Sistemas Dell™ PowerConnect™ 6024/6024F

Notas, avisos y precauciones

NOTA: Una NOTA proporciona información importante que le ayuda a utilizar su equipo de la mejor manera posible.

AVISO: Un AVISO indica la posibilidad de daños en el hardware o pérdida de datos, y le explica cómo evitar el problema.

PRECAUCIÓN: Una PRECAUCIÓN indica un posible daño material, lesión corporal o muerte.

Enero 2005

Regresar a la página de contenido

Información sobre los cables, los puertos y la asignación de patas

Sistemas Dell™ PowerConnect™ 6024/6024F

En esta sección se describen las interfaces físicas del conmutador y también se proporciona información sobre las conexiones de los cables.

Las estaciones se conectan a los puertos del conmutador a través de los puertos de las interfaces físicas ubicadas en el panel anterior. Para cada una de las estaciones se establece la modalidad (dúplex medio/completo, automático) adecuada.

Conexiones de las patas para la interfaz Ethernet 10/100/1000

El puerto de conmutación puede conectarse a estaciones configuradas en modalidad Ethernet RJ-45 estándar mediante cables de red directos. Los dispositivos de transmisión conectados entre sí utilizan cables de red cruzados.

En la Ilustración 3-1 aparecen las patas del conector RJ-45 y en la Tabla 3-1 se indican las asignaciones de patas del mismo.

Ilustración 3-1. Conector RJ-45

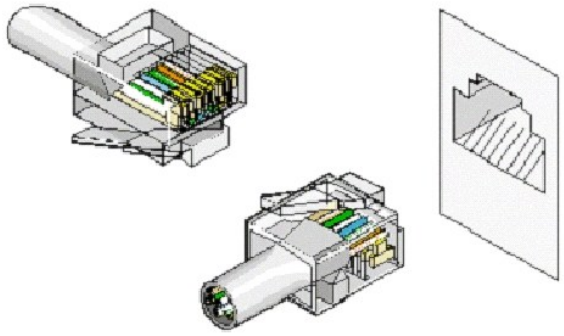


Tabla 3-1. Conexiones de patas del conector RJ-45 para 10/100/1000 Base T

Pata	Utilizar
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Conexiones de las patas para las interfaces SFP

En la Ilustración 3-2 aparece un conector SFP y en la Tabla 3-2 se muestran las asignaciones de patas de un conector SFP opcional.

Ilustración 3-2. Conector SFP

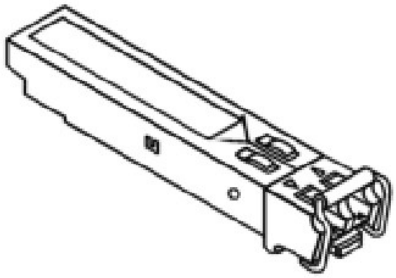


Tabla 3-2. Conexiones de patas de SFP

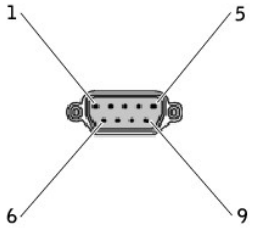
Pata	Utilizar
1	Toma de tierra del transmisor (común con la toma de tierra del receptor).
2	Anomalía del transmisor.
3	Desactivación del transmisor; salida de láser desactivada por sobretensión o si se abre.
4	Definición de módulo 2; línea de datos para el ID serie.
5	Definición de módulo 1; línea de reloj para el ID serie.
6	Definición de módulo 0; toma de tierra incorporada en el módulo.
7	Selección de velocidad; no se requiere ninguna conexión.
8	Pérdida de indicación de señal; el valor lógico 0 indica funcionamiento normal.
9	Toma de tierra del receptor (común con la toma de tierra del transmisor).
10	Toma de tierra del receptor (común con la toma de tierra del transmisor).
11	Toma de tierra del receptor (común con la toma de tierra del transmisor).
12	Salida de datos invertida del receptor; CA acoplada.
13	Salida de datos no invertida del receptor; CA acoplada.
14	Toma de tierra del receptor (común con la toma de tierra del transmisor).
15	Fuente de alimentación del receptor.
16	Fuente de alimentación del transmisor.
17	Toma de tierra del transmisor (común con la toma de tierra del receptor).
18	Entrada de datos no invertida del transmisor.
19	Entrada de datos invertida del transmisor.
20	Toma de tierra del transmisor (común con la toma de tierra del receptor).

Conexión del cable serie

También puede utilizar cables serie (de módem nulo) para conectar el conmutador a un terminal y poder realizar la instalación y configuración iniciales (también puede utilizar un PC en el que se ejecute un software de emulación de terminal). El cable serie del conmutador es un cable de red cruzado con dos conectores DB-9 hembra (véase la Ilustración 3-3).

En la Ilustración 3-3 se muestra el cable serie y en la Tabla 3-3 se muestran las asignaciones de patas del conector serie.

Ilustración 3-3. Conector serie



En la Tabla 3-3 se indican las asignaciones de patas del cable serie.

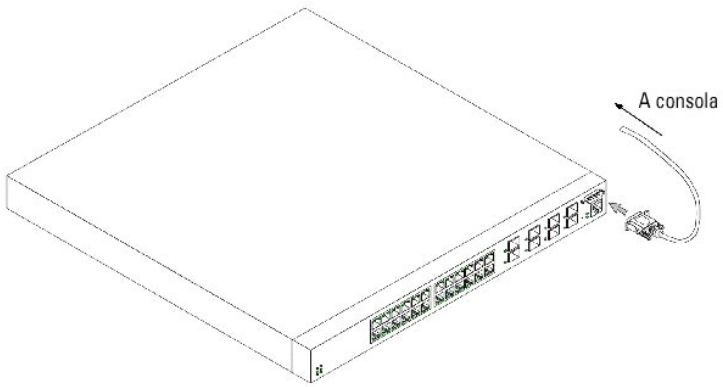
Tabla 3-3. Asignación de patas del conector serie

Señal	Pata	Señal del puerto de la consola de gestión
Sin utilizar	1	Sin utilizar
TXD	2	TXD
RXD	3	RXD
Sin utilizar	4	RXD
GND	5	GND
Sin utilizar	6	Sin utilizar
CTS	7	CTS
RTS	8	RTS
Sin utilizar	9	Sin utilizar

Conexión del conmutador a un terminal

1. Conecte el cable (serie) de módem nulo a la conexión RS-232 DTE ASCII (consola) del terminal.
2. Conecte el cable de la interfaz a la conexión del puerto serie del conmutador (consulte la Ilustración 3-4).

Ilustración 3-4. Conexión serie del conmutador



Conexión de alimentación de CA

1. Mediante un cable de alimentación estándar de 1,5 m (5 pies) con toma de tierra de seguridad, conecte el cable de CA al zócalo principal de CA ubicado en el panel posterior (consulte la Ilustración 3-5).
2. Conecte el cable de alimentación a un enchufe de corriente alterna.

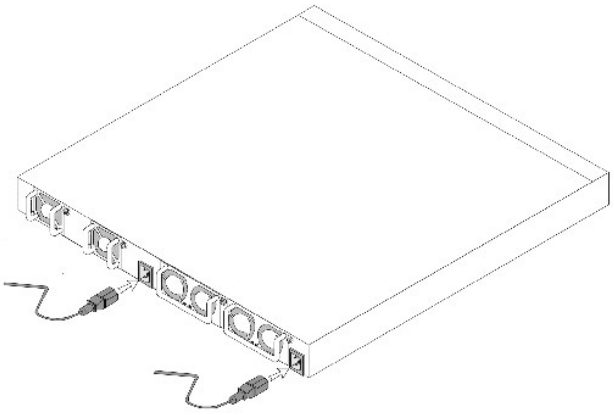
NOTA: Se recomienda que conecte la segunda fuente de alimentación a una toma de corriente distinta.

3. Confirme que el dispositivo se ha conectado y funciona correctamente; para ello, examine los LED de los paneles anterior y posterior.

   Para obtener una explicación completa sobre los LED, consulte el apartado "Descripción del hardware".

4. Repita el mismo proceso con la segunda fuente de alimentación.

Ilustración 3-5. Conexión de la alimentación de CA al conmutador



Regresar a la página de contenido

Regresar a la página de contenido

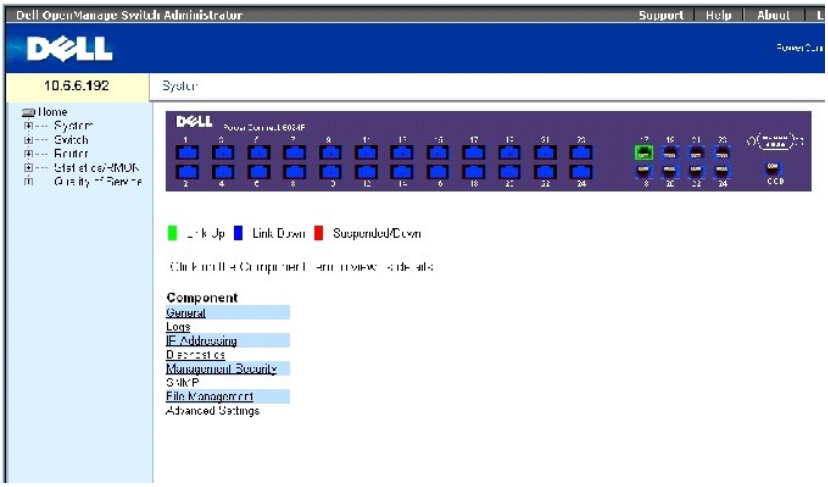
Configuración de la información del sistema

Sistemas Dell PowerConnect 6024/6024F

Apertura de la página del sistema

Para abrir la página **System** (Sistema), haga clic en **System** (Sistema) en la *vista de árbol* (consulte la Ilustración 6-1).

Ilustración 6-1. System (Sistema)



Definición de la información general del dispositivo

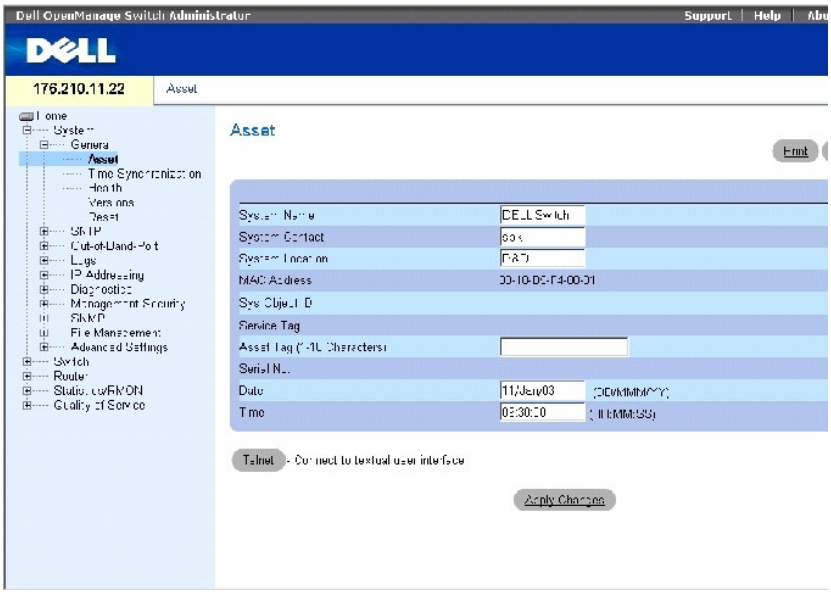
La página **General** contiene enlaces a las páginas que permiten a los administradores de red configurar los parámetros del dispositivo.

Configuración de la información del dispositivo

La página **Asset** (Propiedad) contiene parámetros para configurar y ver información general del dispositivo, incluidos el nombre, la ubicación y el contacto del sistema, la dirección MAC del sistema tanto para el conmutador como para el puerto de gestión fuera de banda, el ID de objetos del sistema, la fecha, la hora y el tiempo límite del sistema.

Para visualizar la página **Asset** (Propiedad), haga clic en **System**→ **General**→ **Asset** (Sistema→ General→ Propiedad) en la *vista de árbol.*

Ilustración 6-2. Asset (Propiedad)



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

System Name (Nombre del sistema): el nombre del dispositivo asignado por el usuario.

System Contact (Contacto del sistema): el nombre de la persona de contacto.

System Location (Ubicación del sistema): la ubicación del sistema que se ejecuta actualmente.

MAC Address (Dirección MAC): la dirección MAC del conmutador.

Sys Object ID (ID de objeto del sistema): el OID de la MIB.

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

Asset Tag (Etiqueta de propiedad): la referencia del dispositivo definida por el usuario. Los valores posibles del parámetro son 1 a 16.

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

Date (DD/MMM/YY) (Fecha [DD/MMM/AA]): la fecha actual del sistema. El formato es día, mes y año. Por ejemplo, 11/01/02 se corresponde al 11 de enero de 2002.

Time (HH/MM/SS) (Hora [HH/MM/SS]): la hora actual del sistema. El formato es hora, minuto y segundo. Por ejemplo, 20:12:03 se corresponde a las 8:12:03 PM.

Definición de la información del sistema

1. Abra la página **Asset** (Propiedad).
2. Defina los campos siguientes: **System Name** (Nombre del sistema), **System Contact** (Contacto del sistema), **System Location** (Ubicación del sistema) y **Asset Tag** (Etiqueta de propiedad).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del sistema se aplican y el dispositivo se actualiza.

Inicio de una sesión Telnet

1. Abra la página **Asset** (Propiedad).

NOTA: Los parámetros de la sesión Telnet adecuados se establecen antes de iniciar una sesión. Consulte el apartado Configuración de una contraseña Telnet inicial para obtener información.

2. Haga clic en **Telnet**.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver los campos que se muestran en la página **Asset** (Propiedad).

Tabla 6-1. Comandos de la CLI para la propiedad

Comando de la CLI	Descripción
`hostname name`	Especifica o modifica el nombre del sistema principal del dispositivo.
`snmp-server contact` `text`	Configura un contacto del sistema.
`snmp-server location` `text`	Especifica información sobre la ubicación del dispositivo.
`show clock`	Muestra la hora y fecha del reloj del sistema.
`asset-tag` `tag`	Especifica la etiqueta de propiedad del dispositivo.
`show system-id`	Muestra la información del ID del sistema, incluida la etiqueta de servicio, la etiqueta de propiedad y el número de serie.
`show system`	Muestra información del sistema.

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

```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_Yorks

Console (config)# exit
```

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


Console# show clock


15:29:03 Jun 17 2002
```

Definición de la configuración de la hora del sistema

La página **Time Synchronization** (Sincronización de la hora) contiene campos para sincronizar la hora del sistema con el reloj de hardware local y con un reloj de SNTP externo.

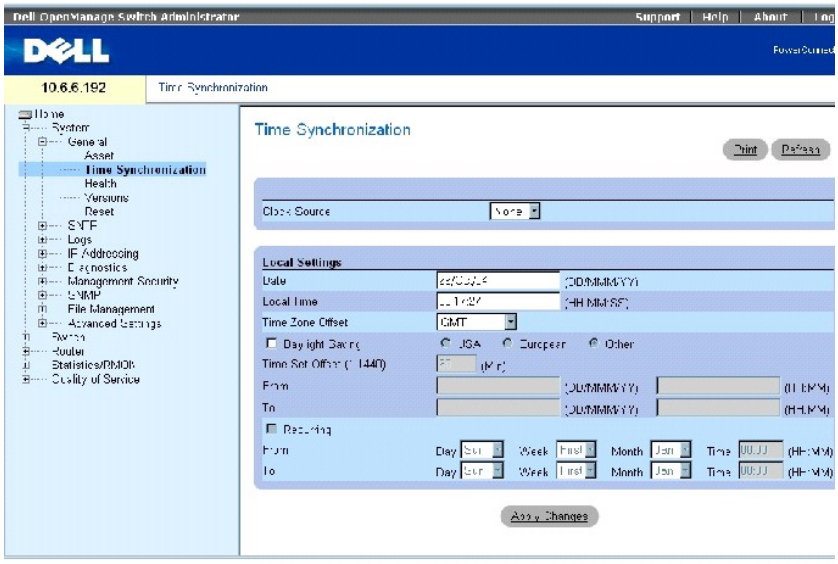
El reloj del sistema se sincroniza con un reloj de SNTP externo y si dicho reloj falla, el reloj del sistema cambia automáticamente al reloj de hardware local.

El reloj del sistema se puede configurar de modo que el cambio al horario de verano (DST) sea automático.

Para obtener más información sobre el SNTP, consulte el apartado **Configuración de los valores de SNTP**.

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

Ilustración 6-3. Time Synchronization (Sincronización de la hora)



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

Clock Source (Código fuente del reloj): el código fuente de la hora utilizado para mantener el reloj del sistema. Los valores de campo posibles son:

None (Ninguno): especifica que la hora del sistema está sincronizada con el reloj de harware local.

SNTP: especifica que la hora del sistema está sincronizada con un reloj del servidor SNTP. Para obtener más información, consulte el apartado **Configuración de los valores de SNTP** .

Date (Fecha): define la fecha del sistema. El formato del campo es DD:MMM:AA.

Local Time (Hora local): define la hora del sistema. El formato del campo es HH:MM:SS.

Time Zone Offset (Diferencia de zona horaria): define la diferencia, en horas, entre la hora del meridiano de Greenwich (GMT) y la hora local.

El reloj del sistema se puede programar para que pase automáticamente al horario de verano (DST) en función de un período de tiempo definido en un año específico o un período de tiempo recurrente. Utilice los parámetros del área Daylight Savings para definir un período de un año específico y utilice los parámetros del área Recurring para definir un período de tiempo recurrente.

Daylight Savings (Horario de verano): haga clic en esta casilla de verificación para activar DST en el dispositivo en función de la ubicación geográfica de éste. Los valores de campo posibles son:

USA (EE.UU): el reloj del dispositivo cambia a DST a las 2:00 h del primer domingo de abril y vuelve a la hora estándar a las 2:00 h del último domingo de octubre.

European (Europeo): el reloj del dispositivo cambia a DST a la 1:00 h del último domingo de marzo y vuelve a la hora estándar a la 1:00 h del último domingo de octubre. Esta opción se aplica a los miembros de la UE y a otros países europeos que utilizan el estándar de la UE.

Other (Otro): el reloj del dispositivo cambia a DST según un intervalo de tiempo definido por el usuario.

Time Set Offset (1-1440) (Compensación de hora establecida [1-1440]): en el caso de países que no sean los EE.UU. o no estén en Europa, la diferencia entre hora estándar y DST se puede establecer en minutos. El valor predeterminado es 60 minutos.

From/To (Desde/Hasta): define la fecha y la hora a la que empieza/finaliza DST en países fuera de los EE.UU. y Europa. El formato de la fecha es DD/MMM/AA y el formato de la hora es HH:MM.

Recurring (Recurrente): haga clic en esta casilla de verificación para activar DST en el dispositivo en función de intervalo de tiempo recurrente. Los valores de campo posibles son:

From/To (Desde/Hasta): define el día, la semana y el mes en que empieza y acaba el DST. El formato de la hora es HH:MM.

Selección del código fuente del reloj

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

El código fuente del reloj se selecciona y el dispositivo se actualiza.

Definición de la configuración del reloj local

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

La configuración del reloj local se aplica y el dispositivo se actualiza.

Definición del horario de verano

1. Abra la página **Time Synchronization** (Sincronización de la hora).
2. Defina los campos de las áreas **Daylight Saving** (Horario de verano) y **Recurring** (Recurrente).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración del horario de verano se aplica y el dispositivo se actualiza.

Definición de la configuración del reloj mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los campos que se muestran en la página **Time Synchronization** (Sincronización de la hora).

Tabla 6-2. Comandos de la CLI para la sincronización de la hora

Comando de la CLI	Descripción
`clock source {sntp}`	Sincroniza la hora del sistema con un reloj del servidor SNTP.
`no clock source`	Sincroniza la hora del sistema con el reloj del dispositivo.
`clock timezone` *`diferencia horaria`* `[minutes` *`diferencia de minutos`*`] [zone` *`sigla`*`]`	Establece la zona horaria para mostrarla en pantalla.
`no clock timezone`	Establece la hora en UTC (Hora universal coordinada).
`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 (DST) según los estándares estadounidenses o europeos o según un intervalo de tiempo recurrente definido por el usuario.
`clock summer-time date fecha mes año hh:mm fecha mes año hh:mm [offset` *`diferencia`*`] [zone` *`sigla`*`]`	Configura el sistema para que cambie automáticamente a DST durante un período de tiempo definido por el usuario.
`no clock summer-time`	Configura el sistema para que no cambie a DST.
`show clock`	Muestra la hora y fecha del reloj del sistema.
`show clock [detail]`	Muestra la configuración del horario de verano (DST), la zona horaria, la fecha y la hora de los relojes del sistema.

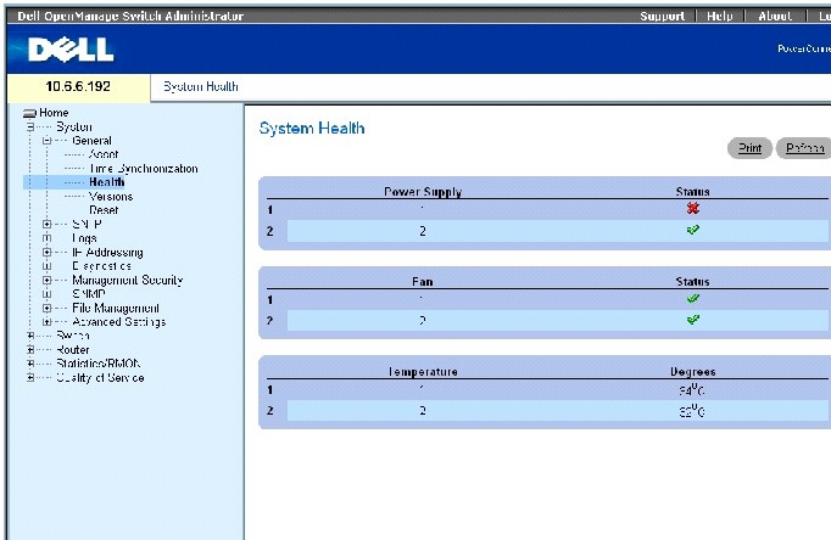
A continuación se muestra un ejemplo de los comandos de la CLI:

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

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

Configuración de la información de estado del sistema

La página **System Health** (Estado del sistema) muestra información sobre el dispositivo físico, incluida información sobre la potencia del conmutador y las fuentes de ventilación. Para visualizar la página **System Health** (Estado del sistema), haga clic en **System**→ **General**→ **Health** (Sistema→ General→ Estado) en la *vista de árbol.*

Ilustración 6-4. System Health (Estado del sistema)



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

Power Supply (Fuente de alimentación): estado de la fuente de alimentación.

: la fuente de alimentación funciona normalmente.

: la fuente de alimentación no funciona normalmente.

Not Present (No presente): actualmente no hay ninguna fuente de alimentación.

Fan (Ventilador): indica el estado del ventilador. El conmutador PowerConnect 6024/6024F tiene dos ventiladores.

: el ventilador funciona normalmente.

: el ventilador no funciona normalmente.

Not Present (No presente): actualmente no hay ningún ventilador.

Temperature (Temperatura): la temperatura a la que normalmente se ejecuta el dispositivo.

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

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

Tabla 6-3. Comandos de la CLI del estado del sistema

Comando de la CLI	Descripción
show system	Muestra información del sistema.

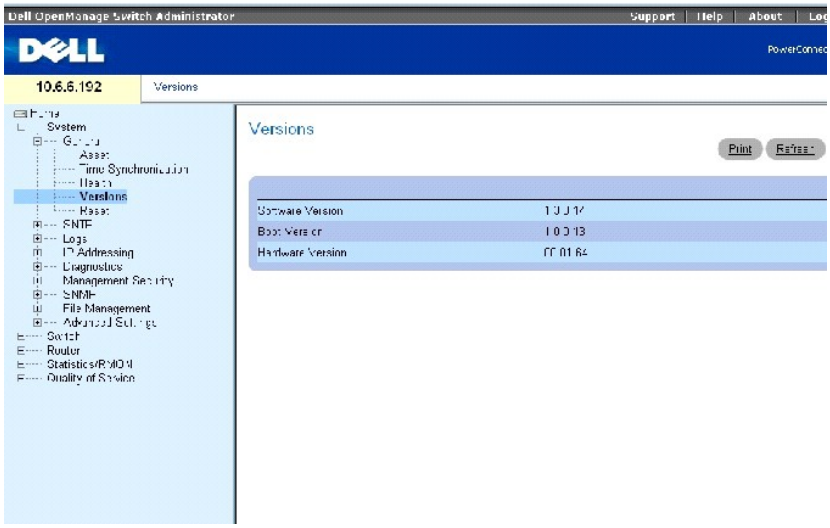
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console# show system

System Description:                 Ethernet Routing Switch
System Up Time (days,hour:min:sec): 0,00:32:04
System Contact:
System Name:
System Location:
System MAC Address:                 00:0d:56:2f:45:30
OOB MAC Address:                    00:00:00:00:00:18
System Object ID:                   1.3.6.1.4.1.674.10895.3000
Type:                               PowerConnect 6024

Main Power Supply Status:           OK
Redundant Power Supply Status:      OK
Fan 1 Status:                       OK
Fan 2 Status:                       OK
Temperature (Celsius):              45
Temperature Sensor Status:          OK
```

