch. Algunos parámetros actuales de configuración pueden conservarse al tiempo que se restablecen los demás parámetros de configuración predeterminados de fábrica.

NOTA: Sólo la opción **Restablecer el sistema** introducirá los parámetros predeterminados de fábrica en la memoria RAM no volátil del switch y lo reiniciará. Todas las demás opciones introducirán los valores predeterminados en la configuración actual, pero no guardan esta configuración. La función de **Restablecer el sistema** recuperará la configuración predeterminada de fábrica del switch.

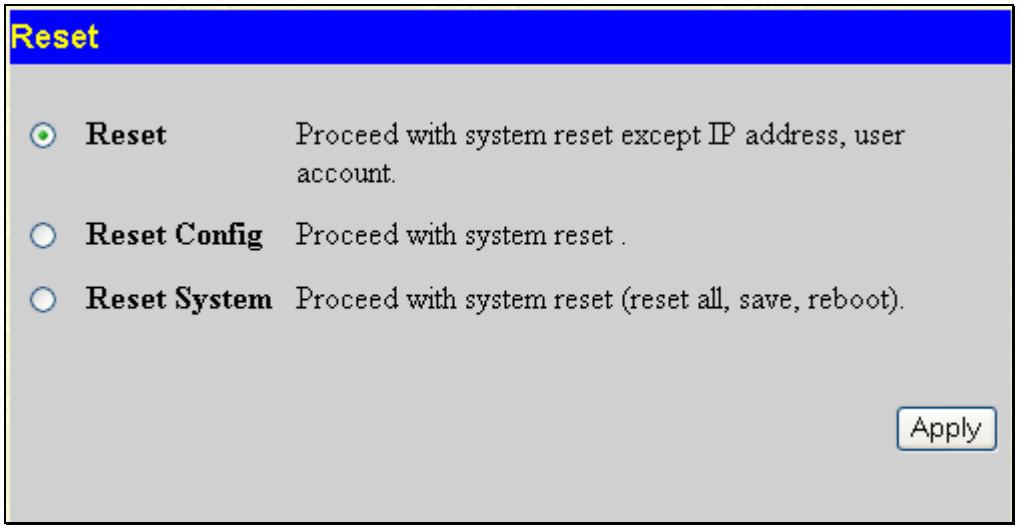


Figura 10- 6. Ventana de Restablecer el sistema

Reiniciar el sistema

La ventana siguiente se utiliza para reiniciar el switch.

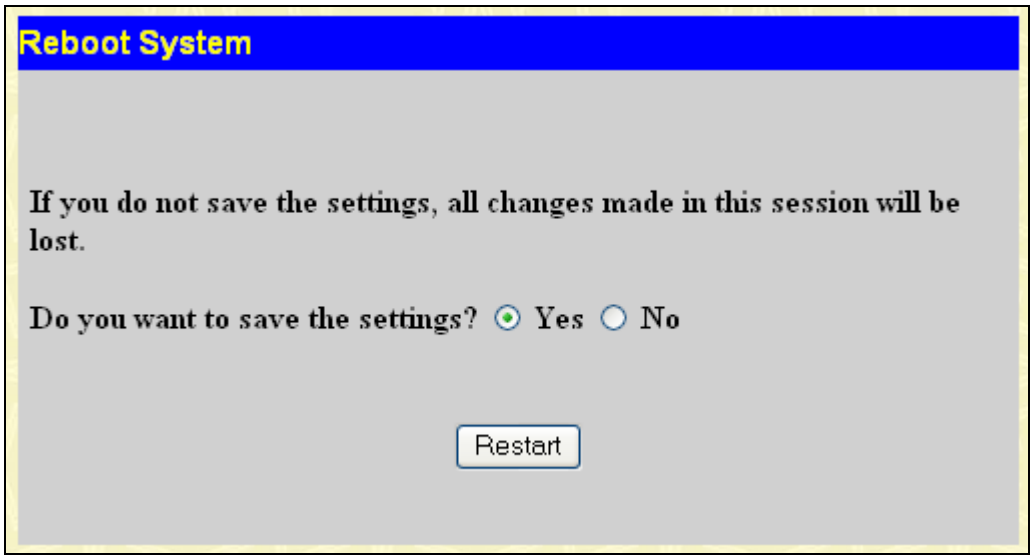


Figura 10- 7. Ventana de Reiniciar el sistema

Haga clic en el botón **Sí** para ordenar al switch que guarde la configuración actual en la memoria RAM no volátil antes de reiniciar el dispositivo.

