Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

Notas, avisos y precauciones

NOTA: una NOTA proporciona información importante que le ayudará a utilizar mejor el ordenador.

AVISO: un AVISO indica la posibilidad de daños en el hardware o la pérdida de datos, e informa de cómo evitar el problema.

PRECAUCIÓN: un mensaje de PRECAUCIÓN indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Marzo de 2005

Regresar a la página de contenido

Introducción

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

PowerConnect 3424/3448 y PowerConnect 3424P/3448P son dispositivos apilables y avanzados de varios niveles. Las unidades PowerConnect pueden funcionar como dispositivos de conmutación o como dispositivos apilables, independientes y de varios niveles, con hasta seis miembros del apilamiento.

Esta guía del usuario contiene la información necesaria para instalar, configurar y realizar el mantenimiento del dispositivo.

Descripción del sistema

PowerConnect 3424/3448 y PowerConnect 3424P/3448P combinan la versatilidad con una necesidad de administración mínima. Las series PowerConnect 3424 y 3448 incluyen los tipos de dispositivo siguientes:

- PowerConnect 3424
- PowerConnect 3424P
- PowerConnect 3448
- PowerConnect 3448P

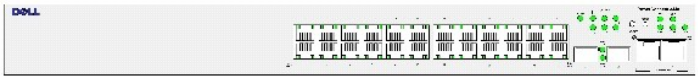
PowerConnect 3424

PowerConnect 3424 tiene 24 puertos 10/100 Mbps y dos puertos SFP, además de dos puertos de cobre que pueden utilizarse para reenviar tráfico en el caso de un dispositivo independiente, o bien como puertos de apilamiento cuando el dispositivo está apilado. Este dispositivo también cuenta con un puerto de consola RS-232. PowerConnect 3424 es un dispositivo apilable, pero también puede funcionar como unidad independiente.

PowerConnect 3424P

PowerConnect 3424P tiene 24 puertos 10/100 Mbps y dos puertos SFP, además de dos puertos de cobre que pueden utilizarse para reenviar tráfico en el caso de un dispositivo independiente, o bien como puertos de apilamiento cuando el dispositivo está apilado. Este dispositivo también cuenta con un puerto de consola RS-232. PowerConnect 3424P es un dispositivo apilable, pero también puede funcionar como unidad independiente. Asimismo, PowerConnect 3424P incorpora la función de alimentación a través de Ethernet (PoE).

Figura 1-1. PowerConnect 3424 y PowerConnect 3424P



PowerConnect 3448

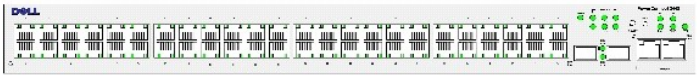
PowerConnect 3448 tiene 48 puertos 10/100 Mbps y dos puertos SFP, además de dos puertos de cobre que pueden utilizarse para reenviar tráfico en el caso de un dispositivo independiente, o bien como puertos de apilamiento cuando el dispositivo está apilado. Este dispositivo también cuenta con un puerto de consola RS-232. PowerConnect 3448 es un dispositivo apilable, pero también puede funcionar como unidad independiente.

PowerConnect 3448P

PowerConnect 3448P tiene 48 puertos 10/100 Mbps, dos puertos SFP y dos puertos de cobre que pueden utilizarse para reenviar tráfico cuando el dispositivo está instalado en modo independiente, o bien como puertos de apilamiento cuando el dispositivo forma parte de una pila. Este dispositivo también cuenta con

un puerto de consola RS-232. Además, PowerConnect 3448P incorpora la función de PoE.

Figura 1-2. PowerConnect 3448 y PowerConnect 3448P



Información general sobre el apilamiento

El apilamiento de PowerConnect 3424/P y PowerConnect 3448/P permite administrar varios conmutadores a través de un único punto, como si todos los miembros de la pila fueran una sola unidad. El acceso a todos los miembros de la pila se realiza mediante una única dirección IP, a través de la cual se administra la pila. La pila se puede administrar desde:

- Una interfaz basada en Web
- Una estación de administración SNMP
- La interfaz de línea de comandos (CLI)

Los dispositivos PowerConnect 3424/P y PowerConnect 3448/P permiten apilar hasta seis unidades por pila, pero también pueden funcionar como unidades independientes.

Durante la instalación del apilamiento, se selecciona un conmutador como unidad maestra de la pila, y se puede seleccionar otro miembro del apilamiento para que actúe como unidad maestra de reserva. Los demás dispositivos se seleccionan como miembros de la pila, y se les asigna una ID de unidad exclusiva.

El software del conmutador se descarga por separado para cada miembro de la pila. Sin embargo, todas las unidades de la pila deben tener instalada la misma versión del software.

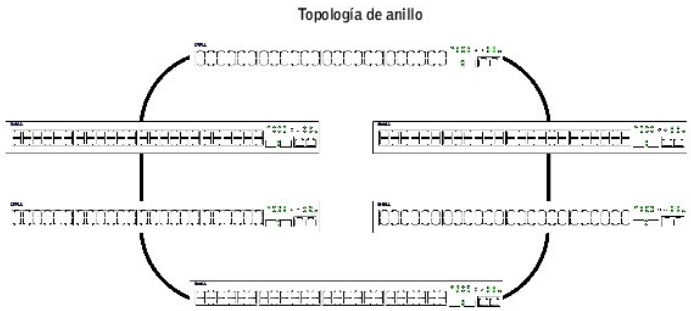
El apilamiento y la configuración del conmutador se realiza mediante la unidad maestra de la pila. La unidad maestra de la pila detecta y vuelve a configurar los puertos con un impacto mínimo sobre el funcionamiento en los casos siguientes:

- Si se produce un error en una unidad.
- Si se produce un error en el enlace de apilamiento entre unidades.
- Si se inserta una unidad.
- Si se extrae una unidad del apilamiento.

Topología de la pila

La serie PowerConnect 3400 funciona con una topología de anillo. En una topología de anillo apilada, todos los dispositivos de la pila están interconectados en forma de círculo. Cada dispositivo de la pila acepta datos y los envía al dispositivo al que está conectado. El paquete sigue su camino a través de la pila hasta que alcanza su destino. El sistema descubre cuál es la mejor ruta para enviar el tráfico.

Figura 1-3. Topología de anillo de apilamiento



La mayor parte de los problemas que se presentan en las toplogías de anillo se producen cuando un dispositivo del anillo deja de estar operativo o cuando hay un error en un enlace. En la pila de PowerConnect 3424/P y PowerConnect 3448/P, el sistema pasa automáticamente a una topología de sustitución tras error de apilamiento sin que se produzca ningún tiempo de inactividad. Se genera un mensaje de SNMP automáticamente, y no es necesario realizar ninguna acción de administración de la pila. Sin embargo, debe repararse el enlace o el miembro del apilamiento afectado para garantizar la integridad del apilamiento.

Una vez resueltos los problemas del apilamiento, es posible volver a conectar el dispositivo a la pila inmediatamente, y se restaura la topología de anillo.

Topología de sustitución tras error de apilamiento

Si se produce un error en la topología de apilamiento, la pila vuelve a la topología de sustitución tras error de apilamiento. En la topología de sustitución tras error de apilamiento, los dispositivos funcionan en cadena. La unidad maestra de la pila determina a dónde deben enviarse los paquetes. Cada unidad se conecta a dos dispositivos contiguos, excepto las unidades superior e inferior.

Miembros del apilamiento e ID de unidad

Las ID de unidad de apilamiento son esenciales para la configuración del apilamiento. El funcionamiento del apilamiento se determina durante el proceso de inicio. El modo de funcionamiento se determina mediante la ID de unidad seleccionada durante el proceso de inicialización. Por ejemplo, si el usuario ha seleccionado el modo independiente, el dispositivo se inicia como dispositivo independiente.

Cada unidad de dispositivo se entrega con una ID de unidad predeterminada de la unidad independiente. Si el dispositivo funciona como unidad independiente, todos los LED de apilamiento están apagados.

Una vez que el usuario seleccione una ID de unidad distinta, ésta ya no se borrará y seguirá siendo válida aunque se reinicie la unidad.

Las ID de unidad 1 y 2 están reservadas para unidades susceptibles de ser maestras. Las ID de unidad de la 3 a la 6 pueden definirse para los miembros de la pila.

Cuando se inicia la unidad maestra, o cuando se inserta o extrae un miembro de la pila, la unidad maestra da comienzo a un proceso de descubrimiento del apilamiento.

NOTA: si se detecta que dos miembros tienen la misma ID de unidad, la pila sigue funcionando, pero únicamente formará parte de la pila la unidad cuya unión se haya realizado antes. Se envía un mensaje al usuario en el que se le comunica que una unidad no ha podido unirse a la pila.

Extracción y sustitución de miembros del apilamiento

Las unidades 1 y 2 son unidades susceptibles de ser maestras. Las unidades 1 y 2 se designan como unidad maestra o como unidad maestra de reserva. La asignación de la unidad maestra de la pila se realiza durante el proceso de configuración. Uno de los miembros de la pila susceptibles de ser unidad maestra se elige como unidad maestra, y el otro se elige como unidad maestra de reserva, de acuerdo con el proceso de decisión siguiente:

- Si en la pila sólo existe una unidad susceptible de ser maestra, se elige ésta como unidad maestra.
- Si en la pila existen dos miembros susceptibles de ser unidad maestra, y uno de ellos se ha configurado manualmente como unidad maestra de la pila, se elige este miembro.
- Si en la pila existen dos unidades susceptibles de ser maestras y ninguna de ellas se ha configurado manualmente como unidad maestra, se elige como unidad maestra de la pila la unidad con un tiempo de actividad superior.
- Si en la pila existen dos unidades susceptibles de ser maestras y ambas se han configurado manualmente como unidad maestra, se elige como unidad maestra de la pila la unidad con un tiempo de actividad superior.
- Si los dos miembros de la pila susceptibles de ser unidad maestra tienen la misma antigüedad, se elige la unidad 1 como unidad maestra de la pila.

NOTA: se considera que dos miembros de un apilamiento tienen la misma antigüedad si ambos se han insertado con una diferencia de tiempo inferior o igual a diez minutos.

Por ejemplo, si la unidad 2 se inserta en el primer minuto de un ciclo de diez minutos y la unidad 1 se inserta en el quinto minuto de dicho ciclo, se considera que ambas unidades tienen la misma antigüedad. Si en la pila hay dos miembros susceptibles de ser unidad maestra que tienen la misma antigüedad, se elige la unidad 1 como unidad maestra.

La unidad maestra y la unidad maestra de copia de seguridad se mantienen en modo de espera activo. El modo de espera activo permite que la unidad

maestra de reserva sustituya la unidad maestra en caso de error. De esta forma, se garantiza que la pila siga funcionando con normalidad.

Durante el modo de espera activo, la unidad maestra y la unidad maestra de reserva sólo se sincronizan con la configuración estática. Cuando se configura la unidad maestra de un apilamiento, ésta debe sincronizarse con la unidad maestra de reserva. La configuración dinámica, como por ejemplo las direcciones MAC obtenidas dinámicamente, no se guarda.

Cada puerto de la pila tiene una ID de unidad, un tipo de puerto y un número de puerto específicos, que forman parte tanto de los comandos de configuración como de los archivos de configuración. Los archivos de configuración se administran únicamente desde la unidad maestra de la pila del dispositivo. Las tareas de administración son las siguientes:

- Guardar en la memoria Flash
- Cargar archivos de configuración en un servidor TFTP externo
- Descargar archivos de configuración desde un servidor TFTP externo

NOTA: se guarda la configuración de la pila para todos los puertos configurados, incluso si se restablece la pila o los puertos dejan de estar presentes.

A cada reinicio, se realiza un descubrimiento de la topología y la unidad maestra identifica todas las unidades de la pila. Las ID de unidad se guardan en la unidad y se obtienen a través del proceso de descubrimiento de la topología. Si una unidad intenta iniciarse sin que exista una unidad maestra seleccionada y la unidad no está en modo independiente, no se iniciará.

Los archivos de configuración sólo se modifican mediante la configuración explícita del usuario. Los archivos de configuración no se modifican automáticamente cuando:

- Se añaden unidades.
- Se extraen unidades.
- Se asignan nuevas ID de unidad a las unidades.
- Las unidades alternan el modo de apilamiento y el modo independiente.

Cada vez que se reinicia el sistema, se utiliza el archivo de configuración de inicio de la unidad maestra para configurar la pila.

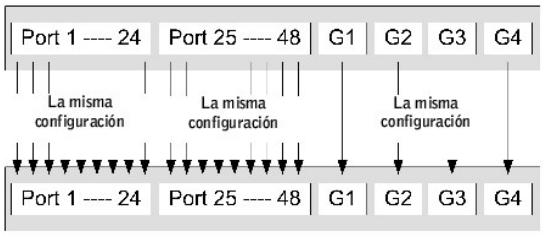
Si se extrae un miembro de la pila y se sustituye por una unidad que tiene la misma ID, el miembro de la pila se definirá con la configuración del dispositivo original. En la página de inicio del administrador de conmutadores PowerConnect OpenManage sólo aparecen los puertos que están presentes físicamente, que pueden configurarse mediante el sistema de administración Web. Los puertos que no están presentes se configuran a través de las interfaces CLI o SNMP.

Sustitución de miembros del apilamiento

Si se sustituye un miembro de la pila por otro miembro de pila con la misma ID de unidad, se aplica la configuración previa del dispositivo al miembro de la pila insertado. Si el nuevo dispositivo insertado tiene un número mayor o menor de puertos que el anterior, se aplica la configuración de puertos correspondiente al nuevo miembro de la pila. Por ejemplo:

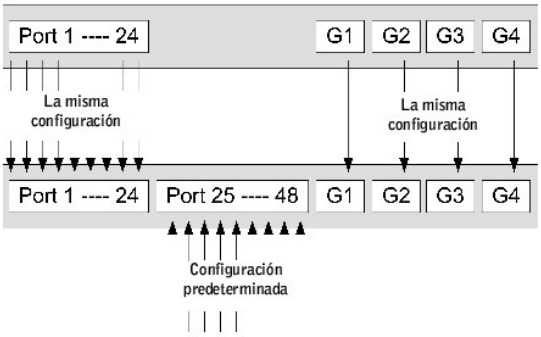
- Si una unidad PowerConnect 3424/P sustituye otra unidad PowerConnect 3424/P, se conservarán todas las configuraciones de puertos.
- Si una unidad PowerConnect 3448/P sustituye otra unidad PowerConnect 3448/P, se conservarán todas las configuraciones de puertos.

Figura 1-4. Unidad PowerConnect 3448/P sustituida por otra unidad PowerConnect 3448/P



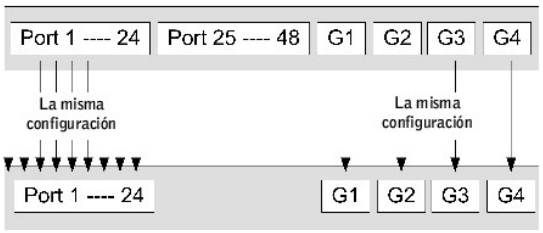
- Si una unidad PowerConnect 3448/P sustituye una unidad PowerConnect 3424/P, los primeros 24 puertos FE de 3448/P recibirán la configuración de los 24 puertos FE de 3424/P. Las configuraciones de los puertos GE no variarán. Para los puertos restantes se utilizará la configuración de puertos predeterminada.

Figura 1-5. Puerto de PowerConnect 3448/P sustituido por puerto de PowerConect 3424/P



- Si una unidad PowerConnect 3424/P sustituye una unidad PowerConnect 3448/P, los 24 puertos FE de PowerConnect 3424/P reciben la configuración de los primeros 24 puertos FE de PowerConnect 3448/P. Las configuraciones de los puertos GE no variarán.

Figura 1-6. Puerto de PowerConect 3424/P sustituido por puerto de PowerConnect 3448/P



Cambio de unidad maestra a unidad maestra de copia reserva

La unidad maestra de reserva sustituye la unidad maestra en los casos siguientes:

- Cuando se extrae la unidad maestra de la pila o se produce un error en dicha unidad.
- Cuando se produce un error en los enlaces de la unidad maestra de la pila a los miembros del apilamiento.
- Cuando se produce una conmutación por software a través de una interfaz Web o la CLI.

El paso de unidad maestra a unidad maestra de reserva conlleva una pérdida de servicio limitada. Las tablas dinámicas se obtendrán nuevamente si se produce un error. El archivo de configuración en ejecución está sincronizado entre la unidad maestra y la unidad maestra de reserva, y seguirá en ejecución en la unidad maestra de reserva.

Información general sobre las funciones

En esta sección se describen las funciones de los dispositivos. Si desea obtener una lista completa y actualizada de todas las funciones del dispositivo, consulte las **notas de la versión** del software más recientes.

Alimentación a través de Ethernet

La alimentación a través de Ethernet (PoE) proporciona alimentación a los dispositivos en un cableado de LAN existente sin que deba actualizarse ni modificarse la infraestructura de la red. PoE elimina la necesidad de colocar los dispositivos de red cerca de fuentes de energía. PoE puede utilizarse en las aplicaciones siguientes:

- Teléfonos IP

- Puntos de acceso inalámbrico
- Puertas de enlace IP
- PDA
- Supervisión remota de audio y vídeo

Para obtener más información sobre la alimentación a través de Ethernet, consulte "Administración de la alimentación a través de Ethernet".

Bloqueo de cabecera de línea

El bloqueo de cabecera de línea (HOL) provoca demoras en el tráfico y la pérdida de tramas debido a que el tráfico compite por los mismos recursos de puertos de salida. El bloqueo HOL pone en cola los paquetes, y los paquetes situados al principio de la cola se reenvían antes que los paquetes situados al final de la cola.

Compatibilidad con el control de flujo (IEEE 802.3X)

El control de flujo permite que dispositivos de velocidad inferior se comuniquen con dispositivos de velocidad superior solicitando que el dispositivo de velocidad mayor deje de enviar paquetes. Las transmisiones se detienen temporalmente para evitar un desbordamiento en el búfer.

Para obtener información sobre la configuración del control de flujo para puertos o LAG, consulte "Definición de la configuración de los puertos" o "Definición de los parámetros de LAG".

Compatibilidad con la contrapresión

En los enlaces semidúplex, el puerto receptor evita que se produzcan desbordamientos en el búfer ocupando el enlace de modo que éste no esté disponible para tráfico adicional.

Para obtener información sobre la configuración del control de flujo para puertos o LAG, consulte "Definición de la configuración de los puertos" o "Definición de los parámetros de LAG".

Pruebas virtuales de cables (VCT)

La función VCT permite detectar y notificar los posibles problemas de los cables en enlaces de cobre, como desconexiones o cortocircuitos. Para obtener más información sobre las pruebas de cables, consulte "Ejecución de los diagnósticos de cables".

Compatibilidad con MDI/MDIX

Cuando la negociación automática está activada, el dispositivo detecta automáticamente si el cable conectado a un puerto RJ-45 es cruzado o directo.

El cableado estándar para las estaciones finales se conoce como **interfaz dependiente del medio** (MDI), mientras que el cableado estándar para los concentradores y los conmutadores se conoce como **interfaz dependiente del medio con cable cruzado** (MDIX).

Para obtener información sobre la configuración de MDI/MDIX para puertos o LAG, consulte "Definición de la configuración de los puertos" o "Definición de los parámetros de LAG".

Negociación automática

La negociación automática permite que un dispositivo anuncie modos de funcionamiento. La función de negociación automática permite el intercambio de

información entre dos dispositivos que comparten un segmento de enlace punto a punto, así como la configuración automática de ambos dispositivos para aprovechar al máximo sus capacidades de transmisión.

La serie PowerConnect 3400 mejora la negociación automática, ya que incorpora la posibilidad de anunciar puertos. El anuncio de puertos permite al administrador del sistema configurar las velocidades de puerto que se anuncian.

Para obtener más información sobre la negociación automática, consulte "Definición de la configuración de los puertos" o "Definición de los parámetros de LAG".

Funciones compatibles con las direcciones MAC

Compatibilidad con la capacidad de las direcciones MAC

El dispositivo admite un máximo de 8.192 direcciones MAC. El dispositivo reserva direcciones MAC específicas para que las utilice el sistema.

Entradas de MAC estáticas

Las entradas de MAC pueden introducirse manualmente en la tabla de direcciones, en lugar de obtenerse a partir de las tramas entrantes. Estas entradas definidas por el usuario no caducan, y se conservan tras cualquier restablecimiento y reinicio.

Para obtener más información, consulte "Definición de direcciones estáticas".

Obtención automática de direcciones MAC

El dispositivo permite obtener automáticamente direcciones MAC a partir de los paquetes entrantes. Las direcciones MAC se almacenan en la tabla de direcciones.

Caducidad automática de las direcciones MAC

Las direcciones MAC desde las que no se ha recibido tráfico durante un periodo determinado caducan. Esto evita que se desborde la tabla de direcciones.

Para obtener más información sobre la configuración del periodo de caducidad de las direcciones MAC, consulte "Visualización de direcciones dinámicas".

Conmutación basada en MAC compatible con VLAN

El dispositivo realiza siempre puentes compatibles con VLAN. En cambio, no realiza puentes clásicos (IEEE802.1D), en los que las tramas se reenvían únicamente en función de su dirección MAC de destino. No obstante, puede configurarse una función parecida para las tramas sin etiqueta. Las tramas dirigidas a una dirección MAC de destino que no esté asociada con ningún puerto se distribuyen a todos los puertos de la VLAN pertinente.

Compatibilidad con la multidifusión de MAC

El servicio de multidifusión es un servicio de difusión limitado que permite las conexiones de uno a varios y de varios a varios para la distribución de la información. En el servicio de multidifusión de nivel 2, se dirige una única trama a una dirección de multidifusión específica desde la cual se transmiten copias de la trama a los puertos pertinentes.

Para obtener más información, consulte "Asignación de parámetros de multidifusión "reenviar todos"".

Funciones del nivel 2

Inspección de IGMP

La inspección de IGMP examina el contenido de las tramas de IGMP cuando las reenvía el dispositivo desde las estaciones de trabajo a un enrutador de multidifusión ascendente. Desde la trama, el dispositivo identifica las estaciones de trabajo configuradas para sesiones de multidifusión y los enrutadores de multidifusión que están enviando tramas de multidifusión.

Para obtener más información, consulte "Inspección de IGMP".

Duplicación de puertos

La duplicación de puertos supervisa y duplica el tráfico de red mediante el reenvío de copias de los paquetes entrantes y salientes de un puerto supervisado a un puerto supervisor. Los usuarios especifican qué puerto de destino recibe las copias de todo el tráfico que pasa por uno puerto de origen concreto.

Para obtener más información, consulte "Definición de sesiones de duplicación de puertos".

Control de tormentas de difusión

El control de tormentas permite limitar la cantidad de tramas de multidifusión y de difusión que el dispositivo acepta y reenvía.

Cuando se reenvían las tramas de nivel 2, las tramas de difusión y de multidifusión se distribuyen a todos los puertos de la VLAN pertinente. De este modo se ocupa amplitud de banda y se cargan todos los nodos conectados en todos los puertos.

Para obtener más información, consulte "Activación del control de tormentas".

Funciones compatibles con VLAN

Compatibilidad con VLAN

Las VLAN son grupos de puertos de conmutación que se componen de un único dominio de difusión. Los paquetes se clasifican como pertenecientes a una VLAN según la etiqueta de VLAN o según una combinación del puerto de entrada y el contenido del paquete. Los paquetes que comparten atributos comunes pueden agruparse en la misma VLAN.

Para obtener más información, consulte "Configuración de redes VLAN".

LAN virtuales (VLAN) basadas en puertos

Las VLAN basadas en puertos clasifican los paquetes entrantes en las VLAN según su puerto de entrada.

Para obtener más información, consulte "Definición de la configuración de puertos de VLAN".

Conformidad completa con el etiquetado de VLAN 802.1Q

El estándar IEEE 802.1Q define una arquitectura para las LAN virtuales con puentes, los servicios incluidos en las VLAN, y los protocolos y algoritmos que intervienen en la prestación de dichos servicios.

Compatibilidad con GVRP

El protocolo de registro de VLAN de GARP (GVRP) permite eliminar y crear dinámicamente VLAN de conformidad con el estándar IEEE 802.1Q en puertos combinados 802.1Q. Cuando se activa GVRP, el dispositivo registra y propaga la pertenencia a la VLAN en todos los puertos que forman parte de la topología activa subyacente de las "Funciones del protocolo de árbol de extensión".

Para obtener más información, consulte "Configuración de los parámetros de GVRP".

VLAN privadas

Los puertos de VLAN privada, una función de seguridad del nivel 2, permiten aislar los puertos entre sí dentro de un mismo dominio de difusión.

Para obtener más información sobre las VLAN privadas, consulte "Configuración de redes VLAN privadas".

Funciones del protocolo de árbol de extensión

Protocolo de árbol de extensión (STP)

El árbol de extensión 802.1d es un requisito del conmutador de nivel 2 estándar que permite crear puentes para evitar y resolver automáticamente los bucles de reenvío de nivel 2 (L2). Los conmutadores intercambian mensajes de configuración utilizando tramas formateadas específicamente, y activan y desactivan de forma selectiva el reenvío en los puertos.

Para obtener más información, consulte "Configuración del protocolo de árbol de extensión".

Enlace rápido

El protocolo STP puede tardar entre 30 y 60 en converger. Durante este tiempo, STP detecta los posibles bucles y deja tiempo para permitir que los cambios de estado se propaguen y que los dispositivos implicados respondan. El intervalo de entre 30 y 60 segundos se considera un tiempo de respuesta demasiado largo para muchas aplicaciones. La opción de enlace rápido evita esta demora y puede utilizarse en topologías de red en las que no se producen bucles de reenvío.

Para obtener más información sobre la activación del enlace rápido para puertos y LAG, consulte "Definición de la configuración STP de puertos" o "Definición de direcciones estáticas".

Protocolo de árbol de extensión rápida IEEE 802.1w

El árbol de extensión puede tardar entre 30 y 60 segundos para que cada host determine si sus puertos reenvían tráfico de forma activa. El protocolo de árbol de extensión rápida (RSTP) detecta los usos de las topologías de red para permitir una convergencia más rápida sin que se creen bucles de reenvío.

Para obtener más información, consulte "Definición del árbol de extensión rápida".

Protocolo de árbol de extensión múltiple IEEE 802.1s

El protocolo de árbol de extensión múltiple (MSTP) asigna las VLAN a instancias de STP. MSTP incorpora un escenario de equilibrado de carga distinto. Los paquetes asignados a varias VLAN se transmiten por distintas rutas dentro de las zonas MSTP (zonas MST). Las zonas son uno o varios puentes MSTP a través de los cuales pueden transmitirse tramas. El estándar permite a los administradores asignar tráfico de VLAN a rutas exclusivas.

Para obtener más información, consulte "Configuración del protocolo de árbol de extensión".

Agregación de enlaces

Agregación de enlaces

Agregación de enlaces

Es posible definir hasta ocho enlaces agregados, que pueden tener hasta ocho puertos cada uno, para formar un grupo agregado de enlaces (LAG). Esto permite lo siguiente:

- Protección de tolerancia a fallos contra la interrupción de enlaces físicos
- Conexiones con una amplitud de banda mayor
- Mejor resolución de la amplitud de banda
- Conectividad del servidor de alta amplitud de banda

Un LAG se compone de puertos que tienen la misma velocidad y que están configurados para funcionar en modo dúplex completo.

Para obtener más información, consulte "Definición de los parámetros de LAG".

Agregación de enlaces y LACP

El protocolo de control de agregación de enlaces (LACP) utiliza intercambios homólogos entre enlaces para determinar contínuamente la capacidad de agregación de diversos enlaces, y proporciona de forma ininterrumpida el máximo nivel de capacidad de agregación posible entre un determinado par de dispositivos. LACP determina, configura, vincula y supervisa automáticamente la vinculación de los puertos dentro del sistema.

Para obtener más información, consulte "Agregado de puertos".

Clientes BootP y DHCP

El protocolo de configuración dinámica de host (DHCP) permite la recepción de parámetros de configuración adicionales desde un servidor de red al iniciarse el sistema. El servicio DHCP es un proceso continuo. DHCP es una extensión de BootP.

Para obtener más información sobre DHCP, consulte "Definición de los parámetros de interfaces IP DHCP".

Funciones de calidad de servicio

Compatibilidad con la clase de servicio 802.1p

La técnica de señalización IEEE 802.1p es un estándar OSI de nivel 2 para marcar y priorizar el tráfico de red en el subnivel MAC/enlace de datos. El tráfico de 802.1p se clasifica y se envía a su destino. No se establecen ni se aplican reservas o límites de amplitud de banda. El estándar 802.1p deriva del estándar 802.1Q (VLAN). 802.1p establece ocho niveles de prioridad, de forma parecida al campo de bits de encabezado IP de precedencia IP.

Para obtener más información, consulte "Configuración de la calidad de servicio".

Funciones de administración de dispositivos

Registros de excepciones y alarmas de SNMP

El sistema registra los eventos con códigos de gravedad e indicación de la hora. Los eventos se envían como excepciones de SNMP a una lista de destinatarios de excepciones.

Para obtener más información sobre las alarmas y las excepciones de SNMP, consulte "Definición de los parámetros de SNMP".

Versiones 1, 2 y 3 de SNMP

El protocolo simple de administración de red (SNMP) sobre el protocolo UDP/IP controla el acceso al sistema; se define una lista de entradas de comunidad, cada una de las cuales se compone de una cadena de comunidad y de los privilegios de acceso correspondientes. Existen tres niveles de seguridad SNMP: de sólo lectura, de lectura y escritura, y super. Sólo un superusuario puede acceder a la tabla de comunidades.

Para obtener más información, consulte "Definición de los parámetros de SNMP".

Administración basada en Web

Con la administración basada en Web, puede administrarse el sistema desde cualquier explorador Web. El sistema cuenta con un servidor Web integrado (EWS) que contiene las páginas HTML a través de las que puede supervisarse y configurarse el sistema. El sistema convierte internamente la entrada basada en Web en comandos de configuración, valores de variables de MIB y otras opciones relativas a la administración.

Carga y descarga del archivo de configuración

La configuración del dispositivo se almacena en un archivo de configuración. El archivo de configuración incluye tanto la configuración del dispositivo de todo el sistema como la específica de cada puerto. El sistema puede mostrar archivos de configuración en forma de grupo de comandos de la CLI, que se almacenan y manipulan como archivos de texto.

Para obtener más información, consulte "Administración de archivos".

Protocolo trivial de transferencia de archivos (TFTP)

El dispositivo admite la carga y descarga de imágenes de inicio, software y configuración a través de TFTP.

Supervisión remota

La supervision remota (RMON) es una extensión de SNMP que proporciona funciones completas de supervisión del tráfico de red, a diferencia de SNMP, que únicamente permite la administración y supervisión del dispositivo de red. La RMON es una MIB estándar que define las estadísticas actuales e históricas del nivel MAC y los objetos de control, lo que permite capturar información en tiempo real en toda la red.

Para obtener más información, consulte "Visualización de estadísticas".

Interfaz de línea de comandos

La sintaxis y la semántica de la interfaz de línea de comandos (CLI) se adaptan a las prácticas habituales en el sector en la medida de lo posible. La CLI se compone de elementos obligatorios y opcionales. El intérprete de la CLI completa comandos y palabras clave para ayudar al usuario y ahorrar tiempo de tecleo.

Syslog

Syslog es un protocolo que permite enviar notificaciones de eventos a un conjunto de servidores remotos, donde se almacenan, analizan y resuelven. El sistema envía notificaciones de los eventos significativos en tiempo real y mantiene un registro de dichos eventos para su uso posterior.

Para obtener más información sobre Syslog, consulte "Administración de registros".

SNTP

El protocolo simple de hora de red (SNTP) garantiza una sincronización de la hora del conmutador Ethernet de la red con una precisión de milisegundos. La sincronización de la hora se lleva a cabo mediante un servidor SNTP de la red. Los recursos de hora se establecen por capas. Las capas definen la distancia desde el reloj de referencia. Cuanto más alta sea la capa (el valor de la parte superior es cero), más preciso será el reloj.

Para obtener más información, consulte "Configuración de SNTP".

Sistema de nombres de dominio

El sistema de nombres de dominio (DNS) convierte los nombres de dominio definidos por el usuario en direcciones IP. Cada vez que se asigna un nombre de dominio, el servicio DNS convierte el nombre en una dirección IP numérica. Por ejemplo, www.ejemploip.com se convierte en 192.87.56.2. Los servidores DNS mantienen las bases de datos de nombres de dominio y las direcciones IP correspondientes.

Para obtener más información, consulte "Configuración de sistemas de nombres de dominio".

Traceroute

Traceroute descubre las rutas IP por las que se han reenviado los paquetes durante el proceso de reenvío. La utilidad Traceroute de la CLI puede ejecutarse tanto desde el modo user-exec como desde otros modos con privilegios.

Funciones de seguridad

SSL

La capa de conexión segura (SSL) es un protocolo de nivel de aplicación que permite realizar de forma segura transacciones de datos, garantizando la confidencialidad, autenticación e integridad de los datos. Se basa en certificados y en claves públicas y privadas.

Autenticación basada en el puerto (802.1x)

La autenticación basada en el puerto permite autenticar a los usuarios del sistema en cada puerto a través de un servidor externo. Únicamente los usuarios autenticados y aprobados por el sistema pueden transmitir y recibir datos. Los puertos se autentican mediante el servidor del servicio de usuario de acceso telefónico de autenticación remota (RADIUS) utilizando el protocolo de autenticación extensible (EAP).

Para obtener más información, consulte "Configuración de la autenticación basada en el puerto".

Compatibilidad con el bloqueo de puertos

El bloqueo de puertos aumenta la seguridad de la red al limitar el acceso en puertos concretos a únicamente usuarios con direcciones MAC específicas. Estas direcciones se definen manualmente o bien se obtienen en el puerto pertinente. Cuando se detecta una trama en un puerto bloqueado y la dirección MAC de origen de la trama no está vinculada a dicho puerto, se inicia el mecanismo de protección.

Para obtener más información, consulte "Configuración de la seguridad de puertos".

Cliente RADIUS

RADIUS es un protocolo de cliente/servidor. Un servidor RADIUS mantiene una base de datos de usuarios que contiene información de autenticación por usuario como el nombre de usuario, la contraseña e información de la cuenta.

Para obtener más información, consulte "Configuración de los valores de RADIUS".

SSH

Secure Shell (SSH) es un protocolo que permite realizar una conexión remota segura con un dispositivo. Actualmente se admite la versión 2 de SSH. La función de servidor SSH permite a los clientes SSH establecer una conexión cifrada segura con un dispositivo. Esta conexión proporciona una funcionalidad parecida a una conexión Telnet de entrada. SSH utiliza el cifrado de clave pública RSA y DSA para las conexiones de dispositivos y la autenticación.

TACACS+

TACACS+ proporciona una seguridad centralizada para la validación de los usuarios que acceden a un dispositivo. TACACS+ es un sistema de administración de usuarios centralizado que, además, es compatible con RADIUS y otros procesos de autenticación.

Para obtener más información, consulte "Definición de la configuración de TACACS+".

Administración de contraseñas

La administración de contraseñas aumenta la seguridad en la red y mejora el control de las contraseñas. Las contraseñas para el acceso SSH, Telnet, HTTP, HTTPS y SNMP tienen funciones de seguridad asignadas. Para obtener más información sobre la administración de contraseñas, consulte "Administración de contraseñas".

Documentación adicional sobre la CLI

En la guía de referencia de la CLI, incluida en el CD de documentación, encontrará información sobre los comandos de la CLI utilizados para configurar el dispositivo. En este documento también se proporciona información como descripciones de los comandos, la sintaxis, los valores predeterminados, pautas y ejemplos.

Regresar a la página de contenido

Regresar a la página de contenido

Descripción del hardware

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

Descripción de los puertos

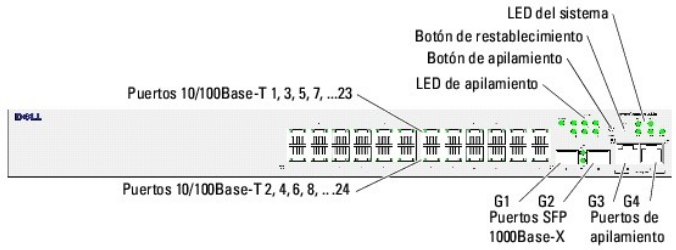
Descripción de los puertos de PowerConnect 3424

El dispositivo PowerConnect 3424 se configura con los puertos siguientes:

- **24 puertos Fast Ethernet**: puertos RJ-45 designados como puertos 10/100Base-T
- **Dos puertos de fibra**: designados como puertos SFP 1000Base-X SFP
- **Dos puertos Gigabit**: designados como puertos 1000Base-T
- **Puerto de consola**: puerto RS-232

En la figura siguiente se muestra el panel frontal de PowerConnect 3424.

Figura 2-1. Panel frontal de PowerConnect 3424



El panel frontal incluye 24 puertos RJ-45 numerados del 1 al 24. La fila superior de puertos aparece marcada con los números impares del 1 al 23, y la fila inferior de puertos aparece marcada con los números pares del 2 al 24. Además, el panel frontal también cuenta con los puertos G1-G2 (puertos de fibra) y los puertos G3-G4 (puertos de cobre). Los puertos G3-G4 se pueden utilizar como puertos de apilamiento o para reenviar tráfico de red en un dispositivo independiente.

El panel frontal incluye dos botones. El botón de ID de pila se utiliza para selecciona el número de unidad. El segundo botón es el botón de restablecimiento, que se utiliza para restablecer manualmente el dispositivo. El botón de restablecimiento está situado en la superficie del panel frontal, lo que evita que se presione accidentalmente. En el panel frontal se encuentran todos los LED del dispositivo.

En la figura siguiente se muestra la parte posterior de PowerConnect 3424:

Figura 2-2. Panel posterior de PowerConnect 3424

La parte posterior incluye un conector RPS, un puerto de consola y un conector de alimentación.

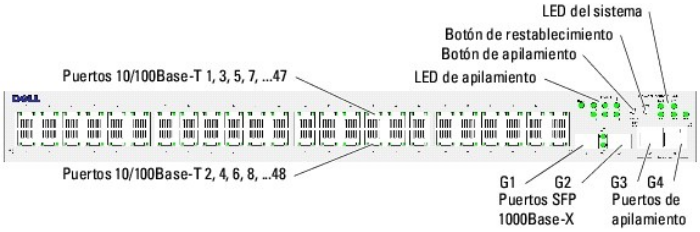
Descripción de los puertos de PowerConnect 3448

El dispositivo PowerConnect 3448 se configura con los puertos siguientes:

- **48 puertos Fast Ethernet**: puertos RJ-45 designados como puertos 10/100Base-T.
- **Dos puertos de fibra**: designados como puertos SFP 1000Base-X SFP
- **Dos puertos Gigabit**: designados como puertos 1000Base-T
- **Puerto de consola**: puerto RS-232 basado en consola

En la figura siguiente se muestra el panel frontal de PowerConnect 3448.

Figura 2-3. Panel frontal de PowerConnect 3448

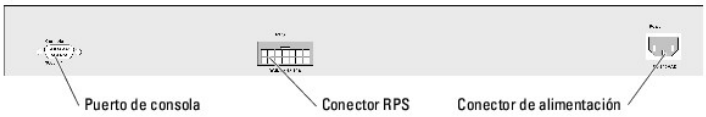


El panel frontal incluye 48 puertos RJ-45 numerados del 1 al 48. La fila superior de puertos aparece marcada con los números impares del 1 al 47, y la fila inferior de puertos aparece marcada con los números pares del 2 al 48. Además, el panel frontal también cuenta con los puertos G1-G2 (puertos de fibra) y los puertos G3-G4 (puertos de cobre). Los puertos G3-G4 se pueden utilizar como puertos de apilamiento o para reenviar tráfico de red en un dispositivo independiente.

El panel frontal incluye dos botones. El botón de ID de pila se utiliza para selecciona el número de unidad. El segundo botón es el botón de restablecimiento, que se utiliza para restablecer manualmente el dispositivo. El botón de restablecimiento está situado en la superficie del panel frontal, lo que evita que se presione accidentalmente. En el panel frontal se encuentran todos los LED del dispositivo.

En la figura siguiente se muestra el panel posterior de PowerConnect 3448:

Figura 2-4. Panel posterior de PowerConnect 3448



La parte posterior incluye un conector RPS, un puerto de consola y un conector de alimentación.

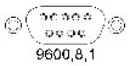
Puertos SFP

Los puertos SFP (factor de forma pequeño conectable) constituyen una interfaz TWSI (interfaz serie de dos cables) para la comunicación a través de un dispositivo CPLD (dispositivo lógico programable complejo) que se designa como 1000Base-SX o LX.

Puerto de consola RS-232

Para llevar a cabo la depuración de errores y la descarga de software, entre otras operaciones, se utiliza un conector DB-9 para una conexión de terminal. La velocidad en baudios predeterminada es 9 600 bps. La velocidad en baudios se puede configurar de 2 400 bps a 115 200 bps.

Figura 2-5. Puerto de consola



Dimensiones físicas

Los dispositivos PowerConnect 3424/P y PowerConnect 3448/P presentan las dimensiones físicas siguientes:

Dispositivo con PoE:

- **Anchura**: 440 mm
- **Profundidad**: 387 mm
- **Altura**: 43,2 mm

Dispositivo sin PoE:

- **Anchura**: 440 mm
- **Profundidad**: 257 mm
- **Altura**: 43,2 mm

Definiciones de los LED

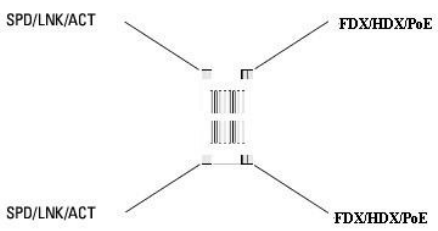
El panel frontal incluye diodos emisores de luz (LED) que indican el estado de los enlaces, las fuentes de alimentación, los ventiladores y los diagnósticos del sistema.

LED de los puertos

Cada puerto 10/100/1000Base-T y 10/100Base-T dispone de dos LED. El LED de velocidad se encuentra en la parte izquierda del puerto, mientras que el LED de enlace/dúplex/actividad se encuentra en la parte derecha.

En la figura siguiente se muestran los LED del puerto 10/100Base-T en los conmutadores PowerConnect 3424/P y PowerConnect 3448/P:

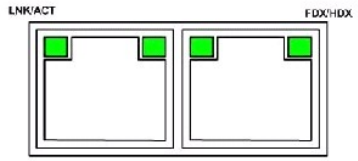
Figura 2-6. LED del puerto RJ-45 10/100Base-T de cobre



El puerto RJ-45 100Base-T de PowerConnect 3424/P y de PowerConnect 3448/P cuenta con dos LED de enlace/actividad (LNK/ACT).

En la figura siguiente se muestran los LED del puerto 100Base-T.

Figura 2-7. LED del puerto RJ-45 100Base-T



Las indicaciones de los LED RJ-45 de PowerConnect 3424 y PowerConnect 3448 se describen en la tabla siguiente:

Tabla 2-1. Indicaciones de los LED RJ-45 100Base-T de PowerConnect 3424 y PowerConnect 3448

LED	Luz	Descripción
Enlace/actividad/ velocidad	Verde fija	El puerto se ejecuta a 100 Mbps.
	Verde parpadeante	El puerto está transmitiendo o recibiendo datos a 100 Mbps.
	Amarilla fija	El puerto se ejecuta a 10 Mbps.
	Amarilla parpadeante	El puerto está transmitiendo o recibiendo datos a 10 Mbps.
	Apagada	El puerto no está en funcionamiento.
Dúplex completo (FDX)	Verde fija	El puerto funciona en modo dúplex completo.
	Apagada	El puerto funciona en modo semidúplex.

Las indicaciones de los LED RJ-45 de PowerConnect 3424/P y PowerConnect 3448/P se describen en la tabla siguiente:

Tabla 2-2. Indicaciones de los LED RJ-45 100Base-T de cobre de PowerConnect 3424/P y PowerConnect 3448/P

LED	Luz	Descripción
Velocidad/enlace/actividad	Verde fija	El puerto está enlazado a 100 Mbps.
	Verde parpadeante	El puerto funciona a 100 Mbps.
	Apagada	El puerto funciona a 10 Mbps o no está enlazado.
PoE	Verde fija	El dispositivo alimentado (PD) se ha detectado y funciona con una carga normal. Para obtener más información sobre los dispositivos alimentados, consulte "Administración de la alimentación a través de Ethernet".
	Ámbar fija	Se ha producido una sobrecarga o un cortocircuito en el dispositivo alimentado. Para obtener más información sobre los fallos de la alimentación a través de Ethernet, consulte "Administración de la alimentación a través de Ethernet".
	Ámbar parpadeante	El consumo de energía del dispositivo alimentado sobrepasa la asignación de energía predefinida. Para obtener más información sobre las asignaciones de energía en la alimentación a través de Ethernet, consulte "Administración de la alimentación a través de Ethernet".
	Apagada	No se ha detectado ningún dispositivo alimentado.

LED del puerto Gigabit

En la tabla siguiente se describen los LED del puerto Gigabit (puerto de apilamiento):

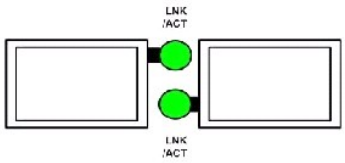
Tabla 2-3. Indicaciones de los LED RJ-45 100Base-T de cobre de PowerConnect 3424 y PowerConnect 3448

LED	Luz	Descripción
Enlace/actividad/ velocidad	Verde fija	El puerto se ejecuta a 1 000 Mbps.
	Verde parpadeante	El puerto está transmitiendo o recibiendo datos a 1 000 Mbps.
	Amarilla fija	El puerto se ejecuta a 10 o 100 Mbps.
	Amarilla parpadeante	El puerto está transmitiendo o recibiendo datos a 10 o 100 Mbps.
	Apagada	El puerto no está en funcionamiento.
Dúplex completo (FDX)	Verde fija	El puerto funciona en modo dúplex completo.
	Apagada	El puerto funciona en modo semidúplex.

LED de SFP

Cada puerto SFP cuenta con un LED de enlace/actividad (LNK/ACT). En los dispositivos PowerConnect 3424/P y PowerConnect 3448/P, los LED se encuentran entre los puertos y tienen forma redonda. En la figura siguiente se muestran los LED de cada dispositivo.

Figura 2-8. LED del puerto SFP



Las indicaciones de los LED de SFP se describen en la tabla siguiente:

Tabla 2-4. Indicaciones de los LED del puerto SFP

LED	Luz	Descripción
Enlace/actividad (LNK/ACT)	Verde fija	Se ha establecido un enlace.
	Verde parpadeante	El puerto está transmitiendo o recibiendo datos.
	Apagada	El puerto no está enlazado.

LED del sistema

Los LED del sistema de los dispositivos PowerConnect 3424/P y PowerConnect 3448/P proporcionan información sobre las fuentes de alimentación, los ventiladores, las condiciones térmicas y los diagnósticos. En la figura siguiente se muestran los LED del sistema.

Figura 2-9. LED del sistema

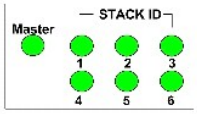
En la tabla siguiente se describen las indicaciones de los LED del sistema.

Tabla 2-5. Indicaciones de los LED del sistema

LED	Luz	Descripción
Fuente de alimentación (PWR)	Verde fija	El conmutador está encendido.
	Apagada	El conmutador está apagado.
Fuente de alimentación redundante (RPS) (modelos: 3424 y 3448)	Verde fija	La RPS está en funcionamiento.
	Roja fija	La RPS ha fallado.
	Apagada	La fuente de alimentación redundante no está conectada.
Fuente de alimentación redundante (RPS) (modelos: 3424P y 3448P)	Verde fija	La RPS está en funcionamiento.
	Apagada	La fuente de alimentación redundante ha fallado o no está conectada.
Diagnósticos (DIAG)	Verde parpadeante	Se está realizando la prueba de diagnóstico del sistema.
	Verde fija	La prueba de diagnóstico del sistema se ha realizado correctamente.
	Roja fija	La prueba de diagnóstico del sistema ha fallado.
	Apagada	El sistema funciona con normalidad.
Temperatura (TEMP)	Roja fija	El dispositivo se encuentra fuera del intervalo de temperaturas permitido.
	Apagada	El dispositivo funciona dentro del intervalo de temperaturas permitido.
Ventilador (FAN)	Verde fija	Todos los ventiladores del dispositivo funcionan correctamente.
	Roja fija	Uno o varios ventiladores del dispositivo no funcionan.

Los LED de apilamiento indican la posición de la unidad en la pila. En la figura siguiente se muestran los LED del panel frontal.

Figura 2-10. LED de apilamiento



Los LED de apilamiento están numerados del 1 al 6. Cada unidad de apilamiento tiene un LED de apilamiento, que indica el número de la ID de unidad. Si se enciende el LED de apilamiento 1 o 2, significa que el dispositivo es la unidad maestra o la unidad maestra de reserva de la pila.

Tabla 2-6.

LED	Luz	Descripción
Todos los LED de apilamiento	Apagada	El conmutador es actualmente un dispositivo independiente.
LED de apilamiento 1-6 (S1-S6)	Verde fija	El dispositivo está designado como N de unidad de apilamiento.
	Apagada	El dispositivo no está designado como N de unidad de apilamiento.
LED de unidad maestra de apilamiento	Verde fija	El dispositivo es la unidad maestra de la pila.
	Apagada	El dispositivo no es la unidad maestra de la pila.

Indicaciones de los LED de apilamiento

Fuentes de alimentación

El dispositivo cuenta con una unidad de fuente de alimentación interna (unidad de CA) y un conector para conectar los dispositivos PowerConnect 3424/P y PowerConnect 3448/P a una unidad PowerConnect EPS-470, o para conectar los dispositivos PowerConnect 3424 y PowerConnect 3448 devices a una unidad PowerConnect RPS-600. Los dispositivos PowerConnect 3424/P y PowerConnect 3448/P cuentan con una fuente de alimentación interna de 12 voltios.

El funcionamiento con ambas unidades de fuente de alimentación se regula a través del reparto de la carga. Los LED de la fuente de alimentación indican el estado de la fuente de alimentación.

Los dispositivos PowerConnect 3424/P y PowerConnect 3448/P cuentan con una fuente de alimentación interna de 470 W (12 V/-48 V), con un total de 370 W para el dispositivo con PoE de 24 puertos.

Unidad de fuente de alimentación de CA

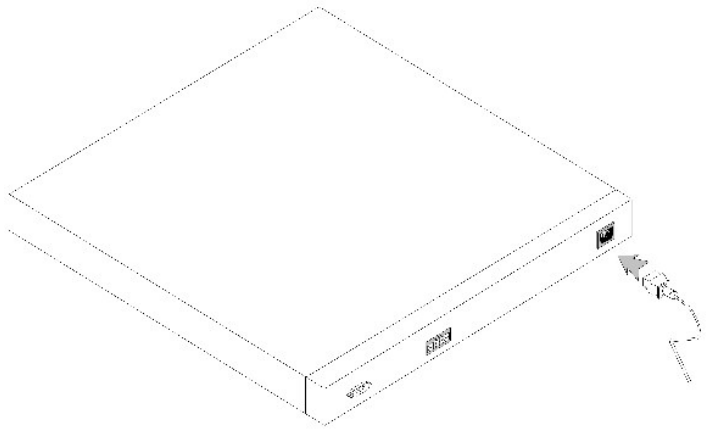
La unidad de fuente de alimentación de CA funciona a 90-264 V CA y 47-63 Hz. La unidad de fuente de alimentación de CA utiliza un conector estándar. El indicador LED se encuentra en el panel frontal e indica si la unidad de CA está conectada.

Unidad de fuente de alimentación de CC

Los conmutadores PowerConnect 3424 y PowerConnect 3448 se conectan a una unidad RPS-600 externa para proporcionar una opción de alimentación redundante. No es necesario realizar ninguna configuración. El LED de "RPS" del panel frontal indica si la unidad RPS-600 externa está conectada. En la tabla 2-5 encontrará una definición de LED de RPS.

Los conmutadores PowerConnect 3424/P y PowerConnect 3448/P se conectan a una unidad EPS-470 externa para proporcionar una opción de alimentación redundante. No es necesario realizar ninguna configuración. El LED de "RPS" del panel frontal indica si la unidad EPS-470 externa está conectada. En la tabla 2-5 encontrará una definición de LED de RPS.

Figura 2-11. Conexión a la alimentación



Cuando se conecta el dispositivo a una fuente de energía distinta, se reduce la probabilidad de que se produzcan fallos en caso interrumpirse la alimentación.

Botón de ID de pila

El panel frontal del dispositivo incluye un botón de ID de pila que permite seleccionar manualmente la ID de unidad para la unidad maestra y los miembros de la pila.

La unidad maestra y los miembros de la pila deben seleccionarse antes de que transcurran 15 segundos tras el inicio del dispositivo. Si no se selecciona la unidad maestra de la pila en ese plazo de tiempo, el dispositivo se iniciará en modo independiente. Para seleccionar una ID de unidad para el dispositivo, deberá reiniciar el dispositivo.

La unidad maestra de la pila recibe la ID de unidad 1 o 2. Si las unidades 1 y 2 están presentes, la unidad que no se seleccione funcionará como unidad maestra de reserva. Los miembros de la pila reciben una ID de unidad diferente (3-6). Por ejemplo, si hay cuatro unidades en una pila, la unidad maestra será la unidad 1 o 2, la unidad maestra de reserva será la unidad 1 o 2 (según cuál sea la ID de unidad de la unidad maestra), el tercer miembro de la pila será la unidad 3, y el cuarto miembro de la pila será la unidad 4.

NOTA: el dispositivo no detecta automáticamente las unidades independientes. Si una ID de unidad ya se ha seleccionado, presione el botón de ID de pila varias veces hasta que no quede ningún LED de apilamiento encendido.

Botón de restablecimiento

Los conmutadores PowerConnect 3424/P y PowerConnect 3448/P cuentan con un botón de restablecimiento, ubicado en el panel frontal, que permite llevar a cabo un restablecimiento manual del dispositivo. Si se restablece el dispositivo maestro, se restablecerá toda la pila. Si sólo se restablece una unidad miembro del apilamiento, no se restablecerán los miembros restantes.

El circuito de restablecimiento sencillo del conmutador se activa por condiciones de encendido o de bajo voltaje.

Sistema de ventilación

Los conmutadores PowerConnect 3424/P y PowerConnect 3448/P con la función PoE (alimentación a través de Ethernet) tienen cinco ventiladores integrados. Los dispositivos PowerConnect 3424 y PowerConnect 3448 sin PoE tienen dos ventiladores integrados. Para verificar el funcionamiento del sistema de ventilación, observe el LED que indica si hay fallos en los ventiladores.

Regresar a la página de contenido

Regresar a la página de contenido

Instalación de PowerConnect 3424/P y PowerConnect 3448/P

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

Preparación del sitio

Los dispositivos PowerConnect 3424/P y PowerConnect 3448/P se pueden montar en un rack estándar de 48,26 cm, colocar sobre un escritorio o montar en una pared. Antes de instalar la unidad, verifique que la ubicación elegida cumpla los requisitos siguientes:

- **Alimentación**: la unidad está instalada cerca de una toma eléctrica de 100-240 V CA y 50-60 Hz de fácil acceso.
- **General**: la fuente de alimentación redundante (RPS) está instalada correctamente; para ello, compruebe que los LED del panel frontal estén encendidos.
- **Modelos PoE**: la RPS ya está instalada; para ello, compruebe que los LED de PoE del panel frontal estén encendidos.
- **Espacio libre**: hay suficiente espacio libre delante del equipo para el acceso del operador. Deje espacio libre para el cableado, las conexiones de alimentación y la ventilación.
- **Cableado**: el cableado está canalizado para evitar fuentes de ruido eléctrico, como radiotransmisores, amplificadores de transmisión, líneas de alimentación e instalaciones fijas de luz fluorescente.
- **Requisitos ambientales**: el intervalo de temperatura ambiental de funcionamiento de la unidad es de 0 a 50 °C con una humedad relativa máxima del 95 %, sin conducción.

Desembalaje

Contenido del paquete

Cuando desembale el dispositivo, asegúrese de que se incluyen los elementos siguientes:

- Dispositivo/conmutador
- Cable de alimentación de CA
- Cable cruzado RS-232
- Almohadillas de goma autoadhesivas
- Kit de montaje en rack para la instalación en rack o kit para montaje en pared
- CD de documentación
- Guía de información del producto

Desembalaje del dispositivo

NOTA: antes de desembalar el dispositivo, examine el paquete e informe inmediatamente de cualquier daño.

1. Coloque la caja en una superficie plana y limpia.
2. Abra la caja o extraiga la parte superior de ésta.
3. Extraiga con precaución el dispositivo de la caja y colóquelo en una superficie estable y limpia.
4. Extraiga todo el material de embalaje.
5. Compruebe que el dispositivo y los accesorios no estén dañados. Informe inmediatamente de cualquier daño.

Montaje del dispositivo

Las instrucciones de montaje siguientes corresponden a los dispositivos PowerConnect 3424/P y PowerConnect 3448/P. El puerto de la consola se encuentra en el panel posterior. Los conectores de alimentación se encuentran en el panel posterior. La conexión de una fuente de alimentación redundante (RPS) es opcional, pero recomendable. El conector RPS está en el panel posterior de los dispositivos.

Instalación en un rack

⚠ **PRECAUCIÓN: en la Guía de información del producto puede consultar información de seguridad relativa a los dispositivos conectados al conmutador o compatibles con éste.**

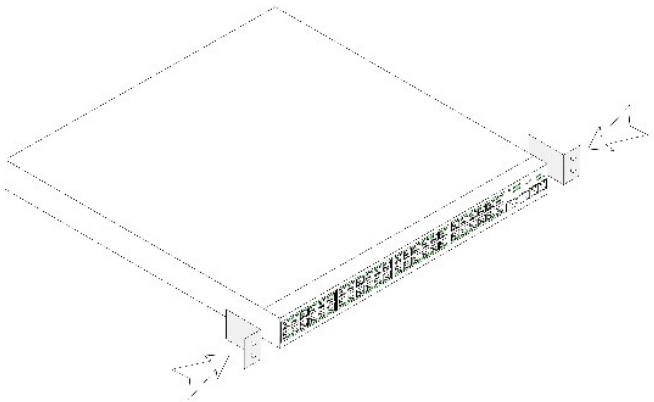
⚠ **PRECAUCIÓN: desconecte todos los cables de la unidad antes de montar el dispositivo en un rack o armario.**

⚠ **PRECAUCIÓN: cuando monte varios dispositivos en un rack, empiece desde abajo.**

1. Coloque el soporte de montaje en rack suministrado en un lateral del dispositivo y asegúrese de que los orificios de montaje del dispositivo coinciden con los orificios de montaje del soporte de montaje en rack.

   En la figura siguiente se muestra dónde deben montarse los soportes.

Figura 3-1. Instalación de los soportes para el montaje en rack



2. Inserte los tornillos suministrados en los orificios de montaje en rack y apriételos con un destornillador.
3. Repita el proceso para el soporte de montaje en rack en el otro lado del dispositivo.
4. Inserte la unidad en el rack de 48,26 cm y asegúrese de que los orificios de montaje en rack del dispositivo coinciden con los orificios de montaje del rack.
5. Fije la unidad al rack con los tornillos de rack (no incluidos). Apriete primero el par inferior de tornillos y después el superior. Asegúrese de que los orificios de ventilación no estén obstruidos.

Instalación en una superficie plana

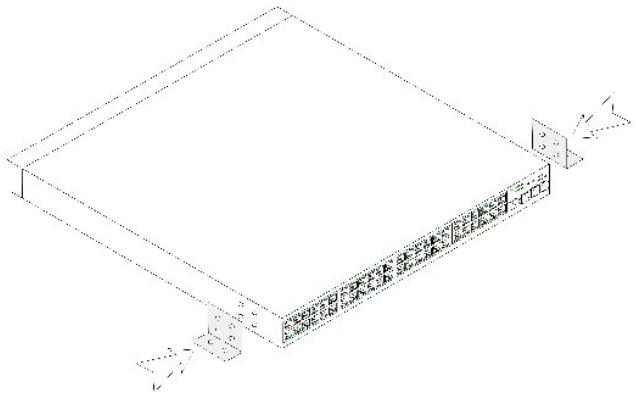
Si no se instala en un rack, el dispositivo debe instalarse en una superficie plana. La superficie debe soportar el peso del dispositivo y de los cables.

1. Fije las almohadillas de goma autoadhesivas en cada zona marcada de la parte inferior del chasis.
2. Coloque el dispositivo en una superficie plana y deje unos 5 cm de separación a cada lado y unos 13 cm en la parte posterior.
3. Asegúrese de que el dispositivo dispone de la ventilación correcta.

Instalación del dispositivo en una pared

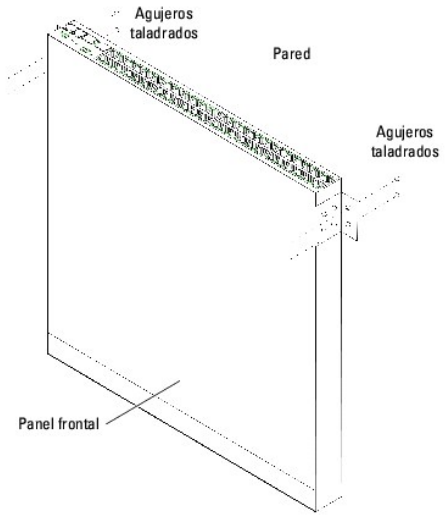
1. Coloque el soporte de montaje en pared suministrado en un lateral del dispositivo y asegúrese de que los orificios de montaje del dispositivo coinciden con los orificios de montaje del soporte de montaje en rack. En la figura siguiente se muestra dónde deben montarse los soportes.

Figura 3-2. Instalación de los soportes para el montaje en pared



2. Inserte los tornillos suministrados en los orificios de montaje en rack y apriételos con un destornillador.
3. Repita el proceso para el soporte de montaje en pared en el otro lado del dispositivo.
4. Coloque el dispositivo en la pared de la sala en la que está realizando la instalación.
5. Marque en la pared los puntos en los que deberán ir los tornillos que sujetan el dispositivo.
6. Taladre los agujeros y coloque los tacos (no incluidos) en la zona marcada.
7. Fije la unidad a la pared con los tornillos (no incluidos). Asegúrese de que los orificios de ventilación no estén obstruidos.

Figura 3-3. Montaje de un dispositivo en la pared



Conexión a un terminal

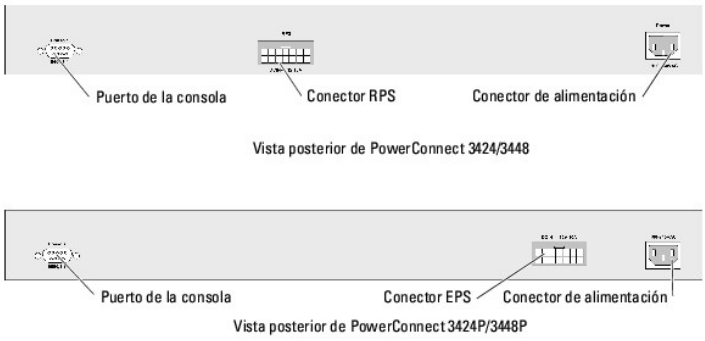
1. Conecte un cable cruzado RS-232 al terminal ASCII o al conector serie de un sistema de escritorio que ejecute software de emulación de terminal.
2. Conecte el conector hembra DB-9 del otro extremo del cable al conector para puerto serie del dispositivo.

Conexión de un dispositivo a una fuente de alimentación

Conecte el cable de alimentación de CA suministrado al conector de alimentación de CA del panel posterior.

NOTA: no conecte el cable de alimentación a una toma eléctrica de CA con conexión a tierra en este momento. Conecte el dispositivo a una fuente de energía durante los pasos que se describen en "Inicio y configuración del dispositivo".

Figura 3-4. Conector de alimentación del panel posterior



Después de conectar el dispositivo a una fuente de energía, compruebe que éste está conectado y funciona correctamente examinando los LED del panel frontal.

Instalación de una pila

Información general

Cada dispositivo puede funcionar como un dispositivo independiente o puede ser miembro de una pila. Cada pila admite un máximo de seis dispositivos o 192 puertos.

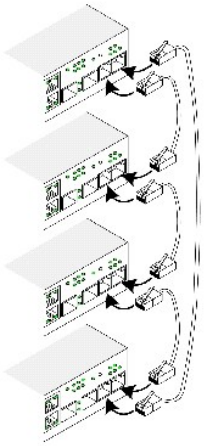
Todas las pilas deben tener una unidad maestra, y pueden tener una unidad de copia de seguridad maestra; los demás dispositivos conectados a la pila se consideran miembros.

Apilamiento de conmutadores de la serie PowerConnect 3400

Cada pila de la serie PowerConnect 3400 contiene una única unidad maestra y puede tener una unidad de copia de seguridad maestra, mientras que el resto de las unidades se consideran miembros del apilamiento.

Los conmutadores de la serie PowerConnect 3400 utilizan los puertos RJ-45 Ethernet Gigabit (G3 y G4) para el apilamiento. Esto proporciona a los dispositivos posibilidades adicionales de apilamiento sin añadirles accesorios adicionales. Para apilar los dispositivos, conecte un cable de categoría 5 estándar al puerto G3 del dispositivo situado en la parte superior de la pila y al puerto G4 del dispositivo situado inmediatamente debajo. Repita este proceso hasta que todos los dispositivos estén conectados. Conecte el puerto G3 del dispositivo situado en la parte inferior de la pila al puerto G4 del dispositivo situado en la parte superior de la pila.

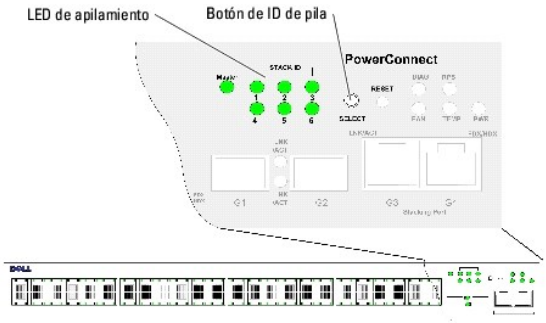
Figura 3-5. Diagrama de cables de apilamiento



NOTA: en el modo de apilamiento, los puertos designados como G3 y G4 no se muestran en el servidor Web integrado (EWS): es como si no estuvieran en el dispositivo. Esto se debe a que los puertos reciben un índice distinto para el apilamiento.

La identificación de la unidad de pila se lleva a cabo en el panel frontal del dispositivo utilizando el botón de ID de pila.

Figura 3-6. Configuración de apilamiento y panel de identificación



Cada dispositivo de la pila tiene una ID de unidad exclusiva que define la posición de la unidad y su función en la pila. Si el dispositivo es una unidad independiente, el LED de pila no está encendido. La configuración predeterminada es como unidad independiente.

La ID de unidad se configura manualmente mediante el botón de ID de pila. La ID de unidad viene indicada por los LED de ID de pila. Las ID de unidad 1 y 2 se reservan para la unidad maestra y la unidad de copia de seguridad maestra, y las ID de unidad de 3 a 6 son para las unidades miembro.

Proceso de selección de ID de unidad

El proceso de selección de la ID de unidad es el siguiente:

1. Asegúrese de que el puerto de consola del dispositivo independiente/maestro está conectado a un dispositivo terminal VT100 o a un emulador de terminal VT100 a través del cable cruzado RS-232.
2. Localice un enchufe de CA.
3. Desactive el enchufe de CA.
4. Conecte el dispositivo al enchufe de CA.
5. Active el enchufe de CA.

Cuando se enciende el dispositivo, el número de LED configurado (que corresponde a la ID de unidad guardada previamente) empieza a parpadear. El LED parapadea durante 15 segundos. Durante este periodo, puede seleccionar una ID de pila específica presionando el botón de ID de pila hasta que se encienda el LED de ID de pila apropiado.

6. Proceso de selección: para avanzar en el número de LED de ID de apilamiento, continúe presionando el botón de ID de pila. Cuando el LED 6 parpadea, al presionar el botón de ID de pila el dispositivo se configura como independiente. Si se vuelve a presionar el botón de ID de pila, se avanza la ID de pila a 1. Las unidades 1 y 2 son susceptibles de ser unidades maestras. Puede consultar el proceso de elección de dispositivos maestros en "Información general sobre el apilamiento".

7. **Fin del proceso de selección**: el proceso de selección de ID de unidad finaliza una vez transcurrido el periodo de parpadeo de 15 segundos. El botón de ID de pila no responde, y la ID de unidad se establece en la ID del LED que parpadea al final del periodo.

NOTA: realice estos pasos para cada unidad por separado hasta que todos los miembros de la pila estén encendidos y se hayan seleccionado sus ID de pila. Si se realizan los pasos anteriores para cada unidad por separado, habrá suficiente tiempo para seleccionar la ID de pila para cada unidad. Sin embargo, la pila completa debe cablearse según las indicaciones de la figura "Diagrama de cables de apilamiento" antes de encender los dispositivos.

Inicio y configuración del dispositivo

Una vez realizadas todas las conexiones externas, conecte un terminal al dispositivo para configurar el dispositivo. En la sección "Configuración avanzada" se describe cómo ejecutar las funciones avanzadas adicionales.

NOTA: antes de continuar, lea las notas de la versión de este producto. Descargue las notas de la versión desde la página Web de asistencia de Dell (**support.dell.com**).

NOTA: se recomienda descargar la revisión más reciente de la documentación del usuario que encontrará en la página Web de asistencia de Dell (**support.dell.com**).

Conexión al dispositivo

Para configurar el dispositivo, éste debe estar conectado a una consola. Sin embargo, si el dispositivo forma parte de una pila, sólo será necesario conectar al terminal un único dispositivo, denominado unidad maestra. Puesto que la pila funciona como un solo dispositivo, únicamente se configura la unidad maestra.

Conexión del terminal al dispositivo

El dispositivo dispone de un puerto de consola que permite la conexión con un sistema de escritorio que ejecute software de emulación de terminal para supervisar y configurar el dispositivo. Este conector de puerto de consola es un conector DB-9 macho instalado como un conector de equipo terminal de datos (DTE).

Para utilizar el puerto de consola, se requiere lo siguiente:

- Un terminal compatible con VT100 o un sistema de escritorio o portátil con un puerto serie y que ejecute el software de emulación de terminal VT100
- Un cable cruzado RS-232 con un conector DB-9 hembra para el puerto de consola y el conector apropiado para el terminal

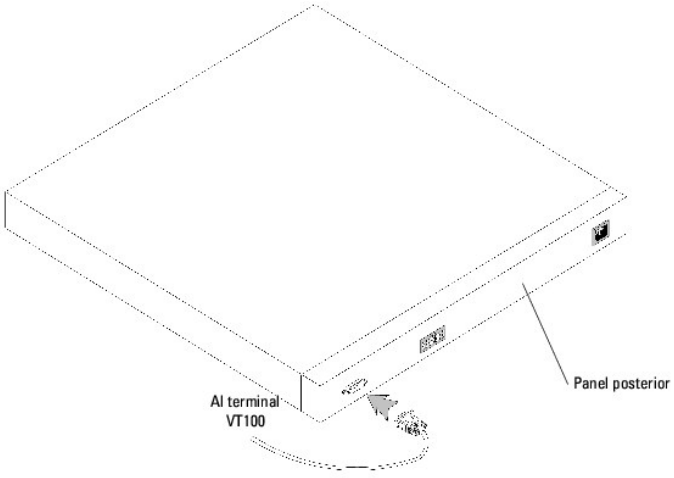
Para conectar un terminal al puerto de la consola del dispositivo:

1. Conecte el cable cruzado RS-232 suministrado al terminal que está ejecutando el software de emulación de terminal VT100.
2. Seleccione el puerto serie apropiado (puerto serie 1 o puerto serie 2) para conectar a la consola.
3. Establezca la velocidad de datos en 9 600 baudios.
4. Establezca el formato de datos en 8 bits de datos, 1 bit de parada y sin paridad.
5. Establezca el control de flujo en ninguno.
6. En Propiedades, seleccione el modo de emulación VT100.
7. Seleccione Teclas de terminal para las teclas de función, flecha y Ctrl. Asegúrese de que establece Teclas de terminal (*no* Teclas de Windows).

AVISO: cuando utilice HyperTerminal con Microsoft® Windows® 2000, asegúrese de que tiene instalado Windows 2000 Service Pack 2 o posterior. Con Windows 2000 Service Pack 2, las teclas de flecha funcionan correctamente en la emulación VT100 de HyperTerminal. Vaya a www.microsoft.com para obtener información sobre los Service Pack de Windows 2000.

8. Conecte el conector hembra del cable cruzado RS-232 directamente al puerto de consola del dispositivo independiente o la unidad maestra y apriete los tornillos cautivos de retención. El puerto de consola de la serie PowerConnect 3400 se encuentra en el panel posterior.

Figura 3-7. Conexión al puerto de consola de la serie PowerConnect 3400



NOTA: es posible conectar una consola al puerto de consola de cualquier unidad de la pila, pero la administración de la pila sólo la lleva a cabo la unidad maestra de la pila (ID de unidad 1 o 2).

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de PowerConnect 3424/P y 3448/P

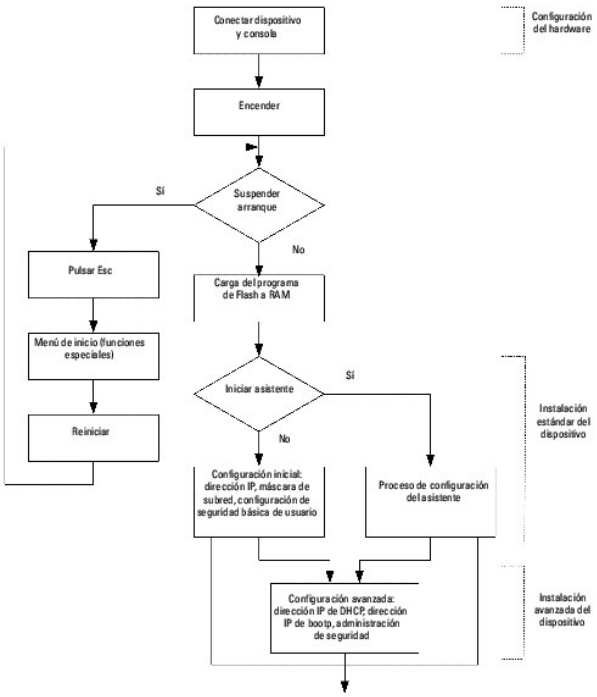
Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

Procedimientos de configuración

Una vez realizadas todas las conexiones externas del dispositivo, debe conectarse un terminal al dispositivo para supervisar el inicio y otros procedimientos. El orden de los procedimientos de instalación y configuración se muestra en la figura siguiente:

NOTA: antes de continuar, lea las notas de la versión de este producto. Descargue las notas de la versión desde **support.dell.com**.

Figura 4-1. Flujo de la instalación y la configuración



Inicio del conmutador

Cuando la alimentación se enciende con el terminal local ya conectado, el conmutador realiza la autoprueba de encendido (POST). La POST se ejecuta cada vez que se inicializa el dispositivo, y comprueba los componentes de hardware para determinar si el dispositivo es totalmente funcional antes del arranque completo. Si se detecta un problema crítico, el flujo de programa se detiene. Si la POST se ejecuta correctamente, se carga una imagen ejecutable válida en la RAM. Se muestran mensajes de la POST en el terminal que indican si la prueba ha finalizado correctamente o no.

El proceso de inicio dura aproximadamente 30 segundos.

Configuración inicial

NOTA: antes de continuar, lea las notas de la versión de este producto. Descargue las notas de la versión desde la página Web de asistencia de Dell (**support.dell.com**).

NOTA: en la configuración inicial se dan por sentado los supuestos siguientes:

- El dispositivo PowerConnect no se había configurado antes y está en el mismo estado que cuando lo recibió.
- El dispositivo PowerConnect se ha iniciado correctamente.
- La conexión de la consola está establecida, y se muestra el indicador de comandos de la consola en la pantalla de un dispositivo terminal VT100.

La configuración inicial del dispositivo se lleva a cabo a través del puerto de consola. Después de la configuración inicial, puede administrarse el dispositivo bien desde el puerto de consola ya conectado o bien remotamente a través de una interfaz definida durante la configuración inicial.

Si se trata de la primera vez que se inicia el dispositivo, o si el archivo de configuración está vacío porque el dispositivo no se ha configurado, se solicita al usuario que utilice el asistente para la instalación. El asistente para la instalación le guía a través de la configuración inicial del dispositivo y pone el dispositivo en funcionamiento lo más rápido posible.

NOTA: obtenga la información siguiente del administrador de red antes de configurar el dispositivo:

- Dirección IP que debe asignarse a la interfaz VLAN 1 a través de la que se administrará el dispositivo (de forma predeterminada, todos los puertos son miembros de la VLAN 1)
- Máscara de subred IP para la red
- Dirección IP de la puerta de enlace predeterminada (enrutador del siguiente salto) para configurar la ruta predeterminada
- Cadena de comunidad SNMP y dirección IP del sistema de administración SNMP (opcional)
- Nombre de usuario y contraseña

El asistente para la instalación le guía a través de la configuración inicial del conmutador y pone el dispositivo en funcionamiento lo más rápido posible. Puede optar por no utilizar el asistente para la instalación y configurar el conmutador manualmente mediante el modo de CLI del dispositivo.

El asistente para la instalación configura los campos siguientes.

- Cadena de comunidad SNMP y dirección IP del sistema de administración SNMP (opcional)
- Nombre de usuario y contraseña
- Dirección IP del dispositivo
- Dirección IP de la puerta de enlace predeterminada

Se muestra el texto siguiente:

```
Welcome to Dell Easy Setup Wizard


The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip
the setup wizard, and enter CLI mode to manually configure the switch.
The system will prompt you with a default answer; by pressing enter, you accept the default.
You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation
using the default system configuration.


Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Y/N)[Y]Y
You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

Si pulsa [N], saldrá del asistente para la instalación. Si no responde en 60 segundos, el asistente para la instalación se cerrará automáticamente y aparecerá el indicador de la consola de la CLI.

Si pulsa [Y], el asistente para la instalación le proporcionará instrucciones interactivas para la configuración inicial del dispositivo.

NOTA: si no responde en 60 segundos y hay un servidor BootP en la red, se obtendrá una dirección de dicho servidor.

NOTA: puede salir del asistente para la instalación en cualquier momento pulsando [Ctrl+z].

Paso 1 del asistente

Se muestra el texto siguiente:

```
The system is not setup for SNMP management by default.
To manage the switch using SNMP (required for Dell Network Manager) you can

   l  Setup the initial SNMP version 2 account now.

   l  Return later and setup additional SNMP v1/v3 accounts.


For more information on setting up SNMP accounts, please see the user documentation.


Would you like to setup the SNMP management interface now? (Y/N)[Y]Y
```

Pulse [N] para ir al paso 2.

Pulse [Y] para continuar con el asistente para la instalación. Se muestra el texto siguiente:

```
To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the
particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to
this account.
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems. For more information on adding
management systems, see the user documentation.
To add a management station:
Please enter the SNMP community string to be used: [Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station: [0.0.0.0].
```

Introduzca lo siguiente:

- Cadena de comunidad de SNMP, por ejemplo, Dell_Network_Manager
- Dirección IP del sistema de administración (A.B.C.D) o un comodín (0.0.0.0) para que la administración se efectúe desde una estación de administración

NOTA: no pueden utilizarse direcciones IP ni máscaras que empiecen por cero.

Pulse **Intro**.

Paso 2 del asistente

Se muestra el texto siguiente:

```
Now we need to setup your initial privilege (Level 15) user account.
This account is used to login to the CLI and Web interface.
You may setup other accounts and change privilege levels later.
For more information on setting up user accounts and changing privilege levels, see the user documentation.
To setup a user account:
Enter the user name<1-20>:[admin]
Please enter the user password:*
Please reenter the user password:*
```

Introduzca lo siguiente:

- Nombre de usuario, por ejemplo, "admin"
- Contraseña y confirmación de la contraseña

NOTA: si la primera y la segunda entrada de contraseña no coinciden, se solicitará al usuario que vuelva a especificarlas hasta que coincidan.

Pulse **Intro**.

Paso 3 del asistente

Se muestra el texto siguiente:

```
Next, an IP address is setup.

The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the
CLI, Web interface, or SNMP interface for the switch.To setup an IP address:

Please enter the IP address of the device (A.B.C.D):[1.1.1.1]

Please enter the IP subnet mask (A.B.C.D or nn): [255.255.255.0]
```

Introduzca la dirección IP y la máscara de subred IP, por ejemplo, 1.1.1.1 como dirección IP y 255.255.255.0 como máscara de subred IP.

Pulse **Intro**.

Paso 4 del asistente

Se muestra el texto siguiente:

```
Finally, setup the default gateway.
Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0]
```

Introduzca la puerta de enlace predeterminada.

Pulse Intro. Aparece el texto siguiente (en caso de utilizar los parámetros mencionados):

```
This is the configuration information that has been collected:

============================================================

SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2

============================================================
```

Paso 5 del asistente

Se muestra el texto siguiente:

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the
information is incorrect, select (N) to discard configuration and restart the wizard: (Y/N)[Y]Y
```

Pulse [N] para volver a iniciar el asistente para la instalación.

Pulse [Y] para finalizar el asistente para la instalación. Se muestra el texto siguiente:

```
Configuring SNMP management interface
Configuring user account......
Configuring IP and subnet......

Thank you for using Dell Easy Setup Wizard. You will now enter CLI mode.
```

Paso 6 del asistente

Aparece el indicador de la CLI.

Configuración avanzada

Esta sección contiene información sobre la asignación dinámica de direcciones IP y la gestión de la seguridad basada en el mecanismo de autenticación, autorización y administración de cuentas (AAA), y consta de los temas siguientes:

- Configuración de direcciones IP a través de DHCP
- Configuración de direcciones IP a través de BOOTP
- Gestión de la seguridad y configuración de contraseñas

Al configurar/recibir direcciones IP a través de DHCP y BOOTP, la configuración recibida de estos servidores incluye la dirección IP y puede incluir la máscara de subred y la puerta de enlace predeterminada.