Información sobre la versión

La página **Versions** (Versiones) contiene información sobre las versiones de software y hardware que se ejecutan actualmente. Para visualizar la página **Versions** (Versiones), haga clic en **System**→ **General**→ **Versions** (Sistema→ General→ Versiones) en la vista de árbol (consulte la Ilustración 6-5).

Ilustración 6-5. Versions (Versiones)



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

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

Boot Version (Versión de arranque): la versión actual de arranque que se ejecuta en el dispositivo.

Hardware Version (Versión de hardware): la versión actual de hardware que se utiliza en el dispositivo.

Visualización de las versiones del dispositivo mediante la CLI

En la siguiente tabla se muestra un resumen del comando de la CLI equivalente para ver los campos que aparecen en la página **Versions** (Versiones).

Tabla 6-4. Comando de la CLI para las versiones

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

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

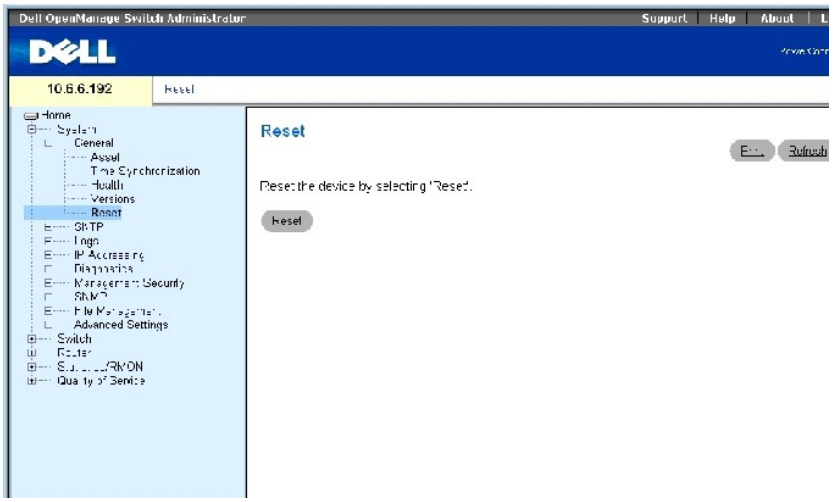
```
Console# show version

SW version 1.0.0.67 (date 26-Jun-2003 time 18:15:42)
```

```
Boot version 1.0.0.11 (date 12-Jun-2003 time 15:55:01)


HW version 00.01.64
```

Restablecimiento del dispositivo

Puede utilizar la página **Reset** (Restablecer) para restablecer el dispositivo. Para abrir la página **Reset** (Restablecer), haga clic en **System**→ **General**→ **Reset** (Sistema→ General→ Restablecer) en la vista de árbol (consulte la Ilustración 6-6).

Ilustración 6-6. Reset (Restablecimiento)



NOTA: Guarde todos los cambios realizados en el archivo **Running Configuration** (Configuración en ejecución) antes de restablecer el dispositivo para evitar que se pierda la configuración actual del dispositivo. Para obtener información sobre cómo guardar archivos de configuración, consulte el apartado Gestión de archivos .

Restablecimiento del dispositivo

1. Abra la página **Reset** (Restablecer).
2. Haga clic en **Reset** (Restablecer).
3. Cuando aparezca el mensaje de confirmación, haga clic en **OK** (Aceptar).

Se restablecerá el dispositivo. Después de restablecer el dispositivo, escriba un nombre de usuario y una contraseña.

Restablecimiento del dispositivo mediante la CLI

1. Si todavía no se encuentra en el modo de ejecución de usuario privilegiado de la CLI, escriba `enable`.
2. Si desea guardar todos los cambios realizados en el archivo de configuración en ejecución del dispositivo, escriba `copy running-config startup-config`.
3. Escriba `reload`.
4. Pulse y cuando le pregunten si desea continuar.

Configuración de los valores de SNTP

El dispositivo es compatible con SNTP (protocolo de hora de la red simple). El protocolo SNTP garantiza una sincronización precisa del tiempo del reloj del dispositivo en red en milisegundos. La sincronización del tiempo la realiza un servidor SNTP en red. El dispositivo funciona sólo como cliente SNTP, y no puede prestar servicio horario a otros sistemas.

Los recursos de tiempo se establecen por niveles. Estos niveles definen la exactitud del reloj de referencia. Cuanto más alto sea el nivel (donde cero es el más alto), más exacto será el reloj. El dispositivo recibe la hora a partir del nivel 1.

A continuación se muestra un ejemplo de los niveles:

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

La información que se recibe de los servidores SNTP se evalúa en función del nivel de tiempo y del tipo de servidor.

Las definiciones de tiempo de SNTP se evalúan y determinan en función de los siguientes niveles de tiempo:

- **T1**: hora en la que el cliente envió la solicitud original.
- **T2**: hora en la que el servidor recibió la solicitud original.
- **T3**: hora en la que el servidor envió una respuesta.
- **T4**: hora en la que el cliente recibió la respuesta del servidor.

El dispositivo puede hacer un sondeo de los siguientes tipos de servidores en cuanto al tiempo de 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 se han configurado en el dispositivo son los únicos que se sondean para obtener información de sincronización. Los niveles de tiempo de T1 a T4 se utilizan para determinar la hora del servidor. Éste es el método preferido para sincronizar la hora del dispositivo porque es el método más seguro. Si se selecciona este método, sólo se acepta información de SNTP de los servidores SNTP definidos en el dispositivo mediante la página **SNTP Servers** (Servidores SNTP).

El sondeo para obtener información de cualquier difusión se utiliza cuando la dirección IP del servidor no se conoce. Si se selecciona este método, todos los servidores SNTP de la red podrán enviar información de sincronización. El dispositivo se sincroniza cuando solicita de manera proactiva información de sincronización. La mejor respuesta (nivel más bajo) de los primeros 3 servidores SNTP para responder a una solicitud de información de sincronización se utiliza para establecer el valor de la hora. Los niveles de tiempo T3 y T4 se utilizan para determinar la hora del servidor.

Es preferible utilizar el sondeo de cualquier difusión (anycast) para obtener información horaria para sincronizar la hora del dispositivo que utilizar el sondeo de difusión (broadcast) para obtener información horaria. Sin embargo, este método es menos seguro que el sondeo de difusión única (unicast) porque los paquetes de SNTP se aceptan desde servidores SNTP que no están configurados en el dispositivo.

La información de difusión se utiliza cuando la dirección IP del servidor es desconocida. Cuando se envía un mensaje de difusión desde un servidor SNTP, el cliente SNTP escucha el mensaje. Si se activa el sondeo de difusión, se acepta 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, ya sea solicitando de manera activa información o en cada intervalo de sondeo. Si se activa el sondeo de difusión única, cualquier difusión y difusión, la información se recupera en este orden:

- Se prefiere la información de los servidores definidos en el dispositivo. Si el sondeo de difusión única no está activado o no hay servidores definidos en el dispositivo, el dispositivo acepta la información horaria de cualquier servidor SNTP que responda.
- Si responde más de un dispositivo de difusión única, se prefiere la información de sincronización del dispositivo con el nivel más bajo.
- Si los servidores tienen el mismo nivel, se acepta la información de sincronización del servidor SNTP que respondió primero.

La autenticación de MD5 (Síntesis del mensaje 5) protege las rutas de acceso de sincronización del dispositivo a los servidores SNTP. MD5 es un algoritmo que produce un hash de 128 bits. MD5 es una variedad de MD4, pero con mayor seguridad. MD5 verifica la integridad de la comunicación y autentica su origen.

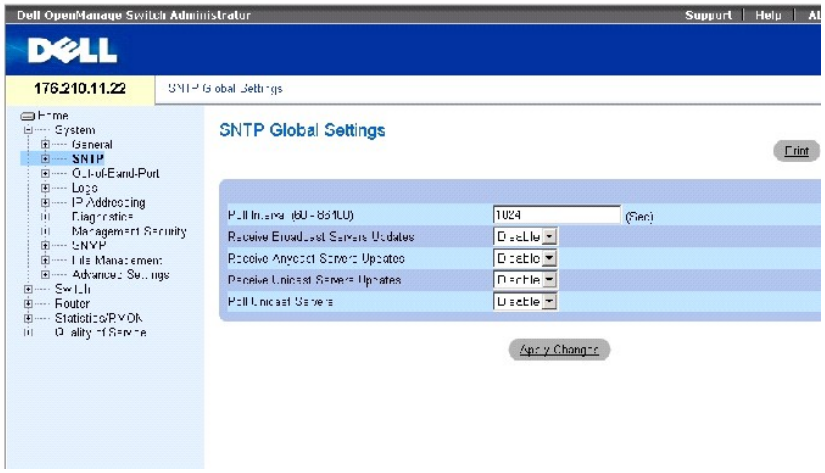
La página SNTP contiene enlaces a las páginas que permiten a los administradores de red configurar los parámetros de SNTP. Para abrir la página **SNTP**, haga clic en **System**→ **SNTP** (Sistema→ SNTP) en la *vista de árbol*.

Definición de los parámetros globales de SNTP

La página **SNTP Global Settings** (Configuración global de SNTP) proporciona información para definir parámetros de SNTP.

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

Ilustración 6-7. SNTP Global Settings (Configuración global de SNTP)



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

Poll Interval (60-86400) (Intervalo de sondeo 60-86400): define el intervalo (en segundos) en el que se realiza un sondeo del servidor SNTP para obtener la información de difusión única.

Receive Broadcast Servers Updates (Recepción de actualizaciones de servidores de difusión): si está activado, escucha a los servidores SNTP para obtener información sobre el tiempo del servidor de difusión en las interfaces seleccionadas. El dispositivo se sincroniza siempre que se recibe un paquete SNTP, aunque no se haya solicitado la sincronización.

Receive Anycast Servers Updates (Recepción de actualizaciones de servidores de cualquier difusión): si está activado, sondea los servidores SNTP para obtener información sobre el tiempo del servidor de cualquier difusión. El dispositivo sólo se sincroniza cuando se envía una solicitud de sincronización desde el dispositivo.

Receive Unicast Servers Updates (Recepción de actualizaciones de servidores de difusión única): si está activado, sondea los servidores SNTP definidos en el dispositivo para obtener información sobre el tiempo del servidor de difusión única. Si los campos **Receive Broadcast Servers Updates** (Recepción de actualizaciones de servidores de difusión), **Receive Anycast Servers Updates** (Recepción de actualizaciones de servidores de cualquier difusión), y **Receive Unicast Servers Updates** (Recepción de actualizaciones de servidores de difusión única) están activados, la hora del sistema se establecerá de acuerdo con la información horaria del servidor de difusión única.

Poll Unicast Servers (Sondear servidores de difusión única): si está activado, envía solicitudes de información horaria del servidor de difusión única SNTP al servidor SNTP.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para establecer los campos que se visualizan en la página **SNTP Global Settings** (Configuración global de SNTP).

Tabla 6-5. Comandos de la CLI para los parámetros globales de SNTP

Comando de la CLI	Descripción
`sntp client poll timer seconds`	Establece el tiempo de intervalo del cliente SNTP.
`sntp broadcast client enable`	Activa los clientes de difusión SNTP.
`sntp unicast client enable`	Activa los clientes predefinidos de difusión única SNTP.
`sntp unicast client poll`	Activa el sondeo de servidores predefinidos de difusión única SNTP.
`show sntp configuration`	Muestra la configuración de SNTP.
`show sntp status`	Muestra el estado de SNTP.

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

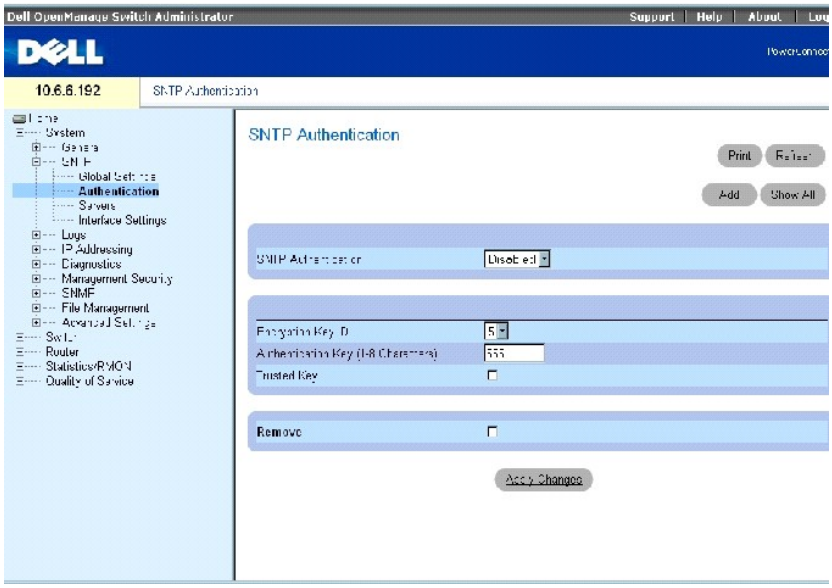
```
Console (config)# sntp anycast client enable
```

Definición de los métodos de autenticación SNTP

En la página **SNTP Authentication** (Autenticación SNTP) se activa la autenticación SNTP entre el dispositivo y un servidor SNTP. El servidor SNTP también se selecciona en la página **SNTP Authentication** (Autenticación SNTP).

Haga clic en **System**→ **SNTP**→ **Authentication** (Sistema→ SNTP→ Autenticación) en la vista de árbol para abrir la página **SNTP Authentication** (Autenticación SNTP).

Ilustración 6-8. SNTP Authentication (Autenticación SNTP)



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

SNTP Authentication (Autenticación SNTP): si está activado, requiere la autenticación de una sesión SNTP entre el dispositivo y un servidor SNTP.

Encryption Key ID (ID de clave de codificación): contiene una lista de ID de clave definidas por el usuario para autenticar el servidor SNTP y el dispositivo. Los valores posibles del campo son de 1 a 4294967295.

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

Trusted Key (Clave fiable): seleccione la casilla de verificación para especificar la clave de codificación utilizada (difusión única/cualquier difusión) o seleccionada (difusión) para autenticar el servidor SNTP.

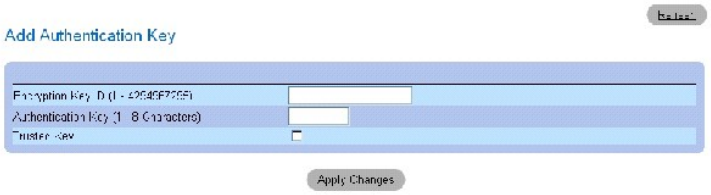
Remove (Eliminar): seleccione la casilla de verificación para eliminar la clave de autenticación seleccionada.

Adición de una clave de autenticación SNTP

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

Se abre la página **Add Authentication Key** (Agregar clave de autenticación):

Ilustración 6-9. Add Authentication Key (Agregar clave de autenticación)



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

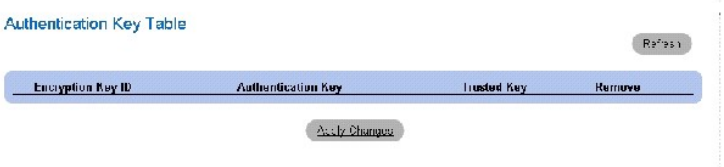
La clave de autenticación SNTP se agregará y el dispositivo se actualizará.

Visualización de la tabla de claves de autenticación

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

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

Ilustración 6-10. Authentication Key Table (Tabla de claves de autenticación)



Supresión de una clave de autenticación

1. Abra la página **SNTP Authentication** (Autenticación 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 **Authentication Key Table** (Tabla de claves de autenticación).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se eliminará y el dispositivo se actualizará.

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

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

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

Comando de la CLI	Descripción
sntp authenticate	Está establecido para solicitar la autenticación del tráfico NTP (Network Time Protocol) de los servidores.
sntp authentication- key *número* **md5** *valor*	Define una clave de autenticación para SNTP.
sntp trusted-key key-*number*	Define la clave de autenticación que se utiliza para autenticar el servidor SNTP.
show sntp configuration	Muestra la configuración de SNTP.

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

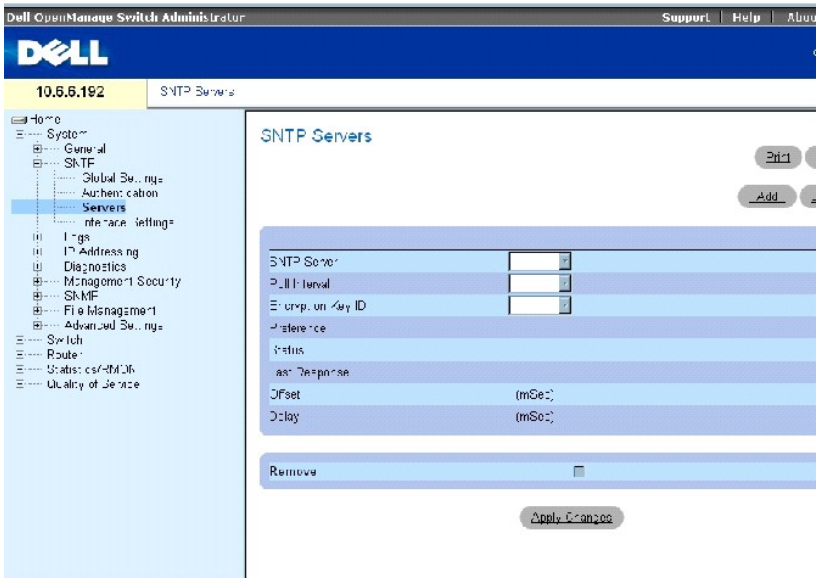
```
Console (config)# sntp authentication-key 8 md5 ClkKey

Console (config)# sntp trusted-key 8

Console (config)# sntp authenticate
```

Definición de los servidores SNTP

La página **SNTP Servers** (Servidores SNTP) contiene información para activar servidores SNTP, así como para agregar nuevos servidores SNTP.

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

Ilustración 6-11. SNTP Servers (Servidores SNTP)



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

SNTP Server (Servidor SNTP): contiene una lista de direcciones IP del servidor SNTP definidas por el usuario. Se pueden definir hasta ocho servidores SNTP.