Haga clic en el botón **No** para ordenar al switch que no guarde la configuración actual antes de reiniciar el dispositivo. Toda la información sobre la configuración introducida desde la última vez que se ejecutó la función **Guardar cambios** se perderán.

Haga clic en el botón **Reiniciar** para reiniciar el switch.

Guardar los cambios

El switch tiene dos niveles de memoria: memoria RAM normal y no volátil (o NV-RAM). Los cambios de configuración se hacen efectivos al hacer clic en el botón **Aplicar.** De este modo, las opciones de configuración se aplicarán inmediatamente en el software de conmutación de la memoria RAM y surtirán efecto de forma inmediata.

Sin embargo, en el caso de algunas opciones es necesario reiniciar el switch antes de que surtan efecto. Al reiniciar el switch se borran todas las opciones de configuración de la memoria RAM y vuelven a cargarse las opciones almacenadas de la memoria NV-RAM. Así, es necesario guardar todos los cambios realizados en las opciones de configuración en la NV-RAM antes de reiniciar el switch.

Para conservar de forma permanente los cambios realizados en la configuración, haga clic en el botón **Guardar** en la página de **Guardar los cambios**, tal y como se muestra a continuación.

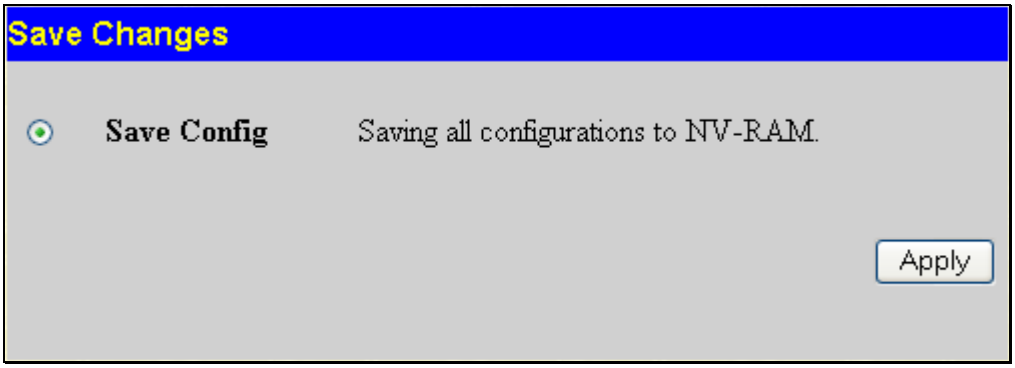


Figura 10- 8. Ventana de Guardar los cambios

Cerrar sesión

Haga clic en el botón **Cerrar sesión** de la ventana **Cerrar sesión** para salir del switch.