Recuperación de una dirección IP de un servidor DHCP

Cuando se utiliza el protocolo DHCP para recuperar una dirección IP, el dispositivo actúa como cliente DHCP. Cuando se restablece el dispositivo, el comando de DHCP se guarda en el archivo de configuración, pero la dirección IP no. Para recuperar una dirección IP de un servidor DHCP, realice los pasos siguientes:

1. Seleccione un puerto y conéctelo a un servidor DHCP o a una subred que contenga un servidor DHCP para recuperar la dirección IP.
2. Introduzca los comandos siguientes para utilizar el puerto seleccionado para recibir la dirección IP. En el ejemplo siguiente, los comandos se basan en el tipo de puerto utilizado para la configuración.
    - Asignación de direcciones IP dinámicas:

```
console# configure

console(config)# interface ethernet 1/e1
```

```
console(config-if)# ip address dhcp hostname powerconnect

console(config-if)# exit

console(config)#
```

- Asignación de direcciones IP dinámicas (en una VLAN):

```
console# configure

console(config)# interface ethernet vlan 1

console(config-if)# ip address dhcp hostname device

console(config-if)# exit

console(config)#
```

La interfaz recibe la dirección IP automáticamente.

3. Para verificar la dirección IP, introduzca el comando **show ip interface** en la línea de comandos tal como se muestra en el ejemplo siguiente.

```
console# show ip interface

IP Address I/F Type



------------- ------ -------

100.1.1.1/24 vlan 1 dynamic
```

NOTA: no es necesario eliminar la configuración del dispositivo para recuperar una dirección IP para el servidor DHCP.

NOTA: al copiar archivos de configuración, evite utilizar un archivo de configuración que contenga una instrucción para activar DHCP en una interfaz que se conecte al mismo servidor DHCP (o a otro cuya configuración sea idéntica). En este caso, el dispositivo recupera el nuevo archivo de configuración y se inicia desde dicho archivo. A continuación, el dispositivo activa DHCP según lo especificado en el nuevo archivo de configuración, y DHCP indica al dispositivo que vuelva a cargar el mismo archivo.

NOTA: si se configura una dirección IP DHCP, dicha dirección se recupera de forma dinámica y el comando `ip address dhcp` se guarda en el archivo de configuración. En caso de error de la unidad maestra, la unidad de reserva intentará recuperar nuevamente una dirección DHCP. Esto puede conducir a una de las situaciones siguientes:

- Puede que se asigne la misma dirección IP.
- Puede que se asigne una dirección IP distinta, lo cual puede provocar la pérdida de la conexión con la estación de administración.
- Puede que el servidor DHCP se desconecte, lo cual provocaría un error durante la recuperación de la dirección IP, así como una posible pérdida de la conexión con la estación de administración.

Recepción de una dirección IP de un servidor BOOTP

Puede utilizarse el protocolo BOOTP estándar, que permite que el dispositivo descargue automáticamente su configuración de host IP de cualquier servidor

BOOTP estándar de la red. En este caso, el dispositivo actúa como cliente BOOTP.

Para recuperar una dirección IP de un servidor BOOTP:

1. Seleccione un puerto y conéctelo a un servidor BOOTP o a una subred que contenga dicho servidor.
2. En la línea de comandos del sistema, introduzca el comando **delete startup configuration** para eliminar la configuración de inicio de la memoria Flash.

El dispositivo se reinicia sin configuración y en 60 segundos comienza a enviar peticiones BOOTP. El dispositivo recibe la dirección IP automáticamente.

NOTA: cuando empiece el proceso de reinicio del dispositivo, las entradas que se realicen desde el terminal ASCII o desde el teclado cancelarán automáticamente el proceso de BOOTP antes de que se complete, y el dispositivo no recibirá ninguna dirección IP procedente del servidor BOOTP.

En el ejemplo siguiente se muestra este proceso:

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

You haven't saved your changes. Are you sure you want to continue (y/n) [n]?

This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?

*****************************************************

/* the device reboots */
```

Para verificar la dirección IP, introduzca el comando **show ip interface**.

Ahora el dispositivo está configurado con una dirección IP.

Gestión de la seguridad y configuración de contraseñas

La seguridad del sistema se gestiona mediante el mecanismo de autenticación, autorización y administración de cuentas (AAA), que administra los derechos de acceso, los privilegios y los métodos de administración de los usuarios. AAA utiliza bases de datos de usuarios locales y remotas. El cifrado de datos se gestiona mediante el mecanismo SSH.

El sistema se entrega sin una contraseña predeterminada configurada: todas las contraseñas las definen los usuarios. Si se pierde una contraseña definida por el usuario, puede ejecutarse un procedimiento de recuperación de contraseña desde el menú **Startup** (Inicio). El procedimiento es aplicable sólo al terminal local y permite el acceso una sola vez al dispositivo desde el terminal local sin introducir una contraseña.

Configuración de contraseñas de seguridad

Las contraseñas de seguridad se pueden configurar para los servicios siguientes:

- Terminal
- Telnet
- SSH
- HTTP
- HTTPS

NOTA: las contraseñas las define el usuario.

NOTA: al crear un nombre de usuario, la prioridad predeterminada es 1, que otorga el acceso pero no derechos de configuración. Se debe establecer una prioridad de 15 para permitir el acceso al dispositivo y otrogar derechos de configuración. Aunque es posible asignar el nivel de privilegio 15 a nombres de usuario sin necesidad de especificar una contraseña, se recomienda asignarla siempre. Si no se ha especificado ninguna contraseña, los usuarios con privilegios pueden acceder a la interfaz Web con cualquier contraseña.

NOTA: es posible proteger las contraseñas mediante comandos de administración de contraseñas para forzar la limitación temporal de las contraseñas o su caducidad. Para obtener más información, consulte "Gestión de la seguridad y configuración de contraseñas".

Configuración de una contraseña inicial de terminal

Para configurar una contraseña inicial de terminal, escriba los comandos siguientes:

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line console

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password david
```

- Al iniciar sesión por primera vez en un dispositivo a través de una sesión de terminal, introduzca `david` en la petición de contraseña.
- Cuando cambie el modo de un dispositivo a activado, introduzca `david` en la petición de contraseña.

Configuración de una contraseña inicial de Telnet

Para configurar una contraseña inicial de Telnet, escriba los comandos siguientes:

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line telnet

console(config-line)# login authentication default

console(config-line)# enable authentication default
```

```
console(config-line)# password laura
```

- Al iniciar sesión por primera vez en un dispositivo a través de una sesión Telnet, introduzca laura en la petición de contraseña.
- Cuando cambie el modo de un dispositivo a activado, introduzca laura.

Configuración de una contraseña inicial de SSH

Para configurar una contraseña inicial de SSH, escriba los comandos siguientes:

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password jones.
```

- Al iniciar sesión por primera vez en un dispositivo a través de una sesión SSH, introduzca jones en la petición de contraseña.
- Cuando cambie el modo de un dispositivo a activado, introduzca jones.

Configuración de una contraseña inicial de HTTP

Para configurar una contraseña inicial de HTTP, escriba los comandos siguientes:

```
console(config)# ip http authentication local

console(config)# username admin password user1 level 15
```

Configuración de una contraseña inicial de HTTPS:

Para configurar una contraseña inicial de HTTPS, escriba los comandos siguientes:

```
console(config)# ip https authentication local

console(config)# username admin password user1 level 15
```

Escriba una vez los comandos siguientes durante la configuración del uso de una sesión de terminal, Telnet o SSH para poder utilizar una sesión HTTPS.

NOTA: en el explorador Web, active SSL 2.0 o superior para que pueda verse el contenido de la página.

```
console(config)# crypto certificate generate key_generate
```

```
console(config)# ip https server
```

Al activar por primera vez una sesión HTTP o HTTPS, introduzca `admin` como nombre de usuario y `user1` como contraseña.

NOTA: los servicios HTTP y HTTPS requieren el nivel de acceso 15 y se conectan directamente con el nivel de acceso a la configuración.

Procedimientos de inicio

Procedimientos del menú de inicio

Los procedimientos que activa el menú Startup (Inicio) son la descarga de software, el uso de la Flash y la recuperación de contraseñas. Los procedimientos de diagnóstico están reservados exclusivamente para el personal de asistencia técnica y no se describen en este documento.

Puede entrar en el menú Startup (Inicio) durante el inicio del dispositivo. El usuario debe intervenir inmediatamente después de la prueba POST.

Para entrar en el menú Startup (Inicio):

1. Encienda el dispositivo y preste atención al mensaje de inicio automático.

```
**************************************************

***************** SYSTEM RESET *****************

**************************************************

Boot1 Checksum Test.....PASS

Boot2 Checksum Test.....PASS

Flash Image Validation Test.....PASS

BOOT Software Version 1.0.0.05 Built 06-Jan-2005 14:46:49

Carrier board, based on PPC8247

128 MByte SDRAM. I-Cache 16 KB. D-Cache 16 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

2. Cuando aparezca el mensaje de inicio automático, pulse <Intro> para entrar en el menú Startup (Inicio). Los procedimientos del menú Startup (Inicio) pueden realizarse mediante el terminal ASCII o HyperTerminal de Windows.

```
[1] Download Software
```

```
[2] Erase Flash File


[3] Password Recovery Procedure


[4] Enter Diagnostic Mode


[5] Set Terminal Baud-Rate


[6] Back
```

En las secciones siguientes se describen las opciones disponibles del menú Startup (Inicio).

NOTA: al seleccionar una opción del menú Startup (Inicio), tenga en cuenta el tiempo: si no realiza ninguna selección en 35 segundos (valor predeterminado), se agotará el tiempo de espera del dispositivo. El valor predeterminado puede modificarse a través de la CLI.

NOTA: únicamente el personal de asistencia técnica puede trabajar en el modo de diagnóstico (opción **[4]**). Por este motivo, la opción Enter Diagnostics Mode (Entrar en el modo de diagnóstico) no se explica en esta guía.

Descargar software (opción [1])

El procedimiento de descarga de software se realiza cuando es necesario descargar una nueva versión para sustituir archivos dañados o para actualizar el software del sistema. Para descargar software desde el menú Startup (Inicio):

1. En el menú Startup (Inicio), pulse [1]. Aparece el mensaje siguiente:

```
Downloading code using XMODEM


****************************************************************


*** Running SW Ver. 1.0.0.30 Date 09-Jan-2005 Time 14:30:02


****************************************************************


HW version is


Base Mac address is  : 00:00:b0:45:54:00


Dram size is : 128M bytes


Dram first block size is : 36864K bytes


Dram first PTR is : 0x1C00000


Flash size is: 16M


Loading running configuration.
```

```
Number of configuration items loaded: 5


Loading startup configuration.


Number of configuration items loaded: 5


Device configuration:


Slot 1 - PowerConnect 3424 HW Rev. 0.0


------------------------------


-- Unit Number 1 Standalone --


------------------------------


BOXP_high_appl_init: dpssIpcInitStandAlone


Tapi Version: v1.3.1.6P_01_03


Core Version: v1.3.1.6P_01_02


01-Jan-2000 01:01:19 %INIT-I-InitCompleted: Initialization task is completed


01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 1 status changed - operational.


01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration change trap.


01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.


01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG: PS# 1 status changed - operational.
```

2. Cuando utilice HyperTerminal, haga clic en Transferir en la barra de menús de HyperTerminal.
3. En el campo Nombre de archivo, especifique la ruta del archivo que se va a descargar.
4. Asegúrese de que el protocolo Xmodem esté seleccionado en el campo Protocolo.
5. Haga clic en Enviar. El software se descarga.

NOTA: tras la descarga del software, el dispositivo se reinicia automáticamente.

Borrar archivo Flash (opción [2])

En algunos casos, es necesario borrar la configuración del dispositivo. Si se borra la configuración, es preciso volver a configurar todos los parámetros configurados a través de la CLI, EWS o SNMP.

Para borrar la configuración del dispositivo:

1. En el menú Startup (Inicio), pulse [2] antes de que transcurran dos segundos para borrar el archivo Flash. Se muestra el mensaje siguiente:

```
Warning! About to erase a Flash file.


Are you sure (Y/N)? y
```

2. Pulse Y. Se muestra el mensaje siguiente:

```
Write Flash file name (Up to 8 characters, Enter for none.):config


File config (if present) will be erased after system initialization


======== Press Enter To Continue ========
```

3. Escriba config como nombre del archivo Flash. Se borra la configuración y se reinicia el dispositivo.
4. Repita la configuración inicial del dispositivo.

Recuperación de contraseña (opción [3])

Si se pierde una contraseña, puede ejecutarse un procedimiento de recuperación de contraseña desde el menú Startup (Inicio). Este procedimiento permite entrar en el dispositivo sin contraseña una sola vez.

Para recuperar una contraseña perdida únicamente al entrar en el terminal local:

1. En el menú Startup (Inicio), escriba [3] y pulse <Intro>. La contraseña se borrará.

   Introduzca su elección o pulse Esc para salir:

```
Current password will be ignored!
```

NOTA: para garantizar la seguridad del dispositivo, vuelva a configurar las contraseñas para los métodos de administración que sean aplicables.

Entrar en el modo de diagnóstico (opción [4])

Sólo para el personal de asistencia técnica.

Establecer velocidad en baudios del terminal (opción [5])

Para establecer la velocidad en baudios del terminal, escriba [5] y pulse <Intro>.

Introduzca su elección o pulse Esc para salir:

```
Set new device baud-rate: 38,400
```

Descarga de software a través del servidor TFTP

Esta sección contiene instrucciones para descargar software del dispositivo (imágenes del sistema y de inicio) a través de un servidor TFTP. Antes de descargar el software, debe haberse configurado el servidor TFTP.

Descarga de la imagen del sistema

El dispositivo se inicia y se ejecuta al descomprimir la imagen del sistema desde el área de la memoria Flash en la que se almacena una copia de la imagen del sistema. Cuando se descarga una nueva imagen, se guarda en la otra área asignada para la copia de la imagen del sistema.

En el próximo inicio, el dispositivo se descomprimirá y se ejecutará desde la imagen del sistema activa actualmente, a menos que se especifique lo contrario.

Para descargar una imagen del sistema a través del servidor TFTP:

1. Compruebe que se haya configurado una dirección IP en uno de los puertos del dispositivo y que puedan enviarse comandos ping a un servidor TFTP.
2. Asegúrese de que el archivo que se descarga se guarde en el servidor TFTP (archivo arc).
3. Introduzca el comando **show version** para comprobar qué versión del software se está ejecutando actualmente en el dispositivo. A continuación se muestra un ejemplo de la información que aparece:

```
console# show version

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4. Introduzca el comando **show bootvar** para verificar cuál es la imagen del sistema activa actualmente. A continuación se muestra un ejemplo de la información que aparece:

```
console# show bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. Introduzca el comando **copy tftp:**//{dirección tftp}/{nombre de archivo} **image** para copiar una nueva imagen del sistema en el dispositivo. Cuando se descarga la nueva imagen, se guarda en el área asignada para la otra copia de la imagen del sistema (image-2, como se muestra en el ejemplo). A continuación se muestra un ejemplo de la información que aparece:

```
console# copy tftp://176.215.31.3/file1.ros image

Accessing file `file1' on 176.215.31.3Ö

Loading file1 from 176.215.31.3:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Copy took 00:01:11 [hh:mm:ss]
```

Los signos de exclamación indican que el proceso de copia se encuentra en curso. Cada signo (!) corresponde a 512 bytes transferidos correctamente. Un punto indica que el proceso de copia ha superado el tiempo de espera. Una fila con varios puntos indica que el proceso de copia ha fallado.

6. Seleccione la imagen para el próximo inicio introduciendo el comando boot system. Después de este comando, introduzca el comando **show bootvar** para verificar que la copia indicada como parámetro en el comando **boot system** se haya seleccionado para el próximo inicio.

A continuación se muestra un ejemplo de la información que aparece:

```
console# boot system image-2
```

```
console# show bootvar
```

```
Images currently available on the Flash
```

```
Image-1 active
```

```
Image-2 not active (selected for next boot)
```

Si la imagen para el próximo inicio no se selecciona mediante el comando boot system, el sistema se iniciará con la imagen activa actualmente.

7. Introduzca el comando **reload**. Se muestra el mensaje siguiente:

```
console# reload
```

```
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

8. Introduzca y. El dispositivo se reinicia.

Descarga de la imagen de inicio

La carga de una nueva imagen de inicio del servidor TFTP y su programación en la memoria Flash actualizan la imagen de inicio. La imagen de inicio se carga cuando se enciende el dispositivo. El usuario no tiene control sobre las copias de imagen de inicio. Para descargar una imagen de inicio a través del servidor TFTP:

1. Compruebe que se haya configurado una dirección IP en uno de los puertos del dispositivo y que puedan enviarse comandos ping a un servidor TFTP.
2. Asegúrese de que el archivo que debe descargarse se guarde en el servidor TFTP (archivo rfb).
3. Introduzca el comando **show version** para comprobar qué versión del software se está ejecutando actualmente en el dispositivo. A continuación se muestra un ejemplo de la información que aparece:

```
console# show version
```

```
SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)
```

```
Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)
```

```
HW version
```

4. Introduzca el comando **copy tftp:**//{dirección tftp}/{nombre de archivo} **boot** para copiar la imagen de inicio en el dispositivo. A continuación se muestra un ejemplo de la información que aparece:

```
console# copy tftp://176.215.31.3/332448-10018.rfb boot


Erasing file..done.


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

5. Introduzca el comando **reload**. Se muestra el mensaje siguiente:

```
console# reload


This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

6. Introduzca y. El dispositivo se reinicia.

Configuración predeterminada de los puertos

La información general para configurar los puertos del dispositivo incluye una breve descripción del mecanismo de negociación automática y la configuración predeterminada para los puertos de conmutación.

Negociación automática

La negociación automática permite la detección automática de la velocidad, el modo dúplex y el control de flujo en todos los puertos 10/100/1000BaseT de conmutación. De forma predeterminada, la negociación automática se activa para cada puerto.

La negociación automática es un mecanismo que se establece entre dos enlaces asociados para permitir que un puerto anuncie sus capacidades de velocidad de transmisión, modo dúplex y control de flujo (el valor predeterminado del control de flujo es "desactivado") a su asociado. De esta manera, ambos puertos funcionan con el común denominador más alto que exista entre ellos.

Si se conecta una NIC que no admite la negociación automática o que no está configurado para ésta, es preciso configurar manualmente el puerto de conmutación del dispositivo y la NIC con la misma velocidad y el modo dúplex.

Si la estación del otro lado del enlace intenta realizar una negociación automática con un puerto 100BaseT de un dispositivo que está configurado para el modo dúplex completo, el resultado de la negociación automática es que la estación intentará operar en el modo semidúplex.

MDI/MDIX

El dispositivo admite la detección automática de cables directos y cruzados en todos los puertos 10/100/1000BaseT de conmutación. Esta función forma parte de la negociación automática y se activa cuando se activa la negociación automática.

Cuando se ha activado MDI/MDIX, la corrección automática de errores de selección de cable es posible, por lo que no es importante distinguir entre un cable directo y un cable cruzado. El cableado estándar para estaciones finales se denomina MDI (interfaz dependiente del medio), y el cableado estándar para concentradores y conmutadores se denomina MDIX (interfaz dependiente del medio con cable cruzado).

Control de flujo

El dispositivo admite el control de flujo 802.3x para los puertos configurados con el modo dúplex completo. De forma predeterminada, esta función está desactivada. Puede activarse para cada puerto. El mecanismo de control de flujo permite que la parte receptora señale a la parte emisora que debe detenerse temporalmente la transmisión a fin de evitar un desbordamiento en el búfer.

Contrapresión

El dispositivo admite la contrapresión para puertos configurados con el modo semidúplex. De forma predeterminada, esta función está desactivada. Puede activarse para cada puerto. El mecanismo de contrapresión impide temporalmente que el emisor transmita más tráfico. El receptor puede ocupar un enlace a fin de dejar de estar disponible para recibir tráfico adicional.

Configuración predeterminada de los puertos de conmutación

En la tabla siguiente se indica la configuración predeterminada de los puertos.

Tabla 4-1. Configuración predeterminada de los puertos

Función	***Valor predeterminado***
Velocidad y modo del puerto	10/100BaseT de cobre: dúplex completo a 100 Mbps con negociación automática
	10/100/1000BaseT de cobre/SFP: dúplex completo a 1 000 Mbps con negociación automática
Estado de reenvío del puerto	Activado
Etiquetas del puerto	Sin etiquetas
Control de flujo	Desactivado (se desactiva en la entrada)
Contrapresión	Desactivada (se desactiva en la entrada)

Regresar a la página de contenido

Regresar a la página de contenido

Uso del administrador de conmutadores OpenManage de Dell

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

En esta sección se ofrece una introducción a la interfaz de usuario del administrador de conmutadores OpenManage de Dell.

Inicio de la aplicación

NOTA: antes de iniciar la aplicación, debe definirse la dirección IP. Para obtener más información, consulte "Configuración inicial".

1. Abra un explorador Web.
2. Introduzca la dirección IP del dispositivo en la barra de direcciones y pulse <Intro>.
3. Cuando se abra la ventana **Log In** (Inicio de sesión), introduzca su nombre de usuario y contraseña.

NOTA: las contraseñas distinguen entre mayúsculas y minúsculas y son alfanuméricas.

4. Haga clic en **Aceptar**.

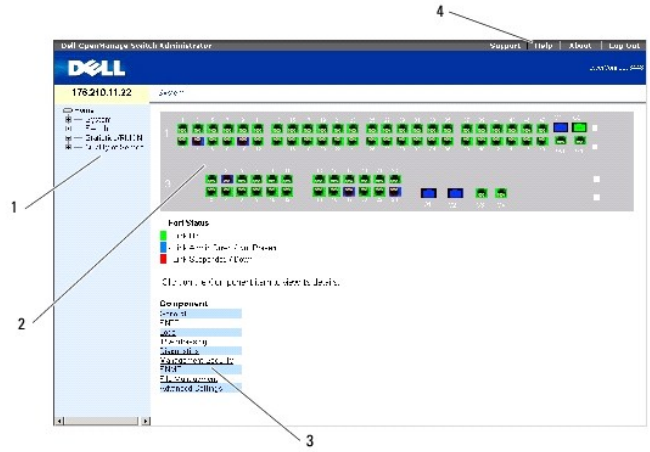
Se abre la página de inicio del **administrador de conmutadores OpenManage™ de Dell**.

Descripción de la interfaz

La página de inicio contiene los campos siguientes:

- Tree view (Vista de árbol): ubicada en la parte izquierda de la página de inicio, la vista de árbol proporciona una vista ampliable de las funciones y los componentes correspondientes.
- Device view (Vista de dispositivo): ubicada en la parte derecha de la página de inicio, esta vista proporciona una vista del dispositivo, un área para información o para una tabla e instrucciones de configuración.

Figura 5-1. Componentes del administrador de conmutadores



En la tabla 5-1 se enumeran los componentes de la interfaz con los números correspondientes.

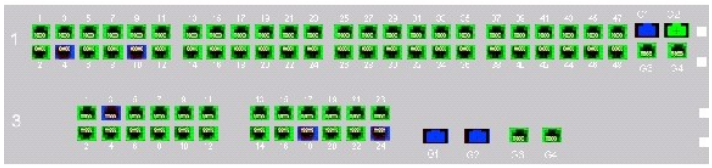
Tabla 5-1. Componentes de la interfaz

Componente	Descripción
1	La vista de árbol incluye una lista de las características del dispositivo. Las bifurcaciones de la vista de árbol se pueden expandir para ver todos los componentes de una característica específica o se pueden contraer para ocultar los componentes de la característica. Si arrastra la barra vertical hacia la derecha, se puede ampliar el área del árbol para visualizar el nombre completo de un componente.
2	La vista del dispositivo proporciona información sobre los puertos del dispositivo, la configuración y el estado actuales, datos de la tabla y los componentes de la función. Según la opción seleccionada, el área de la parte inferior de la vista del dispositivo mostrará otros datos sobre el dispositivo o cuadros de diálogo para configurar parámetros.
3	La lista de componentes contiene una lista de los componentes de las funciones. Los componentes también pueden visualizarse ampliando una función de la vista de árbol.
4	Los botones de información proporcionan acceso a datos sobre el dispositivo y al servicio de asistencia de Dell. Para obtener más información, consulte "Botones de información".

Representación del dispositivo

La página de inicio contiene una representación gráfica del panel frontal del dispositivo.

Figura 5-2. Indicadores de puerto del dispositivo PowerConnect



El color de los puertos indica si un puerto determinado está actualmente activo. Los puertos pueden tener los colores siguientes:

Tabla 5-2. Indicadores de apilamiento y de puerto de PowerConnect

Componente	Descripción
Indicadores de puerto	
Verde	El puerto está activado.
Rojo	Se ha producido un error en el puerto.
Azul	El puerto está desactivado.

Rojo	El dispositivo no está enlazado en una pila.

NOTA: los LED de puerto no se reflejan en el panel frontal de PowerConnect en el administrador de conmutadores OpenManage. El estado de los LED solamente se puede determinar al observar el dispositivo real. Sin embargo, los LED de apilamiento reflejan el estado del puerto de apilamiento. Para obtener más información sobre los LED, consulte **Definiciones de los LED**.

Uso de los botones del administrador de conmutadores

En esta sección se describen los botones de la interfaz del administrador de conmutadores OpenManage. Los botones de la interfaz se dividen en las categorías siguientes:

Botones de información

Los botones de información proporcionan acceso a asistencia y ayuda en línea, así como información sobre las interfaces del administrador de conmutadores OpenManage.

Tabla 5-3. Botones de información

Botón	Descripción
Support (Asistencia)	Abre la página Web de asistencia de Dell **support.dell.com**.
Help (Ayuda)	Muestra la ayuda en línea, que contiene información de ayuda para configurar y administrar el dispositivo. Las páginas de la ayuda en línea son sensibles al contexto. Por ejemplo, si la página **IP Addressing** (Direccionamiento IP) está abierta, cuando se haga clic en **Help** (Ayuda), se abrirá el tema de ayuda correspondiente a dicha página.
About (Acerca de)	Contiene el número de versión y de compilación, además de información de derechos de autor de Dell.
Log Out (Desconectar)	Abre la ventana de cierre de sesión.

Botones de administración de dispositivos

Los botones de administración de dispositivos proporcionan un método sencillo para configurar la información del dispositivo. Dichos botones son:

Tabla 5-4. Botones de administración de dispositivos

Botón	Descripción
Apply Changes (Aplicar cambios)	Aplica los cambios establecidos al dispositivo.
Add (Añadir)	Añade información a las tablas o cuadros de diálogo.
Telnet	Inicia una sesión Telnet.
Query (Consultar)	Consulta las tablas.
Show All (Mostrar todo)	Muestra las tablas de dispositivos.
Flechas izquierda y derecha	Desplaza información entre las listas.
Refresh (Actualizar)	Actualiza la información del dispositivo.
Reset All Counters (Restablecer todos los contadores)	Restablece los contadores de estadísticas.
Print (Imprimir)	Imprime la página **Network Management System** (Sistema de gestión de red) o la información de la tabla.
Draw (Dibujar)	Crea gráficos de estadísticas directamente.

Definiciones de campo

Los campos definidos por el usuario pueden contener entre 1 y 159 caracteres, a menos que se especifique de otro modo en la página Web del administrador de conmutadores OpenManage. Se pueden utilizar todas las letras y caracteres, excepto los siguientes:

- \
- /
- :
- *
- ?
- <
- >
- |

Acceso al dispositivo a través de la CLI

Los dispositivos se pueden administrar a través de una conexión directa con el puerto de terminal o de una conexión Telnet. Si el acceso se realiza a través de una conexión Telnet, asegúrese de que el dispositivo tenga una dirección IP definida y que la estación de trabajo utilizada para acceder al dispositivo esté conectada al mismo antes de utilizar los comandos de la CLI.

Para obtener más información sobre la configuración de una dirección IP inicial, consulte "Configuración inicial".

NOTA: asegúrese de que ha descargado el software en el dispositivo antes de utilizar la CLI para acceder al dispositivo de forma remota.

Conexión a través del terminal

1. Encienda el dispositivo y espere hasta que se haya iniciado completamente.
2. Cuando aparezca la línea de comandos Console>, escriba enable y pulse <Intro>.
3. Configure el dispositivo y escriba los comandos necesarios para completar las tareas requeridas.
4. Cuando haya finalizado, introduzca el comando **exit** del modo Privileged EXEC.

   La sesión finaliza.

NOTA: si otro usuario inicia sesión en el sistema en el modo de comandos Privileged EXEC, el usuario actual se desconectará y se conectará el nuevo usuario.

Conexión a través de Telnet

Telnet es un protocolo TCP/IP de emulación de terminal. Los terminales RS-232 pueden conectarse virtualmente al dispositivo local mediante una red de protocolo TCP/IP. Telnet es una alternativa a un terminal de conexión local cuando se necesita un inicio de sesión remoto.

El dispositivo admite un máximo de cuatro sesiones Telnet simultáneas para administrar el dispositivo. Todos los comandos de la CLI pueden usarse en una sesión Telnet.

Para iniciar una sesión Telnet:

1. Seleccione Inicio > Ejecutar.

   Se abre la ventana Ejecutar.
2. En la ventana **Ejecutar**, escriba Telnet <*dirección IP*> en el campo **Abrir**.
3. Haga clic en **Aceptar**.

   Se inicia la sesión Telnet.

Uso de la CLI

En esta sección se proporciona información sobre la utilización de la CLI.

Información general sobre el modo de comandos

La interfaz de la línea de comandos (CLI) se divide en dos modos de comandos. Cada modo de comandos tiene un grupo de comandos específicos. Si se escribe un signo de interrogación en el indicador del terminal, aparece una lista de los comandos disponibles para ese modo de comandos en particular.

En cada modo se utiliza un comando específico para desplazarse de un modo de comandos a otro.

Durante la inicialización de sesión en la CLI, el modo de la CLI es el modo User EXEC. En este modo sólo hay disponible un pequeño grupo de comandos. Este nivel está reservado para tareas que no modifican la configuración del terminal y se usa para acceder a subsistemas de configuración, como la CLI. Para pasar al siguiente nivel, el modo Privileged EXEC, se necesita una contraseña (si se ha configurado).

El modo Privileged EXEC permite el acceso a la configuración general del dispositivo. Para las configuraciones globales específicas de un dispositivo, pase al siguiente nivel, el modo Global Configuration. No es necesaria una contraseña.

El modo Global Configuration administra la configuración del dispositivo en un nivel global.

El modo Interface Configuration configura el dispositivo en el nivel de interfaz física. Los comandos de la interfaz que requieren subcomandos tienen otro nivel, el modo Subinterface Configuration. No es necesaria una contraseña.

Modo User EXEC

Después de iniciar sesión en el dispositivo, se activa el modo de comandos EXEC. La petición del nivel de usuario consta del nombre host seguido del paréntesis angular (>). Por ejemplo:

```
console>
```

NOTA: el nombre de host predeterminado es console a menos que se haya modificado durante la configuración inicial.

Los comandos del modo User EXEC permiten establecer conexión con los dispositivos remotos, modificar temporalmente la configuración del terminal, realizar pruebas básicas y enumerar la información del sistema.

Para enumerar los comandos User EXEC, introduzca un signo de interrogación en el indicador de comandos.

Modo Privileged EXEC

El acceso al modo Privileged se puede proteger para evitar el acceso no autorizado al mismo y garantizar el funcionamiento de los parámetros operativos. Las contraseñas aparecen en pantalla y distinguen entre mayúsculas y minúsculas.

Para acceder al modo Privileged EXEC y ver los comandos del mismo:

1. En la línea de comandos, escriba `enable` y pulse <Intro>.
2. Cuando aparezca el indicador de contraseña, introduzca la contraseña y pulse <Intro>.

La línea de comandos del modo Privileged EXEC consta del nombre de host del dispositivo seguido del símbolo de almohadilla (#). Por ejemplo:

```
console#
```

Para enumerar los comandos Privileged EXEC, escriba un signo de interrogación en el indicador de comandos.

Para volver del modo Privileged EXEC al modo User EXEC, escriba disable y pulse <Intro>.

En el ejemplo siguiente se muestra cómo acceder al modo Privileged EXEC y, a continuación, volver al modo User EXEC:

```
console> enable

Enter Password: ******

console#

console# disable

console>
```

Utilice el comando **exit** para volver al modo anterior (por ejemplo, para volver del modo Interface Configuration al modo Global Configuration y del modo Global Configuration al modo Privileged EXEC).

Modo Global Configuration

Los comandos de Global Configuration se aplican a las características del sistema en vez de a una interfaz o un protocolo específico.

Para acceder al modo Global Configuration, en la línea de comandos del modo Privileged EXEC, escriba el comando **configure** y pulse <Intro>. El modo Global Configuration aparece consta del nombre de host del dispositivo seguido de (config) y el símbolo de almohadilla (#).

```
console(config)#
```

Para enumerar los comandos del modo Global Configuration, entre un signo de interrogación en el indicador de comandos.

Para volver del modo Global Configuration al modo Privileged EXEC, escriba el comando **exit** o utilice la combinación de teclas <Ctrl>+<Z>.

El ejemplo siguiente ilustra cómo acceder al modo Global Configuration y volver al modo Privileged EXEC:

```
console#

console# configure

console(config)# exit
```

```
console#
```

Para obtener una lista completa de los modos de la CLI, consulte la publicación **Dell™ PowerConnect™3424/P and PowerConnect 3448/P CLI Guide** (Guía de la CLI de Dell™ PowerConnect™3424/P y PowerConnect 3448/P).

Regresar a la página de contenido

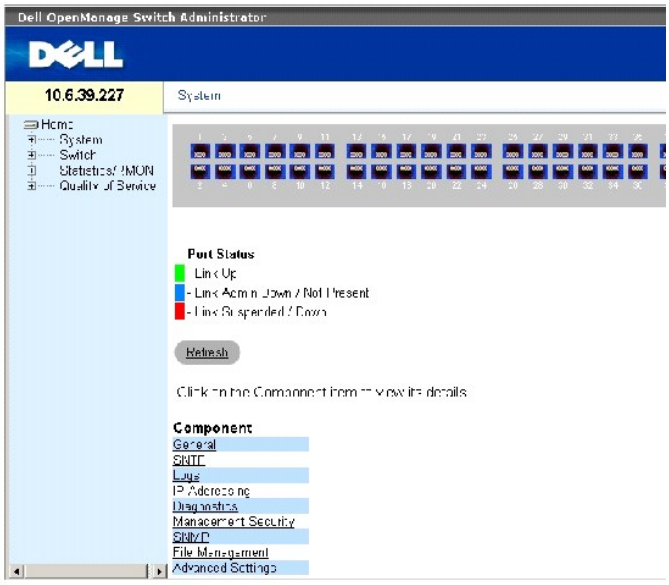
Regresar a la página de contenido

Configuración de la información del sistema

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

En esta sección se proporciona información para definir los parámetros del sistema, como por ejemplo las funciones de seguridad, la descarga de software del conmutador y el restablecimiento del conmutador. Para abrir la página **System** (Sistema), haga clic en **System** (Sistema) en la vista de árbol.

Figura 6-1. System



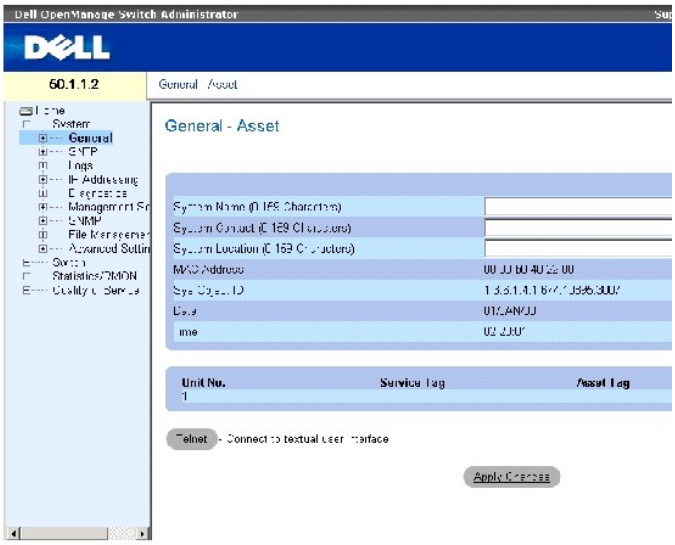
Definición de la información general del conmutador

La página **General** contiene enlaces a páginas que permiten a los administradores de red configurar los parámetros del conmutador.

Visualización de la información de inventario del conmutador

La página **Asset**(Inventario) contiene parámetros para configurar y visualizar información general del dispositivo, incluidos el nombre, la ubicación y el contacto del sistema, la dirección MAC y la ID de objeto del sistema, así como la fecha, la hora y el tiempo de actividad del sistema. Para abrir la página **Asset** (Inventario), haga clic en System (Sistema) → General → Asset (Inventario) en la vista de árbol.

Figura 6-2. Asset



La página **Asset** (Inventario) contiene los campos siguientes:

System Name (0-159 Characters) (Nombre del sistema [0-159 caracteres]): especifica el nombre del dispositivo definido por el usuario.

System Contact (0-159 Characters) (Contacto del sistema [0-159 caracteres]): indica el nombre de la persona de contacto.

System Location (0-159 Characters) (Ubicación del sistema [0-159 caracteres]): indica la ubicación en la que se ejecuta el sistema.

MAC Address (Dirección MAC): indica la dirección MAC del dispositivo.

Sys Object ID (ID de objeto del sistema): identificación de autorización del proveedor para el subsistema de gestión de red incluido en la entidad.

Date (DD/MMM//YY) (Fecha [DD/MMM/AA]): indica la fecha actual. El formato es día, mes, año. Por ejemplo, 10/10/03 corresponde al 10 de octubre de 2003.

Time (HH:MM:SS) (Hora [HH:MM:SS]): indica la hora. El formato es hora, minuto, segundo. Por ejemplo, 20:12:21 corresponde a las ocho horas de la tarde, doce minutos y tres segundos.

Unit No. (Nº de unidades): indica el número de unidades para las que se visualiza la información de inventario del dispositivo.

Service Tag (Etiqueta de servicio): número de referencia de servicio que se utiliza cuando se efectúan tareas de mantenimiento del dispositivo.

Asset Tag (0-16 Characters) (Etiqueta de inventario [0-16 caracteres]): indica la referencia del dispositivo definida por el usuario.

Serial No. (Nº de serie): indica el número de serie del dispositivo.

Definición de la información del sistema

1. Abra la página **Asset** (Inventario).
2. Defina los campos pertinentes.

3. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros del sistema y se actualiza el dispositivo.

Inicio de una sesión Telnet

1. Abra la página **Asset** (Inventario).
2. Haga clic en **Telnet**.

Se inicia una sesión Telnet.

Configuración de la información del dispositivo mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver y configurar los campos de la página **Asset** (Inventario).

Tabla 6-1. Comandos de la CLI para el inventario

Comando de la CLI	Descripción
hostname nombre	Indica o modifica el nombre de host del dispositivo.
snmp-server contact texto	Configura un contacto del sistema.
snmp-server location texto	Introduce información sobre dónde está ubicado el dispositivo.
clock set hh:mm:ss día mes año	Establece manualmente el reloj y la fecha del sistema.
show clock [detail]	Muestra la hora y la fecha del reloj del sistema.
show system id	Muestra información de la etiqueta de servicio.
show system	Muestra información del sistema.
asset-tag texto	Establece la etiqueta de inventario del dispositivo.
show stack <1-6>	Muestra información de la pila del sistema.
show system [unit *unidad*]	Muestra información del sistema.
show system id [unit *unidad*]	Muestra información de identificación del sistema.

A continuación se muestra un ejemplo de definición del nombre de host del dispositivo, el contacto del sistema y la ubicación del dispositivo, y de la configuración de la hora y la fecha del reloj del sistema mediante los comandos de la CLI:

```
console(config)# hostname dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York

dell (config)# exit

Console(config)# snmp-server host 10.1.1.1 management 2

Console# clock set 13:32:00 7 Mar 2002

Console# show clock
```

15:29:03 Jun 17 2002

A continuación se muestra un ejemplo de visualización de información del sistema correspondiente a un dispositivo independiente mediante los comandos de la CLI:

console# show system id	
Service tag :	
Serial number : 51	
Asset tag :	
console# show system	
System Description:	Ethernet Switch
System Up Time (days,hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424
Main Power Supply Status:	OK
Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30
Temperature Sensor Status:	OK

A continuación se muestra un ejemplo de visualización de información del sistema correspondiente a dispositivos apilados mediante los comandos de la CLI:

```
console# show system id

Unit  Serial number  Asset tag  Service tag
----  -------------  ---------  -----------
1     893658972      mkt-1      89788978
2     893658973      mkt-2      89788979
3     893658974      mkt-3      89788980
4     893658975      mkt-4      89788981
5     893658976      mkt-5      89788982
6     893658977      mkt-6      89788983

console# show system

Unit  Type
----  -----------------
1     PowerConnect 3424
2     PowerConnect 3424
3     PowerConnect 3428
4     PowerConnect 3424P
5     PowerConnect 3424P
6     PowerConnect 3424P

Unit  Main Power Supply  Redundant Power Supply
----  -----------------  ----------------------
1     OK
```

2	OK				
3	OK				
4	OK		OK		
5	OK		OK		
6	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
----	----	----	----	----	----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
Unit	Temperature (Celsius)		Temperature Sensor Status		
----	----------		----------		
1	30		OK		
2	30		OK		
3	30		OK		
4	30		OK		
5	30		OK		
6	30		OK		

Definición de los valores de hora del sistema

La página **Time Synchronization** (Sincronización de la hora) contiene campos para definir los parámetros de hora del sistema tanto para el reloj de hardware local como para el reloj SNTP externo. Si la hora del sistema se indica mediante un reloj SNTP externo y dicho reloj falla, la hora del sistema se mostrará en el reloj de hardware local. Es posible activar el horario de verano en el dispositivo. A continuación se muestra una lista de las fechas inicial y final del horario de verano en distintos países:

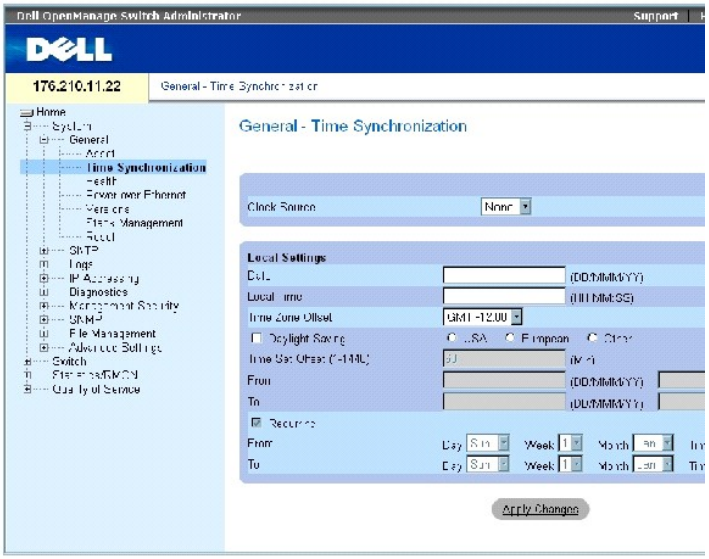
- Albania: del último fin de semana de marzo al último fin de semana de octubre.
- Australia: del último día de octubre al último día de marzo.
- Australia - Tasmania: del primer día de octubre al último día de marzo.
- Armenia: del último fin de semana de marzo al último fin de semana de octubre.
- Austria: del último fin de semana de marzo al último fin de semana de octubre.
- Bahamas: de abril a octubre, coincidiendo con el horario de verano de los Estados Unidos.
- Bielorrusia: del último fin de semana de marzo al último fin de semana de octubre.
- Bélgica: del último fin de semana de marzo al último fin de semana de octubre.
- Brasil: del tercer domingo de octubre al tercer sábado de marzo. Durante el horario de verano, en la mayor parte del sureste de Brasil se adelanta el reloj una hora.
- Chile: en la Isla de Pascua, del 9 de marzo al 12 de octubre. El primer domingo de marzo o después del 9 de marzo.
- China: no se sigue el horario de verano.
- Canadá: del primer domingo de abril al último domingo de octubre. Los gobiernos provinciales y territoriales suelen encargarse de regular el horario de verano. Puede haber excepciones en algunos municipios.
- Cuba: del último domingo de marzo al último domingo de octubre.
- Chipre: del último fin de semana de marzo al último fin de semana de octubre.
- Dinamarca: del último fin de semana de marzo al último fin de semana de octubre.
- Egipto: del último viernes de abril al último jueves de septiembre.
- Estonia: del último fin de semana de marzo al último fin de semana de octubre.
- Finlandia: del último fin de semana de marzo al último fin de semana de octubre.
- Francia: del último fin de semana de marzo al último fin de semana de octubre.
- Alemania: del último fin de semana de marzo al último fin de semana de octubre.
- Grecia: del último fin de semana de marzo al último fin de semana de octubre.
- Hungría: del último fin de semana de marzo al último fin de semana de octubre.
- India: no se sigue el horario de verano.
- Irán: del primer día de Farvardin al primer día de Mehr.
- Irak: del 1 de abril al 1 de octubre.
- Irlanda: del último fin de semana de marzo al último fin de semana de octubre.
- Israel: varía cada año.
- Italia: del último fin de semana de marzo al último fin de semana de octubre.
- Japón: no se sigue el horario de verano.
- Jordania: del último fin de semana de marzo al último fin de semana de octubre.
- Letonia: del último fin de semana de marzo al último fin de semana de octubre.
- Líbano: del último fin de semana de marzo al último fin de semana de octubre.
- Lituania: del último fin de semana de marzo al último fin de semana de octubre.
- Luxemburgo: del último fin de semana de marzo al último fin de semana de octubre.
- Macedonia: del último fin de semana de marzo al último fin de semana de octubre.
- México: desde las 02:00 horas del primer domingo de abril hasta las 02:00 horas del último domingo de octubre.
- Moldavia: del último fin de semana de marzo al último fin de semana de octubre.
- Montenegro: del último fin de semana de marzo al último fin de semana de octubre.
- Países Bajos: del último fin de semana de marzo al último fin de semana de octubre.
- Nueva Zelanda: del primer domingo de octubre al primer domingo a partir del 15 de marzo o después de esta fecha.
- Noruega: del último fin de semana de marzo al último fin de semana de octubre.
- Paraguay: del 6 de abril al 7 de septiembre.
- Polonia: del último fin de semana de marzo al último fin de semana de octubre.
- Portugal: del último fin de semana de marzo al último fin de semana de octubre.
- Rumanía: del último fin de semana de marzo al último fin de semana de octubre.
- Rusia: del último fin de semana de marzo al último fin de semana de octubre.
- Serbia: del último fin de semana de marzo al último fin de semana de octubre.

- República Eslovaca: del último fin de semana de marzo al último fin de semana de octubre.
- Sudáfrica: no se sigue el horario de verano.
- España: del último fin de semana de marzo al último fin de semana de octubre.
- Suecia: del último fin de semana de marzo al último fin de semana de octubre.
- Suiza: del último fin de semana de marzo al último fin de semana de octubre.
- Siria: del 31 de marzo al 30 de octubre.
- Taiwán: no se sigue el horario de verano.
- Turquía: del último fin de semana de marzo al último fin de semana de octubre.
- Reino Unido: del último fin de semana de marzo al último fin de semana de octubre.
- Estados Unidos de América: desde las 02:00 horas del primer domingo de abril hasta las 02:00 horas del último domingo de octubre.

Para obtener más información sobre SNTP, consulte "**Configuración de SNTP**".

Para abrir la página **Time Synchronization** (Sincronización de la hora), haga clic en **System** (Sistema) → **General** → **Time Synchronization** (Sincronización de la hora) en la vista de árbol.

Figura 6-3. Time Synchronization



La página **Time Synchronization** (Sincronización de la hora) contiene los campos siguientes:

Clock Source (Fuente del reloj)

Clock Source (Fuente del reloj): fuente utilizada para establecer el reloj del sistema. Los valores del campo posibles son:

SNTP: indica que la hora del sistema se establece a través de un servidor SNTP. Para obtener más información, consulte "Configuración de SNTP".

None (Ninguna): indica que la hora del sistema no se establece mediante una fuente externa.

Local Settings (Configuración local)

Date (Fecha): define la fecha del sistema. El formato de fecha es DD/MMM/AA; por ejemplo 04/May/05.

Local Time (Hora local): define la hora del sistema. El formato de este campo es HH/MM/SS; por ejemplo 21/15/03.

Time Zone Offset (Diferencia de zona horaria): diferencia entre la hora del meridiano de Greenwich (GMT) y la hora local. Por ejemplo, la diferencia de zona horaria de París es GMT +1:00, mientras que la hora local de Nueva York es GMT −5:00.

Existen dos tipos de configuración del horario de verano: mediante una fecha específica de un año concreto o mediante una configuración periódica independiente del año. Para una configuración específica de un año concreto, complete el área **Daylight Savings** (Horario de verano); para una configuración periódica, complete el área **Recurring** (Periódico)

Daylight Savings (Horario de verano): activa el horario de verano (DST) en el dispositivo de acuerdo con la ubicación de éste. Los valores del campo posibles son:

USA (Estados Unidos): la hora del dispositivo cambia al horario de verano a las 2 a.m. del primer domingo de abril y vuelve al horario estándar a las 2 a.m. del último domingo de octubre.

European (Europa): el dispositivo cambia al horario de verano a la 1:00 a.m. del último domingo de marzo y vuelve al horario estándar a la 1:00 a.m. del último domingo de octubre. El valor European (Europa) se aplica a los miembros de la UE y a otros países europeos que utilizan el estándar de la UE.

Other (Otro): el usuario especifica las definiciones del horario de verano según la ubicación del dispositivo. Si se selecciona el valor **Other** (Otro), deberán completarse los campos **From** (Desde) y **To** (Hasta).

Time Set Offset (1-1440) (Diferencia de hora definida [1-1440]): tiempo en minutos en el que se puede establecer el horario de verano para los países que no son Estados Unidos ni forman parte de Europa. El valor predeterminado es 60 minutos.

From (Desde): define la hora a la que empieza el horario de verano en países que no son Estados Unidos ni forman parte de Europa, con el formato DD/MMM/AA en un campo, y la hora en otro. Por ejemplo, si el horario de verano empieza el 25 de octubre de 2007 a las 5.00 a.m., los dos campos se definen como 25/Oct/07 y 05:00. Los valores del campo posibles son:

Date (Fecha): fecha en la que empieza el horario de verano. El intervalo de valores posibles es 1-31.

Month (Mes): mes del año en el que empieza el horario de verano. El intervalo de valores posibles es Jan-Dec (enero-diciembre).

Year (Año): año en el que empieza el horario de verano configurado.

Time (Hora): hora a la que empieza el horario de verano. El formato de este campo es horas: minutos; por ejemplo, 05:30.

To (Hasta): define la hora a la que termina el horario de verano en países que no son Estados Unidos ni forman parte de Europa, con el formato DD/MMM/AA en un campo, y la hora en otro. Por ejemplo, si el horario de verano finaliza el 23 de marzo de 2008 a las 12:00 a.m., los dos campos se definirán como 23/Mar/08 y 12:00. Los valores del campo posibles son:

Date (Fecha): fecha en la que termina el horario de verano. El intervalo de valores posibles es 1-31.

Month (Mes): mes del año en el que termina el horario de verano. El intervalo de valores posibles es Jan-Dec (enero-diciembre).

Year (Año): año en el que termina el horario de verano configurado.

Time (Hora): hora a la que termina el horario de verano. El formato de este campo es horas:minutos; por ejemplo, 05:30.

Recurring (Periódico): define la hora a la que empieza el horario de verano en países que no son Estados Unidos ni forman parte de Europa y donde el horario de verano es el mismo cada año. Los valores del campo posibles son:

From (Desde): define la hora a la que empieza el horario de verano cada año. Por ejemplo, el horario de verano empieza localmente cada segundo domingo de abril a las 5:00 a.m. Los valores del campo posibles son:

Day (Día): día de la semana en el que empieza el horario de verano cada año. El intervalo de valores posibles es Sunday-Saturday (domingo-sábado).

Week (Semana): semana del mes en la que empieza el horario de verano cada año. El intervalo de valores posibles es 1-5.

Month (Mes): mes del año en el que empieza el horario de verano cada año. El intervalo de valores posibles es Jan-Dec (enero-diciembre).

Time (Hora): hora a la que empieza el horario de verano cada año. El formato de este campo es horas: minutos; por ejemplo, 02:10.

To (Hasta): define la hora recurrente a la que empieza el horario de verano cada año. Por ejemplo, el horario de verano termina localmente cada cuarto viernes de octubre a las 5:00 a.m. Los valores del campo posibles son:

Day (Día): día de la semana en el que termina el horario de verano cada año. El intervalo de valores posibles es Sunday-Saturday (domingo-sábado).

Week (Semana): semana del mes en la que termina el horario de verano cada año. El intervalo de valores posibles es 1-5.

Month (Mes): mes del año en el que termina el horario de verano cada año. El intervalo de valores posibles es Jan-Dec (enero-diciembre).

Time (Hora): hora a la que termina el horario de verano cada año. El formato de este campo es horas:minutos; por ejemplo, 05:30.

Selección de una fuente del reloj

1. Abra la página **Time Synchronization** (Sincronización de la hora).
2. Defina el campo **Clock Source** (Fuente del reloj).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona la fuente del reloj y se actualiza el dispositivo.

Configuración del reloj local

1. Abra la página **Time Synchronization** (Sincronización de la hora).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se aplica la configuración del reloj local.

Configuración del reloj mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página "**Time Synchronization**" (Sincronización de la hora).

NOTA: antes de configurar el reloj en horario de verano, debe realizar los pasos siguientes:

1. Configure la hora de verano.
2. Defina la zona horaria.
3. Configure el reloj.

Por ejemplo:

```
console(config)# clock summer-time recurring usa
console(config)# clock time zone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

Tabla 6-2. Comandos de la CLI para la configuración del reloj

CLI	Descripción
clock source sntp	Configura una fuente externa para la hora del reloj del sistema.
clock time zone *diferencia-horas* [**minutes** *diferencia-minutos*][**zone** *sigla*]	Configura la visualización de la zona horaria.
clock summer-time	Configura el sistema para que cambie automáticamente al horario de verano.
clock summer-time recurring {**usa** | **eu** | *semana día mes hh:mm semana día mes hh:mm}* [**offset** *diferencia*] [**zone** *sigla*]	Configura el sistema para que cambie automáticamente al horario de verano (según los estándares de los Estados Unidos y Europa).
clock summer-time date *día mes año hh:mm día mes año hh:mm* **[offset** *diferencia***] [zone** *sigla***]**	Configura el sistema para que cambie automáticamente al horario de verano durante un periodo específico con el formato fecha/mes/año.

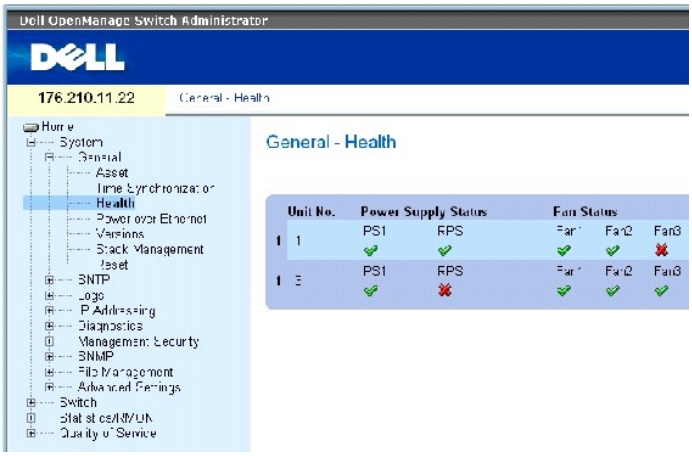
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# clock
timezone -6 zone CST



console(config)# clock
summer-time recurring
first sun apr 2:00 last
sun oct 2:00



console(config)# clock
source sntp



console(config)# interface
ethernet e14



console(config-if)# sntp
client enable



console(config-if)# exit



console(config)# sntp
broadcast client enable
```

Visualización de la información de estado del sistema

La página **System Health** (Estado del sistema) muestra información del dispositivo físico, como por ejemplo el estado de sus fuentes de energía y de ventilación. Para abrir la página **System Health** (Estado del sistema), haga clic en **System** (Sistema) → **General** → **Health** (Estado) en la vista de árbol.

Figura 6-4. System Health



La página **System Health** (Estado del sistema) contiene los campos siguientes:

Unit No. (Nº de unidad): indica el número de la unidad para la que se muestra información de inventario del dispositivo.

Power Supply Status (Estado de la fuente de alimentación): el dispositivo tiene dos fuentes de alimentación. La fuente de alimentación 1 aparece como PS1 en la interfaz, mientras que la fuente de alimentación redundante aparece como RPS. Los valores del campo posibles son:

: la fuente de alimentación funciona con normalidad.

: la fuente de alimentación no funciona con normalidad.

Not Present (No presente): indica que no hay ninguna fuente de alimentación en este momento.

Fan Status (Estado del ventilador): los dispositivos sin PoE disponen de dos ventiladores, mientras que los dispositivos con PoE cuentan con cinco ventiladores. Cada ventilador se identifica mediante "fan" seguido del número de ventilador en la interfaz. Los valores del campo posibles son:

:el ventilador funciona con normalidad.

: el ventilador no funciona con normalidad.

Not Present (No presente): indica que no hay ningún ventilador en este momento.

Temperature (Temperatura): temperatura a la que se está ejecutando el dispositivo actualmente. La temperatura del dispositivo se visualiza en grados Celsius. El umbral de temperatura del dispositivo es 0-40 ºC (32-104 ºF). En la tabla siguiente se muestra la temperatura en grados Fahrenheit en incrementos de 5.

Tabla 6-3. Tabla de conversión de Celsius a Fahrenheit

Celsius	Fahrenheit
0	32
5	41
10	50
15	59
20	68

25	77
30	86
35	95
40	104

Visualización de la información de estado del sistema mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página **System Health** (Estado del sistema).

Tabla 6-4. Comando de la CLI para el estado del sistema

Comando de la CLI	Descripción
show system [unit *unidad*]	Muestra información del sistema.

A continuación se muestra un ejemplo de los comandos de la CLI para el estado del sistema:

```
Console> show system

System Description: Ethernet switch

System Up Time (days,hour:min:sec): 1,22:38:21

System Contact:

System Name: RS1

System location:

System MAC Address: 00.10.B5.F4.00.01

Sys Object ID: 1.3.6.1.4.1.674.10895.3004

Type: PowerConnect 3424

Temperature Sensors:

Unit    Sensor    Temperature (Celsius)    Status
----    ------    ---------------------    ------
1       1                 41               OK
1       2                 41               OK
2       1                 42               OK
```

2	2		42	OK
Unit	Power Supply	Source	Status	
----	----------	------	------	
1	Main	AC	OK	
2	Secondary	AC	OK	
Unit	Fan	Status		
----	---	------		
1	CPU	OK		
2	CPU	OK		

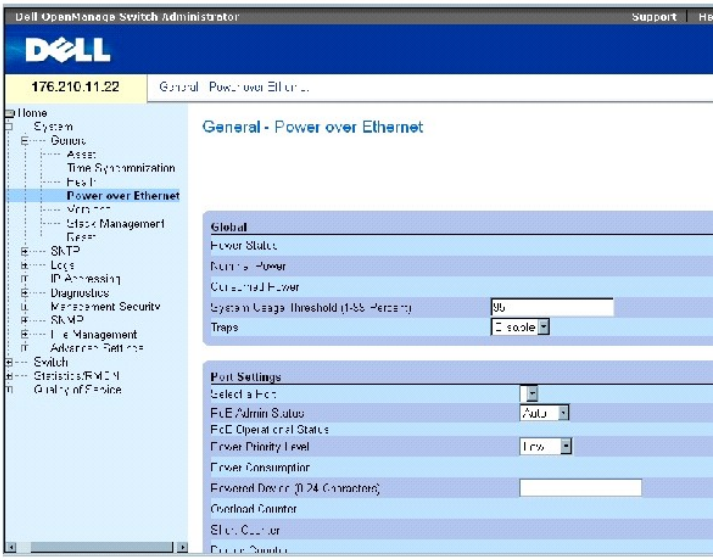
Administración de la alimentación a través de Ethernet

La alimentación a través de Ethernet (PoE) proporciona alimentación a los dispositivos en un cableado de LAN existente sin que deba actualizarse ni modificarse la infraestructura de la red. Con PoE, ya no es necesario colocar los dispositivos de red cerca de fuentes de energía.

Los dispositivos alimentados son dispositivos que reciben alimentación de fuentes de alimentación PowerConnect, como por ejemplo, los teléfonos IP. Los dispositivos alimentados se conectan al dispositivo PowerConnect a través de puertos Ethernet. Los dispositivos alimentados se conectan a través de los 24 puertos FE de PowerConnect 3424P o de los 48 puertos FE de PowerConnect 3448P.

Para abrir la página Power Over Ethernet (Alimentación a través de Ethernet), haga clic en **System** (Sistema) → **General** → **Power over Ethernet** (Alimentación a través de Ethernet) en la vista de árbol.

Figura 6-5. Power Over Ethernet



La página Power Over Ethernet (Alimentación a través de Ethernet) contiene las secciones siguientes:

- Global (Configuración global)
- Port Settings (Configuración de puerto)

Global (Configuración global)

La sección de configuración global de **Power over Ethernet** (Alimentación a través de Ethernet) contiene los campos siguientes:

Power Status (Estado de alimentación): indica el estado de la fuente de energía en línea.

On (Encendida): indica que la unidad de fuente de alimentación está en funcionamiento.

Off (Apagada): indica que la unidad de fuente de alimentación no está en funcionamiento.

Faulty (Error): indica que la unidad de fuente de alimentación funciona, pero se ha producido un error. Por ejemplo, cuando se produce una sobrecarga de alimentación o un cortocircuito.

Nominal Power (Potencia nominal): indica la cantidad real de alimentación que el dispositivo puede proporcionar. El valor de este campo se muestra en vatios.

Consumed Power (Alimentación consumida): indica la cantidad de alimentación utilizada por el dispositivo. El valor de este campo se muestra en vatios.

System Usage Threshold (1-99 Percent) (Umbral de uso del sistema [1-99 por ciento]): indica el porcentaje de alimentación consumida antes de que se genere una alarma. El intervalo de valores posibles del campo es 1-99 por ciento. El valor predeterminado es 95 por ciento.

Traps (Excepciones): activa o desactiva la recepción de excepciones de dispositivo PoE. De forma predeterminada, esta opción está desactivada.

Port Settings (Configuración de puerto)

Select a Port (Seleccione un puerto): indica la interfaz específica para la que se definen los parámetros de PoE y se asignan a la interfaz alimentada conectada al puerto seleccionado.

PoE Admin Status (Estado de administración de PoE): indica el modo PoE del dispositivo. Los valores del campo posibles son:

Auto (Automático): activa el protocolo de detección de dispositivos y suministra alimentación al dispositivo mediante el módulo PoE. El protocolo de detección de dispositivos permite al dispositivo detectar los dispositivos alimentados que están conectados a las interfaces de dispositivo, así como obtener su clasificación. Éste es el valor predeterminado.

Never (Nunca): desactiva el protocolo de detección de dispositivos y detiene el suministro de alimentación al dispositivo mediante el módulo PoE.

PoE Operational Status (Estado operativo de PoE): indica si el puerto está activado para funcionar en modo PoE. Los valores del campo posibles son:

On (Activado): indica que el dispositivo está suministrando alimentación a la interfaz.

Off (Desactivado): indica que el dispositivo no está suministrando alimentación a la interfaz.

Test Fail (Error en la prueba): indica que la prueba del dispositivo alimentado ha fallado. Por ejemplo, un puerto no se ha podido activar y no se puede utilizar para suministrar alimentación al dispositivo alimentado.

Testing (Prueba): indica que se está probando el dispositivo alimentado. Por ejemplo, se prueba un dispositivo alimentado para confirmar que está recibiendo alimentación de una fuente de alimentación.

Searching (Búsqueda): indica que el dispositivo PowerConnect está buscando un dispositivo alimentado. Éste es el estado operativo predeterminado de PoE.

Fault (Fallo): indica que el dispositivo PowerConnect ha detectado un fallo en el dispositivo alimentado. Por ejemplo, no se ha podido leer la memoria del dispositivo alimentado.

Power Priority Level (Nivel de prioridad de alimentación): determina la prioridad de puerto si el nivel de la fuente de alimentación es bajo. La prioridad de alimentación de puerto se utiliza cuando el nivel de la fuente de alimentación es bajo. El valor predeterminado de este campo es **Low** (Bajo). Por ejemplo, supongamos que el puerto 1 tiene asignada la prioridad alta y el puerto 3 tiene asignada la prioridad baja. Si se está utilizando el 99 % de la fuente de alimentación, el puerto 1 tendrá prioridad para recibir alimentación y puede que se deniegue el suministro de alimentación al puerto 3.

Critical (Crítico): asigna el nivel más alto de prioridad de alimentación.

High (Alto): asigna el segundo nivel más alto de prioridad de alimentación.

Low (Bajo): asigna el nivel de prioridad de alimentación más bajo.

Power Consumption (Consumo de energía): indica la cantidad de alimentación asignada al dispositivo alimentado conectado a la interfaz seleccionada. Los dispositivos se clasifican mediante el dispositivo alimentado, y los dispositivos PowerConnect utilizan la información de clasificación. Los valores de este campo se muestran en vatios. Los valores del campo posibles son:

0.44 – 12.95: indica que el puerto tiene asignado un nivel de consumo de energía de entre 0,44 y 12,95 vatios.

0.44 – 3.8: indica que el puerto tiene asignado un nivel de consumo de energía de entre 0,44 y 3,8 vatios.

3.84 – 6.49: indica que el puerto tiene asignado un nivel de consumo de energía de entre 3,84 y 6,49 vatios.

6.49 – 12.95: indica que el puerto tiene asignado un nivel de consumo de energía de entre 6,49 y 12,95 vatios.

Power Device (0-24 characters) (Dispositivo de alimentación [0-24 caracteres]): proporciona una descripción del dispositivo alimentado definida por el usuario. Este campo puede contener un máximo de 24 caracteres.

Overload Counter (Contador de sobrecarga): indica el total de incidencias de sobrecarga de alimentación.

Short Counter (Contador de escasez de alimentación): indica el total de incidencias de escasez de alimentación.

Denied Counter (Contador de denegación): indica las veces que se ha denegado el suministro de alimentación al dispositivo alimentado.

Absent Counter (Contador de ausencia): indica las veces que se ha detenido el suministro de alimentación a un dispositivo alimentado debido a que no se ha detectado dicho dispositivo.

Invalid Signature Counter (Contador de firmas no válidas): indica las veces que se ha recibido una firma no válida. Las firmas son el medio por el cual el dispositivo alimentado se identifica ante PSE. Las firmas se generan durante la detección, la clasificación o el mantenimiento del dispositivo alimentado.

Definición de la configuración de PoE

1. Abra la página Power Over Ethernet (Alimentación a través de Ethernet).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la configuración de PoE y se actualiza el dispositivo.

Administración de PoE mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página Power Over Ethernet (Alimentación a través de Ethernet).

Tabla 6-5. Comandos de la CLI para la configuración de PoE

Comando de la CLI	Descripción
`power inline {auto | never}`	Configura el modo administrativo de la alimentación en línea en una interfaz.
`power inline powered-device tipo-da`	Añade una descripción del tipo de dispositivo alimentado.
`power inline priority {critical | high | low}`	Configura la prioridad de la interfaz desde el punto de vista de la administración de la alimentación en línea.
`power inline usage-threshold`	Configura el umbral para desencadenar alarmas.
`power inline traps enable`	Activa las excepciones de dispositivo PoE.
`show power inline [interfaz ethernet ]`	Muestra información de configuración de PoE.

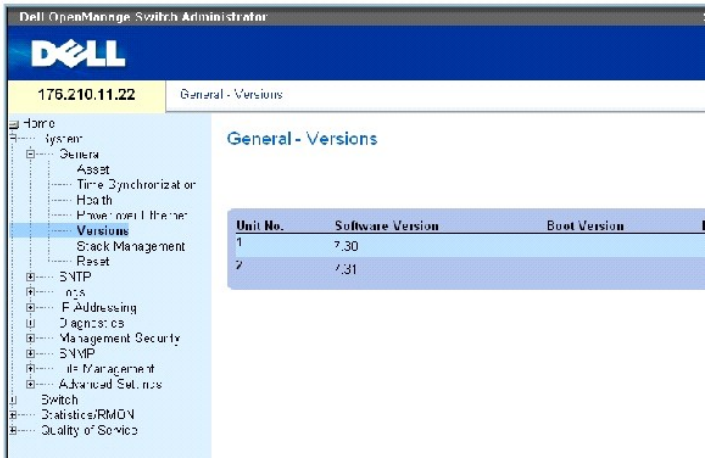
A continuación se muestra un ejemplo de los comandos de la CLI para PoE:

```
Console# show power inline

Power: On

Nominal Power: 150 Watts

Consumed Power: 120 Watts (80%)

Usage Threshold: 95%

Traps: Enabled

Port  Powered Device     State  Priority  Status  Classification [W]
----  --------------     -----  --------  ------  ------------------
1/e1  IP Phone Model A   Auto   High      On      0.44 - 12.95
2/e1  Wireless AP Model  Auto   Low       On      0.44 - 3.84
3/e1                     Auto   Low       Off     N/A


Console# show power inline ethernet 1/e1

Port  Powered Device     State  Priority  Status  Classification [W]
----  --------------     -----  --------  ------  ------------------
1/1e  IP Phone Model A   Auto   High      On      0.44 - 12.95

Overload Counter: 1

Short Counter: 0

Denied Counter: 0

Absent Counter: 0

Invalid Signature Counter: 0
```

Visualización de la información de la versión

La página **Versions** (Versiones) contiene información sobre las versiones de hardware y de software que están en ejecución. Para abrir la página **Versions** (Versiones), haga clic en System (Sistema)→ General→ Versions (Versiones) en la vista de árbol.

Figura 6-6. Versions



La página **Versions** (Versiones) contiene los campos siguientes:

Unit No. (Número de unidad): indica el número de la unidad para la que se muestran las versiones del dispositivo.

Software Version (Versión de software): versión de software que se ejecuta actualmente en el dispositivo.

Boot Version (Versión de inicio): versión de inicio que se ejecuta actualmente en el dispositivo.

Hardware Version (Versión de hardware): versión de hardware actual del dispositivo.

Visualización de las versiones del dispositivo mediante la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página Versions (Versiones).

Tabla 6-6. Comandos de la CLI para versiones

Comando de la CLI	Descripción
show version	Muestra información de la versión del sistema.

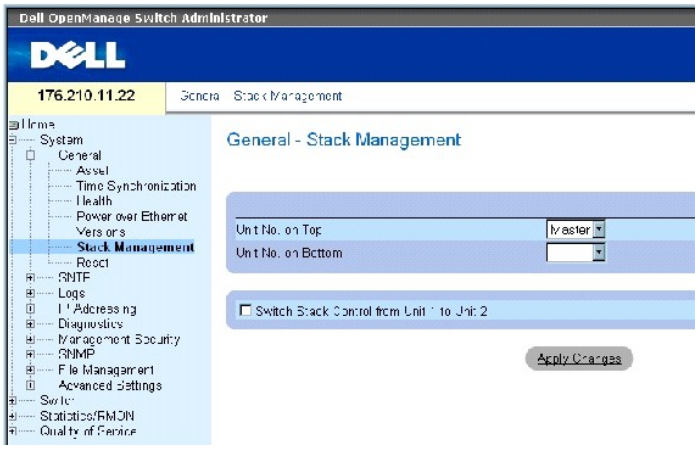
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console> show version

SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)

Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)

HW version 1.0.0
```

Administración de los miembros de una pila

La página **Stack Management** (Administración de la pila) permite a los administradores de red restablecer toda la pila o un dispositivo determinado. Para abrir la página **Stack Management** (Administración de la pila), haga clic en **System** (Sistema)→ **General**→ **Stack Management** (Administración de la pila) en la vista de árbol.

Figura 6-7. Stack Management



NOTA: antes de restablecer el dispositivo, guarde todos los cambios realizados al archivo de configuración en ejecución. De este modo evitará que se pierda la configuración del dispositivo actual. Para obtener más información sobre cómo guardar los archivos de configuración, consulte "Administración de archivos".

Unit No. on Top (Primer número de unidad): número del primer miembro de la pila. Los valores posibles son Master (unidad maestra) y 1-6.

Unit No. on Bottom (Último número de unidad): número del último miembro de la pila. Los valores posibles son Master (unidad maestra) y 1-6.

Switch Stack Control from Unit 1 to Unit 2 (Cambiar control de la pila de la unidad 1 a la unidad 2): permite cambiar de la unidad maestra actual a la unidad maestra de reserva.

NOTA: al restablecer la unidad maestra, se restablece toda la pila.

Cambio entre unidades maestras de la pila

1. Abra la página **Stack Management** (Administración de la pila).
2. Marque la casilla de verificación Switch Stack Control from Unit 1 to Unit 2 (Cambiar control de la pila de la unidad 1 a la unidad 2).
3. Haga clic en Apply Changes (Aplicar cambios).

   Aparece un mensaje de confirmación.
4. Haga clic en OK (Aceptar).

   Se restablece el dispositivo. Una vez restablecido el dispositivo, el sistema solicita un nombre de usuario y una contraseña.

Configuración del orden de visualización de la pila

1. Abra la página **Stack Management** (Administración de la pila).
2. Defina la topología de la pila definiendo las unidades superior e inferior. Estas unidades deben ser adyacentes.
3. Haga clic en **Apply Changes** (Aplicar cambios).

El orden de visualización se reconfigura en la página **System** (Sistema).

Administración de pilas mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página **Stack Management** (Administración de la pila).

Tabla 6-7. Comandos de la CLI para la administración de la pila

Comando de la CLI	Descripción
reload	Vuelve a cargar el sistema operativo.
stack reload	Vuelve a cargar los miembros de la pila.
stack master	Fuerza la selección de la unidad maestra de la pila.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# reload


Are you sure you want to erase running configuration (y/n) [n]
```

Restablecimiento del dispositivo

La página Reset (Restablecer) permite restablecer el dispositivo desde una ubicación remota. Para abrir la página Reset (Restablecer), haga clic en System (Sistema)→ General→ Reset (Restablecer) en la vista de árbol.

La página Reset (Restablecer) contiene el campo siguiente:

Reset Unit No. (Restablecer número de unidad): restablece el miembro del apilamiento seleccionado.

NOTA: antes de restablecer el dispositivo, guarde todos los cambios realizados al archivo de configuración de inicio. De este modo evitará que se pierda la configuración del dispositivo actual. Para obtener más información sobre cómo guardar los archivos de configuración, consulte "Administración de archivos".

Restablecimiento del dispositivo

1. Abra la página **Reset** (Restablecer).
2. Seleccione una unidad en el campo **Reset Unit Number** (Restablecer número de unidad).
3. Haga clic en **Apply Changes** (Aplicar cambios).

   Aparece un mensaje de confirmación.
4. Haga clic en **OK** (Aceptar).

   Se restablece el dispositivo. Una vez restablecido el dispositivo, el sistema solicita un nombre de usuario y una contraseña.
5. Introduzca un nombre de usuario y una contraseña para volver a conectarse a la interfaz Web.

Restablecimiento del dispositivo mediante la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para restablecer el dispositivo mediante la CLI:

Tabla 6-8. Comando de la CLI para el restablecimiento

Comando de la CLI	Descripción
reload	Vuelve a cargar el sistema operativo.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console >reload


This command will reset
the whole system and
disconnect your current
session. Do you want to
continue (y/n) [n] ?
```

Configuración de SNTP

El conmutador admite el protocolo simple de hora de red (SNTP). SNTP asegura una sincronización de la hora del reloj del conmutador de red con una precisión de milisegundos. La sincronización de la hora se lleva a cabo mediante un servidor SNTP de la red. SNTP funciona sólo como cliente y no puede proporcionar servicios de hora a otros sistemas.

El conmutador puede sondear los tipos de servidor siguientes para obtener la hora del servidor:

- Difusión única
- Cualquier difusión
- Difusión

Las fuentes de la hora se establecen por niveles. Estos niveles definen la precisión del reloj de referencia. Cuanto más alto sea el nivel (siendo cero es el valor superior), más preciso será el reloj. El conmutador recibe la hora a partir del nivel 1 y subsiguientes. A continuación se muestra un ejemplo de los niveles:

- **Nivel 0**: se utiliza un reloj de tiempo real como fuente de la hora, por ejemplo, un sistema GPS.
- **Nivel 1**: se utiliza un servidor que está directamente enlazado a una fuente de hora de nivel 0. Los servidores de hora de nivel 0 proporcionan estándares de hora de red primarios.
- **Nivel 2**: la fuente de la hora se aleja del servidor de nivel 1 a través de una ruta de red. Por ejemplo, un servidor de nivel 2 recibe la hora a través de un enlace de red, mediante el protocolo NTP, desde un servidor de nivel 1.

La información que se recibe de los servidores SNTP se evalúa a partir del nivel de hora y el tipo de servidor. Las definiciones de hora de SNTP se evalúan y determinan según los niveles de hora siguientes:

- **T1**: hora a la que el cliente ha enviado la petición original.
- **T2**: hora a la que el servidor ha recibido la petición original.
- **T3**: hora a la que el servidor ha enviado una respuesta al cliente.
- **T4**: hora a la que el cliente ha recibido la respuesta del servidor.

El dispositivo puede sondear los tipos de servidor siguientes para obtener la hora del servidor: difusión única, cualquier difusión y difusión.

El sondeo para obtener información de difusión única se utiliza para analizar un servidor cuya dirección IP se conoce. Los servidores SNTP que están configurados en el dispositivo son los únicos que se sondean para obtener información de sincronización. Los niveles de hora de T1 a T4 sirven para determinar la hora del servidor. Éste es el mejor método para sincronizar la hora del dispositivo, ya que es el más seguro. Si se selecciona este método, sólo se aceptará la información de SNTP procedente de los servidores SNTP que se hayan definido en el dispositivo mediante la página **SNTP Servers** (Servidores SNTP).

El sondeo para obtener información de cualquier difusión se utiliza cuando no se conoce la dirección IP del servidor. Si se selecciona este método, todos los servidores SNTP de la red podrán enviar información de sincronización. El dispositivo se sincroniza cuando realiza una petición proactiva de información de sincronización. Para establecer el valor de la hora, se utilizará la mejor respuesta (nivel inferior) de los tres primeros servidores SNTP que respondan a una

petición de información de sincronización. Los niveles de hora T3 y T4 se utilizan para determinar la hora del servidor.

Para obtener información para la sincronización de la hora del dispositivo, es preferible utilizar el sondeo de difusión única que el sondeo de difusión. Sin embargo, este método es menos seguro que el sondeo de difusión única, ya que se aceptan los paquetes SNTP procedentes de servidores SNTP no configurados en el dispositivo.

La información de difusión se utiliza cuando no se conoce la dirección IP del servidor. Cuando se envía un mensaje de difusión desde un servidor SNTP, el cliente SNTP escuchará dicho mensaje. Si el sondeo de difusión está activado, se aceptará toda la información de sincronización, aunque el dispositivo no la haya solicitado. Éste es el método menos seguro.

El dispositivo recupera la información de sincronización mediante una petición activa de la información o en cada intervalo de sondeo. Si se han activado los sondeos de difusión única, de cualquier difusión y de difusión, la información se recupera en el orden siguiente:

- Tiene preferencia la información recibida de los servidores que están definidos en el dispositivo. Si el sondeo de difusión única no está activado, o si no se ha definido ningún servidor en el dispositivo, el dispositivo aceptará la información de hora de cualquier servidor SNTP que responda.
- Si responde más de un dispositivo de difusión única, tiene preferencia la información de sincronización procedente del dispositivo con el nivel más bajo.
- Si los servidores tienen el mismo nivel, se aceptará la información de sincronización procedente del servidor SNTP que responda primero.

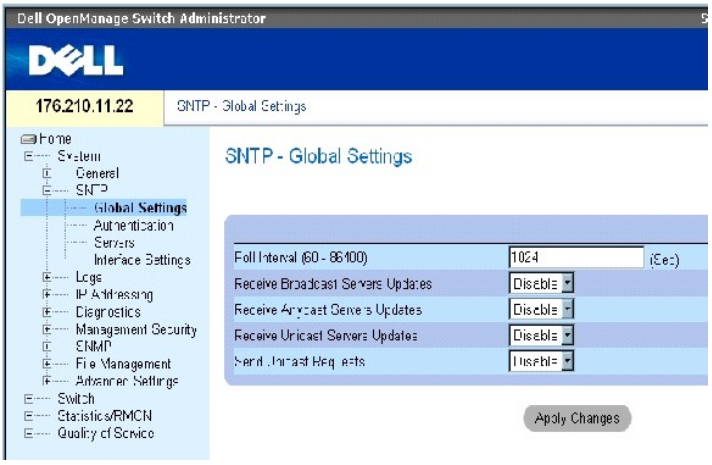
La autenticación MD5 (Message Digest 5) protege las rutas de sincronización del dispositivo hacia los servidores SNTP. MD5 es un algoritmo que genera un hash de 128 bits. MD5 es una variante de MD4 que proporciona una mayor seguridad. MD5 verifica la integridad de la comunicación y autentica su origen.

Para abrir la página **SNTP**, haga clic en **System** (Sistema)→ **SNTP** en la vista de árbol.

Definición de los parámetros globales de SNTP

La página **SNTP Global Settings** (Configuración global de SNTP) contiene información para definir los parámetros SNTP de forma global. Para abrir la página **SNTP Global Settings** (Configuración global de SNTP), haga clic en **System** (Sistema)→ **SNTP**→ **Global Settings** (Configuración global) en la vista de árbol.

Figura 6-8. SNTP Global Settings



La página **SNTP Global Settings** (Configuración global de SNTP) contiene los campos siguientes:

Poll Interval (60-86400) (Intervalo de sondeo): define el intervalo (en segundos) con el que se realiza un sondeo en un servidor SNTP para obtener información de difusión única. De forma predeterminada, el intervalo de sondeo es de 1.024 segundos.

Receive Broadcast Servers Updates (Recibir actualizaciones de servidores de difusión): se escucha los servidores SNTP para obtener información de hora del servidor de difusión en las interfaces seleccionadas.

Receive Anycast Servers Updates (Recibir actualizaciones de servidores de cualquier difusión): se realiza un sondeo del servidor SNTP para obtener información de hora del servidor de cualquier difusión. Si los campos **Receive Anycast Servers Update** (Recibir actualizaciones de servidores de cualquier difusión) y **Receive Broadcast Servers Update** (Recibir actualizaciones de servidores de difusión) están activados, la hora del sistema se establecerá de acuerdo con la información de hora del servidor de cualquier difusión.

Receive Unicast Servers Updates (Recibir actualizaciones de servidores de difusión única): se realiza un sondeo del servidor SNTP para obtener información de hora del servidor de difusión única. Si los campos **Receive Broadcast Servers Updates** (Recibir actualizaciones de servidores de difusión), **Receive Anycast Servers Updates** (Recibir actualizaciones de servidores de cualquier difusión) y **Receive Unicast Servers Updates** (Recibir actualizaciones de servidores de difusión única) están activados, la hora del sistema se configurará de acuerdo con la información de hora del servidor de difusión única.

Send Unicast Requests (Enviar peticiones de difusión única): se envían peticiones de información de hora del servidor de difusión única SNTP al servidor SNTP.

Selección de una fuente del reloj

1. Abra la página **Time Synchronization** (Sincronización de la hora).
2. Defina el campo **Clock Source** (Fuente del reloj).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona la fuente del reloj y se actualiza el dispositivo.

Configuración del reloj local

1. Abra la página **Time Synchronization** (Sincronización de la hora).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se aplica la configuración del reloj local.

Definición de los parámetros globales de SNTP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **SNTP Global Settings** (Configuración global de SNTP).

Tabla 6-9. Comandos de la CLI para los parámetros globales de SNTP

Comando de la CLI	Descripción
sntp broadcast client enable	Activa los clientes de difusión SNTP.
sntp anycast client enable	Activa los clientes de cualquier difusión SNTP.
sntp unicast client enable	Activa los clientes de difusión única SNTP predefinidos.

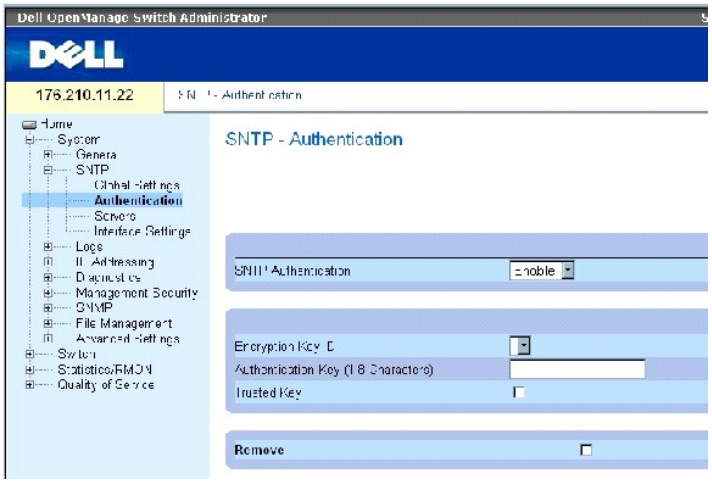
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# sntp
anycast client enable
```

Definición de los métodos de autenticación de SNTP

La página SNTP Authentication (Autenticación de SNTP) permite activar la autenticación de SNTP entre el dispositivo y el servidor SNTP. En la página SNTP Authentication (Autenticación de SNTP) también se puede seleccionar el método con el que se va a autenticar el servidor SNTP. Haga clic en **System** (Sistema) → **SNTP**→ **Authentication** (Autenticación) en la vista de árbol para abrir la página SNTP Authentication (Autenticación de SNTP).