Poll Interval (Intervalo de sondeo): activa el sondeo del servidor SNTP seleccionado para obtener la información sobre el tiempo del sistema cuando está activado.

Encryption Key ID (ID de clave de codificación): contiene una lista de ID de clave definidas por el usuario que se utilizan para establecer comunicación entre el servidor SNTP y el dispositivo. El ID de clave de codificación se define en la página **SNTP Authentication** (Autenticación SNTP).

Preference (Preferencia): el servidor SNTP que proporciona la información sobre el tiempo de SNTP. Los valores de campo posibles son:

Primary (Primario): el servidor primario proporciona información SNTP.

Secondary (Secundario): el servidor de copia de seguridad proporciona información sobre SNTP.

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

Up (Activado): el servidor SNTP está funcionando normalmente en la actualidad.

Down (Inactivo): indica que un servidor SNTP actualmente no está disponible. Por ejemplo, el servidor SNTP actualmente no está conectado o está inactivo.

In progress (En curso): el servidor SNTP actualmente envía o recibe información SNTP.

Unknown (Desconocido): el progreso de la información SNTP que se envía actualmente es desconocido. Por ejemplo, el dispositivo busca actualmente una interfaz.

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

Offset (Diferencia): diferencia de tiempo entre el reloj local del dispositivo y el tiempo indicado en el servidor SNTP.

Delay (Retraso): tiempo que tarda en alcanzar al servidor SNTP.

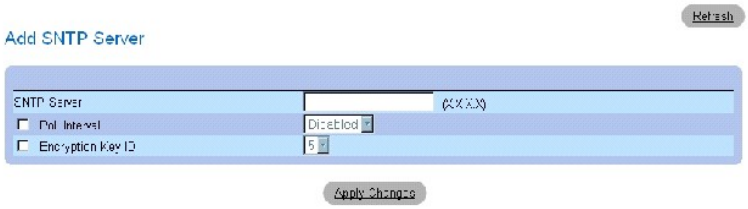
Remove (Eliminar): seleccione la casilla de verificación para eliminar un servidor SNTP específico de la lista **SNTP Servers** (Servidores SNTP).

Adición de un servidor SNTP

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

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

Ilustración 6-12. Add SNTP Server (Agregar servidor SNTP)



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

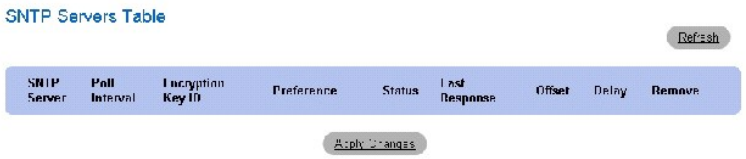
El servidor SNTP se agregará y el dispositivo se actualizará.

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):

Ilustración 6-13. SNTP Servers Table (Tabla de servidores SNTP)



Modificación de un servidor SNTP

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

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

3. Seleccione una entrada del servidor SNTP.
4. Modifique los campos pertinentes.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La información del servidor SNTP se actualizará.

Supresión del servidor SNTP

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

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

3. Seleccione una entrada de **SNTP Server** (Servidor SNTP).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se eliminará y el dispositivo se actualizará.

Definición de los servidores SNTP mediante los comandos de la CLI

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

Tabla 6-7. Comandos de la CLI para la autenticación SNTP

Comando de la CLI	Descripción
sntp server {ip- address | hostname} [**poll**] [**key** keyid]	Define un servidor SNTP que se puede utilizar para sincronizar la información horaria.
no sntp server ip- address	Elimina un servidor de la lista de servidores SNTP.

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

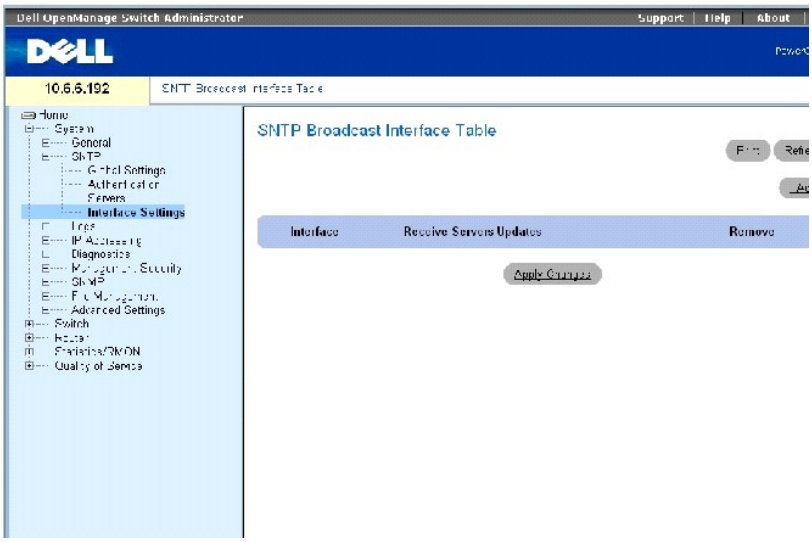
```
Console (config)# sntp server 100.1.1.1 poll key 10
```

Definición de las interfaces SNTP

La **SNTP Broadcast Interface Table** (Tabla de interfaces de difusión SNTP) contiene campos para configurar SNTP en diferentes interfaces.

Para abrir la **SNTP Broadcast Interface Table** (Tabla de interfaces de difusión SNTP), haga clic en **System**→ **SNTP**→ **Interfaces Settings** (Sistema→ SNTP→ Configuración de interfaces).

Ilustración 6-14. SNTP Broadcast Interface Table (Tabla de interfaces de difusión SNTP)



La **SNTP Broadcast Interface Table** (Tabla de interfaces de difusión SNTP) contiene los siguientes campos:

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

Receive Server Updates (Recepción de actualizaciones del servidor): activa o desactiva la recepción de actualizaciones SNTP en la interfaz específica.

Remove (Eliminar): seleccione la casilla de verificación para desactivar SNTP en la interfaz específica.

Activación de SNTP en una interfaz

1. Abra la **SNTP Broadcast Interface Table** (Tabla de interfaces de difusión SNTP).
2. Haga clic en **Add** (Agregar).

   Se abre la página **Add SNTP Interface** (Agregar interfaz SNTP).
3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   SNTP se activará en la interfaz y el dispositivo se actualizará.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los campos que se visualizan en la **SNTP Broadcast Interface Table** (Tabla de interfaces de difusión SNTP).

NOTA: Si se definen las interfaces de difusión o de cualquier difusión, hay que definir como mínimo una dirección IP.

Tabla 6-8. Comandos de la CLI para la configuración de las interfaces SNTP

Comando de la CLI	Descripción
	Activa el cliente de cualquier difusión o de difusión de SNTP (Simple Network Time Protocol) en una interfaz.

sntp client enable	
show sntp configuration	Muestra la configuración de SNTP.

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

```
Console (config)# interface ethernet g1
Console (config-if)# sntp client enable
Console (config-if)# end
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: g1
```

Configuración de los puertos de gestión fuera de banda (OOB)

En este apartado se describe la gestión de las siguientes funciones del dispositivo a través del puerto de gestión fuera de banda. Incluye información sobre el servidor de registro remoto, la puerta de enlace predeterminada, los parámetros de la interfaz IP, el servidor TACACS+ y el servidor RADIUS fuera de banda.

Cuando se gestionan estas funciones mediante el puerto de gestión fuera de banda, se desactiva la gestión dentro de banda de estas funciones. Utilice la interfaz SNMP para configurar estas funciones mediante el puerto fuera de banda.

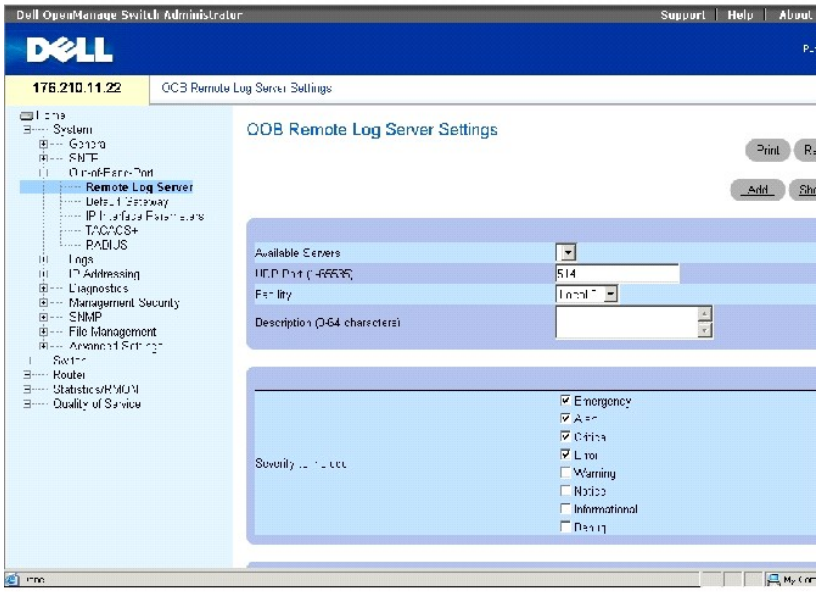
Para abrir la página de configuración OOB, haga clic en **System**→ **Out of Band** (Sistema→ Fuera de banda) en la *vista de árbol.*

Configuración de los servidores de registro remoto fuera de banda

La página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB) contiene los campos para ver los servidores de registros de puertos fuera de banda disponibles. Además, se pueden definir nuevos servidores de registros fuera de banda y enviar la gravedad de los registros al servidor.

Para abrir la página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB), haga clic en **System**→ **Out-of-Band Port**→ **Remote Log Server** (Sistema→ Fuera de banda→ Servidor remoto de registros) en la *vista de árbol.*

Ilustración 6-15. OOB Remote Log Server Settings (Configuración del servidor remoto de registros OOB)



La página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB) contiene los siguientes campos:

Available Servers (Servidores disponibles): servidores a los que se pueden enviar registros.

UDP Port (1-65535) (Puerto UDP [1-65535]): el puerto UDP desde el que se envían los registros. El valor predeterminado es 514.

Facility (Instalación): una aplicación definida por el usuario desde la que se envían los registros del sistema al servidor remoto. Sólo se puede asignar una instalación a un servidor. Si se asigna un nivel de segunda instalación, se anula el nivel de primera instalación. Todas las aplicaciones definidas para un dispositivo utilizan la misma instalación en un servidor. Los valores de campo posibles son local 0, local 1, local 2, local 3, local 4, local 5, local 6 y local 7.

Description (0-64 characters) (Descripción [0-64 caracteres]): muestra la descripción del servidor definido por el usuario.

Severity to Include (Gravedad a incluir): la gravedad del registro. Al seleccionar un nivel de gravedad se seleccionan automáticamente todos los niveles de gravedad superiores.

Delete Server (Suprimir servidor): si se selecciona esta opción, se suprime un servidor de la lista **Available Servers** (Servidores disponibles).

La página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB) también contiene una lista de gravedad. Las definiciones de gravedad son las mismas que las que aparecen en la **RAM Log Table** (Tabla de registros RAM).

Envío de registros a un servidor de registros fuera de banda

1. Abra la página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB).
2. Defina los campos **UDP Port** (Puerto UDP), **Facility** (Instalación) y **Description** (Descripción).
3. Seleccione el tipo de registro y la gravedad de éste.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración del registro se guarda y el dispositivo se actualiza.

NOTA: Antes de agregar un nuevo servidor, determine la dirección IP del servidor remoto de registros fuera de banda.

Definición de un nuevo servidor de registros fuera de banda

1. Abra la página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add an OOB Log Server** (Agregar un servidor de registros OOB).
3. Complete los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define el servidor y se agrega a la lista **Available Servers** (Servidores disponibles).

Supresión de un servidor de registros fuera de banda

1. Abra la página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **OOB Remote Log Servers Table** (Tabla de servidores remotos de registros OOB).
3. Seleccione un servidor y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor se suprime y el dispositivo se actualiza.

Configuración de los servidores remotos de registro fuera de banda mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para trabajar con los campos de la página **OOB Remote Log Server Settings** (Configuración del servidor remoto de registros OOB).

Tabla 6-9. Comandos de la CLI para la configuración del servidor remoto de registros fuera de banda

Comando de la CLI	Descripción
logging *oob/dirección_ip* [**port** *puerto*] [**severity** *nivel*] [**facility** *instalación*] [**description** *texto*]	Define un nuevo servidor remoto de registros.

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

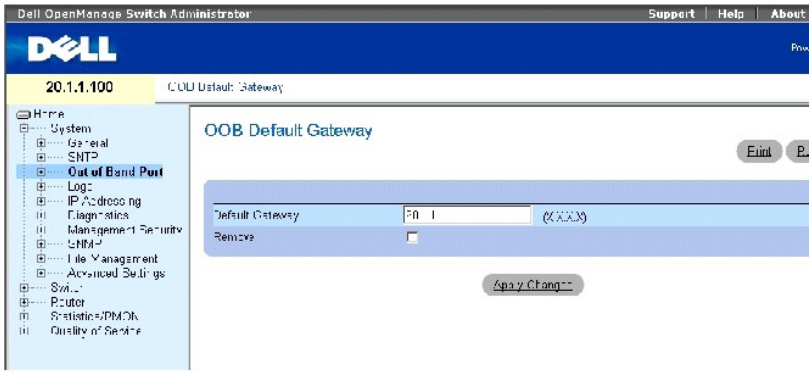
```
Console (config)#logging oob/10.2.2.2 severity critical facility local0 description syslog_server_1
```

Definición de puertas de enlace fuera de banda

Utilice la página **OOB Default Gateway** (Puerta de enlace predeterminada OOB) para asignar dispositivos de puerta de enlace. Los paquetes se reenvían a la IP predeterminada cuando las tramas se reenvían a una red remota. La dirección IP configurada debe pertenecer a la misma subred de dirección IP de una de las interfaces IP. Al eliminar la interfaz IP a la que está conectada una puerta de enlace predeterminada, también se elimina la puerta de enlace predeterminada.

Para abrir la página **OOB Default Gateway** (Puerta de enlace predeterminada OOB), haga clic en **System**→ **Out-of-Band Port**→ **Default Gateway** (Sistema→ Puerto fuera de banda→ Puerta de enlace predeterminada) en la *vista de árbol*.

Ilustración 6-16. OOB Default Gateway (Puerta de enlace predeterminada OOB)



La página **OOB Default Gateway** (Puerta de enlace predeterminada OOB) contiene el siguiente parámetro:

Default Gateway (Puerta de enlace predeterminada): indica la dirección IP del dispositivo de puerta de enlace.

Selección de un dispositivo de puerta de enlace fuera de banda

1. Abra la página **OOB Default Gateway** (Puerta de enlace predeterminada OOB).
2. Defina una dirección IP en el campo **Default Gateway** (Puerta de enlace predeterminada).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El dispositivo de puerta de enlace fuera de banda se define y el dispositivo se actualiza.

Tabla 6-10. Comandos de la CLI para la puerta de enlace predeterminada fuera de banda

Comando de la CLI	Descripción
ip default gateway *dirección_ip*	Define la puerta de enlace IP fuera de banda.

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

```
Console (config)# interface out-of-band-eth
```

```
Console (config-oob)# ip address 10.0.0.1 /8
```

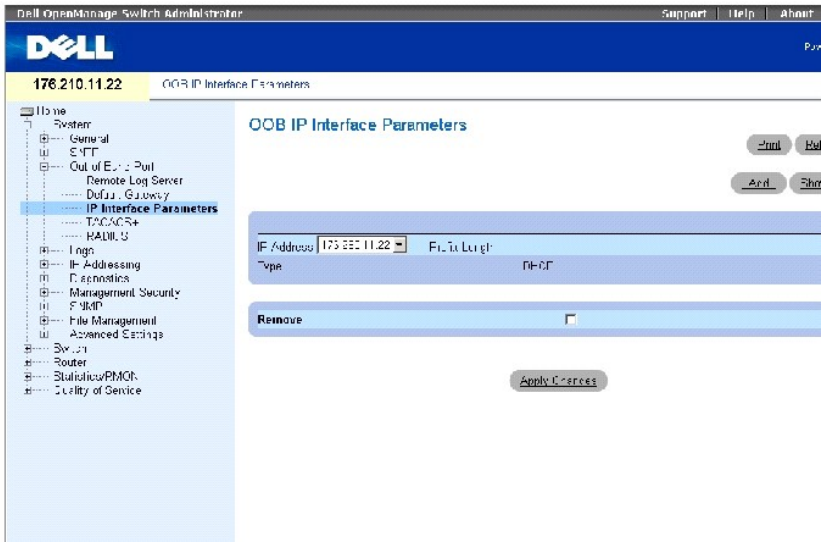
```
Console (config-oob)# ip default-gateway 10.1.1.1
```

Definición de los parámetros de la interfaz IP fuera de banda

La página **OOB IP Interface Parameters** (Parámetros de interfaz IP OOB) contiene los parámetros para asignar direcciones IP fuera de banda a las interfaces.

Para abrir la página **OOB IP Interface Parameters** (Parámetros de interfaz IP OOB), haga clic en **System**→ **Out-of-Band Port**→ **IP Interface Parameters** (Sistema→ Puerto fuera de banda→ Parámetros de interfaz IP) en la *vista de árbol.*

Ilustración 6-17. OOB IP Interface Parameters (Parámetros de interfaz IP OOB)



La página **OOB IP Interface Parameters** (Parámetros de interfaz IP OOB) contiene los siguientes parámetros:

IP Address (Dirección IP): la dirección IP de la interfaz fuera de banda.

Prefix Length (Longitud del 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.

Type (Tipo): el medio por el que se ha creado la interfaz IP fuera de banda; DHCP o estática.

Remove (Eliminar): si se selecciona esta opción, se elimina la interfaz de la lista desplegable **IP Address** (Dirección IP).

NOTA: Puede configurar las direcciones IP DHCP para la gestión fuera de banda en la página **DHCP IP Interface** (**System**→ **IP Address**→ **DHCP IP Interface**) (Sistema→ Dirección IP→ Interfaz IP DHCP).

Adición de una interfaz IP

1. Abra la página **OOB IP Interface Parameters** (Parámetros de interfaz IP OOB).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add a Static OOB IP Interface** (Agregar una interfaz IP OOB estática).

3. El campo **Network Mask** (Máscara de red) especifica la máscara de subred de la dirección IP de origen.
4. Complete los campos de esta página.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva interfaz se agrega y el dispositivo se actualiza.

Supresión de direcciones IP

1. Abra la página **OOB IP Interface Parameters** (Parámetros de interfaz IP OOB).
2. Haga clic en **Show All** (Mostrar todo).
3. Se abre la página **Interface Parameters Table** (Tabla de parámetros de interfaz).
4. Seleccione una dirección IP en la lista desplegable **IP Address** (Dirección IP).
5. Seleccione una entrada de la lista **Interface Parameters Table** (Tabla de parámetros de interfaz).
6. Marque la casilla de verificación **Remove** (Eliminar).
7. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección IP se suprime y el dispositivo se actualiza.

Definición de las interfaces IP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para trabajar con los campos de la página **OOB IP Interface Parameters** (Parámetros de interfaz IP OOB).

Tabla 6-11. Comandos de la CLI para los parámetros de interfaz IP fuera de banda

Comando de la CLI	Descripción
interface out-of- band-eth	Configura el puerto Ethernet fuera de banda y establece el modo de configuración de la interfaz.
ip address *dirección_ip* {*máscara* | *longitud_prefijo*}	Establece una dirección IP.