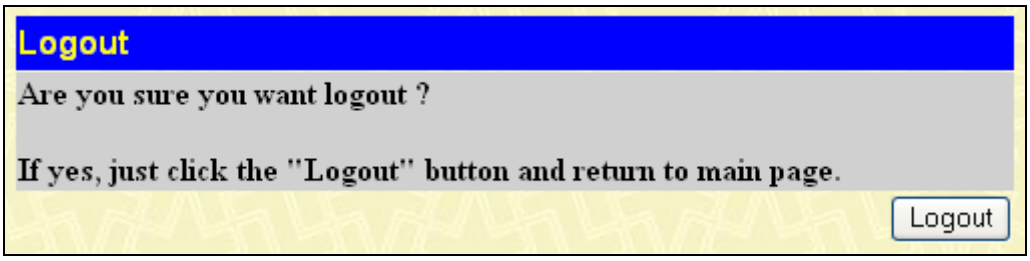


Figura 10- 9. Ventana de Cerrar sesión

Apéndice A

Especificaciones técnicas

Generales	
Protocolos	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP "Mini GBIC") IEEE 802.1D Árbol de expansión IEEE 802.1D/S/W Árbol de expansión IEEE 802.1Q VLAN IEEE 802.1p Colas de prioridad IEEE 802.1X Control de acceso a la red basado en puertos IEEE 802.3ad Control de incorporación de enlaces IEEE 802.3x Control de flujo Full-duplex IEEE 802.3 Autonegociación NWay IEEE802.3af Estándar (sólo para POE)
Fibra óptica	SFP (Mini GBIC) compatibles: DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX) DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DEM-210 (modo individual, 100BASE-FX) DEM-211 (modo múltiple, 100BASE-FX) Transceptores WDM compatibles: DEM-330T (TX-1550/RX-1310nm), hasta 10 km, modo individual DEM-330R (TX-1310/RX-1550nm), hasta 10 km, modo individual DEM-331T (TX-1550/RX-1310nm), hasta 40 km, modo individual DEM-331R (TX-1310/RX-1550nm), hasta 40 km, modo individual
Estándares	CSMA/CD
Velocidades de transferencia de datos: **Ethernet** **Fast Ethernet** **Gigabit Ethernet**	Half-duplex Full-duplex 10 Mbps20Mbps 100Mbps 200Mbps n/a 2000Mbps
Topología	Estrella
Cables de red	Cat. 5 mejorado para 1000BASE-T UTP Cat. 5, Cat. 5 mejorado para 100BASE-TX UTP Cat. 3, 4 y 5 para 10BASE-T EIA/TIA-568 100-ohm testado de par trenzado (STP)(100m)
Número de puertos	CB100S24S: 24 puertos 10/100Base-T 2 puertos Combo 1000Base-T/SFP 2 puertos 1000Base-T CB100S48S: 48 puertos 10/100Base-T 2 puertos Combo 1000Base-T/SFP 2 puertos 1000Base-T

Físicas y ambientales	
Fuente de alimentación interna	40W, entrada AC, 100-240 Vac, 12V/3.33A , 50~60Hz
Temperatura de funcionamiento	0 – 40º C
Temperatura de almacenamiento	-40 – 70º C
Humedad	5 - 95% sin condensación
Dimensiones	Carcasa metálica de 19” 441(W) x 207(D) x 44(H) mm, 1U de tamaño para montaje en rack (CB100S24S) 441(W) x 309(D) x 44(H) mm, 1U de tamaño para montaje en rack (CB100S48S)
EMI	CE Clase A, FCC Clase A, C-Tick, VCCI
Seguridad	Informe CB, UL

Rendimiento	
Método de transmisión	Almacenar y enviar
Buffer de los paquetes	512 KB por dispositivo
Filtrado de paquetes/ Velocidad de envío	14.881 pps (puerto de 10M) 148.810 pps (puerto de 100M) 1.488.100 pps (puerto de 1Gbps)
Memorización de Direcciones MAC	Actualización automática. Compatible con Direcciones MAC de 8K
Colas de prioridad	4 colas de prioridad por puerto.
Tiempo de la tabla de envíos	Tiempo máximo: 10-1000000 segundos. Valor predeterminado: 300.

ESPAÑOL

Alimentación

Característica	*Descripción detallada*
Fuente de alimentación interna	40W, entrada AC, 100-240Vac, 12V/3.33A , 50~60Hz

Rendimiento

Característica	*Descripción detallada*
Velocidad de transmisión en todos los puertos FE/GE	Funcionamiento a velocidad máxima (full-duplex) en todos los puertos FE/GE.
Modo de envío	Almacenar y enviar
Capacidad de conmutación	12.8 Gbps (CB100S24S) 17.6 Gbps (CB100S48S)
Velocidad de envío de paquetes en el sistema (64 Bytes)	9,5 millones de paquetes por segundo (CB100S24S) 13,1 millones de paquetes por segundo (CB100S48S)
Colas de prioridad	4 colas de prioridad por puerto
Tabla de Direcciones MAC	Compatible con Direcciones MAC de 8K
Memoria del Buffer de los paquetes	512KB por dispositivo

ESPAÑOL

Funciones de los puertos

Característica	*Descripción detallada*
Puerto de la consola	DCE RS-232 DB-9 para recuperar los valores de fábrica
24 puertos 10/100BaseT 48 puertos 10/100BaseT	Conformidad con los estándares siguientes: 1. IEEE 802.3 2. IEEE 802.3u 3. Compatibles con operaciones Half/Full-Duplex 4. Todos los puertos son compatibles con auto MDI-X/MDI-II cruzado 5. Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex y prevención de bloqueo de cabeza de línea.
Puertos Combo en el panel frontal	2 puertos Combo 1000BASE-T/SFP Los puertos 1000BASE-T son conformes con los estándares siguientes: IEEE 802.3 IEEE 802.3u IEEE 802.3ab Compatibles con operaciones Full-Duplex Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex y prevención de bloqueo de cabeza de línea. Transceptores SFP compatibles: 1000BASE-LX 1000BASE-SX Conformidad con los estándares siguientes: IEEE 802.3z IEEE 802.3u
2 puertos 1000BASE-T en el panel frontal	Los puertos 1000BASE-T son conformes con los estándares siguientes: IEEE 802.3 IEEE 802.3u IEEE 802.3ab Compatibles con operaciones Full-Duplex Control de flujo IEEE 802.3x compatible con modo Full-Duplex, contrapresión en modo Half-Duplex y prevención de bloqueo de cabeza de línea.