Figura 6-9. SNTP Authentication



La página SNTP Authentication (Autenticación de SNTP) contiene los campos siguientes:

SNTP Authentication (Autenticación de SNTP): permite autenticar una sesión SNTP entre el dispositivo y un servidor SNTP.

Encryption Key ID (ID de clave de cifrado): define la identificación de clave utilizada para autenticar el servidor SNTP y el dispositivo. El valor máximo de este campo es 4294967295.

Authentication Key (1-8 Characters) (Clave de autenticación [1-8 caracteres]): clave utilizada para la autenticación.

Trusted Key (Clave de confianza): indica la clave de cifrado utilizada (difusión única) para autenticar el servidor SNTP.

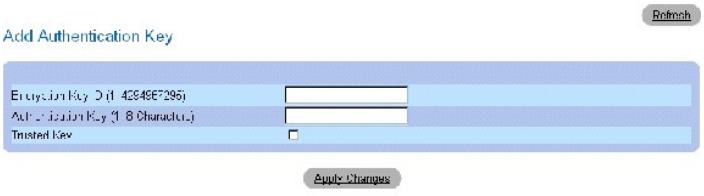
Remove (Eliminar): elimina las claves de autenticación seleccionadas.

Adición de una clave de autenticación de SNTP

1. Abra la página **SNTP Authentication** (Autenticación de SNTP).
2. Haga clic en **Add** (Añadir).

Se abre la página siguiente:

Figura 6-10. Add Authentication Key



3. Defina los campos.
4. Haga clic en Apply Changes (Aplicar cambios).

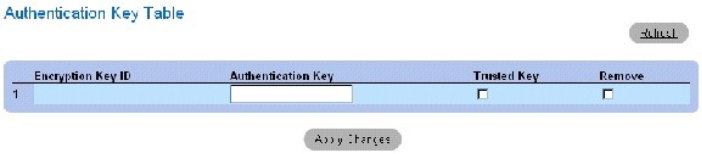
Se añade la clave de autenticación de SNTP y se actualiza el dispositivo.

Visualización de la tabla de claves de autenticación

1. Abra la página **SNTP Authentication** (Autenticación de SNTP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Authentication Key Table** (Tabla de claves de autenticación).

Figura 6-11. Authentication Key Table



Eliminación de la clave de autenticación

1. Abra la página **SNTP Authentication** (Autenticación de SNTP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Authentication Key Table** (Tabla de claves de autenticación).

3. Seleccione una entrada de la tabla de claves de autenticación.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada y se actualiza el dispositivo.

Definición de la configuración de la autenticación de SNTP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **SNTP Authentication** (Autenticación de SNTP).

Tabla 6-10. Comandos de la CLI para la autenticación de SNTP

Comando de la CLI	Descripción
sntp authenticate	Define la autenticación para el tráfico SNTP recibido de los servidores.
sntp trusted key	Autentica la identidad de un sistema con el que SNTP se sincronizará.
sntp authentication-key *número* md5 *valor*	Define una clave de autenticación para SNTP.

A continuación se muestra un ejemplo de los comandos de la CLI:

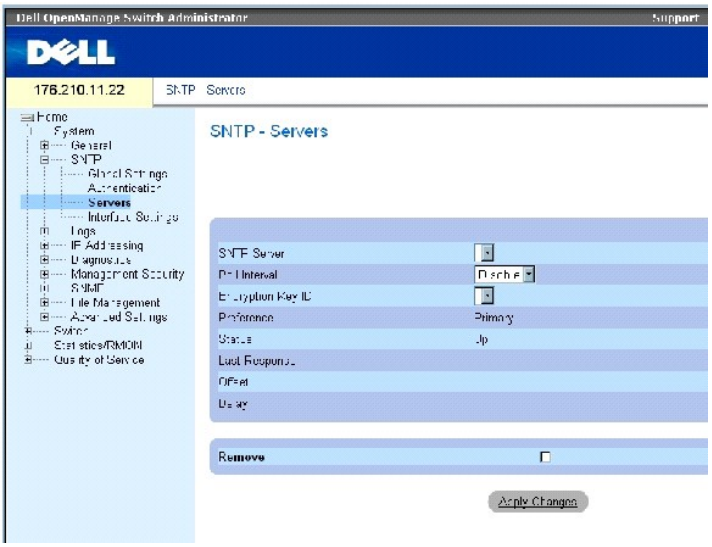
```
console(config)# sntp
authentication-key 8 md5
Calked


console(config)# sntp
trusted-key 8
```

```
Console(config)# sntp
authenticate
```

Definición de servidores SNTP

En la página **SNTP Servers** (Servidores SNTP) es posible activar servidores SNTP y añadir servidores SNTP nuevos. *Para abrir la página* **SNTP Servers** (Servidores SNTP), haga clic en **System** (Sistema)→ **SNTP**→ **Servers** (Servidores) en la vista de árbol.

Figura 6-12. SNTP Servers



La página **SNTP Servers** **(Servidores SNTP) contiene los campos siguientes:**

SNTP Server (Servidor SNTP): seleccione una dirección IP de servidor SNTP definida por el usuario. Se puede definir un máximo de ocho servidores.

Poll Interval (Intervalo de sondeo): activa el sondeo en el servidor SNTP seleccionado para obtener información de hora del sistema.

Encryption Key ID (ID de clave de cifrado): indica la identificación de clave utilizada para la comunicación entre el servidor SNTP y el dispositivo. El intervalo de valores posibles es 1-4294967295.

Preference (Preferencia): servidor SNTP que proporciona información sobre la hora del sistema SNTP. Los valores del campo posibles son:

Primary (Principal): el servidor principal proporciona la información sobre SNTP.

Secondary (Secundario): el servidor de reserva proporciona la información sobre SNTP.

Status (Estado): estado del servidor SNTP operativo. Los valores del campo posibles son:

Up (Activado): el servidor SNTP funciona con normalidad.

Down (Desactivado): un servidor SNTP no se encuentra disponible actualmente. Por ejemplo, el servidor SNTP no está conectado o está desactivado.

In progress (En curso): el servidor SNTP está enviando o recibiendo información sobre SNTP.

Unknown (Desconocido): se desconoce el progreso de la información sobre SNTP que se está enviando. Por ejemplo, el dispositivo está buscando una interfaz.

Last Response (Última respuesta): última vez que se ha recibido una respuesta del servidor SNTP.

Offset (Diferencia): diferencia entre la hora indicada por el reloj local del dispositivo y la hora obtenida del servidor SNTP.

Delay (Demora): tiempo que se tarda en alcanzar el servidor SNTP.

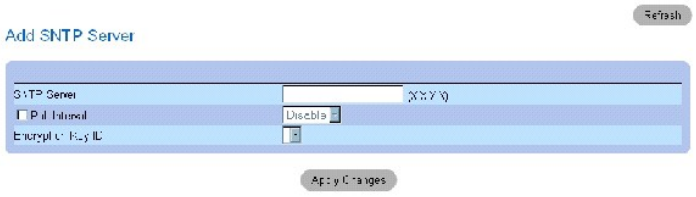
Remove (Eliminar): elimina un servidor SNTP específico de la lista de servidores SNTP.

Adición de un servidor SNTP

1. Abra la página **SNTP Servers** (Servidores SNTP).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add SNTP Server** (Añadir servidor SNTP):

Figura 6-13. Add SNTP Server



3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade el servidor SNTP y se actualiza el dispositivo.

Visualización de la tabla de servidores SNTP

1. Abra la página **SNTP Servers** (Servidores SNTP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **SNTP Servers Table** (Tabla de servidores SNTP):

Figura 6-14. SNTP Servers Table

Modificación de un servidor SNTP

1. Abra la página **SNTP Servers** (Servidores SNTP).
2. Haga clic en **Show All** (Mostrar todo).

   Se abre la página **SNTP Servers Table** (Tabla de servidores SNTP).
3. Seleccione una entrada de servidor SNTP.
4. Modifique los campos pertinentes.
5. Haga clic en **Apply Changes** (Aplicar cambios).

   Se actualiza la información de servidor SNTP.

Eliminación de un servidor SNTP

1. Abra la página **SNTP Servers** (Servidores SNTP).
2. Haga clic en **Show All** (Mostrar todo).

   Se abre la página **SNTP Servers Table** (Tabla de servidores SNTP).
3. Seleccione una entrada de servidor SNTP.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

   Se elimina la entrada y se actualiza el dispositivo.

Definición de la configuración de servidores SNTP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **SNTP Servers** (Servidores SNTP).

Tabla 6-11. Comandos de la CLI para los servidores SNTP

Comando de la CLI	Descripción
sntp server dirección-ip|nombrehost [poll] [key idclave]	Configura el dispositivo de modo que utilice SNTP para solicitar y aceptar tráfico SNTP desde un servidor.

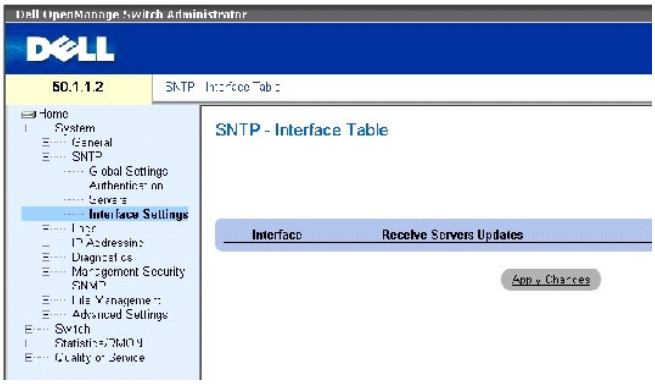
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config)# sntp
server 100.1.1.1 poll key
10
```

Definición de interfaces SNTP

La página **SNTP Interface Settings** (Configuración de interfaces SNTP) contiene información sobre las interfaces SNTP. Para abrir la página **SNTP Interface Settings** (Configuración de interfaces SNTP), haga clic en System (Sistema)→ **SNTP**→ Interface Settings (Configuración de interfaces).

Figura 6-15. SNTP Interface Settings



La página **SNTP Interface Settings** (Configuración de interfaces SNTP) contiene los campos siguientes:

Unit No. (Nº de unidad): indica el miembro de apilamiento en el que se activa la interfaz SNTP.

Interface (Interfaz): contiene una lista de interfaces en las que se puede activar SNTP.

Receive Servers Updates (Recibir actualizaciones de servidores): activa o desactiva SNTP en una interfaz determinada.

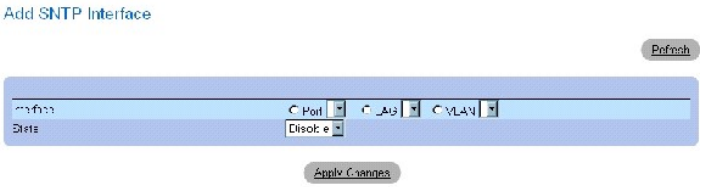
Remove (Eliminar): elimina SNTP de una interfaz determinada.

Adición de una interfaz SNTP

1. Abra la página **SNTP Interface Settings** (Configuración de interfaces SNTP).
2. Haga clic en **Add** (Añadir).

   Se abre la página **Add SNTP Interface** (Añadir interfaz SNTP).

Figura 6-16. Add SNTP Interface



3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se añade la interfaz SNTP y se actualiza el dispositivo.

Definición de la configuración de las interfaces SNTP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **SNTP Interface Settings** (Configuración de interfaces SNTP).

NOTA: para poder definir una interfaz como de cualquier difusión o de difusión, dicha interfaz debe tener definida una dirección IP.

Tabla 6-12. Comandos de la CLI para la configuración de las interfaces SNTP

Comando de la CLI	Descripción
sntp client enable	Activa el cliente SNTP en una interfaz.
show sntp configuration	Muestra la configuración de SNTP.

A continuación se muestra un ejemplo de los comandos de la CLI para visualizar interfaces SNTP:

```
console# show sntp configuration

Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server                          Polling     Encryption Key
------------                    --------    ---------------
176.1.1.8                       Enabled     9
176.1.8.179                     Disabled    Disabled

Broadcast Clients: Enabled

Broadcast Clients Poll: Enabled

Broadcast Interfaces:1/e1, 1/e3
```

Administración de registros

La página **Logs** (Registros) contiene enlaces a diferentes páginas de registro. Para abrir la página **Logs** (Registros), haga clic en System (Sistema)→ Logs (Registros) en la vista de árbol.

Definición de los parámetros globales de registros

Los registros del sistema permiten ver los eventos del dispositivo en tiempo real y registrar los eventos para un uso posterior. Los registros del sistema registran y administran eventos, y notifican errores o mensajes informativos.

Los mensajes sobre eventos tienen un formato único, igual que el formato de mensajes del protocolo de registros del sistema (Syslog) recomendado para la notificación de errores. Por ejemplo, los mensajes Syslog y los mensajes de notificación del dispositivo local tienen asignado un código de gravedad e incluyen una mnemotecnia de mensaje que identifica la aplicación que genera el mensaje. Esto permite filtrar mensajes en función de su urgencia o relevancia. La distribución de mensajes de registro a varios destinos, como por ejemplo el búfer de registro, el archivo de registro o el servidor Syslog, se controla mediante los parámetros de configuración de Syslog. Los usuarios pueden definir un máximo de ocho servidores Syslog.

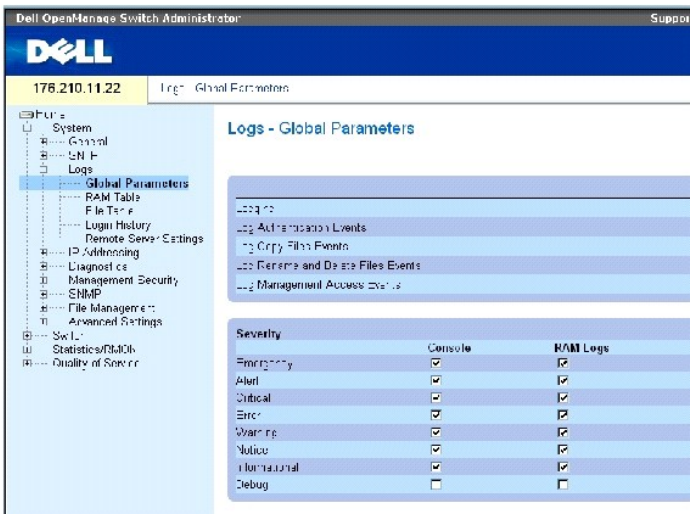
En la tabla siguiente se muestran los niveles de gravedad de los registros:

Tabla 6-13. Niveles de gravedad de los registros

Tipo de gravedad	Nivel de gravedad	Descripción
Emergencia	0	El sistema no funciona.
Alerta	1	El sistema requiere atención inmediata.
Grave	2	El sistema se encuentra en estado grave.
Error	3	Se ha producido un error en el sistema.
Advertencia	4	Se ha producido una advertencia en el sistema.
Aviso	5	El sistema funciona bien, pero se ha producido un aviso en el sistema.
Informativo	6	Proporciona información sobre el dispositivo.
Depuración	7	Proporciona información detallada sobre el registro. Si se produce un error de depuración, póngase en contacto con el servicio de asistencia técnica en línea de Dell.

La página Global Log Parameters (Parámetros globales de registros) contiene campos para definir qué eventos se registrarán y en qué registros. Algunos de estos campos permiten activar registros globalmente, y otros sirven para definir parámetros de los registros. Los mensajes de registro de gravedad se enumeran de mayor a menor gravedad. Para abrir la página Global Log Parameters (Parámetros globales de registros), haga clic en System (Sistema)→ Logs (Registros)→ Global Parameters (Parámetros globales) en la vista de árbol.

Figura 6-17. Global Log Parameters



La página Global Log Parameters (Parámetros globales de registros) contiene los parámetros siguientes:

Logging (Registro): activa los registros globales del dispositivo para registros de caché, de archivo y de servidor. Los registros de consola están activados de forma predeterminada.

Log Authentication Events (Registrar eventos de autenticación): activa la generación de registros cuando se autentica a los usuarios.

Log Copy Files Events (Registrar eventos de copia de archivos): activa la generación de registros cuando se copian archivos.

Log Rename and Delete Files Events (Registrar eventos de cambio de nombre y eliminación de archivos): activa la generación de registros cuando se cambia el nombre de un archivo de configuración de copia de seguridad o cuando se elimina.

Log Management Access Events (Registrar eventos de acceso de administración): activa la generación de registros cuando se accede al dispositivo mediante un método de administración. Por ejemplo, cada vez que se accede al dispositivo mediante SSH, se genera un registro de dispositivo.

Severity (Gravedad): a continuación se muestran los registros de gravedad disponibles:

Emergency (Emergencia): indica el nivel más alto de advertencia. Si el dispositivo está inactivo o no funciona correctamente, se guarda un mensaje de registro de emergencia en la ubicación de registro especificada.

Alert (Alerta): indica el segundo nivel más alto de advertencia. Un registro de alerta se guarda si se produce un fallo grave en el dispositivo, por ejemplo, si se intenta descargar un archivo de configuración que no existe.

Critical (Grave): indica el tercer nivel más alto de advertencia. Un registro grave se guarda cuando ocurre un fallo grave en el dispositivo, por ejemplo, si dos puertos del dispositivo no funcionan mientras los demás puertos del dispositivo sí funcionan.

Error: indica que se ha producido un error en el dispositivo, por ejemplo, una operación de copia no se ha llevado a cabo correctamente.

Warning (Advertencia): indica el nivel más bajo de advertencia en un dispositivo. Por ejemplo, el dispositivo funciona, pero un enlace de puerto está inactivo.

Notice (Aviso): proporciona información importante sobre el dispositivo.

Informational (Informativo): proporciona información sobre el dispositivo. Por ejemplo, un puerto se encuentra activo.

Debug (Depuración): proporciona mensajes sobre depuración.

NOTA: cuando se selecciona un nivel de gravedad, todas las alternativas de nivel de gravedad por encima de la selección se seleccionan automáticamente.

La página **Global Log Parameters** (Parámetros globales de registros) también contiene casillas de verificación que corresponden a un sistema de registro diferente:

Console (Consola): indica el nivel de gravedad mínimo a partir del que se envían registros a la consola.

RAM Logs (Registros de RAM): indica el nivel de gravedad mínimo a partir del que se envían registros al archivo de registro que se guarda en la RAM (caché).

Log File (Archivo de registro): indica el nivel de gravedad mínimo a partir del que se envían registros al archivo de registro que se guarda en la memoria Flash.

Activación de registros:

1. Abra la página **Global Log Parameters** (Parámetros globales de registros).
2. Seleccione **Enable** (Activar) en la lista desplegable de **Logging** (Registro).
3. Seleccione el tipo de registro y la gravedad del registro en las casillas de verificación de la página **Global Log Parameters** (Parámetros globales de registros).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de registros y se actualiza el dispositivo.

Activación de registros mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Global Log Parameters** (Parámetros globales de registros).

Tabla 6-14. Comandos de la CLI para los parámetros globales de registros

Comando de la CLI	Descripción
logging on	Activa el registro de mensajes de error.
logging {dirección-ip | nombrehost} [port puerto] [severity nivel] [facility función] [description texto]	Registra mensajes en un servidor Syslog. Para ver una lista de los niveles de gravedad, consulte "Niveles de gravedad de los registros".
logging console nivel	Limita los mensajes registrados en la consola en función de la gravedad.
logging buffered nivel	Limita los mensajes Syslog que se muestran desde un búfer interno (RAM) en función de la gravedad.
logging file nivel	Limita los mensajes Syslog que se envían al archivo de registro en función de la gravedad.
clear logging	Borra los registros.
clear logging file	Borra los mensajes del archivo de registro.

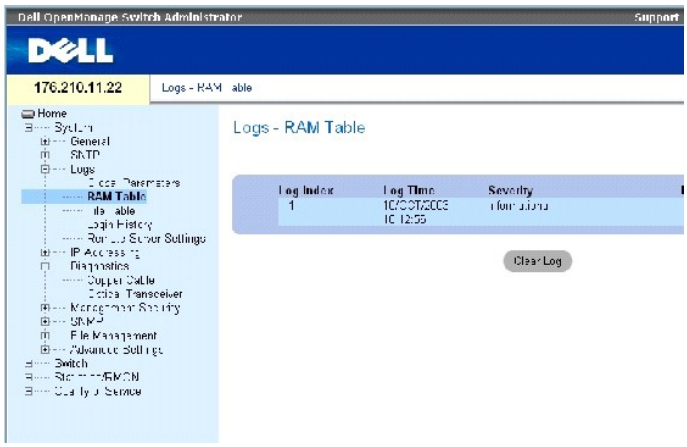
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# logging
on

console(config)# logging
console errors

console(config)# logging
buffered debugging

console(config)# logging
file alerts

console(config)# end

console# clear logging
file

Clear Logging File [y/n]y
```

Visualización de la tabla de registros de RAM

La página **RAM Log Table** (Tabla de registros de RAM) contiene información sobre las entradas de registro almacenadas en la RAM, como la hora de introducción del registro, la gravedad del registro y una descripción del registro. Para abrir la página **RAM Log Table** (Tabla de registros de RAM), haga clic en System (Sistema) → Logs (Registros) → RAM Table (Tabla de RAM) en la vista de árbol.

Figura 6-18. RAM Log Table



La página **RAM Log Table** (Tabla de registros de RAM) contiene los campos siguientes:

Log Index (Índice de registro): indica el número de registro en la tabla de registros de RAM.

Log Time (Hora de registro): indica la hora de introducción del registro en la tabla de registros de RAM.

Severity (Gravedad): indica la gravedad del registro.

Description (Descripción): describe la entrada del registro.

Eliminación de información de registro:

1. Abra la página **RAM Log Table** (Tabla de registros de RAM).
2. Haga clic en Clear Log (Borrar registro).

Se elimina la información de registro de la tabla de registros de RAM y se actualiza el dispositivo.

Visualización y borrado de la tabla de registros de RAM mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver y borrar los campos de la página **RAM Log Table** (Tabla de registros de RAM).

Tabla 6-15. Comandos de la CLI para la tabla de registros de RAM

Comando de la CLI	Descripción
show logging	Muestra el estado de los registros y los mensajes Syslog almacenados en el búfer interno.
clear logging	Borra los registros.

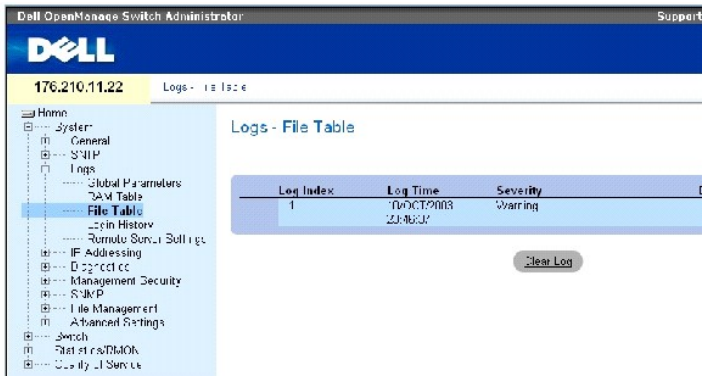
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show logging


Logging is enabled.


Console Logging: Level
info. Console Messages: 0
Dropped.


Buffer Logging: Level
info. Buffer Messages: 26
Logged, 26 Displayed, 200
Max.


File Logging: Level error.
File Messages: 157 Logged,
26 Dropped.


1 messages were not logged


01-Jan-2000 01:03:42 :%
INIT-I-Startup: Cold
Startup


01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e14


01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e13


01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e12


01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e15


01-Jan-2000 01:01:32 :%
INIT-I-InitCompleted:
Initialization task is
completed




console# clear logging


Clear Logging Buffer
[y/n]?
```

Visualización de la tabla de archivos de registro

La página Log File Table (Tabla de archivos de registro) contiene información sobre las entradas de registro almacenadas en el archivo de registros de la memoria Flash, como la hora de introducción del registro, la gravedad del registro y una descripción del mensaje de registro. Para abrir la página Log File Table (Tabla de archivos de registro), haga clic en System (Sistema) → Logs (Registros) → File Table (Tabla de archivos) en la vista de árbol.

Figura 6-19. Log File Table



La página Log File Table (Tabla de archivos de registro) contiene los campos siguientes:

Log Index (Índice de registro): indica el número de registro en la tabla de archivos de registro.

Log Time (Hora de registro): indica la hora de introducción del registro en la tabla de archivos de registro.

Severity (Gravedad): indica la gravedad del registro.

Description (Descripción): muestra el texto del mensaje de registro.

Visualización de la tabla de archivos de registro mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver y configurar los campos de la página Log File Table (Tabla de archivos de registro).

Tabla 6-16. Comandos de la CLI para la tabla de archivos de registro

Comando de la CLI	Descripción
show logging file	Muestra el estado de los registros y los mensajes Syslog almacenados en el archivo de registro.
clear logging file<	Borra los mensajes del archivo de registro.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show logging
file


Logging is enabled.


Console Logging:
Level info. Console
Messages: 0 Dropped.


Buffer Logging: Level
```

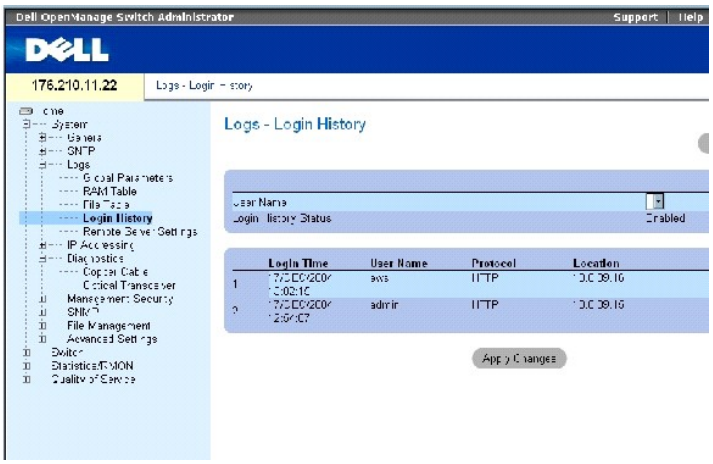
```
info. Buffer
Messages: 62 Logged,
62 Displayed, 200
Max.



File Logging: Level
debug. File Messages:
11 Logged, 51
Dropped.



SysLog server
12.1.1.2 Logging:
warning. Messages: 14
Dropped.



SysLog server 1.1.1.1
Logging: info.
Messages: 0 Dropped.



01-Jan-2000
01:12:01 :%COPY-W-
TRAP: The copy
operation was
completed
successfully



01-Jan-2000
01:11:49 :%LINK-I-Up:
1/e11



01-Jan-2000
01:11:46 :%LINK-I-Up:
1/e12



01-Jan-2000
01:11:42 :%LINK-W-
Down: 1/e13



01-Jan-2000
01:11:35 :%LINK-I-Up:
1/e14
```

Visualización del historial de conexión del dispositivo

La página **Login History** (Historial de conexión) contiene información para visualizar y supervisar la utilización del dispositivo, como por ejemplo la hora a la que el usuario ha iniciado una sesión y el protocolo utilizado para la conexión.

Para abrir la página **Login History** (Historial de conexión), haga clic en System (Sistema) → Logs (Registros) → Login History (Historial de conexión) en la vista de árbol.

Figura 6-20. Login History



La página **Login History** (Historial de conexión) contiene los campos siguientes:

User Name (Nombre de usuario): contiene una lista de nombres de usuario del dispositivo definidos por el usuario.

Login History Status (Estado de historial de conexión): indica si se han activado los registros de historial de contraseñas en el dispositivo.

Login Time (Hora de conexión): indica la hora a la que el usuario seleccionado ha iniciado una sesión en el dispositivo.

User Name (Nombre de usuario): indica el usuario que ha iniciado una sesión en el dispositivo.

Protocol (Protocolo): indica el medio por el cual el usuario ha iniciado una sesión en el dispositivo.

Location (Ubicación): indica la dirección IP de la estación desde la que se ha accedido al dispositivo.

Visualización del historial de conexión

1. Abra la página **Login History** (Historial de conexión).
2. Seleccione un usuario en el campo **User Name** (Nombre de usuario).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Aparece la información de conexión del usuario seleccionado.

Visualización del historial de conexión del dispositivo mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver y configurar los campos de la página **Login History** (Historial de conexión).

Tabla 6-17. Comandos de la CLI para el historial de conexión del dispositivo

Comando de la CLI	Descripción
show users login-history	Muestra información sobre el historial de administración de contraseñas.

A continuación se muestra un ejemplo de los comandos de la CLI:

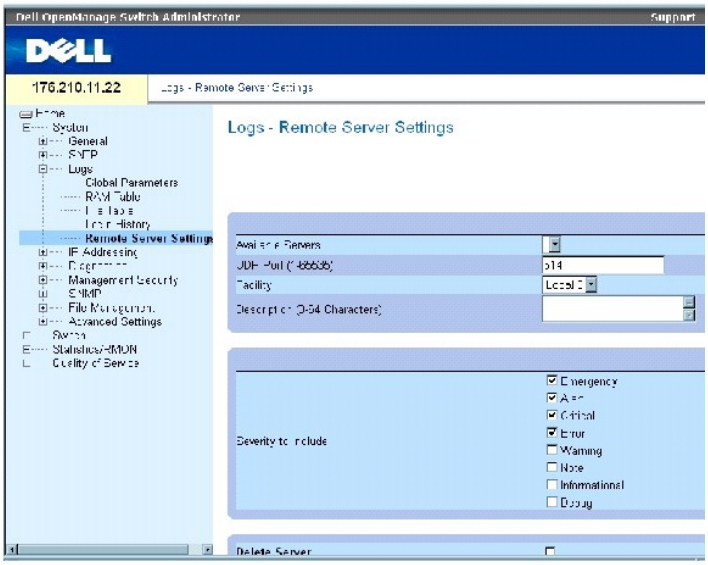
```
console# show users login-history
```

Login Time	Username	Protocol	Location
----------	--------	--------	----------
Jan 1. 2005 23:58:17	Anna	HTTP	172.16.1.8
Jan 1. 2005 07:59:23	Errol	HTTP	172.16.0.8
Jan 1. 2005 08:23:48	Amy	Serial	
Jan 1. 2005 08:29:29	Alan	SSH	172.16.0.8
Jan 1. 2005 08:42:31	Bob	HTTP	172.16.0.1
Jan 1. 2005 08:49:52	Cindy	Telnet	172.16.1.7

Modificación de las definiciones de servidores remotos de registros

La página **Remote Log Server Settings** (Configuración de servidores remotos de registros) contiene campos para ver y configurar los servidores de registros disponibles. Además, es posible definir nuevos servidores de registros y enviar la gravedad del registro a cada servidor. Para abrir la página **Remote Log Server Settings** (Configuración de servidores remotos de registros), haga clic en System (Sistema) → Logs (Registros) → Remote Server Settings (Configuración de servidores remotos) en la vista de árbol.

Figura 6-21. Remote Log Server Settings



La página **Remote Log Server Settings** (Configuración de servidores remotos de registros) contiene los campos siguientes:

Available Servers (Servidores disponibles): contiene una lista de los servidores a los que es posible enviar registros.

UDP Port (1-65535) (Puerto UDP [1-65535]): indica el puerto UDP al que se envían los registros para el servidor seleccionado. El intervalo de valores posibles es 1-65535. El valor predeterminado es 514.

Facility (Función): aplicación definida por el usuario desde la cual se envían los registros del sistema al servidor remoto. Sólo se puede asignar una función por servidor. Si se asigna un segundo nivel de función, éste sobrescribirá el primer nivel. Todas las aplicaciones definidas para un dispositivio utilizan la misma función en un servidor. El valor predeterminado de este campo es Local 7. Los valores posibles son:

Local 0-Local 7

Description (0-64 Characters) (Descripción [0-64 caracteres]): descripción del servidor definida por el usuario.

Delete Server (Eliminar servidor): elimina el servidor seleccionado de la lista de servidores disponibles.

La página **Remote Log Server Settings** (Configuración de servidores remotos de registros) también contiene una lista de niveles de gravedad. Las definiciones de gravedad son las mismas que las de la página **Global Log Parameters** (Parámetros globales de registros).

Envío de registros a un servidor:

1. Abra la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).
2. Seleccione un servidor en la lista desplegable de **Available Servers** (Servidores disponibles).
3. Defina los campos.
4. Seleccione la gravedad del registro en las casillas de verificación de **Severity to Include** (Gravedad que debe incluirse).
5. Haga clic en **Apply Changes** (Aplicar cambios).

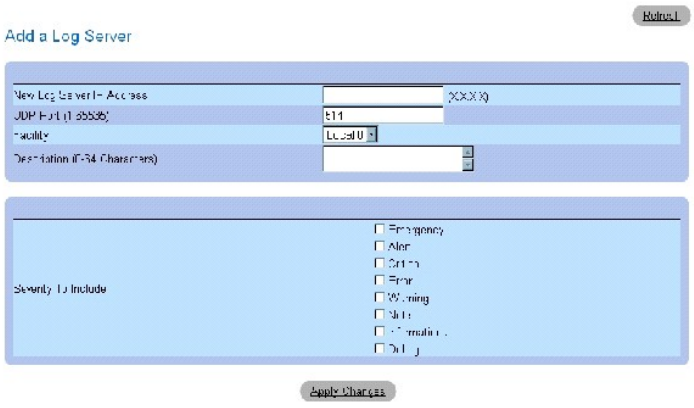
Se guarda la configuración de registros y se actualiza el dispositivo.

Definición de un servidor nuevo:

1. Abra la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add a Log Server** (Añadir servidor de registros):

Figura 6-22. Add a Log Server



La página **Add a Log Server** (Añadir servidor de registros) contiene el campo adicional siguiente:

New Log Server IP Address (Dirección IP del nuevo servidor de registros): define la dirección IP del nuevo servidor de registros.

3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define el servidor y se añade a la lista de servidores disponibles.

Visualización de la página Log Servers Table (Tabla de servidores de registros):

1. Abra la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Log Servers Table** (Tabla de servidores de registros):

Figura 6-23. Log Servers Table

Eliminación de un servidor de registros de la página Log Servers Table (Tabla de servidores de registros):

1. Abra la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Log Servers Table** (Tabla de servidores de registros).

3. Seleccione una entrada en la página **Log Servers Table** (Tabla de servidores de registros).
4. Seleccione la casilla de verificación **Remove** (Eliminar) para eliminar el servidor o los servidores.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la página **Log Servers Table** (Tabla de servidores de registro) y se actualiza el dispositivo.

Operaciones con los registros de servidores remotos mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para realizar operaciones con servidores remotos de registros.

Tabla 6-18. Comandos de la CLI para servidores remotos de registros

Comando de la CLI	Descripción
logging *(dirección-ip* **|** *nombrehost}* **[port** *puerto*] [**severity** *nivel*] [**facility** *función*] [**description** *texto*]	Registra mensajes en un servidor remoto.
no logging	Elimina un servidor Syslog.
show logging	Visualiza el estado de los registros y los mensajes Syslog.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console> enable

console# configure

console(config) # logging
10.1.1.1 severity critical

console(config)# end

console# show logging

Logging is enabled.

Console Logging: Level
debug. Console Messages: 5
Dropped.

Buffer Logging: Level
debug. Buffer Messages: 16
Logged, 16 Displayed, 200
Max.

File Logging: Level error.
File Messages: 0 Logged,
209 Dropped.

SysLog server 31.1.1.2
Logging: error. Messages:
22 Dropped.

SysLog server 5.2.2.2
Logging: info. Messages: 0
Dropped.

SysLog server 10.2.2.2
Logging: critical.
Messages: 21 Dropped.

SysLog server 10.1.1.1
Logging: critical.
Messages: 0 Dropped.

1 messages were not logged

03-Mar-2004 12:02:03 :%
LINK-I-Up: 1/e11

03-Mar-2004 12:02:01 :%
LINK-W-Down: 1/e12
```

```
03-Mar-2004 12:02:01 :%
LINK-I-Up: 1/e13
```

Definición del direccionamiento IP

La página IP Addressing (Direccionamiento IP) contiene enlaces para asignar direcciones IP de puerta de enlace predeterminada y de interfaz, y para definir parámetros ARP y DHCP para las interfaces. Para abrir la página IP Addressing (Direccionamiento IP), haga clic en System (Sistema) → IP Addressing (Direccionamiento IP) en la vista de árbol.

Definición de puertas de enlace predeterminadas

La página **Default Gateway** (Puerta de enlace predeterminada) contiene campos para asignar puertas de enlace a dispositivos. Los paquetes se reenvían a la IP predeterminada cuando se envían los paquetes a una red remota. La dirección IP configurada debe pertenecer a la misma subred de dirección IP de una de las interfaces IP. Para abrir la página **Default Gateway** (Puerta de enlace predeterminada), haga clic en System (Sistema) → IP Addressing (Direccionamiento IP) → Default Gateway (Puerta de enlace predeterminada) en la vista de árbol.

La página **Default Gateway** (Puerta de enlace predeterminada) contiene los campos siguientes:

User Defined (Definida por el usuario): dirección IP de la puerta de enlace del dispositivo.

Active (Activa): indica si la puerta de enlace está activa.

Remove User Defined (Eliminar definida por el usuario): elimina la puerta de enlace del dispositivo de la lista desplegable de **Default Gateway** (Puerta de enlace predeterminada).

Selección de la puerta de enlace de un dispositivo:

1. Abra la página **Default Gateway** (Puerta de enlace predeterminada).
2. Seleccione una dirección IP en la lista desplegable de **Default Gateway** (Puerta de enlace predeterminada).
3. Seleccione la casilla de verificación **Active** (Activa).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona la puerta de enlace predeterminada del dispositivo y se actualiza el dispositivo.

Eliminación de la puerta de enlace predeterminada de un dispositivo:

1. Abra la página **Default Gateway** (Puerta de enlace predeterminada).
2. Seleccione la casilla de verificación **Remove** (Eliminar) para eliminar las puertas de enlace predeterminadas.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de puerta de enlace predeterminada y se actualiza el dispositivo.

Definición de la puerta de enlace de un dispositivo mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Default Gateway** (Puerta de enlace predeterminada).

.

Tabla 6-19. Comandos de la CLI para la puerta de enlace predeterminada

Comando de la CLI	Descripción
ip default-gateway dirección-ip	Define una puerta de enlace predeterminada.
no ip default-gateway	Elimina una puerta de enlace predeterminada.

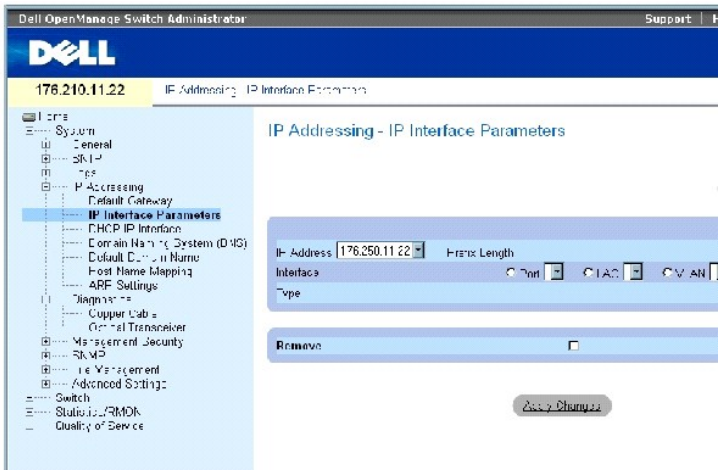
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# ip
default-gateway
196.210.10.1



console(config)# no ip
default-gateway
```

Definición de interfaces IP

La página IP Interfaces Parameters (Parámetros de interfaces IP) contiene campos para asignar parámetros de IP a interfaces. Para abrir la página IP Interfaces Parameters (Parámetros de interfaces IP), haga clic en **System** (Sistema) → **IP Addressing** (Direccionamiento IP) → **IP Interface Parameters** (Parámetros de interfaces IP) en la vista de árbol.

Figura 6-24. IP Interfaces Parameters



La página IP Interfaces Parameters (Parámetros de interfaces IP) contiene los parámetros siguientes:

IP Address (Dirección IP): dirección IP de la interfaz.

Prefix Length (Longitud de prefijo): número de bits que componen el prefijo de la dirección IP de origen o la máscara de red de la dirección IP de origen.

Source Interface (Interfaz de origen): tipo de interfaz para la que se define la dirección IP. Seleccione **Port** (Puerto), **LAG** o **VLAN**.

Type (Tipo): indica si la dirección IP se ha configurado de forma estática o no.

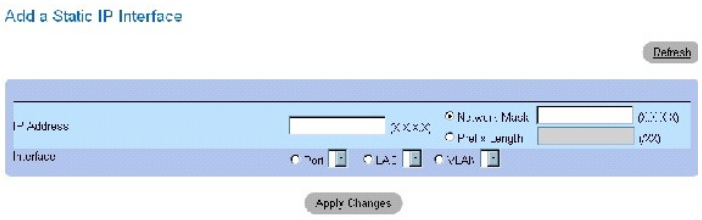
Remove (Eliminar): elimina la interfaz del menú desplegable **IP Address** (Dirección IP).

Adición de una interfaz IP

1. Abra la página IP Interfaces Parameters (Parámetros de interfaces IP).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add a Static IP Interface** (Añadir dirección IP estática):

Figura 6-25. Add a Static IP Interface



Network Mask (Máscara de red): indica la máscara de subred de la dirección IP de origen.

3. Complete los campos de la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade la nueva dirección IP a la interfaz y se actualiza el dispositivo.

Modificación de los parámetros de direcciones IP

1. Abra la página IP Interfaces Parameters (Parámetros de interfaces IP).
2. Seleccione una dirección IP en el menú desplegable **IPAddress** (Dirección IP).
3. Modifique el tipo de interfaz.
4. Haga clic en **Apply Changes** (Aplicar cambios).

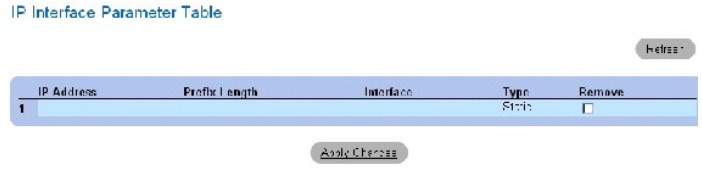
Se modifican los parámetros y se actualiza el dispositivo.

Eliminación de direcciones IP

1. Abra la página IP Interfaces Parameters (Parámetros de interfaces IP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **IP Interface Parameters Table** (Tabla de parámetros de interfaces IP).

Figura 6-26. IP Interface Parameter Table



3. Seleccione una dirección IP y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la dirección IP seleccionada y se actualiza el dispositivo.

Definición de interfaces IP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página IP Interfaces Parameters (Parámetros de interfaces IP).

Tabla 6-20. Comandos de la CLI para los parámetros de interfaces IP

Comando de la CLI	Descripción
ip address dirección-ip {máscara | longitud-prefijo}	Establece una dirección IP.
no ip address [dirección-ip]	Elimina una dirección IP.
show ip interface [ethernet número-interfaz | vlan id-vlan | port-channel número]	Muestra el estado de uso de las interfaces configuradas para IP.

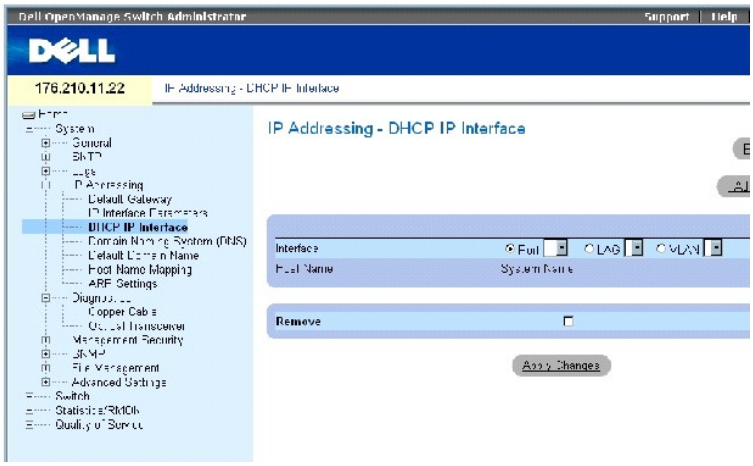
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface
vlan 1

console(config-if)# ip
address 92.168.1.123
255.255.255.0

console(config-if)# no ip
address 92.168.1.123

console(config-if)# end

console# show ip interface
vlan 1

Gateway IP Address
Activity status

---------------------- ----
--------------

192.168.1.1 Active

IP address Interface Type

------------------- ------
------ ------------------

192.168.1.123/24 VLAN 1
Static
```

Definición de los parámetros de interfaces IP DHCP

La página **DHCP IP Interface** (Interfaz IP DHCP) contiene parámetros para definir clientes DHCP conectados al dispositivo. Para abrir la página **DHCP IP Interface (Interfaz IP DHCP),** haga clic en **System** (Sistema) → **IP Addressing** (Direccionamiento IP) → **DHCP IP Interface** (Interfaz IP DHCP) en la vista de árbol.

Figura 6-27. DHCP IP Interface



La página **DHCP IP Interface** (Interfaz IP DHCP) contiene los campos siguientes:

Interface (Interfaz): interfaz específica conectada al dispositivo. Haga clic en el botón de opción que aparece junto a **Port** (Puerto), **LAG** o **VLAN** y seleccione la interfaz conectada al dispositivo.

Host Name (Nombre de host): indica el nombre del host.

Remove (Eliminar): elimina los clientes DHCP.

Adición de clientes DHCP

1. Abra la página DHCP IP Interface (Interfaz IP DHCP).
2. Haga clic en **Add** (Añadir).

   Se abre la página **Add DHCP IP Interface** (Añadir interfaz IP DHCP).
3. Complete la información de la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se añade la interfaz DHCP y se actualiza el dispositivo.

Modificación de una interfaz IP DHCP

1. Abra la página DHCP IP Interface (Interfaz IP DHCP).
2. Modifique los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la entrada y se actualiza el dispositivo.

Eliminación de una interfaz IP DHCP

1. Abra la página DHCP IP Interface (Interfaz IP DHCP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **DHCP Client Table** (Tabla de clientes DHCP).

3. Seleccione una entrada de cliente DHCP.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada seleccionada y se actualiza el dispositivo.

Definición de interfaces IP DHCP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir clientes DHCP.

Tabla 6-21. Comandos de la CLI para interfaces IP DHCP

Comando de la CLI	Descripción
ip address dhcp [**hostname** *nombre-host*]	Permite adquirir una dirección IP en una interfaz Ethernet a partir del protocolo de configuración dinámica de host (DHCP).

A continuación se muestra un ejemplo de los comandos de la CLI:

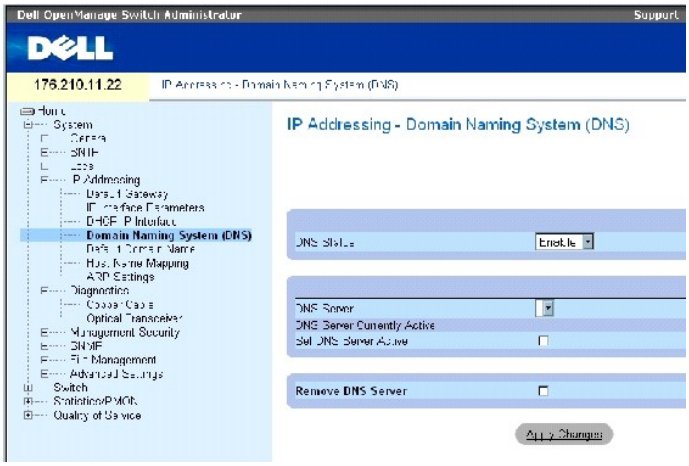
```
console(config)# interface
ethernet 1/e11

console(config-if)# ip
address dhcp
```

Configuración de sistemas de nombres de dominio

El sistema de nombres de dominio (DNS) convierte los nombres de dominio definidos por el usuario en direcciones IP. Cada vez que se asigna un nombre de dominio, el servicio DNS convierte el nombre en una dirección IP numérica. Por ejemplo, www.ipejemplo.com se convierte en 192.87.56.2. Los servidores DNS mantienen las bases de datos de nombres de dominio y las direcciones IP correspondientes.

La página **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]) contiene campos para habilitar y activar servidores DNS específicos. Para abrir la página **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]), haga clic en **System** (Sistema) → **IP Addressing** (Direccionamiento IP) → **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]) en la vista de árbol.

Figura 6-28. Domain Naming System (DNS)



La página **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]) contiene los campos siguientes:

DNS Status (Estado de DNS): activa o desactiva la conversión de nombres DNS en direcciones IP.

DNS Server (Servidor DNS): contiene una lista de servidores DNS. Los servidores DNS se añaden en la página **Add DNS Server** (Añadir servidor DNS).

DNS Server Currently Active (Servidor DNS activo actualmente): indica el servidor que está activo actualmente.

Set DNS Server Active (Activar servidor DNS): activa el servidor DNS seleccionado.

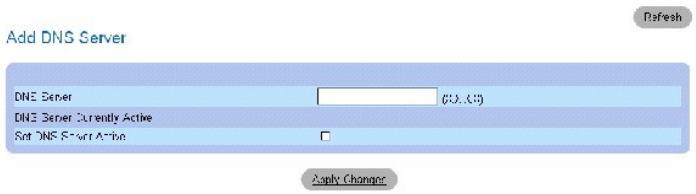
Remove DNS Server (Eliminar servidor DNS): elimina el servidor DNS seleccionado.

Adición de un servidor DNS

1. Abra la página **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add DNS Server** (Añadir servidor DNS):

Figura 6-29. Add DNS Server



DNS Server (Servidor DNS): dirección IP del servidor DNS.

3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

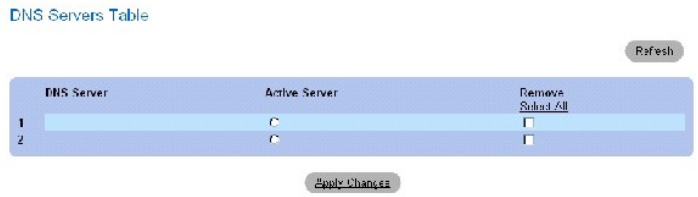
Se define el nuevo servidor DNS y se actualiza el dispositivo.

Visualización de la tabla de servidores DNS

1. Abra la página **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **DNS Server Table** (Tabla de servidores DNS):

Figura 6-30. DNS Server Table



Eliminación de servidores DNS

1. Abra la página **Domain Naming System (DNS)** (Sistema de nombres de dominio [DNS]).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **DNS Server Table** (Tabla de servidores DNS).

3. Seleccione una entrada de la tabla de servidores DNS.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el servidor DNS seleccionado y se actualiza el dispositivo.

Configuración de los servidores DNS mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI que se utilizan para configurar los servidores DNS.

Tabla 6-22. Comandos de la CLI para los servidores DNS

Comando de la CLI	Descripción
ip name-server *dirección-servidor*	Establece los servidores de nombres disponibles. Se puede definir un máximo de ocho servidores de nombres.
no ip name-server *dirección-servidor*	Elimina un servidor de nombres.
ip domain-name *nombre*	Define el nombre de dominio predeterminado que el software utiliza para completar los nombres de host incompletos.
clear host {nombre | *}	Elimina las entradas de la caché de nombre a dirección de host.
show hosts [*nombre*]	Muestra el nombre de dominio predeterminado, una lista de los hosts servidores de nombres, y la lista estática y almacenada en la caché de nombres de host y direcciones.
ip domain-lookup	Activa el sistema DNS para convertir nombres de host en direcciones IP.

A continuación se muestra un ejemplo de los comandos de la CLI:

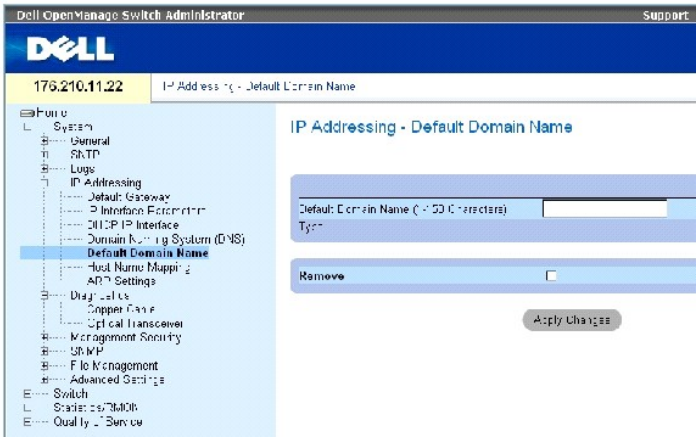
```
console(config)# ip name-
```

```
server 176.16.1.18
```

Definición de dominios predeterminados

La página **Default Domain Name** (Nombre de dominio predeterminado) contiene información para definir nombres de dominio DNS predeterminados. Para abrir la página **Default Domain Name** (Nombre de dominio predeterminado), haga clic en **System** (Sistema) → **IP Addressing** (Direccionamiento IP) → **Default Domain Name** (Nombre de dominio predeterminado).

Figura 6-31. Default Domain Name



La página **Default Domain Name** (Nombre de dominio predeterminado) contiene los campos siguientes:

Default Domain Name (1-158 characters) (Nombre de dominio predeterminado [1-158 caracteres]): nombre de dominio predeterminado definido por el usuario. Una vez definido, el nombre de dominio predeterminado se aplica a todos los nombres de host incompletos.

Type (Tipo): tipo de dirección IP. Los valores del campo posibles son:

Dynamic (Dinámica): la dirección IP se crea de forma dinámica.

Static (Estática): la dirección IP es estática.

Remove (Eliminar): elimina el nombre de dominio predeterminado.

Definición de nombres de dominio DNS mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI que se utilizan para configurar los nombres de dominio DNS.

Tabla 6-23. Comandos de la CLI para los nombres de dominio DNS

Comando de la CLI	Descripción
ip domain-name nombre	Define el nombre de dominio predeterminado que el software utiliza para completar los nombres de host incompletos.
no ip domain-name	Desactiva el uso del sistema de nombres de dominio (DNS).
show hosts [*nombre***]**	Muestra el nombre de dominio predeterminado, una lista de los hosts servidores de nombres, y la lista estática y almacenada en la caché de nombres de host y direcciones.

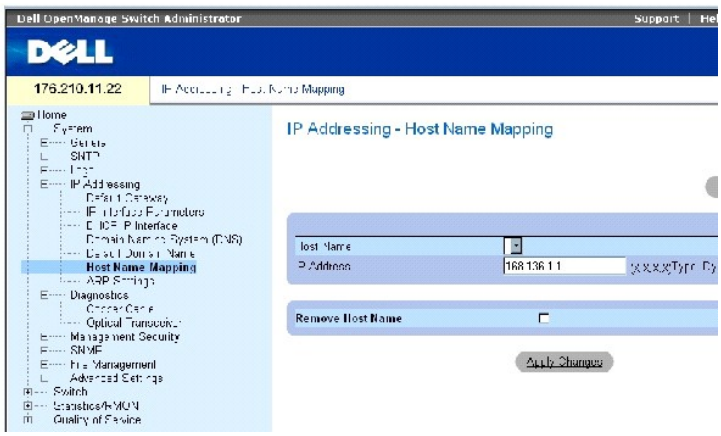
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# ip
domain-name dell.com
```

Asignación de hosts de dominio

La página Host Name Mapping (Asignación de hosts de dominio) contiene parámetros para asignar direcciones IP a nombres de host estáticos. En esta página, se puede asignar una dirección IP por host. Para abrir la página **Host Name Mapping** (Asignación de nombres de host), *haga clic en* **System** (Sistema) → **IP Addressing** (Direccionamiento IP) → **Host Name Mapping (Asignación de nombres de host) en la vista de árbol.**

Figura 6-32. Host Name Mapping



La página Host Name Mapping (Asignación de nombres de host) contiene los campos siguientes:

Host Name (Nombre de host): contiene una lista de nombres de host. Los nombres de host se definen en la página **Add Host Name Mapping** (Añadir asignación de nombres de host). Cada host proporciona una dirección IP.

IP Address (X.X.X.X) (Dirección IP [X.X.X.X]): proporciona una dirección IP que se asigna al nombre de host especificado.

Type (Tipo): tipo de dirección IP. Los valores del campo posibles son:

Dynamic (Dinámica): la dirección IP se crea de forma dinámica.

Static (Estática): la dirección IP es estática.

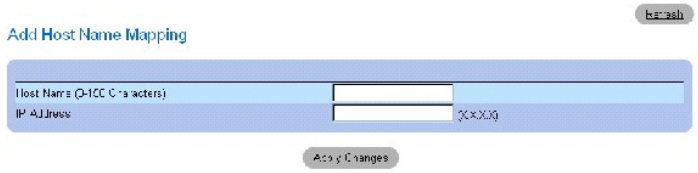
Remove Host Name (Eliminar nombre de host): elimina la asignación de host de DNS.

Adición de nombres de dominios de host

1. Abra la página Host Name Mapping (Asignación de nombres de host).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add Host Name Mapping** (Añadir asignación de nombres de host):

Figura 6-33. Add Host Name Mapping



3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

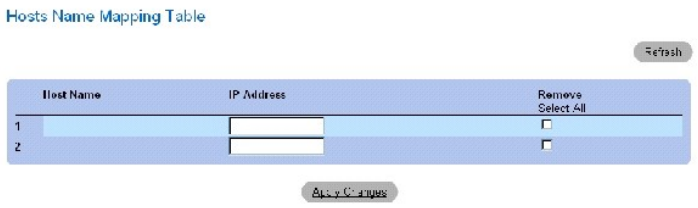
Se asigna la dirección IP al nombre de host y se actualiza el dispositivo.

Visualización de la tabla de asignación de nombres de host

1. Abra la página Host Name Mapping (Asignación de nombres de host).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Hosts Name Mapping Table** (Tabla de asignación de nombres de host):

Figura 6-34. Hosts Name Mapping Table



Eliminación de nombres de host de la asignación de direcciones IP

1. Abra la página Host Name Mapping (Asignación de nombres de host).
2. Haga clic en **Show All** (Mostrar todo).
3. Se abre la página **Host Name Mapping Table** (Tabla de asignación de nombres de host).
4. **Seleccione una entrada de la tabla de asignación de nombres de host.**
5. Seleccione la casilla de verificación **Remove** (Eliminar).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la tabla de asignación de nombres host y se actualiza el dispositivo.

Asignación de direcciones IP a nombres de host de dominio mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para asignar nombres de host de dominio a direcciones IP.

Tabla 6-24. Comandos de la CLI para los nombres de host de dominio

Comando de la CLI	Descripción
ip host *nombre dirección*	Define la asignación estática de nombre a dirección de host en la caché del host.
no ip host nombre	Elimina la asignación de nombre a dirección.
clear host {nombre | *}	Elimina las entradas de la caché de nombre a dirección de host.
show hosts [nombre]	Muestra el nombre de dominio predeterminado, una lista de los hosts servidores de nombres, y la lista estática y almacenada en la caché de nombres de host y direcciones.

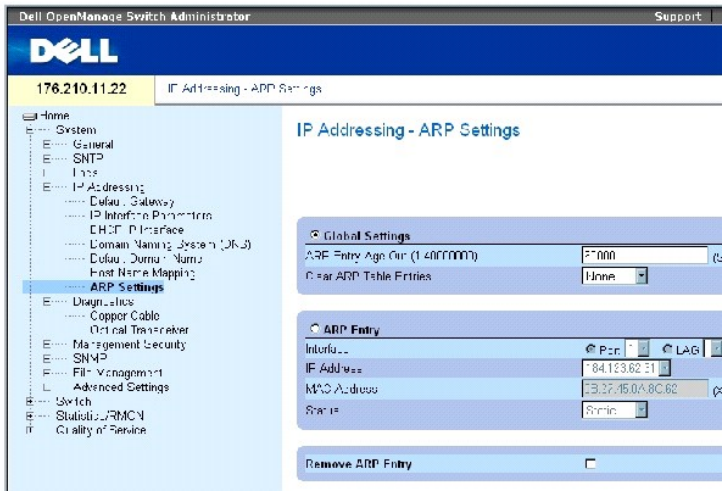
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

Definición de la configuración de ARP

El protocolo de resolución de direcciones (ARP) convierte direcciones IP en direcciones físicas y asigna la dirección IP a una dirección MAC. ARP permite a un host comunicarse con otros hosts sólo cuando se conoce la dirección IP de sus hosts adyacentes. Para abrir la página **ARP Settings** **(Configuración de ARP)**, haga clic en System (Sistema) → IP Addressing (Direccionamiento IP) → ARP en la vista de árbol.

Figura 6-35. ARP Settings



La página **ARP Settings** (Configuración de ARP) contiene los campos siguientes:

Global Settings (Configuración global): seleccione esta opción para activar los campos para la configuración global de ARP.

ARP Entry Age Out (1-40000000) (Caducidad de entrada de ARP [1-40000000]): para todos los dispositivos, indica el tiempo (en segundos) que transcurre entre las peticiones de ARP relativas a una entrada de la tabla de ARP. Después de este periodo, la entrada se elimina de la tabla. El intervalo es 1-40000000. El valor predeterminado es 60000 segundos.

Clear ARP Table Entries (Borrar entradas de la tabla de ARP): indica el tipo de entradas de ARP que se borran en todos los dispositivos. Los valores posibles son:

None (Ninguna): no se borra ninguna entrada de ARP.

All (Todas): se borran todas las entradas de ARP.

Dynamic (Dinámica): sólo se borran las entradas de ARP dinámicas.

Static (Estática): sólo se borran las entradas de ARP estáticas.

ARP Entry (Entrada de ARP): seleccione esta opción para activar los campos para la configuración de ARP en un dispositivo Ethernet.

Interface (Interfaz). número de interfaz del puerto, LAG o VLAN que se conecta al dispositivo.

IP Address (Dirección IP): dirección IP de la estación, que se asocia con la dirección MAC especificada a continuación.

MAC Address (Dirección MAC): dirección MAC de la estación, que se asocia en la tabla de ARP con la dirección IP.

Status (Estado): estado de la entrada de la tabla de ARP. Los valores del campo posibles son:

Dynamic (Dinámica): la entrada de ARP se obtiene de forma dinámica.

Static (Estática): la entrada de ARP es una entrada estática.

Remove ARP Entry (Eliminar entrada de ARP): elimina una entrada de ARP.

Adición de una entrada de tabla de ARP estática:

1. Abra la página **ARP Settings** (Configuración de ARP).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add ARP Entry** (Añadir entrada de ARP).

3. Seleccione una interfaz.
4. Defina los campos.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade la entrada de la tabla de ARP y se actualiza el dispositivo.

Visualización de la tabla de ARP

1. Abra la página **ARP Settings** (Configuración de ARP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **ARP Table** (Tabla de ARP).

Eliminación de una entrada de la tabla de ARP

1. Abra la página **ARP Settings** (Configuración de ARP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **ARP Table** (Tabla de ARP).

3. Seleccione una entrada de la tabla.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada seleccionada de la tabla de ARP y se actualiza el dispositivo.

Configuración de ARP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **ARP Settings** (Configuración de ARP).

Tabla 6-25. Comandos de la CLI para la configuración de ARP

Comando de la CLI	Descripción
arp dir_ip dir_hw {ethernet número-interfaz | vlan id-vlan | port-channel número}	Añade una entrada permanente en la caché de ARP.
arp timeout segundos	Establece el tiempo durante el que una entrada permanece en la caché de ARP.
clear arp-cache<	Elimina todas las entradas dinámicas de la caché de ARP.
show arp	Muestra las entradas de la tabla de ARP.
no arp	Elimina una entrada de ARP de la tabla de ARP.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

Ejecución de los diagnósticos de cables

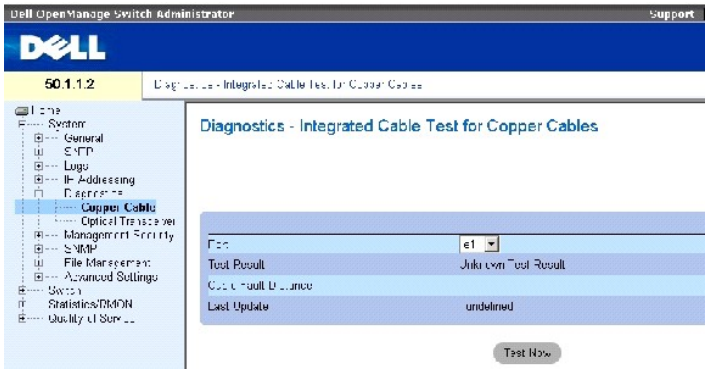
La página **Diagnostics** (Diagnóstico) contiene enlaces a páginas que permiten realizar pruebas virtuales de cables en cables de cobre. Para abrir la página **Diagnostics** (Diagnósticos), haga clic en **System** (Sistema) → **Diagnostics** (Diagnósticos) en la vista de árbol.

Visualización de los diagnósticos de cables de cobre

La página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre) contiene campos para realizar pruebas en los cables de cobre. La comprobación de los cables proporciona información sobre dónde se han producido errores en el cable, la última vez que se ha realizado una prueba del cable y el tipo de error que se ha producido en el cable. Las pruebas utilizan la tecnología de reflectometría en el dominio temporal (TDR) para probar la calidad y las características de un cable de cobre conectado a un puerto. Pueden comprobarse cables de hasta 120 metros de longitud. La comprobación de cables se realiza cuando los puertos se encuentran inactivos, salvo la prueba de longitud aproximada del cable.

Para abrir la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre), haga clic en **System** (Sistema) → **Diagnostics** (Diagnósticos) → **Copper Cable** (Cable de cobre) en la vista de árbol.

Figura 6-36. Integrated Cable Test for Copper Cables



La página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre) contiene los campos siguientes:

Port (Puerto): puerto al que está conectado el cable.

Test Result (Resultado de la prueba): resultados de la prueba de cables. Los valores del campo posibles son:

- **No Cable** (No hay cable): no hay ningún cable conectado al puerto.
- **Open Cable** (Circuito abierto): el cable está conectado sólo a un extremo.
- **Short Cable** (Cortocircuito): se ha producido un cortocircuito en el cable.
- **OK** (Correcto): el cable ha superado la prueba.

Cable Fault Distance (Distancia del error del cable): distancia respecto al puerto donde se ha producido el error del cable.

Last Update (Última actualización): última vez que se ha realizado la comprobación del puerto.

Approximate Cable Length (Longitud aproximada del cable): indica la longitud aproximada del cable. Esta prueba sólo puede realizarse cuando el puerto está activo y funciona a 1 Gbps.

Realización de una prueba de cable

1. Asegúrese de que ambos extremos del cable de cobre están conectados a un dispositivo.
2. Abra la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre).
3. Seleccione la interfaz que desee comprobar.
4. Haga clic en **Test Now** (Probar ahora).

Se lleva a cabo la prueba del cable de cobre y se muestran los resultados en la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre).

Visualización de la tabla de resultados de la prueba virtual del cable

1. Abra la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Integrated Cable Test Results Table** (Tabla de resultados de la comprobación integrada de cables).

NOTA: en esta pantalla se muestran los resultados de las pruebas que se han ejecutado anteriormente, -pero no se lleva a cabo la prueba en todos los puertos en este momento.

Además de los campos de la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre), la página **Integrated Cable Test Results Table** (Tabla de resultados de la comprobación integrada de cables) contiene el campo siguiente:

Unit No (Nº de unidad): número de la unidad cuyo cable se visualiza.

Realización de pruebas de los cables de cobre mediante los comandos de la CLI

En la tabla siguiente se muestran los comandos de la CLI que se utilizan para comprobar los cables de cobre.

Tabla 6-26. Comandos de la CLI para la comprobación de cables de cobre

Comando de la CLI	Descripción
test copper-port tdr *interfaz*	Lleva a cabo pruebas virtuales de cables (VCT).
show copper-port tdr *interfaz*	Muestra los resultados de las últimas pruebas VCT en los puertos.
show copper-port cable-length *interfaz*	Muestra la longitud aproximada del cable de cobre conectado a un puerto.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console> enable

Console# test copper-port
tdr 1/e3

Cable is open at 100
meters.

Console# show copper-port
cable-length
```

Port	Length (meters)
----	---------------
1/e3	110-140
1/e4	Fiber

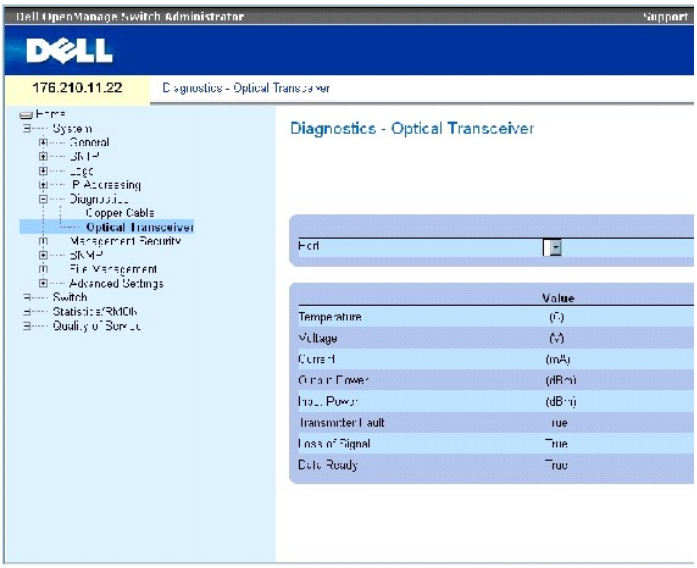
NOTA: la longitud del cable indicada por la herramienta de comprobación integrada de cables (ICT) es una aproximación en intervalos de hasta 50 metros, 50-80 m, 80-110 m, 110-120 m o más de 120 m. La desviación puede ser de un máximo de 20 metros, y la medida de la longitud del cable no funciona para los enlaces a 10 Mbps.

Visualización de los diagnósticos de transceptor óptico

Utilice la página Optical Transceiver (Transceptor óptico) para realizar comprobaciones de los cables de fibra óptica. Para abrir la página Optical Transceiver (Transceptor óptico), haga clic en **System** (Sistema) → **Diagnostics** (Diagnósticos) → **Optical Transceiver** (Transceptor óptico) en la vista de árbol.

NOTA: los diagnósticos de transceptor óptico sólo pueden realizarse cuando el enlace está presente.

Figura 6-37. Optical Transceiver



La página Optical Transceiver (Transceptor óptico) contiene los campos siguientes:

Port (Puerto): dirección IP del puerto en el que se comprueba el cable.

Temperature (Temperatura): temperatura (en Celsius) de funcionamiento del cable.

Voltage (Voltaje): voltaje de funcionamiento del cable.

Current (Corriente): corriente de funcionamiento del cable.

Output Power (Potencia de salida): nivel al que se transmite la potencia de salida.

Input Power (Potencia de entrada): nivel al que se transmite la potencia de entrada.

Transmitter Fault (Fallo del transmisor): indica que se ha producido un fallo durante la transmisión.

Loss of Signal (Pérdida de señal): indica si se ha producido una pérdida de señal en el cable.

Data Ready (Datos preparados): el transceptor óptico se ha encendido y los datos están preparados.

Visualización de la tabla de resultados de la prueba de diagnósticos de transceptor óptico

1. Abra la página Optical Transceiver (Transceptor óptico).
2. Haga clic en **Show All** (Mostrar todo).

Se ejecuta la prueba y se abre la página **Optical Transceiver Diagnostics Table** (Tabla de diagnósticos de transceptor óptico).

Además de los campos de la página **Optical Transceiver** (Transceptor óptico), la tabla de diagnósticos de transceptor óptico contiene el campo siguiente:

Unit No (Nº de unidad): número de la unidad cuyo cable se visualiza.

- N/A (No disponible), N/S (No compatible), W (Advertencia) y E (Error).

NOTA: los transceptores Finisar no admiten la comprobación de diagnósticos de fallo del transmisor.

NOTA: la función de análisis de fibra óptica sólo funciona en SFP compatibles con el estándar de--diagnósticos digitales SFF 872.

Realización de pruebas de los cables de fibra óptica mediante los comandos de la CLI

En la tabla siguiente se muestra el comando de la CLI que se utiliza para comprobar los cables de fibra óptica.

Tabla 6-27. Comandos de la CLI para la comprobación de cables de fibra óptica

Comando de la CLI	Descripción
show fiber-ports optical- transceiver [*interfaz*] [*detailed*]	Muestra los diagnósticos del transceptor óptico.

A continuación se muestra un ejemplo de los comandos de la CLI:

Console# show fiber-ports optical-transceiver detailed

Port	Temp [C]	Voltage	Current [Volt]	Output [mA]	Input [mWatt]	POWER TX [mWatt]	LOS Fault
----	----	------	-----	------	------	------	-----

1/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

Administración de la seguridad del conmutador

La página **Management Security** (Seguridad de administración) proporciona acceso a páginas de seguridad que contienen campos para configurar los parámetros de seguridad para puertos, métodos de administración de dispositivos, usuarios y servidores. Para abrir la página **Management Security** (Seguridad de administración), haga clic en System (Sistema) → Management Security (Seguridad de administración) en la vista de árbol.

Definición de perfiles de acceso

La página **Access Profiles** (Perfiles de acceso) contiene campos para definir perfiles y reglas de acceso al dispositivo. El acceso a las funciones de administración se puede limitar a grupos de usuarios, los cuales se definen mediante interfaces de entrada y direcciones IP de origen o submáscaras IP de origen.

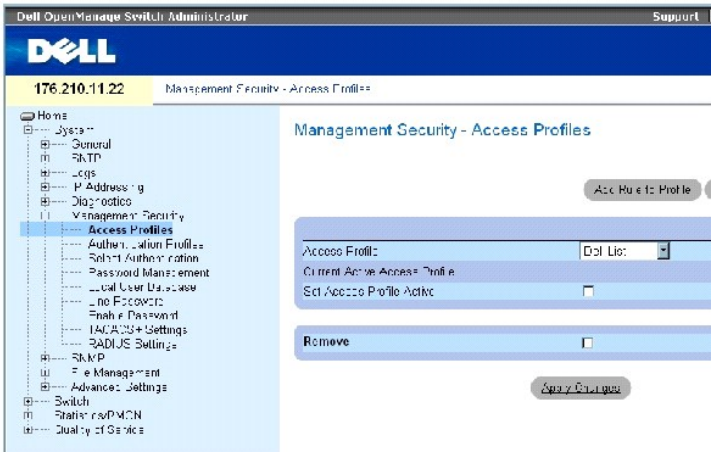
El acceso a la administración puede definirse por separado para cada tipo de método de acceso a la administración, incluidos el acceso Web (HTTP), Web seguro (HTTPS), Telnet y Telnet seguro.

El acceso a diferentes métodos de administración puede variar según el grupo de usuarios. Por ejemplo, el grupo de usuarios 1 puede acceder al dispositivo sólo a través de una sesión HTTPS, mientras que el grupo de usuarios 2 puede acceder al dispositivo a través de sesiones HTTPS y Telnet.

Las listas de acceso a la administración contiene un máximo de 256 regals que determinan qué usuarios pueden administrar el dispositivo y qué métodos pueden utilizar para ello. También es posible bloquear el acceso de los usuarios al dispositivo.

La página **Access Profiles** (Perfiles de acceso) contiene campos para configurar listas de administración y aplicarlas a interfaces determinadas. Para abrir la página **Access Profiles** (Perfiles de acceso), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) → **Access Profiles** (Perfiles de acceso) en la vista de árbol.

Figura 6-38. Access Profiles



La página **Access Profiles** (Perfiles de acceso) contiene los campos siguientes:

Access Profile (Perfil de acceso): contiene listas de perfiles de acceso definidas por el usuario. La lista de perfiles de acceso incluye el valor predeterminado **Console Only** (Sólo consola). Cuando se selecciona este perfil de acceso, la administración activa del dispositivo se lleva a cabo únicamente mediante la conexión de la consola.

Current Active Access Profile (Perfil de acceso activo actual): perfil de acceso que está activo actualmente.

Set Access Profile Active (Activar perfil de acceso): activa un perfil de acceso.

Remove (Eliminar): elimina un perfil de acceso de la lista de nombres de perfil de acceso.

Activación de un perfil

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Seleccione un perfil de acceso en el campo **Access Profile** (Perfil de acceso).
3. Seleccione la casilla de verificación **Set Access Profile Active** (Activar perfil de acceso).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se activa el perfil de acceso.

Adición de un perfil de acceso

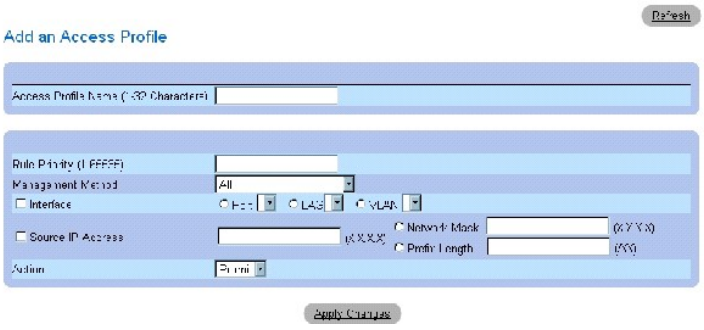
Las reglas actúan como filtros para determinar las prioridades de las reglas, el método de administración de dispositivos, el tipo de interfaz, la dirección IP y la máscara de red de origen, así como la acción de acceso a la administración de dispositivos. Es posible bloquear o permitir el acceso de los usuarios a la administración. La prioridad de las reglas determina el orden en el que se implementan.

Definición de reglas para un perfil de acceso

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Haga clic en **Add Profile** (Añadir perfil).

Se abre la página **Add an Access Profile** (Añadir perfil de acceso):

Figura 6-39. Add an Access Profile



La página Add an Access Profile (Añadir perfil de acceso) contiene los campos adicionales siguientes:

Access Profile Name (1-32 Characters) (Nombre de perfil de acceso [1-32 caracteres]): nombre del perfil de acceso definido por el usuario. El nombre del perfil de acceso puede contener un máximo de 32 caracteres.

Rule Priority (1-65535) (Prioridad de la regla [1-65535]): indica la prioridad de la regla. Cuando el paquete coincide con una regla, se otorga o se deniega a los grupos de usuarios el acceso a la administración del dispositivo. El orden de las reglas se establece mediante la definición de una prioridad de regla en este campo. El número de regla es básico para que los paquetes coincidan con las reglas, puesto que los paquetes coinciden con la primera regla a la que se ajustan. Las prioridades de las reglas pueden verse en la tabla de reglas del perfil.

Management Method (Método de administración): método de administración para el que se define el perfil de acceso. Los usuarios con este perfil de acceso pueden acceder o no al dispositivo mediante el método de administración seleccionado (línea).

Interface (Interfaz): tipo de interfaz a la que se aplica la regla. Este campo es opcional. Esta regla puede aplicarse a un puerto, LAG o VLAN seleccionados marcando la casilla de verificación y seleccionando el botón de opción y la interfaz adecuados.

NOTA: si se asigna un perfil de acceso a una interfaz, se deniega el acceso a través de otras interfaces. Si no se asigna ningún perfil de acceso a ninguna interfaz, se podrá acceder al dispositivo desde todas las interfaces.

Source IP Address (X.X.X.X) (Dirección IP de origen [X.X.X.X]): dirección IP de origen de la interfaz a la que se aplica la regla. Este campo es opcional e indica que la regla es válida para una subred.

Network Mask (X.X.X.X) (Network Mask [X.X.X.X]): máscara de subred IP.

Prefix Length (Longitud de prefijo): número de bits que componen el prefijo de la dirección IP de origen o la máscara de red de la dirección IP de origen.

Action (Acción): define si se debe permitir o denegar el acceso de administración a la interfaz definida.

3. Defina el campo **Access Profile Name** (Nombre de perfil de acceso).
4. Defina los campos pertinentes.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade el nuevo perfil de acceso y se actualiza el dispositivo.

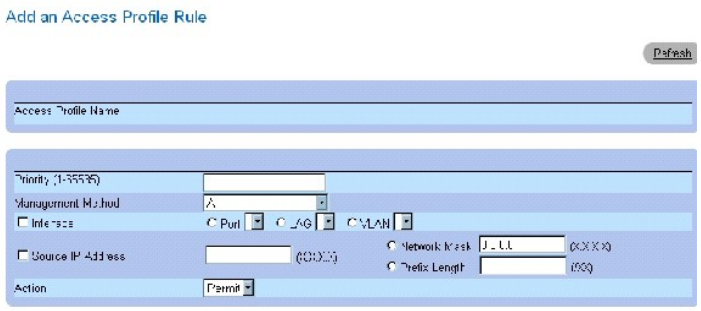
Adición de reglas al perfil de acceso

NOTA: la primera regla debe estar definida para empezar a hacer coincidir el tráfico con los perfiles de acceso.

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Haga clic en **Add Rule to Profile** (Añadir regla a perfil).

Se abre la página **Add an Access Profile Rule** (Añadir regla de perfil de acceso):

Figura 6-40. Add an Access Profile Rule



3. Complete los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade la regla al perfil de acceso y se actualiza el dispositivo.

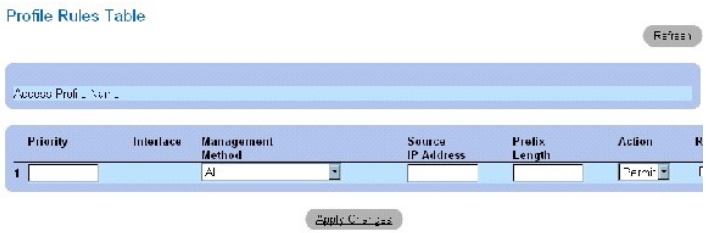
Visualización de la tabla de reglas del perfil

NOTA: el orden en el que aparecen las reglas en la tabla de reglas del perfil es importante. Los paquetes se corresponden con la primera regla que cumple los criterios de ésta.

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Profile Rules Table (Tabla de reglas del perfil)**:

Figura 6-41. Profile Rules Table



Eliminación de una regla

1. Abra la página **Access Profiles** *(Perfiles de acceso)*.
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Profile Rules Table** (Tabla de reglas del perfil).

3. Seleccione una regla.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la regla seleccionada y se actualiza el dispositivo.

Definición de perfiles de acceso mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página Access Profiles (Perfiles de acceso).

Tabla 6-28. Comandos de la CLI para los perfiles de acceso

Comando de la CLI	Descripción
management access-list nombre	Define una lista de acceso a la administración e introduce el contexto de la lista de acceso para la configuración.
permit [ethernet número-interfaz | vlan id-vlan | port-channel número] [service servicio]	Establece condiciones de generación de permisos de puerto para la lista de acceso a la administración.
permit ip-source dirección-ip [mask máscara | longitud-prefijo] [ethernet número-interfaz | vlan id-vlan | port-channel número] [service servicio]	Establece condiciones de generación de permisos de puerto para la lista de acceso a la administración y el método de administración seleccionado.
deny [ethernet número-interfaz | vlan id-vlan | port-channel número] [service servicio]	Establece condiciones de denegación de puerto para la lista de acceso a la administración y el método de administración seleccionado.
deny ip-source dirección-ip [mask máscara | longitud-prefijo] [ethernet número-interfaz | vlan id-vlan | port-channel número] [service servicio]	Establece condiciones de denegación de puerto para la lista de acceso a la administración y el método de administración seleccionado.
management access-class {console-only | nombre}	Define qué lista de acceso se utiliza como conexiones de administración activas.
show management access-list [nombre]	Muestra las listas de acceso a la administración activas.
show management access-class	Muestra información sobre la clase de acceso a la administración.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)#
management access-list
mlist



console(config-macl)#
permit ethernet 1/e1



console(config-macl)#
permit ethernet 1/e2



console(config-macl)# deny
ethernet 1/e3



console(config-macl)# deny
ethernet 1/e4



console(config-macl)# exit



console(config)#
management access-class
mlist



console(config)# exit



console# show management
access-list



mlist



-----



permit ethernet 1/e1



permit ethernet 1/e2



deny ethernet 1/e3



deny ethernet 1/e4



! (Note: all other access
implicitly denied)



Console# show management
access-class



Management access-class is
enabled, using access list
mlist
```

Definición de perfiles de autenticación

La página Authentication Profiles (Perfiles de autenticación) contiene campos para seleccionar el método de autenticación de usuarios en el dispositivo. La autenticación del usuario ocurre:

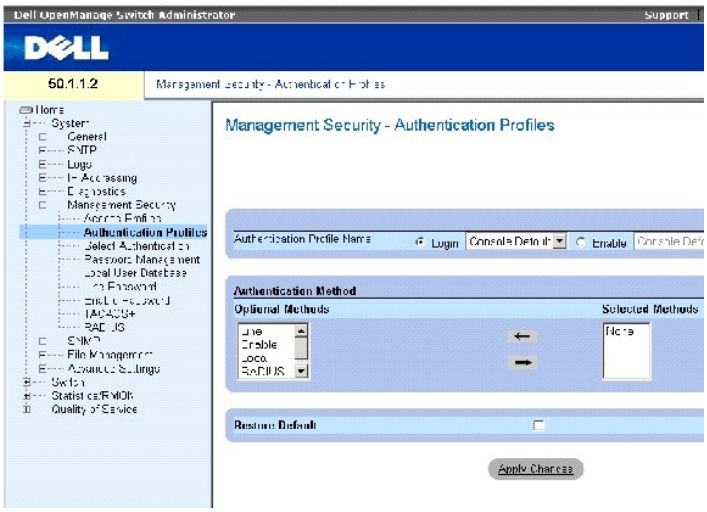
- De forma local
- Mediante un servidor externo

La autenticación del usuario también puede establecerse en None (Ninguna).