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

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 192.168.0.1 /8
```

Configuración de los servidores TACACS+ fuera de banda

El dispositivo proporciona asistencia de Sistema de Control de Acceso al Controlador de Acceso a la Terminal (TACACS+) al cliente. TACACS+ proporciona seguridad centralizada para la validación de usuarios que acceden al dispositivo.

TACACS+ proporciona un sistema de gestión de usuarios centralizado al mismo tiempo que mantiene la coherencia con RADIUS y otros procesos de autenticación. TACACS+ proporciona los siguientes servicios:

- **Authentication** (Autenticación): proporciona autenticación durante el inicio de sesión y a través de nombres de usuario y contraseñas definidas por el usuario.

- **Authorization** (Autorización): otorgada en el inicio de sesión. Cuando la sesión de autenticación se haya completado, se iniciará una sesión de autorización mediante el nombre de usuario autenticado. El servidor TACACS+ comprobará los privilegios del usuario.

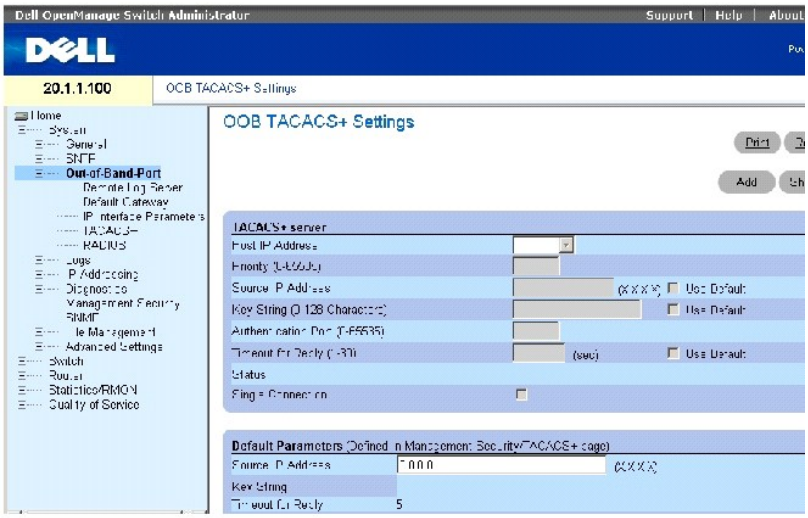
Los servidores TACACS+ se pueden definir en puertos dentro de banda mediante la página **TACACS+ Settings** (Configuración de TACACS+) o en el puerto fuera de banda.

El protocolo TACACS+ garantiza la integridad de la red a través de intercambios de protocolo codificado entre el dispositivo y el servidor TACACS+.

La página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB) contiene tanto la configuración de TACACS+ predeterminada como la definida por el usuario para el puerto de gestión fuera de banda.

Para abrir la página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB), haga clic en **System**→ **Out-of-Band-Port**→ **TACACS+** (Sistema→ Puerto fuera de banda→ TACACS+) en la *vista de árbol.*

Ilustración 6-18. OOB TACACS+ Settings (Configuración de TACACS+ OOB)



La página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB) contiene los siguientes campos:

Host IP Address (Dirección IP del sistema principal): especifica la dirección IP del servidor TACACS+.

Priority (0-65535) (Prioridad [0 - 65535]): especifica 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 de TACACS+ entre el dispositivo y el servidor TACACS+.

Key String (0-128 Characters) (Cadena de clave [0 - 128 caracteres): define la autenticación y la clave de codificación para las comunicaciones de TACACS+ entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con la codificación usada en el servidor TACACS+.

Authentication Port (0-65535) (Puerto de autenticación [0 - 65535]): número del puerto a través del cual se lleva a cabo la sesión de TACACS+. El puerto predeterminado es el 49.

Reply Timeout (1-30) (Tiempo de espera para respuesta [1 - 30]): tiempo que transcurre antes de que caduque la conexión entre el dispositivo y el servidor TACACS+. El intervalo de este campo es de 1 a 30 segundos.

Status (Estado): estado de conexión entre el dispositivo y el servidor TACACS+. Los valores de campo posibles son:

Connected (Conectado): actualmente existe una conexión entre el dispositivo y el servidor TACACS+.

Not Connected (No conectado): actualmente no existe ninguna conexión entre el dispositivo y el servidor TACACS+.

Single Connection (Conexión única): si esta opción está seleccionada, se mantiene una única conexión abierta entre el dispositivo y el servidor TACACS+.

Los parámetros predeterminados de TACACS+ están definidos por el usuario. La configuración predeterminada se aplica a los servidores TACACS+ recientemente definidos. Si los valores predeterminados no están definidos, los valores predeterminados del sistema se aplican a los nuevos servidores TACACS+. Los valores que se muestran a continuación son los valores predeterminados de TACACS+:

Source IP Address (Dirección IP de origen): dirección IP de origen del dispositivo predeterminado utilizada para la sesión de TACACS+ entre el dispositivo y el servidor TACACS+.

Key String (0-128 Characters) (Cadena de clave [0 - 128 caracteres]): autenticación predeterminada y clave de codificación para la comunicación de TACACS+ entre el dispositivo y el servidor TACACS+.

Timeout for Reply (1-30) (Tiempo de espera para repuesta [1 - 30]): tiempo predeterminado que transcurre antes de que caduque la conexión entre el dispositivo y TACACS+.

NOTA: Puede establecer los valores de los valores mencionados anteriormente en la página de **configuración** de TACACS+ (**System**→ **Management Security**→ **TACACS+**) (Sistema→ Gestión de seguridad→ TACACS+).

Definición de los parámetros de TACACS+

1. Abra la página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de TACACS+ se actualiza en el dispositivo.

Adición de un servidor TACACS+

1. Abra la página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add OOB** TACACS+ **Host** (Agregar sistema principal de TACACS+ OOB).

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

El servidor TACACS+ se agregará y el dispositivo se actualizará.

Supresión de un servidor TACACS+ de la lista de servidores TACACS+

1. Abra la página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **TACACS+ Table** (Tabla de TACACS+).

3. Seleccione una entrada de la **TACACS+ Table** (Tabla de TACACS+).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor TACACS+ se eliminará y el dispositivo se actualizará.

Definición de los servidores TACACS+ mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para trabajar con los campos de la página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB).

Tabla 6-12. Comandos de la CLI para la configuración de TACACS+ fuera de banda

Comando de la CLI	Descripción
tacacs-server host {*oob/ip-address* | *hostname*} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]	Especifica el sistema principal de un servidor TACACS+.
no tacacs-server host {*ip-address* | *hostname*}	Suprime el sistema principal de un servidor TACACS+ concreto.
tacacs-server key [key-string]	Especifica la autenticación y la clave de codificación utilizada para todas las comunicaciones de TACACS entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con la codificación utilizada en el daemon de TACACS. (Intervalo:0-128 caracteres)
no tacacs-server key	Vuelve al valor predeterminado.
tacacs-server timeout *tiempo de espera*	Especifica el valor del tiempo de espera en segundos. (Intervalo: 1-30)
no tacacs-server timeout	Vuelve al valor predeterminado.
tacacs-server source-ip *oob/dirección_ip*	Especifica la dirección IP de origen. (Intervalo: dirección IP válida)
no tacacs-server source-ip *oob/dirección_ip*	Vuelve al valor predeterminado.
show tacacs [*oob/ip-address*]	Muestra la configuración y las estadísticas de un servidor TACACS+.

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

```
Console (config)# tacacs-server host oob/172.16.8.1 key abc

Console (config)# end

Console# show tacacs

                                                                  

Device Configuration

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

IP address  Status     Port  Single      TimeOut  Source  Priority
                             Connection          IP
----------  ---------  ----  ----------  -------  ------  --------

No TACACS server is configured.

                                                                  

OOB host Configuration
```

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
----------	---------	----	----------	-------	------	--------
172.16.8.1	Not Connected	49	No	Global	Global	0
Global Values						

TimeOut: 5						
Device Configuration						

Source IP: 0.0.0.0						
OOB host Configuration						

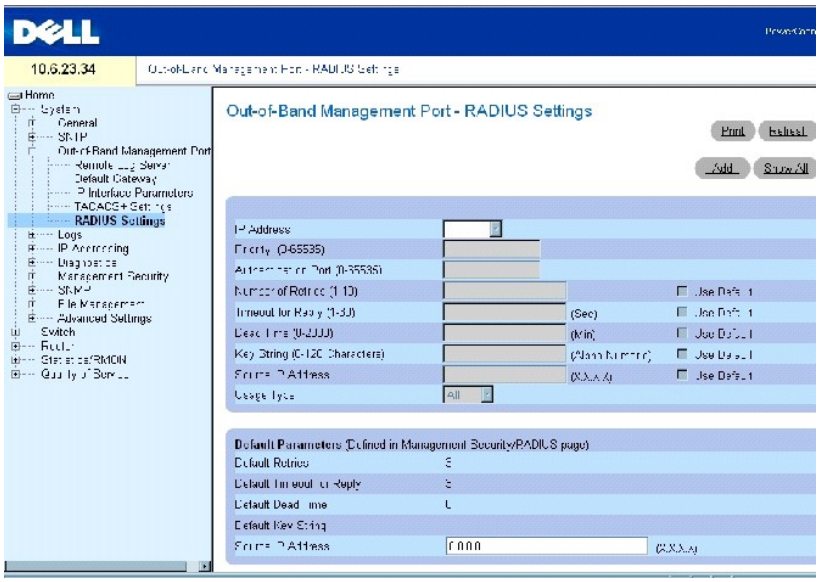
Source IP : 0.0.0.0						

Configuración de los servidores RADIUS fuera de banda

La página **OOB RADIUS Settings** (Configuración de RADIUS OOB) contiene tanto la configuración de RADIUS predeterminada como la definida por el usuario para el puerto de gestión fuera de banda. Para obtener más información sobre los servidores RADIUS, consulte el apartado Configuración de los valores de TACACS+ .

Para abrir la página **OOB RADIUS Settings** (Configuración de RADIUS OOB), haga clic en **System**→ **Out-of-Band Port**→ **RADIUS** (Sistema→ Puerto fuera de banda→ RADIUS) en la vista de árbol (consulte la Ilustración 6-19 OOB RADIUS Settings [Configuración de RADIUS OOB]).

Ilustración 6-19. OOB RADIUS Settings (Configuración de RADIUS OOB)



La página **OOB RADIUS Settings** (Configuración de RADIUS OOB) contiene los siguientes campos:

IP Address (Dirección IP): la dirección IP del puerto fuera de banda de autenticación.

Priority (0-65535) (Prioridad [0-65535]): indica la prioridad del puerto fuera de banda. Los valores posibles son 0-65535.

Authentication Port (Puerto de autenticación): el puerto de autenticación, que se utiliza para comprobar la autenticación del servidor RADIUS.

Number of Retries (1-10) (Número de reintentos [1-10]): número de peticiones transmitidas que se envían al servidor RADIUS antes de que se produzca un fallo. Los valores de campo posibles son 1-10. El valor predeterminado es 3. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales.

Timeout for Reply (1-30) (Tiempo de espera para respuesta [1-30]): cantidad de tiempo en segundos que el dispositivo espera una respuesta del servidor RADIUS antes de expirar. Los valores de campo posibles son 1-30. El valor predeterminado es 3. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales.

Dead Time (0-2000) (Tiempo muerto [0-2000]): cantidad de tiempo (en minutos) durante el que no se envían peticiones de servicio a un servidor RADIUS. El intervalo es 0-2000. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales.

Key String (0-128 Characters) (Cadena de clave [1-128 caracteres]): cadena de clave utilizada para autenticar y codificar todas las comunicaciones de RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la codificación RADIUS. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales.

Source IP Address (Dirección IP de origen): dirección IP del dispositivo que accede al servidor RADIUS.

Los parámetros predeterminados de RADIUS están definidos por el usuario. La configuración predeterminada se aplica a los servidores RADIUS recientemente definidos. Si los valores predeterminados no están definidos, los valores predeterminados del sistema se aplican a los nuevos servidores RADIUS. Los valores que se muestran a continuación son los valores predeterminados de RADIUS:

Default Timeout for Reply (Tiempo de espera predeterminado para respuesta): cantidad de tiempo predeterminada que el dispositivo espera una respuesta del servidor RADIUS antes de expirar.

Default Retries (sec) (Reintentos predeterminados [seg]): número predeterminado de peticiones transmitidas que se envían a un servidor RADIUS antes de que se produzca un fallo.

Default Dead Time (sec) (Tiempo muerto predeterminado [seg]): cantidad de tiempo predeterminada (en minutos) durante el que no se envían peticiones de servicio a un servidor RADIUS. El intervalo es 0-2000.

Default Key String (Cadena de clave predeterminada): cadena de clave predeterminada que se utiliza para autenticar y cifrar todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la codificación RADIUS.

NOTA: Puede establecer los valores de los valores predeterminados mencionados anteriormente en la página **RADIUS Settings** (Configuración de RADIUS) (**System**→ **Management Security**→ **RADIUS** [Sistema→ Gestión de seguridad→ RADIUS]).

Source IP Address (Dirección IP de origen): dirección IP predeterminada de un dispositivo que accede al servidor RADIUS.

Definición de los parámetros RADIUS fuera de banda

1. Abra la página **OOB RADIUS Setting** (Configuración de RADIUS OOB).
2. Defina los campos siguientes: **Default Timeout for Reply** (Tiempo de espera predeterminado para respuesta), **Default Retries** (Entradas predeterminadas), **Default Dead Time** (Tiempo muerto predeterminado) y **Default Key** (Clave predeterminada).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de RADIUS se actualiza en el dispositivo.

Adición de un servidor RADIUS fuera de banda

1. Abra la página **OOB RADIUS Setting** (Configuración de RADIUS OOB).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add OOB RADIUS Server** (Agregar un servidor RADIUS OOB).
3. Complete los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El nuevo servidor RADIUS se agrega y el dispositivo se actualiza.

Supresión de un servidor RADIUS fuera de banda de la lista de servidores RADIUS

1. Abra la página **OOB RADIUS Setting** (Configuración de RADIUS OOB).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la lista **OOB RADIUS Servers** (Servidores RADIUS OOB).
3. Seleccione un servidor RADIUS y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el servidor RADIUS de la lista de servidores RADIUS.

Definición de los servidores RADIUS mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para trabajar con los campos de la página **OOB RADIUS Settings** (Configuración de RADIUS OOB).

Tabla 6-13. Comandos de la CLI para la configuración de RADIUS fuera de banda

Comando de la CLI	Descripción
`radius-server host` *`dirección_ip`* `[auth-port` *`número_puerto_aut`*`] [timeout` *`tiempo de espera`*`] [retransmit retries] [deadtime` *`tiempo muerto`*`] [key` *`cadena_clave`*`] [source` *`origen`*`] [priority` *`prioridad`*`]`	Especifica el sistema principal de un servidor RADIUS.
`no radius-server host` *`dirección_ip`*	Suprime el sistema principal de un servidor RADIUS concreto.

`radius-server source-ip` *`origen`*	Especifica la dirección IP de origen que se utiliza para la comunicación con los servidores RADIUS.
`no radius-server-ip`	Vuelve al valor predeterminado.
`radius-server timeout` *`tiempo de espera`*	Establece el intervalo durante el cual un enrutador espera la respuesta del sistema principal de un servidor.
`no radius-server deadtime`	Establece el tiempo muerto en 0.

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

```
Console (config)#interface out-of-band eth 1
```

```
Console radius-server host oob/10.2.2.2 key 123
```

Gestión de registros

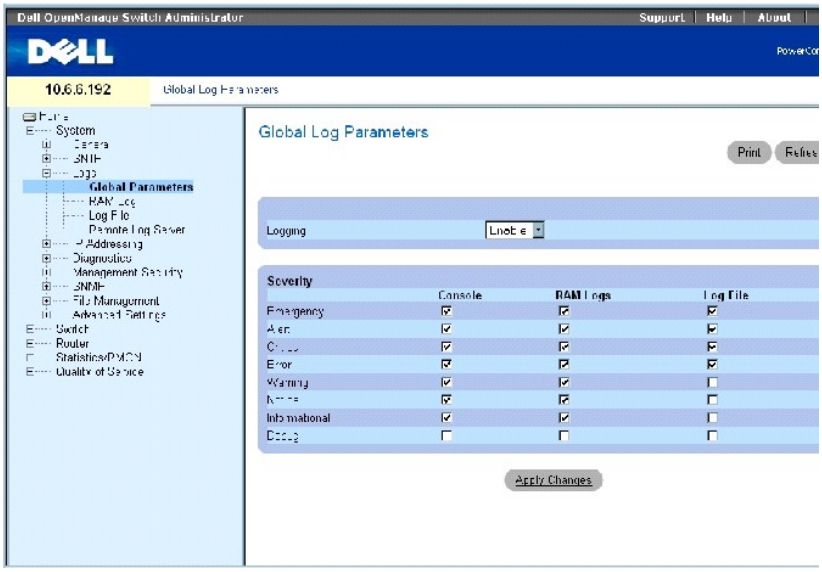
La página **Logs** (Registros) contiene enlaces con diferentes páginas de registros. Para visualizar la página **Logs** (Registros), haga clic en **System**→ **Logs** (Sistema→ Registros) en la *vista de árbol.*

Parámetros de registro globales

La página **Global Log Parameters** (Parámetros de registro globales) contiene los campos para activar los registros globalmente y los campos para definir los parámetros de registros. Los mensajes de registros **Severity** (Gravedad) se enumeran desde el nivel de gravedad más alto al más bajo.

Para abrir la página **Global Log Parameters** (Parámetros de registro globales) haga clic en **System**→ **Logs**→ **Global Parameters** (Sistema→ Registros→ Parámetros globales) en la *vista de árbol.*

Ilustración 6-20. Global Log Parameters (Parámetros de registro globales)



La página **Global Log Parameters** (Parámetros de registro globales) contiene los siguientes campos:

Logging (Registro): activa los registros globales del dispositivo para la caché, el archivo y los registros del servidor. Todos los registros que se imprimen en la consola se guardan en los archivos de registro. Los valores de campo posibles son:

Enable (Activar): activa la característica de guardar los registros en caché (RAM), en archivo (FLASH) y en un servidor externo.

Disable (Desactivar): desactiva la característica de guardar registros. No se puede desactivar el registro de los registros que se imprimen en la consola.

Emergency (Emergencia): el nivel de advertencia superior. Si el dispositivo está inactivo o no funciona correctamente, se guarda un registro de emergencia en el dispositivo.

Alert (Alerta): el segundo nivel de advertencia más alto. Se guarda un registro de alerta si hay un fallo grave del dispositivo como, por ejemplo, si todas las funciones del dispositivo están inactivas.

Critical (Grave): el tercer nivel de advertencia más alto. Se guarda un registro grave si se produce un fallo grave del dispositivo; por ejemplo, si hay dos puertos del dispositivo que no funcionan correctamente mientras el resto de los puertos del dispositivo sí funcionan.

Error: se ha producido un error del dispositivo como, por ejemplo, si un puerto está fuera de línea.

Warning (Advertencia): el nivel más bajo de una advertencia sobre el dispositivo.

Notice (Aviso): proporciona información sobre el dispositivo a los administradores de red.

Informational (Informativo): proporciona información sobre el dispositivo.

Debug (Depurar): proporciona información detallada sobre el registro. La depuración de errores sólo la debe realizar personal de asistencia cualificado.

Las casillas de verificación aparecen bajo las tres columnas siguientes:

Console (Consola): registros que se envían a la consola.

RAM Logs (Registros RAM): registros que se envían a la RAM (caché).

Log File (Archivo de registro): registros que se envían al archivo (FLASH).

Activación de registros

1. Abra la página **Global Log Parameters** (Parámetros de registro globales).
2. Seleccione **Enable** (Activar) en el menú descendente **Logging** (Registro).
3. Utilice las casillas de verificación para seleccionar el tipo de registro y la gravedad.

NOTA: Cuando selecciona un nivel de gravedad, se seleccionan automáticamente todos los niveles de gravedad superiores.

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

La configuración del registro se guarda y el dispositivo se actualiza.

Activación de registros globales mediante la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para trabajar con los campos que se visualizan en la página **Global Log Parameters** (Parámetros de registro globales).

Tabla 6-14. Comandos de la CLI para los parámetros de registro globales

Comando de la CLI	Descripción
`logging on`	Activa el registro de mensajes de error.
`logging dirección-ip [port puerto] [severity nivel] [facility instalación] [description texto]`	Registra los mensajes en un servidor de registro del sistema.
`logging console nivel`	Limita los mensajes registrados en la consola según la gravedad.
`logging buffered nivel`	Limita los mensajes de registro del sistema que se muestran desde un búfer (RAM) interno según la gravedad.
`logging file [nivel]`	Limita los mensajes de registro del sistema que se envían al archivo de registro según la gravedad.

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

```
Console (config)# logging on

Console (config)# logging 10.1.1.1 severity critical

Console (config)# logging console errors

Console (config)# logging buffered debugging
```

```
Console (config)# logging file alerts
```

```
Console # clear logging
```

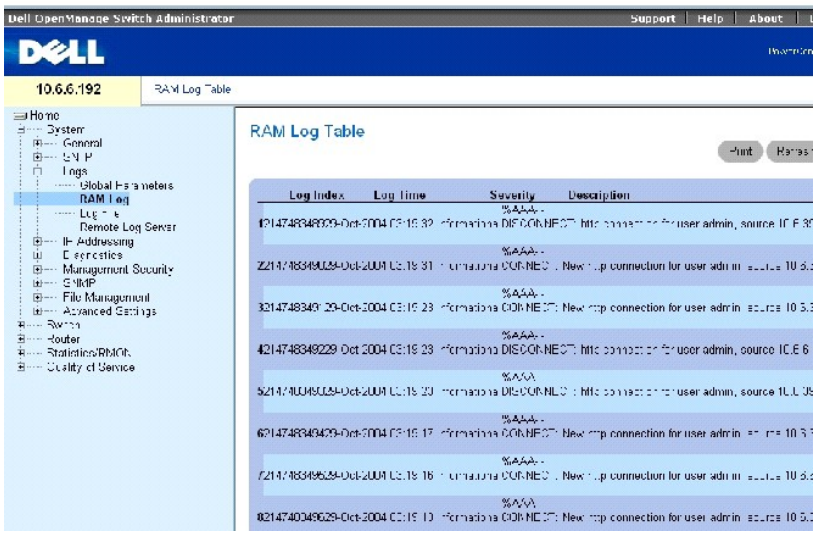
```
Clear Logging Buffer [y/n]? y
```

Tabla de registros RAM

La **RAM Log Table** (Tabla de registros RAM) contiene información acerca de las entradas de registro RAM (caché) específicas, incluida la hora en la que se introdujo el registro, la gravedad del registro y una descripción de éste.

Para visualizar la **RAM Log Table** (Tabla de registros RAM), haga clic en **System**→ **Logs**→ **RAM Log** (Sistema→ Registros→ Registro RAM) en la vista de árbol (consulte la Ilustración 6-21).

Ilustración 6-21. RAM Log Table (Tabla de registros RAM)



La **RAM Log Table** (Tabla de registros RAM) contiene los siguientes campos:

Log Index (Índice de registro): indica el número de registro en la tabla de registros RAM.

Log Time (Hora de registro): la hora a la que se introdujo el registro en la tabla de registros RAM.

Severity (Gravedad): la gravedad del registro.

Description (Descripción): la descripción del registro.

Eliminación de la información del registro

1. Abra la página **RAM Log Table** (Tabla de registros RAM).
2. Haga clic en **Clear Logs** (Borrar registros).

La información del registro se elimina de la tabla de archivos de registro y el dispositivo se actualiza.

Visualización de la tabla de registros RAM mediante la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver los campos que se muestran en la página **RAM Log Table** (Tabla de registros RAM).

Tabla 6-15. Comandos de la CLI para la tabla de registros RAM

Comando de la CLI	Descripción
`show logging`	Muestra el estado del registro y los mensajes de registro del sistema almacenados en el búfer interno.
`clear logging`	Borra los mensajes del búfer de registro.

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

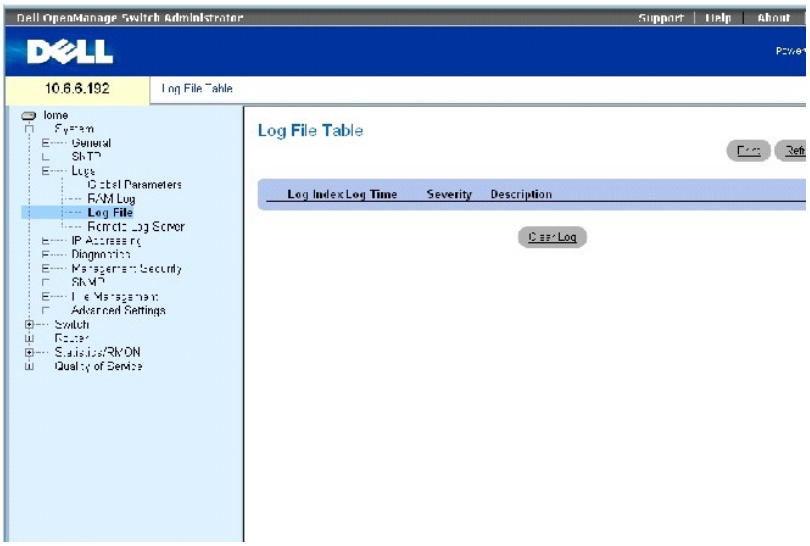
```
Console # show logging