Apéndice B

Entradas de registro del sistema

La tabla siguiente enumera las posibles entradas y sus significados correspondientes que aparecerán en el registro del Sistemas del switch.

Categoría	Descripción de la situación	Contenido del registro	Importancia
Sistema	Sistema iniciado	Unidad <unitID>, sistema iniciado	Fundamental
	Configuración guardada en flash	Unidad <unitID>, configuración guardada en flash por consola (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Registro del sistema guardado en flash	Unidad <unitID>, registro del sistema guardado en flash por consola (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Configuración y registro guardados en flash	Unidad <unitID>, configuración y registro guardados en flash por consola (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
Cargar/Descargar	Firmware actualizado correctamente	Unidad <unitID>, firmware actualizado por consola correctamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Firmware actualizado incorrectamente	Unidad <unitID>, firmware actualizado por consola incorrectamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Configuración descargada correctamente	Configuración descargada por consola correctamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Configuración descargada incorrectamente	Configuración descargada por consola incorrectamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Configuración cargada correctamente	Configuración cargada por consola correctamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Configuración cargada incorrectamente	Configuración cargada por consola incorrectamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Mensaje de registro cargado	Mensaje de registro cargado por consola correctamente (Nombre de usuario:	Informativo

ESPAÑOL

Categoría	Descripción de la situación	Contenido del registro	Importancia
	correctamente	<username>, IP: <ipaddr>, MAC: <macaddr>)	
	Mensaje de registro cargado incorrectamente	Mensaje de registro cargado por consola incorrectamente (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
Interfaz	Enlace ascendente del puerto	Enlace ascendente del puerto <unitID:portNum>, <link state>	Informativo
Consola	Enlace descendente del puerto	Enlace descendente del puerto <unitID:portNum>	Informativo
	Inicio de sesión por consola correcto	Unidad <unitID>, inicio de sesión por consola correcto (Nombre de usuario: <username>)	Informativo
	Error en el inicio de sesión por consola	Unidad <unitID>, error en el inicio de sesión por consola (Nombre de usuario: <username>)	Aviso
	Cerrar sesión por consola	Unidad <unitID>, cerrar sesión por consola (Nombre de usuario: <username>)	Informativo
	Sesión de la consola caducada	Unidad <unitID>, sesión de la consola caducada (Nombre de usuario: <username>)	Informativo
Web	Inicio de sesión por Web correcto	Inicio de sesión por Web correcto (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Web	Error en el inicio de sesión por Web (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Cerrar sesión por Web	Cerrar sesión por Web (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Inicio de sesión por Web (SSL) correcto	Inicio de sesión por Web (SSL) correcto (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Web (SSL)	Error en el inicio de sesión por Web (SSL) (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Cerrar sesión por Web (SSL)	Cerrar sesión por Web (SSL) (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Sesión de Web (SSL) caducada	Sesión de Web (SSL) caducada (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
Telnet	Inicio de sesión por Telnet correcto	Inicio de sesión por Telnet correcto (Nombre de usuario: <username>, IP:	Informativo

Categoría	Descripción de la situación	Contenido del registro	Importancia
		<ipaddr>, MAC: <macaddr>)	
	Error en el inicio de sesión por Telnet	Error en el inicio de sesión por Telnet (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Cerrar sesión por Telnet	Cerrar sesión mediante Telnet (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Sesión de Telnet caducada	Sesión de Telnet caducada (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
SNMP	Solicitud SNMP recibida con una cadena de comunidad no válida	Solicitud SNMP recibida de <ipAddress> con una cadena de comunidad no válida	Informativo
STP	Topología cambiada	Topología cambiada	Informativo
	Nueva raíz seleccionada	Nueva raíz seleccionada	Informativo
	Bucle BPDU de vuelta en el puerto	Bucle BPDU de vuelta en el puerto <unitID:portNum>	Aviso
	El protocolo del árbol de expansión está activado	El protocolo del árbol de expansión está activado	Informativo
	El protocolo del árbol de expansión está desactivado	El protocolo del árbol de expansión está desactivado	Informativo
SSH	Inicio de sesión por SSH correcto	Inicio de sesión por SSH correcto (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por SSH	Error en el inicio de sesión por SSH (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Aviso
	Cerrar sesión mediante SSH	Cerrar sesión mediante SSH (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Sesión de SSH caducada	Sesión de SSH caducada (Nombre de usuario: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informativo
	Servidor SSH activado	Servidor SSH activado	Informativo
	Servidor SSH desactivado	Servidor SSH desactivado	Informativo
AAA	La Política de Autenticación está activada	La Política de Autenticación está activada (Módulo: AAA)	Informativo
	La Política de Autenticación está desactivada	La Política de Autenticación está desactivada (Módulo: AAA)	Informativo