La autenticación del usuario se lleva a cabo siguiendo el orden de selección de los métodos. Por ejemplo, si se seleccionan las opciones Local y RADIUS, el usuario se autentica primero de forma local. Si la base de datos de usuarios local está vacía, entonces el usuario se autentica mediante el servidor RADIUS. Si se produce un error de autenticación al utilizar el primer método, el proceso de autenticación finaliza.

Cuando ocurre un error durante la autenticación, se utiliza el siguiente método seleccionado. Para abrir la página Authentication Profiles (Perfiles de autenticación), haga clic en System (Sistema) → Management Security (Seguridad de administración) → Authentication Profiles (Perfiles de autenticación) en la vista de árbol.

Figura 6-42. Authentication Profiles



La página Authentication Profiles (Perfiles de autenticación) contiene los campos siguientes:

Authentication Profile Name (Nombre de perfil de autenticación): contiene listas de perfiles de autenticación definidas por el usuario a las que se añaden los perfiles de autenticación definidos por el usuario. Los valores predeterminados son **Network Default** (Predeterminado de red) y **Console Default** (Predeterminado de consola).

- Login (Inicio de sesión): especifica la lista de perfiles de autenticación definida por el usuario para contraseñas de inicio de sesión.
- Enable (Activación): especifica la lista de perfiles de autenticación definida por el usuario para contraseñas de activación.

Optional Methods (Métodos opcionales): métodos de autenticación de usuarios. Las opciones posibles son:

None (Ninguna): no se realiza autenticación del usuario.

Local: la autenticación del usuario se lleva a cabo en el nivel de dispositivo. El dispositivo comprueba el nombre de usuario y la contraseña para su autenticación.

RADIUS: la autenticación del usuario se lleva a cabo en el servidor RADIUS. Para obtener más información, consulte "Configuración de los valores de RADIUS".

Line (Línea): indica que se utiliza la contraseña de línea para la autenticación del usuario.

Enable (Activación): indica que se utiliza la contraseña de activación para la autenticación.

TACACS+: la autenticación del usuario se lleva a cabo en el servidor TACACS+.

Restore Default(Restablecer predeterminado): restablece el método de autenticación de usuario predeterminado en el dispositivo. Este campo sólo está disponible para el perfil predeterminado.

Remove (Eliminar): elimina el perfil seleccionado. No es posible eliminar perfiles activos. Este campo sólo está disponible para los perfiles definidos por el usuario.

Selección de un perfil de autenticación:

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Seleccione un perfil en el campo **Authentication Profile Name** (Nombre de perfil de autenticación).
3. Seleccione el método de autenticación mediante las flechas de desplazamiento. La autenticación se lleva a cabo siguiendo el orden en el que se enumeran los métodos de autenticación.
4. Haga clic en Apply Changes (Aplicar cambios).

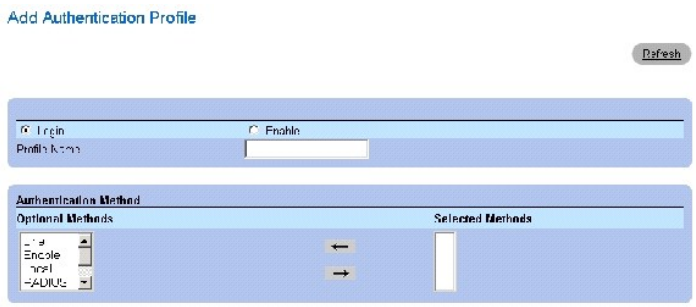
Se actualiza el perfil de autenticación de usuario en el dispositivo.

Adición de un perfil de autenticación:

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Haga clic en Add (Añadir).

Se abre la página **Add Authentication Profile** (Añadir perfil de autenticación):

Figura 6-43. Add Authentication Profile



3. Configure el perfil.

NOTA: no incluya espacios en blanco en el nombre del nuevo perfil.

4. Haga clic en Apply Changes (Aplicar cambios).

Se actualiza el perfil de autenticación en el dispositivo.

Visualización de la tabla de perfiles de autenticación

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Authentication Profiles Table** (Tabla de perfiles de autenticación).

Eliminación de un perfil de autenticación:

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Authentication Profile Table** (Tabla de perfiles de autenticación).

3. Seleccione un perfil de autenticación.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el perfil de autenticación seleccionado.

Configuración de un perfil de autenticación mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Authentication Profiles** (Perfiles de autenticación).

Tabla 6-29. Comandos de la CLI para los perfiles de autenticación

Comando de la CLI	Descripción
aaa authentication login {default | nombre-lista} método1 [método2.]	Configura la autenticación de inicio de sesión.
no aaa authentication login {default | nombre-lista}	Elimina un perfil de autenticación de inicio de sesión.

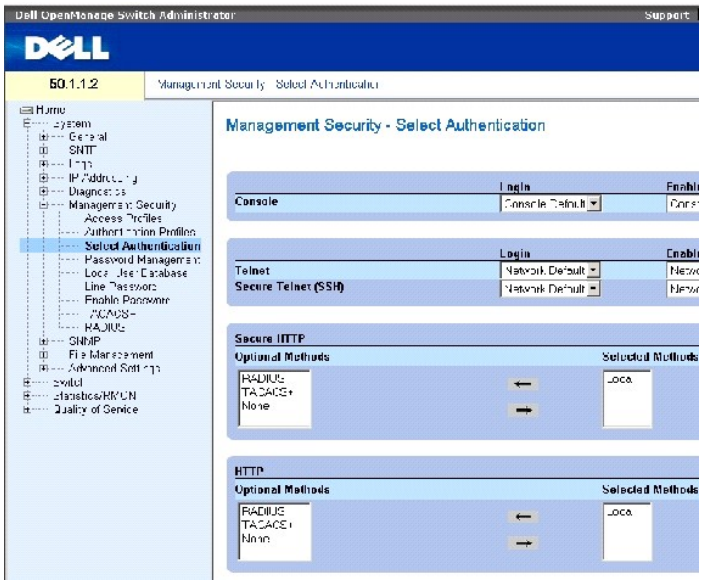
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# aaa
authentication login
default radius local
enable none



console(config)# no aaa
authentication login
default
```

Selección de perfiles de autenticación

Una vez definidos los perfiles de autenticación, éstos pueden aplicarse a los métodos de acceso a la administración. Por ejemplo, los usuarios de la consola se pueden autenticar mediante la lista de métodos de autenticación 1, mientras que los usuarios de Telnet se autentican mediante la lista de métodos de autenticación 2. Para abrir la página **Select Authentication** (Seleccionar autenticación), haga clic en System (Sistema) → Management Security (Seguridad de administración) → Select Authentication (Seleccionar autenticación) en la vista de árbol.

Figura 6-44. Select Authentication



La página **Select Authentication** (Seleccionar autenticación) contiene los campos siguientes:

Console (Consola): muestra los perfiles de autenticación utilizados para autenticar a los usuarios de la consola.

Login (Inicio de sesión): especifica los perfiles de autenticación que los usuarios deben utilizar para iniciar una sesión en la interfaz de la consola.

Enable (Activación): especifica los perfiles de autenticación que deben utilizarse para los usuarios que activan el modo Privileged EXEC desde la interfaz de la consola.

Telnet: muestra los perfiles de autenticación utilizados para autenticar a los usuarios de Telnet.

Secure Telnet (SSH) (Telnet seguro [SSH]): muestra los perfiles de autenticación utilizados para autenticar a los usuarios de Secure Shell (SSH). SSH permite a los clientes conectarse remotamente a un dispositivo de forma segura y con cifrado.

HTTP y **Secure HTTP** (HTTP seguro): método de autenticación utilizado para el acceso HTTP y el acceso HTTP seguro, respectivamente. Los valores del campo posibles son:

None (Ninguno): no se utiliza ningún método de autenticación para el acceso.

Local: la autenticación se lleva a cabo de forma local.

RADIUS: la autenticación se lleva a cabo en el servidor RADIUS.

TACACS+: la autenticación se lleva a cabo en el servidor TACACS+.

Aplicación de una lista de autenticación a sesiones de consola

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. Seleccione un perfil de autenticación en el campo **Console** (Consola).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna una lista de autenticación a las sesiones de consola.

Aplicación de un perfil de autenticación a sesiones Telnet

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. Seleccione un perfil de autenticación en el campo **Telnet**.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna una lista de autenticación a las sesiones Telnet.

Aplicación de un perfil de autenticación a sesiones Telnet seguro (SSH)

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. Seleccione un perfil de autenticación en el campo **Secure Telnet (SSH)** (Telnet seguro [SSH]).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna un perfil de autenticación a las sesiones Telnet seguro (SSH).

Asignación de una secuencia de autenticación a sesiones HTTP

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. Seleccione una secuencia de autenticación en el campo **HTTP**.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna una secuencia de autenticación a las sesiones HTTP.

Asignación de una secuencia de autenticación a sesiones HTTP seguro

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. Seleccione una secuencia de autenticación en el campo **Secure HTTP** (HTTP seguro).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna una secuencia de autenticación a las sesiones HTTP seguro.

Asignación de secuencias o perfiles de autenticación de acceso mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Select Authentication** (Seleccionar autenticación).

Tabla 6-30. Comandos de la CLI para la selección de autenticación

Comando de la CLI	Descripción
enable authentication [default | nombre-lista]	Indica la lista de métodos de autenticación cuando se accede a un nivel de privilegio superior desde un Telnet, una consola o SSH remotos.
login authentication [default | nombre-lista]	Indica la lista de métodos de autenticación de inicio de sesión para un Telnet, una consola o SSH remotos.
ip http authentication método1 [método2.]	Indica los métodos de autenticación para los servidores HTTP.
ip https authentication método1 [método2.]	Indica los métodos de autenticación para los servidores HTTPS.
show authentication methods	Muestra información sobre los métodos de autenticación.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config-line)# enable
authentication default
```

```
console(config-line)# login
authentication default
```

```
console(config-line)# exit
```

```
console(config)# ip http
authentication radius local
```

```
console(config)# ip https
authentication radius local
```

```
console(config)# exit
```

```

```

```
console# show authentication methods
```

```
Login Authentication Method Lists


---------------------------------
```

Console_Default	: None	
Network_Default	: Local	

```
Enable Authentication Method Lists


---------------------------------
```

Console_Default	: Enable None	
Network_Default	: Enable	
Line	Login Method List	Enable Method List
----	---------- ----	------- ------- ----
Console	Default	Default
Telnet	Default	Default

SSH	Default	Default
http	: Local	
https	: Local	
dot1x	:	

Administración de contraseñas

La administración de contraseñas aumenta la seguridad en la red y mejora el control de las contraseñas. Las contraseñas para el acceso SSH, Telnet, HTTP, HTTPS y SNMP tienen funciones de seguridad asignadas, entre ellas:

- Definición de longitudes mínimas de contraseñas
- Caducidad de contraseñas
- Prevención de reutilización frecuente de contraseñas
- Bloqueo de los usuarios tras intentos de inicio de sesión incorrectos

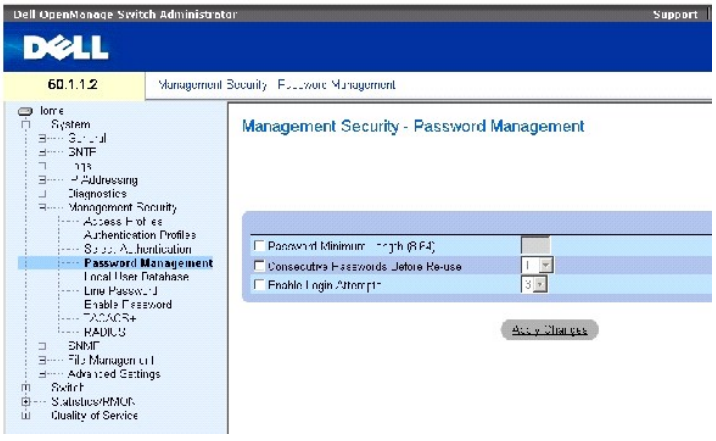
La caducidad de las contraseñas se inicia inmediatamente en cuanto se activa la administración de contraseñas. Las contraseñas caducan en función de la hora/día que el usuario haya definido al especificar la caducidad. Diez días antes de que caduque la contraseña, el dispositivo muestra un mensaje de advertencia de caducidad de la contraseña.

Una vez que la contraseña ha caducado, los usuarios puede iniciar sesión tres veces más. Durante estos tres inicios de sesión, aparece un mensaje de advertencia adicional que informa al usuario de que debe cambiarse inmediatamente la contraseña. Si no se cambia la contraseña, los usuarios verán bloqueado su acceso al sistema y sólo podrán iniciar sesión mediante la consola. Las advertencias de contraseña se registran en el archivo Syslog.

Si se redefine un nivel de privilegios, también deberá redefinirse el usuario. No obstante, la caducidad de la contraseña se basa en la definición inicial del usuario.

Para abrir la página **Password Management** (Administración de contraseñas), haga clic en System (Sistema) → Management Security (Seguridad de administración) → Password Management (Administración de contraseñas) en la vista de árbol.

Figura 6-45. Password Management



La página **Password Management** (Administración de contraseñas) contiene los campos siguientes:

Password Minimum Length (8-64) (Longitud mínima de contraseña [8-64]): indica la longitud mínima de la contraseña. Por ejemplo, el administrador puede definir que todas las contraseñas tengan un mínimo de 10 caracteres.

Consecutive Passwords Before Re-use (Contraseñas consecutivas antes de reutilización): indica el número de veces que debe cambiarse una contraseña antes de poder volver a utilizarla. Los valores del campo posibles son 1-10.

NOTA: el usuario recibe una notificación antes de que la contraseña caduque, y se deberá cambiar la contraseña. Sin embargo, esta notificación no se visualiza para el usuario Web.

Enable Login Attempts (Activar intentos de inicio de sesión): bloquea el acceso de un usuario al dispositivo cuando se ha utilizado una contraseña incorrecta un número de veces superior al definido por el usuario. Por ejemplo, si se selecciona este campo y se establece en 5, cuando un usuario haya intentado iniciar una sesión con una contraseña incorrecta cinco veces, al sexto intento el usuario verá bloqueado su acceso al dispositivo. Los valores del campo posibles son 1-5.

Definición de la administración de contraseñas

1. Abra la página **Password Management** **(Administración de contraseñas).**
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la administración de contraseñas y se actualiza el dispositivo.

Administración de contraseñas mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Password Management** (Administración de contraseñas).

Tabla 6-31. Administración de contraseñas mediante los comandos de la CLI

Comando de la CLI	Descripción
password min-length *longitud*	Define la longitud mínima de las contraseñas.
password history número	Define el número de veces que debe cambiarse una contraseña antes de poder volver a utilizarla.
password lock-out *número*	Define el número de veces que se puede introducir una contraseña incorrecta antes de que se bloquee el acceso del usuario al dispositivo.
show password configuration	Muestra información sobre la administración de contraseñas.

A continuación se muestra un ejemplo de los comandos de la CLI:

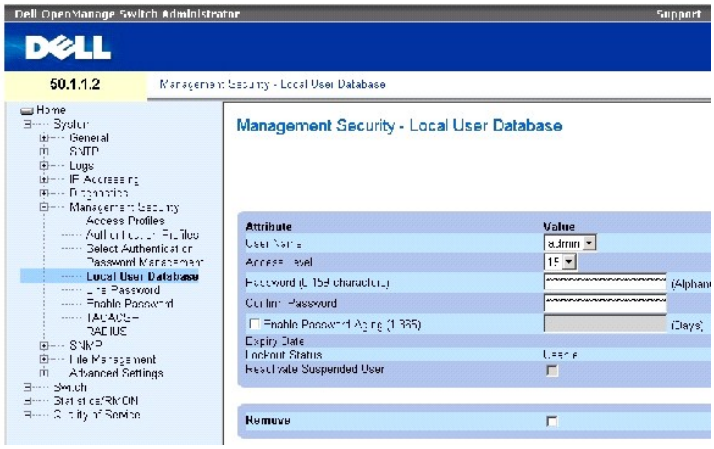
```
console # show passwords configuration

Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled
```

Enable Passwords				
Level	Password Aging	Password Expiry date	Lockout	
-----	--------	----------	-------	
1	-	-	-	
15	-	-	-	
Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
SSH	-	-	-	
Console	-	-	-	
console # show users accounts				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	----------	-------
nim	15	39	18-Feb-2005	

Definición de las bases de datos de usuarios locales

La página **Local User Database** (Base de datos de usuarios local) contiene campos para definir usuarios, contraseñas y niveles de acceso. Para abrir la página **Local User Database** (Base de datos de usuarios local), haga clic en System (Sistema) → Management Security (Seguridad de administración) → Local User Database (Base de datos de usuarios local) en la vista de árbol.

Figura 6-46. Local User Database



La página **Local User Database** (Base de datos de usuarios local) contiene los campos siguientes:

User Name (Nombre de usuario): contiene una lista de usuarios.

Access Level (Nivel de acceso): nivel de acceso de los usuarios. El nivel de acceso más bajo es **1**, y el nivel de acceso más alto es **15**. Los usuarios con el nivel de acceso 15 son usuarios con privilegios y son los únicos que pueden acceder al administrador de conmutadores OpenManage y utilizarlo.

Password (0-159 Characters) (Contraseña [0-159 caracteres]): contraseña definida por el usuario.

Confirm Password (Confirmar contraseña): confirma la contraseña definida por el usuario.

Enable Password Aging (1-365) (Caducidad de contraseña de activación [1-365]): indica el tiempo, en días, que debe transcurrir para que caduque la contraseña.

Expiry Date (Fecha de caducidad): indica la fecha de caducidad de la contraseña definida por el usuario.

Lockout Status (Estado de bloqueo): especifica el número de intentos de autenticación incorrectos desde la última vez que el usuario ha iniciado sesión correctamente, si se ha seleccionado la casilla de verificación **Enable Login Attempts** (Activar intentos de inicio de sesión) en la página **Password Management** (Administración de contraseñas). Cuando la cuenta de usuario está bloqueada, el valor que se muestra es **LOCKOUT** (Bloqueo).

Reactivate Suspended User (Volver a activar usuario suspendido): vuelve a activar los derechos de acceso del usuario especificado. Los derechos de acceso pueden suspenderse después de haber intentado iniciar una sesión incorrectamente.

Remove (Eliminar): elimina a los usuarios de la lista de nombres de usuario.

Asignación de derechos de acceso a un usuario:

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Seleccione un usuario en el campo **User Name** (Nombre de usuario).
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

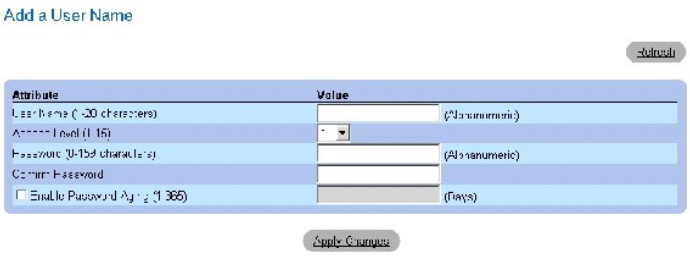
Se definen los derechos de acceso y las contraseñas de los usuarios y se actualiza el dispositivo.

Definición de un nuevo usuario:

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add User** (Añadir usuario):

Figura 6-47. Add a User



3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define el nuevo usuario y se actualiza el dispositivo.

Visualización de la tabla de usuarios locales:

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de usuarios locales:

Figura 6-48. Local User Table

Reactivación de un usuario suspendido:

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de usuarios locales.

3. Seleccione una entrada de nombre de usuario.
4. Seleccione la casilla de verificación **Reactivate Suspender User** (Volver a activar usuario suspendido).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se vuelven a activar los derechos de acceso del usuario y se actualiza el dispositivo.

Eliminación de usuarios:

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Haga clic en **Show All** (Mostrar todo).

   Se abre la página **Local User Table** (Tabla de usuarios locales).
3. Seleccione un nombre de usuario.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

   Se elimina el usuario seleccionado y se actualiza el dispositivo.

Asignación de usuarios mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Local User Database** (Base de datos de usuarios local).

Tabla 6-32. Comandos de la CLI para la base de datos de usuarios local

Comando de la CLI	Descripción
username nombre [password contraseña] [level nivel] [encrypted]	Establece un sistema de autenticación basado en el nombre de usuario.
set username nombre active	Vuelve a activar los derechos de acceso del usuario suspendido.

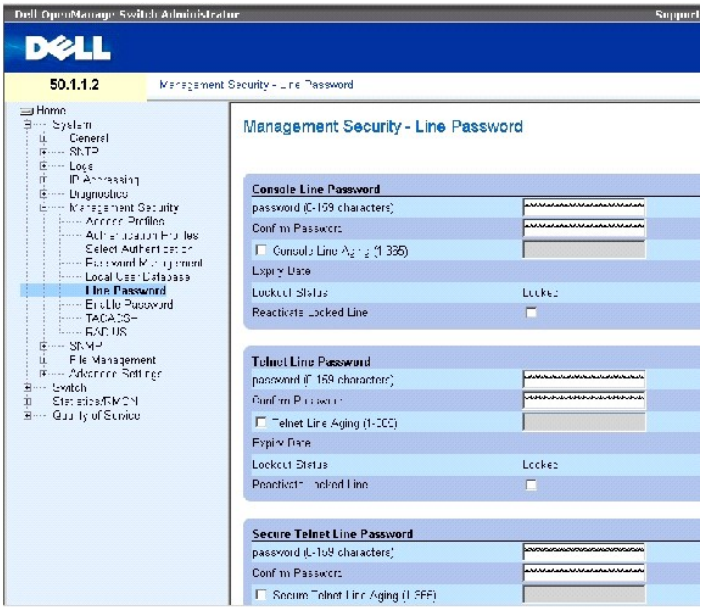
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# username
bob password lee level 15


console# set username bob
active
```

Definición de contraseñas de línea

La página Line Password (Contraseña de línea) contiene campos para definir contraseñas de línea para métodos de administración. Para abrir la página Line Password(Contraseña de línea), haga clic en System (Sistema)→ Management Security (Seguridad de administración)→ Line Passwords (Contraseñas de línea) en la vista de árbol.

Figura 6-49. Line Password



La página Line Password (Contraseña de línea) contiene los campos siguientes:

Line Password for Console / Telnet / Secure Telnet (Contraseña de línea para consola/Telnet/Telnet seguro): contraseña de línea para acceder al dispositivo a través de una sesión de consola, Telnet o Telnet seguro.

Confirm Password for Console / Telnet / Secure Telnet (Confirmar contraseña para consola/Telnet/Telnet seguro): confirma la nueva contraseña de línea. La contraseña se muestra con el formato *****.

Line Aging (1-365) for Console / Telnet / Secure Telnet (Caducidad de línea [1-365] para consola/Telnet/Telnet seguro): indica el tiempo (en días) que debe transcurrir para que caduque una contraseña de línea.

Expiry Date for Console / Telnet / Secure Telnet (Fecha de caducidad para consola/Telnet/Telnet seguro): indica la fecha de caducidad de la contraseña de línea.

Lockout Status for Console / Telnet / Secure Telnet (Estado de bloqueo para consola/Telnet/Telnet seguro): especifica el número de intentos de autenticación incorrectos desde la última vez que el usuario ha iniciado sesión correctamente, si se ha seleccionado la casilla de verificación **Enable Login Attempts** (Activar intentos de inicio de sesión) en la página **Password Management** (Administración de contraseñas). Cuando la cuenta de usuario está bloqueada, el valor que se muestra es **LOCKOUT** (Bloqueo).

Reactivate Locked Line for Console / Telnet / Secure Telnet (Volver a activar línea bloqueada para consola/Telnet/Telnet seguro): vuelve a activar la contraseña de línea para una sesión de consola/Telnet/Telnet seguro. Los derechos de acceso pueden suspenderse después de haber intentado iniciar una sesión incorrectamente.

Definición de contraseñas de línea para sesiones de consola

1. Abra la página **Line Password** (Contraseña de línea).
2. Defina el campo **Console Line Password** (Contraseña de línea para consola).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la contraseña de línea para las sesiones de consola y se actualiza el dispositivo.

Definición de contraseñas de línea para sesiones Telnet

1. Abra la página **Line Password** (Contraseña de línea).
2. Defina el campo Telnet Line Password (Contraseña de línea para Telnet).
3. Haga clic en Apply Changes (Aplicar cambios).

Se define la contraseña de línea para las sesiones Telnet y se actualiza el dispositivo.

Definición de contraseñas de línea para sesiones Telnet seguro

1. Abra la página **Line Password** (Contraseña de línea).
2. Defina el campo **Secure Telnet Line Password** (Contraseña de línea para Telnet seguro).
3. Haga clic en Apply Changes (Aplicar cambios).

Se define la contraseña de línea para las sesiones Telnet seguro y se actualiza el dispositivo.

Asignación de contraseñas de línea mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Line Password** (Contraseña de línea).

Tabla 6-33. Comandos de la CLI para las contraseñas de línea

Comando de la CLI	Descripción
password contraseña [encrypted]	Indica una contraseña en una línea.

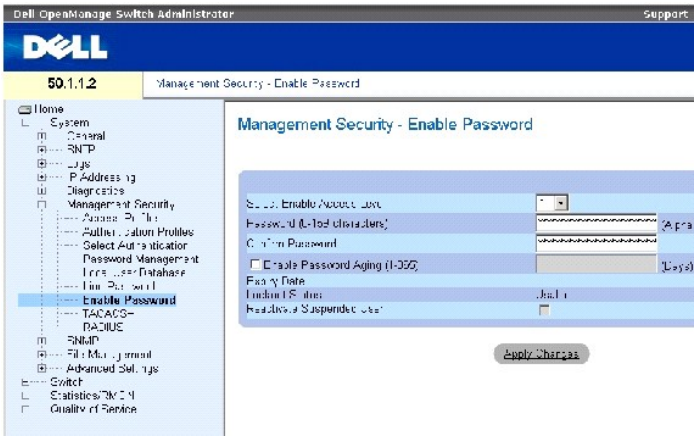
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config-line)#
password dell
```

Definición de contraseñas de activación

La página **Enable Password** (Contraseña de activación) permite establecer una contraseña local para controlar el acceso a los niveles normal y de privilegio. Para abrir la página **Enable Password** (Contraseña de activación), haga clic en System (Sistema) → Management Security (Seguridad de administración) → Enable Passwords (Contraseñas de activación) en la vista de árbol.

Figura 6-50. Enable Password



La página **Enable Password** (Contraseña de activación) contiene los campos siguientes:

Select Enable Access Level (Seleccionar nivel de acceso de activación): identifica el nivel de acceso asociado con la contraseña de activación. Los valores del campo posibles son 1-15.

Password (0-159 Characters) (Contraseña [0-159 caracteres]): contraseña de activación actual.

Confirm Password (Confirmar contraseña): confirma la nueva contraseña de activación. La contraseña se muestra con el formato *****.

Enable Password Aging (1-365) (Caducidad de contraseña de activación [1-365]): indica el tiempo, en días, que debe transcurrir para que caduque la contraseña.

Expiry Date (Fecha de caducidad): indica la fecha de caducidad de la contraseña de activación.

Lockout Status (Estado de bloqueo): especifica el número de intentos de autenticación incorrectos desde la última vez que el usuario ha iniciado sesión correctamente, si se ha seleccionado la casilla de verificación **Enable Login Attempts** (Activar intentos de inicio de sesión) en la página **Password Management** (Administración de contraseñas). Cuando la cuenta de usuario está bloqueada, el valor que se muestra es **LOCKOUT** (Bloqueo).

Reactivate Suspended User (Volver a activar usuario suspendido): vuelve a activar los derechos de acceso del usuario especificado. Los derechos de acceso pueden suspenderse después de haber intentado iniciar una sesión incorrectamente.

Definición de una nueva contraseña de activación:

1. Abra la página **Enable Password** (Contraseña de activación).
2. Defina los campos.
3. Haga clic en Apply Changes (Aplicar cambios).

Se define la nueva contraseña de activación y se actualiza el dispositivo.

Asignación de contraseñas de activación mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Enable Password** (Contraseña de activación).

Tabla 6-34. Comandos de la CLI para modificar contraseñas de activación

Comando de la CLI	Descripción
enable password [level nivel] contraseña [encrypted]	Establece una contraseña local para controlar el acceso a niveles usuario y de privilegio.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# enable
password level 15 secret
```

Definición de la configuración de TACACS+

Los dispositivos pueden ejercer de clientes del sistema de control de acceso al controlador de acceso al terminal (TACACS+). TACACS+ proporciona una seguridad centralizada para la validación de los usuarios que acceden a un dispositivo.

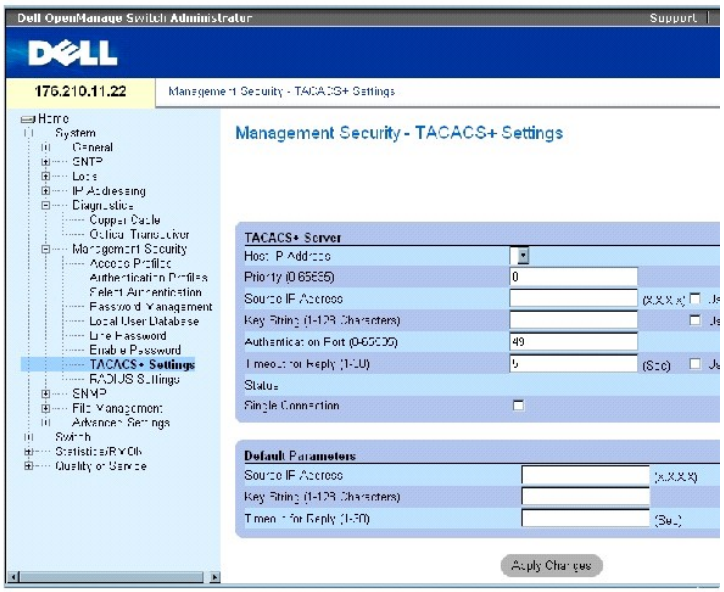
TACACS+ es un sistema de administración de usuarios centralizado que, además, es compatible con RADIUS y otros procesos de autenticación. TACACS+

proporciona los servicios siguientes:

- Authentication (Autenticación): proporciona autenticación durante el inicio de sesión y a través de nombres de usuario y contraseñas definidas por el usuario.
- Authorization (Autorización): se lleva a cabo cuando se iniciar una sesión. Una vez que se ha completado la sesión de autenticación, se inicia una sesión de autorización mediante el nombre de usuario autenticado. El servidor TACACS+ comprueba los privilegios de usuario.

El protocolo TACACS+ asegura la integridad de la red por medio de intercambios de protocolo cifrados entre el dispositivo y el servidor TACACS+. Para abrir la página **TACACS+ Settings** **(Configuración de TACACS+)**, haga clic en **System** (Sistema) → **Management Security (Seguridad de administración)** → **TACACS+** en la vista de árbol.

Figura 6-51. TACACS+ Settings



La página **TACACS+ Settings** (Configuración de TACACS+) contiene los campos siguientes:

Host IP Address (Dirección IP de host): indica la dirección IP del servidor TACACS+.

Priority (0-65535) (Prioridad [0-65535]): indica el orden en el que se utilizan los servidores TACACS+. El valor predeterminado es 0.

Source IP Address (Dirección IP de origen): dirección IP de origen del dispositivo utilizada para la sesión TACACS+ entre el dispositivo y el servidor TACACS+.

Key String (0-128 Characters) (Cadena de clave [0-128 caracteres]): define la clave de autenticación y de cifrado para las comunicaciones TACACS+ entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con la clave de cifrado utilizada en el servidor TACACS+. Esta clave está cifrada.

Authentication Port (0-65535) (Puerto de autenticación [0-65535]): número de puerto a través del cual se realiza la sesión TACACS+. El valor predeterminado es 49.

Timeout for Reply (1-30) (Tiempo de espera para respuesta): cantidad de tiempo que transcurre antes de que se agote el tiempo de la conexión entre el dispositivo y el servidor TACACS+. El intervalo de valores de este campo es 1-30 segundos.

Status (Estado): estado de la conexión entre el dispositivo y el servidor TACACS+. Los valores del campo posibles son:

Connected (Con conexión): existe una conexión entre el dispositivo y el servidor TACACS+.

Not Connected (Sin conexión): no existe ninguna conexión entre el dispositivo y el servidor TACACS+.

Single Connection (Conexión única): se mantiene una única conexión abierta entre el dispositivo y el servidor TACACS+.

Los parámetros predeterminados de TACACS+ los define el usuario. La configuración predeterminada se aplica a los nuevos servidores TACACS+ definidos. Si no se han definido valores predeterminados, se aplicarán los valores predeterminados del sistema a los nuevos servidores TACACS+.

Los valores predeterminados de TACACS+ son los siguientes:

Source IP Address (Dirección IP de origen): dirección IP de origen del dispositivo predeterminada utilizada para la sesión TACACS+ entre el dispositivo y el servidor TACACS+. La dirección IP de origen predeterminada es 0.0.0.0.

Key String (0-128 Characters) (Cadena de clave [0-128 caracteres]): cadena de clave predeterminada utilizada para la autenticación y el cifrado de todas las comunicaciones entre el dispositivo y el servidor TACACS+. Esta clave está cifrada.

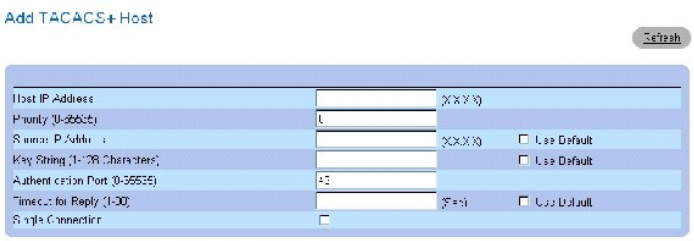
Timeout for Reply (1-30) (Tiempo de espera para respuesta): cantidad de tiempo predeterminada que transcurre antes de que se agote el tiempo de la conexión entre el dispositivo y el servidor TACACS+. El valor predeterminado es 5 segundos.

Adición de un servidor TACACS+

1. Abra la página **TACACS+ Settings** (Configuración de TACACS+).
2. Haga clic en Add (Añadir).

Se abre la página **Add TACACS+ Host** (Añadir host TACACS+):

Figura 6-52. Add TACACS+ Host



3. Defina los campos.
4. Haga clic en Apply Changes (Aplicar cambios).

Se añade el servidor TACACS+ y se actualiza el dispositivo.

Visualización de la página TACACS+ Table (Tabla de TACACS+)

1. Abra la página **TACACS+ Settings** (Configuración de TACACS+).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **TACACS+ Table** (Tabla de TACACS+).

Figura 6-53. TACACS+ Table

Eliminación de un servidor TACACS+

1. Abra la página **TACACS+ Table** (Tabla de TACACS+).
2. Haga clic en Show All (Mostrar todo).

   Se abre la página **TACACS+ Table** (Tabla de TACACS+).
3. Seleccione una entrada en la página **TACACS+ Table** (Tabla de TACACS+).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en Apply Changes (Aplicar cambios).

   Se elimina el servidor TACACS+ y se actualiza el dispositivo.

Definición de la configuración de TACACS+ mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **TACACS+ Settings** (Configuración de TACACS+).

Tabla 6-35. Comandos de la CLI para TACACS+

Comando de la CLI	Descripción
tacacs-server host {*dirección-ip* | *nombrehost*} [**single-connection**] [**port** *número-puerto*] [**timeout** *tiempo-espera*] [**key** *cadena-clave*] [**source** *origen*] [**priority** *prioridad*]	Indica un host TACACS+.
tacacs-server key cadena-clave	Indica la clave de autenticación y de cifrado para todas las comunicaciones TACACS+ entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con el cifrado utilizado en el daemon TACACS+. El intervalo de valores de este campo es 0-128 caracteres.
tacacs-server timeout tiempo-espera	Indica el valor del tiempo de espera en segundos. El intervalo de valores de este campo es 1-30.
tacacs-server source-ip origen	Indica la dirección IP de origen. El intervalo de valores de este campo es dirección IP válida.
show tacacs [*dirección-ip*]	Muestra la configuración y las estadísticas de un servidor TACACS+.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show tacacs

Device Configuration

IP address  Status  Port  Single Connection  TimeOut  Source IP  Priority
----------  ------  ----  -----------------  -------  ---------  --------
12.1.1.2    Not     49    Yes                1        12.1.1.1   1
```

	Connected					
Global values						

TimeOut : 5						
Device Configuration ----------						
Source IP : 0.0.0.0						
console#						

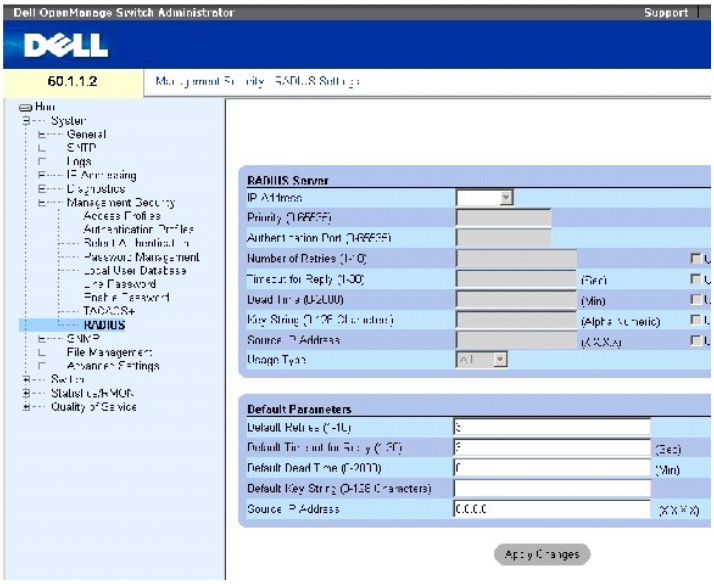
Configuración de los valores de RADIUS

Los servidores RADIUS (servicio de usuario de acceso telefónico de autenticación remota) proporcionan una seguridad adicional para las redes. Se puede definir un máximo cuatro servidores RADIUS. Los servidores RADIUS proporcionan un método de autenticación centralizado para:

- Acceder a Telnet
- Acceder a Secure Shell
- Acceder a la Web
- Acceder a la consola

Para abrir la página RADIUS Settings (Configuración de RADIUS), haga clic en System (Sistema) → Management Security (Seguridad de administración) → RADIUS en la vista de árbol.

Figura 6-54. RADIUS Settings



La página RADIUS Settings (Configuración de RADIUS) contiene los campos siguientes:

IP Address (Dirección IP): lista de direcciones IP de servidor de autenticación.

Priority (0-65535) (Prioridad [0-65535]): prioridad del servidor. Los valores posibles son 0-65535, donde 0 es el valor más alto. La prioridad se utiliza para configurar el orden en el que se consultan los servidores.

Authentication Port (Puerto de autenticación): indica el puerto de autenticación. El puerto de autenticación se utiliza para comprobar la autenticación del servidor RADIUS.

Number of Retries (1-10) (Número de reintentos [1-10]): indica el número de peticiones transmitidas enviadas al servidor RADIUS antes de que se produzca un error. Los valores del campo posibles son 1-10.

Timeout for Reply (1-30) (Tiempo de espera para respuesta [1-30]): indica el tiempo, en segundos, durante el que el dispositivo espera una respuesta del servidor RADIUS antes de reintentar la consulta o pasar al siguiente servidor. Los valores del campo posibles son 1-30.

Dead Time (0-2000) (Tiempo muerto [0-2000]): indica el tiempo, en minutos, durante el que no se envían peticiones de servicio al servidor RADIUS. El intervalo de valores posibles es 0-2000.

Key String (1-128 Characters) (Cadena de clave [1-128 caracteres]): cadena de clave utilizada para la autenticación y el cifrado de todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave está cifrada.

Source IP Address (Dirección IP de origen): indica la dirección IP de origen utilizada para la comunicación con servidores RADIUS.

Usage Type (Tipo de uso): indica el tipo de uso del servidor. Se puede utilizar uno de los valores siguientes: "login" (inicio de sesión), "802.1x" o "all" (todos). Si no se especifica ningún valor, se utilizará de forma predeterminada el valor "all" (todos).

Los campos siguientes permiten establecer los valores predeterminados de RADIUS:

NOTA: si no se especifican los valores de tiempo de espera, de reintento ni de tiempo muerto específicos del host, se aplicarán los valores globales (valores predeterminados) a cada host.

Default Retries (1-10) (Reintentos predeterminados [1-10]): indica el número predeterminado de peticiones transmitidas enviadas al servidor RADIUS antes de

que ocurra un fallo.

Default Timeout for Reply (1-30) (Tiempo de espera predeterminado para respuesta [1-30]): indica el tiempo predeterminado, en segundos, durante el que el dispositivo espera una respuesta del servidor RADIUS antes de que se agote el tiempo de espera. El valor predeterminado es 5 segundos.

Default Dead time (0-2000) (Tiempo muerto predeterminado [0-2000]): indica el tiempo predeterminado, en minutos, durante el que no se envían peticiones de servicio al servidor RADIUS. El intervalo de valores posibles es 0-2000.

Default Key String (1-128 Characters) (Cadena de clave predeterminada [1-128 caracteres]): cadena de clave predeterminada utilizada para la autenticación y el cifrado de todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave está cifrada.

Source IP Address (Dirección IP de origen): indica la dirección IP de origen predeterminada utilizada para la comunicación con servidores RADIUS. La dirección IP de origen predeterminada es 0.0.0.0.

Definición de los parámetros de RADIUS:

1. Abra la página RADIUS Settings (Configuración de RADIUS).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de RADIUS se actualiza en el dispositivo.

Adición de un servidor RADIUS:

1. Abra la página RADIUS Settings (Configuración de RADIUS).
2. Haga clic en Add (Añadir).

Se abre la página **Add RADIUS Server** (Añadir servidor RADIUS):

Figura 6-55. Add RADIUS Server

3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

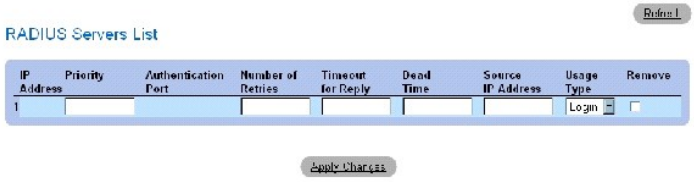
Se añade el nuevo servidor RADIUS y se actualiza el dispositivo.

Visualización de la lista de servidores RADIUS:

1. Abra la página RADIUS Settings (Configuración de RADIUS).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página RADIUS Servers List (Lista de servidores RADIUS):

Figura 6-56. RADIUS Servers List



Eliminación de un servidor RADIUS

1. Abra la página **RADIUS Settings** (Configuración de RADIUS).
2. Haga clic en Show All (Mostrar todo).

   Se abre la página RADIUS Servers List (Lista de servidores RADIUS).
3. Seleccione una entrada en la página RADIUS Servers List (Lista de servidores RADIUS).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en Apply Changes (Aplicar cambios).

   Se elimina el servidor RADIUS y se actualiza el dispositivo.

Definición de servidores RADIUS mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir los campos de la página **RADIUS Settings** (Configuración de RADIUS).

Tabla 6-36. Comandos de la CLI para los servidores RADIUS

Comando de la CLI	Descripción
radius-server timeout *tiempo-espera*	Establece el intervalo durante el que un enrutador espera la respuesta de un host de servidor.
radius-server retransmit *reintentos*	Especifica el número de veces que el software busca en la lista de hosts de servidores RADIUS.
radius-server deadtime tiempo-muerto	Establece los servidores no disponibles que deben omitirse.
radius-server key *cadena-clave*	Establece la clave de autenticación y de cifrado predeterminada para todas las comunicaciones RADIUS entre el enrutador y el entorno RADIUS.
radius-server host *dirección-ip* [**auth-port** *número-puerto-aut*] [**timeout** tiempo-espera] [**retransmit** *reintentos*] [**deadtime** *tiempo- muerto*] [**key** *cadena- clave*] [**source** *origen*] [**priority** *prioridad*]	Especifica un host de servidor RADIUS.
show radius-servers	Muestra la configuración del servidor RADIUS.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config)# radius-
server timeout 5
```

```
Console(config)# radius-
server retransmit 5



Console(config)# radius-
server deadtime 10



Console(config)# radius-
server key dell-server



Console(config)# radius-
server host 196.210.100.1
auth-port 127 timeout 20



Console# show radius-
servers



IP address Auth Acct
TimeOut Retransmit
Deadtime Source IP
Priority



-------- ---- ---- ------
--------- ------- -------
------



172.16.1.1 164 51646 3 3 0
01 172.16.1.2 164 51646 3
3 0 02
```

Definición de los parámetros de SNMP

El protocolo simple de administración de red (SNMP) proporciona un método para administrar los dispositivos de una red. El conmutador admite las versiones de SNMP siguientes:

- SNMPv1 (versión 1)
- SNMPv2 (versión 2)
- SNMPv3 (versión 3)

SNMPv1 y SNMPv2

Los agentes SNMP mantienen una lista de variables que se utilizan para administrar el conmutador. Estas variables se definen en la base de datos de información de administración (MIB). La MIB presenta las variables controladas por el agente. El agente SNMP define el formato de especificación de la MIB, así como el formato utilizado para acceder a la información en la red. Las cadenas de acceso controlan los derechos de acceso al agente SNMP.

Las versiones SNMPv1 y SNMPv2 están activadas de forma predeterminada.

SNMPv3

SNMPv3 también aplica el control de acceso y un nuevo mecanismo de excepciones para unidades PDU de SNMPv1 y SNMPv2. Además, SNMPv3 tiene definido un modelo de seguridad basado en el usuario (USM) que incluye lo siguiente:

- **Autenticación**: proporciona autenticación de la integridad y el origen de los datos.

- **Privacidad**: impide la divulgación del contenido del mensaje. Para el cifrado se utiliza el encadenamiento de bloques de cifrado (CBC). En un mensaje SNMP, puede activarse la autenticación o bien la autenticación y la privacidad. Sin embargo, no es posible activar la privacidad sin la autenticación.
- **Determinismo temporal**: evita que se produzcan demoras en los mensajes o mensajes redundantes. El agente SNMP compara el mensaje entrante con la información de hora del mensaje.
- **Administración de claves**: define la generación, las actualizaciones y la utilización de las claves.

El conmutador admite filtros de notificación de SNMP basados en ID de objeto (OID). El sistema utiliza las OID para administrar las funciones del conmutador. SNMPv3 admite las funciones siguientes:

- Seguridad
- Control de acceso a funciones
- Excepciones

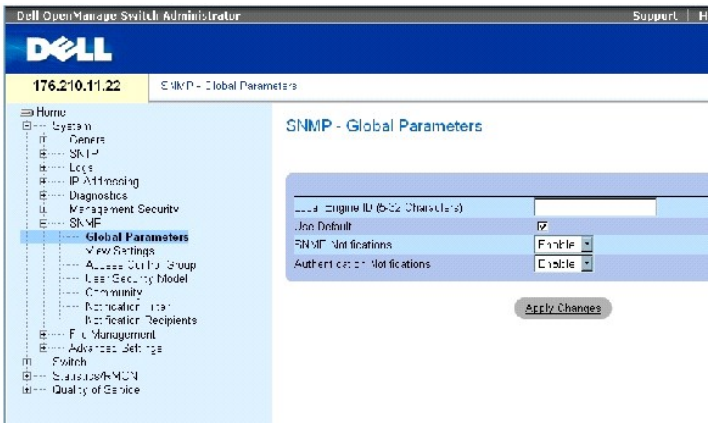
Las claves de autenticación o de privacidad se modifican en el modelo de seguridad basado en el usuario (USM).

SNMPv3 puede activarse si la ID de motor local está activada.

Definición de los parámetros globales de SNTP

La página **SNMP Global Parameters** (Parámetros globales de SNMP) permite activar las notificaciones de SNMP y de autenticación. Para abrir la página **SNMP Global Parameters** (Parámetros globales de SNMP), haga clic en System (Sistema) → SNMP → Global Parameters (Parámetros globales) en la vista de árbol.

Figura 6-57. SNMP Global Parameters



La página **SNMP Global Parameters** (Parámetros globales de SNMP) contiene los campos siguientes:

Local Engine ID (ID de motor local): indica la ID de motor del dispositivo local. El valor de este campo es una cadena hexadecimal. Cada byte de la cadena de caracteres hexadecimales equivale a dos dígitos hexadecimales. Cada byte puede separarse mediante un punto o dos puntos. La ID de motor debe definirse antes de activar SNMPv3.

En el caso de los dispositivos independientes, seleccione una ID de motor predeterminada que esté formada por el número de empresa y la dirección MAC predeterminada.

En el caso de un sistema apilable, configure la ID de motor y verifique que dicha ID es exclusiva para el dominio administrativo. Esto evita que dos dispositivos de una red tengan la misma ID de motor.

Use Defaults (Utilizar valores predeterminados): utiliza la ID de motor generada por el dispositivo. La ID de motor predeterminada se basa en la dirección

MAC del dispositivo y se define de forma estándar de la manera siguiente:

First 4 octets (Primeros 4 octetos): primer bit = 1; el resto corresponde al número de empresa asignado por la IANA = 674.

Fifth octet (Quinto octeto): se establece en 3 para indicar la dirección MAC que se especifica a continuación.

Last 6 octets (Últimos 6 octetos): dirección MAC del dispositivo.

SNMP Notifications (Notificaciones de SNMP): activa o desactiva el envío de notificaciones de SNMP por parte del enrutador.

Authentication Notifications (Notificaciones de autenticación): activa o desactiva el envío de excepciones de SNMP por parte del enrutador cuando falla la autenticación.

Activación de las notificaciones de SNMP

1. Abra la página **SNMP Global Parameters** (Parámetros globales de SNMP).
2. Seleccione **Enable** (Activar) en el campo **SNMP Notifications** (Notificaciones de SNMP).
3. Haga clic en Apply Changes (Aplicar cambios).

Se activan las notificaciones de SNMP y se actualiza el dispositivo.

Activación de las notificaciones de autenticación

1. Abra la página **SNMP Global Parameters** (Parámetros globales de SNMP).
2. Seleccione **Enable** (Activar) en el campo **Authentication Notifications** (Notificaciones de autenticación).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Activación de las notificaciones de SNMP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página **SNMP Global Parameters** (Parámetros globales de SNMP).

Tabla 6-37. Comandos para la notificación de SNMP

Comando de la CLI	Descripción
snmp-server enable traps	Permite al enrutador enviar excepciones de protocolo simple de administración de red (SNMP).
snmp-server trap authentication	Permite al enrutador enviar excepciones de protocolo simple de administración de red (SNMP) cuando falla la autenticación.
show snmp	Comprueba el estado de las comunicaciones de SNMP.
snmp-server engine ID local {*cadena-idmotor* | **default**}	Indica la ID de motor del dispositivo local. El valor de este campo es una cadena hexadecimal. Cada byte de la cadena de caracteres hexadecimales equivale a dos dígitos hexadecimales. Cada byte puede separarse mediante un punto o dos puntos. La ID de motor debe definirse antes de activar SNMPv3.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config)# snmp-server enable traps

Console(config)# snmp-server trap authentication
```

```
Console# show snmp

Community-String                Community-Access        View name       IP address
------------------------------  ----------------------  --------------  ----------
public                          read only               view-1          All

Community-String                Group name              IP address      Type
------------------------------  ----------------------  --------------  ----
Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications

Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
--------------  ----  ---------  -------  --------  -----------  ------  -------

Version 3 notifications

Target Address  Type  Username   Security Level  Udp Port  Filter name  To Sec  Retries
--------------  ----  ---------  --------------  --------  -----------  ------  -------
System Contact: Robert
System Location: Marketing
```

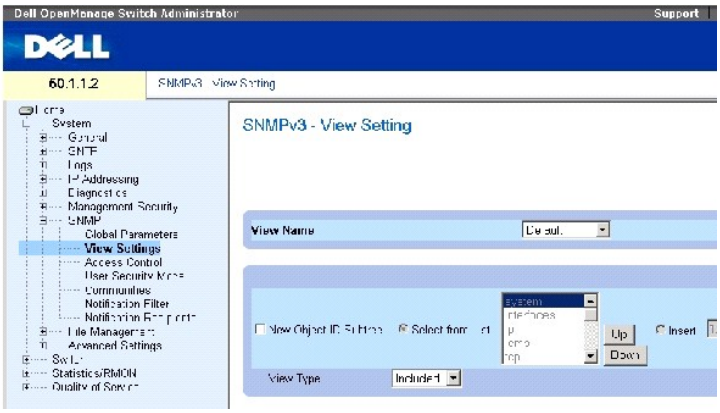
Definición de la configuración de las vistas de SNMP

Las vistas de SNMP proporcionan acceso o bloquean el acceso a funciones del dispositivo o a aspectos de las funciones. Por ejemplo, se puede definir una vista que especifique que el grupo A de SNMP tenga acceso de sólo lectura a los grupos de multidifusión, y que el grupo B de SNMP tenga acceso de lectura/escritura a los grupos de multidifusión. El acceso a las funciones se concede a través del nombre o la ID de objeto de la MIB.

Las flechas hacia arriba y hacia abajo permiten desplazarse por el árbol y las bifurcaciones de la MIB.

Para abrir la página **SNMPv3 View Settings** (Configuración de vistas de SNMPv3), haga clic en **System** (Sistema) → **SNMP** → **View Settings** (Configuración de vistas) en la vista de árbol.

Figura 6-58. SNMPv3 View Settings



La página **SNMPv3 View Settings** (Configuración de vistas de SNMPv3) contiene los campos siguientes:

View Name (Nombre de la vista): contiene una lista de las vistas definidas por el usuario. El nombre de la vista puede contener un máximo de 30 caracteres alfanuméricos.

New Object ID Subtree (Nuevo subárbol de ID de objeto): indica la OID de función del dispositivo incluida o excluida en la vista de SNMP seleccionada.

Selected from List (Lista de selección): seleccione la OID de función del dispositivo utilizando los botones **Up** (Arriba) y **Down** (Abajo) para desplazarse por la lista de OID de dispositivo.

Insert (Insertar): especifique la OID de función del dispositivo.

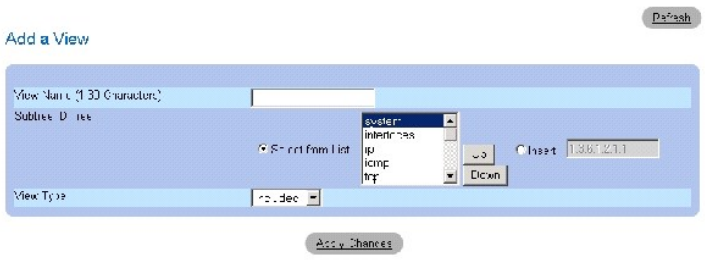
View Type (Tipo de vista): indica si la bifurcación de OID definida se incluirá o excluirá en la vista de SNMP seleccionada.

Adición de una vista

1. Abra la página **SNMPv3 View Settings** (Configuración de vistas de SNMPv3).
2. Haga clic en Add (Añadir).

Se abre la página **Add a View** (Añadir vista):

Figura 6-59. Add a View



3. Defina el campo.
4. Haga clic en Apply Changes (Aplicar cambios).

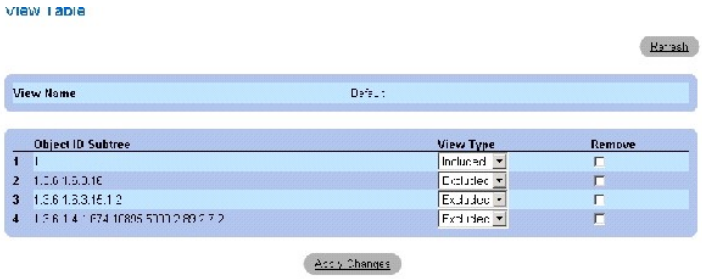
Se añade la vista de SNMP y se actualiza el dispositivo.

Visualización de la tabla de vistas

1. Abra la página **SNMPv3 View Settings** (Configuración de vistas de SNMPv3).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **View Table** (Tabla de vistas):

Figura 6-60. View Table



Definición de las vistas de SNMPv3 mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir los campos de la página **SNMPv3 View Settings** (Configuración de vistas de SNMPv3).

Tabla 6-38. Comandos de la CLI para las vistas de SNMP

Comando de la CLI	Descripción
snmp-server view *nombre-vista árbol- oid* {**included** | **excluded**}	Crea o actualiza una entrada de la vista.
show snmp views [*nombrevista*]	Muestra la configuración de las vistas.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config)# snmp-server view user1
1 included

Console(config)# end

Console# show snmp views
```

Name	OID Tree	Type

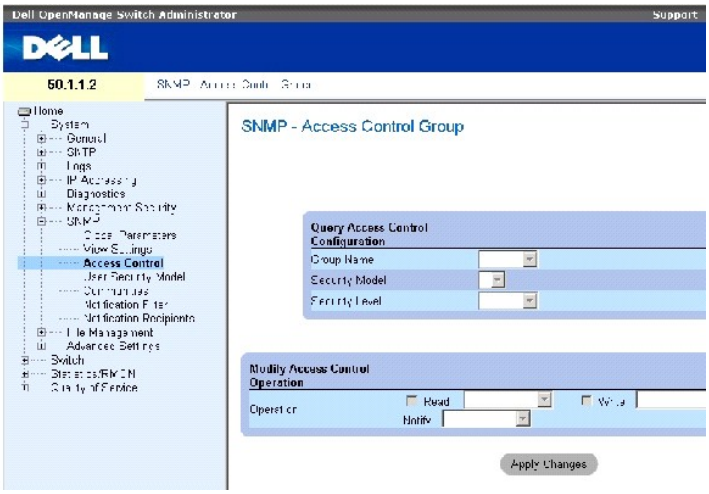
----------	----------	--------
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

Definición del control de acceso de SNMP

La página Access Control (Control de acceso) proporciona información para crear grupos SNMP y para asignar privilegios de control de acceso de SNMP a grupos SNMP. Los grupos permiten a los administradores de red asignar derechos de acceso a funciones específicas del dispositivo o a aspectos de las funciones.

Para abrir la página **Access Control Group** (Grupo de control de acceso), haga clic en System (Sistema) → SNMP → Access Control (Control de acceso) en la vista de árbol.

Figura 6-61. Access Control Group



La página **Access Control Group** (Grupo de control de acceso) contiene los campos siguientes:

Group Name (Nombre del grupo): grupo definido por el usuario al que se aplican reglas de control de acceso. El valor de este campo puede tener un máximo de 30 caracteres.

SNMP Version (Versión de SNMP): define la versión de SNMP asociada al grupo. Los valores del campo posibles son:

SNMPv1: el grupo tiene definida la versión SNMPv1.

SNMPv2: el grupo tiene definida la versión SNMPv2.

SNMPv3: el grupo tiene definida la versión SNMPv3.

Security Level (Nivel de seguridad): nivel de seguridad asociado al grupo. Los niveles de seguridad sólo se aplican a SNMPv3. Los valores del campo posibles son:

No Authentication (Sin autenticación): no se asigna al grupo ni el nivel de seguridad de autenticación ni el nivel de seguridad de privacidad.

Authentication (Autenticación): se autentican los mensajes SNMP y se garantiza la autenticación del origen de los mensajes SNMP.

Privacy (Privacidad): se cifra el mensaje SNMP.

Operation (Operación): define los derechos de acceso del grupo. Los valores del campo posibles son:

Read (Lectura): el acceso a la administración está restringido a sólo lectura, y no es posible realizar cambios en la vista de SNMP asignada.

Write (Escritura): el acceso a la administración es de lectura/escritura, y es posible realizar cambios en la vista de SNMP asignada.

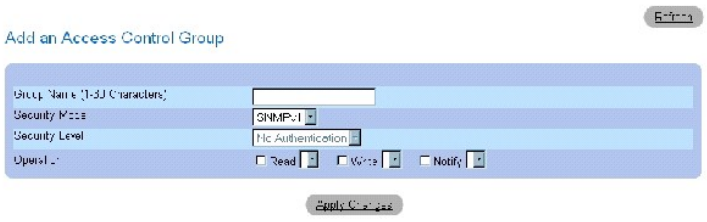
Notify (Notificar): se envían excepciones para la vista de SNMP asignada.

Definición de grupos SNMP

1. Abra la página Access Control Group (Grupo de control de acceso).
2. Haga clic en Add (Añadir).

Se abre la página **Add an Access Control Group** (Añadir grupo de control de acceso):

Figura 6-62. Add an Access Control Group



3. Defina los campos de la página Add an Access Control Group (Añadir grupo de control de acceso).
4. Haga clic en Apply Changes (Aplicar cambios).

Se añade el grupo y se actualiza el dispositivo.

Visualización de la tabla de accesos

1. Abra la página Access Control Group (Grupo de control de acceso).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **Access Table** (Tabla de accesos).

Figura 6-63. Access Table

Eliminación de grupos SNMP

1. Abra la página Access Control Group (Grupo de control de acceso).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **Access Table** (Tabla de accesos).

3. Seleccione un grupo SNMP.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en Apply Changes (Aplicar cambios).

Se elimina el grupo SNMP y se actualiza el dispositivo.

Definición del control de acceso de SNMP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir los campos de la página Access Control Group (Grupo de control de acceso).

Tabla 6-39. Comandos de la CLI para el control de acceso de SNMP

Comando de la CLI	Descripción
snmp-server group *nombregrupo* {**v1 | v2 | v3** {**noauth** | **auth** | **priv**}} [**read** *vistalectura*] [**write** *vistaescritura*] [**notify** *vistanotificar*]	Configura un nuevo grupo de protocolo simple de administración de red (SNMP) o una tabla que asigna usuarios de SNMP a vistas de SNMP.
show snmp groups [*nombregrupo*]	Muestra la configuración de los grupos.

A continuación se muestra un ejemplo de los comandos de la CLI:

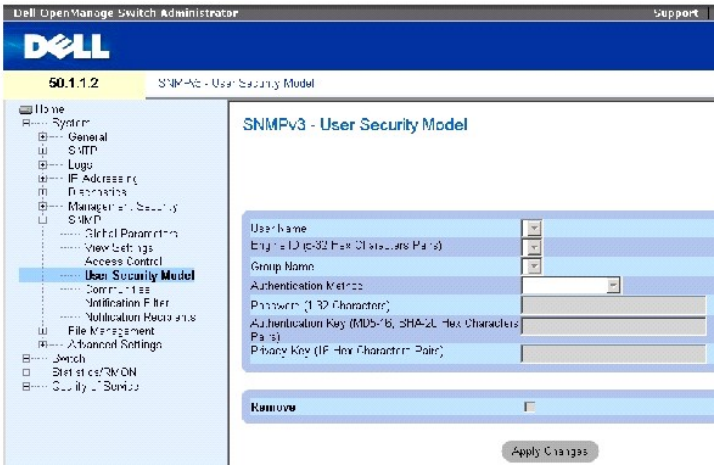
```
console (config)# snmp-
server group user-group v3
priv read user- view
```

Asignación de seguridad de usuarios de SNMP

La página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3) permite asignar usuarios del sistema a grupos SNMP y definir el método de autenticación de usuarios.

Para abrir la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3), haga clic en **System** (Sistema) → **SNMP** → **User Security Model** (Modelo de seguridad basado en el usuario) en la vista de árbol.

Figura 6-64. SNMPv3 User Security Model (USM)



La página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3) contiene los campos siguientes:

User Name (Nombre de usuario): contiene una lista de nombres de usuario definidos por el usuario. El valor de este campo puede tener un máximo de 30 caracteres alfanuméricos.

Engine ID (ID de motor): indica la entidad SNMP local o remota a la que está conectado el usuario. Si se cambia o se elimina la ID de motor de SNMP local, se elimina la base de datos de usuarios de SNMPv3.

Local: indica que el usuario está conectado a una entidad SNMP local.

Remote (Remota): indica que el usuario está conectado a una entidad SNMP remota. Si se define la ID de motor, los dispositivos remotos recibirán mensajes informativos.

Group Name (Nombre de grupo): contiene una lista de grupos SNMP definidos por el usuario. Los grupos SNMP se definen en la página Access Control Group (Grupo de control de acceso).

Authentication Method (Método de autenticación): método de autenticación utilizado para autenticar a los usuarios. Los valores del campo posibles son:

MD5 Key (Clave MD5): los usuarios se autentican mediante el algoritmo HMAC-MD5.

SHA Key (Clave SHA): los usuarios se autentican mediante el nivel de autenticación HMAC-SHA-96.

MD5 Password (Contraseña MD5): indica que se utiliza la contraseña HMAC-MD5-96 para la autenticación. El usuario debe introducir una contraseña.

SHA Password (Contraseña SHA): los usuarios se autentican mediante el nivel de autenticación HMAC-SHA-96. El usuario debe introducir una contraseña.

None (Ninguna): no se realiza autenticación del usuario.

Password **(0-32 Characters)** (Contraseña [0-32 caracteres]): modifica la contraseña definida por el usuario para un grupo. Las contraseñas pueden contener un máximo de 32 caracteres alfanuméricos.

Authentication Key (MD5-16; SHA-20 hexa chars) (Clave de autenticación [caracteres hexadecimales: 16 para MD5 y 20 para SHA]): define el nivel de autenticación HMAC-MD5-96 o HMAC-SHA-96. Las claves de autenticación y de privacidad se introducen para definir la clave de autenticación. Si sólo es necesaria la autenticación, se definen 16 bytes para MD5. Si son necesarias la privacidad y la autenticación, se definirán 32 bytes para MD5. Cada byte de la cadena de caracteres hexadecimales equivale a dos dígitos hexadecimales. Cada byte puede separarse mediante un punto o dos puntos.

Privacy Key (16 hexa characters) (Clave de privacidad [16 caracteres hexadecimales]): si sólo se requiere la autenticación, se definen 20 bytes. Si son necesarias la privacidad y la autenticación, se definen 16 bytes. Cada byte de la cadena de caracteres hexadecimales equivale a dos dígitos hexadecimales. Cada byte puede separarse mediante un punto o dos puntos.

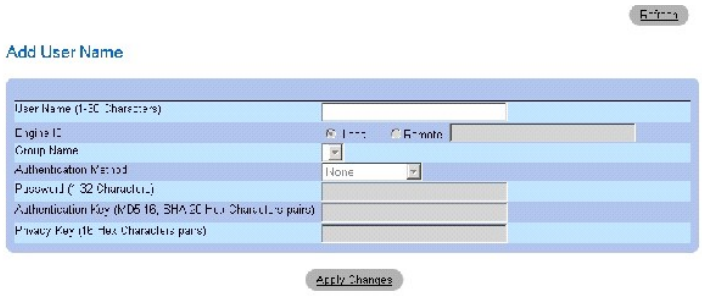
Remove (Eliminar): elimina usuarios de un grupo específico.

Adición de usuarios a un grupo

1. Abra la página SNMPv3 User Security Model (USM) (Modelo de seguridad basado en el usuario [USM] de SNMPv3).
2. Haga clic en Add (Añadir).

Se abre la página Add SNMPv3 User Name (Añadir nombre de usuario de SNMPv3):

Figura 6-65. Add SNMPv3 User Name



3. Defina los campos pertinentes.
4. Haga clic en Apply Changes (Aplicar cambios).

Se añade el usuario al grupo y se actualiza el dispositivo.

Visualización de la tabla de modelos de seguridad basados en el usuario

1. Abra la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **User Security Model Table** (Tabla de modelos de seguridad basados en el usuario).

Figura 6-66. User Security Model Table

Eliminación de una entrada de la tabla de modelos de seguridad basados en el usuario

1. Abra la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3).
2. Haga clic en Show All (Mostrar todo).

   Se abre la página **User Security Model Table** (Tabla de modelos de seguridad basados en el usuario).

3. Seleccione una entrada en la página **User Security Model Table** (Tabla de modelos de seguridad basados en el usuario).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en Apply Changes (Aplicar cambios).

   Se elimina la entrada de la página **User Security Model Table** (Tabla de modelos de seguridad basados en el usuario) y se actualiza el dispositivo.

Definición de usuarios de SNMPv3 mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir los campos de la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3).

Tabla 6-40. Comandos de la CLI para los usuarios de SNMPv3

Comando de la CLI	Descripción
snmp-server user *nombreusuario nombregrupo* [**remote** cadena- idmotor][**auth-md5** password | **auth-sha contraseña** | **auth-md5-key** *clave-des-md5* | **auth-sha-key** *clave-des- sha*]	Configura un nuevo usuario de SNMPv3.
show snmp users [*nombreusuario*]	Muestra la configuración de los usuarios.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console (config)# snmp-server user John user-group auth-md5 1234

console (config)# end

console# show snmp users
```

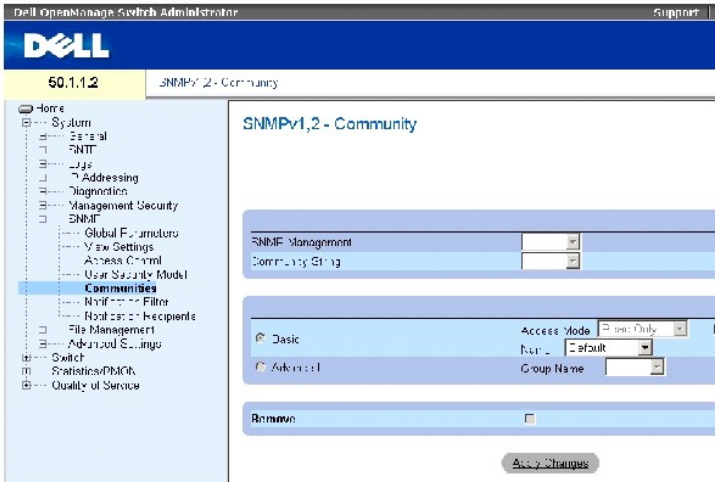
Name	Group Name	Auth Method	Remote
-------	----------	-----------	------

John	user-group	md5	

Definición de comunidades SNMP

Los derechos de acceso se administran mediante la definición de comunidades en la página **SNMPv1,2 Community** (Comunidad SNMP1 y SNMP2). Cuando se cambian los nombres de comunidad, también se cambian los derechos de acceso. Las comunidades SNMP se definen sólo para las versiones SNMPv1 y SNMPv2. Para abrir la página **SNMPv1,2 Community** (Comunidad SNMP1 y SNMP2), haga clic en **System** (Sistema) → **SNMP** → **Communities** (Comunidades) en la vista de árbol.

Figura 6-67. SNMPv1,2 Community



La página **SNMPv1,2 Community** **(Comunidad SNMP1 y SNMP2) contiene los campos siguientes:**

SNMP Management Station (Estación de administración SNMP): dirección IP de la estación de administración para la que se define la comunidad SNMP.

Community String (Cadena de comunidad): funciona como una contraseña y sirve para autenticar la estación de administración para el dispositivo.

Basic (Básico): activa el modo básico SNMP para una comunidad seleccionada. Los valores del campo posibles son:

Access Mode (Modo de acceso): define los derechos de acceso de la comunidad. Los valores del campo posibles son:

Read Only (Sólo lectura): el acceso a la administración está restringido a sólo lectura, y no es posible realizar cambios en la comunidad.

Read-Write (Lectura/escritura): el acceso a la administración es de lectura/escritura, y es posible realizar cambios en la configuración del dispositivo, pero no en la comunidad.

SNMP Admin (Administración SNMP): el usuario tiene acceso a todas las opciones de configuración del dispositivo, así como permisos para modificar la comunidad.

View Name (Nombre de la vista): contiene una lista de las vistas SNMP definidas por el usuario.

Name (Nombre): especifica el nombre de la comunidad utilizado para SNMPv1 y SNMPv2.

Advanced (Avanzado): contiene una lista de grupos definidos por el usuario. Cuando se selecciona el modo avanzado de SNMP, las reglas de control de acceso de SNMP que forman el grupo se activan para la comunidad seleccionada. El modo avanzado también activa grupos SNMP para comunidades SNMP específicas. El modo avanzado de SNMP sólo se define con SNMPv3. El valor del campo posible es:

Group Name (Nombre del grupo): especifica el nombre del grupo cuando se trabaja en el modo avanzado de SNMP.

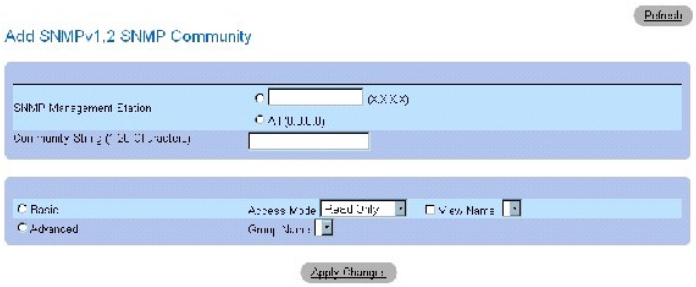
Remove (Eliminar): elimina una comunidad.

Definición de una nueva comunidad

1. Abra la página **SNMPv1,2 Community** (Comunidad SNMP1 y SNMP2).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add SNMP Community** (Añadir comunidad SNMP):

Figura 6-68. Add SNMP Community



3. Complete los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la nueva comunidad y se actualiza el dispositivo.

Eliminación de comunidades

1. Abra la página **SNMPv1,2 Community** (Comunidad SNMP1 y SNMP2).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Community Table** (Tabla de comunidades).

3. Seleccione una comunidad y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de comunidad y se actualiza el dispositivo.

Configuración de comunidades mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página **SNMPv1,2 Community** (Comunidad SNMPv1 y SNMPv2).

Tabla 6-41. Comandos de la CLI para las comunidades SNMP

Comando de la CLI	Descripción
snmp-server community *comunidad* [**ro** | **rw** | **su**] [*dirección- ip*][**view** *nombre- vista*]	Configura la cadena de acceso de la comunidad para permitir el acceso al protocolo SNMP.
snmp-server community-group *comunidad nombre- grupo* [*dirección-ip*]	Configura la cadena de acceso de la comunidad para permitir un acceso limitado al protocolo SNMP de acuerdo con los derechos de acceso del grupo.
show snmp	Muestra la configuración de dispositivo SNMP actual.

A continuación se muestra un ejemplo de los comandos de la CLI:

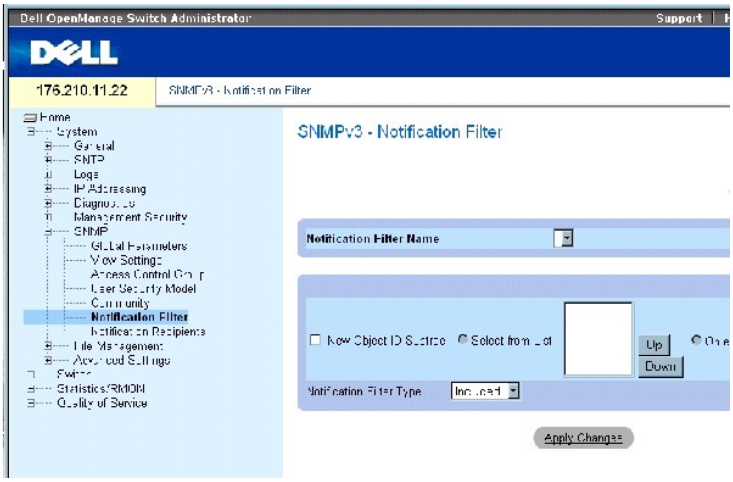
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Definición de filtros de notificación de SNMP

La página **Notification Filter** (Filtro de notificación) permite filtrar excepciones según las OID. Cada OID se enlaza a una función del dispositivo o a un aspecto de la función. La página **Notification Filter** (Filtro de administración) también permite a los administradores de red filtrar las notificaciones.

Para abrir la página **Notification Filter** (Filtro de notificación), haga clic en **System** (Sistema) → **SNMP** → **Notification Filters** (Filtros de notificación) en la vista de árbol.

Figura 6-69. Notification Filter



La página **Notification Filter** (Filtro de notificación) contiene los campos siguientes:

Notification Filter Name (Nombre del filtro de notificación): filtro de notificación definido por el usuario.

New Object Identifier Tree (Nuevo árbol de ID de objeto): ID de objeto para el que se envían o bloquean notificaciones. Si se asocia un filtro a una OID, se generan excepciones o informes que se envían a los destinatarios de excepciones. Las OID se seleccionan en *Select from List* (Lista de selección) o en *Object ID List* (Lista de ID de objeto).

Notification Filter Type (Tipo de filtro de notificación): indica si se envían informes o excepciones relativos a la OID a los destinatarios de excepciones.

Excluded (Exclusión): se restringe el envío de excepciones o informes de OID.

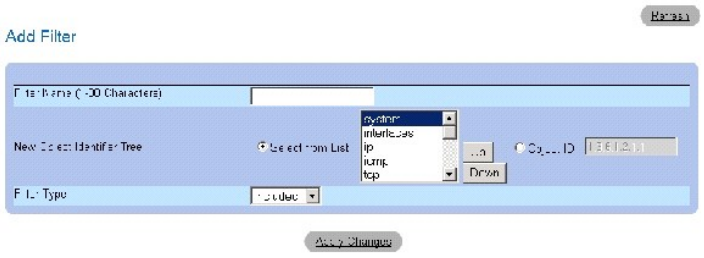
Included (Inclusión): se envían excepciones o informes de OID.

Adición de filtros de SNMP

1. Abra la página **Notification Filter** (Filtro de notificación).
2. Haga clic en Add (Añadir).

Se abre la página Add Filter (Añadir filtro):

Figura 6-70. Add Filter



3. Defina los campos pertinentes.
4. Haga clic en Apply Changes (Aplicar cambios).

Se añade el nuevo filtro y se actualiza el dispositivo.