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated

10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup
```

Tabla de archivos de registro

La página **Log File Table** (Tabla de archivos de registro) contiene información sobre entradas de registro específicas, incluida la hora en que se introdujo el registro, la gravedad del registro y una descripción de éste.

Para visualizar la página **Log File Table** (Tabla de archivos de registro), haga clic en **System**→ **Logs**→ **Log File** (Sistema→ Registros→ Archivo de registro) en la vista de árbol (consulte la Tabla 6-22).

Ilustración 6-22. Log File Table (Tabla de archivos de registro)



La página **Log File Table** (Tabla de archivos de registro) contiene los siguientes campos:

- **Log Index** (Índice de registro): el número de registro de la **Log File Table** (Tabla de archivos de registro).
- **Log Time** (Hora de registro): la hora a la que se introdujo el registro en la **Log File Table** (Tabla de archivos de registro).
- **Severity** (Gravedad): la gravedad del registro.
- **Description** (Descripción): la descripción del registro.

Visualización de la tabla de archivos de registro mediante la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver los campos que se muestran en 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 del registro y los mensajes de registro del sistema almacenados en el archivo de registro.
`clear logging`	Borra los mensajes del búfer de registro.

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

```
Console # show logging file


Console Logging: Level info. Console Messages: 0 Dropped.
```

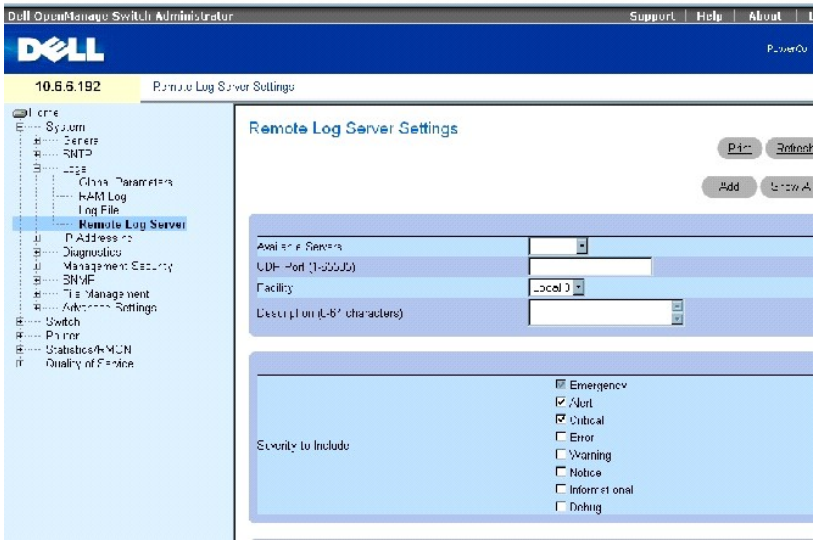
```
Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated

10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup

10-Jan-2003 09:22:51 :%LINK-I-Up: Oob-eth 1

10-Jan-2003 09:22:51 :%LINK-W-Down: g24

10-Jan-2003 09:22:51 :%LINK-W-Down: g23

10-Jan-2003 09:22:51 :%LINK-W-Down: g22

10-Jan-2003 09:22:51 :%LINK-W-Down: g21
```

Servidor de registros remoto

La página **Remote Log Server Settings** (Configuración del servidor de registros remoto) contiene campos para ver los servidores de registro disponibles. Además, se pueden definir nuevos servidores de registros y enviar la gravedad de los registros al servidor.

Para abrir la página **Remote Log Server Settings** (Configuración del servidor de registros remoto), haga clic en **System**→ **Logs**→ **Remote Log Server** (Sistema→ Registros→ Servidor de registros remoto).

Ilustración 6-23. Remote Log Server Settings (Configuración del servidor de registros remoto)



La página **Remote Log Server Settings** (Configuración del servidor de registros remoto) contiene los siguientes campos:

Available Servers (Servidores disponibles): servidores a los que se pueden enviar registros.

UDP Port (1-65535) (Puerto UDP [1-65535]): el puerto UDP desde el que se envían los registros. El valor predeterminado es 514.

Facility (Instalación): una aplicación definida por el usuario desde la que se envían los registros del sistema al servidor remoto. Sólo se puede asignar una instalación a un servidor. Si se asigna un nivel de segunda instalación, se anula el nivel de primera instalación. Todas las aplicaciones definidas para un dispositivo utilizan la misma instalación en un servidor. Los valores posibles son **Local 0** - **Local 7**.

Description (Descripción): la descripción del servidor. La longitud máxima es de 64 caracteres.

Severity (Gravedad): la gravedad del registro. Al seleccionar un nivel de gravedad se seleccionan automáticamente todos los niveles de gravedad superiores.

Delete Server (Suprimir servidor): suprime un servidor de la lista **Available Server** (Servidores disponibles). Si se marca esta casilla de verificación se suprime el servidor de la lista. Si esta casilla no se marca, el servidor permanece en la lista.

La página **Remote Log Server Settings** (Configuración del servidor de registros remoto) también contiene una lista de gravedad. Las definiciones de gravedad son las mismas que las definiciones de gravedad que aparecen en la página **RAM Log Table** (Tabla de registros RAM).

Envío de registros a un servidor

1. Abra la página **Remote Log Server Settings** (Configuración del servidor de registros remoto).
2. Defina los campos **UDP Port** (Puerto UDP), **Facility** (Instalación) y **Description** (Descripción).
3. Seleccione el tipo de registro y la gravedad de registro utilizando las casillas de verificación **Log Parameters** (Parámetros de registro).

NOTA: Cuando selecciona un nivel de gravedad, se seleccionan automáticamente todos los niveles de gravedad superiores.

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

La configuración del registro se guarda y el dispositivo se actualiza.

Definición de un nuevo servidor

1. Abra la página **Remote Log Server Settings** (Configuración del servidor de registros remoto).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add a Log Server** (Agregar un servidor de registros).

NOTA: Antes de agregar un nuevo servidor, determine la dirección IP del servidor remoto de registros.

3. Complete los campos del cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

La página **Remote Log Server Settings** (Configuración del servidor de registros remoto) muestra el servidor en la lista **Available Server** (Servidores disponibles) sólo después de que haya actualizado manualmente la página.

Supresión de un servidor de registros

1. Abra la página **Remote Log Server Settings** (Configuración del servidor de registros remoto).
2. Haga clic en **Show All** (Mostrar todo) para abrir la página **Log Server Table** (Tabla de servidores de registro).
3. Seleccione un servidor y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor se suprime y el dispositivo se actualiza.

Trabajo con registros de servidores remotos mediante los comandos de la CLI

La siguiente tabla muestra un resumen de los comandos de la CLI para trabajar con los registros de servidores remotos.

Tabla 6-17. Comandos de la CLI para el servidor de registros remoto

Comando de la CLI	Descripción
`logging` *`dirección_ip`* `[port port] [severity` *`nivel`*`] [facility` *`instalación`*`] [`*`texto_descripción`*`]`	Registra los mensajes en un servidor remoto.

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

```
Console (config) # logging 10.1.1.1 severity critical
```

Definición del direccionamiento IP

Utilice la página **IP Addressing** (Direccionamiento IP) para asignar direcciones IP de puerta de enlace predeterminada y de interfaz, y definir los parámetros ARP y DHCP de las interfaces.

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

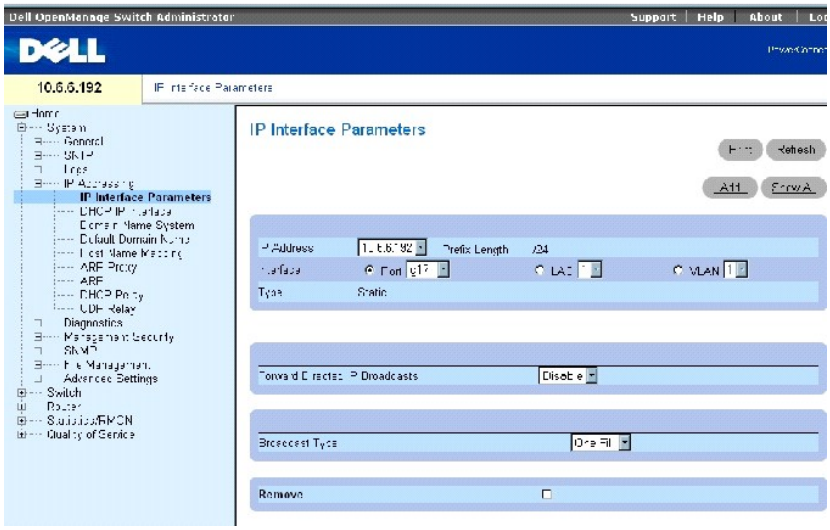
Definición de las interfaces IP

La página **IP Interface Parameters** (Parámetros de interfaz IP) contiene los parámetros para asignar direcciones IP a las interfaces.

Para abrir la página **IP Interface Parameters** (Parámetros de interfaz IP), haga clic en **System**→ **IP Addressing**→ **Interface Parameters** (Sistema→

Direccionamiento IP→ Parámetros de interfaz) en la *vista de árbol.*

Ilustración 6-24. IP Interface Parameters (Parámetros de interfaz IP)



La página **IP Interface Parameters** (Parámetros de interfaz IP) contiene los siguientes campos:

IP Address (Dirección IP): dirección IP de la interfaz.

Prefix Length (Longitud del 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.

Interface (Interfaz): tipo de interfaz para la que está definida la dirección IP. Los posibles valores del campo son **Port** (Puerto), **LAG** o **VLAN**.

Para obtener información sobre la configuración de grupos agregados de conexiones (LAG), consulte el apartado Adición de puertos . Para obtener información sobre la configuración de VLAN, consulte el apartado Configuración de VLAN .

Type (Tipo): indica si la dirección IP se ha configurado estáticamente o no.

Forward Directed IP Broadcasts (Reenviar difusiones IP dirigidas): activa la conversión de una difusión dirigida en difusiones físicas. La desactivación omite las difusiones dirigidas por IP y no las reenvía.

Broadcast Type (Tipo de difusión): define una dirección de difusión de interfaz.

One Fill (Relleno con unos): indica que la dirección de difusión de la interfaz es de relleno con unos (255.255.255.255).

Zero Fill (Relleno con ceros): indica que la dirección de difusión de la interfaz es de relleno con ceros (0.0.0.0).

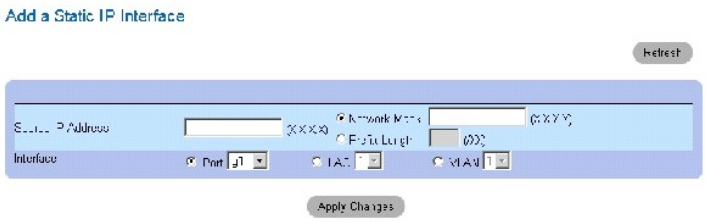
Remove (Eliminar): si se selecciona esta opción, se elimina la interfaz del menú descendente **IP Address** (Dirección IP).

Adición de una interfaz IP

1. Abra la página **IP Interface Parameters** (Parámetros de interfaz IP).

2. Haga clic en **Add** (Agregar) para abrir la página **Add a Static IP Interface** (Agregar una interfaz IP estática).

Ilustración 6-25. Add a Static IP Interface (Agregar una interfaz IP estática)



3. Complete los campos de esta página.

Network Mask (Máscara de red) especifica la máscara de subred de la dirección IP de origen.

Cada parte de la dirección IP debe empezar con un número distinto de cero. Por ejemplo, las direcciones IP 001.100.192.6 y 192.001.10.3 no son válidas.

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

La nueva interfaz se agrega y el dispositivo se actualiza.

Modificación de los parámetros de dirección IP

1. Abra la página **IP Interface Parameters** (Parámetros de interfaz IP).
2. Seleccione una dirección IP en el menú descendente **IP Address** (Dirección IP).
3. Modifique los campos obligatorios.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se modifican y el dispositivo se actualiza.

Supresión de direcciones IP

1. Abra la página **IP Interface Parameters** (Parámetros de interfaz IP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Interface Parameters Table** (Tabla de parámetros de interfaz).
3. Seleccione una dirección IP y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección IP se suprime y el dispositivo se actualiza.

Definición de los parámetros de la interfaz IP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para trabajar con los campos de la página **IP Interface Parameters** (Parámetros de interfaz IP).

Tabla 6-18. Comandos de la CLI para parámetros de la interfaz IP

Comando de la CLI	Descripción
	Establece una dirección IP.

`ip address dirección_ip {mask | prefix-length}`	
`no ip address [dirección_ip]`	Elimina una dirección IP.
`show ip interface [ethernet s | vlan id_vlan | número_canal_puerto]`	Muestra el estado de uso de las interfaces configuradas para IP.
`directed-broadcast`	Activa la conversión de una difusión dirigida en difusiones físicas.

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

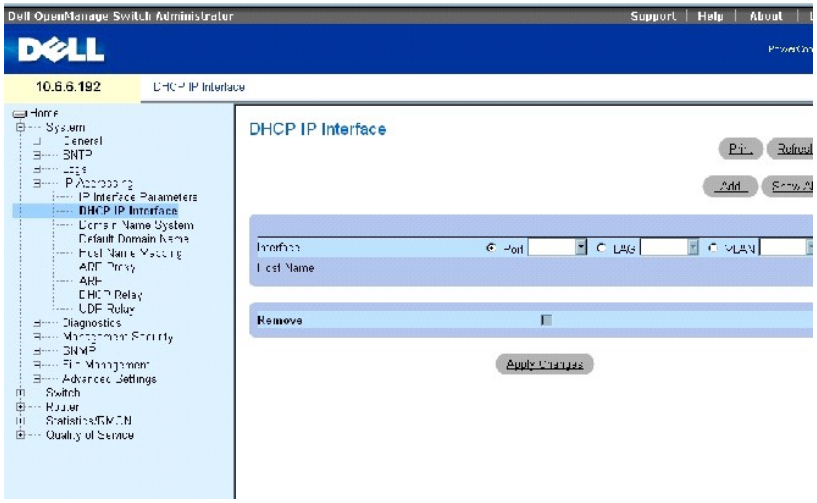
```
Console (config)# interface vlan 1

Console (config-if)# ip address 192.168.1.1 255.255.255.0

Console (config-if)# no ip address 192.168.1.1
```

Definición de los parámetros de interfaz IP DHCP

La página **DHCP IP Interface** (Interfaz IP DHCP) especifica qué clientes DHCP están conectados al dispositivo.

Para abrir la página **DHCP IP Interface** (Interfaz IP DHCP), haga clic en **System**→ **IP Addressing**→ **DHCP IP Interface** (Sistema→ Direccionamiento IP→ Interfaz IP DHCP) en la *vista de árbol*.

Ilustración 6-26. DHCP IP Interface (Interfaz IP DHCP)



La página **DHCP IP Interface** (Interfaz IP DHCP) contiene los siguientes campos:

Interface (Interfaz): interfaz específica conectada al dispositivo. Haga clic en el botón de opción que hay al lado de **Port** (Puerto), **LAG** o **VLAN** y seleccione la interfaz conectada al dispositivo.

Host Name (Nombre del sistema principal): nombre del sistema.

Remove (Eliminar): si se selecciona esta opción, se eliminan los clientes DHCP.

Adición de clientes DHCP

1. Abra la página **DHCP IP Interface** (Interfaz IP DHCP).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add DHCP IP Interface** (Agregar interfaz IP DHCP).
3. Complete la información de la página y haga clic en **Apply Changes** (Aplicar cambios).

Se agrega la interfaz DHCP y el dispositivo se actualiza.

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).

La entrada se modifica y el dispositivo se actualiza.

Supresión de una interfaz IP DHCP

1. Abra la página **DHCP IP Interface** (Interfaz IP DHCP).
2. Haga clic en **Show All** (Mostrar todo) para abrir la página **DHCP IP Interface Table** (Tabla de interfaces IP DHCP).
3. Seleccione una entrada de cliente DHCP.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se suprime y el dispositivo se actualiza.

Definición de las interfaces IP DHCP mediante los comandos de la CLI

La siguiente tabla contiene el comando de la CLI para definir los clientes DHCP.

Tabla 6-19. Comandos de la CLI para la interfaz IP DHCP

Comando de la CLI	Descripción
`ip address dhcp [hostname` *`nombre_sistema_principal`*`]`	Para adquirir una dirección IP en una interfaz Ethernet a partir del DHCP (Dynamic Host Configuration Protocol o protocolo de configuración dinámica del host)

A continuación se muestra un ejemplo del comando de la CLI:

```
Console (config-if)# ip address dhcp hostname LA01
```

Configuración de sistemas de nombres de dominio

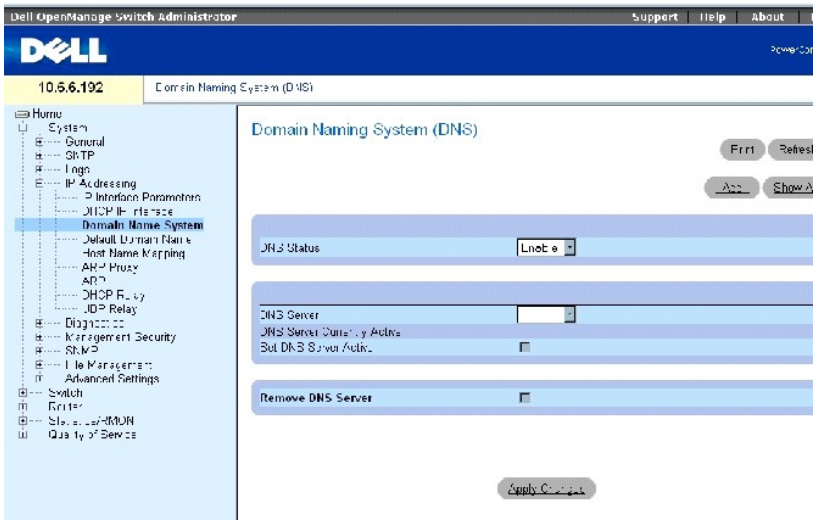
El DNS (Sistema de nombres de dominio) convierte los nombres de dominio definidos por el usuario en las direcciones IP. Cada vez que se asigna un servicio de DNS a un nombre de dominio, el nombre se convierte en una dirección IP numérica. Por ejemplo, www.ipexample.com se convierte en 192.87.56.2. Los

servidores DNS conservan las bases de datos de nombres de dominios y las direcciones IP correspondientes.

La página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]) contiene campos para habilitar y activar determinados servidores DNS.

Para abrir la página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]), haga clic en **System**→ **IP Addressing**→ **Domain Name System** (Sistema→ Direccionamiento IP→ Sistema de nombres de dominio) en la *vista de árbol*.

Ilustración 6-27. Domain Naming System (DNS) (DNS [Sistema de nombres de dominio])



La página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]) contiene los siguientes campos:

DNS Status (Estado DNS): activa o desactiva el paso de nombres DNS a direcciones IP.

DNS Server (Servidor DNS): contiene una lista de servidores DNS. Los servidores DNS se agregan a la página **Add DNS Server** (Agregar servidor DNS).

DNS Server Currently Active (Servidor DNS actualmente activo): el servidor DNS que está actualmente activo.

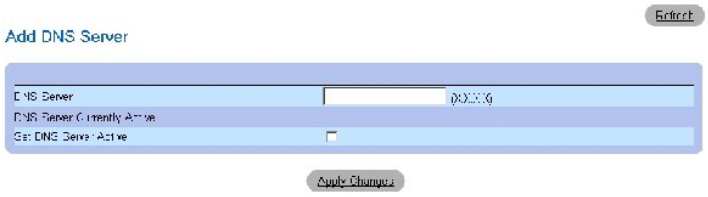
Remove DNS Server (Eliminar servidor DNS): si esta opción está seleccionada, se elimina el servidor DNS seleccionado.

Adición de un servidor DNS

1. Abra la página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add DNS Server** (Agregar servidor DNS):

Ilustración 6-28. Add DNS Server (Agregar servidor DNS)



La página **Add DNS Server**(Agregar servidor DNS) contiene los siguientes campos:

DNS Server (Servidor DNS): especifica la dirección IP del servidor DNS.

DNS Server Currently Active (Servidor DNS actualmente activo): indica el servidor DNS que está actualmente activo.

Set DNS Server Active (Establecer el servidor DNS activo): seleccione la casilla de verificación para definir el servidor DNS como el servidor DNS activo.

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

El nuevo servidor DNS se definirá y el dispositivo se actualizará.

Visualización de la tabla de servidores DNS

1. Abra la página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **DNS Server Table** (Tabla de servidores DNS):

Ilustración 6-29. DNS Server Table (Tabla de servidores DNS)

Eliminación de servidores DNS

1. Abra la página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]).
2. Haga clic en **Show All** (Mostrar todo).
3. Se abre la página **DNS Server Table** (Tabla de servidores DNS).
4. Seleccione una *entrada* de la **DNS Server Table** (Tabla de servidores DNS).
5. Seleccione la casilla de verificación **Remove** (Eliminar).
6. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor DNS seleccionado se suprimirá y el dispositivo se actualizará.

Configuración de los servidores DNS mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para configurar servidores DNS.

Tabla 6-20. Comandos de la CLI para el servidor DNS

Comando de la CLI	Descripción
ip name-server *dirección_servidor*	Establece los servidores de nombres disponibles. Se pueden establecer hasta ocho servidores de nombres.
no ip name-server *dirección_servidor*	Elimina un servidor de nombres.
ip domain-name *nombre*	Define un nombre de dominio predeterminado que el software utiliza para completar nombres de sistemas principales no calificados. (Intervalo: 1-158 caracteres)
no ip domain-name	Suprime el nombre de dominio predeterminado (DNS).
clear host {name | *}	Suprime entradas de la caché de nombres de sistemas principales a direcciones.
show hosts [*nombre*]	Muestra el nombre del dominio predeterminado, la lista de sistemas principales de servidores de nombres, así como la lista de nombres y direcciones de sistemas principales estáticas y en caché.
ip domain-lookup	Habilita el sistema DNS para la conversión de nombres de sistemas principales en direcciones IP.
no ip domain-lookup	Inhabilita el sistema DNS para la conversión de nombres de sistemas principales en direcciones IP.

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

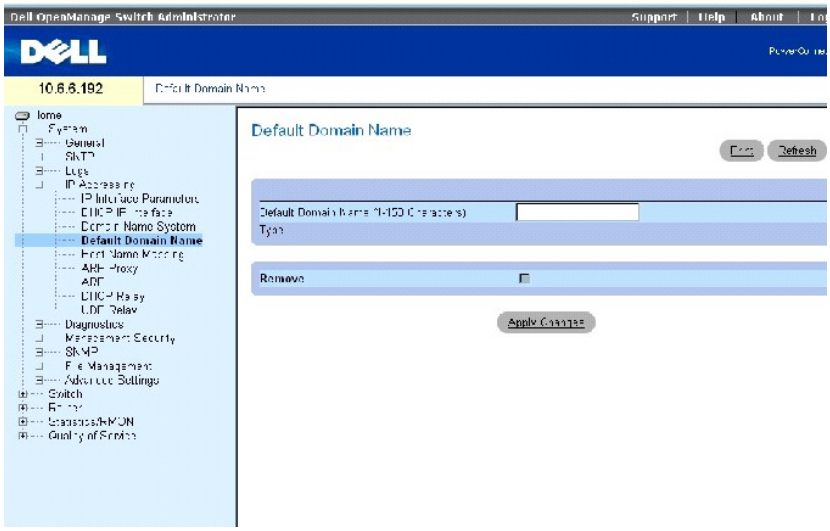
```
Console (config)# ip name-server 176.16.1.18
```

Definición de los dominios predeterminados

La página **Default Domain Name** (Nombre de dominio predeterminado) proporciona información para definir nombres de dominio DNS predeterminados.

Para abrir la página **Default Domain Name** (Nombre de dominio predeterminado), haga clic en **System**→ **IP Addressing**→ **Default Domain Name** (Sistema→ Direccionamiento IP→ Nombre de dominio predeterminado).

Ilustración 6-30. Default Domain Name (Nombre de dominio predeterminado)



La página **Default Domain Name** (Nombre de dominio predeterminado) contiene los siguientes campos:

Default Domain Name (1-158 characters) (Nombre de dominio predeterminado [1 - 158 caracteres]): contiene un servidor de nombres de dominio DNS definido por el usuario. Cuando se configura, el nombre de dominio predeterminado se aplica a todos los nombres de sistemas principales no calificados.

Type (Tipo): indica que el nombre de dominio predeterminado se ha creado estática o dinámicamente.

Remove (Eliminar): si se selecciona esta opción, se elimina el nombre de dominio predeterminado.

Definición de los nombres de dominio DNS mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para configurar nombres de dominio DNS.

Tabla 6-21. Comandos de la CLI para el nombre de dominio DNS

Comando de la CLI	Descripción
ip domain-name *nombre*	Define un nombre de dominio predeterminado que el software utiliza para completar nombres de sistemas principales no calificados.
no ip domain-name	Suprime el nombre de dominio predeterminado (DNS)
show hosts [*nombre*]	Muestra el nombre del dominio predeterminado, la lista de sistemas principales de servidores de nombres, así como la lista de nombres y direcciones de sistemas principales estáticas y en caché.

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

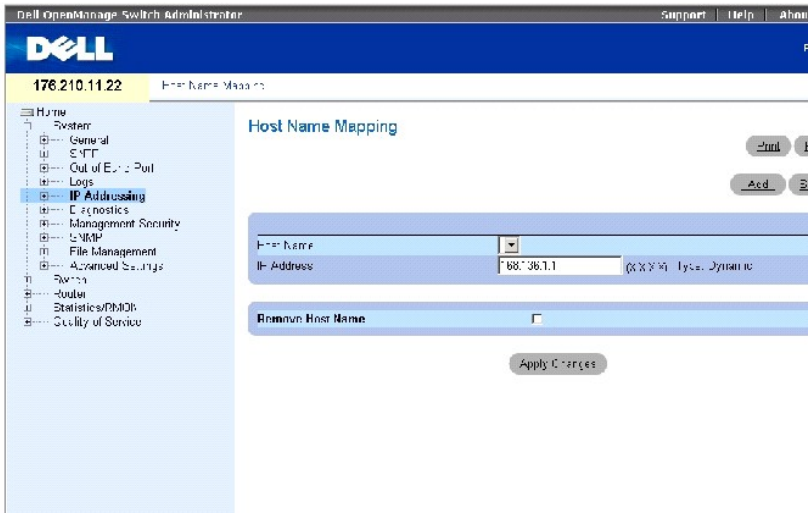
```
Console (config)# ip domain-name dell.com
```

Asignación del sistema principal del dominio

La página **Host Name Mapping** (Asignación de nombres de sistemas principales) proporciona parámetros para asignar una dirección IP a un nombre de sistema principal estático. La página **Host Name Mapping** (Asignación de nombres de sistemas principales) proporciona una dirección IP por sistema principal.

Para abrir la página **Host Name Mapping** (Asignación de nombres de sistemas principales), haga clic en **System→ IP Addressing→ Host Name Mapping** (Sistema→ Direccionamiento IP→ Asignación de nombres de sistemas principales).

Ilustración 6-31. Host Name Mapping (Asignación de nombres de sistemas principales)



La página **Host Name Mapping** (Asignación de nombres de sistemas principales) contiene los siguientes campos:

Host Name (Nombre de sistema principal): contiene una lista de nombres de sistemas principales. Los nombres de sistemas principales se definen en la página **Add Host Name Mapping** (Agregar asignación de nombres de sistemas principales). Cada sistema principal proporciona una dirección IP.

IP Address (X.X.X.X) (Dirección IP [X.X.X.X]): proporciona una dirección IP que está asignada al nombre del sistema principal especificado.

Type (Tipo): tipo de dirección IP. Los valores de campo posibles son:

Dynamic (Dinámica): la dirección IP se ha creado dinámicamente.

Static (Estática): la dirección IP es una dirección estática.

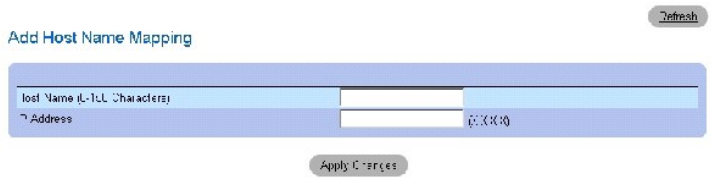
Remove Host Name Mapping (Eliminar asignación de nombres de sistemas principales): si se selecciona esta opción, se elimina la asignación de sistemas principales DNS.

Adición de nombres de dominios de sistemas principales

1. Abra la página **Host Name Mapping** (Asignación de nombres de sistemas principales).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add Host Name Mapping** (Agregar asignación de nombres de sistemas principales):

Ilustración 6-32. Add Host Name Mapping (Agregar asignación de nombres de sistemas principales)



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

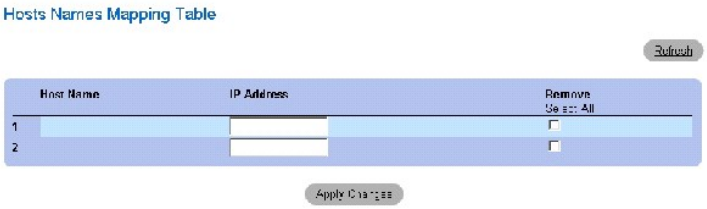
La dirección IP se asignará al nombre del sistema principal y el dispositivo se actualizará.

Visualización de la tabla de asignación de nombres de sistemas principales

1. Abra la página **Host Name Mapping** (Asignación de nombres de sistemas principales).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Host Name Mapping Table** (Tabla de asignación de nombres de sistemas principales):

Ilustración 6-33. Host Name Mapping Table (Tabla de asignación de nombres de sistemas principales)



Eliminación de un nombre de sistema principal de la asignación de direcciones IP

1. Abra la página **Host Name Mapping** (Asignación de nombres de sistemas principales).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Host Name Mapping Table** (Tabla de asignación de nombres de sistemas principales):

3. Seleccione una entrada de la **Host Name Mapping Table** (Tabla de asignación de nombres de sistemas principales).
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la **Host Name Mapping Table** (Tabla de asignación de sistemas principales) se suprimirá y el dispositivo se actualizará.

Asignación de una dirección IP a nombres de sistemas principales del dominio mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar nombres de sistemas principales del dominio a las direcciones IP.

Tabla 6-22. Comandos de la CLI para los nombres de los sistemas principales del dominio

Comando de la CLI	Descripción
	Define la asignación estática de nombres de sistemas principales a direcciones en la caché de los sistemas principales.

ip host nombre dirección	
no ip host name	Elimina la asignación de nombres a direcciones.
clear host {name | *}	Suprime entradas de la caché de nombres de sistemas principales a direcciones.
clear host dhcp {name | *}	Suprime entradas de la caché de nombres de sistemas principales a direcciones que se reciben del DHCP (Dynamic Host Configuration Protocol).
show hosts [*nombre*]	Muestra el nombre del dominio predeterminado, la lista de sistemas principales de servidores de nombres, así como la lista de nombres y direcciones de sistemas principales estáticas y en caché.

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

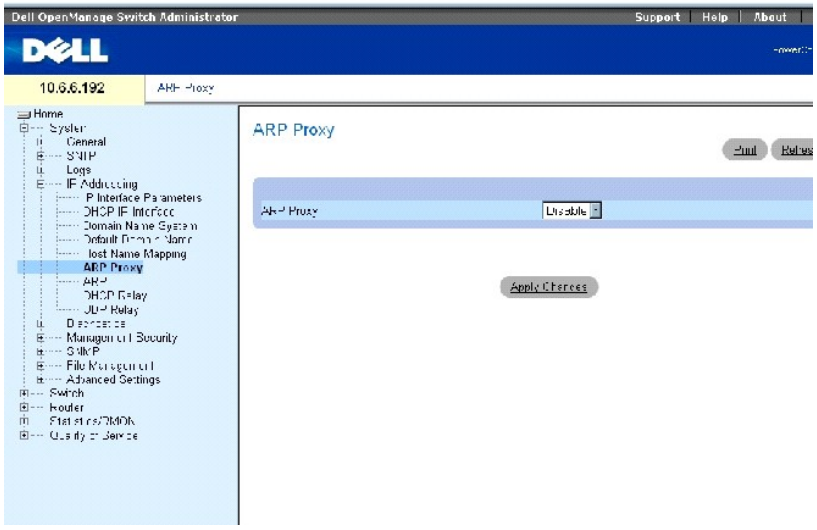
```
Console (config)# ip host accounting.abc.com 176.10.23.1
```

Activación del proxy ARP

El Protocolo de resolución de direcciones (ARP) es un protocolo TCP/IP que convierte las direcciones IP en direcciones físicas. La página **ARP Proxy** (Proxy ARP) permite que los administradores de red activen el proxy ARP en el conmutador.

Para abrir la página **ARP Proxy** (Proxy ARP), haga clic en **System**→ **IP Addressing**→ **ARP Proxy** (Sistema→ Direccionamiento IP→ Proxy ARP) en la *vista de árbol.*

Ilustración 6-34. ARP Proxy (Proxy ARP)



El campo **ARP Proxy** (Proxy ARP) permite que el dispositivo responda a las peticiones ARP de nodos localizados. Si está desactivado, el dispositivo responde con su propia dirección MAC.

Activación de ARP

1. Abra la página **ARP Proxy** (Proxy ARP).
2. Seleccione **Enabled** (Activado) en el campo **ARP Proxy** (Proxy ARP).

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

El proxy ARP se activa en el dispositivo.

Activación del proxy ARP mediante comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para activar el proxy ARP.

Tabla 6-23. Comandos de la CLI para el proxy ARP

Comando de la CLI	Descripción
`ip proxy-arp`	Activa el proxy ARP
`no ip proxy-arp`	Desactiva el proxy ARP

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

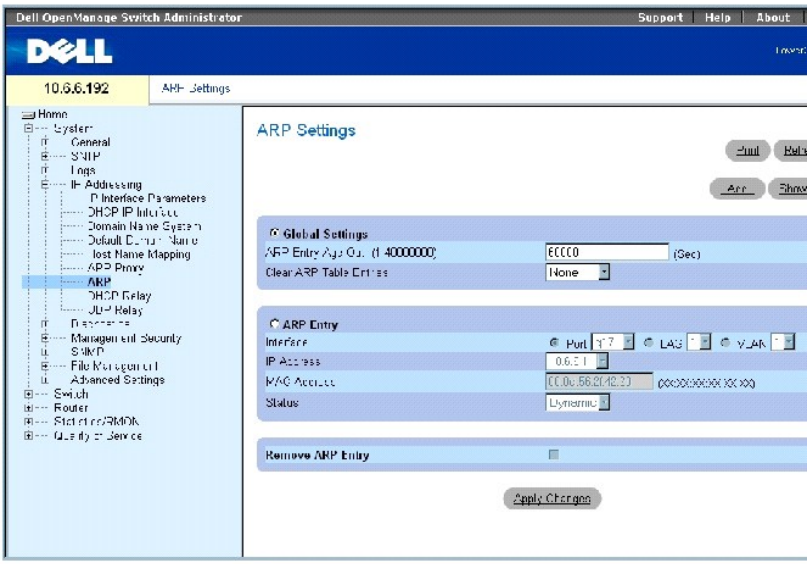
```
Console (config)# ip proxy-arp
```

Definición de la configuración de ARP

Utilice la página **ARP Settings** (Configuración de ARP) para definir los parámetros de ARP de una interfaz IP. La tabla de ARP se utiliza para mantener una correlación entre cada una de las direcciones MAC y su correspondiente dirección IP. El usuario puede rellenar la tabla de ARP estáticamente. Cuando se define una entrada de ARP estática, se pone una entrada permanente en la tabla, que el sistema utiliza para convertir las direcciones IP en direcciones MAC.

Para abrir la página **ARP Settings** (Configuración de ARP), haga clic en **System**→ **IP Addressing**→ **ARP** (Sistema→ Direccionamiento IP→ ARP) en la *vista de árbol*.

Ilustración 6-35. ARP Settings (Configuración de ARP)



La página **ARP Settings** (Configuración de ARP) contiene los siguientes campos:

Global Settings (Configuración global): seleccione esta opción para activar los campos de la configuración global de ARP.

ARP Entry Age Out (0- 40000000) (Caducidad de entrada de ARP [0-4000000]): para todos los dispositivos, la cantidad de tiempo (en segundos) que pasa entre las peticiones ARP sobre una entrada de tabla de ARP. Después de este período, la entrada se elimina de la tabla. El intervalo es 0 - 4000000, donde cero indica que las entradas nunca se borran de la caché.

Clear ARP Table Entries (Borrar entradas de la tabla de ARP): el tipo de entradas de ARP que se borran en todos los dispositivos. Los valores posibles son:

None (Ninguna): las entradas de ARP no se borran.

All (Todas): todas las entradas de ARP se borran.

Dynamic (Dinámicas): sólo las entradas dinámicas de ARP se borran.

Static (Estáticas): sólo las entradas estáticas de ARP se borran.

ARP Entry (Entrada de ARP): seleccione esta opción para activar los campos para la configuración de ARP en un solo dispositivo.

Interface (Interfaz): el número de interfaz del puerto, LAG o VLAN que se conecta al dispositivo.

IP Address (Dirección IP): la dirección IP de la estación, que está asociada a la dirección MAC que aparece a continuación.

MAC Address (Dirección MAC): la dirección MAC de la estación, que está asociada a la tabla de ARP con la dirección IP.

Status (Estado): el estado de las entradas de la ARP Table (Tabla de ARP). Los valores posibles del campo son:

Other (Otro): la entrada de ARP no se obtiene de forma dinámica ni es una entrada estática.

Invalid (No válida): la entrada de ARP no es válida.

Dynamic (Dinámica): la entrada de ARP se ha obtenido de forma dinámica.

Static (Estática): la entrada de ARP es una entrada estática.

Remove ARP Entry (Eliminar entrada de ARP): si se selecciona esta opción, se elimina una entrada de ARP.

Adición de una entrada de tabla de ARP

1. Abra la página **ARP Settings** (Configuración de ARP).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add ARP Entry** (Agregar entrada de ARP).

Ilustración 6-36. Página Add ARP Entry (Agregar entrada de ARP)

3. Seleccione una interfaz y complete los campos de la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se agrega la entrada estática de tabla de ARP y el dispositivo se actualiza.

Modificación de una entrada de tabla de ARP

1. Abra la página **ARP Settings** (Configuración de ARP).
2. Seleccione una entrada de la tabla.
3. Modifique los campos obligatorios de un determinada interfaz.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la entrada estática **ARP Table** (Tabla de ARP) y el dispositivo se actualiza.

Supresión de una entrada de tabla de ARP

1. Abra la página **ARP Settings** (Configuración de ARP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **ARP Table** (Tabla de ARP).
3. Seleccione una entrada de la tabla.
4. Seleccione **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la tabla se suprime y el dispositivo se actualiza.

Configuración de ARP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar el ARP.

Tabla 6-24. Comandos de la CLI para la configuración de ARP

Comando de la CLI	Descripción
`arp` *`dirección_ip dirección_hw`* {`ethernet interface- number | vlan` *`id_vlan`* `| port-channel number | out-of-band-eth oob- interface`}	Para agregar una entrada permanente en la caché de ARP (Address Resolution Protocol o protocolo de resolución de direcciones).
`arp timeout`	Para configurar durante cuánto tiempo permanece una entrada en la caché de ARP.
`show arp`	Para visualizar las entradas de la tabla de ARP.

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

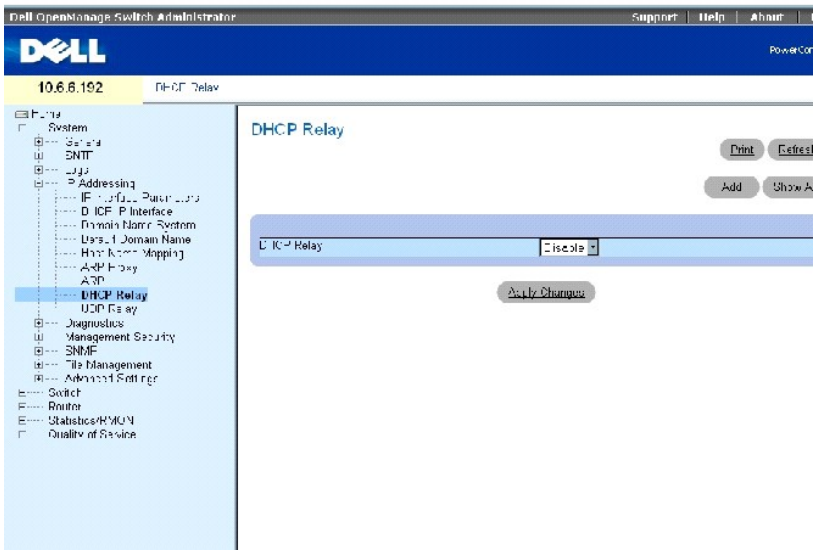
```
Console (config)# arp timeout 5