Categoría	Descripción de la situación	Contenido del registro	Importancia
	Inicio de sesión por consola correcto autenticado por método local AAA	Inicio de sesión por consola correcto autenticado por método local AAA (Nombre de usuario: <username>)	Informativo
	Error en el inicio de sesión por consola autenticado por método local AAA	Error en el inicio de sesión por consola autenticado por método local AAA (Nombre de usuario: <username>)	Aviso
	Inicio de sesión por Web correcto autenticado por método local AAA	Inicio de sesión por Web correcto de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Web autenticado por método local AAA	Error en el inicio de sesión por Web de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por Web (SSL) correcto autenticado por método local AAA	Inicio de sesión por Web (SSL) correcto de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Web (SSL) autenticado por método local AAA	Error en el inicio de sesión por Web (SSL) de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por Telnet correcto autenticado por método local AAA	Inicio de sesión por Telnet correcto de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Telnet autenticado por método local AAA	Error en el inicio de sesión por Telnet de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por SSH correcto autenticado por método local AAA	Inicio de sesión por SSH correcto de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por SSH autenticado por método local AAA	Error en el inicio de sesión por SSH de <userIP> autenticado por método local AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por consola correcto autenticado por método “none” AAA	Inicio de sesión por consola correcto autenticado por método “none” AAA (Nombre de usuario: <username>)	Informativo

ESPAÑOL

Categoría	Descripción de la situación	Contenido del registro	Importancia
	Inicio de sesión por Web correcto autenticado por método “none” AAA	Inicio de sesión por Web correcto de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Inicio de sesión por Web (SSL) correcto autenticado por método “none” AAA	Inicio de sesión por Web (SSL) correcto de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Inicio de sesión por Telnet correcto autenticado por método “none” AAA	Inicio de sesión por Telnet correcto de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Inicio de sesión por SSH correcto autenticado por método “none” AAA	Inicio de sesión por SSH correcto de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Inicio de sesión por consola correcto autenticado por servidor AAA	Inicio de sesión por consola correcto autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>)	Informativo
	Error en el inicio de sesión por consola autenticado por servidor AAA	Error en el inicio de sesión por consola autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>)	Aviso
	Inicio de sesión por Web correcto autenticado por servidor AAA	Inicio de sesión por Web correcto de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Web autenticado por servidor AAA	Error en el inicio de sesión por Web de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por Web (SSL) correcto autenticado por servidor AAA	Inicio de sesión por Web (SSL) correcto de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por Web (SSL) autenticado por servidor AAA	Error en el inicio de sesión por Web (SSL) de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Error en el inicio de sesión por Web (SSL) debido a un tiempo de espera del servidor AAA o a una configuración inadecuada	Error en el inicio de sesión por Web (SSL) de <userIP> debido a un tiempo de espera del servidor AAA o a una configuración inadecuada (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por Telnet	Inicio de sesión por Telnet correcto de	Informativo

Categoría	Descripción de la situación	Contenido del registro	Importancia
	correcto autenticado por servidor AAA	<userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	
	Error en el inicio de sesión por Telnet autenticado por servidor AAA	Error en el inicio de sesión por Telnet de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Inicio de sesión por SSH correcto autenticado por servidor AAA	Inicio de sesión por SSH correcto de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en el inicio de sesión por SSH autenticado por servidor AAA	Error en el inicio de sesión por SSH de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Activación del Administrador correcta por consola autenticado por método local de activación AAA	Activación del Administrador correcta por consola autenticado por método local de activación AAA (Nombre de usuario: <username>)	Informativo
	Error en la activación del Administrador por consola autenticado por método local de activación AAA	Error en la activación del Administrador por consola autenticado por método local de activación AAA (Nombre de usuario: <username>)	Aviso
	Activación del Administrador correcta por Web autenticado por método local de activación AAA	Activación del Administrador correcta por Web de <userIP> autenticado por método local de activación AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en la activación del Administrador por Web autenticado por método local de activación AAA	Error en la activación del Administrador por Web de <userIP> autenticado por método local de activación AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Activación del Administrador correcta por Telnet autenticado por método local de activación AAA	Activación del Administrador correcta por Telnet de <userIP> autenticado por método local de activación AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en la activación del Administrador por Telnet autenticado por método local de activación AAA	Error en la activación del Administrador por Telnet de <userIP> autenticado por método local de activación AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Activación del Administrador correcta por SSH autenticado por método local de activación AAA	Activación del Administrador correcta por SSH de <userIP> autenticado por método local de activación AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo

ESPAÑOL

Categoría	Descripción de la situación	Contenido del registro	Importancia
	Error en la activación del Administrador por SSH autenticado por método local de activación AAA	Error en la activación del Administrador por SSH de <userIP> autenticado por método local de activación AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Activación del Administrador correcta por consola autenticado por método “none” AAA	Activación del Administrador correcta por consola autenticado por método “none” AAA (Nombre de usuario: <username>)	Informativo
	Activación del Administrador correcta por Web autenticado por método “none” AAA	Activación del Administrador correcta por Web de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Activación del Administrador correcta por Telnet autenticado por método “none” AAA	Activación del Administrador correcta por Telnet de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Activación del Administrador correcta por SSH autenticado por método “none” AAA	Activación del Administrador correcta por SSH de <userIP> autenticado por método “none” AAA (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Activación del Administrador correcta por consola autenticado por servidor AAA	Activación del Administrador correcta por consola autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>)	Informativo
	Error en la activación del Administrador por consola autenticado por servidor AAA	Error en la activación del Administrador por consola autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>)	Aviso
	Activación del Administrador correcta por Web autenticado por servidor AAA	Activación del Administrador correcta por Web de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en la activación del Administrador por Web autenticado por servidor AAA	Error en la activación del Administrador por Web de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
	Activación del Administrador correcta por Telnet autenticado por servidor AAA	Activación del Administrador correcta por Telnet de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en la activación del Administrador por Telnet autenticado por servidor AAA	Error en la activación del Administrador por Telnet de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso

ESPAÑOL

Categoría	Descripción de la situación	Contenido del registro	Importancia
	Activación del Administrador correcta por SSH autenticado por servidor AAA	Activación del Administrador correcta por SSH de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Informativo
	Error en la activación del Administrador por SSH autenticado por servidor AAA	Error en la activación del Administrador por SSH de <userIP> autenticado por servidor AAA <serverIP> (Nombre de usuario: <username>, MAC: <macaddr>)	Aviso
Seguridad de los puertos	La seguridad de los puertos ha superado su tamaño máximo de memorización y no memorizará más direcciones nuevas	Infracción de la seguridad de los puertos(Puerto: <unitID:portNum>, MAC: <macaddr>)	Aviso
Cambio de IP y Contraseña	Cambio de actividad de la Dirección IP	Unidad <unitID>, la dirección IP de gestión ha sido modificada por (Nombre de usuario: <username>, IP: <ipaddr>,MAC: <macaddr>)	Informativo
	Cambio de actividad de la Contraseña	Unidad <unitID>, la contraseña ha sido modificada por (Nombre de usuario: <username>, IP: <ipaddr>,MAC: <macaddr>)	Informativo
Motor de salvaguarda	El motor de salvaguarda está en modo normal	El motor de salvaguarda pasa a modo NORMAL	Informativo
	El motor de salvaguarda está en modo de filtro de paquetes	El motor de salvaguarda pasa a modo AGOTADO	Aviso
Tormenta de paquetes	Tormenta de difusión	Se está produciendo una tormenta de difusión en el puerto <unitID:portNum>	Aviso
	La tormenta de difusión ha pasado	La tormenta de difusión en el puerto <unitID:portNum> ha pasado	Informativo
	Tormenta multicast	Se está produciendo una tormenta multicast en el puerto <unitID:portNum>	Aviso
	La tormenta multicast ha pasado	La tormenta multicast en el puerto <unitID:portNum> ha pasado	Informativo
	Cierre del puerto debido a una tormenta de paquetes	El puerto <unitID:portNum> está cerrado debido a una tormenta de paquetes	Aviso

Apéndice C

Longitudes de los cables

Utilice la tabla siguiente a modo orientativo para las longitudes máximas de los cables.

Estándar	Tipo de dispositivo	Distancia máxima
Mini GBIC	1000BASE-LX, módulo de fibra (modo individual) 1000BASE-SX, módulo de fibra (modo múltiple) 1000BASE-LHX, módulo de fibra (modo individual) 1000BASE-ZX, módulo de fibra (modo individual)	10 km 550 m 40 km 80 km
1000BASE-T	Cable de categoría 5e UTP Cable de categoría 5 UTP (1000 Mbps)	100 m
100BASE-TX	Cable de categoría 5 UTP (100 Mbps)	100 m
10BASE-T	Cable de categoría 3 UTP (10 Mbps)	100 m

Apéndice D

Glosario

1000BASE-SX: Amplitud de onda láser corta en un cable de fibra óptica multimodo para una distancia máxima de 2.000 metros.