Visualización de la tabla de filtros

1. Abra la página **Notification Filter** (Filtro de notificación).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **Filter Table** (Tabla de filtros).

Figura 6-71. Filter Table

Eliminación de un filtro

1. Abra la página **Notification Filter** (Filtro de notificación).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **Filter Table** (Tabla de filtros).

3. Seleccione una entrada en la página **Filter Table** (Tabla de filtros).
4. Seleccione la casilla de verificación **Remove** (Eliminar).

Se elimina la entrada del filtro y se actualiza el dispositivo.

Configuración de filtros de notificación mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir los campos de la página **Notification Filter** (Filtro de notificación).

Tabla 6-42. Comandos de la CLI para los filtros de notificación de SNMP

Comando de la CLI	Descripción
snmp-server filter nombre-filtro árbol- oid {**included** | **excluded**}	Crea o actualiza un filtro de notificación de SNMP.
show snmp filters [nombrefiltro]	Muestra la configuración de los filtros de notificación de SNMP.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# snmp-server filter user1 iso included

Console(config)# end

Console # show snmp filters

Name        OID Tree      Type
----------  ------------  --------
user1       iso           Included
```

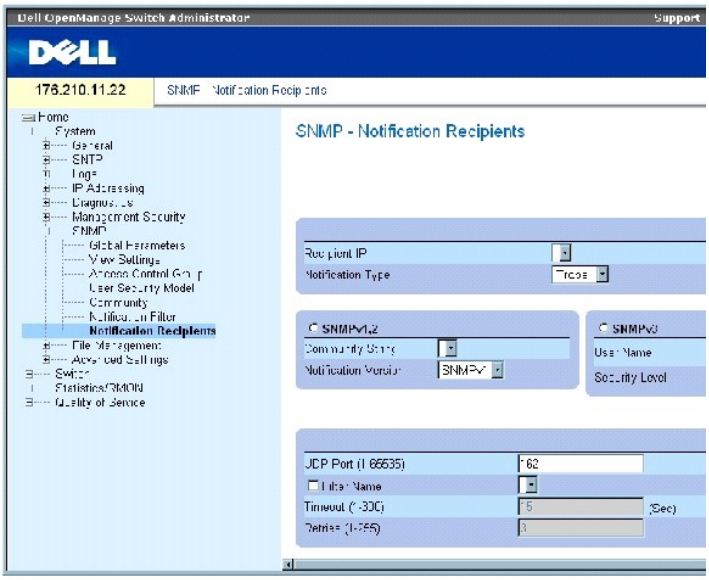
Definición de los destinatarios de notificaciones de SNMP

La página **Notification Recipients** (Destinatarios de notificaciones) contiene información para definir filtros que determinan si se envían excepciones a usuarios específicos y qué tipo de excepción se envía. Los filtros de notificación de SNMP proporcionan los servicios siguientes:

- Identificación de destinos de excepción de administración
- Filtrado de excepciones
- Selección de parámetros de generación de excepciones
- Comprobaciones de control de acceso

Para abrir la página **Notification Recipients** (Destinatarios de notificaciones), haga clic en **System** (Sistema) → **SNMP** → **Notification Recipients** (Destinatarios de notificaciones) en la vista de árbol.

Figura 6-72. Notification Recipients



La página **Notification Recipients** (Destinatarios de notificaciones) contiene los campos siguientes:

Recipient IP (IP del destinatario): dirección IP a la que se envían las excepciones.

Notification Type (Tipo de notificación): tipo de notificación enviada. Los valores del campo posibles son:

Trap (Excepción): se envían excepciones.

Inform (Informe): se envían informes.

SNMPv1,2: las versiones 1 y 2 de SNMP están activadas para el destinatario seleccionado. Defina los campos siguientes para SNMPv1 y SNMPv2:

Community String (1-20 Characters) (Cadena de comunidad [1-20 caracteres]): identifica la cadena de comunidad del administrador de excepciones.

Notification Version (Versión de notificación): determina el tipo de excepción. Los valores del campo posibles son:

SNMPV1: se envían excepciones de la versión 1 de SNMP.

SNMPV2: se envían excepciones de la versión 2 de SNMP.

SNMPv3: se utiliza SNMPv3 para enviar y recibir excepciones. Defina los campos siguientes para SNMPv3:

User Name (Nombre de usuario): usuario al que se envían las notificaciones de SNMP.

Security Level (Nivel de seguridad): medio por el que se autentica el paquete. Los valores del campo posibles son:

No Authentication (Sin autenticación): no se lleva a cabo la autenticación ni el cifrado del paquete.

Authentication (Autenticación): se realiza la autenticación del paquete.

Privacy (Privacidad): se realiza la autenticación y el cifrado del paquete.

UDP Port (1-65535) (Puerto UDP [1-65535]): puerto UDP utilizado para enviar notificaciones. El valor predeterminado es 162.

Filter Name (Nombre de filtro): incluye o excluye filtros de SNMP.

Timeout (1-300) (Tiempo de espera [1-300]): tiempo, en segundos, que el dispositivo espera antes de volver a enviar informes. El valor predeterminado es 15 segundos.

Retries (1-255) (Reintentos [1-255]): número de veces que el dispositivo vuelve a enviar una petición de informe. El valor predeterminado es 3.

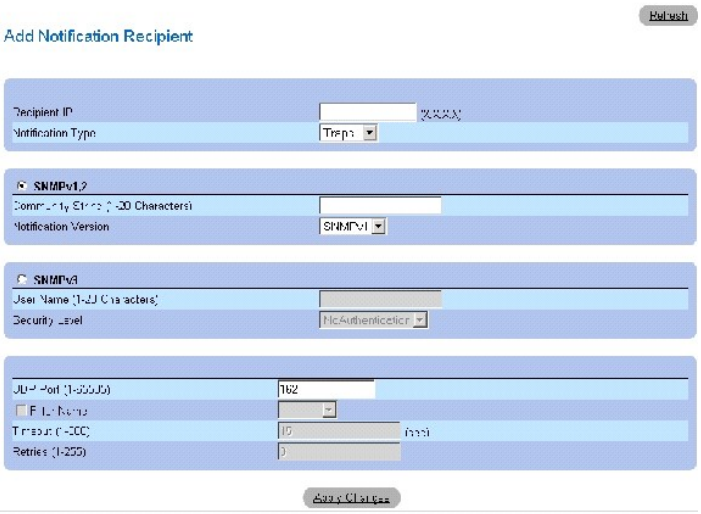
Remove Notification Recipient (Eliminar destinatario de notificaciones): elimina los destinatarios de notificaciones seleccionados.

Adición de un nuevo destinatario de excepciones

1. Abra la página **Notification Recipients** (Destinatarios de notificaciones).
2. Haga clic en Add (Añadir).

Se abre la página **Add Notification Recipients** (Añadir destinatarios de notificaciones):

Figura 6-73. Add Notification Recipients



3. Defina los campos pertinentes.
4. Haga clic en Apply Changes (Aplicar cambios).

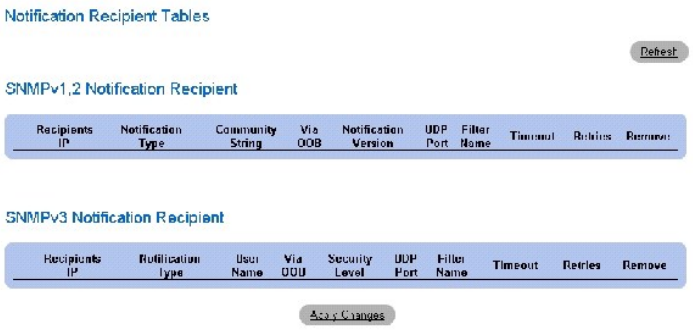
Se añade el destinatario de notificaciones y se actualiza el dispositivo.

Visualización de las tablas de destinatarios de notificaciones

1. Abra la página **Notification Recipients** (Destinatarios de notificaciones).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **Notification Recipients Tables** (Tablas de destinatarios de notificaciones):

Figura 6-74. Notification Recipients Tables



Eliminación de destinatarios de notificaciones

1. Abra la página **Notification Recipients** (Destinatarios de notificaciones).
2. Haga clic en Show All (Mostrar todo).

Se abre la página **Notification Recipients Tables** (Tablas de destinatarios de notificaciones).

3. Seleccione un destinatario de notificaciones en **SNMPV1,2 Notification Recipient** (Destinatario de notificaciones de SNMPV1,2) o en **SNMPv3 Notification Recipient Tables** (Tablas de destinatarios de notificaciones de SNMPv3).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en Apply Changes (Aplicar cambios).

Se elimina el destinatario y se actualiza el dispositivo.

Configuración de destinatarios de notificaciones de SNMP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página **Notification Recipients** **(Destinatarios de notificaciones).**

Tabla 6-43. Comandos de la CLI para las comunidades SNMP

Comando de la CLI	Descripción
snmp-server host {direcciónip | nombrehost} *cadena-comunidad* [**traps** | **informs**] [**1** | **2**] [**udp-port** puerto] [**filter** nombrefiltro] [**timeout** segundos] [**retries** reintentos]	Crea o actualiza un destinatario de notificaciones que recibe notificaciones en las versiones 1 o 2 de SNMP.
snmp-server v3-host {dirección-ip | nombrehost} *nombreusuario* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *puerto*] [**filter** nombrefiltro] [**timeout** segundos] [**retries** reintentos]	Crea o actualiza un destinatario de notificaciones que recibe notificaciones en la versión 3 de SNMP.
show snmp	Muestra la configuración de SNMP actual.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# snmp-server host 172.16.1.1
private


console(config)# end


console# show snmp
```

Community-String	Community-Access	View name	IP address
public	read only	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Administración de archivos

La página **File Management** (Administración de archivos) permite administrar el software del dispositivo, el archivo de imagen y los archivos de configuración. Los archivos pueden descargarse o cargarse a través de un servidor TFTP.

Información general sobre los archivos de administración

La estructura de los archivos de administración consta de los archivos siguientes:

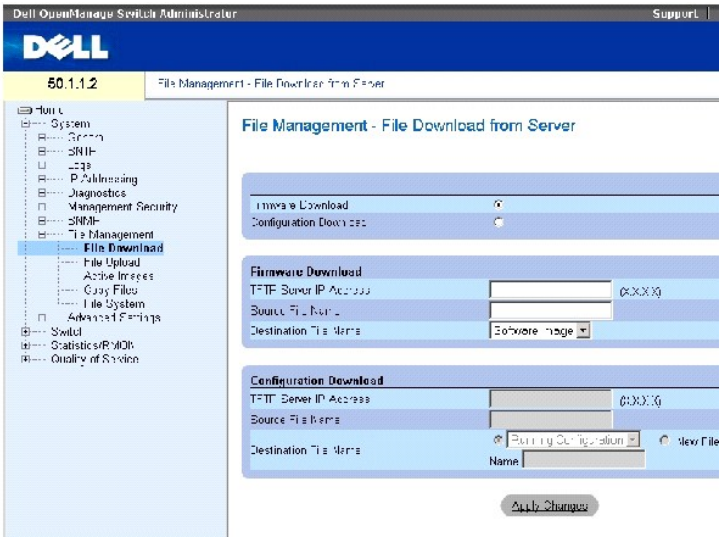
- Archivo de configuración de inicio: contiene los comandos necesarios parar configurar el dispositivo durante el inicio o después del reinicio. El archivo de configuración de inicio se crea copiando los comandos de configuración del archivo de configuración en ejecución o del archivo de configuración de copia de seguridad en el archivo de configuración de inicio.
- Archivo de configuración en ejecución: contiene todos los comandos del archivo de configuración de inicio y todos los comandos introducidos durante la sesión actual. Tras apagar o reiniciar el dispositivo, se pierden todos los comandos almacenados en el archivo de configuración en ejecución. Durante el proceso de inicio, todos los comandos del archivo de configuración de inicio se copian en el archivo de configuración en ejecución y se aplican al dispositivo. Durante la sesión, todos los comandos nuevos se añaden a los comandos ya existentes del archivo de configuración en ejecución. Para actualizar el archivo de configuración de inicio, antes de apagar el dispositivo, debe copiarse el archivo de configuración en ejecución en el archivo de configuración de inicio.
- Archivo de configuración de copia de seguridad: contiene una copia de seguridad de la configuración del dispositivo. Es posible guardar un máximo de cinco archivos de configuración de copia de seguridad en el dispositivo con nombres configurados por el usuario. Estos archivos se generan cuando el usuario copia el archivo de configuración en ejecución o el archivo de configuración de inicio en un archivo con un nombre asignado por el usuario. El contenido del archivo de configuración de copia de seguridad puede copiarse en el archivo de configuración en ejecución o en el archivo de configuración de inicio.
- Archivos de imagen: los archivos de imagen del sistema se guardan en dos archivos Flash denominados Image 1 e Image 2. La imagen activa almacena la copia activa, mientras que la otra imagen almacena una segunda copia. El dispositivo se inicia y se ejecuta desde la imagen activa. Si la imagen activa está dañada, el sistema arranca automáticamente desde la imagen no activa. Ésta es una función de seguridad contra fallos que tienen lugar durante el proceso de actualización de software.

Para abrir la página File Management (Administración de archivos), haga clic en System (Sistema) → File Management (Administración de archivos) en la vista de árbol.

Descarga de archivos

La página **File Download from Server** (Descarga de archivos del servidor) contiene campos para descargar archivos de imagen del sistema y de configuración del servidor TFTP al dispositivo. Para abrir la página **File Download from Server** (Descarga de archivos del servidor), haga clic en System (Sistema) → File Management (Administración de archivos) → File Download (Descarga de archivos) en la vista de árbol.

Figura 6-75. File Download from Server



La página **File Download from Server** (Descarga de archivos del servidor) contiene los campos siguientes:

Firmware Download (Descarga de firmware): se descarga el archivo de firmware. Si se selecciona **Firmware Download** (Descarga de firmware), se atenúan los campos de **Configuration Download** (Descarga de configuración).

Configuration Download (Descarga de configuración): se descarga el archivo de configuración. Si se selecciona **Configuration Download** (Descarga de configuración), se atenúan los campos de **Firmware Download** (Descarga de firmware).

Descarga de firmware

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP del que se descargan los archivos de firmware.

Source File Name (Nombre del archivo de origen): nombre del archivo que se va a descargar.

Destination File Name (Nombre del archivo de destino): tipo de archivo de destino en el que se va a descargar el archivo. Los valores del campo posibles son:

Software Image (Imagen de software): se descarga el archivo de imagen.

Boot Code (Código de inicio): se descarga el archivo de inicio.

Descarga de configuración

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP del que se descargan los archivos de configuración.

Source File Name (Nombre del archivo de origen): nombre del archivo de configuración que se va a descargar.

Destination File Name (Nombre del archivo de destino): archivo de destino en el que se va a descargar el archivo de configuración. Los valores del

campo posibles son:

Running Configuration (Configuración en ejecución): los comandos se descargan en el archivo de configuración en ejecución.

Startup Configuration (Configuración de inicio): se descarga el archivo de configuración de inicio y se sobrescribe.

User Defined Backup Configuration (Configuración de copia de seguridad definida por el usuario): se descarga el archivo de configuración de copia de seguridad definido por el usuario y se sobrescribe.

New File Name (Nombre del nuevo archivo): se descarga un nuevo archivo de configuración de copia de seguridad que puede especificarse como archivo de destino.

NOTA: el archivo de imagen sobrescribe la imagen no activa. Se recomienda especificar que la imagen no activa se convierta en activa después del reinicio y, a continuación, reiniciar el dispositivo tras la descarga.

Durante la descarga del archivo de imagen, aparece un cuadro de diálogo donde se muestra el progreso de la descarga. La ventana se cerrará automáticamente cuando se haya completado la descarga.

Descarga de archivos

1. Abra la página **File Download from Server** (Descarga de archivos del servidor).
2. Defina el tipo de archivo que va a descargar.
3. Defina los campos.
4. Haga clic en Apply Changes (Aplicar cambios).

Se descarga el software en el dispositivo.

NOTA: para activar el archivo de imagen seleccionado, reinicie el dispositivo. Para obtener información sobre cómo reiniciar el dispositivo, consulte "Cambio entre unidades maestras de la pila".

Descarga de archivos mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **File Download from Server** (Descarga de archivos del servidor).

Tabla 6-44. Comandos de la CLI para la descarga de archivos

Comando de la CLI	Descripción
copy url-origen url-destino	Copia un archivo de un origen a un destino.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# copy
tftp://10.6.6.64/pp.txt
startup-config



....!



Copy: 575 bytes copied in
00:00:06 [hh:mm:ss]



01-Jan-2000 06:41:55 %
```

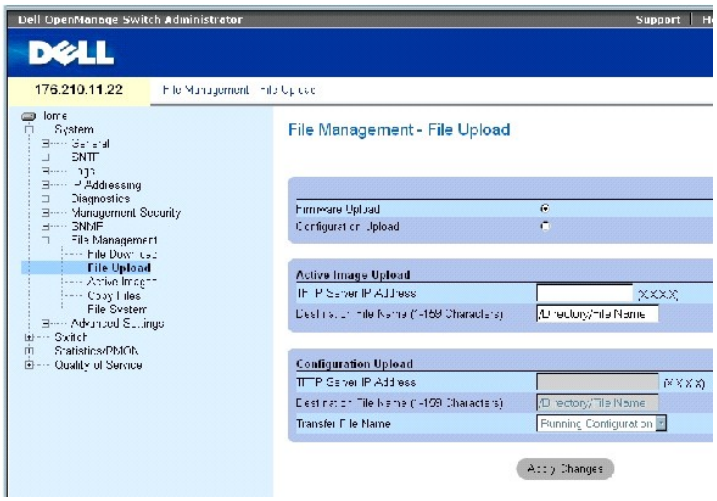
```
COPY-W-TRAP: The copy
operation was completed
successfully
```

NOTA: cada signo de exclamación (!) indica que se han transferido correctamente diez paquetes.

Carga de archivos

La página **File Upload to Server** (Carga de archivos en el servidor) contiene campos para cargar el software del dispositivo al servidor TFTP. La página **File Upload to Server** (Carga de archivos en el servidor) también permite cargar el archivo de imagen. Para abrir la página **File Upload to Server** (Carga de archivos en el servidor), haga clic en System (Sistema) → File Management (Administración de archivos) → File Upload (Carga de archivos) en la vista de árbol.

Figura 6-76. File Upload to Server



La página **File Upload to Server** (Carga de archivos en el servidor) contiene los campos siguientes:

Firmware Upload (Carga de firmware): se carga el archivo de firmware. Si se selecciona **Firmware Upload** (Carga de firmware), los campos de **Configuration Upload** (Carga de configuración) dejan de estar disponibles.

Configuration Upload (Carga de configuración): se carga el archivo de configuración. Si se selecciona **Configuration Upload** (Carga de configuración), los campos de **Active Image Upload**(Carga de imagen activa) dejan de estar disponibles.

Carga de imagen activa

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP en el que se carga la imagen de software.

Destination File Name (1-159 Characters) (Nombre del archivo de destino [1-159 caracteres]): indica la ruta del archivo de imagen de software en el que se carga el archivo.

Carga de configuración

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP en el que se carga el archivo de configuración.

Destination File Name (1-159 Characters) (Nombre del archivo de destino [1-159 caracteres]): indica la ruta del archivo de configuración en el que se carga el archivo.

Transfer File Name (Nombre del archivo de transferencia): archivo de software en el que se va a cargar la configuración. Los valores del campo posibles son:

Running Configuration (Configuración en ejecución): se carga el archivo de configuración en ejecución.

Startup Configuration (Configuración en ejecución): se carga el archivo de configuración de inicio.

List of User Defined Configuration Files (Lista de archivos de configuración definidos por el usuario): se carga un archivo de configuración definido por el usuario.

NOTA: la lista de archivos de configuración definidos por el usuario sólo aparece si el usuario ha creado archivos de configuración de copia de seguridad. Por ejemplo, si el usuario ha copiado el archivo de configuración en ejecución en un archivo de configuración definido por el usuario llamado BACKUP- SITE-1, dicha lista aparecerá en la página **File Upload to Server** (Descarga de archivos en el servidor) y el archivo de configuración BACKUP-SITE-1 aparecerá en la lista.

Carga de archivos

1. Abra la página **File Upload to Server** (Carga de archivos en el servidor).
2. Defina el tipo de archivo que va a cargar.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se carga el software en el servidor TFTP.

Carga de archivos mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **File Upload to Server** (Carga de archivos en el servidor).

Tabla 6-45. Comandos de la CLI para la carga de archivos

Comando de la CLI	Descripción
copy url-origen url-destino	Copia un archivo de un origen a un destino.

A continuación se muestra un ejemplo de los comandos de la CLI:

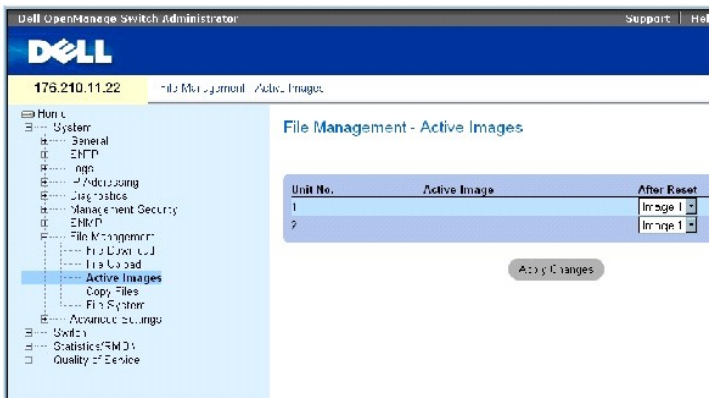
```
console# copy image tftp://10.6.6.64/uploaded.ros

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully
```

Activación de archivos de imagen

La página **Active Images** (Inmágenes activas) permite a los administradores de red seleccionar y restablecer los archivos de imagen. Es posible seleccionar por separado el archivo de imagen activa para cada unidad de una configuración de apilamiento. Para abrir la página **Active Images** (Imágenes activas), haga clic en System (Sistema) → File Management (Administración de archivos) → Active Images (Imágenes activas) en la vista de árbol.

Figura 6-77. Active Images



La página **Active Images** (Imágenes activas) contiene los campos siguientes:

Unit No. (N° de unidad): número de la unidad cuyo archivo de imagen se ha seleccionado.

Active Image (Imagen activa): archivo de imagen que está activo en la unidad.

After Reset (Después del restablecimiento): archivo de imagen que está activo en la unidad después de restablecer el dispositivo. Los valores del campo posibles son:

Image 1 (Imagen 1): activa el archivo de imagen 1 después de restablecer el dispositivo.

Image 2 (Imagen 2): activa el archivo de imagen 2 después de restablecer el dispositivo.

Selección de un archivo de imagen:

1. Abra la página **Active Images** (Imágenes activas).
2. Seleccione un archivo de imagen para una unidad específica en el campo **After Reset** (Después del restablecimiento).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona el archivo de imagen. El archivo de imagen vuelve a cargarse únicamente después del siguiente restablecimiento. El archivo de imagen seleccionado actualmente continúa ejecutándose hasta el siguiente restablecimiento del dispositivo.

Operaciones con el archivo de imagen activa mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para ver los campos de la página **Active Images** (Imágenes activas).

Tabla 6-46. Comandos de la CLI para la carga de archivos

Comando de la CLI	Descripción
boot system [**unit** | *unidad*] {**image-1** | **image-2**}	Indica la imagen del sistema que el dispositivo carga durante el inicio.
show version [**unit** *unidad*]	Muestra información de la versión del sistema.

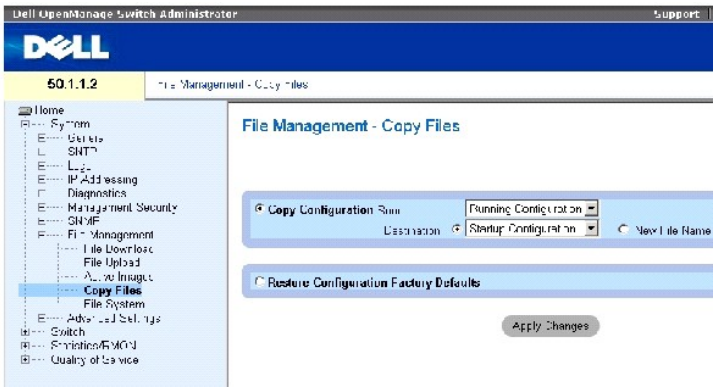
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console# boot system
image-1
```

Copia de archivos

Los archivos pueden copiarse y eliminarse desde la página **Copy Files** (Copiar archivos). Para abrir la página **Copy Files** (Copiar archivos), haga clic en System (Sistema) → File Management (Administración de archivos) → Copy Files (Copiar archivos) en la vista de árbol.

Figura 6-78. Copy Files



La página **Copy Files** (Copiar archivos) contiene los campos siguientes:

Copy Configuration (Copiar configuración): se copia el archivo de configuración en ejecución, de inicio o de copia de seguridad del archivo maestro al archivo de destino.

Source (Origen): indica el tipo de archivo que va a copiarse en el archivo de destino. Seleccione el archivo de configuración en ejecución, el archivo de configuración de inicio o uno de los archivos de configuración de copia de seguridad definidos por el usuario.

Destination (Destino): indica el archivo de configuración de destino en el que se va a copiar el archivo de origen. Los archivos no se pueden copiar en el archivo de copia de seguridad del maestro de copias de seguridad. Los archivos de copia de seguridad aparecen en el campo **Destination Unit** (Unidad de destino) sólo si se han definido archivos de copia de seguridad. Seleccione la casilla de verificación New File Name (Nombre del nuevo archivo) e indique el nombre del nuevo archivo para copiar el archivo de origen en un archivo de configuración de copia de seguridad nuevo.

New File Name (Nombre del nuevo archivo): indica el nombre del archivo de configuración de copia de seguridad recién creado.

Restore Configuration Factory Defaults (Restaurar configuración predeterminada de fábrica): se indica que debe sustituirse la configuración actual por la configuración predeterminada de fábrica. Si no se selecciona este campo, se indica que la configuración actual no debe modificarse.

Copia de archivos

1. Abra la página **Copy Files** (Copiar archivos).
2. Defina los campos **Source** (Origen) y **Destination** (Destino).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se copia el archivo y se actualiza el dispositivo.

Restauración de la configuración predeterminada de fábrica

1. Abra la página **Copy Files** (Copiar archivos).
2. Haga clic en **Restore Configuration Factory Defaults** (Restaurar configuración predeterminada de fábrica).
3. Haga clic en Apply Changes (Aplicar cambios).

Se restaura la configuración predeterminada de fábrica y se actualiza el dispositivo.

Copia y eliminación de archivos mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Copy Files** (Copiar archivos).

Tabla 6-47. Comandos de la CLI para la copia de archivos

Comando de la CLI	Descripción
copy *url-origen url-destino*	Copia un archivo de un origen a un destino.
delete startup-config	Elimina el archivo de configuración de inicio.

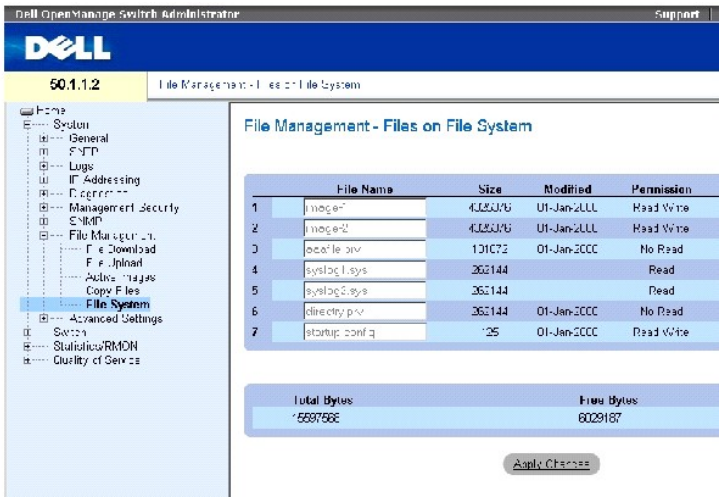
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# delete startup-
config


Startup file was deleted


console#


console# copy running-
config startup-config


01-Jan-2000 06:55:32 %
COPY-W-TRAP: The copy
operation was completed
successfully


Copy succeeded


console#
```

Administración de archivos del dispositivo

La página Files on File System (Archivos del sistema de archivos) proporciona información sobre los archivos almacenados actualmente en el sistema, incluidos los nombres, tamaños, modificaciones y permisos de archivo. El sistema de archivos permite administrar un máximo de cinco archivos y un tamaño de archivo total de 3 MB. Para abrir la página Files on File System (Archivos del sistema de archivos), haga clic en System (Sistema) → File Management (Administración de archivos) → File System (Sistema de archivos) en la vista de árbol.

Figura 6-79. Files on File System



La página Files on File System (Archivos del sistema de archivos) contiene los campos siguientes:

File Name (Nombre de archivo): indica el archivo que está almacenado actualmente en el sistema de administración de archivos.

Size (Tamaño): indica el tamaño del archivo.

Modified (Modificado): indica la fecha de la última modificación del archivo.

Permission (Permiso): indica el tipo de permiso asignado al archivo. Los valores del campo posibles son:

Read Only (Sólo lectura): indica que se trata de un archivo de sólo lectura.

Read Write(Lectura/escritura): indica que se trata de un archivo de lectura/escritura.

Remove (Eliminar): elimina el archivo.

Rename (Cambiar nombre): permite cambiar el nombre del archivo. El nombre de archivo se cambia en el campo **File Name** (Nombre de archivo).

Total Bytes (Total de bytes): indica la cantidad total de espacio utilizado actualmente.

Free Bytes (Bytes libres): indica la cantidad total de espacio libre actualmente.

Administración de archivos mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para administrar los archivos de sistema.

Tabla 6-48. Comandos de la CLI para la copia de archivos

Comando de la CLI	Descripción
dir	Muestra una lista de archivos en un sistema de archivos Flash.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# dir

Directory of flash:

File Name       Permis-sion  Flash Size  Data Size  Modified
--------------  ------       ------      ------     ----------------
3.txt           rw           524288      523776     22-Feb-2005 18:49:27
setup           rw           524288      95         22-Feb-2005 15:58:19
setup2          rw           524288      95         22-Feb-2005 15:58:35
image-1         rw           4325376     4325376    06-Feb-2005 17:55:32
image-2         rw           4325376     4325376    06-Feb-2005 17:55:31
test.txt        rw           524288      95         22-Feb-2005 12:16:44
aaafile.prv     --           131072      --         06-Feb-2005 19:09:02
syslog1.sys     r-           262144      --         22-Feb-2005 18:49:27
syslog2.sys     r-           262144      --         22-Feb-2005
```

				18:49:27
directory.prv	--	262144	--	06-Feb-2005 17:55:31
startup-config	rw	524288	347	22-Feb-2005 11:56:03
Total size of flash: 16646144 bytes				
Free size of flash: 4456448 bytes				

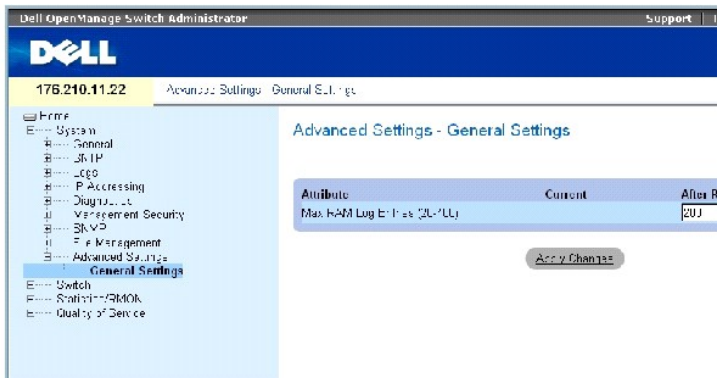
Configuración de los valores generales

Utilice la configuración avanzada para establecer diversos atributos globales del conmutador. Los cambios realizados en estos atributos se aplican sólo después de restablecer el conmutador. Haga clic en **System** (Sistema) → **Advanced Settings** (Configuración avanzada) en la vista de árbol para abrir la página **Advanced Settings** (Configuración avanzada).

La página **Advanced Settings** (Configuración avanzada) contiene un enlace para configurar los valores generales.

La página **General Settings** (Configuración general) proporciona información para definir parámetros generales del dispositivo. Para abrir la página **General Settings** (Configuración general), haga clic en System (Sistema) → Advanced Settings (Configuración avanzada) → General Settings (Configuración general) en la vista de árbol.

Figura 6-80. General Settings



La página **General Settings** (Configuración general) contiene la información siguiente:

Attribute (Atributo): atributo de configuración general.

Current (Actual): valor configurado actualmente.

After Reset (Después del restablecimiento): valor futuro (tras el restablecimiento). Cuando se introduce un valor en la columna After Reset (Después del restablecimiento), se asigna memoria a la tabla de campos.

Max RAM Log Entries (20-400) (Entradas máximas de registros de RAM [20-400]): número máximo de entradas de registro de RAM. Cuando las entradas de registro están llenas, se borra el registro y se reinicia el archivo de registro.

Visualización del contador de entradas de registro de RAM mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **General Settings** (Configuración general).

Tabla 6-49. Comandos de la CLI para la configuración general

Comando de la CLI	Descripción
logging buffered size número	Establece el número de mensajes Syslog almacenados en el búfer interno (RAM).

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# logging
buffered size 300
```

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la información del conmutador

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

En esta sección se describe el funcionamiento del sistema y se incluye información general sobre cómo configurar la seguridad de la red, puertos, tablas de direcciones, el protocolo GARP, redes VLAN, el árbol de extensión, el agregado de puertos y la compatibilidad con multidifusión.

Configuración de la seguridad de la red

Utilice la página **Network Security** (Seguridad de la red) para configurar la seguridad de la red a través de listas de control de acceso y de puertos bloqueados. Para abrir la página **Network Security** (Seguridad de la red), seleccione **Switch** (Conmutador)→ **Network Security** (Seguridad de la red).

Autenticación basada en el puerto

La autenticación basada en el puerto permite autenticar los usuarios del sistema en cada puerto a través de un servidor externo. Únicamente los usuarios autenticados y aprobados por el sistema pueden transmitir y recibir datos. Los puertos se autentican a través del servidor RADIUS mediante el protocolo de autenticación extensible (EAP). La autenticación de puerto incluye:

- **Authenticators** (Autenticadores): especifica el puerto de dispositivo que se autentica antes de permitir el acceso al sistema.
- **Supplicants** (Suplicadores): especifica el host conectado al puerto autenticado que solicita acceso a los servicios del sistema.
- **Authentication Server** (Servidor de autenticación): especifica el servidor externo, por ejemplo, el servidor RADIUS que realiza la autenticación en nombre del autenticador e indica si el suplicador puede acceder a los servicios del sistema.

La autenticación basada en el puerto crea dos estados de acceso:

- **Controlled Access** (Acceso controlado): permite la comunicación entre el suplicador y el sistema, si el suplicador está autorizado.
- **Uncontrolled Access** (Acceso no controlado): permite la comunicación no controlada independientemente del estado del puerto.

Actualmente, el dispositivo admite la autenticación basada en el puerto a través de servidores RADIUS.

Autenticación avanzada basada en el puerto

La autenticación avanzada basada en el puerto:

- Permite conectar varios hosts a un único puerto.
- Requiere la autorización de un único host para que todos los hosts tengan acceso al sistema. Si el puerto no está autorizado, se denegará el acceso a la red a todos los hosts conectados al mismo.
- Permite la autenticación basada en el usuario. Siempre hay unas redes VLAN específicas del dispositivo disponibles, aun cuando puertos determinados conectados a la VLAN no estén autorizados.
- Por ejemplo, el tráfico de voz sobre IP no requiere autenticación, mientras que con el tráfico de datos ocurre lo contrario. Pueden definirse las redes VLAN para las que no se necesita autorización. Hay redes VLAN no autenticadas disponibles para los usuarios, aun cuando los puertos conectados a la VLAN estén definidos como autorizados.

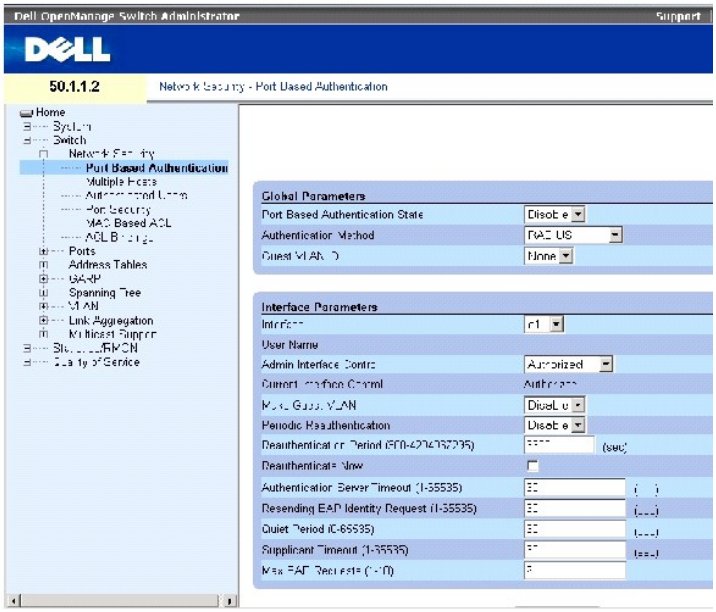
La autenticación avanzada basada en el puerto se implementa en los modos siguientes:

- **Single Host Mode** (Modo de un único host): el puerto autorizado es el único que tiene acceso al puerto.
- **Multiple Host Mode** (Modo de varios hosts): es posible conectar varios hosts a un único puerto. Sólo debe haber un host autorizado para que todos los hosts tengan acceso a la red. Si la autenticación del host falla, o si se recibe un mensaje de cierre de sesión EAPOL, se denegará el acceso a la red a todos los clientes conectados.
- **Guest VLANs** (Redes VLAN invitadas): proporciona acceso a la red limitado autorizado a los puertos. Si se deniega el acceso a la red a un puerto a través de la autorización basada en el puerto, pero la VLAN invitada está activada, el puerto recibe acceso limitado a la red. Por ejemplo, un administrador de la red puede utilizar redes VLAN invitadas para denegar el acceso a la red a través de la autenticación basada en el puerto, pero otorgar acceso a Internet a usuarios no autorizados.

Configuración de la autenticación basada en el puerto

La página Port Based Authentication (Autenticación basada en el puerto) permite a los administradores de red configurar la autenticación basada en el puerto. Para abrir la página Port Based Authentication (Autenticación basada en el puerto), haga clic en **Switch** (Conmutador) → **Network Security** (Seguridad de la red) → **Port Based Authentication** (Autenticación basada en el puerto).

Figura 7-1. Port Based Authentication



La página Port Based Authentication (Autenticación basada en el puerto) contiene los campos siguientes:

Port Based Authentication State (Estado de la autenticación basada en el puerto): permite realizar la autenticación basada en el puerto en el dispositivo. Los valores del campo posibles son:

Enable (Activar): activa la autenticación basada en el puerto en el dispositivo.

Disable (Desactivar): desactiva la autenticación basada en el puerto en el dispositivo.

Authentication Method (Método de autenticación): indica el método de autenticación utilizado. Los valores del campo posibles son:

None (Ninguno): indica que no se utiliza ningún método para autenticar el puerto.

RADIUS: indica que la autenticación del puerto se realiza a través del servidor RADIUS.

RADIUS, None (RADIUS, Ninguno): indica que la autenticación del puerto se realiza primero a través del servidor RADIUS. Si el puerto no está autenticado, no se utiliza ningún método de autenticación y se permite la sesión.

Guest VLAN (VLAN invitada): permite utilizar una VLAN invitada para puertos no autorizados. Si se activa el uso de una VLAN invitada, el puerto no autorizado se une automáticamente a la VLAN seleccionada en el campo **VLAN List** (Lista de VLAN). De forma predeterminada, el uso de esta red está desactivado.

Interface (Interfaz): contiene una lista de las interfaces para las que se ha activado la autenticación basada en el puerto.

User Name (Nombre de usuario): indica el nombre de usuario del suplicador.

Admin Interface Control (Control de la interfaz del administrador): define el estado de autorización del puerto. Los valores del campo posibles son:

Auto (Automático): activa la autenticación basada en el puerto en el dispositivo. La interfaz pasa del estado de autorización al estado de no autorización en función del intercambio de autenticación entre el dispositivo y el cliente.

Authorized (Autorizada): sitúa a la interfaz en un estado de autorización sin que se haya autenticado. La interfaz vuelve a enviar y recibe tráfico normal sin la autenticación basada en el puerto del cliente.

Unauthorized (No autorizada): deniega a la interfaz seleccionada el acceso al sistema situándola en el estado de no autorización. El dispositivo no puede proporcionar servicios de autenticación al cliente a través de la interfaz.

Current Interface Control (Control de la interfaz actual): indica el estado de autorización del puerto actual.

Make Guest VLAN (Establecer VLAN invitada): si se habilita esta opción, indica que los usuarios no autorizados conectados a esta interfaz pueden acceder a la VLAN invitada.

Periodic Reauthentication (Reautenticación periódica): permite volver a autenticar el puerto de forma inmediata.

Reauthentication Period (300-4294967295) (Periodo de reautenticación [300-4294967295]): indica el lapso de tiempo en el que se vuelve a autenticar el puerto. El valor del campo se expresa en segundos. El valor predeterminado del campo es 3600 segundos.

Reauthenticate Now (Volver a autenticar ahora): si se selecciona esta opción, permite volver a autenticar el puerto de forma inmediata.

Authentication Server Timeout (1-65535) (Tiempo de espera del servidor de autenticación [1-65535]): define el tiempo que transcurre antes de que el dispositivo vuelva a enviar una petición al servidor de autenticación. El valor del campo se expresa en segundos. El valor predeterminado del campo es 30 segundos.

Resending EAP Identity Request (1-65535) (Reenvío de la petición de identidad EAP [1-65535]): define el tiempo que transcurre antes de enviar de nuevo la petición EAP. El valor predeterminado del campo es 30 segundos.

Quiet Period (0-65535) (Periodo de silencio [0-65535]): indica el número de segundos durante los que el dispositivo permanece en estado de silencio después de un intercambio de autenticación fallido. El intervalo de valores posibles de este campo es 0-65535 y el valor predeterminado es 60 segundos.

Supplicant Timeout (1-65535) (Tiempo de espera del suplicador [1-65535]): indica el tiempo que transcurre antes de volver a enviar las peticiones EAP al suplicador. El valor del campo se expresa en segundos. El valor predeterminado del campo es 30 segundos.

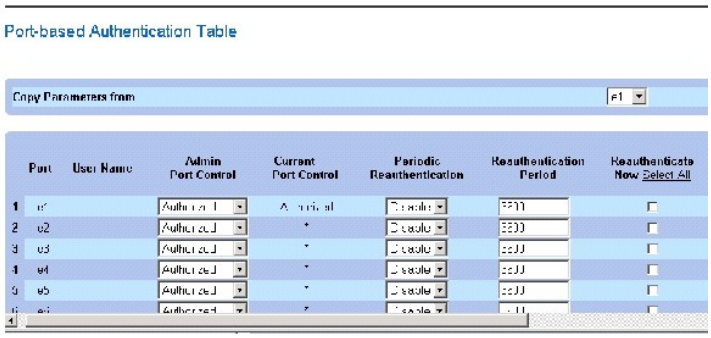
Max EAP Requests (1-10) (Número máximo de peticiones EAP [1-10]): indica el número total de peticiones EAP enviadas. Si no se recibe ninguna respuesta después del periodo definido, se reinicia el proceso de autenticación. El valor predeterminado del campo es 2 reintentos.

Visualización de la tabla de autenticación basada en el puerto

1. Abra la página Port Based Authentication (Autenticación basada en el puerto).
2. Haga clic en Show All (Mostrar todo).

Se abre la tabla de autenticación basada en el puerto:

Figura 7-2. Port Based Authentication Table



Además de los campos de la página de autenticación basada en el puerto, la tabla de autenticación basada en el puerto (**Port Based Authentication Table**) también muestra estos campos:

Unit No. (Número de unidad): selecciona un miembro de apilamiento.

Copy Parameters from Port No. (Copiar parámetros del puerto número): copia los parámetros del puerto seleccionado.

Copia de parámetros en la tabla de autenticación basada en el puerto (Port Based Authentication Table)

1. Abra la página.
2. Haga clic en Show All (Mostrar todo).

Se abre la tabla de autenticación basada en el puerto (**Port Based Authentication Table**).

3. Seleccione una interfaz en el campo **Copy Parameters from Port No.** (Copiar parámetros del puerto número).
4. Seleccione una interfaz en la tabla de autenticación basada en el puerto (**Port Based Authentication Table**).
5. Active la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que se copiarán los parámetros de la autenticación basada en el puerto.
6. Haga clic en Apply Changes (Aplicar cambios).

Activación de la autenticación basada en el puerto mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para activar la autenticación basada en el puerto de la tabla Port Based Authentication (Autenticación basada en el puerto).

Tabla 7-1. Comandos de la CLI para la autenticación de puertos

Comando de la CLI	Descripción
aaa authentication dot1x default *método1* [*método2*.]	Especifica uno o más métodos de autenticación, autorización y contabilidad (AAA) que deberán utilizarse en las interfaces que ejecuten IEEE 802.1X.
dot1x max-req *número*	Establece el número máximo de veces que el dispositivo envía una petición EAP al cliente antes de reiniciar el proceso de autenticación.

dot1x re-authenticate [**ethernet** *interfaz*]	Inicia manualmente una reautenticación de todos los puertos habilitados para 802.1X o del puerto habilitado para 802.1X especificado.
dot1x re-authentication	Activa la reautenticación periódica del cliente.
dot1x timeout quiet-period segundos	Establece el número de segundos durante los que el dispositivo permanece en estado de silencio después de un intercambio de autenticación fallido.
dot1x timeout re-authperiod *segundos*	Establece el número de segundos que transcurren entre los intentos de reautenticación.
dot1x timeout server-timeout *segundos*	Establece el tiempo para la retransmisión de paquetes al servidor de autenticación.
dot1x timeout supp-timeout *segundos*	Establece el tiempo para la retransmisión de una trama de peticiones EAP al cliente.
dot1x timeout tx-period *segundos*	Establece el número de segundos durante los que el dispositivo espera una respuesta a una trama de peticiones/identificación EAP del cliente antes de volver a enviar la petición.
show dot1x [ethernet *interfaz*]	Muestra el estado de 802.1X para el dispositivo o para la interfaz especificada.
show dot1x users [nombre_usuario nombre_usuario]	Muestra los usuarios de 802.1X para el dispositivo.
dot1x guest-vlan enable	Permite utilizar una VLAN invitada para puertos no autorizados. Si se activa el uso de una VLAN invitada, el puerto no autorizado se une automáticamente a la VLAN seleccionada en el campo **VLAN List** (Lista de VLAN). De forma predeterminada, el uso de esta red está desactivado.
dot1x guest-vlan	Contiene una lista de las redes VLAN. La VLAN invitada se selecciona en **VLAN List** (Lista de VLAN).

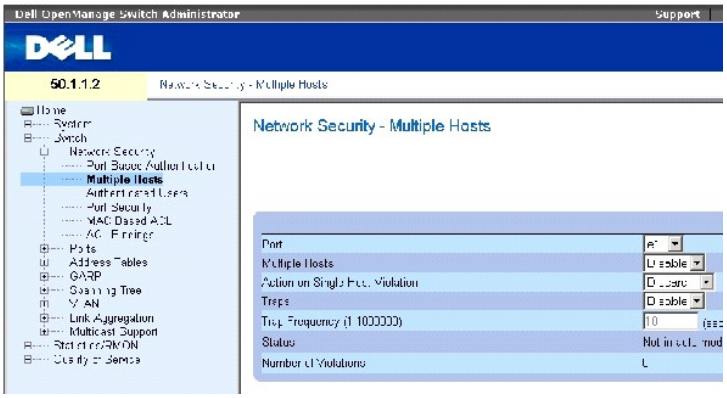
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console# show dot1x

Interface  Admin Mode  Oper Mode     Reauth Control  Reauth Period  Username
---------  ----------  ----------    --------------  -------------  --------
1/e1       Auto        Authorized    Ena             3600           Bob
1/e2       Auto        Authorized    Ena             3600           John
1/e3       Auto        Unauthorized  Ena             3600           Clark
1/e4       Force-auth  Authorized    Dis             3600           n/a
```

Configuración de la autenticación avanzada basada en el puerto

La página **Multiple Hosts** (Varios hosts) proporciona información para definir valores avanzados de la autenticación basada en el puerto para puertos y redes VLAN específicos. Para obtener más información sobre la autenticación avanzada basada en el puerto, consulte la sección **Autenticación avanzada basada en el puerto**. Para abrir la página **Multiple Hosts** (Varios hosts), haga clic en Switch (Conmutador) → Network Security (Seguridad de la red) → Multiple Hosts (Varios hosts).

Figura 7-3. Multiple Hosts



La página **Multiple Hosts** (Varios hosts) **contiene los campos siguientes:**

Port (Puerto): número de puerto para el que se activa la autenticación avanzada basada en el puerto.

Multiple Hosts (Varios hosts): activa o desactiva un único host para autorizar varios hosts para el acceso al sistema. Este valor debe activarse para desactivar el filtro de entrada o para utilizar la seguridad de bloqueo de puerto en el puerto seleccionado.

Action on Single Host Violation (Acción tras infracción de un único host): define la acción que debe aplicarse en los paquetes que llegan en modo de un único host, desde un host cuya dirección MAC no es la dirección MAC del cliente (suplicador). Los valores del campo posibles son:

Forward (Reenviar): reenvía los paquetes de origen desconocido; sin embargo, la dirección MAC no se obtiene.

Discard (Descartar): descarta los paquetes de cualquier origen no obtenido. Éste es el valor predeterminado.

Shutdown (Apagar): descarta los paquetes de cualquier origen no obtenido y bloquea el puerto. Los puertos permanecen apagados hasta que se activan, o hasta que se restablece el conmutador.

Traps (Excepciones): activa o desactiva el envío de excepciones al host si se produce una infracción.

Trap Frequency (1-1000000) (Sec) (Frecuencia de excepciones [1-1000000] [seg.]): define el periodo de tiempo que rige el envío de excepciones al host. El campo **Trap Frequency (1-1000000)** (Frecuencia de excepciones [1-1000000]) sólo puede definirse si el valor del campo **Multiple Hosts** (Varios hosts) es **Disable** (Desactivar). El valor predeterminado es 10 segundos.

Status (Estado): indica el estado del host. Los valores del campo posibles son:

Unauthorized (No autorizado): indica que el control de puerto es *Force Unauthorized* (Forzar no autorizado), el enlace de puerto está inactivo o el control de puerto es Auto, pero que no se ha autenticado ningún cliente a través del puerto.

Not in Auto Mode (No en modo automático): indica que el control de puerto es *Forced Authorized* (Forzar autorizado) y que los clientes tienen acceso completo al puerto.

Single-host Lock (Bloqueo de un único host): indica que el control de puerto es *Auto* y que se ha autenticado un solo cliente a través del puerto.

No Single Host (No host único): indica que la opción activada es Multiple Host (Varios hosts).

Number of Violations (Número de infracciones): indica el número de paquetes que ha llegado a la interfaz en modo de un único host desde un host cuya

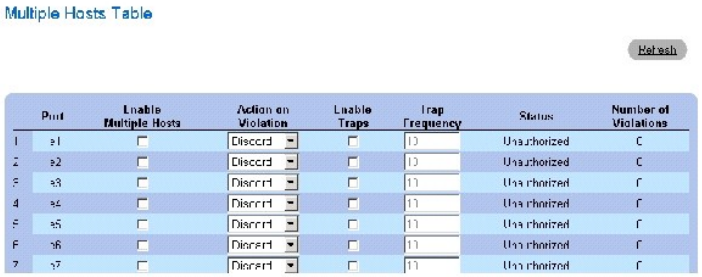
dirección MAC no es la dirección MAC del cliente (suplicador).

Visualización de la página Multiple Hosts Table (Tabla de varios hosts)

1. Abra la página **Multiple Hosts** (Varios hosts).
2. Haga clic en Show All (Mostrar todo).

Se abre la tabla de varios hosts (**Multiple Hosts Table**).

Figura 7-4. Multiple Hosts Table



Activación de la opción Multiple Hosts (Varios hosts) mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para activar la autenticación avanzada basada en el puerto que se muestra en la página **Multiple Hosts** (Varios hosts).

Tabla 7-2. Comandos de la CLI para varios hosts

Comando de la CLI	Descripción
dot1x multiple-hosts	Permite varios hosts (clientes) en un puerto autorizado por 802.1X cuyo comando de configuración de la interfaz dot1x port-control está establecido en auto.
dot1x single-host-violation {forward |discard |discard-shutdown}[trap segundos]	Configura la acción que debe llevarse a cabo cuando una estación cuya dirección MAC no es la dirección MAC del cliente (suplicador) intenta acceder a la interfaz.

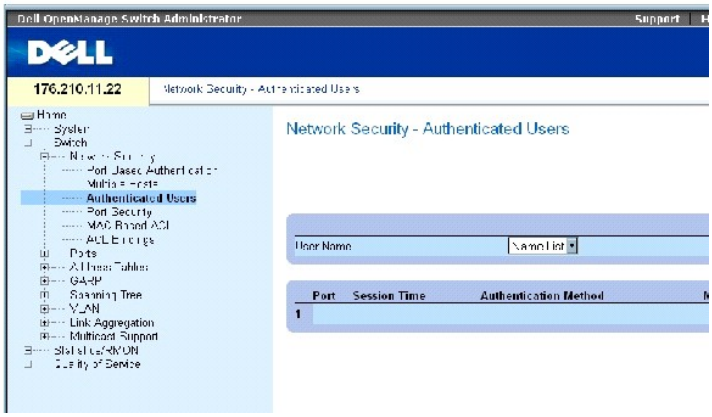
A continuación se muestra un ejemplo de comandos de la CLI.

```
Console(config)# interface
ethernet 1/e1


Console(config-if)# dot1x
multiple-hosts
```

Autenticación de usuarios

La página Authenticated Users (Usuarios autenticados) muestra las listas de acceso de los usuarios a los puertos. Las listas de acceso de los usuarios se definen en la página Add User Name (Añadir nombre de usuario). Para abrir la página Authenticated Users (Usuarios autenticados), haga clic en Switch (Conmutador) → Network Security (Seguridad de la red) → Authenticated Users (Usuarios autenticados).

Figura 7-5. Authenticated Users



La página Authenticated Users (Usuarios autenticados) contiene los campos siguientes:

User Name (Nombre de usuario): muestra una lista de usuarios autorizados a través del servidor RADIUS.

Port (Puerto): indica el número de los puertos utilizados para la autenticación, por nombre de usuario.

Session Time (Tiempo de sesión): indica el tiempo durante el que el usuario ha tenido una sesión iniciada en el dispositivo. El formato del campo es **día:hora:minutos:segundos**, como por ejemplo, 3 días: 2 horas: 4 minutos: 39 segundos.

Authentication Method (Método de autenticación): método utilizado para autenticar la última sesión. Los valores del campo posibles son:

Remote (Remoto): el usuario se ha autenticado desde un servidor remoto.

None (Ninguno): el usuario no se ha autenticado.

MAC Address (Dirección MAC): dirección MAC del suplicador.

Visualización de la tabla de usuarios autenticados

1. Abra la página Authenticated Users (Usuarios autenticados).
2. Haga clic en Show All (Mostrar todo).

Se abre la tabla de usuarios autenticados:

Figura 7-6. Authenticated Users Table

Autenticación de usuarios mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para autenticar usuarios, como se muestra en la página Authenticated Users (Usuarios autenticados).

Tabla 7-3. Comandos de la CLI para añadir nombres de usuario

Comando de la CLI	Descripción
show dot1x users [nombre_usuario nombre_usuario]	Muestra los usuarios de 802.1X para el dispositivo.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show dot1x users

Port Username Session Time Auth Method MAC Address

---------------------------------------------------------------

1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

Configuración de la seguridad de puertos

La seguridad de la red puede mejorarse limitando el acceso en puertos concretos únicamente a usuarios con direcciones MAC específicas. Las direcciones MAC pueden obtenerse de forma dinámica, hasta ese punto, o pueden configurarse de forma estática. La seguridad de puerto bloqueado controla los paquetes recibidos y obtenidos que se reciben en puertos específicos. El acceso al puerto bloqueado queda limitado a los usuarios que tienen direcciones MAC específicas. Estas direcciones se definen manualmente en el puerto o se obtienen en el puerto hasta el punto en que éste se bloquea. Cuando se recibe un paquete en un puerto bloqueado y la dirección MAC de origen del paquete no está vinculada a dicho puerto (se ha obtenido en un puerto distinto o se trata de una dirección desconocida en el sistema), el mecanismo de protección se invoca y puede proporcionar varias opciones. Con los paquetes no autorizados que llegan en un puerto bloqueado se realiza una de las acciones siguientes:

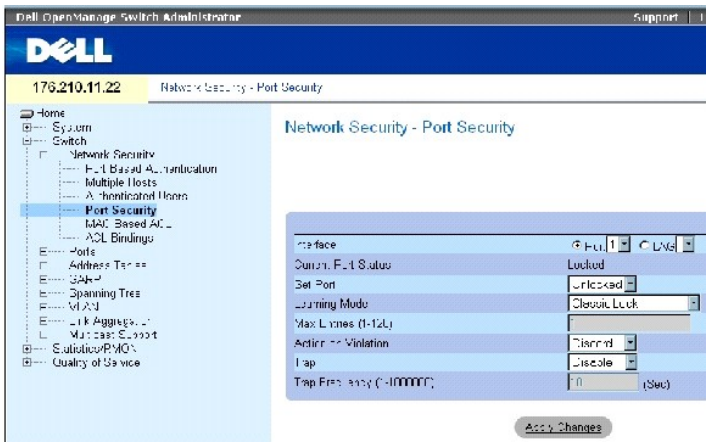
- Se reenvían
- Se descartan sin ninguna excepción
- Se descartan con una excepción
- Se cierra el puerto

La seguridad de puerto bloqueado también permite almacenar una lista de direcciones MAC en el archivo de configuración. Esta lista puede restaurarse una vez restablecido el dispositivo.

NOTA: para poder activar la seguridad del puerto, active la característica **Multiple Hosts** (Varios hosts) en los puertos necesarios.

Los puertos desactivados se activan desde la página Port Security (Seguridad de puertos). La página **Ports** (Puertos) proporciona enlaces para funciones de configuración de puertos, que incluyen funciones como el control de tormentas y la duplicación de puertos, así como funciones para realizar pruebas de puertos virtuales. Para abrir la página Port Security (Seguridad de puertos), haga clic en Switch (Conmutador) → Network Security (Seguridad de la red) → Port Security (Seguridad de puertos).

Figura 7-7. Port Security



La página Port Security (Seguridad de puertos) contiene los campos siguientes:

Interface (Interfaz): indica el tipo de interfaz seleccionado en el cual el puerto bloqueado está activado.

Port (Puerto): indica que el tipo de interfaz seleccionado es un puerto.

LAG: indica que el tipo de interfaz seleccionado es un LAG.

Current Port Status (Estado actual del puerto): indica el estado actual del puerto configurado.

Set Port (Establecer puerto): indica que el puerto está bloqueado o desbloqueado. Los valores del campo posibles son:

Unlocked (Desbloqueado): desbloquea el puerto. Éste es el valor predeterminado.

Locked (Bloqueado): bloquea el puerto.

Learning Mode (Modo de obtención): define el tipo de puerto bloqueado. El campo **Learning Mode (Modo de obtención)** sólo se activa si se ha seleccionado **Locked** (Bloqueado) en el campo **Set Port** (Establecer puerto). Los valores posibles del campo son:

Classic Lock (Bloqueo clásico): bloquea el puerto mediante el mecanismo clásico de bloqueo. El puerto se bloquea de forma inmediata, independientemente del número de direcciones que se hayan obtenido.

Limited Dynamic Lock (Bloqueo dinámico limitado): bloquea el puerto suprimiendo las direcciones MAC dinámicas actuales asociadas con el puerto. El puerto obtiene el número máximo de direcciones permitidas en el mismo. Se permite tanto la nueva obtención como la caducidad de las direcciones MAC.

Max Entries (Número máximo de entradas): especifica el número de direcciones MAC que pueden obtenerse en el puerto. El campo **Max Entries** (Número máximo de entradas) sólo se activa si se ha seleccionado **Locked** (Bloqueado) en el campo **Set Port** (Establecer puerto). Además, se selecciona el modo Limited Dynamic Lock (Bloqueo dinámico limitado). El valor predeterminado es 1.

Action on Violation (Acción tras infracción): indica la acción que debe aplicarse a los paquetes que lleguen a un puerto bloqueado. Los valores del campo posibles son:

Forward (Reenviar): reenvía los paquetes de origen desconocido; sin embargo, la dirección MAC no se obtiene.

Discard (Descartar): descarta los paquetes de cualquier origen no obtenido. Éste es el valor predeterminado.

Shutdown (Apagar): descarta los paquetes de cualquier origen no obtenido y bloquea el puerto. Los puertos permanecen apagados hasta que se activan, o hasta que se restablece el dispositivo.

Trap (Excepción): activa el envío de excepciones cuando se recibe un paquete en un puerto bloqueado.

Trap Frequency (1-1000000) (Frecuencia de excepciones [1-1000000]): indica el tiempo (en segundos) que transcurrirá entre las excepciones. El valor predeterminado es 10 segundos.

Definición de un puerto bloqueado

1. Abra la página **Port Security** (Seguridad de puertos).
2. Seleccione un tipo y un número de interfaz.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto bloqueado se añade a la tabla de seguridad de puertos (**Port Security Table**) y el dispositivo se actualiza.

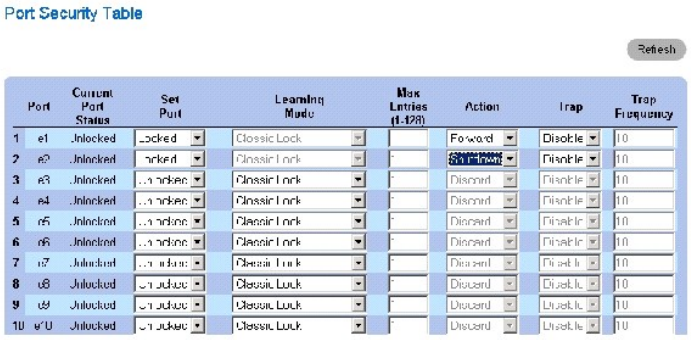
Visualización de la tabla de seguridad de puertos

1. Abra la página **Port Security** (Seguridad de puertos).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de seguridad de puertos (**Port Security Table**).

NOTA: los puertos bloqueados se definen en la tabla de seguridad de puertos (**Port Security Table**).

Figura 7-8. Port Security Table



La tabla de seguridad de puertos (**Port Security Table**) **contiene los campos adicionales siguientes:**

Unit No. (Número de unidad): especifica la unidad de apilamiento para la que aparece la información de seguridad de puertos.

Copy Parameters from (Copiar parámetros de): copia parámetros del número de unidad seleccionado.

Configuración de la seguridad de los puertos bloqueados con comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar la seguridad de los puertos bloqueados como se muestra en la página Port Security (Seguridad de puertos).

Tabla 7-4. Comandos de la CLI para la seguridad de los puertos

Comando de la CLI	Descripción
shutdown	Desactiva las interfaces.
set interface active {ethernet interfaz | port-channel número-canal-puerto}	Vuelve a activar una interfaz que está apagada por motivos de seguridad de puertos.
port security learning {disabled | dynamic}	Define el tipo de puerto bloqueado.
port security max número_máximo_direcciones	Especifica el número de direcciones MAC que pueden obtenerse en el puerto.
port security [**forward** | **discard** | **discard-shutdown**] [**trap** segundos]	Bloquea la obtención de direcciones nuevas en una interfaz.
show ports security {**ethernet** interfaz | **port-channel** número-canal-puertos}	Muestra el estado de bloqueo de los puertos.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console # show ports security

Port   Status    Action    Trap      Frequency  Counter
-----  -------   -------   -------   ---------  -------
1/e1   locked    Discard   Enable    100        88
1/e2   locked    Discard,  Disable
                 Shutdown
1/e3   Unlocked  -         -         -          -
```

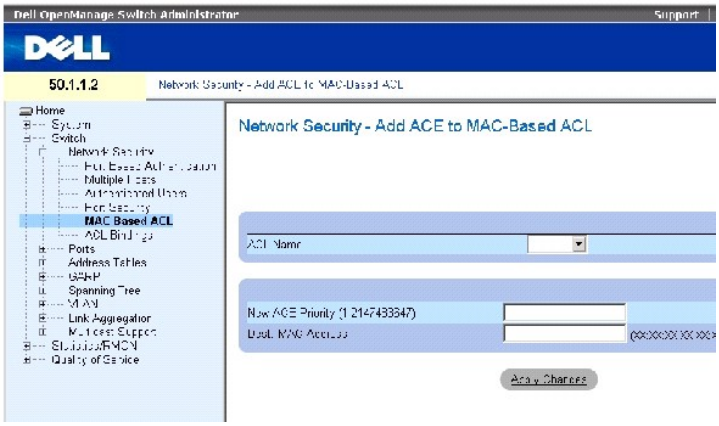
Definición de las ACL basadas en MAC

Las listas de control de acceso (ACL) permiten a los administradores de red definir acciones y reglas de clasificación para puertos de entrada específicos. Las ACL contienen varias acciones y reglas de clasificación. Cada una de estas acciones y reglas de clasificación se conoce como entrada de control de acceso (ACE). Las ACE son los filtros que determinan las clasificaciones de tráfico. Las listas ACL basadas en MAC se aplican a cualquier paquete, incluyendo los paquetes que no son IP. Los campos de clasificación se basan sólo en campos de nivel 2.

La página MAC Based ACL (ACL basada en MAC) muestra la ACL basada en MAC que debe definirse. Para obtener una descripción de las listas ACL, consulte "Definición de las ACL basadas en MAC."

Para abrir la página MAC Based ACL (ACL basada en MAC), seleccione **Switch** (Conmutador) → **Network Security** (Seguridad de la red) → **MAC based ACL** (ACL basada en MAC).

Figura 7-9. MAC Based ACL



La página MAC Based ACL (ACL basada en MAC) contiene los campos siguientes:

ACL Name (Nombre de ACL): ACL definida por el usuario.

New ACE Priority (1-2147483647) (Nueva prioridad de ACE [1-2147483647]): índice de la regla de ACE del campo de ACL.

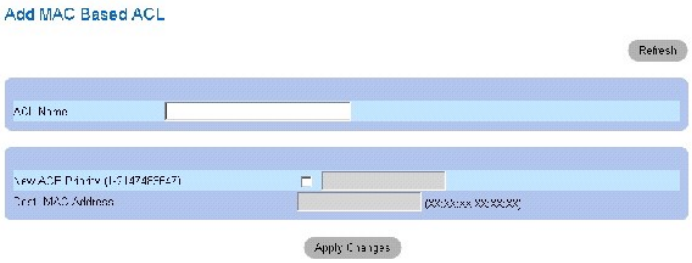
Destination MAC Address (Dirección MAC de destino): hace coincidir la dirección MAC de destino hacia la cual se direccionan los paquetes con la ACE.

Adición de una ACL basada en MAC:

1. Abra la página MAC Based ACL (ACL basada en MAC).
2. Haga clic en **Add** (Añadir).

Se abre la página Add MAC Based ACLs (Añadir ACL basadas en MAC).

Figura 7-10. Add MAC Based ACLs



3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la ACL basada en MAC y se actualiza el dispositivo.

Visualización de las ACE específicas de la ACL

1. Abra la página MAC Based ACL (ACL basada en MAC).
2. Seleccione una ACL.
3. Haga clic en **Show All** (Mostrar todo).

Se abre la página **ACEs Associated with MAC ACL** (ACE asociadas con ACL basada en MAC).

Eliminación de listas ACL

1. Abra la página MAC Based ACL (ACL basada en MAC).

NOTA: las ACL sólo pueden eliminarse si no están vinculadas a una interfaz.

2. Seleccione una ACL.
3. Haga clic en **Show All** (Mostrar todo).

Se abre la página **ACEs Associated with MAC ACL** (ACE asociadas con ACL basada en MAC).

4. Seleccione la casilla de verificación **Remove ACL** (Eliminar ACL).

Asignación de entradas ACE basadas en MAC a listas ACL mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para asignar entradas ACE basadas en MAC a listas ACL, como se muestra en la página MAC Based ACL (ACL basada en MAC).

Tabla 7-5. Comandos de la CLI para entradas ACE basadas en MAC

Comando de la CLI	Descripción
mac access-list nombre	Crea ACL basadas en MAC de nivel 2 y ejecuta el modo de configuración de lista de acceso basada en MAC.
deny *destino*	Deniega el tráfico si las condiciones definidas en la ACL basada en MAC coinciden.
show access-lists [*nombre*]	Muestra las listas de control de acceso configuradas en el dispositivo.

A continuación se muestra un ejemplo de los comandos de la CLI:

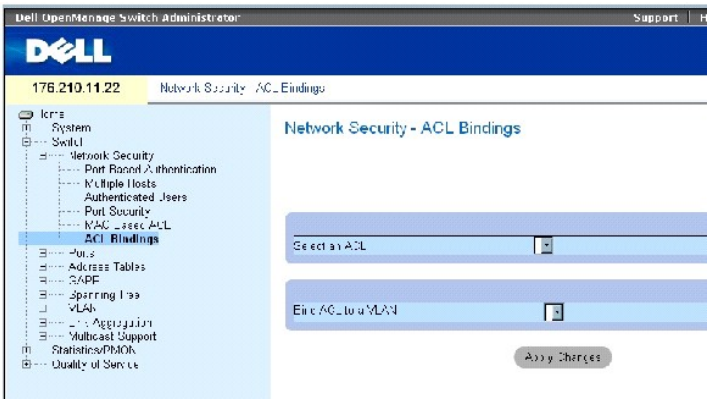
```
console (config)# mac access-list dell
```

```
console (config-mac-al)# deny 00-10-B5-F4-00-01
```

Configuración de vinculaciones de ACL

Si una ACL está vinculada a una interfaz, la ACL se aplica a la interfaz seleccionada. Utilice la página ACL Bindings (Vinculaciones de ACL) para asignar listas ACL a interfaces y métodos de clasificación. Para abrir la página ACL Bindings (Vinculaciones de ACL), seleccione **Switch** (Conmutador) → **Network Security** (Seguridad de la red) → **ACL Binding** (Vinculación de ACL).

Figura 7-11. ACL Bindings



La página ACL Bindings (Vinculaciones de ACL) contiene los campos siguientes:

Select an ACL (Seleccionar una ACL): indica el tipo de ACL con el que coinciden los paquetes entrantes.

Bind ACL to VLAN (Vincular ACL a VLAN): indica la VLAN a la que se conecta la ACL.

Asignación de una ACL a una interfaz

1. Abra la página ACL Bindings (Vinculaciones de ACL).
2. Seleccione el tipo de ACL en el campo **Select an ACL** (Seleccionar una ACL).
3. Seleccione la VLAN a la que está conectada la ACL en el campo **Bind ACL to an VLAN** (Vincular ACL a una VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La ACL se conecta a la interfaz.

Eliminación de una entrada de la tabla de vinculaciones de ACL

1. Abra la página ACL Bindings (Vinculaciones de ACL).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de vinculaciones de ACL.

3. Seleccione la casilla de verificación **Remove** (Eliminar) que corresponda a la entrada que debe eliminarse.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada seleccionada se elimina de la tabla y se actualiza el dispositivo.

Visualización de la tabla de vinculaciones de ACL

1. Abra la página ACL Bindings (Vinculaciones de ACL).
2. Haga clic en **Show All** (Mostrar todo) para abrir la tabla de vinculaciones de ACL (**ACL Bindings Table**).

Los campos de la tabla de vinculaciones de ACL (**ACL Bindings Table**) son los mismos que los de la página **ACL Bindings** (Vinculaciones de ACL).

Copia de los parámetros de la tabla de vinculaciones de ACL

1. Abra la página ACL Bindings (Vinculaciones de ACL).

2. Haga clic en **Show All** (Mostrar todo).

   Se abre la tabla de vinculaciones de ACL.

3. Seleccione una interfaz en el campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione una VLAN del menú desplegable **VLAN**.

   Las definiciones para esta interfaz se copian en los puertos y las combinaciones de puertos seleccionados.

5. Seleccione la casilla de verificación **Copy to** (Copiar en) que corresponda a la entrada que debe editarse o copie las definiciones en todos los puertos y las combinaciones de puertos disponibles.
6. Haga clic en **Select All** (Seleccionar todo).
7. Haga clic en **Apply Changes** (Aplicar cambios).

   Los parámetros se copian en los puertos y las combinaciones de puertos de la tabla de vinculaciones de ACL (*ACL Bindings Table*) y el dispositivo se actualiza.

Asignación de pertenencia a ACL mediante los comandos de la CLI

La siguiente tabla muestra un resumen de los comandos de la CLI equivalentes para asignar pertenencia a ACL como se muestra en la página **ACL Binding** (Vinculación de ACL).

Tabla 7-6. Comandos de la CLI para la vinculación de ACL

Comando de la CLI	Descripción
service-acl {**input** *nombre_ACL*}	Aplica una lista de acceso a la entrada de la interfaz.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface vlan 123

console(config-if)# service-acl input dell
```

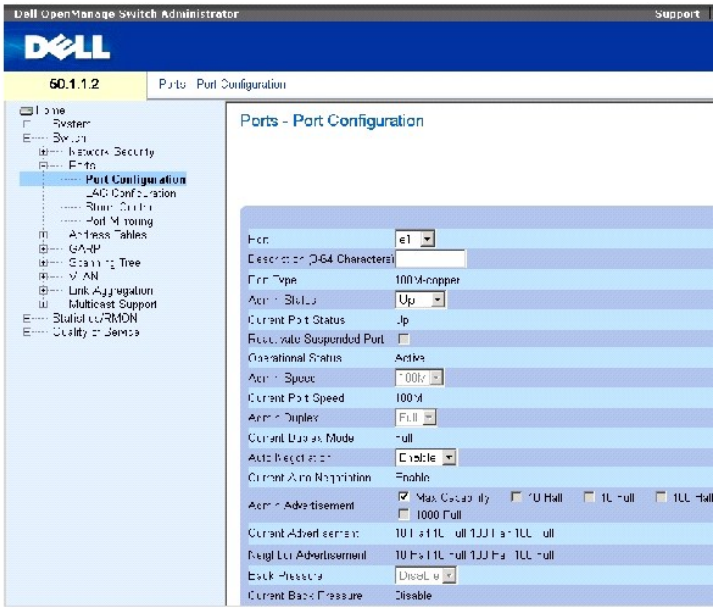
Configuración de puertos

La página **Ports** (Puertos) proporciona enlaces para funciones de configuración de puertos, que incluyen funciones como el control de tormentas y la duplicación de puertos, así como funciones para realizar pruebas de puertos virtuales. Para abrir la página **Ports** (Puertos), seleccione **Switch** (Conmutador) → **Ports** (Puertos).

Definición de la configuración de los puertos

Utilice la página **Port Configuration** (Configuración de puertos) para definir los parámetros de los puertos. Si la configuración del puerto se modifica mientras éste es miembro de un LAG, el cambio de configuración sólo se hace efectivo una vez que se ha eliminado el puerto del LAG. Para abrir la página **Port Configuration** (Configuración de puertos), haga clic en **Switch** (Conmutador) → **Ports** (Puertos) → **Port Configuration** (Configuración de puertos) en la vista de árbol.

Figura 7-12. Port Configuration



La página **Port Configuration** (Configuración de puertos) contiene los campos siguientes:

Port (Puerto): número de puerto para el que se definen los parámetros de puerto.

Description (0 - 64 Characters) (Descripción [0 - 64 caracteres]): breve descripción de la interfaz, como por ejemplo, Ethernet.

Port Type (Tipo de puerto): indica el tipo de puerto.

Admin Status (Estado del administrador): activa o desactiva el reenvío de tráfico a través del puerto.

Current Port Status (Estado actual del puerto): especifica si el puerto está operativo o no actualmente.

Reactivate Suspended Port (Reactivar puerto suspendido): vuelve a activar el puerto si se ha desactivado a través de la opción de seguridad de puerto bloqueado.

Operational Status (Estado operativo): indica el estado operativo del puerto. Los valores del campo posibles son:

Suspended (Suspendido): el puerto está activo y no está recibiendo ni transmitiendo tráfico.

Active (Activo): el puerto está activo y está recibiendo y transmitiendo tráfico.

Disable (Desactivado): el puerto está desactivado y no está recibiendo ni transmitiendo tráfico.

Admin Speed (Velocidad del administrador): velocidad configurada para el puerto. El tipo de puerto determina las opciones de configuración de velocidad disponibles. La velocidad de administrador sólo puede designarse cuando el puerto está desactivado.

Current Port Speed (Velocidad actual del puerto): indica la velocidad real del puerto sincronizado en bps.

Admin Duplex (Dúplex de administrador): especifica el modo dúplex de puerto en bps. **Full** (Dúplex completo): indica que la interfaz admite la transmisión entre el dispositivo y el cliente en ambas direcciones simultáneamente. **Half** (Semidúplex): indica que la interfaz admite la transmisión entre el dispositivo y el cliente en una sola dirección cada vez.

Current Duplex Mode (Modo dúplex actual): especifica el modo dúplex del puerto sincronizado.

Auto Negotiation (Negociación automática): activa la negociación automática en el puerto. La negociación automática es un protocolo entre dos enlaces asociados que permite que un puerto anuncie sus capacidades de velocidad de transmisión, modo dúplex y control de flujo a su asociado.

Current Auto Negotiation (Negociación automática actual): indica la configuración actual de la negociación automática.

Admin Advertisement (Anuncio de administrador): define el valor de negociación automática que el puerto anuncia. Los valores del campo posibles son:

Max Capability (Capacidad máxima): indica que se aceptan todos los valores de velocidad de los puertos y del modo dúplex.

10 Half (Semidúplex 10): indica que el puerto anuncia para un puerto de 10 mbps de velocidad y el valor de modo semidúplex.

10 Full (Dúplex completo10): indica que el puerto anuncia para un puerto de 10 mbps de velocidad y el valor de modo dúplex completo.

100 Half (Semidúplex 100): indica que el puerto anuncia para un puerto de 10 mbps de velocidad y el valor de modo semidúplex.

100 Full (Dúplex completo100): indica que el puerto anuncia para un puerto de 100 mbps de velocidad y el valor de modo dúplex completo.

1000 Full (Dúplex completo1000): indica que el puerto anuncia para un puerto de 1000 mbps de velocidad y el valor de modo dúplex completo.

Current Advertisement (Anuncio actual): el puerto anuncia su velocidad al puerto vecino para iniciar el proceso de negociación. Los valores posibles del campo son los que se especifican en el campo Admin Advertisement (Anuncio de administrador).

Neighbor Advertisement (Anuncio de vecino): indica los valores de anuncio del puerto vecino. Los valores del campo son idénticos a los valores del campo **Admin Advertisement (Anuncio de administrador).**

Back Pressure (Contrapresión): activa el modo de contrapresión en el puerto. El modo de contrapresión se utiliza con el modo de semidúplex para desactivar la recepción de mensajes en los puertos. La contrapresión no se admite en puertos OOB.

Current Back Pressure (Contrapresión actual): indica el valor de contrapresión actual.

Flow Control (Control de flujo): activa o desactiva el control de flujo, o activa la negociación automática del control de flujo en el puerto.

Current Flow Control (Control de flujo actual): indica el valor actual del control de flujo.

MDI/MDIX: permite que el dispositivo descifre entre cables cruzados y no cruzados. Los concentradores y conmutadores se cablean deliberadamente en el sentido opuesto al cableado de las estaciones finales, de modo que cuando se conecta un concentrador o conmutador a una estación final, se puede usar un cable Ethernet directo y los pares coinciden correctamente. Cuando se conectan dos concentradores/conmutadores entre sí o dos estaciones finales entre sí, se utiliza un cable cruzado para garantizar que se conecten los pares correctos. La MDIX automática no funciona en los puertos FE si la negociación automática está desactivada. Los valores del campo posibles son:

Auto (Automática): utilice este valor para detectar automáticamente el tipo de cable.

MDIX: utilice este valor para los concentradores y los conmutadores.

MDI: utilice este valor para las estaciones finales.

Current MDI/MDIX (MDI/MDIX actual): indica los valores actuales de la MDIX del dispositivo. Los valores del campo posibles son:

MDI: el valor actual de MDI es MDI.

MDIX: el valor actual de MDI es MDIX.

LAG: especifica si el puerto forma parte de un LAG.

NOTA: si la configuración del puerto se modifica mientras éste es miembro de un LAG, el cambio de configuración sólo se hace efectivo una vez que se ha eliminado el puerto del LAG.

Definición de parámetros de puerto

1. Abra la página **Port Configuration** (Configuración de puertos).
2. Seleccione un puerto en el campo **Port** (Puerto).
3. Defina los campos disponibles del diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

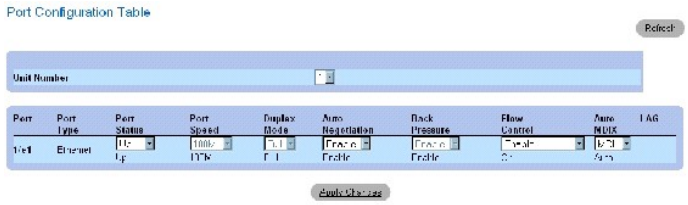
Los parámetros de puerto se guardan en el dispositivo.

Visualización de la tabla de puertos

1. Abra la página **Port Configuration** (Configuración de puertos).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de configuración de puertos.

Figura 7-13. Port Configuration Table



Configuración de puertos con comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar los puertos como se muestra en la página Port Configuration (Configuración de puertos).

Tabla 7-7. Comandos de la CLI para la configuración de los puertos

Comando de la CLI	Descripción

interface ethernet *interfaz*	Ejecuta el modo de configuración de interfaz para configurar una interfaz de tipo Ethernet.
description *cadena*	Añade una descripción a una configuración de interfaz.
shutdown	Desactiva las interfaces que forman parte del contexto fijado actualmente.
set interface active {**ethernet** *interface* | **port-channel** *número-canal-puerto*}	Vuelve a activar una interfaz que está apagada por motivos de seguridad.
speed *Mbps*	Configura la velocidad de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
duplex {half | full}	Configura el funcionamiento dúplex completo o semidúplex de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
negotiation [capability1 [capability2...capability5]	Permite el funcionamiento con negociación automática para los parámetros de velocidad y dúplex de una interfaz determinada.
back-pressure	Activa la contrapresión en una interfaz determinada.
flowcontrol {auto | on | off}	Configura el control de flujo en una interfaz determinada.
mdix {on | auto}	Activa el cable cruzado automático en una interfaz o un canal de puertos determinado.
show interfaces configuration [**ethernet** *interfaz* |**port-channel** *número-canal-puerto*]	Muestra la configuración de todas las interfaces configuradas.
show interface advertise	Muestra los valores de anuncio de negociación de la interfaz.
show interfaces status [**ethernet** *interfaz* | **port-channel** *número-canal-puerto*]	Muestra el estado de todas las interfaces configuradas.
show interfaces description [**ethernet** *interfaz* | **port-channel** *número-canal-puerto*]	Muestra la descripción de todas las interfaces configuradas.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface ethernet 1/e3

console(config-if)# description "RD SW#3"

console(config-if)# shutdown

console(config-if)# no shutdown

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# negotiation

console(config-if)# back-pressure

console(config-if)# flowcontrol on

console(config-if)# mdix auto

console(config-if)# end

console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix

								Mode
----	-----	------	------	----	------	-----	------	----
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

Console# **show interfaces status**

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	-----	------	------	----	------	-----	------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

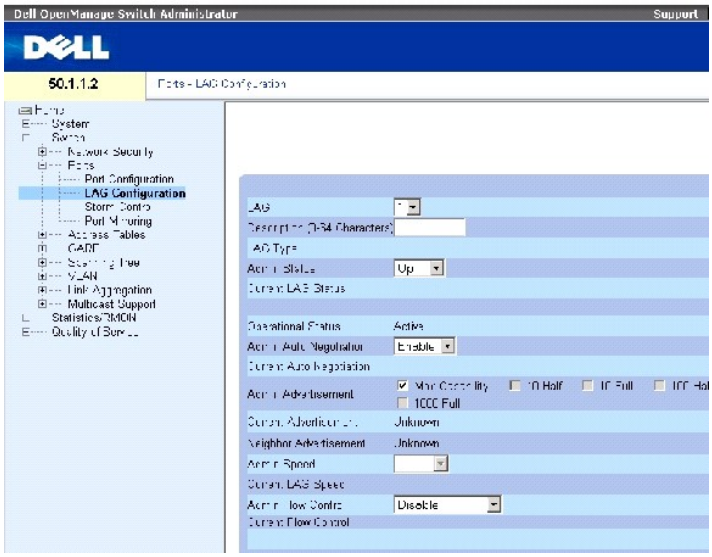
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	------	-----	-----	-------	--------	------	
1	1000	Full	1000	Off	Off	Disable	Up	

Definición de los parámetros de LAG

La página **LAG Configuration** (Configuración de LAG) contiene campos para configurar parámetros para grupos LAG configurados. El dispositivo admite hasta ocho puertos por LAG y ocho grupos LAG por sistema. Para obtener información sobre los grupos de agregado de enlaces (LAG) y la asignación de puertos, consulte **Agregado de puertos** (Agregado de puertos).

Para abrir la página **Port Configuration** (Configuración de puertos), pulse Switch (Conmutador) → Ports (Puertos) → LAG Configuration (Configuración de LAG) en la vista de árbol.

Figura 7-14. LAG Configuration



La página **LAG Configuration** (Configuración de LAG) contiene los campos siguientes:

LAG: indica el número de LAG.

Description (0 - 64 Characters) (Descripción [0 - 64 caracteres]): proporciona una descripción definida por el usuario del LAG configurado.

LAG Type (Tipo de LAG): tipos de puerto que componen el LAG.

Admin Status (Estado de administrador): activa o desactiva el LAG seleccionado.

Current LAG Status (Estado de LAG actual): indica si el LAG está en funcionamiento.

Operational Status (Estado de funcionamiento): activa o desactiva el reenvío de tráfico a través del LAG seleccionado.

Admin Auto Negotiation (Negociación automática de administrador): activa o desactiva la negociación automática en el LAG. La negociación automática es un protocol entre dos enlaces asociados para permitir que un LAG anuncie sus capacidades de velocidad de transmisión, modo dúplex y control de flujo (el valor predeterminado del control de flujo es "desactivado") a su asociado.

Current Auto Negotiation (Negociación automática actual): valor actual de la negociación automática configurada.

Admin Advertisement (Anuncio de administrador): define el valor de negociación automática que el LAG anuncia. Los valores del campo posibles son:

Max Capability (Capacidad máxima): indica que se aceptan todos los valores de velocidad del LAG y del modo dúplex.

10 Half (Semidúplex 10): indica que el LAG anuncia para un LAG de 10 mbps de velocidad y el valor de modo semidúplex.

10 Full (Dúplex completo 10): indica que el LAG anuncia para un LAG de 10 mbps de velocidad y el valor de modo dúplex completo.

100 Half (Semidúplex 100): indica que el LAG anuncia para un LAG de 10 mbps de velocidad y el valor de modo semidúplex.

100 Full (Dúplex completo 100): indica que el LAG anuncia para un LAG de 10 mbps de velocidad y el valor de modo dúplex completo.

1000 Full (Dúplex completo 1000): indica que el LAG anuncia para un LAG de 10 mbps de velocidad y el valor de modo dúplex completo.

Current Advertisement (Anuncio actual): el LAG anuncia su velocidad al LAG vecino para iniciar el proceso de negociación. Los valores posibles del campo son los que se especifican en el campo Admin Advertisement (Anuncio de administrador).

Neighbor Advertisement (Anuncio de vecino): indica los valores de anuncio del LAG vecino. Los valores del campo son idénticos a los valores del campo **Admin Advertisement (Anuncio de administrador).**

Admin Speed (Velocidad de administrador): indica la velocidad a la cual está funcionando el LAG.

Current LAG Speed (Velocidad actual del LAG): indica la velocidad actual a la cual está funcionando el LAG.

Admin Flow Control (Control de flujo de administrador): activa o desactiva el control de flujo, o activa la negociación automática del control de flujo en el LAG. El modo de control de flujo es efectivo en los puertos que funcionan en modo Full Duplex (Dúplex completo) en el LAG.

Current Flow Control (Control de flujo actual): indica el valor de control de flujo designado por el usuario.

Definición de parámetros de LAG

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Seleccione un LAG en el campo **LAG**.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG se guardan en el dispositivo.

Modificación de parámetros de LAG

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Seleccione un LAG en el campo **LAG**.
3. Modifique los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

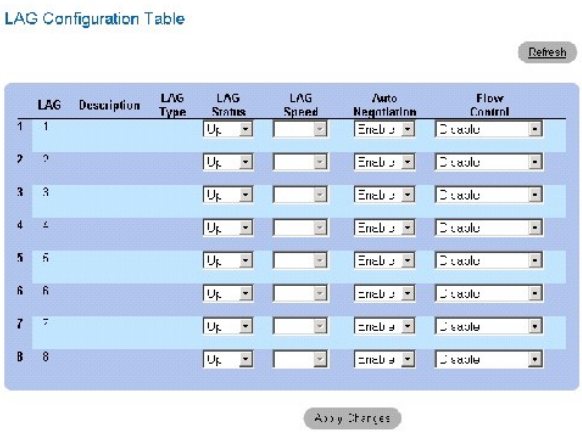
Los parámetros de LAG se guardan en el dispositivo.

Para mostrar la tabla de configuración de LAG:

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de configuración de LAG (**LAG Configuration Table**).

Figura 7-15. LAG Configuration Table



Configuración de grupos LAG con comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar los LAG como se muestra en la página **LAG Configuration** (Configuración de LAG).

Tabla 7-8. Comandos de la CLI para la configuración de los LAG

Comando de la CLI	Descripción
interface port-channel *número-canal-puertos*	Entra en el modo de configuración de interfaz de un puerto de canal específico.
description *cadena*	Añade una descripción a una configuración de interfaz.
shutdown	Desactiva las interfaces que forman parte del contexto fijado actualmente.
speed *bps*	Configura la velocidad de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
negotiation [capability1 [capability2...capability5]	Permite la operación de negociación automática de la velocidad de la interfaz.
back-pressure	Activa la contrapresión en una interfaz determinada.
flowcontrol {auto | on | off}	Configura el control de flujo en una interfaz determinada.
show interfaces configuration [**ethernet** *interfaz* |**port-channel** *número-canal-puerto*]	Muestra la configuración de todas las interfaces configuradas.
show interfaces status [**ethernet** *interfaz* | **port-channel** *número-canal-puerto*]	Muestra el estado de todas las interfaces configuradas.
show interfaces description [**ethernet** *interfaz* |**port-channel** *número-canal-puerto*]	Muestra la descripción de todas las interfaces configuradas.
show interfaces port-channel [*número-canal-puerto*]	Muestra información del canal de puertos (qué puertos son miembros del canal de puertos y si están o no activos actualmente).

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface port-channel 2

console(config-if)# no negotiation

console(config-if)# speed 100

console(config-if)# flowcontrol on

console(config-if)# exit
```

```
console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive: 1/e(11-13)
ch2	Active: 1/e14

Activación del control de tormentas

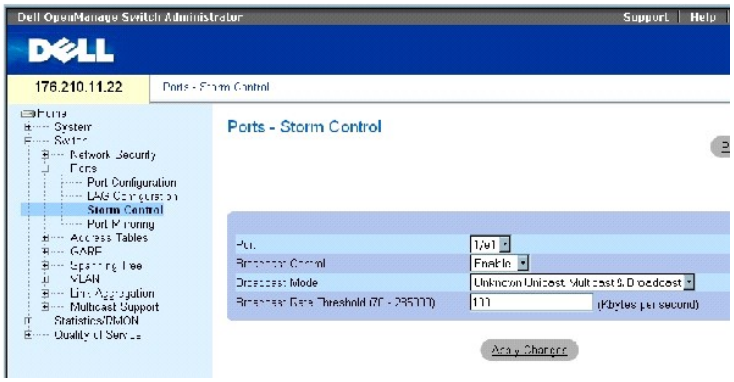
Una tormenta de transmisión es el resultado de una cantidad excesiva de mensajes de transmisión simultánea a través de una red mediante un único puerto. Las respuestas a mensajes reenviados se acumulan en la red, lo que provoca una sobrecarga en los recursos de ésta o que se agote el tiempo de espera.

El control de tormentas se activa en cada puerto mediante la definición del tipo de paquete y la velocidad de transmisión de los paquetes.

El sistema mide la velocidad de las tramas entrantes de transmisión, unidifusión y multidifusión por separado en cada puerto y descarta las tramas cuando la velocidad supera un valor definido por el usuario.

La página **Storm Control** (Control de tormentas) proporciona campos para activar y configurar el control de tormentas. Para abrir la página **Storm Control** (Control de tormentas), haga clic en Switch (Conmutador) → Ports (Puertos) → Storm Control (Control de tormentas) en la vista de árbol.

Figura 7-16. Storm Control



La página **Storm Control** (Control de tormentas) contiene los campos siguientes:

Port (Puerto): puerto desde el que se activa el control de tormentas.

Broadcast Control (Control de difusión): activa o desactiva el reenvío de tipos de paquetes de difusión en la interfaz específica.

Broadcast Mode (Modo de difusión): especifica el modo de difusión activo actualmente en el dispositivo o la pila. Los valores del campo posibles son:

Unknown Unicast, Multicast & Broadcast (Unidifusión desconocida, multidifusión y difusión): cuenta el tráfico de unidifusión, multidifusión y difusión.

Multicast & Broadcast (Multidifusión y difusión): cuenta el tráfico de difusión y multidifusión conjuntamente.

Broadcast Only (Sólo difusión): cuenta sólo el tráfico de difusión.

Broadcast Rate Threshold (70-285000) (Umbral de velocidad de difusión [70-285000]): velocidad máxima (kilobytes por segundo) de reenvío de los paquetes desconocidos. El rango del campo es 70-285000 kilobytes por segundo.

Activación del control de tormentas

1. Abra la página **Storm Control** (Control de tormentas).
2. Seleccione la interfaz en la que desea implementar el control de tormentas.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El control de tormentas está activado.

Modificación de los parámetros de puerto de control de tormentas

1. Abra la página **Storm Control** (Control de tormentas).
2. Modifique los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

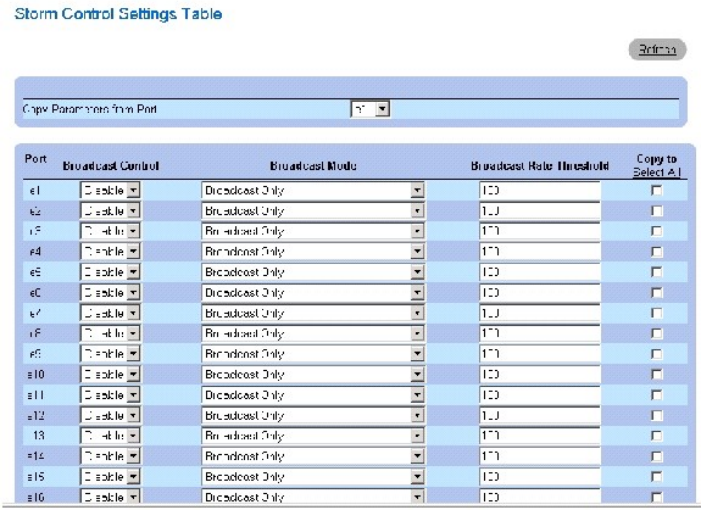
Los parámetros de puerto de control de tormentas se guardan en el dispositivo.

Visualización de la tabla de parámetros de puerto

1. Abra la página **Storm Control** (Control de tormentas).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de configuración de control de tormentas (**Storm Control Settings Table**).

Figura 7-17. Storm Control Settings Table



Además de los campos de la página Storm Control (Control de tormentas), la tabla de configuración de control de tormentas (**Storm Control Settings Table**) contiene los campos adicionales siguientes:

Copy Parameters from Port (Copiar parámetros del puerto): indica el puerto específico del que se copian los parámetros de control de tormentas.

Copia de parámetros en la tabla de configuración de control de tormentas

1. Abra la página **Storm Control** (Control de tormentas).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de configuración de control de tormentas (**Storm Control Settings Table**).

3. Seleccione el puerto desde el que se copian los valores en el campo **Copy Parameters from Port** (Copiar parámetros del puerto).
4. Seleccione la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que se copiarán las definiciones de control de tormentas, o haga clic en **Select All** (Seleccionar todo) para copiar las definiciones en todos los puertos.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian en los puertos seleccionados en la tabla de configuración de control de tormentas (**Storm Control Settings Table**) y se actualiza el dispositivo.

Configuración de control de tormentas con comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar el control de tormentas como se muestra en la página **Storm Control** (Control de tormentas).

Tabla 7-9. Comandos de la CLI para el control de tormentas

Comando de la CLI	Descripción

`port storm-control include-multicast`	Permite al dispositivo contar los paquetes de multidifusión, unidifusión y difusión conjuntamente.
`port storm-control broadcast enable`	Activa el control de tormentas de difusión.
`port storm-control broadcast rate`	Configura la velocidad máxima de transmisión.
`show ports storm-control` *puerto*	Muestra la configuración de control de tormentas.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# port storm-control include-multicast

console(config)# interface ethernet 1/e1

console(config-if)# port storm-control broadcast enable

console(config-if)# port storm-control broadcast rate 100000

console(config-if)# end

console# show ports storm-control
```

Port	Broadcast Storm control [kbyes/sec]
----	----------
1/e1	8000
2/e1	Disabled
3/e2	Disabled

Definición de sesiones de duplicación de puertos

Duplicación de puertos:

- Supervisa y duplica el tráfico de red mediante el reenvío de copias de los paquetes entrantes y salientes de un puerto a un puerto supervisor.
- Puede utilizarse como herramienta de diagnóstico y como función de depuración de errores.

- Activa el rendimiento y la supervisión del dispositivo.

La duplicación de puertos se configura seleccionando un puerto específico en el que copiar todos los paquetes y diferentes puertos desde los que copiar los paquetes.

Antes de configurar la duplicación de puertos, tenga en cuenta lo siguiente:

- La duplicación de puertos supervisa y duplica el tráfico de red mediante el reenvío de copias de paquetes entrantes y salientes de un puerto supervisado a un puerto supervisor.
- El puerto supervisado no puede funcionar más rápido que el puerto supervisor.
- Todos los paquetes RX/TX deben supervisarse para el mismo puerto.

Las restricciones siguientes se aplican a los puertos configurados como puertos de destino:

- Los puertos no pueden estar configurados como puertos de origen.
- Los puertos no pueden ser miembros de un LAG.
- Las interfaces IP no se configuran en el puerto.
- El GVRP no se activa en el puerto.
- El puerto no es miembro de una VLAN.
- Se puede definir un solo puerto de destino.

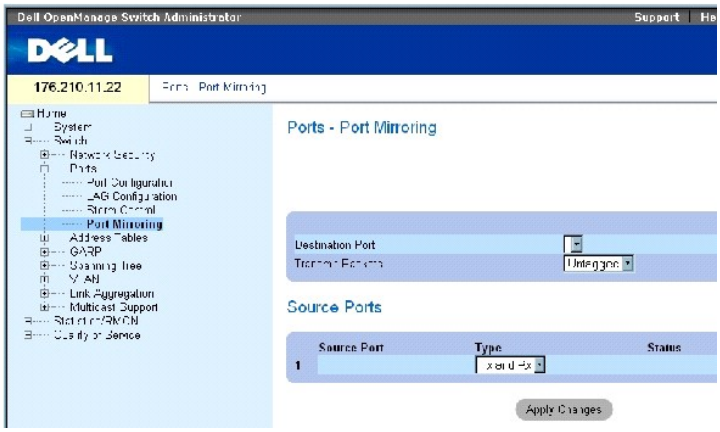
Las siguientes restricciones se aplican a los puertos configurados como puertos de origen:

- Los puertos de origen no pueden ser miembros de un LAG.
- Los puertos no pueden estar configurados como puertos de destino.
- Se admiten ocho puertos de origen como máximo.

Para abrir la página **Port Mirroring** (Duplicación de puertos), haga clic en **Switch** (Conmutador) → **Ports** (Puertos) → **Port Mirroring** (Duplicación de puertos) en la vista de árbol.

NOTA: cuando se define un puerto como puerto de destino para una sesión de duplicación de puertos, se suspenden todas las operaciones normales en ese puerto. Esto incluye el árbol de extensión y el LACP.

Figura 7-18. Port Mirroring



La página **Port Mirroring** **(Duplicación de puertos) contiene los campos siguientes:**

Destination Port (Puerto de destino): indica el número de puerto en el que se copia el tráfico del puerto.

Transmit Packets (Transmitir paquetes): define cómo se duplican los paquetes. Los valores del campo posibles son:

Untagged (Sin etiquetar): duplica los paquetes como paquetes vlan sin etiquetar. Éste es el valor predeterminado.

Tagged (Etiquetados): duplica los paquetes como paquetes vlan etiquetados.

Type (Tipo): indica si los paquetes duplicados son RX, TX o ambos.

Status (Estado): indica si el puerto está duplicado actualmente (**Active** [Activo]) o no (**Ready** [Listo]).

Remove (Eliminar): si se selecciona esta opción, elimina la sesión de duplicación de puertos.

Adición de una sesión de duplicación de puertos

1. Abra la página Port Mirroring (Duplicación de puertos).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add Source Port** (Adición de un puerto de origen).

3. Defina los campos **Source Port** (Puerto de origen) y **Type** (Tipo).
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. Seleccione el puerto de destino en el menú desplegable **Destination Port** (Puerto de destino).
6. Haga clic en el botón **Refresh** (Actualizar) de la página Port Mirroring (Duplicación de puertos).
7. Defina el campo **Tagged Packets** (Paquetes etiquetados).
8. Defina el campo **Type** (Tipo).
9. Haga clic en **Apply Changes** (Aplicar cambios).

Se define un puerto de origen nuevo y se actualiza el dispositivo.

Eliminación de un puerto de copia de una sesión de duplicación de puertos

1. Abra la página Port Mirroring (Duplicación de puertos).
2. Seleccione la casilla de verificación **Remove** (Eliminar).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se borra la sesión de duplicación de puertos seleccionada y se actualiza el dispositivo.

Configuración de una sesión de duplicación de puertos mediante los comandos de la CLI

La siguiente tabla muestra un resumen de los comandos de la CLI equivalentes para configurar la sesión de duplicación de puertos como aparece en la página Port Mirroring (Duplicación de puertos).

Tabla 7-10. Comandos de la CLI para la duplicación de puertos

Comando de la CLI	Descripción
port monitor *interfaz*-origen [**rx** | **tx**]	Inicia una sesión de supervisión de puertos.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface ethernet
1/e1


console(config-if)# port monitor 1/e2


console(config-if)# end


console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
---	---	---	---	---
1/e2	1/e1	RX, TX	Active	No

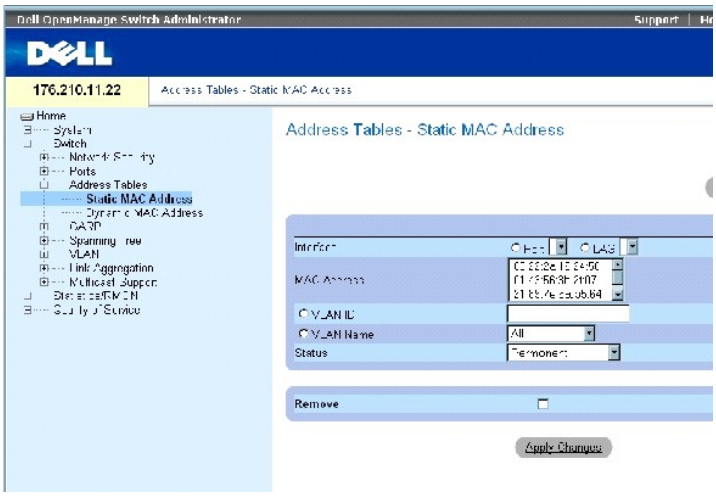
Configuración de tablas de direcciones

Las direcciones MAC se almacenan en la base de datos Static Address (Dirección estática) o Dynamic Address (Dirección dinámica). Un paquete direccionado hacia un destino almacenado en una de las bases de datos se reenvía de inmediato al puerto. La tabla de direcciones dinámicas puede almacenarse por interfaz, VLAN y dirección MAC. Las direcciones MAC se obtienen de forma dinámica a medida que los paquetes de los orígenes llegan al dispositivo. Las direcciones se asocian con puertos mediante la obtención de los puertos de la dirección de origen de la trama. Las tramas dirigidas a una dirección MAC de destino que no esté asociada con ningún puerto se distribuyen a todos los puertos de la VLAN pertinente. Las direcciones estáticas se configuran manualmente. A fin de evitar el desbordamiento de la tabla de puentes, las direcciones MAC dinámicas en las que no se percibe ningún tipo de tráfico durante un periodo de tiempo determinado se borran. Para abrir la página Address Tables (Tablas de direcciones), haga clic en Switch (Conmutador) → Address Tables (Tablas de direcciones) en la vista de árbol.

Definición de direcciones estáticas

La página Static MAC Address Table (Tabla de direcciones MAC estáticas) contiene una lista de direcciones MAC estáticas. Es posible añadir direcciones de este tipo desde la página Static MAC Address Table (Tabla de direcciones MAC estáticas). Además, es posible definir varias direcciones MAC para un único puerto. Para abrir la página Static MAC Address Table (Tabla de direcciones MAC estáticas), haga clic en Switch (Conmutador) → Address Tables (Tablas de direcciones) → Static Address Table (Tabla de direcciones estáticas) en la vista de árbol.

Figura 7-19. Static MAC Address Table



La página Static MAC Address Table (Tabla de direcciones MAC estáticas) contiene los campos siguientes:

Interface (Interfaz): puerto o LAG específico al que se aplica la dirección MAC estática.

MAC Address (Dirección MAC): indica las direcciones MAC que aparecen en la lista de direcciones estáticas actuales.

VLAN ID (ID de VLAN): ID de la VLAN conectada a MAC.

VLAN Name (Nombre de VLAN): nombre de VLAN definido por el usuario.

Status (Estado): estado de la dirección MAC. Los valores posibles son:

Secure (Seguro): se utiliza para definir direcciones MAC estáticas para los puertos bloqueados.

Permanent (Permanente): indica que la dirección MAC es permanente.

Delete on Reset (Borrar al restablecer): la dirección MAC se borra al restablecer el dispositivo.

Delete on Timeout (Eliminar al exceder el tiempo de espera): la dirección MAC se elimina cuando se excede el tiempo de espera.

NOTA: a fin de evitar la eliminación de las direcciones MAC estáticas al restablecer el dispositivo Ethernet, asegúrese de que el puerto conectado a la dirección MAC esté bloqueado.

Remove (Eliminar): si se selecciona esta opción, la dirección MAC seleccionada se elimina de la tabla de direcciones MAC.

Adición de una dirección MAC estática

1. Abra la página Static MAC Address Table (Tabla de direcciones MAC estáticas).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add Static MAC Address** (Añadir dirección MAC estática).

3. Cumplimente los campos.

4. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección estática nueva se añade a la tabla de direcciones MAC estáticas (**Static MAC Address Table**) y el dispositivo se actualiza.

Modificación de un valor de dirección estática en la tabla de direcciones MAC estáticas

1. Abra la página Static MAC Address Table (Tabla de direcciones MAC estáticas).
2. Seleccione una interfaz.
3. Modifique los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la dirección MAC estática y se actualiza el dispositivo.

Eliminación de una dirección estática de la tabla de direcciones estáticas

1. Abra la página Static MAC Address Table (Tabla de direcciones MAC estáticas).
2. Seleccione una interfaz.
3. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de direcciones MAC estáticas.

4. Seleccione una entrada de la tabla.
5. Seleccione la casilla de verificación **Remove** (Eliminar).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la dirección estática seleccionada y se actualiza el dispositivo.

Configuración de parámetros de direcciones estáticas mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar los parámetros de direcciones estáticas como se muestra en la página Static MAC Address Table (Tabla de direcciones MAC estáticas).

Tabla 7-11. Comandos de la CLI para direcciones estáticas

Comando de la CLI	Descripción
bridge address *dirección-mac* [permanent | delete-on-reset | delete-on-timeout | secure] {ethernet interfaz | port-channel *número-canal-puerto*}	Añade una dirección de origen de la estación de nivel MAC estática a la tabla puente.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interfaz* | **port-channel** *número-canal-puerto*]	Muestra entradas en la base de datos de envío de puentes.

A continuación se muestra un ejemplo de comandos de la CLI.

```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table

Aging time is 300 sec

vlan    mac address                port    type
```

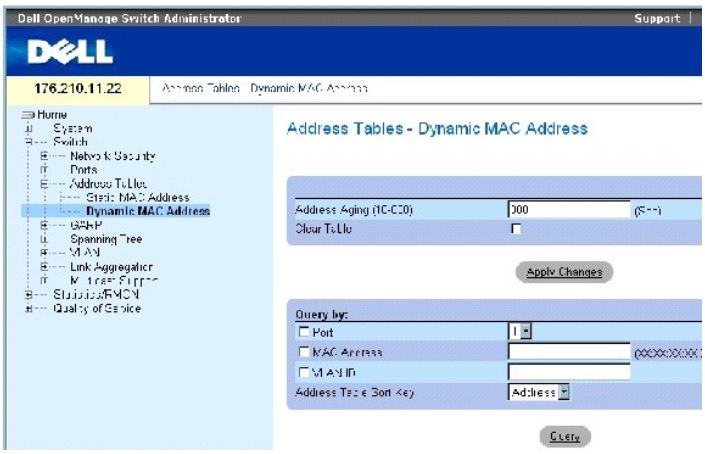
----	----------	----	--------
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e9	static

Visualización de direcciones dinámicas

La página **Dynamic MAC Address** (Dirección MAC dinámica) contiene información para realizar consultas sobre datos de la tabla de direcciones dinámicas, incluidos el tipo de interfaz, direcciones MAC, VLAN y ordenamiento de tablas. Los paquetes reenviados a una dirección almacenada en la tabla de direcciones se reenvían directamente a esos puertos. La página **Dynamic MAC Address** (Dirección MAC dinámica) también contiene información sobre el tiempo de caducidad antes de que se elimine una dirección MAC dinámica, e incluye parámetros para realizar consultas y visualizar la lista de direcciones dinámicas. La tabla de la dirección actual contiene los parámetros de dirección dinámica según los cuales se reenvían directamente los paquetes a los puertos.

Para abrir la página **Dynamic MAC Address** (Dirección MAC dinámica), haga clic en Switch (Conmutador) → Address Tables (Tablas de direcciones) → Dynamic **MAC Address** (Dirección MAC dinámica) en la vista de árbol.

Figura 7-20. Dynamic MAC Address



La página **Dynamic MAC Address** (Dirección MAC dinámica) contiene los campos siguientes:

Address Aging (10-630) (Duración de direcciones [10-630]): especifica el periodo de tiempo durante el que la dirección MAC permanece en la página Dynamic MAC Address (Dirección MAC dinámica) antes de expirar si no se detecta ningún tipo de tráfico desde el origen. El valor predeterminado es 300 segundos.

Clear Table (Borrar tabla): si se selecciona esta opción, se borra la tabla de direcciones dinámicas.

Port (Puerto): especifica la interfaz para la que se consulta la tabla. Pueden seleccionarse dos tipos de interfaz.

MAC Address (Dirección MAC): especifica la dirección MAC para la que se consulta la tabla.

VLAN ID (ID de VLAN): indica la ID de la VLAN para la que se consulta la tabla.

Address Table Sort Key (Clave de ordenamiento de la tabla de direcciones): especifica cómo se ordena la tabla de direcciones dinámicas. La tabla de direcciones puede ordenarse por dirección, VLAN o interfaz.

Redefinición del tiempo de caducidad

1. Abra la página **Dynamic MAC Address** (Dirección MAC dinámica).
2. Defina el campo **Aging Time** (Tiempo de caducidad).
3. Haga clic en Apply Changes (Aplicar cambios).

Se modifica el tiempo de caducidad y se actualiza el dispositivo.

Consulta de la tabla de direcciones dinámicas

1. Abra la página **Dynamic MAC Address** (Dirección MAC dinámica).
2. Defina el parámetro por el que se consultará la tabla de direcciones dinámicas.

Las entradas pueden consultarse por el valor de **Port** (Puerto), **MAC Address** (Dirección MAC) o **VLAN ID** (ID de VLAN).

3. Haga clic en **Query** (Consulta).

Se consulta la página Dynamic MAC Address (Dirección MAC dinámica).

Orden de la tabla de direcciones dinámicas

1. Abra la página **Dynamic MAC Address** (Dirección MAC dinámica).
2. En el menú desplegable **Address Table Sort Key** (Clave de ordenamiento de la tabla de direcciones), seleccione si desea ordenar la tabla por dirección, ID de VLAN o interfaz.
3. Haga clic en **Query** (Consulta).

Se ordena la página Dynamic MAC Address (Dirección MAC dinámica).

Consulta y ordenamiento de direcciones dinámicas mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para establecer la caducidad, consultar y ordenar direcciones dinámicas como se muestra en la página Dynamic MAC Address (Dirección MAC dinámica).

Tabla 7-12. Comandos de la CLI de consulta y ordenamiento

Comando de la CLI	Descripción
bridge aging-time *segundos*	Establece el tiempo de caducidad de la tabla de direcciones.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interfaz* | **port-channel** *número-canal-puerto*]	Muestra clases de entradas creadas de manera dinámica en la base de datos de reenvío de puente.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console (config)# bridge aging-time 250

console (config)# end

console# show bridge address-table

Aging time is 250 sec
```

vlan	mac address	port	type
----	-----------	----	----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e8	static

Configuración de GARP

El protocolo genérico de registro de atributos (GARP) es un protocolo de propósitos generales que registra cualquier información de conectividad de red o de estilo de pertenencia. GARP define un conjunto de dispositivos interesados en un atributo de red determinado, como VLAN o dirección de multidifusión.

Al configurar el protocolo GARP, asegúrese de lo siguiente:

- El tiempo de cese debe ser igual o mayor que tres veces el tiempo de unión.
- El tiempo de cese de todos debe ser mayor que el tiempo de cese.
- Establezca los mismos valores de temporizador de GARP en todos los dispositivos conectados en el nivel 2. Si los temporizadores de GARP se establecen de forma distinta en los dispositivos conectados en el nivel 2, la aplicación GARP no funciona correctamente.

Para abrir la página **GARP**, haga clic en Switch (Conmutador) → **GARP** en la vista de árbol.

Definición de temporizadores GARP

La página GARP Timers (Temporizadores de GARP) contiene campos para activar GARP en el dispositivo. Para abrir la página GARP Timers (Temporizadores de GARP), haga clic en Switch (Conmutador) → **GARP** → **GARP Timers** (Temporizadores de GARP) en la vista de árbol.

Figura 7-21. GARP Timers

La página GARP Timers (Temporizadores de GARP) contiene los siguientes campos:

Interface (Interfaz): seleccione un puerto o LAG para editar los temporizadores de GARP.

GARP Join Timer (10-2147483640) (Temporizador de unión de GARP [10-2147483640]): indica el tiempo, en milisegundos, en que se transmiten las PDU. El valor predeterminado es 200 ms.

GARP Leave Timer (10-2147483640) (Temporizador de cese de GARP [10-2147483640] Ms.): indica el tiempo, en milisegundos, durante el que el dispositivo espera antes de abandonar su estado GARP. El tiempo de cese se activa mediante un mensaje Leave All Time (Tiempo de cese de todos) enviado/recibido y se cancela mediante el mensaje Join (Unión) recibido. El tiempo de cese debe ser igual o mayor que tres veces el tiempo de unión. El valor predeterminado es 600 ms.

GARP Leave All Timer (10 - 2147483640) (Msec) (Temporizador de cese de todos de GARP (10-2147483640) Ms.): indica el tiempo, en milisegundos, durante el que todos los dispositivos esperan antes de abandonar su estado GARP. El tiempo de cese de todos debe ser mayor que el tiempo de cese. El valor predeterminado es 10000 ms.

Definición de temporizadores GARP

1. Abra la página GARP Timers (Temporizadores de GARP).
2. Seleccione una interfaz.
3. Cumplimente los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de GARP se guardan en el dispositivo.

Copia de parámetros en la tabla de temporizadores de GARP

1. Abra la página GARP Timers (Temporizadores de GARP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de temporizadores de GARP.

3. Seleccione el tipo de interfaz en el campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione una interfaz en el menú desplegable **Port** (Puerto) o **LAG**.

Las definiciones para esta interfaz se copian en las interfaces seleccionadas. Consulte el paso 6.

5. Seleccione la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que se copiarán las definiciones de temporizador de GARP, o haga clic en **Select All** (Seleccionar todo) para copiar las definiciones en todos los puertos o grupos LAG.
6. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian en los puertos o LAG seleccionados en la tabla de temporizadores de GARP (**GARP Timers Table**) y se actualiza el dispositivo.

Definición de temporizadores de GARP mediante los comandos de la CLI

En esta tabla se presenta un resumen de los comandos de la CLI equivalentes para definir temporizadores de GARP como se muestra en la página GARP Timers (Temporizadores de GARP).

Tabla 7-13. Comandos de la CLI para temporizadores de GARP

Comando de la CLI	Descripción
garp timer {join | leave | leaveall} *valor_temporizador*	Ajusta los valores del temporizador de GARP "Join", "Leave" y "Leaveall".

A continuación se muestra un ejemplo de los comandos de la CLI:

```
```

```
console(config)# interface ethernet 1/e1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11


GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
1/e11	Disabled	Normal	Enabled	200	900	10000

Configuración del protocolo de árbol de extensión

El protocolo de árbol de extensión (STP) permite obtener una topografía de árbol de cualquier combinación de puentes. El STP proporciona una ruta entre las estaciones finales de una red para eliminar los bucles.

Los bucles se producen cuando existen rutas alternativas entre hosts. En una red extendida, pueden hacer que los puentes reenvíen tráfico indefinidamente, lo que provoca un aumento del tráfico y una disminución del rendimiento de la red.

El dispositivo admite las siguientes versiones de árbol de extensión:

- Classic STP (STP clásico): proporciona una única ruta entre estaciones finales, con lo que se evitan y eliminan los bucles. Para obtener más información sobre el STP clásico, consulte **Definición de la configuración global de STP**.
- Rapid STP (STP rápida): detecta y utiliza topologías de red que proporcionan una convergencia más rápida del árbol de extensión, sin crear bucles de reenvío. Si se ha activado RSTP en el dispositivo, pero en el dispositivo vecino se ha activado STP, el dispositivo local utiliza STP.

  Para obtener más información sobre el RSTP, consulte **Definición del árbol de extensión rápida**.
- Multiple STP (STP múltiple): proporciona total conectividad para los paquetes asignados a cualquier VLAN. El STP múltiple se basa en el RSTP. Además, el STP múltiple transmite paquetes asignados a distintas redes VLAN a través de distintas regiones MST. Las regiones MST actúan como un único puente si se ha activado MSTP en el dispositivo. No obstante, si se ha activado RSTP en el dispositivo vecino y el dispositivo local utiliza STP, RSTP y MSTP, ambos dispositivos pueden interoperar.

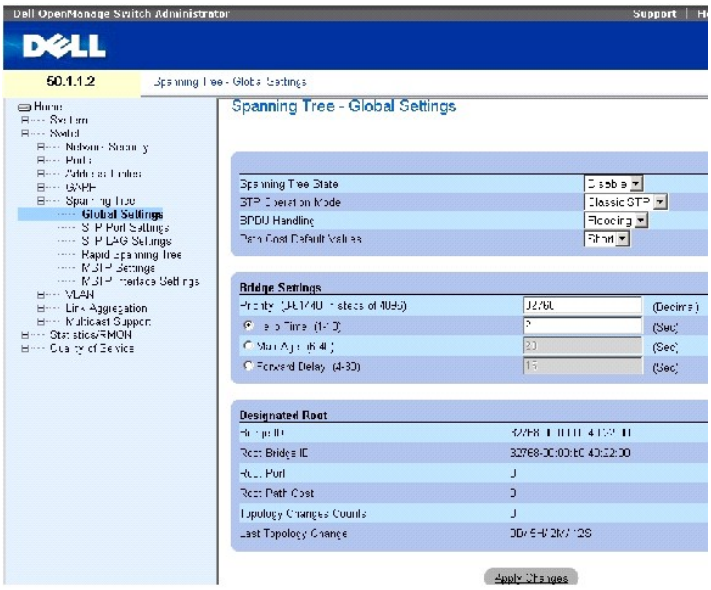
Para obtener más información sobre el STP múltiple, consulte **Configuración del árbol de extensión múltiple**.

Para abrir la página **Spanning Tree** (Árbol de extensión), haga clic en **Switch** (Conmutador) → **Spanning Tree** (Árbol de extensión) en la vista de árbol.

Definición de la configuración global de STP

La página Spanning Tree Global Settings (Configuración global del árbol de extensión) contiene campos para activar STP en el dispositivo. Para abrir la página Spanning Tree Global Settings (Configuración global del árbol de extensión), haga clic en **Switch** (Conmutador) → **Spanning Tree** (Árbol de extensión) → **Global Settings** (Configuración global) en la vista de árbol.

Figura 7-22. Spanning Tree Global Settings



La página Spanning Tree Global Settings (Configuración global del árbol de extensión) contiene los campos siguientes:

Spanning Tree State (Estado del árbol de extensión): activa o desactiva STP, RSTP o MSTP en el dispositivo.

STP Operation Mode (Modo de funcionamiento de STP): indica el modo STP mediante el cual se activa el STP en el dispositivo. Los valores del campo posibles son:

Classic STP (STP clásico): activa el STP clásico en el dispositivo. Éste es el valor predeterminado.

Rapid STP (STP rápida): activa el RSTP en el dispositivo.

Multiple STP (STP múltiple): activa el STP múltiple en el dispositivo.

BPDU Handling (Manipulación de BDPU): determina cómo se gestionan los paquetes BPDU si se ha desactivado STP en el puerto o dispositivo. Los paquetes BPDU se utilizan para transmitir información del árbol de extensión. Los valores del campo posibles son:

Filtering (Filtrado): filtra los paquetes BPDU cuando el árbol de extensión está desactivado en una interfaz. Éste es el valor predeterminado.

Flooding (Distribución): distribuye los paquetes BPDU cuando el árbol de extensión está desactivado en una interfaz.

Path Cost Default Values (Valores predeterminados del coste de ruta): especifica el método utilizado para asignar los costes de la ruta predeterminada a los puertos STP. Los valores del campo posibles son:

Short (Corto): especifica el intervalo de 1 a 65.535 para los costes de ruta de puerto. Éste es el valor predeterminado.

Long (Largo): especifica el intervalo de 1 a 200.000.000 para los costes de ruta de puerto.

Los costes de la ruta predeterminada asignados a una interfaz varían en función del método seleccionado.

Interfaz	Largo	Corto
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

Priority (0-65535) (Prioridad [0-65535]): especifica el valor de prioridad del puente. Cuando los conmutadores o puentes ejecutan el STP, se asigna una prioridad a cada uno. Después de intercambiar paquetes BPDU, el dispositivo que tiene el valor de prioridad menor se transforma en el puente raíz. El valor predeterminado es 32768. El valor de prioridad de puerto se proporciona en incrementos de 4096; por ejemplo, 4096, 8192, 12288, y así sucesivamente.

Hello Time (1-10) (Tiempo de saludo [1-10]): especifica el tiempo de saludo del dispositivo. Esto indica la cantidad de tiempo en segundos durante el que espera un puente raíz entre los mensajes de configuración. El valor predeterminado es 2 segundos.

Max Age (6-40) (Caducidad máxima [6-40]): especifica el tiempo máximo de caducidad del dispositivo. Esto indica la cantidad de tiempo en segundos durante el que espera un puente raíz antes de enviar mensajes de configuración. El tiempo máximo de caducidad predeterminado es 20 segundos.

Forward Delay (4-30) (Demora de reenvío [4-30]): especifica el tiempo de demora de reenvío del dispositivo. Esto indica la cantidad de tiempo en segundos durante el que un puente permanece en los estados de escucha y de obtención antes de reenviar paquetes. El valor predeterminado es 10 segundos.

Bridge ID (ID de puente): identifica la prioridad del puente y la dirección MAC.

Root Bridge ID (ID de puente raíz): identifica la prioridad del puente raíz y la dirección MAC.

Root Port (Puerto raíz): indica el número de puerto que ofrece la ruta de menor coste desde este puente hasta el puente raíz. Es significativo cuando el puente no es la raíz.

Root Path Cost (Coste de la ruta raíz): coste de la ruta desde este puente hasta la raíz.

Topology Changes Counts (Recuentos de cambios de topología): especifica la cantidad total de cambios de estado de STP que se han producido

Last Topology Change (Último cambio de topología): indica la cantidad de tiempo transcurrido desde que se ha inicializado o restablecido el puente y desde que se ha producido el último cambio topográfico. El tiempo se muestra con el formato D/H/M/S; por ejemplo, 2D/5H/10M/4S.

Definición de los parámetros globales de STP

1. Abra la página.
2. Seleccione **Enable** (Activar) en el campo **Spanning Tree State** (Estado del árbol de extensión).
3. Seleccione el modo **STP** en el campo **STP Operation Mode** (Modo de funcionamiento de STP) y defina la configuración del puente.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El STP se activa en el dispositivo.

Modificación de los parámetros globales de STP

1. Abra la página.
2. Defina los campos del diálogo.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros de STP y se actualiza el dispositivo.

Definición de los parámetros globales de STP con comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para definir parámetros globales de STP como se muestra en la página **Spanning Tree Global Settings** (Configuración global del árbol de extensión).

Tabla 7-14. Comandos de la CLI para los parámetros globales de STP

Comando de la CLI	Descripción
spanning-tree	Activa la funcionalidad del árbol de extensión.
spanning-tree mode {**stp** | **rstp** | **mstp**}	Configura el modo del protocolo del árbol de extensión.
spanning-tree priority prioridad	Configura la prioridad del árbol de extensión.
spanning-tree hello-time *segundos*	Configura el tiempo de saludo del puente del árbol de extensión, que es la frecuencia con la que el dispositivo transmite mensajes de saludo a otros dispositivos.
spanning-tree max-age *segundos*	Configura la caducidad máxima del puente del árbol de extensión.
spanning-tree forward- time segundos	Configura el tiempo de reenvío del puente del árbol de extensión, que es el tiempo durante el cual un puerto permanece en los estados de escucha y de obtención antes de pasar al estado de reenvío.
show spanning-tree [**ethernet** *interfaz* | **port-channel** *número- canal-puerto*] [**instance** *id-instancia*]	Muestra la configuración del árbol de extensión.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *id-instancia*]	Muestra información detallada sobre el árbol de extensión en los puertos activos o bloqueados.
show spanning-tree mst- configuration	Muestra el identificador de configuración MST del árbol de extensión.

S

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288
```

```
console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 12

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree
```

Spanning tree enabled mode MSTP							
Default port cost method: short							
Gathering information							
###### MST 0 Vlans Mapped:			16-4094				
CST Root ID Priority 20480							
	Address		00:30:ab:00:00:08				
	Path Cost		4				
	Root Port		ch2				
	This switch is the IST master						
	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec						
Bridge ID Priority			32768				
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e2	enabled	128.2	100	DSBL	Dsbl	No	P2p Intr
1/e3	enabled	128.3	100	DSBL	Dsbl	No	P2p Intr
1/e4	enabled	128.4	100	DSBL	Dsbl	No	P2p Intr

1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr

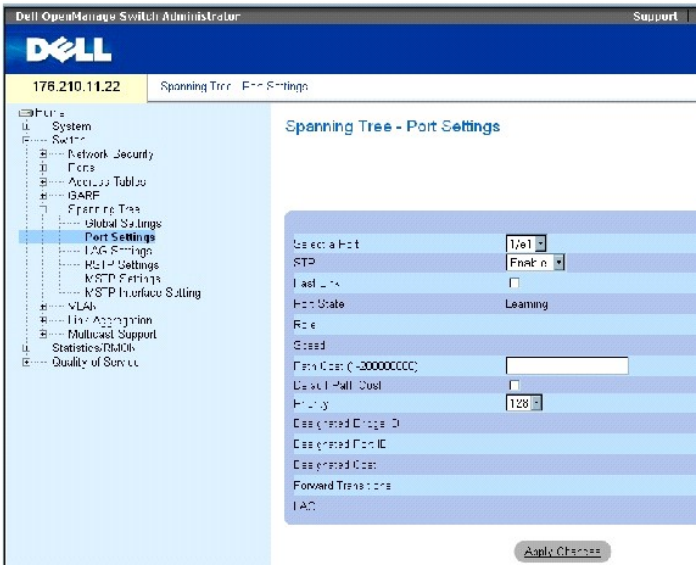
```
console# show spanning-tree active
Spanning tree enabled mode MSTP
Default port cost method: short
Gathering information ..........
###### MST 0 Vlans Mapped: 16-4094
CST Root ID Priority 20480
         Address                00:30:ab:00:00:08
         Path Cost              4
         Root Port              ch2
         This switch is the IST master
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority              32768
         Address                00:00:00:16:00:64
         Max hops               20

Name   State    Prio.Nbr  Cost  Sts  Role  PortFast  Type
----   -----    -------   ----  ---  ----  -------   ----
```

1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)
1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr
1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

Definición de la configuración STP de puertos

Utilice la página Spanning Tree Port Settings (Configuración de puertos del árbol de extensión) para asignar propiedades STP a puertos individuales. Para abrir la página Spanning Tree Port Settings (Configuración de puertos del árbol de extensión), haga clic en **Switch** (Conmutador) → **Spanning Tree** (Árbol de extensión) → **Port Settings** (Configuración de puertos) en la vista de árbol.

Figura 7-23. Spanning Tree Port Settings



La página Spanning Tree Port Settings (Configuración de puertos del árbol de extensión) contiene los campos siguientes:

Select a Port (Seleccionar un puerto): especifica el número de puerto en el que deben modificarse los valores de STP.

STP: activa o desactiva el STP en el puerto.

Fast Link (Enlace rápido): si se selecciona esta opción, activa el modo de enlace rápido para el puerto. Si se activa el modo de enlace rápido para un puerto, el valor de **Port State** (Estado del puerto) se establece automáticamente en el estado **Forwarding** (Reenvío) si el enlace del puerto está activo. El modo de enlace rápido optimiza el tiempo necesario para la convergencia del protocolo STP. La convergencia de STP puede tardar unos 30-60 segundos en redes de gran tamaño.

Port State (Estado de puerto): indica el estado STP actual de un puerto. Si está activado, el estado del puerto determina qué acción de reenvío se realiza con el tráfico. El puerto puede tener estos estados:

Disabled (Desactivado): STP está desactivado en el puerto. El puerto reenvía el tráfico a la vez que obtiene direcciones MAC.

Blocking (Bloqueo): indica que el puerto está bloqueado actualmente y que no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC. El bloqueo se muestra si se ha activado el STP clásico.

Listening (Escucha): el puerto está actualmente en el modo de escucha. No puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): el puerto está actualmente en el modo de obtención. No puede reenviar tráfico pero sí obtener direcciones MAC nuevas.

Forwarding (Reenvío): el puerto está actualmente en el modo de reenvío. Puede reenviar tráfico y obtener direcciones MAC nuevas.

Role (Función): indica la función de puerto asignada por el algoritmo STP que proprociona rutas STP. Los valores del campo posibles son:

Root (Raíz): proporciona la ruta de coste inferior para reenviar paquetes al conmutador raíz.

Designated (Designado): indica el puerto a través del que el conmutador designado se conecta a la LAN.

Alternate (Alternativo): proporciona una ruta alternativa al conmutador raíz desde la interfaz raíz.

Backup (Reserva): proporciona una ruta de reserva para la ruta de puerto designada hacia las hojas del árbol de extensión. Los puertos de reserva sólo existen si hay dos puertos conectados en un bucle mediante un enlace de punto a punto. Los puertos de reserva también existen si una LAN tiene dos o más conexiones conectadas a un segmento compartido.

Disabled (Desactivado): indica que el puerto no participa en el árbol de extensión.

Speed (Velocidad): velocidad de funcionamiento del puerto.

Path Cost (1-200000000) (Coste de ruta [1-200000000]): indica la contribución del puerto al coste de la ruta raíz. El coste de la ruta se ajusta a un valor mayor o menor y se utiliza para reenviar el tráfico cuando se redirecciona la ruta.

Default Path Cost (Coste de la ruta predeterminada): indica el coste de la ruta predeterminada. Los valores predeterminados para los costes de ruta larga son:

Ethernet: 2.000.000

Fast Ethernet: 200.000

Gigabit Ethernet: 20.000

Los valores predeterminados para los costes de ruta corta son:

Ethernet: 100

Fast Ethernet: 19

Gigabit Ethernet: 4

Priority (0-240, in steps of 16) (Prioridad [0-240, en pasos de 16]): valor de prioridad del puerto. El valor de prioridad influye en la selección del puerto cuando un puente tiene dos puertos conectados en un bucle. El valor de prioridad oscila entre 0 y 240 y se proporciona en incrementos de 16.

Designated Bridge ID (ID del puente designado): indica la prioridad del puente y la dirección MAC del puente designado.

Designated Port ID (ID del puerto designado): indica la prioridad y la interfaz del puerto designado.

Designated Cost (Coste designado): indica el coste del puerto que participa en la topología STP. Los puertos cuyo coste es menor presentan menos probabilidad de ser bloqueados si STP detecta bucles.

Forward Transmission (Transmisión de reenvío): indica el número de veces que el puerto ha pasado del estado **Forwarding** (Reenvío) al estado **Blocking** (Bloqueo).

LAG: indica el LAG al que está conectado el puerto.

Activación de STP en un puerto

1. Abra la página Spanning Tree **Port Settings** (Configuración de puertos del árbol de extensión).
2. Seleccione el puerto.
3. Seleccione **Enabled** (Activado) en el campo **STP**.
4. Defina los campos **Fast Link** (Enlace rápido), **Path Cost** (Coste de ruta) y **Priority** (Prioridad).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El STP se activa en el puerto.

Modificación de las propiedades STP del puerto

1. Abra la página Spanning Tree Port Settings (Configuración de puertos del árbol de extensión).
2. Seleccione el puerto.
3. Modifique los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros STP del puerto y se actualiza el dispositivo.

Visualización de la tabla de puertos STP

1. Abra la página Spanning Tree Port Settings (Configuración de puertos del árbol de extensión).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de puertos STP.

Definición de la configuración de los puertos STP con comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para definir parámetros STP de puertos como se muestra en la página **STP Port Settings** (Configuración STP de puertos).

Tabla 7-15. Comandos de la CLI para la configuración STP de puertos

Comando de la CLI	Descripción
spanning-tree disable	Desactiva el árbol de extensión en un puerto específico.
spanning-tree cost coste	Configura la contribución del coste del árbol de extensión de un puerto.
spanning-tree port-priority prioridad	Configura la prioridad del puerto.
show **spanning-tree** [**ethernet** interfaz | **port-channel** número-canal- puerto] [**instance** *id- instancia*]	Muestra la configuración del árbol de extensión.
spanning-tree portfast	Activa el modo PortFast.
show spanning-tree [detail] [**active** | **blockedports**] [**instance** *id-instancia*]	Muestra información detallada sobre el árbol de extensión en los puertos activos o bloqueados.
show spanning-tree mst- configuration	Muestra el identificador de configuración MST del árbol de extensión.

A continuación se muestra un ejemplo de los comandos de la CLI:

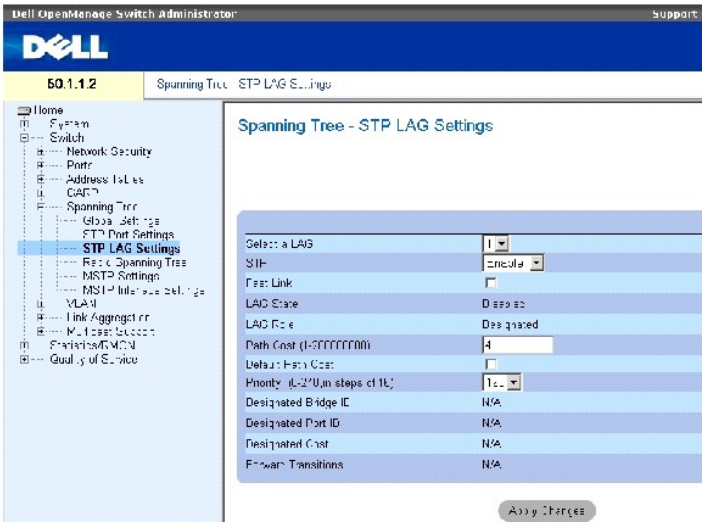
```
console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e15
```

```
Port 1/e15 enabled

State: forwarding                                  Role: designated

Port id: 128.15                                    Port cost: 19

Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)

Designated bridge Priority : 32768                 Address: 00:00:00:16:00:64

Designated port id: 128.15                         Designated path cost: 4

Guard root: Disabled

Number of transitions to forwarding state: 2

BPDU: sent 483, received 1037

console# show spanning-tree ethernet 1/e15 instance 12

Port 1/e15 enabled

State: discarding                                  Role: alternate

Port id: 128.15                                    Port cost: 19

Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)

Designated bridge Priority : 32768                 Address: 00:00:b0:07:07:49

Designated port id: 128.11                         Designated path cost: 0

Guard root: Disabled

Number of transitions to forwarding state: 3

BPDU: sent 482, received 1035
```

Definición de la configuración STP de LAG

Utilice la página **Spanning Tree LAG Settings** (Configuración de LAG del árbol de extensión) para asignar parámetros de agregado de puertos STP. Para abrir la página Spanning Tree LAG Settings (Configuración de LAG del árbol de extensión), haga clic en **Switch** (Conmutador)→ **Spanning Tree** (Árbol de extensión) → **LAG Settings** (Configuración de LAG) en la vista de árbol.

Figura 7-24. Spanning Tree LAG Settings



La página **Spanning Tree LAG Settings** (Configuración de LAG del árbol de extensión) contiene los siguientes campos:

Select a LAG (Seleccionar un LAG): indica el número de LAG cuya configuración de STP se desea modificar.

STP: activa o desactiva el STP en el LAG.

Fast Link (Enlace rápido): activa el modo de enlace rápido para el LAG. Si se activa el modo de enlace rápido para un LAG, el valor de **LAG State** (Estado del LAG) se establece automáticamente en el estado **Forwarding** (Reenvío) si LAG está activo. El modo de enlace rápido optimiza el tiempo necesario para la convergencia del protocolo STP. La convergencia de STP puede tardar unos 30-60 segundos en redes de gran tamaño.

LAG State (Estado del LAG): indica el estado STP actual de un LAG. Si está activado, el estado del LAG determina qué acción de reenvío se realiza con el tráfico. Si el puente descubre un LAG que no funciona correctamente, el LAG se coloca en el estado **Broken** (Interrumpido). El LAG puede tener estos estados:

Disabled (Desactivado): STP está desactivado en el LAG. El LAG reenvía el tráfico a la vez que obtiene direcciones MAC.

Blocking (Bloqueado): el LAG está bloqueado y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC.

RSTP Discarding State (Estado Descartando de RSTP): en este estado el puerto no obtiene direcciones MAC y no reenvía tramas.

Este estado es la unión del estado Bloquing (Bloqueado) y Listening (Escucha) introducido en STP (802.1.D).

Listening (Escucha): el LAG se encuentra en modo de escucha y no puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): el LAG se encuentra en modo de obtención y no puede reenviar tráfico, pero puede obtener direcciones MAC nuevas.

Forwarding (Reenvío): el LAG se encuentra en el modo de reenvío y puede reenviar tráfico y obtener direcciones MAC.

Broken (Interrumpido): el LAG no funciona correctamente y no puede utilizarse para reenviar tráfico.

LAG Role (Función de LAG): indica la función de LAG asignada por el algoritmo STP que proporciona rutas STP. Los valores del campo posibles son:

Root (Raíz): proporciona la ruta de coste inferior para reenviar paquetes al conmutador raíz.

Designated (Designado): indica el LAG a través del cual el conmutador designado se conecta a la LAN.

Alternate (Alternativo): proporciona un LAG alternativo al conmutador raíz desde la interfaz raíz.

Backup (Reserva): proporciona una ruta de reserva para la ruta de puerto designada hacia las hojas del árbol de extensión. Los puertos de reserva sólo existen si hay dos puertos conectados en un bucle mediante un enlace de punto a punto. Los puertos de reserva también existen si una LAN tiene dos o más conexiones conectadas a un segmento compartido.

Disabled (Desactivado): indica que el LAG no participa en el árbol de extensión.

Path Cost (1-200000000) (Coste de ruta [1-200000000]): indica la contribución del LAG al coste de la ruta raíz. El coste de la ruta se ajusta a un valor mayor o menor y se utiliza para reenviar el tráfico cuando se redirecciona la ruta. El coste de la ruta tiene un valor de 1 a 200000000.

Default Path Cost (Coste de ruta predeterminada): indica si se utiliza el coste de la ruta predeterminada. Los valores predeterminados del coste de la ruta del LAG son:

Long Method for LAG **(Método largo para LAG): 20.000**

Short Method for LAG **(Método corto para LAG):** 4

Priority (0-240, in steps of 16) (Prioridad [0-240, en pasos de 16]): valor de prioridad del LAG. El valor de prioridad influye en la elección del LAG cuando un puente tiene puertos en bucle. El valor de prioridad oscila entre 0 y 240, en pasos de 16.

Designated Bridge ID (ID del puente designado): indica la prioridad y la dirección MAC del puente designado.

Designated Port ID (ID del puerto designado): ID de la interfaz seleccionada.

Designated Cost (Coste designado): indica el coste del puerto que participa en la topología STP. Los puertos cuyo coste es menor presentan menos probabilidad de ser bloqueados si STP detecta bucles.

Forward Transitions (Transiciones de reenvío): número de veces que el valor de **LAG State** (Estado del LAG) ha pasado del estado **Forwarding** (Reenvío) a un estado **Blocking** (Bloqueado).

Modificación de los parámetros STP del LAG

1. Abra la página **Spanning Tree LAG Settings** (Configuración del LAG del árbol de extensión).
2. Seleccione un LAG en el menú desplegable **Select a LAG** (Seleccionar un LAG).
3. Modifique los campos según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros STP del LAG y se actualiza el dispositivo.

Definición de la configuración STP del LAG mediante los comandos de la CLI

La siguiente tabla incluye los comandos de la CLI para definir la configuración STP del LAG.

Tabla 7-16. Comandos de la CLI para la configuración STP del LAG

Comando de la CLI	Descripción
`spanning-tree`	Activa el árbol de extensión.
`spanning-tree disable`	Desactiva el árbol de extensión en un LAG específico.
`spanning-tree cost` *`coste`*	Configura la contribución del coste del árbol de extensión de un LAG.
`spanning-tree port-priority` *`prioridad`*	Configura la prioridad del puerto.
`show spanning-tree [`**`ethernet`** `interfaz |` **`port-channel`** *`número-canal- puerto`*`] [`**`instance`** *`id- instancia`*`]`	Muestra la configuración del árbol de extensión.
`show spanning-tree [detail] [active | blockedports] [`**`instance`** *`id-instancia`*`]`	Muestra información detallada sobre el árbol de extensión en los puertos activos o bloqueados.

A continuación se muestra un ejemplo de los comandos de la CLI:

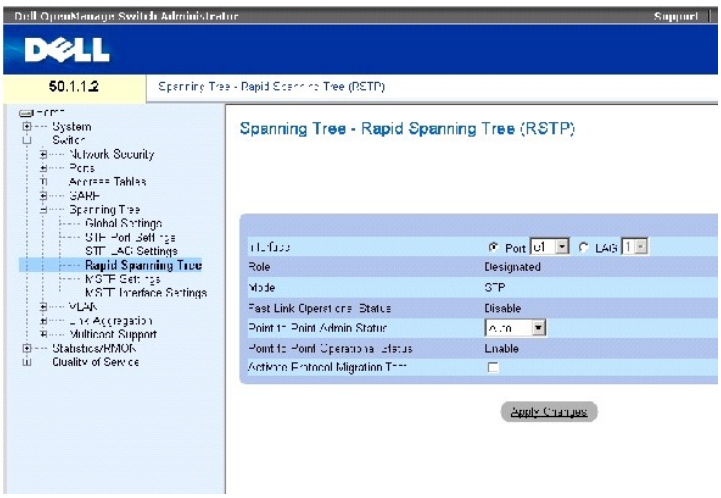
```
console(config)# interface
port-channel 1

console(config-if)#
spanning-tree disable

console(config-if)#
spanning-tree cost 35000

console(config-if)#
spanning-tree port-
priority 96

console(config-if)#
spanning-tree portfast
```

Definición del árbol de extensión rápida

Si bien el árbol de extensión clásico impide los bucles de reenvío de nivel 2 en una topología de red general, la convergencia puede tardar de 30 a 60 segundos. La demora permite tener tiempo para detectar posibles bucles y propagar cambios de estado.

El protocolo de árbol de extensión rápida (RSTP) detecta y utiliza topologías de red que permiten una convergencia más rápida del árbol de extensión, sin crear bucles de reenvío. Para abrir la página Rapid Spanning Tree (RSTP) settings (Configuración del árbol de extensión rápida [RSTP]), haga clic en **Switch** (Conmutador) → **Spanning Tree** (Árbol de extensión) → **Rapid Spanning Tree** (Árbol de extensión rápida) en la vista de árbol.

Figura 7-25. Rapid Spanning Tree (RSTP) settings



La página Spanning Tree RSTP (RSTP de árbol de expansión) contiene los siguientes campos:

Interface (Interfaz): puerto o LAG para el que se pueden visualizar y editar valores de RSTP.

State (Estado): desactiva el estado de RSTP de la interfaz seleccionada.

Role (Función): indica la función de puerto asignada por el algoritmo STP para proporcionar rutas STP. Los valores del campo posibles son:

Root (Raíz): proporciona la ruta de coste inferior para reenviar paquetes al conmutador raíz.

Designated (Designado): indica el puerto o el LAG a través del que el conmutador designado se conecta a la LAN.

Alternate (Alternativo): proporciona una ruta alternativa al conmutador raíz desde la interfaz raíz.

Backup (Reserva): proporciona una ruta de reserva para la ruta de puerto designada hacia las hojas del árbol de extensión. Los puertos de reserva sólo existen si hay dos puertos conectados en un bucle mediante un enlace de punto a punto. Los puertos de reserva también existen si una LAN tiene dos o más conexiones conectadas a un segmento compartido.

Disabled (Desactivado): indica que el puerto no participa en el árbol de extensión.

Mode (Modo): indica el modo actual del árbol de extensión. El módo del árbol de extensión se selecciona en la página Spanning Tree Global Settings (Configuración global del árbol de extensión). Los valores del campo posibles son:

Classic STP (STP clásico): indica que el STP clásico está activado en el dispositivo.

Rapid STP (STP rápida): indica que el RSTP está activado en el dispositivo.

Multiple STP (STP múltiple): indica que el STP múltiple está activado en el dispositivo.

Fast Link Operational Status (Estado operativo del enlace rápido): indica si el enlace rápido está activado o desactivado para el puerto o el LAG. Si el enlace rápido está activado para una interfaz, ésta se coloca automáticamente en el estado de reenvío.

Point-to-Point Admin Status (Estado de administrador de punto a punto): activa o desactiva el dispositivo para establecer un enlace punto a punto, o especifica que el dispositivo establezca automáticamente un enlace punto a punto.

Para establecer comunicaciones a través de un enlace punto a punto, el PPP que lo origina envía primero paquetes de protocolo de control de enlace (LCP) para configurar y probar el enlace de datos. Una vez que se ha establecido un enlace y que el LCP ha negociado según proceda los recursos opcionales, el PPP que origina el enlace envía paquetes de protocolo de control de red (NCP) para seleccionar y configurar uno o más protocolos de nivel de red. Cuando se han configurado todos los protocolos de nivel de red seleccionados, los paquetes de cada protocolo de nivel de red pueden enviarse a través del enlace. El enlace permanece configurado para las comunicaciones hasta que paquetes LCP o NCP explícitos cierran el enlace o hasta que se produce algún suceso externo. Éste es el tipo de enlace de puerto de conmutador real. Puede ser distinto del estado de administración.

Point-to-Point Operational Status (Estado operativo punto a punto): indica el estado operativo punto a punto.

Activate Protocol Migrational (Activar migración de protocolo): si se selecciona esta opción, PPP puede enviar paquetes LCP (protocolo de control de enlace) para configurar y probar el enlace de datos.

Definición de parámetros RSTP

1. Abra la página Spanning Tree RSTP Settings (Configuración de RSTP del árbol de extensión).
2. Seleccione una interfaz.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros de RSTP y se actualiza el dispositivo.

Visualización de la tabla del árbol de extensión rápida (RSTP)

1. Abra la página Rapid Spanning Tree (RSTP) (Árbol de extensión rápida).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla del árbol de extensión rápida (RSTP).

Definición de los parámetros del RSTP mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para definir parámetros de STP rápida como se muestra en la página Rapid Spanning Tree (RSTP) (Árbol de extensión rápida [RSTP]).

Tabla 7-17. Comando de la CLI para configurar RSTP

Comando de la CLI	Descripción
`spanning-tree link-type {point-to-point | shared}`	Reemplaza el valor del tipo de enlace predeterminado.
`spanning tree mode {stp | rstp | mstp}`	Configura el protocolo de árbol de extensión que se está ejecutando actualmente.
`clear spanning-tree detected-protocols [ethernet interfaz | port-channel número- canal-puerto]`	Reinicia el proceso de migración de protocolo.
`show spanning-tree [ethernet interfaz | port-channel número- canal-puerto]`	Muestra la configuración del árbol de extensión.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface ethernet 1/e5
```

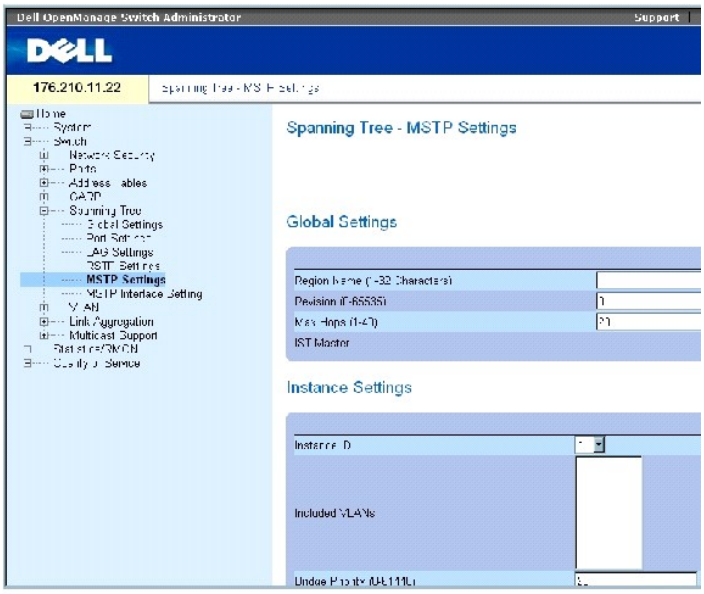
```
console(config-if)# spanning-tree link-type shared

console(config-if)# spanning tree mode rstp
```

Configuración del árbol de extensión múltiple

MSTP correlaciona las redes VLAN en instancias de STP. El árbol de extensión múltiple proporciona un escenario de equilibrado de carga distinto. Por ejemplo, mientras el puerto A está bloqueado en una instancia de STP, el mismo puerto se coloca en el estado Forwarding (Reenvío) en otra instancia de STP.

Además, los paquetes asignados a varias redes VLAN se transmiten a través de distintas rutas de las regiones de árboles de extensión múltiples (Regiones de MST). Las zonas son uno o varios puentes de árboles de extensión múltiples a través de los cuales pueden transmitirse tramas. Para abrir la página MSTP Settings (Configuración de MSTP), haga clic en Switch (Conmutador) → Spanning Tree (Árbol de extensión) → MSTP Settings (Configuración de MSTP) en la vista de árbol.

Figura 7-26. MSTP Settings



La página MSTP Settings (Configuración de MSTP) contiene los campos siguientes:

Region Name (1-32 Characters) (Nombre de región [1-32 caracteres]): indica el nombre de región de MSTP definido por el usuario.

Revision (0-65535) (Revisión [0-65535]): define un número sin signo de 16 bits que identifica la revisión de la configuración de MST actual. El número de revisión es necesario como parte de la configuración de MST. El intervalo de campo posible es 0-65535.

Max Hops (1-40) (Número máximo de saltos [1-40]): define el número total de saltos que se producen en una región específica antes de que se descarte el paquete BPDU. Una vez que se ha descartado el paquete BPDU, la información del puerto caduca. El intervalo de valores posibles de este campo es 1-40 y el valor predeterminado es 20 saltos.

IST Master (Maestro de IST): indica la ID del maestro del árbol de extensión interno (IST). El maestro de IST es la raíz 0 de la instancia.

Instance ID (ID de instancia): define la instancia de MSTP. El intervalo de valores posibles de este campo es 1-15.

Included VLANs (Redes VLAN incluidas): muestra las redes VLAN asignadas a la instancia seleccionada. Cada VLAN pertenece a una instancia.

Bridge Priority (0-61440) (Prioridad de puente [0-61440]): especifica la prioridad del dispositivo de instancia de árbol de extensión seleccionado. El intervalo de valores posibles del campo es 0-61440 en pasos de 4096.

Designated Root Bridge ID (ID de puente raíz designado): indica la ID del puente raíz de la instancia seleccionada.

Root Port (Puerto raíz): indica el puerto raíz de la instancia seleccionada.

Root Path Cost (Coste de la ruta raíz): indica el coste de la ruta de la instancia seleccionada.

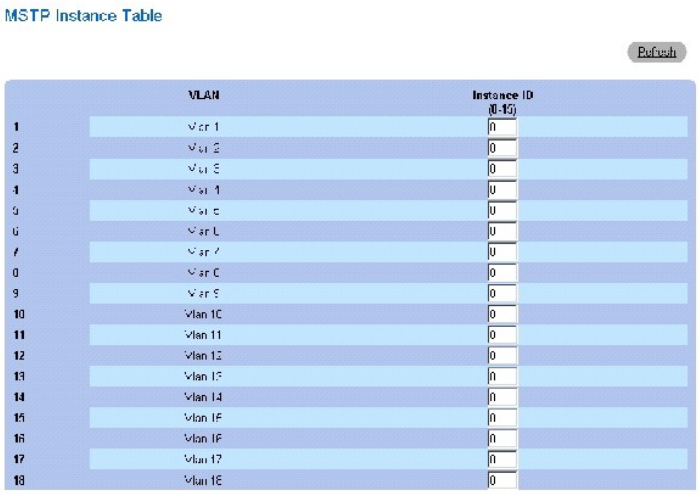
Bridge ID (ID de puente): indica la ID de puente de la instancia seleccionada.

Remaining Hops (Saltos restantes): indica el número de saltos que faltan hasta el siguiente destino.

Visualización de la página MSTP Instance Table (Tabla de instancias MSTP)

1. Abra la página **Spanning Tree** MSTP Settings (Árbol de extensión).
2. Haga clic en **Show All** (Mostrar todo) para abrir la tabla de instancias MSTP (MSTP Instance Table).

Figura 7-27. MSTP Instance Table



Definición de instancias MST mediante los comandos de la CLI

La siguiente tabla muestra un resumen de los comandos de la CLI equivalentes para definir grupos de instancias MST como se muestra en la página **Spanning Tree** MSTP Settings (Configuración MSTP del árbol de extensión).

Tabla 7-18. Comandos de la CLI para instancias de MSTP

Comando de la CLI	Descripción
`spanning-tree mst configuration`	Entra en el modo de configuración de MST.

instance ID-instancia {add | remove} vlan intervalo-vlan	Asigna redes VLAN a la instancia de MST.
name cadena	Establece el nombre de la configuración.
revision valor	Establece el número de la revisión de la configuración.
spanning-tree **mst** id- instancia port-priority prioridad	Establece la prioridad de un puerto.
spanning-tree mst id- instancia priority prioridad	Establece la prioridad del dispositivo para la instancia de árbol de extensión especificada.
spanning-tree mst max- hops número-saltos	Establece el número de saltos en una región de MST antes de que se descarte el paquete BPDU y que caduque la información guardada para un puerto.
spanning-tree mst id- instancia **cost** coste	Establece el coste de la ruta del puerto para cálculos de MST.
exit	Sale del modo de configuración de la región de MST y aplica cambios de configuración.
abort	Sale del modo de configuración de la región de MST sin aplicar cambios de configuración.
show {current | pending}	Muestra la configuración de la región de MST actual o pendiente.

A continuación se muestra un ejemplo de los comandos de la CLI:

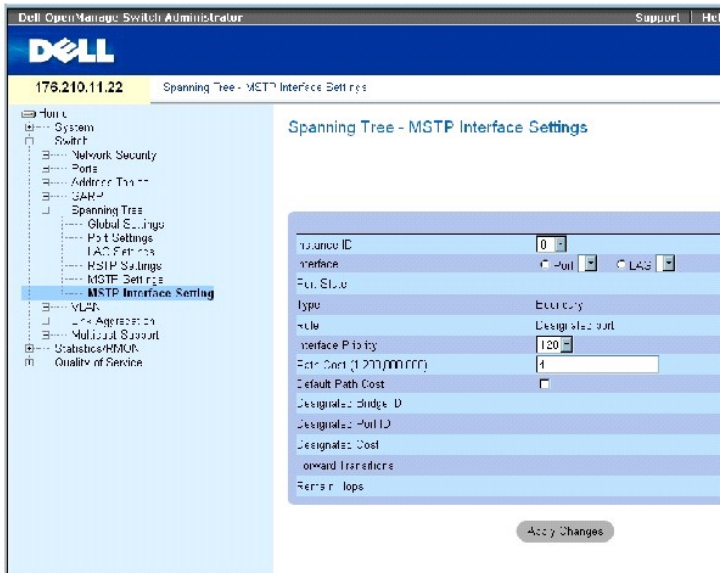
```
console(config)# spanning-tree mst configuration

console(config-mst)# instance 1 add vlan 10-20

console(config-mst)# name region1

console(config-mst)# revision 1

console(config)# spanning-tree mst configuration

console(config-mst)# instance 2 add vlan 21-30

console(config-mst)# name region1

console(config-mst)# revision 1

console(config-mst)# show pending

Pending MST configuration

Name: Region1
```

```
Revision: 1

Instance Vlans Mapped

-------- ------------

0 1-9,31-4094

1 10-20

2 21-30
```

Definición de la configuración de la interfaz MSTP

La página MSTP Interface Settings (Configuración de la interfaz MSTP) contiene parámetros que asignan valores de MSTP a interfaces específicas. Para abrir la página MSTP Interface Settings (Configuración de la interfaz MSTP), haga clic en Switch (Conmutador) → Spanning Tree (Árbol de extensión) → MSTP Interface Settings (Configuración de la interfaz MSTP) en la vista de árbol.

Figura 7-28. MSTP Interface Settings



La página MSTP Interface Settings (Configuración de la interfaz MSTP) contiene los campos siguientes:

Instance ID (ID de instancia): indica las instancias MSTP configuradas en el dispositivo. El intervalo de valores posibles del campo es 1-15.

Interface (Interfaz): asigna puertos o grupos LAG a la instancia MSTP seleccionada.

Port State (Estado del puerto): indica si el puerto está activado o desactivado en la instancia específica.

Type (Tipo): indica si MSTP trata el puerto como un puerto de punto a punto, o como un puerto conectado a un concentrador, y si el puerto es interno en la región de MST o se trata de un puerto de límite. Un puerto maestro proporciona conectividad desde una región de MSTP a la raíz CIST externa. Un puerto de límite conecta los puentes MST a la LAN en una región externa. Si el puerto es un puerto de límite, también indica si el dispositivo del otro lado del enlace funciona en modo RSTP o STP.

Role (Función): indica la función de puerto asignada por el algoritmo STP para proporcionar rutas STP. Los valores del campo posibles son:

Root (Raíz): proporciona la ruta de coste inferior para reenviar paquetes al dispositivo raíz.

Designated (Designado): indica el puerto o el LAG a través del que el dispositivo designado se conecta a la LAN.

Alternate (Alternativo): proporciona una ruta alternativa al dispositivo raíz desde la interfaz raíz.

Backup (Reserva): proporciona una ruta de reserva para la ruta de puerto designada hacia las hojas del árbol de extensión. Los puertos de reserva sólo existen si hay dos puertos conectados en un bucle mediante un enlace de punto a punto. Los puertos de reserva también existen si una LAN tiene dos o más conexiones conectadas a un segmento compartido.

Disabled (Desactivado): indica que el puerto no participa en el árbol de extensión.

Interface Priority (0-240, in steps of 16) (Prioridad de la interfaz [0-240, en pasos de 16]): define la prioridad de la instancia especificada. El valor predeterminado es 128.

Path Cost- (Coste de ruta): indica la contribución del puerto a la instancia del árbol de extensión. El intervalo siempre debería ser 1-200.000.000.

Default Path Cost (Coste de la ruta predeterminada): indica que el coste de la ruta predeterminada se asigna según el método seleccionado en la página Spanning Tree Global Settings (Configuración global del árbol de extensión).

Designated Bridge ID (ID del puente designado): indica el número de la ID que conecta el enlace o la LAN compartida a la raíz.

Designated Port ID (ID del puerto designado): indica el número de la ID del puerto en el puente designado que conecta el enlace o la LAN compartida a la raíz.

Designated Cost (Coste designado): indica el coste de la ruta desde el enlace o la LAN compartida a la raíz.

Forward Transitions (Transiciones de reenvío): indica el número de veces que el puerto pasa al estado **Forwarding** (Reenvío).

Remaining Hops (Saltos restantes): indica el número de saltos que faltan hasta el siguiente destino.

Definición de la configuración de la interfaz MSTP

1. Abra la página MSTP Interface Settings (Configuración de la interfaz de MSTP).
2. Seleccione una interfaz.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

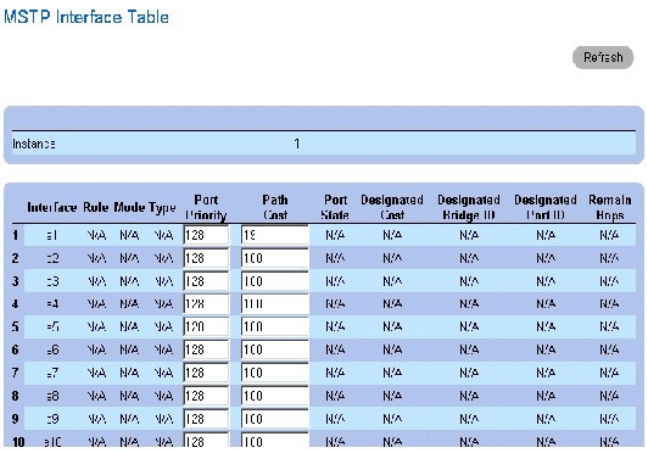
Se definen los parámetros de MSTP y se actualiza el dispositivo.

Visualización de la tabla de interfaces de MSTP

1. Abra la página MSTP Interface Settings (Configuración de la interfaz de MSTP).
2. Haga clic en Show All (Mostrar todo).

Se abre la página MSTP Interface Table (Tabla de interfaces de MSTP):

Figura 7-29. MSTP Interface Table



Definición de interfaces de MSTP mediante los comandos de la CLI

La siguiente tabla muestra un resumen de los comandos de la CLI equivalentes para definir interfaces de MSTP como se muestra en la página **Spanning Tree** MSTP Interface Settings (Configuración de la interfaz de MSTP del árbol de extensión).

Tabla 7-19. Comandos de la CLI para la interfaz de MSTP

Comando de la CLI	Descripción
`spanning-tree mst id- instancia cost coste`	Establece el coste de la ruta del puerto para cálculos de MST.
`spanning-tree mst id- instancia priority prioridad`	Establece la prioridad del dispositivo para la instancia de árbol de extensión especificada.
`show spanning-tree mst- configuration`	Muestra la configuración de MST.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show spanning-tree mst-configuration

Gathering information .....

Current MST configuration

Name: Gili

Revision: 65000

Instance        Vlans Mapped            State
                ------------------------ ----------
```

0	16-4094	enabled
1	1	enabled
2	2	enabled
3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

Configuración de redes VLAN

Las redes VLAN son subgrupos lógicos con una LAN creada a través del software, en lugar de definir una solución de hardware. Las redes VLAN combinan estaciones de usuario y dispositivos de red en una sola unidad, independientemente del segmento físico de LAN al que se conecten. Las VLAN permiten que el tráfico de red fluya con mayor eficiencia dentro de subgrupos. Cuando se administran a través de software, las VLAN reducen el tiempo de implementación de los cambios, las adiciones y los movimientos en la red.

Las VLAN no tienen un número mínimo de puertos, y pueden crearse por unidad, por dispositivo, por pila o cualquier otra combinación de conexiones lógicas, ya que las redes VLAN se basan en el software y no se definen mediante atributos físicos.