1000BASE-LX: Amplitud de onda larga para un cable de fibra óptica "de larga distancia" para una distancia máxima de 10 kilómetros.

100BASE-FX: Implementación Ethernet de 100Mbps sobre fibra.

100BASE-TX: Implementación Ethernet de 100Mbps sobre cableado de categoría 5 y Tipo 1 de par trenzado.

10BASE-T: Especificación IEEE 802.3 para Ethernet sobre cableado de par trenzado apantallado (UTP).

Envejecimiento: Retirada automática de entradas dinámicas de la base de datos del switch que han caducado y han dejado de ser válidas.

ATM: Modo de Transferencia Asincrónico. Protocolo de transmisión orientado a conexiones basado en células de longitud fija (paquetes). El protocolo ATM está pensado para soportar una completa gama de tráfico de usuarios, incluyendo voz, datos y señales de vídeo.

Autonegociación: Característica de un puerto que le permite advertir las capacidades en cuanto a velocidad, duplex y control de flujo. Cuando está conectado a una estación final que también incluye autonegociación, el enlace puede detectar su propia configuración de funcionamiento óptima.

Puerto de red troncal: Puerto que no memoriza las direcciones de los dispositivos y que recibe todos los frames con direcciones desconocidas. Los puertos de red troncal suelen utilizarse para conectar el switch con la red troncal de su red. Recuerde que los puertos de red troncal anteriormente se conocían como “puertos de enlace descendente”.

Red troncal: Parte de una red utilizada como ruta principal para transportar el tráfico entre segmentos de red.

Ancho de banda: Capacidad de información medida en bits por segundo que un canal puede transmitir. El ancho de banda de Ethernet es de 10Mbps, mientras que el de Fast Ethernet es de 100Mbps.

Velocidad de transmisión: Velocidad de conmutación de una línea. Conocida también como velocidad de línea entre segmentos de una red.

BOOTP: Protocolo que le permite distribuir automáticamente una dirección IP en una dirección MAC determinada cada vez que se inicia un dispositivo. Asimismo, el protocolo puede asignar la máscara de subred y la puerta de enlace predeterminada a un dispositivo.

Puente: Dispositivo que interconecta redes locales o remotas al margen de los protocolos de alto nivel que están implicados. Los puentes forman una red lógica simple y centralizan la administración de la red.

Difusión: Mensaje enviado a todos los dispositivos de destino presentes en una red.

Tormenta de difusión: Difusiones múltiples simultáneas que suelen absorber el ancho de banda disponible de la red y provocan errores.

Puerto de la consola: Puerto del switch que acepta un conector de terminal o módem. Convierte la disposición paralela de los datos dentro de los ordenadores en una forma en serie que se utiliza en los enlaces de transmisión de datos. Este tipo de puertos se utiliza más frecuentemente para administración local compleja.

CSMA/CD: Método de acceso al canal utilizado por Ethernet y por las normas IEEE 802.3 en el que los dispositivos transmiten únicamente tras encontrar libre el canal de datos durante un período de tiempo determinado. Cuando dos dispositivos transmiten simultáneamente, se produce una colisión y los dos dispositivos implicados retrasan la retransmisión durante un tiempo aleatorio.

Conmutación del centro de datos: Punto de incorporación dentro de una red corporativa en el que un switch ofrece acceso de alto rendimiento a agrupaciones centralizadas de servidores, una conexión de red troncal de alta velocidad y un punto de control para la administración y la seguridad de la red.

Ethernet: Especificación LAN desarrollada conjuntamente por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet funcionan a una velocidad de 10Mbps utilizando CSMA/CD para operar con cables.

Fast Ethernet: Tecnología de 100Mbps basada en el método de acceso a una red Ethernet/CMSA/CD.

Control de flujo: (IEEE 802.3z) Medio de mantener los paquetes en el puerto de transmisión de la estación final conectada. Evita que se pierdan paquetes en un puerto ocupado del switch.

Envío: Proceso de transmisión de un paquetes hacia su destino por un dispositivo de redes.

Full duplex: Sistema que permite transmitir y recibir paquetes al mismo tiempo y, efectivamente, duplica el rendimiento potencial de un enlace.

Half duplex: Sistema que permite transmitir y recibir paquetes, pero no al mismo tiempo. Contrasta con el modo full duplex.

Dirección IP: Dirección del protocolo de internet. Identificador único de un dispositivo conectado a una red mediante TCP/IP. La dirección se expresa con cuatro octetos separados por puntos (períodos) y está formada por una sección de red, una sección de subred opcional y una sección del host.