Las VLAN funcionan en el nivel 2. Puesto que las VLAN aislan el tráfico en la VLAN, se necesita un enrutador que funcione en el nivel de protocolo 3 para permitir el flujo de tráfico entre ellas. Los enrutadores de nivel 3 identifican segmentos y se coordinan con las VLAN. Las VLAN son dominios de transmisión y de multidifusión. El tráfico de transmisión y de multidifusión sólo se transmite en la VLAN en la que se genera el tráfico.

El etiquetado de redes VLAN proporciona un método para transferir información de la VLAN entre grupos de redes VLAN. Se adjunta una etiqueta de cuatro

bytes a las cabeceras de los paquetes. La etiqueta de VLAN indica a qué VLAN pertenece el paquete. Las etiquetas de VLAN se adjuntan a la VLAN mediante la estación final o el dispositivo de red. Las etiquetas de VLAN también contienen información de prioridad de la red VLAN.

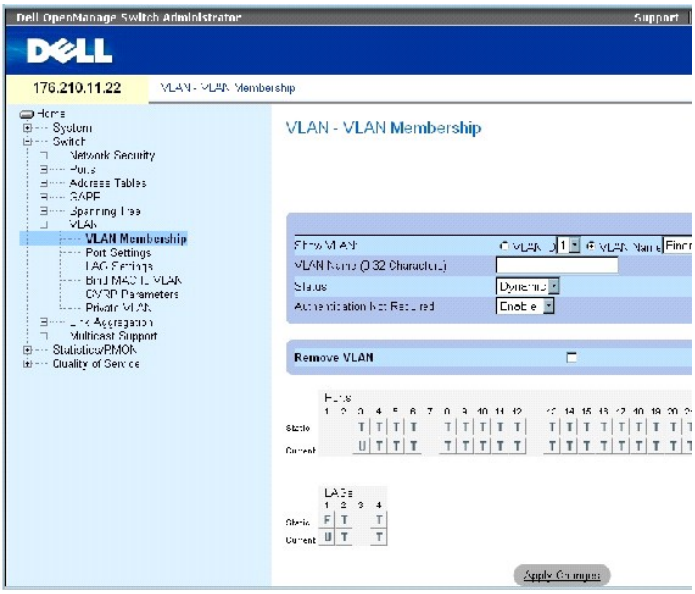
La combinación de redes VLAN y GVRP permite a los administradores de red definir nodos de red en dominios de difusión. El tráfico de difusión y multidifusión se limita al grupo de origen.

Para abrir la página **VLAN**, haga clic en **Switch** (Conmutador) → **VLAN** en la vista de árbol.

Definición de pertenencia a la VLAN

La página **VLAN Membership** (Pertenencia a la VLAN) contiene campos para definir grupos de VLAN. El dispositivo admite la asignación de 4 094 ID de VLAN para 256 VLAN. Todos los puertos deben tener una ID de VLAN definida. Si no hay otro valor configurado, utilice la PVID de VLAN predeterminada. La VLAN predeterminada del sistema es la VLAN con ID 1 y no puede eliminarse del sistema. Para abrir la página **VLAN Membership** (Pertenencia a la VLAN), haga clic en **Switch** (Conmutador) → **VLAN** → **VLAN Membership** (Pertenencia a la VLAN) en la vista de árbol.

Figura 7-30. VLAN Membership



La página **VLAN Membership** (Pertenencia a la VLAN) contiene los campos siguientes:

Show VLAN (Mostrar VLAN): enumera y muestra información de VLAN según la ID o el nombre de la VLAN.

VLAN Name (0-32 Characters) (Nombre de la VLAN [0-32 caracteres]): especifica el nombre de la VLAN definido por el usuario.

Status (Estado): indica el tipo de VLAN. Los valores posibles son:

Dynamic (Dinámica): indica que la VLAN se ha creado de manera dinámica a través de GVRP.

Static (Estática): indica que la VLAN la ha definido el usuario.

Default (Predeterminada): indica que la VLAN es la predeterminada.

Authentication Not Required (Autenticación no necesaria): activa o desactiva el acceso de usuarios no autorizados a una VLAN.

Remove VLAN (Eliminar VLAN): si se selecciona esta opción, se elimina la VLAN de la tabla de pertenencia a la VLAN.

Adición de redes VLAN nuevas

1. Abra la página (Pertenencia a la VLAN).
2. Haga clic en **Add** (Añadir).

   Se abre la página **Create New VLAN** (Crear nueva VLAN).
3. Especifique la ID y el nombre de la VLAN.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se añade la nueva VLAN y se actualiza el dispositivo.

Modificación de grupos de pertenencia a la VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN del menú desplegable **Show VLAN** (Mostrar VLAN).
3. Modifique los campos según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se modifica la información de pertenencia a la VLAN y se actualiza el dispositivo.

Eliminación de una VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN en el campo **Show VLAN** (Mostrar VLAN).
3. Seleccione la casilla de verificación **Remove VLAN** (Eliminar VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se elimina la VLAN seleccionada y se actualiza el dispositivo.

Definición de grupos de pertenencia a la VLAN mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para definir grupos de pertenencia a la VLAN como aparecen en la página VLAN Membership (Pertenencia a la VLAN).

Tabla 7-20. Comandos de la CLI para grupos de pertenencia a la VLAN

Comando de la CLI	Descripción
vlan database	Entra en el modo de configuración de la VLAN.
vlan {*intervalo-vlan*}	Crea una VLAN.
name *cadena*	Añade un nombre a una VLAN.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# vlan
database


console(config-vlan)# vlan
1972


console(config-vlan)# end


console(config)# interface
vlan 1972


console(config-if)# name
Marketing


console(config-if)# end
```

Tabla de pertenencia de puertos a la VLAN

La tabla de pertenencia de puertos a la VLAN (**VLAN Port Membership Table**) contiene una tabla de puertos (**Port Table**) para asignar puertos a las VLAN. Para asignar los puertos a una VLAN, debe alternarse la configuración de **Port Control** (Control de puertos). Los puertos pueden tener los valores siguientes:

Tabla 7-21. Tabla de pertenencia de puertos a la VLAN

Control de puertos	Definición
T	La interfaz es miembro de una VLAN. Todos los paquetes reenviados por la interfaz tienen etiqueta. Los paquetes contienen información de VLAN.
U	La interfaz es un miembro de la VLAN. Los paquetes reenviados por la interfaz no tienen etiqueta.
F	La interfaz tiene denegada la pertenencia a una VLAN.
En blanco	La interfaz no es un miembro de la VLAN. Los paquetes asociados con la interfaz no se reenvían.

La tabla de pertenencia de puertos a la VLAN (**VLAN Port Membership Table**) muestra los puertos y los estados de puertos, así como también los LAG.

Asignación de puertos a un grupo de VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Haga clic en el botón de opción **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN) y seleccione una VLAN en el menú desplegable.
3. Seleccione un puerto en la tabla de pertenencia de puertos (**Port Membership Table**) y asígnele un valor.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna el puerto al grupo de VLAN y se actualiza el dispositivo.

Eliminación de una VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Haga clic en el botón de opción **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN) y seleccione una VLAN en el menú desplegable.
3. Seleccione la casilla de verificación **Remove VLAN** (Eliminar VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la VLAN seleccionada y se actualiza el dispositivo.

Asignación de puertos a grupos de VLAN mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para asignar puertos a grupos de VLAN.

Tabla 7-22. Comandos de la CLI para las asignaciones de puertos a grupos de VLAN

Comando de la CLI	Descripción
switchport general acceptable-frame-types tagged-only	Descarta las tramas sin etiqueta en la entrada.
switchport forbidden vlan {**add** *lista-vlan* | **remove** *lista-vlan*}	Prohíbe la adición de VLAN específicas al puerto.
switchport mode {access | trunk | general}	Configura el modo de pertenencia a la VLAN de un puerto.
switchport access vlan id-vlan	Configura la ID de VLAN cuando la interfaz se encuentra en modo de acceso.
switchport trunk allowed vlan {add vlan-list | remove lista-vlan}	Añade o elimina redes VLAN de una combinación de puertos.
switchport trunk native vlan id-vlan	Define al puerto como miembro de la VLAN especificada, y la ID de VLAN como la ID de VLAN de puerto (PVID) predeterminada.
switchport general allowed vlan add vlan-list [tagged | untagged]	Añade o elimina redes VLAN para un puerto en modo general.
switchport general pvid id-vlan	Configura el valor de PVID cuando la interfaz se encuentra en modo general.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# vlan
database

console(config-vlan)# vlan
23-25

console(config-vlan)# end

console(config)# interface
vlan 23

console(config-if)# name
Marketing

console(config-if)# end

console(config)# interface
ethernet 1/e8

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 23

console(config-if)# end
```

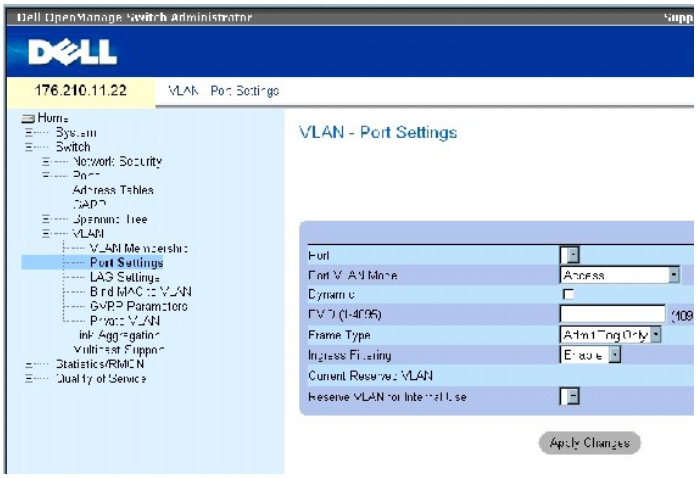
```
console(config)# interface
ethernet 1/e9



console(config-if)#
switchport mode trunk



console(config-if)#
switchport mode trunk
allowed vlan add 23-25



console(config-if)# end



console(config)# interface
ethernet 1/e11



console(config-if)#
switchport mode general



console(config-if)#
switchport general allowed
vlan add 23,25 tagged



console(config-if)#
switchport general pvid 25
```

Definición de la configuración de puertos de VLAN

La página VLAN Port Settings (Configuración de puertos de VLAN) contiene campos para administrar puertos que forman parte de una VLAN. La ID de VLAN de puerto (PVID) predeterminada se configura en la página VLAN Port Settings (Configuración de puertos de VLAN). Las PVID de puerto asignan etiquetas a todos los paquetes sin etiqueta que llegan al dispositivo.

Para abrir la página VLAN Port Settings (Configuración de puertos de VLAN), haga clic en **Switch** (Conmutador) → **VLAN** → **Port Settings** (Configuración de puertos) en la vista de árbol.

Figura 7-31. VLAN Port Settings



La página VLAN Port Settings (Configuración de puertos de VLAN) contiene los campos siguientes:

Port (Puerto): indica el número del puerto incluido en la VLAN.

Port VLAN Mode (Modo de VLAN de puerto): indica el modo del puerto. Los valores posibles son:

General: el puerto pertenece a redes VLAN, y cada VLAN está definida por el usuario como etiquetada o sin etiquetar (modo 802.1Q completo).

Access (Acceso): el puerto pertenece a una única VLAN sin etiquetar. Cuando un puerto se encuentra en modo de acceso, no es posible designar los tipos de paquete que se aceptan en el puerto. El filtrado de entrada no puede activarse ni desactivarse en un puerto de acceso.

Trunk (Combinación de puertos): el puerto pertenece a redes VLAN en las que todos los puertos están etiquetados (excepto un puerto que puede estar sin etiquetar).

PV**E** Promiscuous (PVE promiscuo): el puerto forma parte de una VLAN de PVE promiscuo.

VE **Community** (Comunidad de PVE): el puerto forma parte de una VLAN de comunidad de PVE.

PVE **Isolated** (PVE aislado): el puerto forma parte de una VLAN de PVE aislado.

Dynamic (Dinámico): **asigna un puerto a una VLAN en función de la dirección MAC fuente del host conectada al puerto.**

PVID: asigna una ID de VLAN a paquetes sin etiqueta. Los valores posibles son 1-4095. La VLAN 4095 se define según los procedimientos estándar y del sector como Discard VLAN (Descartar VLAN). Los paquetes clasificados en esta VLAN se descartan.

Frame Type (Tipo de trama): tipo de paquete aceptado por el puerto. Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): el puerto sólo acepta paquetes con etiqueta.

Admit All (Admitir todos): el puerto acepta paquetes con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): activa o desactiva el filtrado de entrada en el puerto. El filtrado de entrada descarta los paquetes que están destinados a redes VLAN a las que el puerto específico no pertenece.

Current Reserved VLAN (VLAN reservada actual): indica la VLAN designada actualmente por el sistema como VLAN reservada.

Reserve VLAN for Internal Use (Reservar VLAN para uso interno): indica la VLAN seleccionada por el usuario que debe ser la VLAN reservada si no la utiliza el sistema.

Asignación de valores de configuración de puertos

1. Abra la página VLAN Port Settings (Configuración de puertos de VLAN).
2. Seleccione en el menú desplegable **Port** (Puerto) el puerto al que deben asignarse valores.
3. Complete los campos restantes de la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la configuración de los puertos de VLAN y se actualiza el dispositivo.

Visualización de la tabla de puertos de VLAN

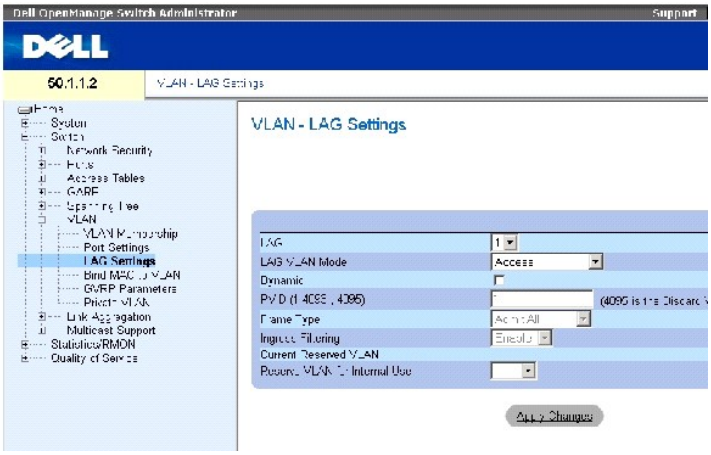
1. Abra la página VLAN Port Settings (Configuración de puertos de VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de puertos de VLAN.

Definición de la configuración VLAN de los LAG

La página VLAN LAG Settings (Configuración de LAG de VLAN) proporciona parámetros para administrar grupos LAG que forman parte de una VLAN. Las redes VLAN pueden estar formadas por puertos individuales o por grupos LAG. Los paquetes sin etiqueta que entran en el dispositivo se etiquetan con la ID de los LAG especificada por la PVID. Para abrir la página VLAN LAG Settings (Configuración VLAN de LAG), haga clic en **Switch** (Conmutador)→ **VLAN**→ **LAG Settings** (Configuración de LAG) en la vista de árbol.

Figura 7-32. VLAN LAG Settings



La página VLAN LAG Settings (Configuración de LAG de VLAN) contiene los campos siguientes:

LAG: indica el número del LAG incluido en la VLAN.

LAG VLAN Mode (Modo de VLAN de LAG): indica el modo de VLAN de LAG. Los valores posibles son:

General: el LAG pertenece a redes VLAN, y cada VLAN está definida por el usuario como etiquetada o sin etiquetar (modo 802.1Q completo).

Access (Acceso): el LAG pertenece a una única VLAN sin etiquetar.

Trunk (Combinación de puertos): el LAG pertenece a redes VLAN en las que todos los puertos están etiquetados (excepto un puerto que puede estar sin etiquetar).

PVE Promiscuous (PVE promiscuo): el LAG forma parte de una VLAN de PVE promiscuo.

PVE Community (PVE de comunidad): el LAG forma parte de una VLAN de PVE de comunidad.

PVE Isolated (PVE aislado): el LAG forma parte de una VLAN de PVE aislado.

Dynamic (Dinámico): asigna un LAG a una VLAN en función de la dirección MAC fuente del host conectada al LAG.

PVID (1-4093, 4095): asigna una ID de VLAN a paquetes sin etiqueta. Los valores del campo posibles son 1-4095. La VLAN 4095 se define en los procedimientos estándar y del sector como Discard VLAN (Descartar VLAN). Los paquetes clasificados en esta VLAN se descartan.

Frame Type (Tipo de trama): tipo de paquete aceptado por el LAG. Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): el LAG sólo acepta paquetes con etiqueta.

Admit All (Admitir todos): el LAG acepta paquetes con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): activa o desactiva el filtrado de entrada en el LAG. El filtrado de entrada descarta los paquetes que están destinados a redes VLAN a las que el LAG específico no pertenece.

Current Reserved VLAN (VLAN reservada actual): indica la VLAN designada actualmente como VLAN reservada.

Reserve VLAN for Internal Use (Reservar VLAN para uso interno): indica la VLAN que se ha designado como VLAN reservada después de restablecer el dispositivo.

Asignación de la configuración de LAG de VLAN

1. Abra la página VLAN LAG Settings (Configuración de LAG de VLAN).
2. Seleccione un LAG en el menú desplegable **LAG** y cumplimente los campos de esta página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros de LAG de la VLAN y se actualiza el dispositivo.

Visualización de la tabla de LAG de la VLAN

1. Abra la página VLAN LAG Settings (Configuración de LAG de VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de LAG de VLAN.

Asignación de grupos LAG a grupos de VLAN mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para asignar grupos LAG a grupos de VLAN como se muestra en la página VLAN LAG Settings (Configuración de LAG de VLAN).

Tabla 7-23. Comandos de la CLI para asignar grupos LAG a redes VLAN

Comando de la CLI	Descripción
switchport mode {access | trunk | general}	Configura el modo de pertenencia de un LAG a la VLAN.
switchport trunk native vlan *id-vlan*	Define el puerto como miembro de la VLAN especificada, y la ID de VLAN como la ID de VLAN predeterminada del LAG.
switchport general pvid *id-vlan*	Configura la ID de VLAN de LAG cuando la interfaz está en modo general.
switchport general allowed vlan add *lista-vlan* [**tagged | untagged**]	Añade o elimina redes VLAN de un LAG general.

switchport general acceptable-frame-type tagged-only	Descarta los paquetes sin etiqueta en la entrada.
switchport access vlan dynamic	Enlaza la dirección MAC con la VLAN.
switchport general ingress-filtering disable	Desactiva el filtrado de entrada del LAG.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface
port-channel 1

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 2

console(config-if)# exit

console(config)# interface
port-channel 2

console(config-if)#
switchport mode general

console(config-if)#
switchport general allowed
vlan add 2-3 tagged

console(config-if)#
switchport general pvid 2

console(config-if)#
switchport general
acceptable-frame-type
tagged-only

console(config-if)#
switchport general
ingress-filtering disable

console(config-if)# exit

console(config)# interface
port-channel 3

console(config-if)#
switchport mode trunk

console(config-if)#
switchport trunk native
vlan 3
```

```
console(config-if)#
switchport trunk allowed
vlan add 2
```

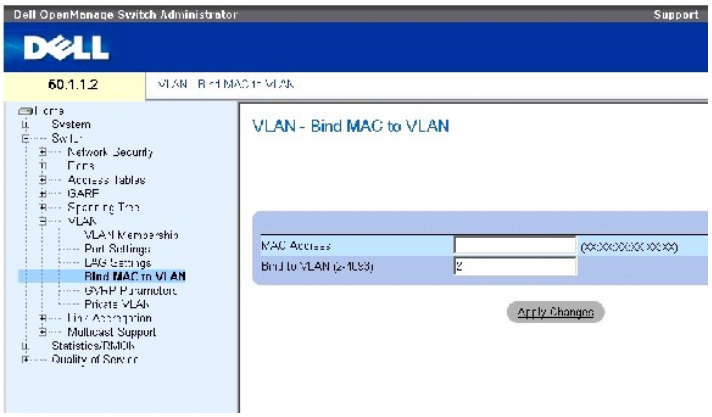
Enlace de direcciones MAC con redes VLAN

El enlace de direcciones MAC con redes VLAN proporciona una asignación de puerto a VLAN basada en las direcciones MAC. Una vez que se ha asignado una dirección MAC a una VLAN, y que un puerto ha obtenido dicha dirección, el puerto se une a la VLAN vinculada. Cuando la dirección MAC caduca, el puerto abandona la VLAN. Sólo pueden vincularse a direcciones MAC las VLAN dinámicas.

Para vincular direcciones MAC a una VLAN, asegúrese de que los puertos de VLAN se han añadido de forma dinámica y que no se trata de puertos VLAN estáticos.

Para abrir la página **Bind MAC to VLAN** (Vincular MAC a VLAN), haga clic en **Switch** (Conmutador) → **VLAN**→ **Bind MAC to VLAN** (Vincular MAC a VLAN) en la vista de árbol.

Figura 7-33. Bind MAC to VLAN



La página Bind MAC to VLAN (Vincular MAC a VLAN) contiene los campos siguientes:

MAC Address (Dirección MAC): indica la dirección MAC que está vinculada a la VLAN.

Bind to VLAN (2-4093) (Vincular a VLAN [2-4093]): indica la VLAN a la que se vincula la dirección MAC.

Visualización de la tabla de MAC a VLAN

1. Abra la página Bind MAC to VLAN (Vincular MAC a VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de MAC a VLAN.

Vinculación de direcciones MAC a VLAN mediante comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para vincular direcciones MAC a VLAN.

Tabla 7-24. Comandos de la CLI para vincular direcciones MAC a VLAN

Comando de la CLI	Descripción
mac-to-vlan dirección-mac id-vlan	Enlaza la dirección MAC con la VLAN.
switchport access vlan dynamic	Configura VLAN privadas.
show mac-to-vlan	Muestra la base de datos de direcciones MAC vinculadas a VLAN.
no mac-to-vlan dirección-mac	Anula el enlace de la dirección MAC con la VLAN.

A continuación se muestra un ejemplo de los comandos de la CLI:

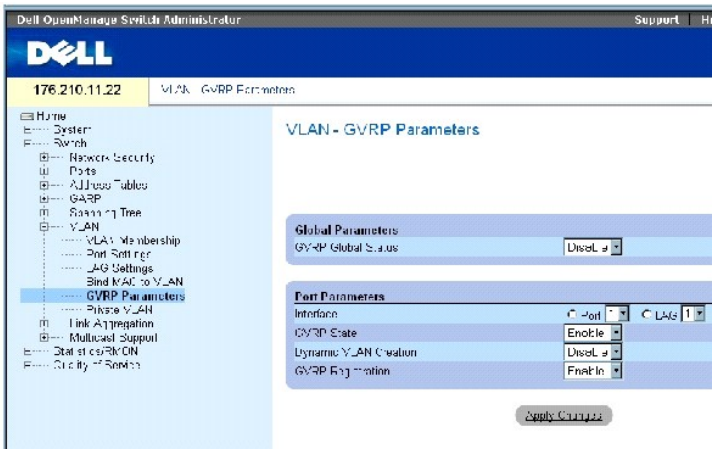
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

------------ ------

0060.704c.73ff 123
```

Configuración de los parámetros de GVRP

El protocolo de registro de VLAN GARP (GVRP) se proporciona específicamente para la distribución automática de información de pertenencia a la VLAN entre puentes con capacidad de reconocimiento de VLAN. El GVRP permite que los puentes con capacidad de reconocimiento de VLAN obtengan automáticamente las VLAN para la asignación de puertos puente sin tener que configurar individualmente cada puente, y también permite que dichos puentes registren la pertenencia a la VLAN.

La página **GVRP Parameters** (Parámetros de GVRP) activa el protocolo GVRP globalmente. El protocolo GVRP también puede activarse en cada interfaz por separado. Para abrir la página GVRP Parameters (Parámetros de GVRP), haga clic en **Switch** (Conmutador) → **VLAN** → **GVRP Parameters** (Parámetros de GVRP) en la vista de árbol.

Figura 7-34. GVRP Parameters



La página GVRP Parameters (Parámetros de GVRP) contiene los campos siguientes:

GVRP Global Status (Estado global de GVRP): activa o desactiva el GVRP en el dispositivo. El protocolo GVRP está desactivado de forma predeterminada.

Interface (Interfaz): especifica puerto o LAG para editar valores de GVRP.

GVRP State (Estado de GVRP): activa o desactiva el protocolo GVRP en una interfaz.

Dynamic VLAN Creation (Creación de VLAN dinámica): activa o desactiva la creación de VLAN a través de GVRP en una interfaz.

GVRP Registration (Registro de GVRP): activa o desactiva el registro de VLAN a través de GVRP en una interfaz.

Activación de GVRP en el dispositivo

1. Abra la página GVRP Global Parameters (Parámetros globales de GVRP).
2. Seleccione **Enable** (Activar) en el campo **GVRP Global Status** (Estado global de GVRP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El GVRP se activa en el dispositivo.

Activación del registro de VLAN a través de GVRP

1. Abra la página GVRP Global Parameters (Parámetros globales de GVRP).
2. Seleccione **Enable** (Activar) en el campo **GVRP Global Status** (Estado global de GVRP).
3. Seleccione **Enable** en el campo GVRP State (Estado de GVRP) para la interfaz que desee.
4. Seleccione **Enable** (Activar) en el campo **GVRP Registration** (Registro de GVRP).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El registro de VLAN de GVRP se activa en el puerto y el dispositivo se actualiza.

Configuración de GVRP mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar el GVRP como se muestra en la página GVRP Global Parameters (Parámetros globales de GVRP).

Tabla 7-25. Comandos de la CLI para parámetros globales de GVRP

Comando de la CLI	Descripción
gvrp enable (global**)**	Activa el GVRP de manera global.
gvrp enable (interface)	Activa el GVRP en una interfaz.
gvrp vlan-creation-forbid	Activa o desactiva la creación de VLAN dinámica.
gvrp registration-forbid	Anula el registro de todas las redes VLAN dinámicas e impide el registro de redes VLAN dinámicas en el puerto.
show gvrp configuration [**ethernet** *interfaz*| **port-channel** *número-canal-puerto*]	Muestra información de la configuración de GVRP, incluidos los valores de temporizador, si la creación de GVRP y VLAN dinámicas está activada y qué puertos están ejecutando GVRP.
show gvrp error-statistics [**ethernet** *interfaz*| **port-channel** *número-canal-puerto*]	Muestra las estadísticas de error de GVRP.
show gvrp statistics [**ethernet** *interfaz*| **port-channel** *número-canal-puerto*]	Muestra las estadísticas de GVRP.
clear gvrp statistics [**ethernet** *interfaz*| **port-**	Borra toda la información de las estadísticas de GVRP.

channel *número-canal-puerto*]	

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# gvrp enable

console(config)# interface ethernet 1/e1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
---	---	---	---	---	---	---
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

Configuración de redes VLAN privadas

Las redes VLAN privadas (PVLAN) aumentan la seguridad de la red limitando la comunicación entre puertos en una VLAN. Las redes VLAN privadas limitan el tráfico de la red en el nivel 2. Los administradores de la red definen una VLAN principal. En la VLAN principal hay redes VLAN aisladas y de comunidad. Los puertos de VLAN privados pueden tener los estados siguientes:

- Promiscuous (Promiscuo): los puertos promiscuos pueden conectarse con todos los puertos de una PVLAN. Todos los paquetes promiscuos se asignan automáticamente a las redes VLAN aisladas y de comunidad.
- **Isolated** (Aislado): los puertos aislados están totalmente aislados de los demás puertos de una misma PVLAN. No obstante, estos puertos pueden comunicarse con los puertos promiscuos. Además, todo el tráfico que se genera desde y hacia los puertos aislados con redes VLAN se bloquea, exceptuando el tráfico de los puertos promiscuos. Todos los puertos aislados se asignan automáticamente a la VLAN aislada.
- **Community** (Comunidad): los puertos de comunidad se comunican con otros puertos de comunidad y con puertos promiscuos. Los puertos de comunidad están separados de todas las demás interfaces en otros puertos de comunidad o puertos aislados de la misma PVLAN. Todos los puertos de comunidad se asignan automáticamente a la VLAN de comunidad y a la VLAN privada.

NOTA: los puertos no pueden definirse como puertos promiscuos o aislados si se trata de puertos que son miembros de VLAN existentes.

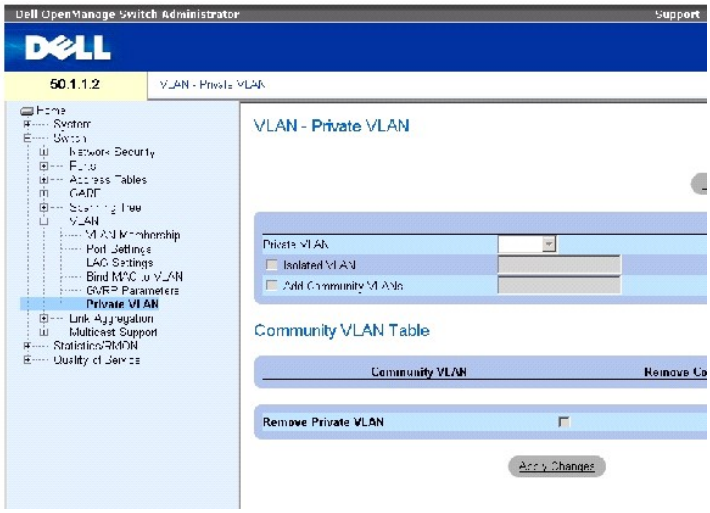
NOTA: las redes VLAN creadas con anterioridad no pueden configurarse como VLAN aisladas ni de comunidad.

NOTA: las redes VLAN aisladas y de comunidad se incluyen en el número total de VLAN.

Si se elimina una VLAN principal, también se eliminan las VLAN aisladas y de comunidad. Además, las VLAN asiladas y de comunidad sólo reenvían tráfico sin etiquetar.

Para abrir la página Private VLAN (VLAN privada), haga clic en **Switch** (Conmutador) → **VLAN** → **Private VLAN** (VLAN privada) en la vista de árbol.

Figura 7-35. Private VLAN



La página Private VLAN (VLAN privada) contiene los campos siguientes:

Private VLAN (VLAN privada): contiene una lista de las VLAN privadas definidas por el usuario. Las VLAN privadas se definen en la página **Add Private VLAN** (Añadir VLAN privada).

Isolated VLAN (VLAN aislada): indica qué puertos aislados están asignados a cada VLAN.

Add Community VLANs (Añadir VLAN de comunidad): añade una VLAN de comunidad a la que se asignan puertos de comunidad.

Community VLAN (VLAN de comunidad): muestra una lista de las VLAN de comunidad.

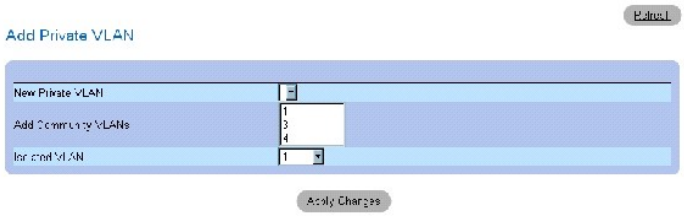
Remove Community (Eliminar comunidad): cuando se selecciona esta opción, se elimina una VLAN de comunidad.

Remove Private VLAN (Eliminar VLAN privada): cuando se selecciona esta opción, se elimina una VLAN privada.

Adición de VLAN privadas

1. Abra la página **Private VLAN** (VLAN privada).
2. Haga clic en **Add** (Añadir). Se abre la página **Add Private VLAN** (Añadir VLAN privada):

Figura 7-36. Add Private VLAN



La página Add Private VLAN (Añadir VLAN privada) contiene los campos adicionales siguientes:

New Private VLAN (VLAN privada nueva): contiene una lista de las VLAN privada. Las VLAN de comunidad se añaden a la VLAN privada.

Add Community VLANs (Añadir VLAN de comunidad): añade una VLAN de comunidad a la VLAN privada.

Isolated VLAN (VLAN aislada): añade una VLAN aislada a la VLAN privada.

3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

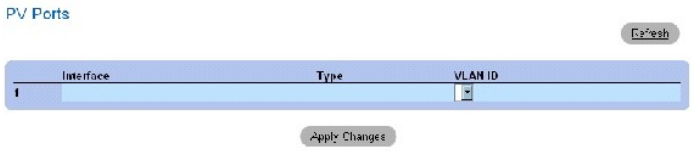
Se define la VLAN privada y se actualiza el dispositivo.

Visualización de la tabla de puertos PV

1. Abra la página Private VLAN (VLAN privada).
2. Haga clic en **Show PV Ports** (Mostrar puertos PV).

Se abre la tabla de puertos PV (**PV Ports Table**).

Figura 7-37. PV Ports Table



Configuración de las PVLAN mediante comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar las PVLAN como se muestra en la página **Private VLAN** (VLAN privada).

Tabla 7-26. Comandos de la CLI para VLAN privadas

Comando de la CLI	Descripción
switchport mode private vlan promiscuous	**Añade un puerto promiscuo a una VLAN promiscua.**
switchport mode private vlan community	**Añade un puerto de comunidad a una VLAN de comunidad.**
switchport mode private vlan isolated	**Añade un puerto aislado a una VLAN aislada.**
private-vlan primary	Define una VLAN principal.
private-vlan community {add lista-vlan-comunidad | remove lista-vlan-comunidad }	Define o elimina una VLAN de comunidad de la VLAN principal.

private-vlan isolated	Define una VLAN aislada de la VLAN principal.
switchport private-vlan *pvlan* **[community** *cvlan***]**	Define puertos de VLAN privada**.**
show vlan private-vlan [primary vlan-id]	Muestra la VLAN principal privada.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# vlan
database

console(config-vlan)# vlan
2

console(config-vlan)# exit

console(config)# interface
vlan 2

console(config-if)#
private-vlan primary

console(config)# interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community add
20

console# show vlan
private-vlan

console(config-if)# end
```

Agregado de puertos

El agregado de puertos optimiza el uso de los mismos vinculando un grupo de puertos para formar un único LAG (grupo agregado). La adición de puertos multiplica el ancho de banda entre los dispositivos, incrementa la flexibilidad de los puertos y proporciona redundancia de enlaces.

El dispositivo admite tanto grupos LAG estáticos como grupos LAG de LACP (protocolo de control de agregación de enlaces). Los grupos LAG de LACP negocian enlaces de puertos agregados con otros puertos de LACP ubicados en otro dispositivo. Si los otros puertos del dispositivo son también puertos de LACP, los dispositivos establecen un LAG entre ellos.

Al añadir puertos, debe tenerse en cuenta lo siguiente:

- Todos los puertos de un LAG deben ser del mismo tipo de medio.
- Una VLAN no se configura en el puerto.
- El puerto no se asigna a un LAG distinto.

- El modo de negociación automática no se configura en el puerto.
- El puerto se encuentra en modo dúplex completo.
- Todos los puertos del LAG tienen los mismos modos de etiquetado y de filtrado de entrada.
- Todos los puertos del LAG tienen los mismos modos de contrapresión y control de flujo.
- Todos los puertos del LAG tienen la misma prioridad.
- Todos los puertos del LAG tienen el mismo tipo de transceptor.
- El dispositivo admite hasta ocho grupos LAG y ocho puertos en cada LAG.
- Los puertos se pueden configurar como puertos de LACP sólo si no forman parte de un LAG previamente configurado.

Los puertos que se añaden a un LAG pierden su configuración de puerto individual. Cuando se eliminan puertos del LAG, se aplica la configuración de puerto original a todos los puertos.

El dispositivo utiliza una función hash para determinar qué paquetes se transportan en un miembro determinado del enlace agregado. La función hash equilibra estadísticamente la carga de los miembros del enlace agregado. El dispositivo considera que un enlace agregado es un único puerto lógico.

Definición de parámetros de LACP

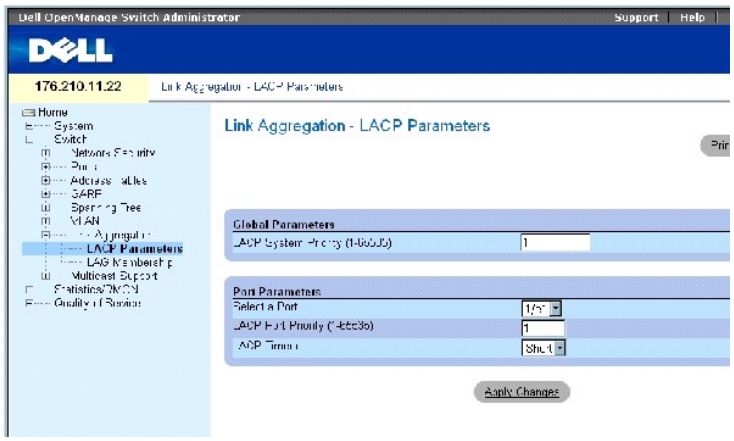
Los puertos agregados se pueden enlazar en grupos de puertos de agregación de enlaces. Cada grupo se compone de puertos que tienen la misma velocidad y que están configurados para funcionar en modo dúplex completo.

Los puertos de un grupo agregado de enlaces (LAG) pueden tener distintos tipos de medio si funcionan a la misma velocidad. Los enlaces agregados se pueden configurar manual o automáticamente activando el protocolo de control de agregación de enlaces (LACP) en los enlaces relevantes.

Definición de parámetros de LACP

La página **LACP Parameters** (Parámetros de LACP) contiene campos para configurar los grupos LAG de LACP. Los puertos agregados se pueden enlazar en grupos de puertos de agregación de enlaces. Cada grupo consta de puertos con la misma velocidad. Los enlaces agregados se pueden configurar manualmente o establecer automáticamente activando el protocolo de control de agregación de enlaces (LACP) en los enlaces relevantes. Para abrir la página LACP Parameters (Parámetros de LACP), haga clic en **Switch** (Conmutador) → **Link Aggregation** (Agregación de enlaces) → **LACP Parameters** (Parámetros de LACP) en la vista de árbol.

Figura 7-38. LACP Parameters



La página LACP Parameters (Parámetros de LACP) contiene los campos siguientes:

LACP System Priority (1-65535) (Prioridad del sistema de LACP [1-65535]): indica el valor de prioridad de LACP para los valores globales. El intervalo posible es 1-65535. El valor predeterminado es 1.

Select a Port (Seleccionar un puerto): número de puerto al que se asignan valores de tiempo de espera y de prioridad.

LACP Port Priority (1-65535) (Prioridad de puerto de LACP [1-65535]): indica la prioridad de LACP para el puerto.

LACP Timeout (Tiempo de espera de LACP): indica un tiempo de espera de LACP administrativo. Los valores del campo posibles son:

Short (Breve): especifica un valor de tiempo de espera breve.

Long (Prolongado): especifica un valor de tiempo de espera prolongado.

Definición de parámetros globales de agregación de enlaces

1. Abra la página LACP Parameters (Parámetros de LACP).
2. Complete el campo **LACP System Priority** (Prioridad del sistema de LACP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros y se actualiza el dispositivo.

Definición de parámetros de puertos de agregación de enlaces

1. Abra la página LACP Parameters (Parámetros de LACP).
2. Complete los campos del área **Port Parameters** (Parámetros de puerto).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros y se actualiza el dispositivo.

Visualización de la tabla de parámetros de LACP

1. Abra la página LACP Parameters (Parámetros de LACP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de parámetros de LACP.

Configuración de los parámetros de LACP mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para configurar parámetros de LACP como se muestra en la página LACP Parameters (Parámetros de LACP).

Tabla 7-27. Comandos de la CLI para parámetros de LACP

Comando de la CLI	Descripción
lacp system-priority *valor*	Configura la prioridad del sistema.
lacp port-priority *valor*	Configura el valor de prioridad para puertos físicos.
lacp timeout {**long** | **short**}	Asigna un tiempo de espera de LACP administrativo.
show lacp ethernet *interfaz* [**parameters** | **statistics** | **protocol-state**]	Muestra información de LACP para puertos Ethernet.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# lacp
system-priority 120



Console (config)#
interface ethernet 1/e11



Console (config-if)# lacp
port-priority 247



Console (config-if)# lacp
timeout long



Console (config-if)# end



Console# show lacp
ethernet 1/e11 statistics



Port 1/e11 LACP
Statistics:



LACP PDUs sent:2



LACP PDUs received:2
```

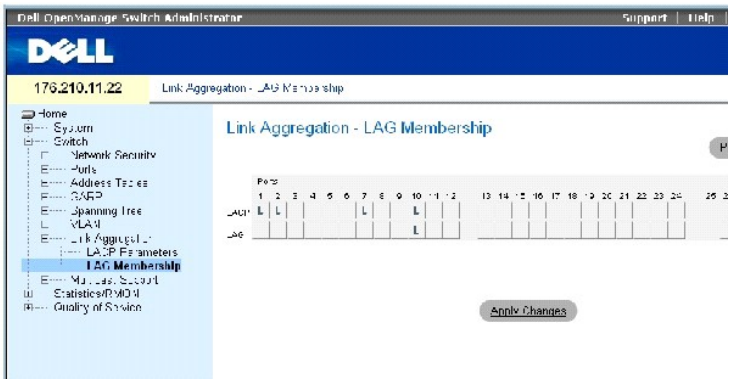
Definición de pertenencia a LAG

El dispositivo admite hasta ocho LAG por sistema y ocho puertos por LAG, ya sea el dispositivo independiente o se encuentre en una pila.

Cuando se añade un puerto a un LAG, el puerto adquiere las propiedades del LAG. Si el puerto no puede configurarse con las propiedades del LAG, no se añade al LAG. Se genera un mensaje de error. No obstante, si el primer puerto que une al LAG no puede configurarse con los valores del LAG, el puerto se añade al LAG utilizando los valores predeterminados del puerto. Se genera un mensaje de error. Sin embargo, puesto que se trata del único puerto en el LAG, todo el LAG funciona con los valores del puerto, en lugar de utilizar los valores definidos del LAG.

Utilice la página **LAG Membership** (Pertenencia a LAG) para asignar puertos a grupos LAG. Para abrir la página **LAG Membership** (Pertenencia a LAG), haga clic en **Switch** (Conmutador) → **Link Aggregation** (Agregación de enlaces) → **LAG Membership** (Pertenencia a LAG) en la vista de árbol.

Figura 7-39. LAG Membership



La página **LAG Membership** (Pertenencia a LAG) contiene los campos siguientes:

LACP: agrega el puerto a un LAG mediante LACP.

LAG: añade un puerto a un LAG e indica el LAG específico al que pertenece el puerto.

Adición de puertos a un LAG o LACP

1. Abra la página **LAG Membership** (Pertenencia a LAG).
2. En la fila de LAG (segunda fila), alterne el botón a un número específico para añadir o eliminar el puerto a dicho número de LAG.
3. En la fila de LACP (primera fila), alterne el botón situado bajo el número de puerto para asignar el LACP o el LAG estático.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade el puerto al LAG o LACP y se actualiza el dispositivo.

Adición de puertos a grupos LAG mediante los comandos de la CLI

La siguiente tabla presenta un resumen de los comandos de la CLI equivalentes para asignar puertos a grupos LAG como se muestra en la página **LAG Membership** (Pertenencia a LAG).

Tabla 7-28. Comandos de la CLI para la pertenencia a LAG

Comando de la CLI	Descripción
channel-group *número-canal-puerto* **mode** {**on** | **auto**}	Asocia un puerto con un canal de puertos. Utilice el valor "on" de este comando para eliminar la configuración de grupo de canales de la interfaz.
show interfaces port-channel [*número-canal-puerto*]	Muestra información sobre el canal de puertos.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface
ethernet 1/e11


console(config-if)#
channel-group 1 mode on
```

Compatibilidad con reenvío de multidifusión

El reenvío de multidifusión permite reenviar un mismo paquete a varios destinos. El servicio de multidifusión de nivel 2 se basa en un dispositivo de nivel 2 que recibe un paquete destinado a direcciones de multidifusión específicas. El reenvío de multidifusión crea copias del paquete y transmite los paquetes a los puertos pertinentes.

Registered Multicast traffic (Tráfico de multidifusión registrado): si se detecta tráfico destinado a un grupo de multidifusión registrado, se gestiona mediante una entrada en la base de datos de filtrado de multidifusión y sólo se reenvía a los puertos registrados.

Unregistered Multicast traffic (Tráfico de multidifusión no registrado): si se detecta tráfico destinado a un grupo de multidifusión no registrado, se gestiona mediante una entrada especial en la base de datos de filtrado de multidifusión. El valor predeterminado es distribuir todo el tráfico de este tipo (tráfico de los grupos de multidifusión no registrados).

El dispositivo admite:

- **Forwarding L2 Multicast Packets** (Reenvío de paquetes de multidifusión L2): reenvía paquetes de multidifusión de nivel 2. El filtrado de multidifusión de nivel 2 se activa de forma predeterminada y el usuario no puede configurarlo.

NOTA: el sistema admite el filtrado de multidifusión para grupos de multidifusión 256.

- **Filtering L2 Multicast Packets** (Filtrado de paquetes de multidifusión L2): reenvía paquetes de multidifusión de nivel 2 a las interfaces. Si se desactiva el filtrado de multidifusión, los paquetes de multidifusión se distribuyen a todos los puertos pertinentes.

Para abrir la página **Multicast Support** (Soporte para multidifusión), haga clic en **Switch** (Conmutador) → **Multicast Support** (Soporte para multidifusión) en la vista de árbol.

Definición de parámetros globales de multidifusión

La conmutación de nivel 2 reenvía paquetes de multidifusión a todos los puertos de VLAN pertinentes de manera predeterminada, gestionando el paquete como un único paquete de multidifusión. Si bien el reenvío de tráfico de multidifusión es efectivo, no es óptimo, ya que puertos no relevantes también reciben paquetes de multidifusión. El exceso de paquetes provoca un aumento del tráfico de la red. Los filtros de reenvío de multidifusión permiten reenviar paquetes de nivel 2 a subconjuntos de puertos.

Cuando la inspección de IGMP (IGMP Snooping) está activada de forma global, todos los paquetes de IGMP se reenvían a la CPU. La CPU analiza los paquetes entrantes y determina lo siguiente:

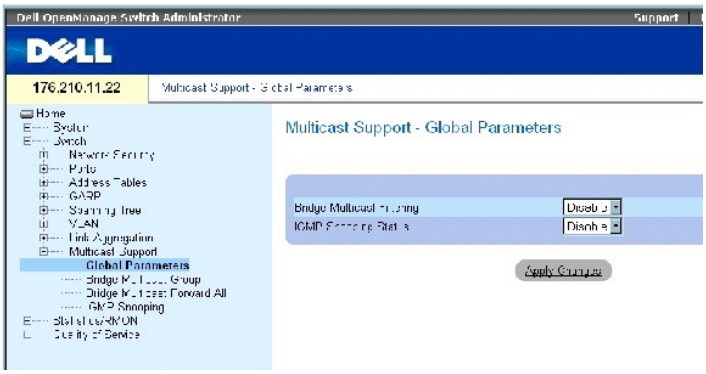
- Qué puertos deben unirse a grupos de multidifusión específicos.
- Qué puertos tienen enrutadores de multidifusión que generan consultas de IGMP.
- Qué protocolos de enrutamiento reenvían paquetes y tráfico de multidifusión.

Los puertos que solicitan unirse a un grupo de multidifusión específico emiten un informe IGMP en el que se especifica que el grupo de multidifusión acepta miembros. Esto da lugar a la creación de la base de datos de filtrado de multidifusión.

Para abrir la página **Multicast Support** (Soporte para multidifusión), haga clic en **Switch** (Conmutador) → **Multicast Support** (Soporte para multidifusión) en la vista de árbol.

La página **Global Parameters** (Parámetros globales) contiene campos para activar la inspección IGMP en el dispositivo. Para abrir la página **Global Parameters** (Parámetros globales), haga clic en **Switch** (Conmutador) → **Multicast Support** (Soporte para multidifusión) → **Global Parameters** (Parámetros globales) en la vista de árbol.

Figura 7-40. Global Parameters



La página **Global Parameters** (Parámetros globales) contiene los campos siguientes:

Bridge Multicast Filtering (Filtrado de multidifusión de puente): activa o desactiva el filtrado de multidifusión de puente. De forma predeterminada, esta opción está desactivada.

IGMP Snooping Status (Estado de inspección de IGMP): activa o desactiva la inspección de IGMP en el dispositivo. De forma predeterminada, esta opción está desactivada. La inspección de IGMP sólo puede activarse si se ha activado **Global Parameters** (Parámetros globales).

Activación del filtrado de multidifusión de puente en el dispositivo

1. Abra la página **Global Parameters** (Parámetros globales).
2. Seleccione **Enable** (Activar) en el campo **Bridge Multicast Filtering** (Filtrado de multidifusión de puente).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se activa el *filtrado de multidifusión de puente* en el dispositivo.

Activación de la inspección de IGMP en el dispositivo

1. Abra la página **Global Parameters** (Parámetros globales).
2. Seleccione **Enable** (Activar) en el campo **IGMP Snooping Status** (Estado de inspección de IGMP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se activa la inspección de IGMP en el dispositivo.

Activación del filtrado de multidifusión y la inspección de IGMP mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para activar el reenvío de multidifusión y la inspección de IGMP como se muestra en la página **Global Parameters** (Parámetros globales).

Tabla 7-29. Comandos de la CLI para la inspección y el filtrado de multidifusión

Comando de la CLI	Descripción
bridge multicast filtering	Activa el filtrado de direcciones de multidifusión.
ip igmp snooping	Activa la inspección de IGMP (protocolo de pertenencia a grupos de Internet).

A continuación se muestra un ejemplo de los comandos de la CLI:

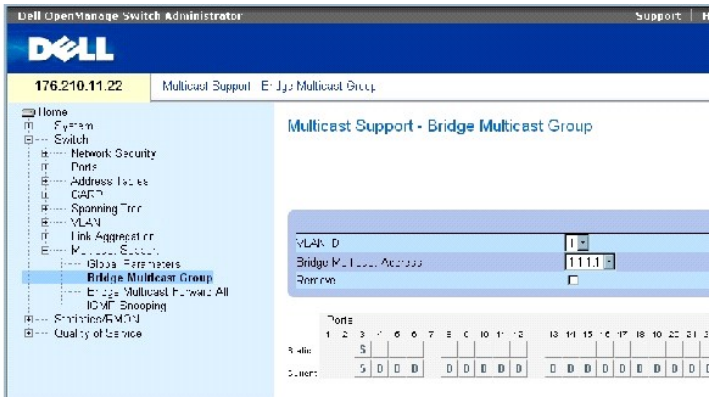
```
console(config)# bridge
multicast filtering

console(config)# ip igmp
snooping
```

Adición de miembros de las direcciones de multidifusión de puente

La página **Bridge Multicast Group** (Grupo de multidifusión de puente) muestra los puertos y los grupos LAG conectados al grupo de servicio de multidifusión en las tablas **Ports** (Puertos) y **LAGs** (LAG). Las tablas de puertos y de LAG también reflejan la manera en que el puerto o los LAG se han unido al grupo de multidifusión. Los puertos se pueden añadir a grupos existentes o a grupos de servicio de multidifusión nuevos. La página **Bridge Multicast Group** (Grupo de multidifusión de puente) permite crear nuevos grupos de servicio de multidifusión. La página **Bridge Multicast Group** (Grupo de multidifusión de puente) también asigna puertos a un grupo de direcciones de servicio de multidifusión específico.

Para abrir la página **Bridge Multicast Group** (Grupo de multidifusión de puente), haga clic en **Switch** (Conmutador) → **Multicast Support** (Soporte para multidifusión) → **Bridge Multicast Group** (Grupo de multidifusión de puente) en la vista de árbol.

Figura 7-41. Bridge Multicast Group



La página **Bridge Multicast Group** (Grupo de multidifusión de puente) contiene los campos siguientes:

VLAN ID (ID de VLAN): identifica una VLAN y contiene información sobre la dirección del grupo de multidifusión.

Bridge Multicast Address (Dirección de multidifusión de puente): identifica la dirección MAC/IP del grupo de multidifusión.

Remove (Eliminar): si se selecciona esta opción, se elimina una dirección de multidifusión de puente.

Ports (Puertos): indica el puerto que puede añadirse a un servicio de multidifusión.

LAGSs (LAG): indica los grupos LAG que pueden añadirse a un servicio de multidifusión.

La tabla siguiente contiene los valores de administración de los miembros de LAG y puertos IGMP:

Tabla 7-30. Configuración de los controles de la tabla de puertos de IGMP/miembros de LAG

Control de puertos	Definición
D	Indica que el puerto o LAG se ha unido al grupo de multidifusión de manera dinámica en la fila *Current* (Actual).
S	Conecta el puerto al grupo de multidifusión como miembro estático en la fila *Static* (Estático).

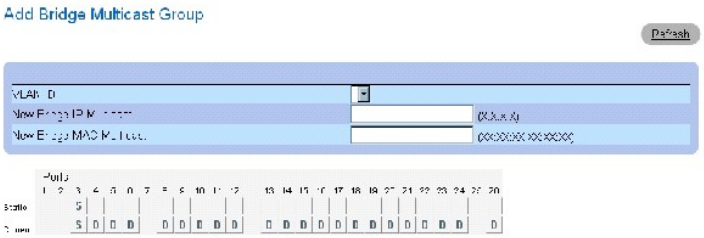
	Indica que el puerto o LAG se ha unido al grupo de multidifusión de manera estática en la fila *Current* (Actual).
F	Indica que está prohibido.
En blanco	Indica que el puerto no está conectado a ningún grupo de multidifusión.

Adición de direcciones de multidifusión de puente

1. Abra la página **Bridge Multicast Group** (Grupo de multidifusión de puente).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add Bridge Multicast Group** (Añadir grupo de multidifusión de puente):

Figura 7-42. Add Bridge Multicast Group



3. Defina los campos **VLAN ID** (ID de VLAN) y **New Bridge Multicast Address** (Dirección de multidifusión de puente nueva).
4. Cambie el valor del puerto a **S** para unir el puerto al grupo de multidifusión seleccionado.
5. Cambie el valor del puerto a **F** para impedir la adición de direcciones de multidifusión específicas a un puerto específico.
6. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección de multidifusión de puente se asigna al grupo de multidifusión y se actualiza el dispositivo.

Definición de los puertos de modo que reciban servicio de multidifusión

1. Abra la página **Bridge Multicast Group** (Grupo de multidifusión de puente).
2. Defina los campos **VLAN ID** (ID de VLAN) y **Bridge Multicast Address** (Dirección de multidifusión de puente).
3. Cambie el valor del puerto a **S** para unir el puerto al grupo de multidifusión seleccionado.
4. Cambie el valor del puerto a **F** para impedir la adición de direcciones de multidifusión específicas a un puerto específico.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna el puerto al grupo de multidifusión y se actualiza el dispositivo.

Asignación de grupos LAG de modo que reciban servicio de multidifusión

1. Abra la página **Bridge Multicast Group** (Grupo de multidifusión de puente).
2. Defina los campos **VLAN ID** (ID de VLAN) y **Bridge Multicast Address** (Dirección de multidifusión de puente).
3. Cambie el valor del LAG a **S** para unir el LAG al grupo de multidifusión seleccionado.
4. Cambie el valor del LAG a **F** para impedir la adición de direcciones de multidifusión específicas a un LAG específico.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna el LAG al grupo de multidifusión y se actualiza el dispositivo.

Administración de los miembros del servicio de multidifusión mediante los comandos de la CLI

En la tabla siguiente se presenta un resumen de los comandos de la CLI equivalentes para administrar los miembros del servicio de multidifusión como se muestra en la página **Bridge Multicast Group** (Grupo de multidifusión de puente).

Tabla 7-31. Comandos de la CLI para miembros de servicio de multidifusión

Comando de la CLI	Descripción
bridge multicast address {*dirección-mac-multidifusión* | *dirección-ip-multidifusión*}	Registra las direcciones de multidifusión de nivel MAC en la tabla puente y añade puertos estáticos al grupo.
bridge multicast forbidden address {*dirección-mac-multidifusión* | *dirección-ip-multidifusión*}[**add** | **remove**] {**ethernet** *lista-interfaces* | **port-channel** *lista-números-canal-puerto*}	Impide la adición de una dirección de multidifusión específica a puertos específicos. Utilice el valor "on" de este comando para regresar al valor predeterminado.
show bridge multicast address-table [**vlan** *id-vlan*] [**address** {*dirección-mac-multidifusión* | *dirección-ip-multidifusión*}] [**format ip** | **mac**]	Muestra información de la tabla de direcciones MAC de multidifusión.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet 1/e11,1/e12

console(config-if)# end

console # show bridge multicast address-table

Vlan   MAC Address          Type      Ports
----   -----------          -----     ----------
1      0100.5e02.0203       static    1/e11, 1/e12
19     0100.5e02.0208       static    1/e11-16
19     0100.5e02.0208       dynamic   1/e11-12

Forbidden ports for multicast addresses:

Vlan   MAC Address          Ports
----   -----------          ----------
1      0100.5e02.0203       1/e8
19     0100.5e02.0208       1/e8
```

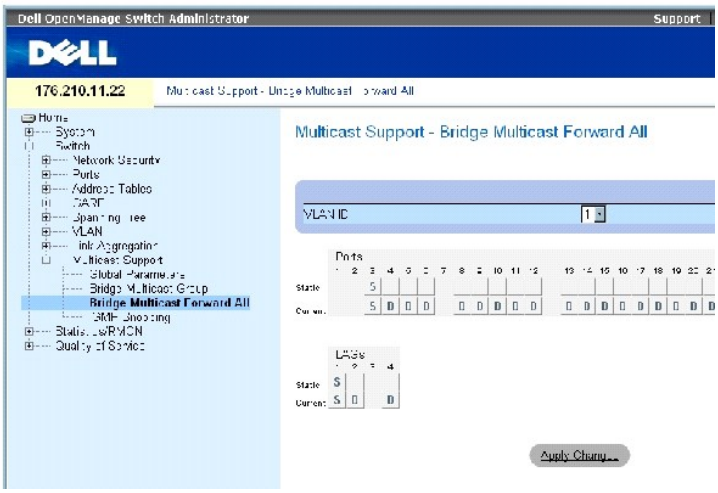
```
console # show bridge multicast address-table format ip

Vlan  IP Address            Type        Ports
----  ------------          -----       ----------
1     224-239.130|2.2.3     static      1/e11, 1/e12
19    224-239.130|2.2.8     static      1/e11-16
19    224-239.130|2.2.8     dynamic     1/e11-12

Forbidden ports for multicast addresses:

Vlan  IP Address            Ports
----  ------------          ----------
1     224-239.130|2.2.3     1/e8
19    224-239.130|2.2.8     1/e8
```

Asignación de parámetros de multidifusión "reenviar todos"

La página **Bridge Multicast Forward All** (Multidifusión de puente "reenviar todos") contiene campos para conectar puentes o grupos LAG a un dispositivo que está conectado a un enrutador o conmutador de multidifusión vecino. Una vez activada la inspección del IGMP, los paquetes de multidifusión se reenvían a la LAN o al puerto apropiado.

Para abrir la página **Bridge Multicast Forward All** (Multidifusión de puente "reenviar todos"), haga clic en **Switch** (Conmutador) → **Multicast Support** (Soporte para multidifusión) → **Bridge Multicast Forward All** (Multidifusión de puente "reenviar todos") en la vista de árbol.

Figura 7-43. Bridge Multicast Forward All



La página Bridge Multicast Forward All (Multidifusión de puente "reenviar todos") contiene los campos siguientes:

VLAN ID (ID de la VLAN): identifica una VLAN.

Ports (Puertos): indica los puertos que pueden añadirse a un servicio de multidifusión.

LAGSs (LAG): indica los grupos LAG que pueden añadirse a un servicio de multidifusión.

La tabla de configuración de control del conmutador/puerto de multidifusión de puente "reenviar todos" (**Tabla de configuración de control del conmutador/puerto de multidifusión de puente "reenviar todos"**) contiene la configuración para administrar los valores de enrutador y de puerto.

Administración de la tabla de configuración de control del conmutador/puerto de multidifusión de puente "reenviar todos"

En la tabla siguiente se describen los controles utilizados para definir los controles de puerto.

Tabla 7-32. Tabla de configuración de control del conmutador/puerto de multidifusión de puente "reenviar todos"

Control de puertos	Definición
D	Conecta el puerto al enrutador o conmutador de multidifusión como puerto dinámico.
S	Conecta el puerto al enrutador o conmutador de multidifusión como puerto estático.
F	Indica que está prohibido.
En blanco	Indica que el puerto no está conectado a ningún enrutador ni conmutador de multidifusión.

Conexión de un puerto a un enrutador o conmutador de multidifusión:

1. Abra la página **Bridge Multicast Forward All** (Multidifusión de puente "reenviar todos").
2. Defina el campo **VLAN ID** (ID de VLAN).
3. Seleccione un puerto en la tabla **Ports** (Puertos) y asígnele un valor.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se conecta al enrutador o conmutador de multidifusión.

Conexión de un LAG a un enrutador o conmutador de multidifusión:

1. Abra la página **Bridge Multicast Forward All** (Multidifusión de puente "reenviar todos").
2. Defina el campo **VLAN ID** (ID de VLAN).
3. Seleccione un puerto en la tabla **LAGs** (LAG) y asigne un valor al LAG.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El LAG se conecta al enrutador o conmutador de multidifusión.

Administración de grupos LAG y puertos conectados a enrutadores de multidifusión mediante los comandos de la CLI

La siguiente tabla presenta un resumen de los comandos de la CLI equivalentes para administrar grupos LAG y puertos conectados a enrutadores de multidifusión como se muestra en la página **Bridge Multicast Forward All** (Multidifusión de puente "reenviar todos").

Tabla 7-33. Comandos de la CLI para administrar grupos LAG y puertos conectados a enrutadores de multidifusión

Comando de la CLI	Descripción
show bridge multicast filtering *id-vlan*	Muestra la configuración del filtrado de multidifusión.
bridge multicast forward-all {**add** | **remove**} {**ethernet** *lista-interfaces* | **port-channel** *lista-números-canal-puerto*}	Activa el reenvío de todos los paquetes de multidifusión en un puerto. Utilice el valor "on" de este comando para regresar al valor predeterminado.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet 1/e3

Console(config-if)# end

Console# show bridge multicast filtering 1
```

```
Filtering: Enabled

VLAN:   Forward-All

Port    Static          Status
-------  ----------------  -----------
1/e11   Forbidden       Filter
1/e12   Forward         Forward(s)
1/e13   -               Forward(d)
```

Inspección de IGMP

La página **IGMP Snooping** (Inspección de IGMP) contiene campos para activar la inspección de IGMP en cada VLAN y campos para definir el tiempo de caducidad de los paquetes. Para abrir la página **IGMP Snooping** (Inspección de IGMP), haga clic en **Switch** (Conmutador) → **Multicast Support** (Soporte para multidifusión) → **IGMP Snooping** (Inspección de IGMP) en la vista de árbol.

Figura 7-44. IGMP Snooping

VLAN ID (ID de la VLAN): indica la ID de la VLAN.

IGMP Snooping Status (Estado de inspección de IGMP): activa o desactiva la inspección de IGMP en la VLAN.

Auto Learn (Obtención automática): activa o desactiva la obtención automática en el dispositivo Ethernet.

Host Timeout (1-2147483647) (Tiempo de espera de host [(1-2147483647)]): indica el tiempo que transcurre antes de que caduque una entrada de inspección de IGMP. El valor predeterminado es 260 segundos.

Multicast Router Timeout (1-2147483647) (Tiempo de espera de enrutador de multidifusión [1-2147483647]): indica el tiempo que transcurre antes de que caduque una entrada de enrutador de multidifusión. El valor predeterminado es 300 segundos.

Leave Timeout (0-2147483647) (Tiempo de espera de cese [0-2147483647]): especifica el tiempo, en segundos, que transcurre tras recibir un mensaje de cese del puerto antes de que caduque la entrada. El valor predeterminado de tiempo de espera es 10 segundos.

Activación de la inspección de IGMP en el dispositivo

1. Abra la página **IGMP Snooping** (Inspección de IGMP).
2. Seleccione la ID de la VLAN para el dispositivo en el que debe activarse la inspección de IGMP.
3. Seleccione **Enable** (Activar) en el campo **IGMP Snooping Status** (Estado de inspección de IGMP).
4. Complete los campos de la página.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se activa la inspección de IGMP en el dispositivo.

Visualización de la tabla de inspección de IGMP

1. Abra la página **IGMP Snooping** (Inspección de IGMP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla de Inspección del IGMP.

Configuración de la inspección de IGMP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar IGMP Snooping (Inspección de IGMP) en el dispositivo.

Tabla 7-34. Comandos de la CLI para la inspección de IGMP

Comando de la CLI	Descripción
ip igmp snooping	Activa la inspección de IGMP (protocolo de pertenencia a grupos de Internet).
ip igmp snooping mrouter learn-pim-dvmrp	Activa la obtención automática de puertos de enrutador de multidifusión en el contexto de una VLAN específica.
ip igmp snooping host-time-out tiempo de espera	Establece el tiempo de espera del host.
ip igmp snooping mrouter-time-out *tiempo-espera*	Establece el tiempo de espera del enrutador de multidifusión.
ip igmp snooping leave-time-out {*tiempo-espera* | **immediate-leave**}	Establece el tiempo de espera para el cese.
show ip igmp snooping groups [**vlan** *id-vlan*] [**address** *dirección-ip-multidifusión*]	Muestra los grupos de multidifusión obtenidos por la inspección de IGMP.
show ip igmp snooping interface *id-vlan*	Muestra la configuración de la inspección de IGMP.
show ip igmp snooping mrouter [interface id-vlan]	Muestra información sobre interfaces de enrutadores de multidifusión obtenidas de manera dinámica.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console> enable

console# config

console(config)# ip igmp snooping

console(config)# interface vlan 1

console(config-if)# ip igmp
snooping mrouter learn-pim-dvmrp

console(config-if)# ip igmp
snooping host-time-out 300

Console(config-if)# ip igmp
snooping mrouter-time-out 200

console(config-if)# ip igmp
snooping leave-time-out 60

console(config-if)# end

console# show ip igmp snooping
groups

Vlan  IP Address       Querier   Ports
----- ---------------- --------- --------
---   ---------------- ------    --------
```

	-		--------
1	224-239.130|2.2.3	Yes	1/e11, 1/e12
19	224-239.130|2.2.8	Yes	1/e11-13

```
console# show ip igmp snooping interface 1/e1


IGMP Snooping is globally enabled


IGMP Snooping is enabled on VLAN 1


IGMP host timeout is 300 sec


IGMP Immediate leave is disabled.
IGMP leave timeout is 60 sec


IGMP mrouter timeout is 200 sec


Automatic learning of multicast
router ports is enabled


console# show ip igmp snooping mrouter
```

VLAN	Ports		
----	------		
1	1/e11		

Regresar a la página de contenido

Regresar a la página de contenido

Visualización de estadísticas

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

La página **Statistics** (Estadísticas) contiene información de dispositivos para el uso del dispositivo, la interfaz, GVRP, etherlike y RMON. Para abrir la página **Statistics** (Estadísticas), haga clic en **Statistics** (Estadísticas) en la vista de árbol.

NOTA: los comandos de la CLI no se encuentran disponibles para todas las páginas de estadísticas.

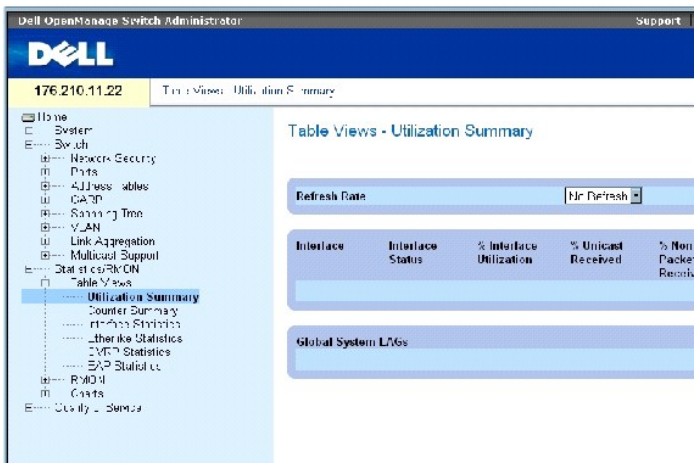
Visualización de las tablas

La página **Table Views** (Vistas de tabla) contiene enlaces para visualizar estadísticas en formato de tabla. Para abrir la página, haga clic en **Statistics** (Estadísticas) → **Table** (Tabla) en la vista de árbol.

Visualización del resumen de utilización

La página Utilization Summary contiene estadísticas de la utilización de la interfaz. Para abrir la página, haga clic en **Statistics** (Estadísticas) → **Table Views** (Vistas de tabla) → **Utilization Summary** (Resumen de utilización) en la vista de árbol.

Figura 8-1. Utilization Summary



NOTA: esta pantalla se actualiza de forma periódica para minimizar el impacto en ordenadores con menos memoria. La imagen puede aparecer distorsionada mientras se lleva a cabo esta operación.

La página Utilization Summary (Resumen de utilización) contiene los campos siguientes:

Refresh Rate (Frecuencia de actualización): indica el tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Interface (Interfaz): indica el número de la interfaz.

Interface Status (Estado de la interfaz): indica el estado de la interfaz.

% Interface Utilization (Porcentaje de utilización de la interfaz): indica el porcentaje de utilización de la interfaz de red basado en el modo dúplex de la interfaz. El intervalo de este porcentaje es del 0 al 200%. El porcentaje máximo de 200% de una conexión dúplex completa indica que el tráfico que tiene lugar a través de la interfaz utiliza el 100% del ancho de banda de las conexiones entrantes y salientes. El porcentaje máximo de una conexión semidúplex media es 100%.

% Unicast Received (Porcentaje de difusión única recibido): indica el porcentaje de paquetes de difusión única recibidos en la interfaz.

% Non Unicast Packets Received (Porcentaje de paquetes que no son de difusión única recibidos): indica el porcentaje de paquetes que no son difusión única que se han recibido en la interfaz.

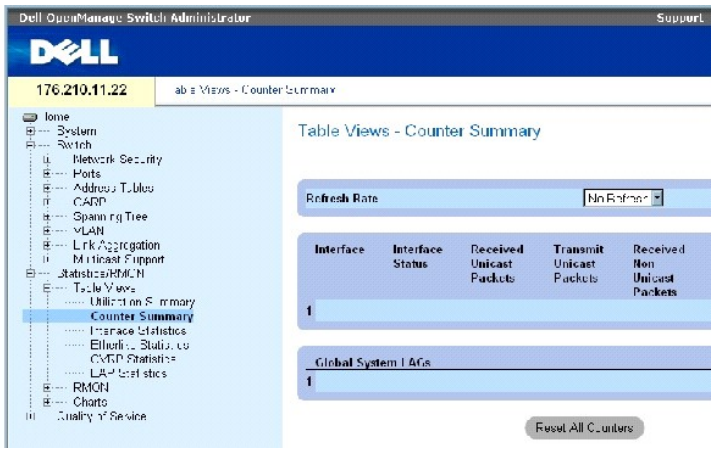
% Error Packets Received (Porcentaje de paquetes con error recibidos): indica el porcentaje de paquetes con errores recibidos en la interfaz.

Global System LAGs (LAG de sistema global): indica la utilización del LAG global actual.

Visualización del resumen de contador

La página **Counter Summary** (Resumen de contadores) contiene estadísticas para la utilización del puerto en sumas numéricas en vez de porcentajes. Para abrir la página **Counter Summary** (Resumen de contadores), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **Counter Summary** (Resumen de contadores) en la vista de árbol.

Figura 8-2. Counter Summary



La página Counter Summary (Resumen de contadores) contiene los campos siguientes:

Refresh Rate (Frecuencia de actualización): indica el tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Interface (Interfaz): indica el número de la interfaz.

Interface Status (Estado de la interfaz): indica el estado de la interfaz.

Received Unicast Packets (Paquetes de difusión única recibidos): indica el número de paquetes de difusión única recibidos en la interfaz.

Transmit Unicast Packets (Paquetes de difusión única transmitidos): indica el número de paquetes de difusión única transmitidos desde la interfaz.

Received Non Unicast Packets (Paquetes que no son de difusión única recibidos): indica el número de paquetes que no son de difusión única recibidos en la interfaz.

Transmit Non Unicast Packets (Paquetes que no son de difusión única transmitidos): indica el número de paquetes que no son de difusión única transmitidos desde la interfaz.

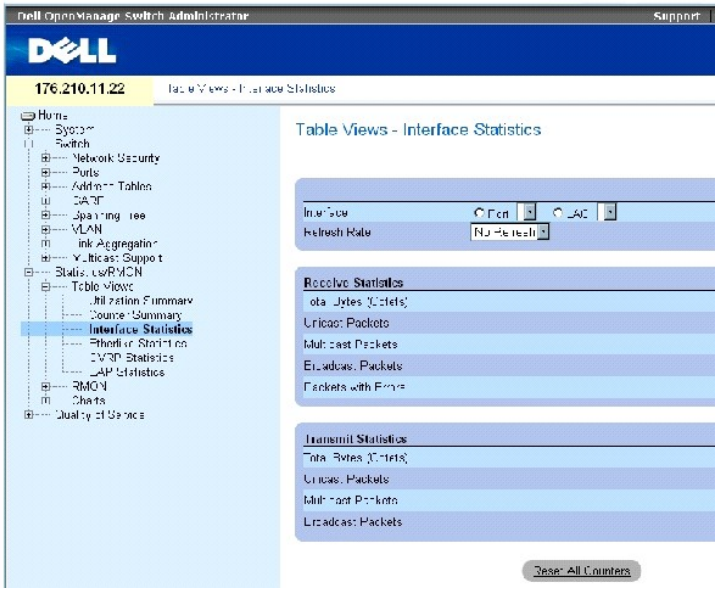
Received Errors (Errores recibidos): indica el número de paquetes recibidos con errores en la interfaz.

Global System LAGs (LAG de sistema global): proporciona un resumen de contadores de los LAG de sistema global.

Visualización de las estadísticas de interfaz

La página **Interface Statistics** (Estadísticas de interfaz) contiene estadísticas de los paquetes recibidos y transmitidos. Los campos de los paquetes recibidos y transmitidos son idénticos. Para abrir la página **Interface Statistics** (Estadísticas de interfaz), haga clic en **Statistics/RMON** (Estadística/RMON) → **Table Views** (Vistas de tabla) → **Interface Statistics** (Estadísticas de interfaz) en la vista de árbol.

Figura 8-3. Interface Statistics



La página **Interface Statistics** (Estadísticas de interfaz) contiene los campos siguientes:

Interface (Interfaz): especifica si las estadísticas se visualizan para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas de la interfaz.

Receive Statistics (Recepción de estadísticas)

Total Bytes (Octets) (Total de bytes [Octetos]): número de octetos recibidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): número de paquetes de difusión única recibidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): número de paquetes de multidifusión recibidos en la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): número de paquetes de difusión recibidos en la interfaz seleccionada.

Transmit Statistics (Transmisión de estadísticas)

Total Bytes (Octets) (Total de bytes [Octetos]): número de octetos transmitidos desde la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): número de paquetes de difusión única transmitidos desde la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): número de paquetes de multidifusión transmitidos desde la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): número de paquetes de difusión transmitidos desde la interfaz seleccionada.

Visualización de estadísticas de interfaz

1. Abra la página **Interface Statistics** (Estadísticas de interfaz).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Aparecen las estadísticas para la interfaz seleccionada.

Restablecimiento de los contadores de estadísticas de la interfaz

1. Abra la página **Interface Statistics** (Estadísticas de interfaz).
2. Haga clic en **Reset All Counters** (Restablecer todos los contadores).

Se restablecen los contadores de estadísticas de la interfaz.

Visualización de las estadísticas de la interfaz mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver las estadísticas de la interfaz.

Tabla 8-1. Comandos de la CLI de estadísticas de la interfaz

Comando de la CLI	Descripción
show interfaces counters [**ethernet** *interfaz* | **port- channel** *número-canal-puerto*]	Muestra el tráfico visto por la interfaz física.

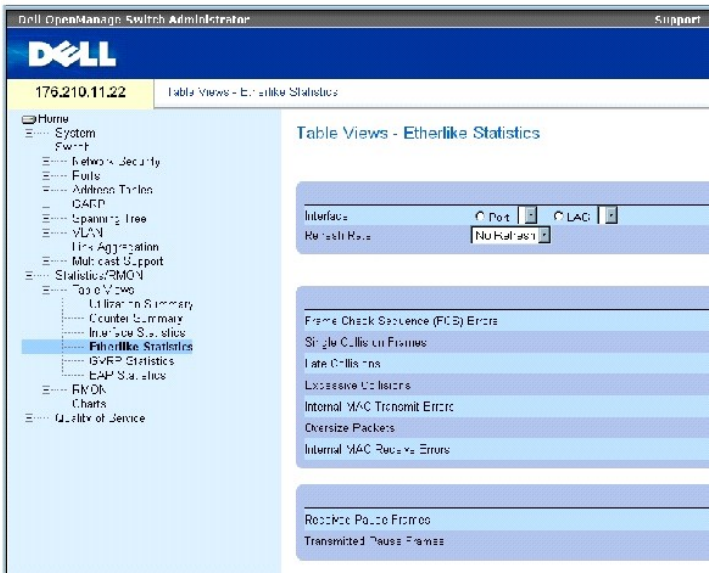
A continuación se muestra un ejemplo de comandos de la CLI.

```
console> enable

console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

------ --------- ----------- ----------- -----------

1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0

1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

1/e9 0 0 0 0

1/e10 0 0 0 0
```

Visualización de estadísticas de Etherlike

La página **Etherlike Statistics** (Estadísticas de Etherlike) contiene estadísticas de error de la interfaz. Para abrir la página **Etherlike Statistics** (Estadísticas de Etherlike), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **Etherlike Statistics** (Estadísticas de Etherlike) en la vista de árbol.

Figura 8-4. Etherlike Statistics



La página **Etherlike Statistics** (Estadísticas de Etherlike) contiene los campos siguientes:

Interface (Interfaz): especifica si las estadísticas se visualizan para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas de la interfaz.

Frame Check Sequence (FCS) Errors (Errores de secuencia de verificación de tramas [FCS]): número de errores FCS recibidos en la interfaz seleccionada.

Single Collision Frames (Tramas de colisión única): número de errores de tramas de colisión única recibidos en la interfaz seleccionada.

Late Collisions (Colisiones tardías): número de colisiones demoradas recibidas en la interfaz seleccionada.

Oversize Packets (Paquetes demasiado grandes): número de paquetes demasiado grandes en la interfaz seleccionada.

Internal MAC Transmit Errors (Errores de transmisión MAC internos): número de errores de transmisión MAC internos en la interfaz seleccionada.

Received Pause Frames (Tramas de pausa recibidas): número de errores de pausa recibidos en la interfaz seleccionada.

Transmitted Pause Frames (Tramas de pausa transmitidas): número de errores de pausa transmitidos en la interfaz seleccionada.

Visualización de estadísticas de Etherlike para una interfaz

1. Abra la página **Etherlike Statistics** (Estadísticas de Etherlike).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Restablecimiento de estadísticas de Etherlike

1. Abra la página **Etherlike Statistics** (Estadísticas de Etherlike).
2. Haga clic en **Reset All Counters** (Restablecer todos los contadores).

Se restablecen los contadores de Etherlike Statistics (Estadísticas de Etherlike).

Visualización de las estadísticas de Etherlike mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver las estadísticas de Etherlike.

Tabla 8-2. Comandos de la CLI de estadísticas de Etherlike

Comando de la CLI	Descripción
show interfaces counters [**ethernet** *interfaz* | **port- channel** número-canal-puerto]	Muestra el tráfico visto por la interfaz física.

A continuación se muestra un ejemplo de comandos de la CLI.

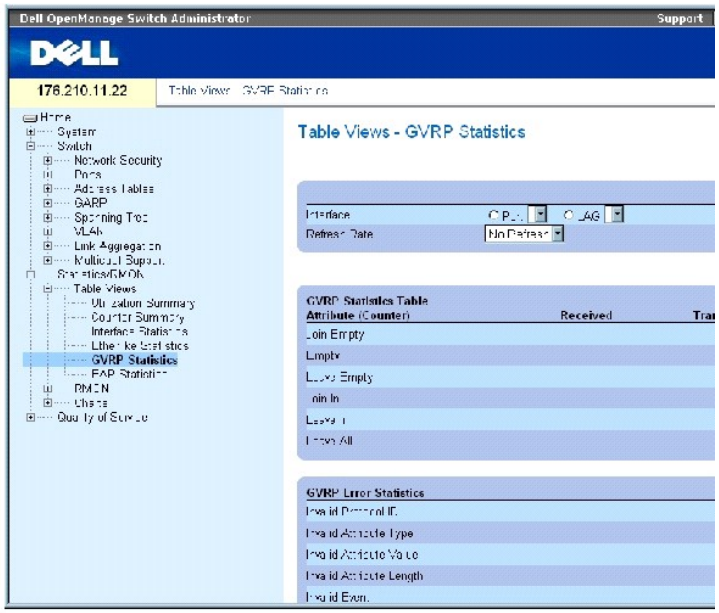
```
Console# show interfaces counters ethernet 1/1

Port    IN Octets    InUcastPkts    InMcastPkts    InBcastPkts
----    ---------    -----------    -----------    -----------
1/e1    183892       1289           987            8

Port    OUT Octets   OutUcastPkts   OutMcastPkts   OutBcastPkts
----    ----------   ------------   ------------   ------------
1/e1    9188         9              8              0

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0
```

Excessive Collisions: 0	
Internal MAC Tx Errors: 0	
Carrier Sense Errors: 0	
Oversize Packets: 0	
Internal MAC Rx Errors: 0	
Received Pause Frames: 0	
Transmitted Pause Frames: 0	

Visualización de estadísticas de GVRP

La página **GVRP Statistics** (Estadísticas de GVRP) contiene estadísticas de dispositivos para GVRP. Para abrir la página, haga clic en **Statistics / RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **GVRP Statistics** (Estadísticas de GVRP) en la vista de árbol.

Figura 8-5. GVRP Statistics



La página **GVRP Statistics** (Estadísticas de GVRP) contiene los campos siguientes:

Interface (Interfaz): especifica si las estadísticas se visualizan para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas de la interfaz.

Join Empty (Unir vacíos): estadísticas de Join Empty de GVRP del dispositivo.

Leave Empty (Dejar vacíos): estadísticas de Leave Empty de GVRP del dispositivo.

Empty (Vacío): indica el número de estadísticas de Empty de GVRP.

Join In (Unir): estadísticas de Join In de GVRP del dispositivo.

Leave In (Dejar): estadísticas de Leave In de GVRP del dispositivo.

Leave All (Dejar todo): estadísticas de Leave all de GVRP del dispositivo.

Invalid Protocol ID (ID de protocolo no válido): estadísticas de Invalid Protocol ID de GVRP del dispositivo.

Invalid Attribute Type (Tipo de atributo no válido): estadísticas de Invalid Attribute Type de GVRP del dispositivo.

Invalid Attribute Value (Valor de atributo no válido): estadísticas de Invalid Attribute Value de GVRP del dispositivo.

Invalid Attribute Length (Longitud de atributo no válida): estadísticas de Invalid Attribute Length de GVRP del dispositivo.

Invalid Events (Evento no válido): estadísticas de Invalid Events de GVRP del dispositivo.

Visualización de estadísticas de GVRP para un puerto

1. Abra la página **GVRP Statistics** (Estadísticas de GVRP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Aparecen las estadísticas de GVRP para la interfaz seleccionada.

Restablecimiento de las estadísticas de GVRP

1. Abra la página **GVRP Statistics** (Estadísticas de GVRP).
2. Haga clic en **Reset All Counters** (Restablecer todos los contadores).

Se restablecen los contadores de estadísticas de GVRP.

Visualización de las estadísticas de GVRP mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver las estadísticas de GVRP.

Tabla 8-3. Comandos de la CLI de estadísticas de GVRP

Comando de la CLI	Descripción
show gvrp statistics [**ethernet** *interfaz*| **port- channel** *número-canal- puerto*]	Muestra las estadísticas de GVRP.
show gvrp error- statistics [**ethernet** *interfaz*| **port-channel** *número-canal-puerto*]	Muestra las estadísticas de error de GVRP.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show gvrp statistics

GVRP statistics:

----------------

Legend:

rJE: Join Empty Received

rJIn: Join In Received

rEmp: Empty Received

rLIn: Leave In Received

rLE: Leave Empty Received

rLA: Leave All Received

sJE: Join Empty Sent

sJIn: Join In Sent

sEmp: Empty Sent

sLIn: Leave In Sent

sLE: Leave Empty Sent

sLA: Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE
sLA

---- --- ---- ---- ---- --- --- --- --- --- ---- --- --
-

1/e1 0 0 0 0 0 0 0 0 0 0 0 0
```

```
1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 00 0
```

```
Console# show gvrp error-statistics

GVRP error statistics:

----------------

Legend:

INVPROT : Invalid Protocol Id

INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type

INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value

INVEVENT : Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

---- ------- ------- ------- ------ - ------ - -------

1/e1 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0
```

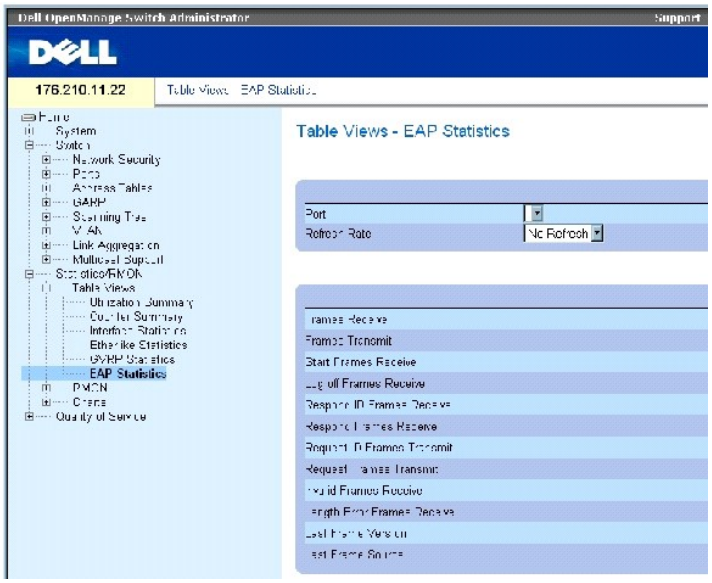
```
sLE: Leave Empty Sent

sLA: Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE
```

```
sLA


---- --- ---- ---- ---- --- --- --- --- --- ---- --- --
-


1/e1 0 0 0 0 0 0 0 0 0 0 0 0


1/e2 0 0 0 0 0 0 0 0 0 0 0 0


1/e3 0 0 0 0 0 0 0 0 0 0 0 0


1/e4 0 0 0 0 0 0 0 0 0 0 0 0


1/e5 0 0 0 0 0 0 0 0 0 0 0 0


1/e6 0 0 0 0 0 0 0 0 0 0 0 0


1/e7 0 0 0 0 0 0 0 0 0 0 0 0


1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

Visualización de las estadísticas EAP

La página **EAP Statistics** (Estadísticas de EAP) contiene información sobre paquetes EAP recibidos en un puerto específico. Para obtener más información sobre EAP, consulte "**Configuración de la autenticación basada en el puerto**". Para abrir la página **EAP Statistics** (Estadísticas de EAP), haga clic en Statistics/RMON (Estadísticas/RMON) → Table Views (Vistas de tabla) → EAP Statistics (Estadísticas EAP) en la vista de árbol.

Figura 8-6. EAP Statistics



La página EAP Statistics (Estadísticas de EAP) contiene los campos siguientes:

Port (Puerto): indica el puerto que se sondea para las estadísticas.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas de la interfaz.

Frames Receive (Tramas recibidas): indica el número de tramas EAPOL válidas recibidas en el puerto.

Frames Transmit (Tramas transmitidas): indica el número de tramas EAPOL transmitidas a través del puerto.

Start Frames Receive (Tramas de inicio recibidas): indica el número de tramas de inicio EAPOL recibidas en el puerto.

Log off Frames Receive (Tramas de cierre de sesión recibidas): indica el número de tramas de cierre de sesión EAPOL recibidas en el puerto.

Respond ID Frames Receive (Tramas de ID de respuesta recibidas): indica el número de tramas de respuesta/ID EAP recibidas en el puerto.

Respond Frames Receive (Tramas de respuesta recibidas): indica el número de tramas de respuesta EAP válidas recibidas en el puerto.

Request ID Frames Transmit (Tramas de ID de petición transmitidas): indica el número de tramas de petición/ID EAP transmitidas a través del puerto.

Request Frames Transmit (Tramas de petición transmitidas): indica el número de tramas de petición EAP transmitidas a través del puerto.

Invalid Frames Receive (Tramas no válidas recibidas): indica el número de tramas EAPOL no reconocidas que se han recibido en este puerto.

Length Error Frames Receive (Tramas con longitud errónea recibidas): indica el número de tramas EAPOL con una longitud de cuerpo de paquete no válida recibidas en este puerto.

Last Frame Version (Versión de la última trama): indica el número de versión del protocolo que va unido a la trama de EAPOL que se ha recibido más recientemente.

Last Frame Version (Origen de la última trama): indica la dirección MAC de origen que va unida a la trama de EAPOL que se ha recibido más recientemente.

Visualización de las estadísticas de EAP para un puerto

1. Abra la página **EAP Statistics** (Estadísticas de EAP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de EAP.

Para restablecer las estadísticas de EAP

1. Abra la página **EAP Statistics** (Estadísticas de EAP).
2. Haga clic en Reset All Counters (Restablecer todos los contadores).

Se restablecen los contadores de estadísticas de EAP.

Visualización de las estadísticas de EAP mediante los comandos de la CLI

En la tabla siguiente se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de EAP.

Tabla 8-4. Comandos de la CLI de estadísticas de EAP

Comando de la CLI	Descripción
show dot1x statistics	Muestra las estadísticas 802.1X de la interfaz especificada.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console# show dot1x statistics ethernet 1/e1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

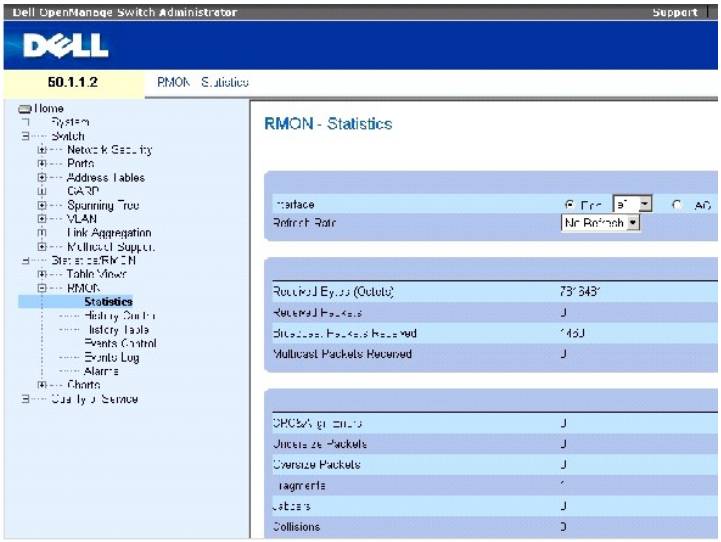
Visualización de las estadísticas de RMON

RMON (Supervisión remota) permite que los administradores de red vean la información del tráfico de red desde una ubicación remota. Para abrir la página **RMON**, haga clic en **Statistics / RMON** (Estadísticas/RMON) → **RMON** en la vista de árbol.

Visualización del grupo de estadísticas de RMON

Utilice la información que se visualiza en la página RMON Statistics (Estadísticas de RMON) sobre la utilización del dispositivo y los errores producidos en éste. Para abrir la página RMON Statistics (Estadísticas de RMON), haga clic en **Statistics / RMON** (Estadísticas/RMON) → **RMON** → **Statistics** (Estadísticas) en la vista de árbol.

Figura 8-7. RMON Statistics



La página RMON Statistics (Estadísticas de RMON) contiene los campos siguientes:

Interface (Interfaz): especifica el puerto o LAG cuyas estadísticas se visualizan.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas.

Received Bytes (Octets) (Bytes recibidos [Octetos]): número de bytes recibidos en la interfaz seleccionada.

Received Packets (Paquetes recibidos): número de paquetes recibidos en la interfaz seleccionada.

Broadcast Packets Received (Paquetes de difusión recibidos): número de paquetes de difusión correctos recibidos en la interfaz desde la última actualización del dispositivo. Este número no incluye los paquetes de multidifusión.

Multicast Packets Received (Paquetes de multidifusión recibidos): número de paquetes de multidifusión correctos recibidos en la interfaz desde la última actualización del dispositivo.

CRC & Align Errors (Errores de CRC y de alineación): número de errores de CRC (verificación de redundancia cíclica) y de alineación que se han producido en la interfaz desde la última actualización del dispositivo.

Undersize Packets (Paquetes demasiado pequeños): número de paquetes cuyo tamaño es demasiado pequeño (menos de 64 octetos) recibidos en la interfaz desde la última actualización del dispositivo.

Oversize Packets (Paquetes demasiado grandes): número de paquetes cuyo tamaño es demasiado grande (más de 1.518 octetos) recibidos en la interfaz desde la última actualización del dispositivo.

Fragments (Fragmentos): número de fragmentos (paquetes con menos de 64 octetos, sin incluir los bits de trama, pero incluyendo los octetos FCS) recibidos en la interfaz desde la última actualización del dispositivo.

Jabbers (Mensajes jabber): número de mensajes jabber (paquetes de más de 1.518 octetos) recibidos en la interfaz desde la última actualización del dispositivo.

Collisions (Colisiones): número de colisiones recibidas en la interfaz desde la última actualización del dispositivo.

Frames of *xx* Bytes (Tramas de xx bytes): número de tramas de *xx* bytes recibidas en la interfaz desde la última actualización del dispositivo.

Visualización de las estadísticas de interfaz

1. Abra la página RMON Statistics (Estadísticas de RMON).
2. Seleccione un tipo y número de interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de la interfaz.

Visualización de las estadísticas de RMON mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver las estadísticas de RMON.

Tabla 8-5. Comandos de la CLI de estadísticas de RMON

Comando de la CLI	Descripción
show rmon statistics {**ethernet** *interfaz* | **port- channel** *número-canal- puerto*}	Muestra las estadísticas de Ethernet de RMON.

A continuación se muestra un ejemplo de los comandos de la CLI:

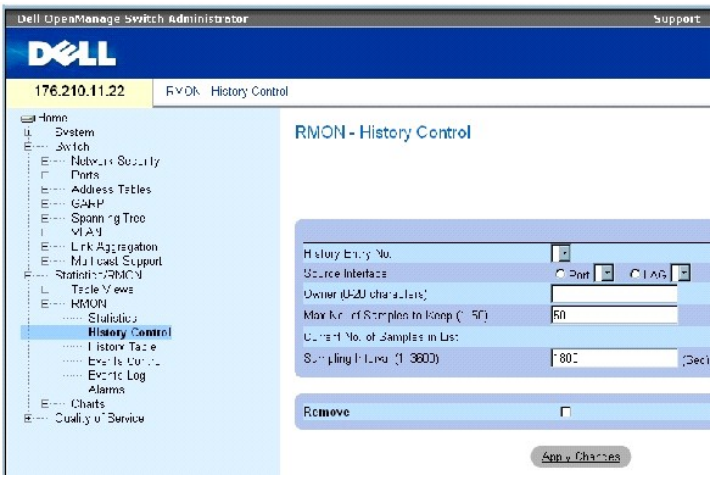
```
console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0
```

```
Undersize Pkts: 0 Oversize Pkts: 0


Fragments: 0 Jabbers: 0


64 Octets: 98 65 to 127 Octets: 0


128 to 255 Octets: 256 to 511 Octets: 0


512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Visualización de las estadísticas de control de historial de RMON

La página **RMON History Control** (Control de historial de RMON) contiene información sobre muestras de datos obtenidos desde los puertos. Por ejemplo, las muestras pueden incluir definiciones de interfaz o periodos de sondeo. Para abrir la página **RMON History Control** (Control de historial de RMON), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **History Control** (Control del historial) en la vista de árbol.

Figura 8-8. RMON History Control



La página **RMON History Control** (Control de historial de RMON) contiene los campos siguientes:

History Entry No. (Nº de entrada del historial): indica el número de entrada de la página **History Control** (Control del historial).

Source Interface (Interfaz de origen): puerto o LAG desde el que se han obtenido las muestras del historial.

Owner (0-20 characters) (Propietario [0-20 caracteres]): usuario o estación de RMON que ha solicitado información sobre RMON.

Max No. of Samples to Keep (1-50) (Número máximo de muestras que se deben conservar [1-50]): número máximo de muestras que se guardarán. El valor predeterminado es 50.

Current No. of Samples in List (Número actual de muestras en la lista): indica el número actual de muestras obtenidas.

Sampling Interval (1-3600) (Intervalo de muestreo [1-3600]): indica el tiempo, expresado en segundos, que se tarda en obtener los muestreos desde los

puertos. Los valores posibles están comprendidos entre 1 y 3.600 segundos. El valor predeterminado es 1.800 segundos (30 minutos).

Remove (Eliminar): si se selecciona esta opción, se elimina la entrada **History Control Table** (Tabla de control del historial).

Adición de una entrada del control de historial

1. Abra la página **RMON History Control** (Control de historial de RMON).
2. Haga clic en **Add** (Añadir).

   Se abre la página **Add History Entry** (Añadir entrada del historial).
3. Complete los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   La entrada se añade a la tabla **History Control Table** (Tabla de control del historial).

Modificación de una entrada de la tabla de control del historial

1. Abra la página **RMON History Control** (Control de historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).
3. Modifique los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se modifica la entrada de la tabla y se actualiza el dispositivo.

Eliminación de una entrada de la tabla de control de historial

1. Abra la página **RMON History Control** (Control de historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).
3. Haga clic en **Apply Changes** (Aplicar cambios).

   Se elimina la entrada de la tabla y se actualiza el dispositivo.

Visualización del control del historial de RMON mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver el control del historial de RMON.

Tabla 8-6. Comandos de la CLI del historial de RMON

Comando de la CLI	Descripción
rmon collection history indice [**owner** *nombre de propietario* | **buckets** *número de depósito*] [**interval** *segundos*]	Activa y configura RMON en una interfaz.
show rmon collection history [**ethernet** *interfaz* | **port-channel** *número-puerto-canal*]	Muestra las estadísticas del historial de recopilación de RMON.

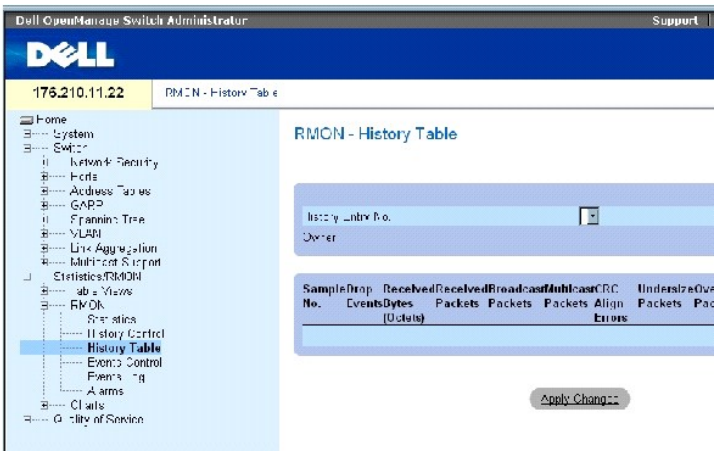
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface ethernet 1/e8


console(config-if)# rmon collection history 1 interval
2400
```

Visualización de la tabla historial de RMON

La tabla **RMON History Table** (Tabla de historial de RMON) contiene muestreos estadísticos de red específicos de la interfaz. Cada entrada de la tabla representa todos los valores del contador recopilados durante un solo muestreo. Para abrir la página **RMON History Table** (Tabla de historial de RMON), haga clic en **Statistics / RMON** (Estadísticas/RMON) → **RMON**→ **History Table** (Tabla del historial) en la vista de árbol.

Figura 8-9. RMON History Table



La página **RMON History Table** (Tabla de historial de RMON) contiene los campos siguientes:

NOTA: en la tabla de historial de RMON no aparecen todos los campos.

History Entry No. (Nº de entrada del historial): especifica el número de entrada de la página **History Control** (Control del historial).

Owner (Propietario): indica el usuario o la estación RMON que solicitó la información sobre RMON.

Sample No. (N° de muestra): indica el número de la muestra específica que refleja la información de la tabla.

Drop Events (Eventos descartados): número de paquetes descartados debido a la falta de recursos de la red durante el intervalo de muestreo. Probablemente no represente el número exacto de paquetes descartados, sino el número de veces en que se detectaron paquetes descartados.

Received Bytes (Octets) (Bytes [octetos] recibidos): número de octetos de datos, incluidos los paquetes deficientes, recibidos en la red.

Received Packets (Paquetes recibidos): número de paquetes recibidos durante el intervalo de muestreo.

Broadcast Packets (Paquetes de difusión): número de paquetes de difusión en buen estado que se han recibido durante el intervalo de muestreo.

Multicast Packets (Paquetes de multidifusión): número de paquetes de multidifusión en buen estado que se han recibido durante el intervalo de muestreo.

CRC Align Errors (Errores de alineación de CRC): número de paquetes recibidos durante la sesión de muestreo con una longitud de 64-1.518 octetos. Sin embargo, los paquetes tienen una secuencia de comprobación de tramas (FCS) errónea con un número entero de octetos o una FCS errónea con un número no entero de octetos.

Undersize Packets (Paquetes demasiado pequeños): número de paquetes con una longitud inferior a 64 octetos recibidos durante la sesión de muestreo.

Oversize Packets (Paquetes demasiado grandes): número de paquetes con una longitud superior a 1.518 octetos recibidos durante la sesión de muestreo.

Fragments (Fragmentos): número de paquetes recibidos cuya longitud es inferior a 64 octetos y que han tenido una FCS durante la sesión de muestreo.

Jabbers (Mensajes jabber): número de paquetes recibidos cuya longitud es superior a 1.518 octetos y que han tenido una FCS durante la sesión de muestreo.

Collisions (Colisiones): realiza una estimación del número total de colisiones de paquetes que se han producido durante la sesión de muestreo. Las colisiones se detectan cuando los puertos repetidores detectan dos ó más estaciones que transmiten simultáneamente.

Utilization (Uso): estima el uso de red de capa física principal en una interfaz durante la sesión de muestreo. El valor se refleja en tanto por ciento hasta dos decimales.

Visualización de las estadísticas para una entrada específica del historial

1. Abra la página **RMON History Table** (Tabla de historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).

Las estadísticas de entrada aparecen en la tabla de historial de RMON.

Visualización del control del historial de RMON mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver el historial de RMON.

Tabla 8-7. Comandos de la CLI de control del historial de RMON

Comando de la CLI	Descripción
show rmon history index {throughput | errors | other} [period segundos]	Muestra el historial de las estadísticas de Ethernet de RMON.

A continuación se muestra un ejemplo de los comandos de la CLI para visualizar las estadísticas de Ethernet de RMON sobre la producción en el índice 1:

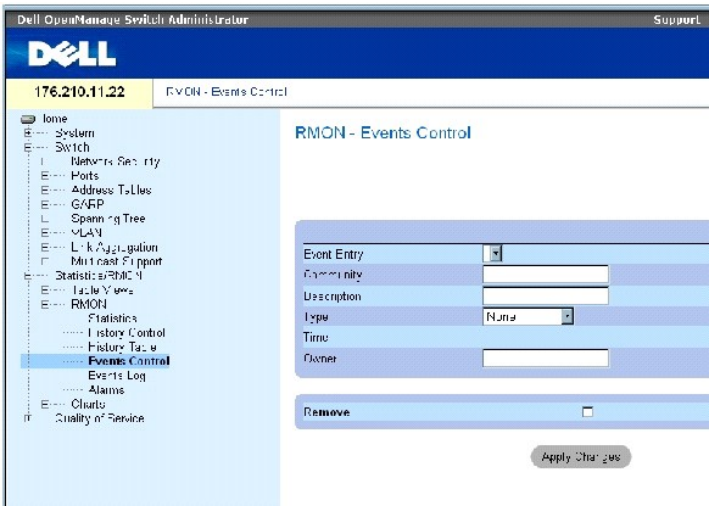
```
console> enable

console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10
```

```
Requested samples: 50 Granted samples: 50


Maximum table size: 270


Time Octets Packets Broadcast Multicast %


------------------ -- ---- -- ------- ------- -- ------
--- ---


09-Mar-2003 18:29:32 0 0 0 0 0


09-Mar-2003 18:29:42 0 0 0 0 0


09-Mar-2003 18:29:52 0 0 0 0 0


09-Mar-2003 18:30:02 0 0 0 0 0


09-Mar-2003 18:30:12 0 0 0 0 0


09-Mar-2003 18:30:22 0 0 0 0 0
```

Definición de los eventos de RMON del dispositivo

Utilice la página **RMON Events Control** (Control de eventos de RMON) para definir los eventos de RMON. Para abrir la página **RMON Events Control** (Control de eventos de RMON), haga clic en **Statistics / RMON** (Estadísticas/RMON) → **RMON** → **Events Control** (Control de eventos) en la vista de árbol.

Figura 8-10. RMON Events Control



La página **RMON Events Control** (Control de eventos de RMON) contiene los campos siguientes:

Event Entry (Entrada de evento): indica el evento.

Community (Comunidad): indica la comunidad a la que pertenece el evento.

Description (Descripción): descripción del evento definida por el usuario.

Type (Tipo): describe el tipo de evento. Los valores posibles son:

Log (Registro): el tipo de evento es una entrada de registro.

Trap (Captura): el tipo de evento es una captura.

Log and Trap (Registro y captura): el tipo de evento es una entrada de registro y una captura.

None (Ninguno): no hay ningún evento.

Time (Hora): hora en la que se ha producido el evento.

Owner (Propietario): dispositivo o usuario que ha definido el evento.

Remove (Eliminar): si se selecciona esta opción, se elimina el evento de la tabla de eventos de RMON.

Adición de un evento de RMON

1. Abra la página **RMON Events Control** (Control de eventos de RMON).
2. Haga clic en **Add** (Añadir).

   Se abre la página **Add an Event Entry** (Añadir una entrada de evento).
3. Complete la información en el cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

   Se añade la entrada de la **tabla de eventos** y se actualiza el dispositivo.

Modificación de un evento de RMON

1. Abra la página **RMON Events Control** (Control de eventos de RMON).
2. Seleccione una entrada en **Event Table** (Tabla de eventos).
3. Modifique los campos en el cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

   Se modifica la entrada de **Event Table** (Tabla de eventos) y se actualiza el dispositivo.

Eliminación de entradas de eventos de RMON

1. Abra la página **RMON Events Control** (Control de eventos de RMON).
2. Haga clic en **Show All** (Mostrar todo).

   Se abre la página **RMON Events Table** (Tabla de eventos de RMON).

3. Seleccione la casilla de verificación **Remove** (Eliminar) para eliminar los eventos que desee y, a continuación, haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la tabla y se actualiza el dispositivo.

NOTA: se puede eliminar una única entrada de evento desde la página **RMON Events Control** (Control de eventos de RMON) seleccionando la casilla de verificación **Remove** (Eliminar) de dicha página.

Definición de eventos de dispositivo mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para definir eventos de dispositivo.

Tabla 8-8. Comandos de la CLI de definición de eventos de dispositivo

Comando de la CLI	Descripción
rmon event *tipo índice* [**community** *texto*] [**description** *texto*] [**owner nombre**]	Configura los eventos de RMON.
show rmon events	Muestra la tabla de eventos de RMON.

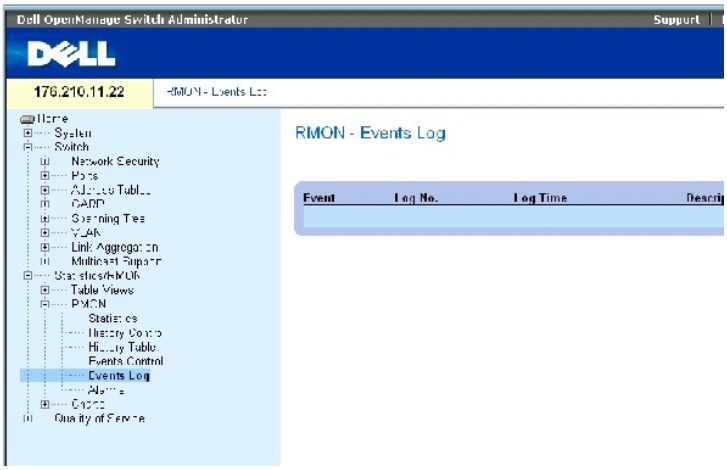
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# rmon event 1 log

console(config)# exit

console# show rmon events

Index  Description  Type  Community  Owner  Last Time Sent
-----  -----------  ----  ---------  -------  ----------
1      Errors       Log              CLI    Jan 18 2002 23:58:17
2      High Broadcast  Log-Trap  router  Manager  Jan 18 2002 23:59:48
```

Visualización del registro de eventos de RMON

La página **RMON Events Log** (Registro de eventos de RMON) contiene una lista de eventos de RMON. Para abrir la página **RMON Events Log** (Registro de eventos de RMON), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **Events Log** (Registro de eventos) en la vista de árbol.

Figura 8-11. RMON Events Log



La página **RMON Events Log** (Registro de eventos de RMON) contiene los campos siguientes:

Event (Evento): número de entrada de registro de eventos de RMON.

Log No (N° de registro): indica el número de registro.

Log Time (Tiempo de registro): hora en la que se ha introducido la entrada del registro.

Description (Descripción): describe la entrada del registro.

Definición de eventos de dispositivo mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para definir eventos de dispositivo.

Tabla 8-9. Comandos de la CLI de definición de eventos de dispositivo

Comando de la CLI	Descripción
show rmon log [*evento*]	Muestra la tabla de registros de RMON.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500

Event Description Time
```

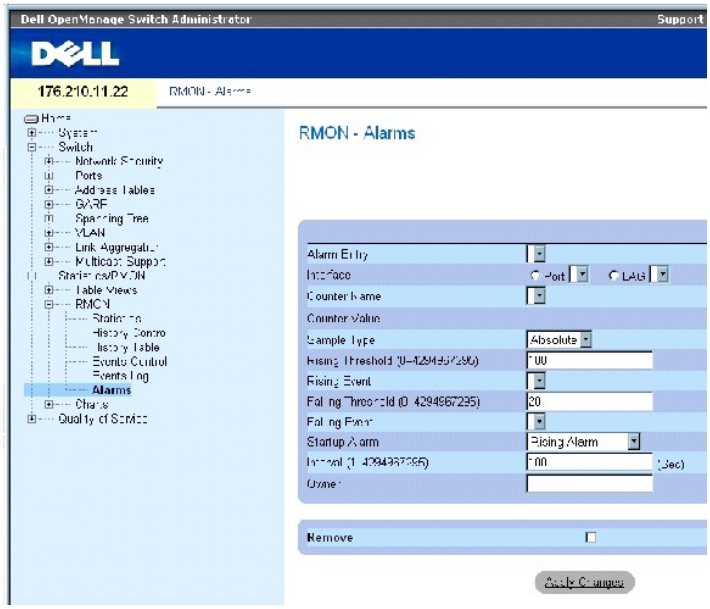
```
----- ---------- ----- --------------


1 Errors Jan 18 2002 23:58:17


2 High Broadcast Jan 18 2002 23:59:48
```

Definición de alarmas de dispositivo de RMON

Utilice la página **RMON Alarms** (Alarmas de RMON) para establecer las alarmas de red. Las alarmas de la red se activan cuando se detecta un problema o un evento en la red. El cruce de umbrales superiores e inferiores genera eventos. Para obtener más información sobre eventos, consulte "Visualización del registro de eventos de RMON".

Para abrir la página **RMON Alarms** (Alarmas de RMON), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **Alarms** (Alarmas) en la vista de árbol.

Figura 8-12. RMON Alarms



La página **RMON Alarms** (Alarmas de RMON) contiene los campos siguientes:

Alarm Entry (Entrada de alarma): indica una alarma específica.

Interface (Interfaz): indica la interfaz para la que se muestran las estadísticas de RMON.

Counter Name (Nombre del contador): indica la variable MIB seleccionada.

Counter Value (Valor del contador): valor de la variable MIB seleccionada.

Sample Type (Tipo de muestra): especifica el método de muestreo para la variable seleccionada y compara el valor con los umbrales. Los valores del campo posibles son:

Delta: resta el último valor muestreado del valor actual. La diferencia de los valores se compara con el umbral.

Absolute (Absoluto): compara los valores directamente con los umbrales al finalizar el intervalo de muestreo.

Rising Threshold (0–4294967295) (Umbral superior [0-4294967295]): indica el valor del contador superior que activa la alarma del umbral superior. El umbral superior aparece en la parte superior de las barras de gráficos. Cada variable supervisada tiene asignado un color. El valor predeterminado de este campo es 100 segundos.

Rising Event (Evento superior): mecanismo en el que se notifican alarmas, incluyendo un registro, una excepción o ambos. Cuando se selecciona un registro, no existe ningún mecanismo de almacenamiento en el dispositivo ni en el sistema de administración. Sin embargo, si el dispositivo no se restablece, permanece en la tabla de registros del dispositivo. Si se selecciona una captura, se genera una captura SNMP y se notifica a través del mecanismo de la captura. La captura se puede guardar con el mismo mecanismo.

Falling Threshold (0–4294967295) (Umbral inferior [0-4294967295]): indica el valor del contador inferior que activa la alarma del umbral inferior. El umbral inferior se presenta gráficamente en la parte superior de las barras de gráficos. Cada variable supervisada tiene asignado un color. El valor predeterminado del campo es 20.

Startup Alarm (Alarma de inicio): activador que hace funcionar la generación de alarmas. El superior se define cruzando el umbral desde un umbral de valor inferior hasta un umbral de valor superior.

Interval (1–4294967295) **(sec)** (Intervalo [1-4294967295] [seg]): intervalo de tiempo entre alarmas. El valor predeterminado de este campo es 100 segundos.

Owner (Propietario): dispositivo o usuario que ha definido la alarma.

Remove (Eliminar): si se selecciona esta opción, se elimina una alarma de RMON.

Adición de una entrada de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
2. Haga clic en **Add** (Añadir).

Se abre la página **Add an Alarm Entry** (Añadir una entrada de alarma).

Figura 8-13. Add an Alarm Entry Page

3. Seleccione una interfaz.
4. Complete los campos.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade la alarma de RMON y se actualiza el dispositivo.

Modificación de una entrada de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
2. Seleccione una entrada en el menú desplegable **Alarm Entry** (Entrada de alarma).
3. Modifique los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la entrada y se actualiza el dispositivo.

Visualización de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla **Alarms Table** (Tabla de alarmas).

Eliminación de una entrada de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
2. Seleccione una entrada en el menú desplegable **Alarm Entry** (Entrada de alarma).
3. Seleccione la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada y se actualiza el dispositivo.

Definición de alarmas de dispositivo mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para definir alarmas de dispositivo.

Tabla 8-10. Comandos de la CLI de alarma de dispositivo

Comando de la CLI	Descripción
rmon alarm *índice ID_Objeto_MIB intervalo umbral_superior umbral_inferior evento_superior evento_inferior* [**type** *tipo*] [**startup** *dirección*] [**owner** *nombre*]	Configura las condiciones de la alarma de RMON.
show rmon alarm-table	Muestra el resumen de la tabla de alarmas.
show rmon alarm	Muestra la configuración de la alarma de RMON.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1
360000 1000000 1000000 10 20
```

```
Console# show rmon alarm-table

Index OID Owner

----- ---------------------- -- -----

1 1.3.6.1.2.1.2.2.1.10.1 CLI

2 1.3.6.1.2.1.2.2.1.10.1 Manager

3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

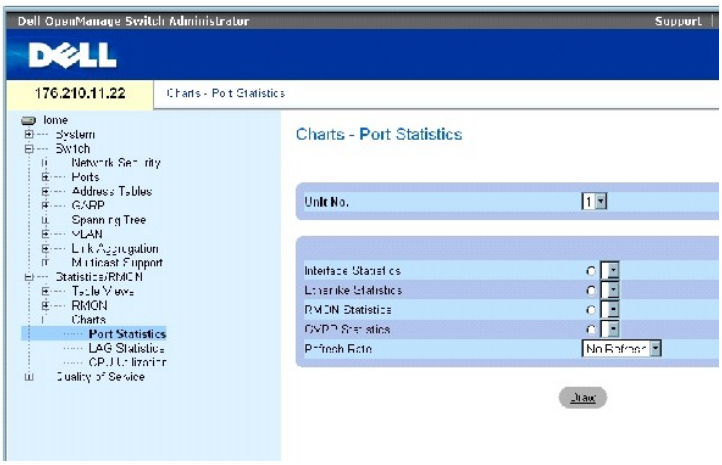
Visualización de los gráficos

La página **Chart** (Gráfico) incluye enlaces para ver las estadísticas en forma de gráfico. Para abrir la página, haga clic en Statistics (Estadísticas) → Charts (Gráficos) en la vista de árbol.

Visualización de las estadísticas de puertos

Utilice la página **Port Statistics** (Estadísticas de puerto) para abrir las estadísticas en forma de gráfico para los elementos del puerto. Para abrir la página **Port Statistics** (Estadísticas de puerto), haga clic en **Statistics/RMON** (Estadísticas(RMON) → **Charts** (Gráficos) → **Port Statistics** (Estadísticas de puerto) en la vista de árbol.

Figura 8-14. Port Statistics



La página Port Statistics (Estadísticas de puerto) contiene los campos siguientes:

Unit No. (Número de unidad): indica la unidad de apilamiento para la que se muestran las estadísticas.

Interface Statistics (Estadísticas de interfaz): selecciona las estadísticas de la interfaz que se deben visualizar.

Etherlike Statistics (Estadísticas de Etherlike): selecciona las estadísticas de Etherlike que se deben visualizar.

RMON Statistics (Estadísticas de RMON): selecciona las estadísticas de RMON que se deben visualizar.

GVRP Statistics (Estadísticas de GVRP): selecciona el tipo de estadísticas de GVRP que se deben visualizar.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas.

Visualización de las estadísticas de puerto

1. Abra la página **Port Statistics** (Estadísticas de puerto).
2. Seleccione el tipo de estadísticas que se debe abrir.
3. Seleccione la frecuencia de actualización que desee en el menú desplegable **Refresh Rate** (Frecuencia de actualización).
4. Haga clic en **Draw** (Dibujar).

Aparece el gráfico de las estadísticas seleccionadas.

Visualización de las estadísticas de puerto mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver las estadísticas de puerto.

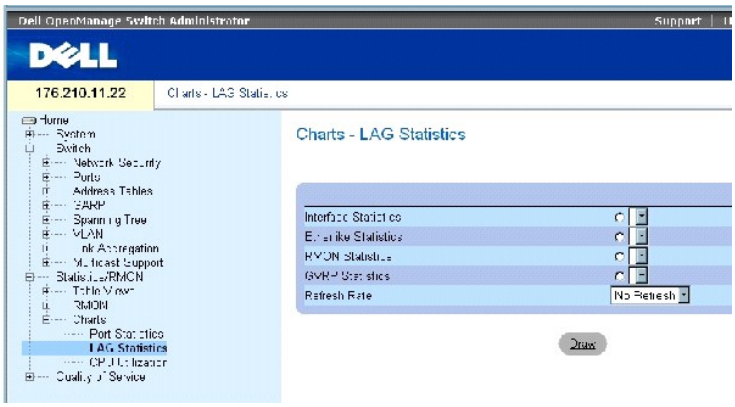
Tabla 8-11. Comandos de la CLI de estadísticas de puerto

Comando de la CLI	Descripción
show interfaces counters [**ethernet** *interfaz* | **port- channel** *número-canal-puerto*]	Muestra el tráfico visto por la interfaz física.
show rmon statistics {**ethernet** *interfaz* | **port-channel** *número- canal-puerto*}	Muestra las estadísticas de Ethernet de RMON.
show gvrp statistics {**ethernet** *interfaz* | **port-channel** *número- canal-puerto*}	Muestra las estadísticas de GVRP.
show gvrp-error statistics {**ethernet** *interfaz* | **port- channel** *número-canal-puerto*}	Muestra las estadísticas de error de GVRP.

Visualización de las estadísticas de LAG

Utilice la página **LAG Statistics** (Estadísticas de LAG) para abrir las estadísticas en forma de gráfico para los grupos LAG. Para abrir la página **LAG Statistics** (Estadísticas de LAG), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Charts** (Gráficos) → **LAG Statistics** (Estadísticas de LAG) en la vista de árbol.

Figura 8-15. LAG Statistics



La página LAG Statistics (Estadísticas de LAG) contiene los campos siguientes:

Interface Statistics (Estadísticas de interfaz): selecciona las estadísticas de la interfaz que se deben visualizar.

Etherlike Statistics (Estadísticas de Etherlike): selecciona las estadísticas de Etherlike que se deben visualizar.

RMON Statistics (Estadísticas de RMON): selecciona las estadísticas de RMON que se deben visualizar.

GVRP Statistics (Estadísticas de GVRP): selecciona el tipo de estadísticas de GVRP que se deben visualizar.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas.

Visualización de las estadísticas de LAG

1. Abra la página LAG Statistics (Estadísticas de LAG).
2. Seleccione el tipo de estadística que se debe abrir.
3. Seleccione la frecuencia de actualización que desee en el menú desplegable **Refresh Rate** (Frecuencia de actualización).
4. Haga clic en **Draw** (Dibujar).

Aparece el gráfico de las estadísticas seleccionadas.

Visualización de las estadísticas de LAG mediante los comandos de la CLI

La tabla siguiente incluye los comandos de la CLI para ver las estadísticas de LAG.

Tabla 8-12. Comandos de la CLI de estadística de LAG

Comando de la CLI	Descripción
show interfaces counters [**ethernet** *interfaz* | **port- channel** *número-canal-puerto*]	Muestra el tráfico visto por la interfaz física.
show rmon statistics {**ethernet** *interfaz* | **port-channel** *número- canal-puerto*}	Muestra las estadísticas de Ethernet de RMON.
show gvrp statistics {**ethernet** *interfaz* | **port-channel** *número- canal-puerto*}	Muestra las estadísticas de GVRP.

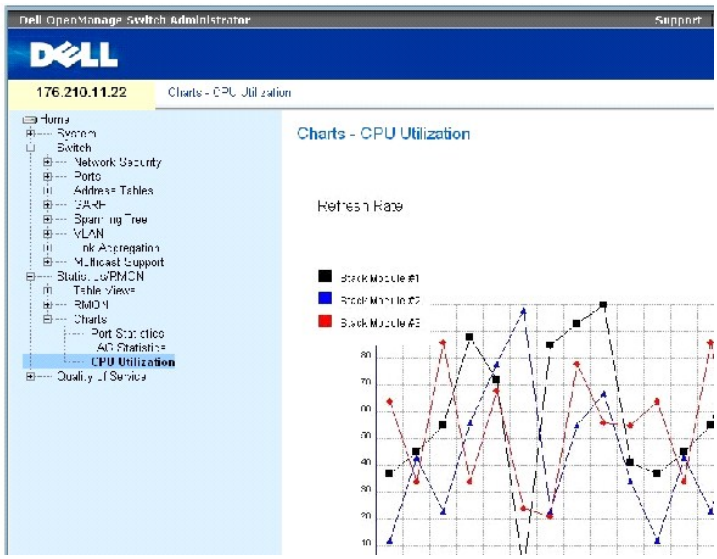
show gvrp-error statistics {**ethernet** *interfaz* | **port- channel** *número-canal-puerto*}	Muestra las estadísticas de error de GVRP.

Visualización del uso de la CPU

La página **CPU Utilization** (Uso de la CPU) contiene información sobre el uso de la CPU del sistema y el porcentaje de los recursos de la CPU consumidos por cada miembro del apilamiento. En el gráfico, se asigna un color a cada miembro del apilamiento.

Para abrir la página **CPU Utilization** (Uso de la CPU), haga clic en **Statistics / RMON** (Estadísticas/RMON) → **Charts** (Gráficos) → **CPU Utilization** (Uso de la CPU) en la vista de árbol.

Figura 8-16. CPU Utilization



La página **CPU Utilization** (Uso de la CPU) contiene la información siguiente:

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que se actualicen las estadísticas.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la calidad de servicio

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

En esta sección se proporciona información para definir y configurar los parámetros de la calidad de servicio (QoS). Para abrir la página Quality of Service (Calidad de servicio), haga clic en Quality of Service (Calidad de servicio) en la vista de árbol.

Información general sobre la calidad de servicio (QoS)

La calidad de servicio (QoS) ofrece la posibilidad de implementar la calidad de servicio y la prioridad de las colas en una red.

QoS puede ser necesaria en implementaciones como las de determinados tipos de tráfico, como voz, vídeo y tráfico en tiempo real, a los que se puede asignar una cola de prioridad alta, mientras que a otros tipos de tráfico se les puede asignar una cola de prioridad inferior. El resultado es un mejor flujo de tráfico en situaciones de tráfico muy intenso.

QoS se define mediante lo siguiente:

- Clasificación: especifica qué campos del paquete coinciden con valores específicos. Todos los paquetes que coinciden con las especificaciones definidas por el usuario se clasifican juntos.
- Acción: define la administración del tráfico en la que los paquetes que se reenvían se basan en la información del paquete y en los valores de los campos del paquete, como por ejemplo la etiqueta de prioridad de VLAN (VPT) y el punto de código de servicios diferenciados (DSCP).

Información de clasificación de VPT

Las etiquetas de prioridad de VLAN se utilizan para clasificar los paquetes asignándolos a una de las colas de salida. El usuario puede definir las asignaciones de etiquetas de prioridad de VLAN a la cola. En la tabla siguiente se detallan los valores predeterminados de la asignación de VPT a la cola:

Tabla 9-1. Valores predeterminados de la tabla de asignación de CoS a colas

Valor de CoS	Valores de las colas de envío
0	q1 (prioridad más baja)
1	q1 (prioridad más baja)
2	q1 (prioridad más baja)
3	q1 (prioridad más baja)
4	q2
5	q2
6	q3
7	q3

NOTA: en una configuración de apilamiento, la cola 4 se usa para reenviar tráfico de apilamiento. Por lo tanto, la asignación de tráfico adicional a la cola 4 puede interferir en el reenvío de tráfico.

A los paquetes que llegan sin etiqueta se les asigna un valor de VPT predeterminado, que se establece por puerto. La VPT asignada se utiliza para asignar el paquete a la cola de salida.

Los valores de DSCP pueden asignarse a colas de prioridad. En la tabla siguiente se muestran los valores predeterminados de la asignación de DSCP a la cola de salida:

Tabla 9-2. Valores predeterminados de la tabla de asignación de DSCP a colas

Valor de DSCP	Valores de las colas de envío
0-15	q1 (prioridad más baja)
16-39	q2
40-63	q3

La asignación de DSCP se activa por sistema.

Servicios de CoS

Una vez que se han asignado los paquetes a una cola de salida determinada, es posible asignar servicios de CoS a las colas. Las colas de salida se configuran con un esquema de planificación mediante uno de los métodos siguientes:

- Prioridad estricta: garantiza el reenvío de las aplicaciones para las que el tiempo es muy importante. La prioridad estricta (SP) permite priorizar el tráfico más vital y para el que el tiempo es más importante por encima de las aplicaciones para las que el tiempo no es tan importante.
  Por ejemplo, en prioridad estricta, es posible priorizar el tráfico de voz sobre IP de modo que se reenvíe antes el tráfico IP que el tráfico de correo electrónico (SMTP) o FTP.
- Turno rotativo ponderado: garantiza que una sola aplicación no domine la capacidad de reenvío del dispositivo. El turno rotativo ponderado (WRR) reenvía colas enteras siguiendo un orden de turno rotativo. Todas las colas pueden participar en WRR, excepto las colas SP.
  Las colas SP reciben servicio antes que las colas WRR. Si el flujo de tráfico es muy bajo y las colas SP no ocupan toda la amplitud de banda asignada a un puerto, las colas WRR pueden compartir la amplitud de banda con las colas SP. De este modo se garantiza que la amplitud de banda restante se distribuya de acuerdo con el ratio ponderado. Si se selecciona WRR, se asignan las ponderaciones siguientes a las colas: 1, 2, 4, 8.

Definición de los parámetros globales de QoS

La página **QoS Parameters** (Parámetros de QoS) contiene enlaces a páginas que permiten establecer los parámetros globales de la calidad de servicio.

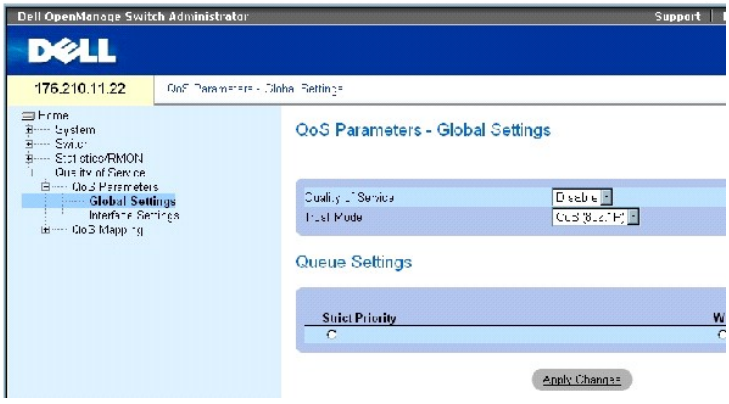
Configuración de los valores globales de QoS

La página **Global Settings** (Configuración global) contiene un campo para activar o desactivar QoS. También contiene un campo para seleccionar el modo de confianza. El modo de confianza se basa en campos predefinidos dentro del paquete para determinar la cola de salida.

Además, la página **Global Settings** (Configuración global) permite definir las colas como SP (prioridad estricta) o como WRR (turno rotativo ponderado).

Para abrir la página **Global Settings** (Configuración global), haga clic en Quality of Service (Calidad de servicio) → QoS Parameters (Parámetros de QoS) → Global Settings (Configuración global) en la vista de árbol.

Figura 9-1. Global Settings



La página **Global Settings** (Configuración global) contiene las secciones siguientes:

- QoS Settings (Configuración de QoS)
- Queue Settings (Configuración de la cola)

QoS Settings (Configuración de QoS)

Quality of Service (Calidad de servicio): activa o desactiva la administración del tráfico de red mediante la calidad de servicio.

Trust Mode (Modo de confianza): determina qué campos de paquete deben utilizarse para clasificar los paquetes que llegan al dispositivo. Cuando no se ha definido ninguna regla, el tráfico que contiene el campo de paquete CoS o DSCP predefinido se asigna según el modo de confianza seleccionado. El tráfico que no contiene un campo de paquete predefinido se asigna a la cola de mejor esfuerzo (q2). Los valores posibles del campo de modo de confianza son:

CoS (802.1p): la asignación de la cola de salida está determinada por la etiqueta de prioridad de VLAN (VPT) IEEE802.1p o por la VPT predeterminada asignada a un puerto. El dispositivo predeterminado es IEEE802.1p.

DSCP: la asignación de la cola de salida está determinada por el campo DSCP.

NOTA: la configuración del modo de confianza de la interfaz anula la configuración del modo de confianza global.

Queue Settings (Configuración de la cola)

Strict Priority (Prioridad estricta): cuando se selecciona, indica que las colas del sistema son colas SP.

WRR: cuando se selecciona, indica que las colas del sistema son colas WRR.

Activación de la calidad de servicio:

1. Abra la página **Global Settings** (Configuración global).
2. Seleccione **Enable** (Activar) en el campo **Quality of Service** (Calidad de servicio).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La clase de servicio se activa en el dispositivo.

Activación del modo de confianza:

1. Abra la página **Global Settings** (Configuración global).
2. Defina el campo **Trust Mode** (Modo de confianza).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El modo de confianza se activa en el dispositivo.

Activación del modo de confianza mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Global Settings** (Configuración global).

Tabla 9-3. Comandos de la CLI para la configuración de QoS

Comando de la CLI	Descripción

qos trust [**cos** | **dscp**]	Establece el sistema en el modo de confianza.
no qos trust	Restablece el modo de "no confianza".

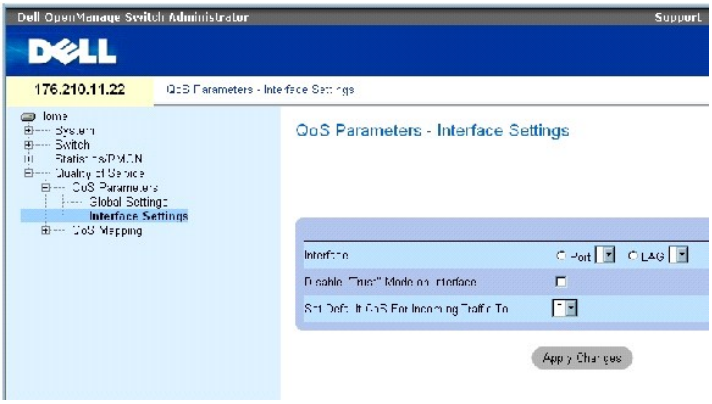
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# qos trust
dscp
```

Definición de la configuración de la interfaz de QoS

La página **Interface Settings**(Configuración de la interfaz) contiene campos para desactivar el modo de confianza y definir el valor de CoS predeterminado para los paquetes de entrada sin etiqueta. Para abrir la página **Interface Settings** (Configuración de la interfaz), haga clic en Quality of Service (Calidad de servicio) → QoS Parameters (Parámetros de QoS) → Interface Settings (Configuración de la interfaz) en la vista de árbol.

Figura 9-2. Interface Settings



La página **Interface Settings** (Configuración de la interfaz) contiene los campos siguientes:

Interface (Interfaz): puerto o LAG específicos que deben configurarse.

Disable "Trust" Mode on Interface (Desactivar modo de confianza en la interfaz): desactiva el modo de confianza en la interfaz especificada. Esta opción anula el modo de confianza configurado globalmente en el dispositivo.

Set Default CoS For Incoming Traffic To (Establecer CoS predeterminada para el tráfico entrante en): establece el valor de la etiqueta de CoS predeterminada para los paquetes sin etiqueta. Los valores de la etiqueta de CoS comprenden del 0 al 7. El valor predeterminado es 0.

Asignación de la configuración de QoS para una interfaz:

1. Abra la página **Interface Settings** (Configuración de la interfaz).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de CoS se asigna a la interfaz.

Visualización de la configuración de QoS/CoS:

1. Abra la página **Interface Settings** (Configuración de la interfaz).
2. Haga clic en **Show All** (Mostrar todo).

Se muestra la tabla de interfaces.

Asignación de las interfaces de QoS mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **Interface Settings** (Configuración de la interfaz).

Tabla 9-4. Comandos de la CLI para la interfaz de QoS

Comando de la CLI	Descripción
qos trust	Activa el modo de confianza.
no qos trust	Desactiva el modo de confianza en todos los puertos.

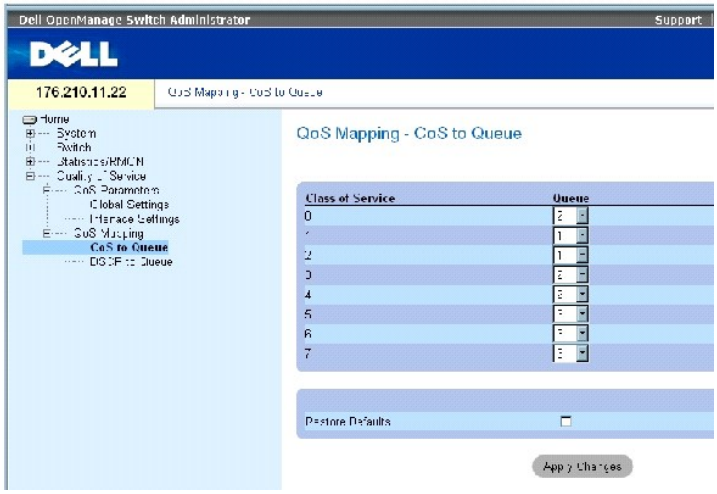
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# interface
ethernet 1/e15


console(config-if)# qos
trust
```

Asignación de valores de CoS a las colas

La página **CoS to Queue** (CoS a cola) contiene campos para clasificar los valores de CoS en colas de tráfico. Para abrir la página **CoS to Queue** (CoS a cola), haga clic en Quality of Service (Calidad de servicio) → **QoS Mapping** (Asignación de QoS) → CoS to Queue (CoS a Cola) en la vista de árbol.

Figura 9-3. CoS to Queue



La página **CoS to Queue** (CoS a cola) contiene los campos siguientes:

Class of Service (Clase de servicio): especifica los valores de las etiquetas de prioridad de CoS, siendo cero el valor más bajo y siete el más alto.

Queue (Cola): cola a la que se asigna la prioridad de CoS. Se admiten cuatro colas de prioridad de tráfico.

Restore Defaults (Restablecer valores predeterminados): restablece los valores predeterminados de fábrica del dispositivo para la asignación de valores de CoS a una cola de salida.

Asignación de un valor de CoS a una cola

1. Abra la página **CoS to Queue** (CoS a cola).
2. Seleccione una entrada de CoS.
3. Defina el número de cola en el campo **Queue** (Cola).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna el valor de CoS a una cola de salida y se actualiza el dispositivo.

Asignación de valores de CoS a colas mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **CoS to Queue** (CoS a cola).

Tabla 9-5. Comandos de la CLI para la configuración de CoS a cola

Comando de la CLI	Descripción
wrr-queue cos-map id-cola cos0.cos7	Asigna los valores de CoS asignados a las colas de salida.

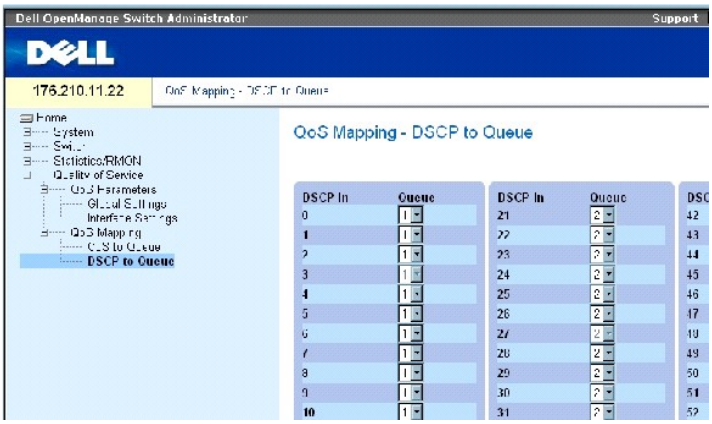
A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# wrr-queue
cos-map 4 7
```

Asignación de valores de DSCP a las colas

La página **DSCP to Queue** (DSCP a cola) contiene campos para definir la cola de salida para campos DSCP específicos. Para abrir la página **DSCP to Queue** (DSCP a cola), haga clic en Quality of Service (Calidad de servicio) → **QoS** Mapping (Asignación) → DSCP to Queue (DSCP a cola) en la vista de árbol.

Figura 9-4. DSCP to Queue



La página **DSCP to Queue** (DSCP a cola) contiene los campos siguientes:

DSCP In (Entrada DSCP): valores del campo DSCP dentro del paquete entrante.

Queue (Cola): cola a la que se asignan los paquetes con el valor de DSCP específico. Los valores comprenden del 1 al 4, siendo 1 el valor más bajo y 4 el más alto.

Asignación de un valor de DSCP y asignación de una cola de prioridad

1. Abra la página **DSCP to Queue** (DSCP a cola).
2. Seleccione un valor en la columna **DSCP In** (Entrada DSCP).
3. Defina el campo **Queue** (Cola).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se sobrescribe el DSCP y se asigna una cola de salida al valor.

Asignación de valores de DSCP mediante los comandos de la CLI

En la tabla siguiente se resumen los comandos de la CLI equivalentes para configurar los campos de la página **DSCP to Queue** (DSCP a cola).

Tabla 9-6. Comandos de la CLI para el valor de DSCP a cola

Comando de la CLI	Descripción
qos map dscp-queue lista-dscp **to** id-cola	Modifica la asignación de DSCP a cola.

A continuación se muestra un ejemplo de los comandos de la CLI:

```
console(config)# qos map
dscp-queue 33 40 41 to 1
```

Regresar a la página de contenido

Regresar a la página de contenido

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

NOTA: una NOTA proporciona información importante que le ayudará a utilizar mejor el ordenador.

AVISO: un AVISO indica la posibilidad de daños en el hardware o la pérdida de datos, e informa de cómo evitar el problema.

PRECAUCIÓN: un mensaje de PRECAUCIÓN indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Marzo de 2005

Regresar a la página de contenido

Regresar a la página de contenido

Información sobre interacciones de las funciones del dispositivo

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

La tabla siguiente contiene información sobre las interacciones de las funciones del dispositivo.

Función	Notas sobre la función
VLAN 802.1x no autenticada	Las VLAN 802.1x no autenticadas presentan restricciones con el uso de: • VLAN 802.1x invitada • VLAN privada • VLAN aislada • VLAN comunitaria • VLAN especial
Puerto de VLAN 802.1x no autenticada	Los puertos de VLAN 802.1x no autenticada presentan restricciones con el uso de: • Puertos aislados • Puertos comunitarios • Puertos promiscuos • Puertos de VLAN basada en MAC • Filtrado de entrada
ACL	Las ACL presentan restricciones con el uso de: • ACL basadas en MAC • VLAN especiales
Negociación automática	No hay restricciones ni limitaciones de interacción de las funciones.
Compatibilidad con la contrapresión	
Filtrado de multidifusión de puente	No hay restricciones ni limitaciones de interacción de las funciones.
Comprobaciones de cables	No hay restricciones ni limitaciones de interacción de las funciones.
Puertos comunitarios	Los puertos comunitarios presentan restricciones con el uso de puertos bloqueados.
VLAN comunitaria	Las VLAN comunitarias presentan restricciones con el uso de: • Direcciones MAC estáticas • ACL • GVRP • Inspección de IGMP • VLAN especiales
DNS	Sin restricciones ni limitaciones.
Modo dúplex	
Control de flujo	No hay restricciones ni limitaciones de interacción de las funciones.
GARP	No hay restricciones ni limitaciones de interacción de las funciones.
VLAN invitadas	Las VLAN invitadas no funcionan con: • VLAN privada • VLAN aislada • VLAN comunitaria • VLAN basadas en MAC • VLAN especiales
GVRP	No hay restricciones ni limitaciones de interacción de las funciones.
Inspección de IGMP	No hay restricciones ni limitaciones de interacción de las funciones.
Filtrado de	No hay restricciones ni limitaciones de

entrada	interacción de las funciones.
Puerto aislado	Los puertos aislados no funcionan con: • Puertos comunitarios • Puertos promiscuos • Bloqueo de puertos • GVRP • ACL basadas en MAC • Filtrado de entrada
VLAN aislada	Las VLAN aisladas no funcionan con: • VLAN comunitarias • Direcciones MAC estáticas • ACL • GVRP • Inspección de IGMP • VLAN especiales
Estadísticas de LAG	No hay restricciones ni limitaciones de interacción de las funciones.
Agregación de enlaces	No hay restricciones ni limitaciones de interacción de las funciones. Sin embargo, esta función presenta varias pautas para configurar la agregación de enlaces. Para consultar todas las pautas de esta función, consulte "Definición de los parámetros de LAG".
Puertos bloqueados	Los puertos bloqueados presentan restricciones con el uso de: • ACL basadas en MAC • Filtrado de entrada
Registro	No hay restricciones ni limitaciones de interacción de las funciones.
Compatibilidad con direcciones MAC	No hay restricciones ni limitaciones de interacción de las funciones.
Detección de MDI/MDIX	No hay restricciones ni limitaciones de interacción de las funciones.
Filtrado de multidifusión	No hay restricciones ni limitaciones de interacción de las funciones.
Varios hosts	El estándar 802.1X (varios hosts) no funciona con: • Puerto aislado • Puerto de VLAN basada en MAC
Árbol de extensión múltiple	El árbol de extensión múltiple no funciona con: • Puerto aislado • Filtrado de entrada
Autenticación basada en el puerto	La autenticación basada en el puerto presenta limitaciones o restricciones con el uso de: • 802.1 sencillo • Puerto aislado • Puertos bloqueados • VLAN basadas en MAC • Puertos de entrada
Duplicación de puertos	No hay restricciones ni limitaciones de interacción de las funciones. Sin embargo, esta función presenta varias pautas para configurar el control de tormentas. Para consultar todas las pautas de esta función, consulte "Definición de sesiones de duplicación de puertos".
Estadísticas de puerto	No hay restricciones ni limitaciones de interacción de las funciones.
VLAN privada	Las VLAN privadas no funcionan con: • Puertos aislados • Puertos comunitarios • GVRP • Inspección de IGMP • VLAN especial
VLAN privada	Las VLAN privadas presentan

	limitaciones o restricciones con el uso de: • VLAN aisladas • GVRP • Inspección de IGMP • VLAN especial
Puertos promiscuos	Los puertos promiscuos no funcionan con: • Puertos bloqueados • GVRP • Puertos de VLAN basada en MAC
Calidad de servicio	No hay restricciones ni limitaciones de interacción de las funciones.
Estadísticas de RMON	No hay restricciones ni limitaciones de interacción de las funciones.
Notificaciones de autenticación de SNMP	No hay restricciones ni limitaciones de interacción de las funciones.
Notificaciones de SNMP	No hay restricciones ni limitaciones de interacción de las funciones.
Autenticación de SNTP	No hay restricciones ni limitaciones de interacción de las funciones.
Árbol de extensión	No hay restricciones ni limitaciones de interacción de las funciones.
VLAN especial	No hay restricciones ni limitaciones de interacción de las funciones.
Dirección MAC estática	No hay restricciones ni limitaciones de interacción de las funciones.
Control de tormentas	No hay restricciones ni limitaciones de interacción de las funciones.
Registros del sistema	No hay restricciones ni limitaciones de interacción de las funciones.
Sincronización de la hora del sistema	No hay restricciones ni limitaciones de interacción de las funciones.
Puertos de VLAN no autenticada	Los puertos de VLAN no autenticada presentan restricciones con el uso de: • Puertos aislados • Puertos comunitarios • Puertos promiscuos • GVRP • Puertos de VLAN basada en MAC • Filtrado de entrada

---

Regresar a la página de contenido

Regresar a la página de contenido

Glosario

Sistemas Dell™ PowerConnect™ 34XX Guía del usuario

Este glosario contiene palabras técnicas clave que pueden ser de su interés.

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

A

Aleteo

El aleteo se produce cuando el estado de una interfaz cambia constantemente. Por ejemplo, un puerto STP que cambia continuamente entre los estados de escucha, obtención de datos y reenvío. Esta situación puede provocar la pérdida de tráfico.

Amplitud de banda

Cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. Para los módulos de conmutador digitales, la amplitud de banda se define en bits por segundo (bps) o en bytes por segundo.

Archivo de configuración en ejecución

Contiene todos los comandos del archivo de configuración de inicio y todos los comandos introducidos durante la sesión actual. Tras apagar o reiniciar el módulo de conmutador, se pierden todos los comandos almacenados en el archivo de configuración en ejecución.

Archivo de imagen

Las imágenes del sistema se guardan en dos sectores de la memoria Flash denominados imágenes (Image 1 e Image 2). La imagen activa almacena la copia activa, mientras que la otra imagen almacena una segunda copia.

Archivos de configuración de copia de seguridad

Contienen una copia de seguridad de la configuración del módulo de conmutador. El archivo de copia de seguridad cambia cuando se copia el archivo de configuración en ejecución o el archivo de configuración de inicio en el archivo de copia de seguridad.

ARP (Address Resolution Protocol) (protocolo de resolución de direcciones).

Protocolo que convierte direcciones IP en direcciones físicas.

ASIC

Application Specific Integrated Circuit (circuito integrado específico para la aplicación). Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

Cantidad de amplitud de banda asignada a una aplicación, un usuario o una interfaz determinados.

B

Baudio

Número de elementos de señalización que se transmite cada segundo.

BootP

Bootstrap Protocol (protocolo de inicio automático). Permite que una estación de trabajo detecte su dirección IP, una dirección IP de un servidor BootP en una red o un archivo de configuración cargado en el inicio de un módulo de conmutador.

BPDU

Bridge Protocol Data Unit (unidad de datos del protocolo de puente). Proporciona información sobre el puente en un formato de mensaje. Las BPDU se envían con la información del módulo de conmutador dentro de la configuración del árbol de extensión. Los paquetes de BPDU contienen información sobre puertos, direcciones, prioridades y costes de reenvío.

C

CDB

Configuration Data Base (base de datos de configuración). Archivo que contiene la información de configuración de un dispositivo.

CLI

Command Line Interface (interfaz de línea de comandos). Conjunto de comandos de línea utilizados para configurar el sistema. Para obtener más información sobre el uso de la CLI, consulte "Uso de la CLI".

Cliente DHCP

Dispositivo que utiliza DHCP para obtener parámetros de configuración, como por ejemplo una dirección de red.

Combinación de puertos

Agregación de enlaces. Optimiza el uso de los puertos enlazando un grupo de los mismos para que formen una única combinación de puertos (grupos agregados).

Comunidades

Especifica un grupo de usuarios que comparten los mismos derechos de acceso al sistema.

Configuración de inicio

Conserva la configuración exacta del módulo de conmutador cuando se enciende o se reinicia dicho módulo.

Conmutador

Filtra y reenvía paquetes entre segmentos de LAN. Los conmutadores admiten todos los tipos de protocolos de paquetes.

Consulta

Extrae información de una base de datos y presenta la información para su utilización.

Contrapresión

Mecanismo utilizado con el modo semidúplex que permite hacer que un puerto no reciba un mensaje.

Control de flujo

Permite que dispositivos de velocidad inferior se comuniquen con dispositivos de velocidad superior, es decir, que los dispositivos de velocidad superior dejen de enviar paquetes.

CoS

Class of Service (clase de servicio). La clase de servicio es el esquema de prioridad 802.1p. Proporciona un método para etiquetar paquetes con información sobre prioridad. Se añade un valor de CoS de entre 0 y 7 a la cabecera de nivel II de los paquetes, siendo cero la prioridad más baja y siete la más alta.

Superposición de transmisión de dos o más paquetes que están en colisión. Los datos transmitidos no pueden utilizarse y se reinicia la sesión.

CPU

Central Processing Unit (unidad central de proceso). Parte del ordenador que procesa la información. Las CPU se componen de una unidad de control y una ALU.

D

Difusión

Método para transmitir los paquetes a todos los puertos de una red.

Difusión única

Forma de enrutamiento que transmite un paquete a un usuario.

Dirección IP

Dirección de protocolo Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección de control de acceso a medios. Dirección específica de hardware que identifica cada nodo de red.

Dominio

Grupo de ordenadores y dispositivos de una red que están agrupados con reglas y procedimientos comunes.

Dominio de difusión

Conjuntos de dispositivos que reciben tramas de difusión originadas en uno de los dispositivos de un conjunto designado. Los enrutadores enlazan dominios de difusión, ya que no reenvían tramas de difusión.

DRAC/MC

Proporciona un único punto de control de los componentes del sistema de servidores modulares de Dell.

DSCP

DiffServe Code Point (punto de código de servicios diferenciados). Proporciona un método para etiquetar los paquetes IP con información sobre prioridad de QoS.

Duplicación de puertos

Supervisa y duplica el tráfico de red mediante el reenvío de copias de los paquetes entrantes y salientes de un puerto a un puerto supervisor.

Para obtener más información sobre la duplicación de puertos, consulte "Definición de sesiones de duplicación de puertos".

E

Enrutador

Dispositivo que se conecta a redes diferentes. Los enrutadores reenvían paquetes entre dos o más redes. Los enrutadores funcionan en el nivel 3.

Equilibrado de carga

Permite distribuir de forma equilibrada los datos o paquetes de proceso entre los recursos de red disponibles. Por ejemplo, el equilibrado de carga puede distribuir los paquetes entrantes uniformemente entre todos los servidores, o bien redirigirlos al siguiente servidor disponible.

Ethernet

Ethernet cumple con el estándar IEEE 802.3. Ethernet es el estándar de LAN implementado más conocido. Admite velocidades de transferencia de datos de 10, 100 o 1 000 Mbps.

Ethernet Gigabit

Ethernet Gigabit transmite a 1 000 Mbps y es compatible con los estándares Ethernet 10/100 Mbps existentes.

Etiqueta de inventario

Especifica la referencia del módulo de conmutador definida por el usuario.

EWS

Embedded Web Server (servidor Web integrado). Permite la administración de dispositivos mediante un explorador Web estándar. Los servidores Web integrados se utilizan como complemento o sustitución de una CLI o un NMS.

Excepción

Mensaje enviado por SNMP que indica que se ha producido un evento en el sistema.

F

FFT

Fast Forward Table (tabla de reenvío rápido).Proporciona información sobre rutas de reenvío. Si un paquete llega a un dispositivo con una ruta conocida, el paquete se reenvía a través de una ruta enumerada en la FFT. Si no existe una ruta conocida, la CPU reenvía el paquete y actualiza la FFT.

FIFO

First In First Out (primera entrada, primera salida). Proceso de cola según el que el primer paquete de la cola es el primer paquete en salir de la misma.

Fragmento

Paquetes Ethernet de menos de 576 bits.

G

GARP

General Attributes Registration Protocol (protocolo genérico de registro de atributos). Registra las estaciones cliente en un dominio de multidifusión.

GVRP

Protocolo de registro de VLAN de GARP. Registra las estaciones cliente en una VLAN.

H

HOL

Head of Line (cabecera de línea). Los paquetes se colocan en la cola. Los paquetes situados al principio de la cola se reenvían antes que los que están al final de la línea.

Host

Ordenador que actúa como fuente de información o servicios para otros ordenadores.

HTTP

HyperText Transport Protocol (protocolo de transferencia de hipertexto). Transmite documentos HTML entre servidores y clientes en Internet.

I

IC

Integrated Circuit (circuito integrado). Los circuitos integrados son pequeños dispositivos electrónicos compuestos de material semiconductor.

ICMP

Internet Control Message Protocol (protocolo de mensajes de control de Internet). Permite que la puerta de enlace o el host de destino se comuniquen con un host de origen, por ejemplo, para notificar un error de procesamiento.

IEEE

Institute of Electrical and Electronics Engineers. Organización de ingeniería que desarrolla estándares de comunicaciones y de redes.

IEEE 802.1d

Se utiliza en el protocolo de árbol de extensión (SPT) y admite puentes MAC para impedir la formación de bucles de red.

IEEE 802.1p

Prioriza el tráfico de red en el subnivel MAC/enlace de datos.

IEEE 802.1Q

Define la operación de los puentes de VLAN que permite definir, utilizar y administrar las VLAN dentro de infraestructuras de LAN con puentes.

IP

Internet Protocol (protocolo Internet).Especifica el formato de los paquetes y su método de direccionamiento. IP dirige los paquetes y los reenvía al puerto correcto.

L

LAG

Link Aggregated Group (grupo agregado de enlaces). Agrega puertos o VLAN a un único puerto virtual o VLAN.

Para obtener más información sobre los LAG, consulte "Configuración de pertenencia a LAG".

LAN

Local Area Network (red de área local). Red comprendida en una sola sala, edificio, campus u otra área geográfica limitada.

M

Máscara

Filtro que incluye o excluye determinados valores, por ejemplo, partes de una dirección IP.

Por ejemplo, si la unidad 2 se inserta en el primer minuto de un ciclo de diez minutos y la unidad 1 se inserta en el quinto minuto de dicho ciclo, se considera que ambas unidades tienen la misma antigüedad.

Máscara comodín

Especifica qué bits de una dirección IP se utilizan y cuáles se ignoran. Una máscara comodín de un módulo de conmutador con el valor 255.255.255.255 indica que ningún bit es importante. Un comodín con el valor 0.0.0.0 indica que todos los bits son importantes.

Por ejemplo, si la dirección IP de destino es 149.36.184.198 y la máscara comodín es 255.36.184.00, se utilizan los dos primeros bits de la dirección IP, mientras que los dos últimos se pasan por alto.

Máscara de subred

Sirve para enmascarar toda una dirección IP, o parte de ella, utilizada en una dirección de subred.

MD5

Message Digest 5. Se trata de un algoritmo que genera un hash de 128 bits. MD5 es una variante de MD4 que proporciona una mayor seguridad. MD5 verifica la integridad de la comunicación y autentica su origen.

MDI

Media Dependent Interface (interfaz dependiente del medio). Cable utilizado para estaciones finales.

MDIX

Media Dependent Interface with Crossover (interfaz dependiente del medio con cable cruzado). Cable utilizado para concentradores y conmutadores.

Mejor esfuerzo

El tráfico se asigna a la cola de prioridad más baja, y la entrega del paquete no está garantizada.

MIB

Management Information Base (base de datos de información de administración). Las MIB contienen información que describe aspectos específicos de componentes de red.

Modo de acceso

Especifica el método mediante el que se otorga el acceso de usuario al sistema.

Modo dúplex

Permite transmitir y recibir datos simultáneamente. Existen dos tipos de modo dúplex:

- **Modo dúplex completo**: permite la comunicación bisíncrona, por ejemplo, un teléfono. Dos partes pueden transmitir información a la vez.
- **Modo semidúplex**: permite la comunicación asíncrona, por ejemplo, un walkie-talkie. Sólo una parte puede transmitir información a la vez.

Multidifusión

Transmite copias de un mismo paquete a varios puertos.

N

Negociación automática

Permite establecer puertos Ethernet 10/100 Mbps o 10/100/1 000 Mbps para las funciones siguientes:

- Modo dúplex/semidúplex
- Control de flujo
- Velocidad

Nivel 2

Nivel de enlace de datos o nivel MAC. Contiene la dirección física de una estación cliente o servidor. El procesamiento del nivel 2 es más rápido que el del nivel 3, ya que hay menos información por procesar.

Nivel 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel 4 se analizan, y las decisiones de reenvío se basan en sus aplicaciones.

Nivel MAC

Subnivel del nivel de control de enlace de datos (DTL).

NMS

Network Management System (sistema de administración de red). Interfaz que proporciona un método para administrar un sistema.

Nodo

Punto final de una conexión de red o punto de unión común de varias líneas de red. Existen varios tipos de nodo:

- Procesadores
- Controladoras
- Estaciones de trabajo

O

Obtención de direcciones MAC

La obtención de direcciones MAC caracteriza un puente de obtención, en el que se registra la dirección MAC de origen del paquete. Los paquetes destinados a esta dirección se reenvían sólo a la interfaz de puente en la que se encuentra dicha dirección. Los paquetes dirigidos a direcciones desconocidas se reenvían a todas las interfaces de puente. La obtención de direcciones MAC minimiza el tráfico en las LAN conectadas.

OID

Object Identifier (identificación de objeto). ID utilizada por SNMP para identificar objetos administrados. En el paradigma de administración de red del administrador/agente SNMP, cada objeto administrado debe tener una OID que lo identifique.

P

Paquetes

Bloques de información para la transmisión en sistemas conmutados de paquetes.

PDU

Protocol Data Unit (unidad de datos del protocolo). Unidad de datos especificada en un protocolo de nivel que consta de información de control del protocolo y datos de usuario de nivel.

Perfiles de acceso

Permite a los administradores de red definir perfiles y reglas para el acceso al módulo de conmutador. El acceso a las funciones de administración puede limitarse a grupos de usuarios, que se definen según los criterios siguientes:

- Interfaces de entrada
- Dirección IP de origen y subredes IP de origen

Perfiles de autenticación

Conjuntos de reglas que permiten el inicio de sesión y la autenticación de los usuarios y las aplicaciones.

PING

Packet Internet Groper (sonda de paquetes de Internet). Comprueba si una dirección IP concreta está disponible. Se envía un paquete a otra dirección IP y se espera respuesta.

Plano posterior

BUS principal que transporta información en el módulo de conmutador.

Protocolo

Conjunto de reglas que rigen el modo en que los dispositivos intercambian información a través de las redes.

Protocolo de árbol de extensión

Impide la formación de bucles en el tráfico de la red. El protocolo de árbol de extensión (STP) permite obtener una topografía de árbol de cualquier combinación de puentes. STP proporciona una ruta entre las estaciones finales de una red para eliminar los bucles.

Puente

Dispositivo que conecta dos redes. Los puentes son específicos del hardware, pero independientes del protocolo. Los puentes operan en los niveles 1 y 2.

Puerto

Los puertos físicos proporcionan componentes de conexión que permiten a los microprocesadores comunicarse con equipos periféricos.

Puerto de entrada

Puertos en los que se recibe el tráfico de red.

Puertos de salida

Puertos desde los que se transmite el tráfico de red.

Q

QoS

Quality of Service (calidad de servicio). Permite a los administradores de red decidir cómo se reenvía el trafico de red y qué tráfico de red se reenvía de acuerdo con las prioridades, los tipos de aplicación y las direcciones de origen y de destino.

R

RADIUS

Remote Authentication Dial-In User Service (servicio de usuario de acceso telefónico de autenticación remota). Método que permite autenticar a los usuarios del sistema y hacer un seguimiento de los tiempos de conexión.

RMON

Remote Monitoring (supervisión remota). Proporciona información de la red que debe recopilarse desde una única estación de trabajo.

RSTP

Rapid Spanning Tree Protocol (protocolo de árbol de extensión rápida). Detecta y utiliza topologías de red que permiten una convergencia más rápida del árbol de extensión, sin crear bucles de reenvío.

S

Segmentación

Divide las LAN en segmentos de LAN independientes para la formación de puentes. La segmentación elimina las limitaciones de amplitud de banda de la LAN.

Servidor

Ordenador central que porporciona servicios a otros ordenadores de una red. Estos servicios incluyen el almacenamiento de archivos y el acceso a aplicaciones.

Sistema final

Dispositivo de usuario final en una red.

SNMP

Simple Network Management Protocol (protocolo simple de administración de red). Administra redes LAN. El software basado en SNMP se comunica con dispositivos de red con agentes SNMP incorporados. Los agentes SNMP recopilan información sobre la actividad de la red y sobre el estado del dispositivo y, a continuación, la envían de nuevo a una estación de trabajo.

SNTP

Simple Network Time Protocol (protocolo simple de hora de red). SNTP asegura una sincronización de la hora del reloj del conmutador de red con una precisión de milisegundos.

SoC

System on a Chip (sistema en un chip). ASIC que contiene un sistema completo. Por ejemplo, una aplicación SoC de telecomunicaciones puede incluir un microprocesador, un procesador de señales digitales, una RAM y una ROM.

SSH

Secure Shell. Permite iniciar una sesión en otro ordenador a través de una red, ejecutar comandos en un equipo remoto y mover archivos de un equipo a otro. Secure Shell proporciona potentes métodos de autenticación y comunicación segura en canales inseguros.

Subred

Las subredes son partes de una red que comparten un componente de dirección común. En las redes TCP/IP, los dispositivos que tienen un prefijo en común forman parte de la misma subred. Por ejemplo, todos los dispositivos con el prefijo 157.100.100.100 forman parte de la misma subred.

T

Telnet

Protocolo de emulación de terminal. Permite a los usuarios del sistema iniciar sesión y utilizar recursos en redes remotas.

TCP/IP

Transmissions Control Protocol/Internet Protocol (protocolo de control de transmisión/protocolo Internet.). Permite que dos hosts se comuniquen e intercambien flujos de datos. TCP garantiza que la entrega del paquete y, además, que los paquetes se transmitan y se reciban en el orden en el que se han enviado.

TFTP

Trivial File Transfer Protocol (protocolo trivial de transferencia de archivos). Utiliza el protocolo de datos de usuario (UDP) sin funciones de seguridad para transferir archivos.

Tormenta de difusión

Cantidad excesiva de mensajes de difusión transmitidos simultáneamente a través de una red por un mismo puerto. Las respuestas a mensajes reenviados se acumulan en la red, lo que provoca una sobrecarga en los recursos de ésta o que se agote el tiempo de espera.

Para obtener más información sobre tormentas de difusión, consulte "Definición de los parámetros de LAG".

Trama

Paquetes que contienen la información de cabecera y de cola necesaria para el medio físico.

Tramas gigantes

Permiten transportar la misma cantidad de datos en un número menor de tramas. Las tramas gigantes aprovechan mejor la amplitud de banda y reducen el tiempo de procesamiento y el número de interrupciones.

U

UDP

User Data Protocol (protocolo de datos de usuario). Transmite paquetes pero no garantiza su entrega.

V

Velocidad del puerto

Indica la velocidad del puerto. Esta velocidad puede ser:

- Ethernet a 10 Mbps
- Fast Ethernet a 100 Mbps
- Ethernet Gigabit a 1 000 Mbps

Versión de inicio

La versión de inicio.

VLAN

Virtual Local Area Network (red de área local virtual). Subgrupos lógicos con una red de área local (LAN) creados a través de software en lugar de mediante la definición de una solución de hardware.

VLAN agregada

Agrupa varias VLAN en una única VLAN agregada. La agregación de varias VLAN permite a los enrutadores responder a las peticiones ARP de nodos ubicados en distintas VLAN secundarias pertenecientes a una misma VLAN principal. Los enrutadores responden con su dirección MAC.

W

WAN

Wide Area Network (red de área amplia). Red que cubre un área geográfica grande.

Regresar a la página de contenido