IPX: Intercambio de paquetes de internet. Protocolo que permite la comunicación en una red NetWare.

LAN: **Red de área local:** Red de recursos informáticos conectados (como ordenadores, impresoras, servidores) que cubren un área geográfica relativamente pequeña (normalmente no supera la superficie de una planto o un edificio). Se caracteriza por la alta velocidad de datos y el bajo nivel de errores.

Latencia: Retraso entre el momento en el que un dispositivo recibe un paquete y el momento en el que el paquete se envía al puerto de destino.

Velocidad de línea: Véase Velocidad de transmisión.

Puerto principal: Puerto de un enlace flexible que lleva el tráfico de datos en condiciones de funcionamiento normales.

MDI: **Interfaz dependiente del medio:** Conexión a puerto Ethernet en el que el transmisor de un dispositivo está conectado al receptor de otro dispositivo.

MDI-X: **Interfaz cruzada dependiente del medio:** Conexión a puerto Ethernet en el que las líneas internas de transmisión y recepción está cruzadas.

MIB: **Base de información de gestión:** Almacena las características y parámetros de gestión de un dispositivo. El Protocolo simple de administración de red (SNMP) utiliza las MIBs para conservar los atributos de sus sistemas gestionados. El switch contiene su propia MIB interna.

Multicast: Paquetes simples copiados en un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de direcciones de destino del paquete.

Protocolo: Conjunto de reglas de comunicación entre dispositivos de una red. Las reglas dictan el formato, el tiempo, la secuenciación y el control de errores.

Enlace flexible: Par de puertos que pueden configurarse para que uno se encargue de la transmisión de datos en caso de que el otro falle. Véanse también las definiciones de Puerto principal y Puerto standby.

RJ-45: Conectores estándar de 8 contactos para redes IEEE 802.3 10BASE-T.

RMON: Control remoto. Subred de SNMP MIB II que permite controlar y administrar capacidades tratando hasta un máximo de diez grupos de información diferentes.

RPS: **Sistema de Energía Redundante:** Dispositivo que ofrece una fuente de alimentación de apoyo cuando está conectado al Switch.

Agrupación centralizada de servidores: Conjunto de servidores en una ubicación centralizada para una gran población de usuarios.

SLIP: **Protocolo de internet sobre líneas serie:** Protocolo que permite que la IP funcione en una conexión de línea serie.

SNMP: **Protocolo simple de administración de red:** Protocolo diseñado originalmente para utilizarse en la administración de redes TCP/IP. Actualmente el protocolo SNMP se aplica en una amplia variedad de ordenadores y equipos de redes y pueden emplearse para administrar muchos aspectos del funcionamiento de redes y estaciones finales.

Protocolo del árbol de expansión (STP): Sistema basado en puentes para aportar tolerancia a fallos en redes. El protocolo STP funciona permitiendo implementar rutas paralelas para el tráfico de la red, y garantizar que las rutas redundantes están desactivadas cuando las rutas principales están operativas y activas si las rutas principales fallan.

Pila: Grupo de dispositivos de red integrados para formar un dispositivo lógico individual.

Puerto standby: Puerto de un enlace flexible que se encargará de la transmisión de datos si el puerto principal del enlace falla.

Switch: Dispositivo que filtra, envía y llena paquetes basados en la dirección de destino de los mismos. El switch memoriza las direcciones asociadas a cada puerto del switch y construye tablas basadas en esa información que se usarán en la decisión de conmutación.

TCP/IP: Conjunto formado por capas de protocolos de comunicaciones que ofrecen emulación de terminal Telnet, transferencia de archivos FTP y otros servicios de comunicación entre una gran variedad de equipos informáticos.

Telnet: Protocolo de aplicación TCP/IP que ofrece servicio de terminal virtual y permite al usuario conectarse a otro sistema informático y acceder a un host como si estuviera conectado directamente a este último.

TFTP: **Protocolo de Transferencia de Archivos Trivial:** Permite transferir archivos (como actualizaciones de software) de un dispositivo remoto utilizando capacidades de administración local del switch.

UDP: **Protocolo de Datagramas de Usuario:** Protocolo estándar de internet que permite que una aplicación de un dispositivo envíe un datagrama a una aplicación de otro dispositivo.

VLAN: **LAN virtual:** Grupo de dispositivos de ubicación y topología independientes que se comunican como si estuvieran en una LAN física común.

VLT: **Enlace troncal de LAN virtual**: Enlace switch a switch que lleva el tráfico de todas las VLANs en cada switch.

VT100: Tipo de terminal que utiliza caracteres ASCII. Los monitores VT100 tienen un aspecto basado en texto.