Console (config)# arp 10.1.1.1 0060.704C.73FF ethernet g5


Console# show arp


Interface  IP Address  HW Address      Status


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


g20        10.1.1.1    0060.704c.73ff  dynamic
```

Definición de los parámetros del relé DHCP

Utilice la página **DHCP Relay** (Relé DHCP) para proporcionar información con objeto de establecer una configuración DHCP con varios servidores DHCP para garantizar la redundancia. Las direcciones IP se controlan y distribuyen de una en una para evitar sobrecargar el dispositivo.

Para abrir la página **DHCP Relay** (Relé DHCP), haga clic en **System**→ **IP Addressing**→ **DHCP Relay** (Sistema→ Direccionamiento IP→ Relé DHCP) en la *vista de árbol*.

Ilustración 6-37. DHCP Relay (Relé DHCP)



Activación del relé DHCP

1. Abra la página **DHCP Relay** (Relé DHCP).
2. Seleccione **Enable** (Activar) en el menú descendente **DHCP Relay** (Relé DHCP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada **DHCP Relay** (Relé DHCP) se agrega a la tabla de relé DHCP.

Adición de una entrada de relé DHCP

1. Abra la página **DHCP Relay** (Relé DHCP).
2. Haga clic en **Add** (Agregar) para abrir la página **Add DHCP Server** (Agregar un servidor DHCP).
3. Introduzca un **valor** en la opción **New DHCP Server** (Nuevo servidor DHCP).

   Los servidores DHCP funcionan como un relé si este parámetro no es igual a 0.0.0.0. Las peticiones DHCP únicamente se retransmiten si su campo SEC es superior o igual al valor umbral. Esto permite que los servidores DHCP locales respondan primero.
4. Haga clic en **Apply Changes** (Aplicar cambios).

   El servidor DHCP se agrega a la tabla de relé DHCP.

Supresión de una entrada de la tabla de relé DHCP

1. Abra la página **DHCP Relay** (Relé DHCP).
2. Haga clic en **Show All** (Mostrar todo) para abrir la página **DHCP Servers Table** (Tabla de servidores DHCP).
3. Seleccione un **servidor DHCP** y marque la casilla **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

   La entrada se suprime y el dispositivo se actualiza.

Definición de servidores de relé DHCP mediante comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir los servidores de relé DHCP.

Tabla 6-25. Comandos de la CLI para los servidores de relé DHCP

Comando de la CLI	Descripción
`ip dhcp relay enable`	Activa las funciones del relé DHCP (Dynamic Host Configuration Protocol o protocolo de configuración dinámica del host) en el enrutador.
`ip dhcp relay address` *`dirección_ip`*	Establece los servidores DHCP disponibles para el relé DHCP.

A continuación se muestra un ejemplo de un comando de la CLI para activar el servicio de relé DHCP:

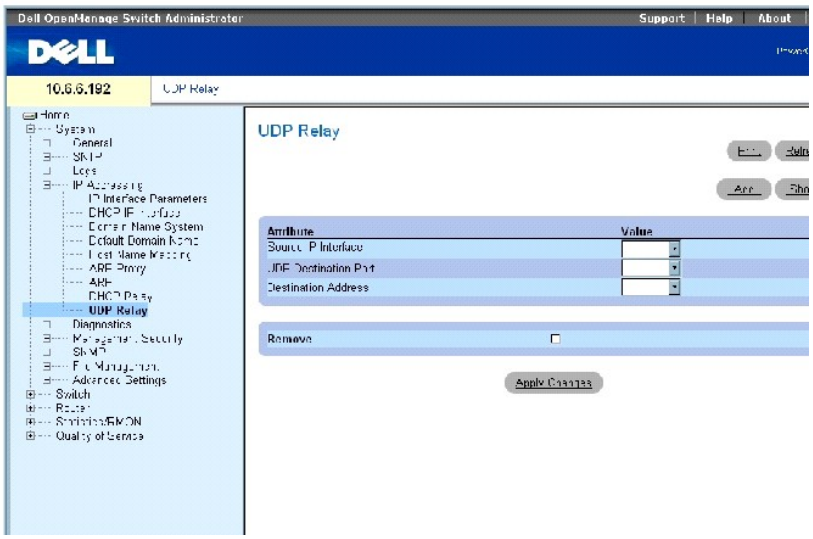
```
Console (config)# ip dhcp relay enable
```

Configuración del relé UDP

El relé UDP permite que los paquetes UDP lleguen a otras redes. Esta función permite buscar desde estaciones de trabajo a servidores en redes diferentes.

Para abrir la página **UDP Relay** (Relé UDP), haga clic en **System**→ **IP Addressing**→ **UDP Relay** (Sistema→ Direccionamiento IP→ Relé UDP) en la *vista de árbol.*

Ilustración 6-38. UDP Relay (Relé UDP)



La página **UDP Relay** (Relé UDP) contiene los siguientes campos:

Source IP Interface (Interfaz IP de origen): la interfaz IP de entrada que retransmite los paquetes UDP. Si este campo es 255.255.255.255, se retransmiten los paquetes UDP de todas las interfaces. Los siguientes intervalos de dirección no son válidos:

de 0.0.0.0 a 0.255.255.255.

de 127.0.0.0 a 127.255.255.255.

UDP Destination Port (1-65535) (Puerto de destino UDP [1-65535]): el número de identificación del puerto UDP de destino de los paquetes UDP que se van a retransmitir. En la siguiente tabla se muestra una lista de las asignaciones de puertos UDP.

Tabla 6-26. Asignaciones de puertos UDP

Número de puerto UDP	Sigla	Aplicación
7	Echo	Echo
11	SysStat	Usuario activo
15	NetStat	Estado de la red
17	Quote	Cita del día
19	CHARGEN	Generador de caracteres
20	FTP-data	Datos de FTP
21	FTP	FTP
37	Time	Hora
42	NAMESERVER	Servidor de nombres de sistema principal
43	NICNAME	Quién está conectado actualmente
53	DOMAIN	Servidor de nombres de dominio
69	TFTP	Protocolo trivial de transferencia de archivos
111	SUNRPC	Rpc de Sun Microsystems
123	NTP	Hora de la red
137	NetBiosNameService	Conexiones del servidor NT a la estación
138	NetBiosDatagramService	Conexiones del servidor NT a la estación
139	NetBios	Conexiones del servidor SessionService NT a la estación
161	SNMP	Administración de red simple
162	SNMP-trap	Capturas de gestión de red simple
513	who	Daemon Rwho de Unix
514	syslog	Registro del sistema

525	timed	Daemon de la hora

Destination Address (Dirección de destino): la interfaz IP que recibe los relés de paquetes UDP. Si este campo es 0.0.0.0, los paquetes UDP se rechazan. Si este campo es 255.255.255.255, los paquetes UDP se dirigen a todas las interfaces IP.

Adición de una entrada de relé UDP

1. Abra la página **UDP Relay** (Relé UDP).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add UDP Relay** (Agregar un relé UDP).
3. Especifique la dirección IP del servidor UDP en el campo **UDP Destination Port** (Puerto de destino UDP).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor DHCP se agrega a la tabla de relé DHCP.

Modificación de una entrada de la tabla de relé UDP

NOTA: Si el relé UDP está activado, pero no se ha especificado ningún número de puerto UDP, el dispositivo reenvía de manera predeterminada paquetes de difusión UDP para los siguientes servicios: IEN-116 Name Service (puerto 42), DNS (puerto 53), NetBIOS Name Server (puerto 137), NetBIOS Datagram Server (puerto 138), TACACS Server (puerto 49) y Time Service (puerto 37)

1. Abra la página **UDP Relay** (Relé UDP).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada de UDP se agrega a la tabla **UDP Relay** (Relé UDP) y el dispositivo se actualiza.

Supresión de una entrada de la tabla de relé UDP

1. Abra la página **UDP Relay** (Relé UDP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **UDP Relay Table** (Tabla de relé de UDP).
3. Seleccione un servidor de relé UDP y marque la casilla **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se suprime y el dispositivo se actualiza.

Configuración de la tabla de relé UDP mediante los comandos de la CLI

La siguiente tabla contiene el comando de la CLI para configurar el relé UDP.

Tabla 6-27. Comandos de la CLI para el relé UDP

Comando de la CLI	Descripción
helper-address *dirección* [*lista_puerto_udp*]	Activa el reenvío de las difusiones UDP (User Datagram Protocol) que se han recibido en una interfaz. Este comando no activa el reenvío de paquetes mediante BOOTP/DHCP. Para reenviar paquetes mediante BOOTP/DHCP, utilice los comandos de relé **ip dhcp relay enable**, **ip dhcp relay address** y **show ip dhcp**. Para obtener información acerca de estos comandos, consulte el apartado **Definición de los parámetros del relé DHCP** .

A continuación se muestra un ejemplo del comando de la CLI:

```
Console (config-ip)# helper-address 172.16.9.9 49 53
```

Ejecución de los diagnósticos de los cables

Utilice la página **Diagnostics** (Diagnósticos) con objeto de realizar pruebas virtuales de cables para cables de cobre y fibra óptica.

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

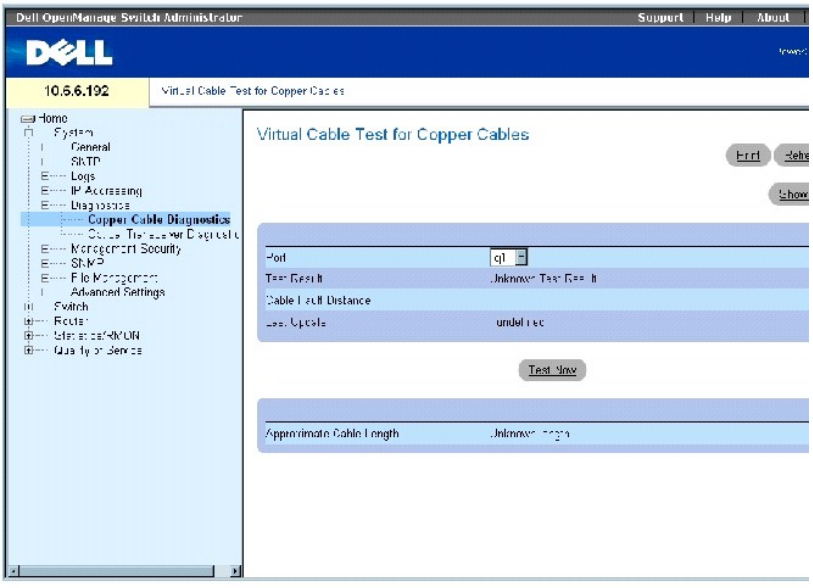
La página **Diagnostics** (Diagnósticos) contiene enlaces con páginas de diagnósticos para cables de cobre y transceptores ópticos.

Visualización de los diagnósticos de los cables de cobre

Utilice la página **Virtual Cable Test for Copper Cables** (Prueba virtual de cable para cables de cobre) para realizar pruebas en cables de cobre. Las pruebas de cables proporcionan información sobre dónde se producen errores en el cable, la última vez que se realizó una prueba de cable, y el tipo de error de cable que se produjo. En las pruebas se utiliza la tecnología de reflectometría de dominio temporal (TDR) para probar la calidad y las características de un cable de cobre conectado a un puerto. Se pueden probar cables de hasta 120 metros de longitud. Los cables se prueban cuando los puertos están inactivos, con la excepción de la prueba de longitud aproximada del cable.

Para abrir la página **Virtual Cable Test for Copper Cables** (Prueba virtual de cable para cables de cobre), haga clic en **System**→ **Diagnostics**→ **Copper Cable Diagnostics** (Sistema→ Diagnósticos→ Diagnósticos de cables de cobre) en la *vista de árbol.*

Ilustración 6-39. Virtual Cable Test for Copper Cables (Prueba virtual de cable para cables de cobre)



La página **Virtual Cable Test for Copper Cables** (Prueba virtual de cable para cables de cobre) contiene los siguientes campos:

Port (Puerto): el puerto al cual se conecta el cable.

Test Result (Resultado de la prueba): los resultados de la prueba de cable. Los valores posibles son:

No Cable (Sin cable): no hay ningún cable conectado al puerto.

Open Cable (Cable abierto): el cable está abierto.

Short Cable (Cable cortocircuitado): se ha producido un cortocircuito en el cable.

OK (Aceptar): el cable ha pasado la prueba.

Fiber Cable (Cable de fibra): un cable de fibra se ha conectado al puerto.

Cable Fault Distance (Distancia de error del cable): distancia desde el puerto en el que se ha producido el error del cable.

Last Update (Última actualización): la última vez que se ha probado el puerto.

Approximate Cable Length (Longitud aproximada del cable): longitud aproximada del cable. Esta prueba sólo se puede realizar cuando el puerto está activo y funciona a 1 gbps.

Ejecución de una prueba de cable

1. Asegúrese de que ambos extremos del cable de cobre estén conectados a un dispositivo.
2. Abra la página **Virtual Cable Test for Copper Cables** (Prueba virtual de cable para cables de cobre).
3. Haga clic en **Test Now** (Probar ahora).

La prueba de cables de cobre se efectuará y los resultados se mostrarán en la página **Virtual Cable Test for Copper Cables** (Prueba virtual de cable para cables de cobre).

Visualización de la tabla de resultados de la prueba de cable virtual

1. Abra la página **Virtual Cable Test for Copper Cables** (Prueba virtual de cable para cables de cobre).
2. Haga clic en **Show All** (Mostrar todo) para ejecutar las pruebas y mostrar la página **Virtual Cable Test Results Table** (Tabla de resultados de la prueba virtual de cable).

Ejecución de las pruebas de cables de cobre mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para realizar las pruebas de cables de cobre.

Tabla 6-28. Comandos de la CLI para la prueba de cables de cobre

Comando de la CLI	Descripción
`test copper-port tdr` *`interfaz`*	Realiza las pruebas VCT.
`show copper-port tdr` *`interfaz`*	Muestra los resultados de las últimas pruebas VCT realizadas en los puertos.
`show copper-port cable-length` *`interfaz`*	Muestra la longitud estimada del cable de cobre conectado a un puerto.

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

```
Console# show copper-ports cable-length
```

```
Port  Length [meters]

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

g1    < 50

g2    Copper not active

g3    110-140

g4    Fiber
```

NOTA: La longitud de cable que devuelve VCT es una aproximación en intervalos de hasta 50 metros, 50m- 80m, 80m-110m, 110m-120m o más de 120m. La variación puede ser de hasta 20 metros, y la medición de la longitud del cable no funcionará para conexiones de 10 Mbps.

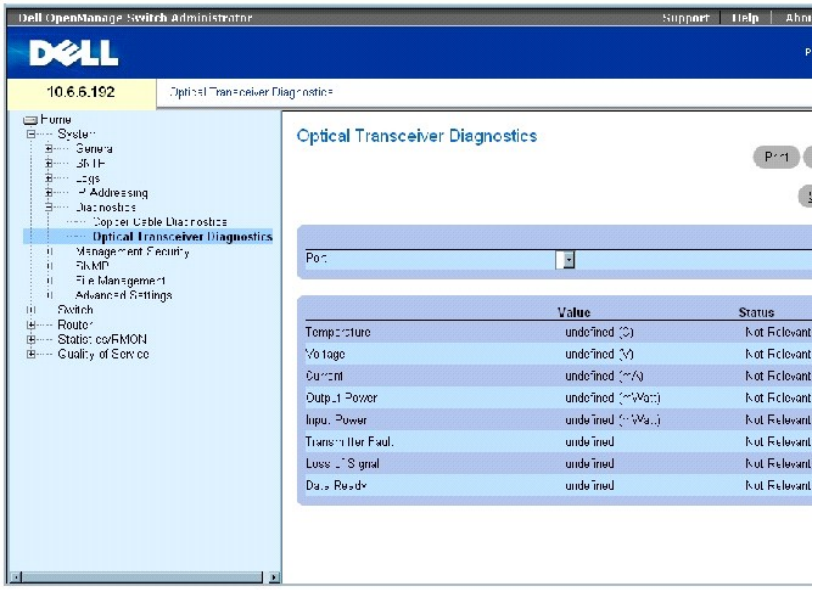
Visualización de los diagnósticos del transceptor óptico

Utilice la página **Optical Transceiver Diagnostics** (Diagnósticos del transceptor óptico) para realizar pruebas en cables de fibra óptica.

Para abrir la página **Optical Transceiver Diagnostics** (Diagnósticos del transceptor óptico), haga clic en **System**→ **Diagnostics**→ **Optical Transceiver Diagnostics** (Sistema→ Diagnósticos→ Diagnósticos del transceptor óptico) en la *vista de árbol.*

NOTA: Los diagnósticos del transceptor óptico sólo se pueden realizar cuando el enlace está presente.

Ilustración 6-40. Optical Transceiver Diagnostics (Diagnósticos del transceptor óptico)



La página **Optical Transceiver Diagnostics** (Diagnósticos del transceptor óptico) contiene los siguientes campos:

Port (Puerto): la dirección IP del puerto en el que se prueba el cable.

Temperature (Temperatura): la temperatura (C) a la que funciona el cable.

Voltage (Voltaje): voltaje al que funciona el cable.

Current (Actual): corriente a la que funciona el cable.

Output Power (Potencia de salida): velocidad a la que se transmite la potencia de salida.

Input Power (Potencia de entrada): velocidad a la que se transmite la potencia de entrada.

Transmitter Fault (Fallo del transmisor): indica si se ha producido un error 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): indica que el transceptor está en marcha y los datos están preparados.

Visualización de la tabla de resultados de la prueba de diagnósticos del transceptor óptico

1. Abra la página **Optical Transceiver Diagnostics** (Diagnósticos del transceptor óptico).
2. Haga clic en **Show All** (Mostrar todo) para ejecutar la prueba y abrir la **Virtual Cable Test Results Table** (Tabla de resultados de la prueba virtual de cable).

Ejecución de las pruebas de cables de fibra óptica mediante los comandos de la CLI

La siguiente tabla contiene el comando de la CLI para realizar las pruebas de cables de fibra óptica.

Tabla 6-29. Comando de la CLI para la prueba de cables de fibra óptica

Comando de la CLI	Descripción
`show fiber-ports optical- transceiver [interfaz] [detallada]`	Muestra los diagnósticos del transceptor óptico.

A continuación se muestra un ejemplo del comando de la CLI:

```
Console# show fiber-ports optical-transceiver
```

En la pantalla aparecen las siguientes columnas:

- **Temp** (Temperatura): temperatura del transceptor tomada internamente.
- **Voltage** (Voltaje): voltaje de alimentación medido internamente.
- **Current** (Corriente): corriente de polarización del transceptor medido.
- **Output Power** (Potencia de salida): potencia de salida del transceptor medida en milivatios.
- **Input Power** (Potencia de entrada): potencia recibida del receptor medida en milivatios.
- **TX Fault** (Fallo del transceptor): fallo del transmisor.

NOTA: Los transceptores de Finisar no son compatibles con las pruebas de diagnóstico de fallo del transmisor.

- **LOS**: pérdida de señal.
- **Data Ready** (Datos preparados): indica que el transceptor tiene energía archivada y que los datos están preparados.
- **N/A**: no disponible, N/S: no compatible, W: advertencia, E: error.

NOTA: La función de análisis de fibra óptica sólo funciona en SFP que son compatibles con el estándar de diagnóstico digital SFF 4872.

Gestión de la seguridad del dispositivo

Utilice la página **Management Security** (Seguridad de gestión) para establecer los parámetros de seguridad de gestión del puerto, del usuario, y de la seguridad del servidor.

Para abrir la página **Management Security** (Seguridad de gestión), haga clic en **System**→ **Management Security** (Sistema→ Seguridad de gestión) en la *vista de árbol*.

Definición de los perfiles de acceso

Utilice la página **Access Profiles** (Perfiles de acceso) para definir los perfiles y las reglas para acceder al dispositivo. Puede limitar el acceso a las funciones de gestión a los grupos de usuarios, que están definidos por las interfaces de entrada y la dirección IP o las subredes IP de origen.

El acceso de gestión se puede definir por separado para cada tipo de método de acceso de gestión, incluidos la web (HTTP), la web segura (HTTPS), Telnet y SNMP.

El acceso a diferentes métodos de gestión puede variar entre los grupos 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 las sesiones HTTPs y Telnet.

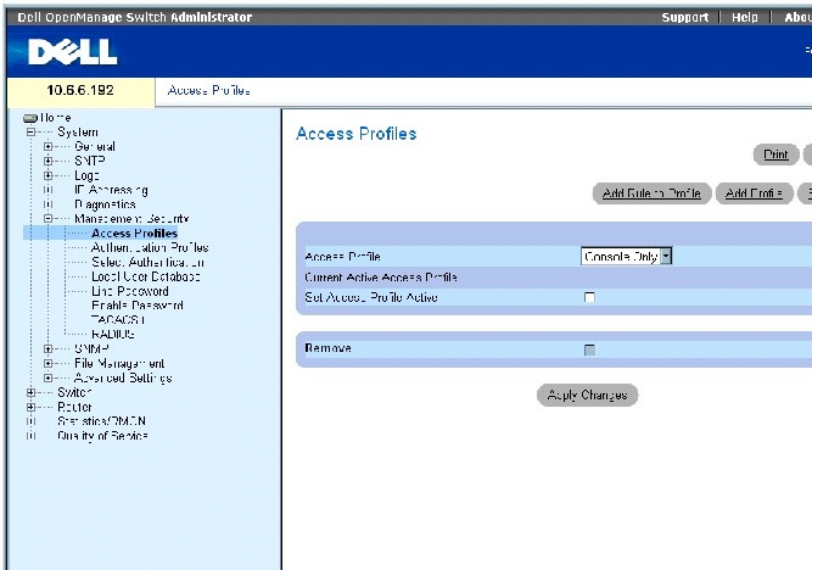
Las listas de acceso de gestión contienen las reglas que determinan cuáles son los usuarios que pueden gestionar el dispositivo, y mediante qué métodos.

También se puede bloquear a usuarios para impedir que accedan al dispositivo.

Utilice la página **Access Profiles** (Perfiles de acceso) para configurar las listas de gestión y aplicarlas a interfaces específicas.

Para abrir la página **Access Profiles** (Perfiles de acceso), haga clic en **System**→ **Management Security**→ **Access Profiles** (Sistema→ Seguridad de gestión→ Perfiles de acceso) en la *vista de árbol.*

Ilustración 6-41. Access Profiles (Perfiles de acceso)



Access Profile (Perfil de acceso): contiene una lista de todos los perfiles de acceso. El valor predeterminado es **Console Only** (Sólo consola), al que se agregan los perfiles de acceso definidos por el usuario. Si se selecciona **Console Only** (Sólo consola) como el nombre **Access Profile** (Perfil de acceso), se desconecta la sesión, y se activa el acceso al dispositivo sólo desde la consola.

Current Active Access Profile (Perfil de acceso activo actual): perfil de acceso que está actualmente activo.

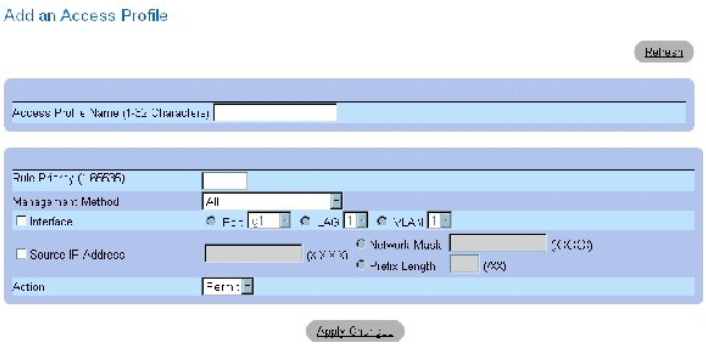
Set Access Profile Active (Establecer perfil de acceso como activo): activa un perfil de acceso.

Remove (Eliminar): si se selecciona esta opción, se elimina un perfil de acceso de la lista **Access Profile Name** (Nombre de perfil de acceso).

Adición de un perfil de acceso

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Haga clic en **Add Profile** (Agregar perfil) para abrir la página **Add an Access Profile** (Agregar un perfil de acceso).

Ilustración 6-42. Add an Access Profile (Agregar un perfil de acceso)



La página **Add an Access Profile** (Agregar un perfil de acceso) contiene los siguientes campos:

Access Profile Name (Nombre de perfil de acceso): nombre definido por el usuario para el perfil de acceso.

Rule Priority (Prioridad de reglas): indica la prioridad de las reglas. Cuando el paquete coincide con una regla, se otorga o se niega a los grupos de usuarios el acceso de gestión del dispositivo. El orden de las reglas se establece definiendo un número de regla dentro de la tabla **Profile Rules** (Reglas de perfil). El número de regla es vital para que los paquetes coincidan con las reglas, puesto que los paquetes coinciden con la primera regla a la que se ajusten. Las prioridades de las reglas se asignan en la tabla de reglas de perfil.

Management Method (Método de gestión): el método de gestión para el que se define el perfil de acceso. Los usuarios con este perfil de acceso pueden acceder al dispositivo mediante el método de gestión seleccionado.

Interface (Interfaz): tipo de interfaz a la que se aplica la regla. Se trata de un campo opcional. Puede aplicar esta regla a un puerto, LAG o VLAN seleccionados al marcar la casilla de verificación y seleccionar la interfaz y el botón de la opción adecuada.

NOTA: Asignar un perfil de acceso a una interfaz implica que se niega el acceso a través de otras interfaces. Si no se asigna ningún perfil de acceso a ninguna interfaz, todos pueden acceder al dispositivo.

Source IP Address (Dirección IP de origen): la dirección IP de origen de la interfaz a la que se aplica la regla. Se trata de un campo opcional e indica que la regla es válida para una subred.

Network Mask (Máscara de red): máscara de subred IP.

Prefix Length (Longitud del 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 gestión a la interfaz definida.

3. Escriba el nombre del perfil en el cuadro de texto **Access Profile Name** (Nombre de perfil de acceso).
4. Complete los campos y haga clic en **Apply Changes** (Aplicar cambios).

El nuevo perfil de acceso se agrega y el dispositivo se actualiza.

Activación de un perfil de acceso

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Seleccione un perfil de acceso de la lista.
3. Marque la casilla de verificación **Set Access Profile Active** (Establecer perfil de acceso como activo).
4. Haga clic en **Apply Changes** (Aplicar cambios).

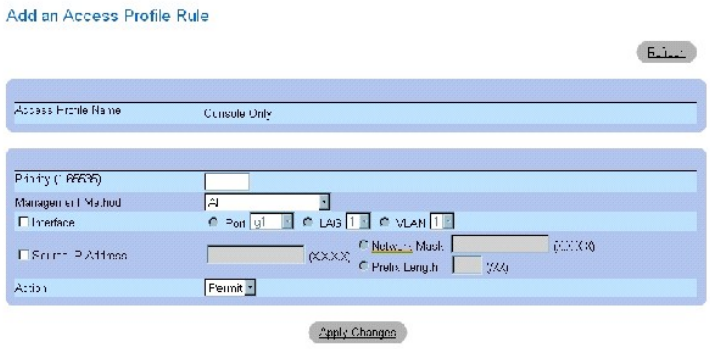
El perfil de acceso se activa para el usuario.

Adición de reglas a un perfil de acceso

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Seleccione un perfil de acceso del menú descendente.

   Éste es el perfil al que se agregan reglas cuando se abre la página **Add an Access Profile Rule** (Agregar una regla de perfil de acceso).
3. Haga clic en **Add Rule to Profile** (Agregar regla al perfil) para abrir la página **Add an Access Profile Rule** (Agregar una regla de perfil de acceso).

Ilustración 6-43. Add An Access Profile Rule (Agregar una regla de perfil de acceso)



4. Complete los campos del cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

   La regla se agrega al perfil de acceso y el dispositivo se actualiza.

Eliminación de una regla

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Profile Rules Table** (Tabla de reglas de perfil).
3. Seleccione una regla.
4. Marque la casilla de verificación **Remove** (Eliminar) y haga clic en **Apply Changes** (Aplicar cambios).

   La regla se suprime y el dispositivo se actualiza.

Definición de los perfiles de acceso mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los perfiles de acceso.

Tabla 6-30. Comandos de la CLI para perfiles de acceso

Comando de la CLI	Descripción
`management access-list` *`nombre`* **NOTA:** Ponga *n o m b r e* entre comillas dobles si contiene espacios. Por ejemplo, grupo de trabajo 1 .	Define una lista de acceso para la gestión e introduce el contexto de la lista de acceso para la configuración.
`permit [ethernet` *`número_interfaz`* `| vlan` *`id_vlan`* `| port- channel` *`número`*`]`	Establece condiciones de generación de permisos de puerto para la lista de acceso de gestión.

[service *servicio*]	
permit ip-source ip-address [mask mask | *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 de gestión y el método de gestión seleccionado.
deny [ethernet *número_interfaz* | vlan *id_vlan* | port- channel *número*] [service *servicio*]	Establece condiciones de denegación de puerto para la lista de acceso de gestión y el método de gestión seleccionado.
deny ip-source ip-address [mask mask | *longitud_prefijo*] [ethernet *número_interfaz* | vlan *id_vlan* | port-channel *número*] [service *servicio*]	Establece condiciones de denegación de puerto para la lista de acceso de gestión y el método de gestión seleccionado.
management access-class {console-only | *nombre*}	Define qué lista de acceso se utiliza como conexiones de gestión activas.
show management access-list [*nombre*]	Muestra las listas de acceso de gestión activas.
show management access-class	Muestra información sobre la clase de acceso de gestión.

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

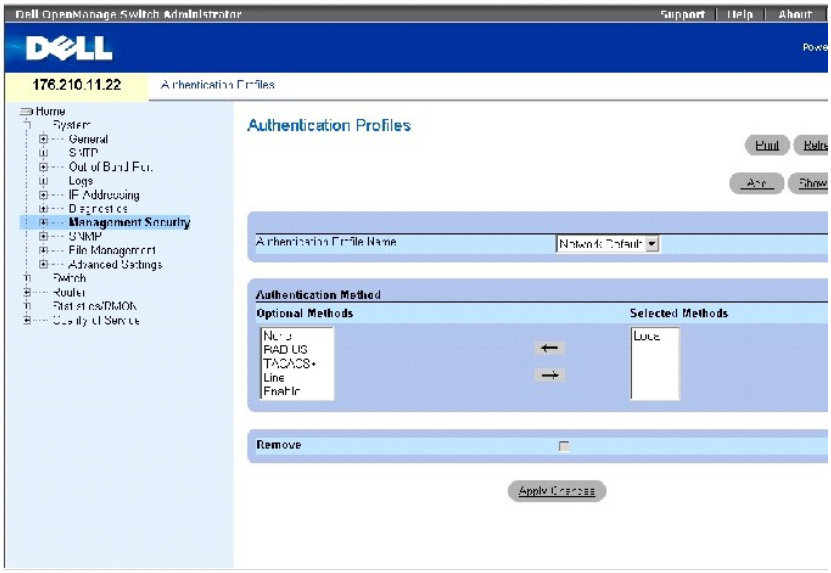
```
Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# exit

Console# show management access-class

Management access-class is enabled, using access list mlist
```

Definición de los perfiles de autenticación

La autenticación de usuarios se realiza localmente y en un servidor externo. Utilice la página **Authentication Profiles** (Perfiles de autenticación) para seleccionar el método de autenticación de usuarios en el dispositivo.

Para abrir la página **Authentication Profiles** (Perfiles de autenticación), haga clic en **System**→ **Management Security**→ **Authentication Profiles** (Sistema→ Seguridad de gestión→ Perfiles de autenticación) en la *vista de árbol*.

Ilustración 6-44. Authentication Profiles (Perfiles de autenticación)



La página **Authentication Profiles** (Perfiles de autenticación) contiene los siguientes campos:

Authentication Profile Name (Nombre de perfil de autenticación): listas de perfiles de autenticación definidos por el usuario en las que se agregan los perfiles de autenticación definidos por el usuario. Los valores predeterminados son **Network Default** (Valor predeterminado de red) y **Console Default** (Valor predeterminado de consola).

Optional Methods (Métodos opcionales): método de autenticación de usuarios. Las opciones posibles son:

None (Ninguna): no se realiza ninguna autenticación de usuario.

Local: la autenticación de usuarios se realiza en el nivel del dispositivo; el dispositivo comprueba el nombre de usuario y la contraseña para su autenticación.

RADIUS (RADIUS): la autenticación de usuarios se realiza en el servidor RADIUS. Para obtener más información sobre los servidores RADIUS, consulte el apartado Configuración de los valores de RADIUS .

TACACS+: la autenticación de usuarios se realiza en el servidor TACACS+. Para obtener más información sobre los servidores TACACS+, consulte el apartado Configuración de los valores de TACACS+ .

Line (Línea): la contraseña de línea se utiliza para la autenticación de usuarios.

Enable (Activar): la contraseña de activación se utiliza para la autenticación.

NOTA: La autenticación de usuarios se produce en el orden en el que se seleccionan los métodos. Si se produce un error durante la autenticación, se utiliza el siguiente método seleccionado. Por ejemplo, si se seleccionan las opciones **Local** y **RADIUS**, primero se autentica al usuario localmente y, a continuación, a través de un servidor externo.

Selected Methods (Métodos seleccionados): el método de autenticación seleccionado.

Adición de un perfil de autenticación

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).

2. Haga clic en **Add** (Agregar) para visualizar la página **Add Authentication Profile** (Agregar perfil de autenticación).
3. Escriba el nombre del perfil de 1-12 caracteres en el campo **Profile Name** (Nombre de perfil).

NOTA: El nombre de perfil no debe incluir espacios.

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

Se asigna un perfil de autenticación a las sesiones.

Selección de un método de autenticación

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Seleccione un elemento de la lista en el campo **Authentication Profile Name** (Nombre de perfil de autenticación).
3. Seleccione un valor de **Optional Methods** (Métodos opcionales) utilizando las flechas.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El perfil de autenticación del usuario se actualiza en el dispositivo.

Eliminación de una entrada de los perfiles de autenticación

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Authentication Profile Table** (Tabla de perfiles de autenticación):

3. Marque la casilla de verificación **Remove** (Eliminar) que hay junto al perfil que se va a eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se elimina.

Configuración de un perfil de autenticación mediante los comando de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir perfiles de autenticación.

Tabla 6-31. Comandos de la CLI para 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.
`show authentication methods`	Muestra información sobre los métodos de autenticación.

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

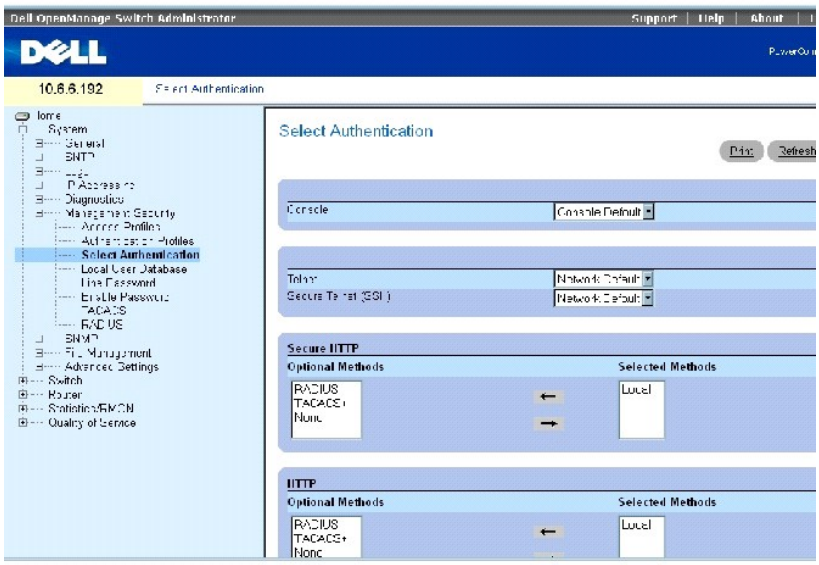
```
Console (config)# aaa authentication login default radius local enable none

Console (config)# no aaa authentication login default
```

Selección de perfiles de autenticación

Cuando los perfiles de autenticación estén definidos, se podrán aplicar a los métodos de gestión de acceso. Por ejemplo, se puede autenticar a los usuarios de consola mediante la lista de métodos de autenticación 1, mientras se autentica a los usuarios de Telnet mediante la lista de métodos de autenticación 2.

Para abrir la página **Select Authentication** (Seleccionar autenticación), haga clic en **System**→ **Management Security**→ **Select Authentication** (Sistema→ Seguridad de gestión→ Seleccionar autenticación) en la *vista de árbol*.

Ilustración 6-45. Select Authentication (Seleccionar autenticación)



La página **Select Authentication** (Seleccionar autenticación) contiene los siguientes campos:

Console (Consola): perfiles de autenticación utilizados para autenticar a los usuarios de la consola.

Telnet (Telnet): perfiles de autenticación utilizados para autenticar a los usuarios de Telnet.

Secure Telnet (SSH): perfiles de autenticación utilizados para autenticar a los usuarios de Secure Shell (SSH). SSH proporciona a los clientes conexiones remotas seguras y codificadas con un dispositivo.

HTTP (HTTP) y **Secure HTTP** (HTTP seguro): métodos de autenticación utilizados para el acceso HTTP y el acceso HTTP seguro, respectivamente. Los valores posibles del campo son:

None (Ninguno): no se utiliza ningún método de autenticación para el acceso.

Local (Local): la autenticación se realiza localmente.

RADIUS (RADIUS): la autenticación se realiza en el servidor RADIUS.

TACACS+ (TACACS+): la autenticación se realiza en el servidor TACACS+.

Local, None (Local, Ninguno): la autenticación se realiza primero localmente. Si la autenticación no se puede verificar, no se utiliza ningún método de autenticación.

RADIUS, None (RADIUS, Ninguno): la autenticación se realiza primero en el servidor RADIUS. Si la autenticación no se puede verificar, no se utiliza ningún método de autenticación.

TACACS+, None (TACACS+, Ninguno): la autenticación se realiza primero en el servidor TACACS+. Si la autenticación no se puede verificar, no se utiliza ningún método de autenticación.

Local, RADIUS: la autenticación se realiza primero localmente. Si la autenticación no se puede verificar de forma local, el servidor RADIUS autentica el método de gestión. Si el servidor RADIUS no puede autenticar el método de gestión, se bloquea la sesión.

Local, TACACS+: la autenticación se realiza primero localmente. Si la autenticación no se puede verificar de forma local, el servidor TACACS+ autentica el método de gestión. Si el servidor TACACS+ no puede autenticar el método de gestión, se bloquea la sesión.

RADIUS, Local: la autenticación se realiza primero en el servidor RADIUS. Si la autenticación no se puede verificar en el servidor RADIUS, la sesión se autentica de forma local. Si la sesión no se puede autenticar de forma local, se bloquea.

TACACS+, Local: la autenticación se realiza primero en el servidor TACACS+. Si la autenticación no se puede verificar en el servidor TACACS+, la sesión se autentica de forma local. Si la sesión no se puede autenticar de forma local, se bloquea.

Local, RADIUS, None (Local, RADIUS, Ninguno): la autenticación se realiza primero localmente. Si la autenticación no se puede verificar de forma local, el servidor RADIUS autentica el método de gestión. Si el servidor RADIUS no puede autenticar el método de gestión, se permite la sesión.

RADIUS, Local, None (RADIUS, Local, Ninguno): la autenticación se realiza primero en el servidor RADIUS. Si la autenticación no se puede verificar en el servidor RADIUS, la sesión se autentica de forma local. Si la sesión no se puede autenticar de forma local, ésta se permite.

Local, TACACS+, None (Local, TACACS+, Ninguno): la autenticación se realiza primero localmente. Si la autenticación no se puede verificar de forma local, el servidor TACACS+ autentica el método de gestión. Si el servidor TACACS+ no puede autenticar el método de gestión, se permite la sesión.

TACACS+, Local, None (TACACS+, Local, Ninguno): la autenticación se realiza primero en el servidor TACACS+. Si la autenticación no se puede verificar en el servidor TACACS+, la sesión se autentica de forma local. Si la sesión no se puede autenticar de forma local, ésta se permite.

Aplicación de una lista de métodos 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 métodos de autenticación a las sesiones de consola.

Aplicación de un perfil de autenticación a sesiones de 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 asignan perfiles de autenticación a las sesiones de consola.

Aplicación de un perfil de autenticación a sesiones de SSH (Secure Telnet)

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. Seleccione un perfil de autenticación en el campo **Secure Telnet (SSH)**.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asignan perfiles de autenticación a las sesiones de SSH (Secure Telnet).

Asignación de sesiones de HTTP a una secuencia de autenticación

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. En HTTP, seleccione un método de autenticación en el campo **Optional Methods** (Métodos opcionales) y haga clic en el botón de la flecha derecha.

El método de autenticación seleccionado pasa al campo **Selected Methods** (Métodos seleccionados).

3. Repita este paso hasta que en el campo **Selected Methods** (Métodos seleccionados) se muestre la secuencia de autenticación que desea.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna la secuencia de autenticación a sesiones de HTTP.

Asignación de sesiones de HTTP seguro a una secuencia de autenticación

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. En **Secure HTTP** (HTTP seguro), seleccione un método de autenticación en el campo **Optional Methods** (Métodos opcionales) y haga clic en el botón de la flecha derecha.

El método de autenticación seleccionado pasa al campo **Selected Methods** (Métodos seleccionados).

3. Repita este paso hasta que en el campo **Selected Methods** (Métodos seleccionados) se muestre la secuencia de autenticación que desea.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna la secuencia de autenticación a sesiones de HTTP seguro.

Asignación de secuencias o perfiles de autenticación de métodos de acceso

La siguiente tabla contiene los comandos de la CLI para asignar los métodos de acceso, las listas de métodos de autenticación o las secuencias.

Tabla 6-32. Comandos de la CLI para los métodos de acceso

Comando de la CLI	Descripción
`enable authentication {default | nombre_lista}`	Especifica la lista de métodos de autenticación cuando el usuario accede a niveles de privilegio superior desde un Telnet o una consola remotos.
`login authentication {default | nombre_lista}`	Especifica la lista de métodos de autenticación de inicio de sesión para un Telnet o una consola remotos.
`ip http authentication method1 [método2...]`	Especifica los métodos de autenticación para los usuarios de servidores http.
`ip https authentication method1 [método2...]`	Especifica los métodos de autenticación para los usuarios de 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# show authentication methods

Login Authentication Method Lists

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

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
```

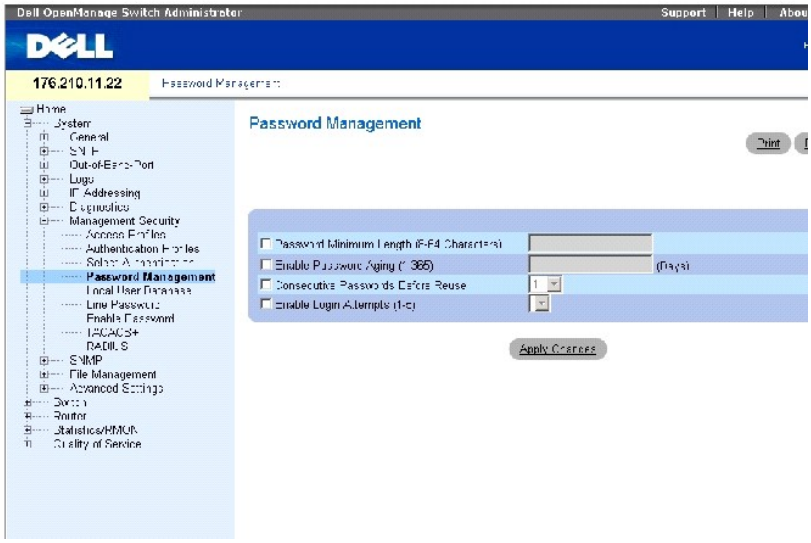
Gestión de contraseñas

La gestión de contraseñas ofrece una mayor seguridad de la red y un mejor control de las contraseñas. A las contraseñas para el acceso a SSH, Telnet, HTTP, HTTPS y SNMP se les asignan funciones de seguridad, incluidas:

- Definición de las longitudes mínimas de las contraseñas
- Caducidad de las contraseñas
- Evitar la reutilización de contraseñas frecuentes
- Bloqueo de usuarios después de intentos de inicio de sesión fallidos

Para abrir la página **Password Management** (Gestión de contraseñas), haga clic en **System**→ **Management Security**→ **Password Management** (Sistema→ Gestión de seguridad→ Gestión de contraseñas) en la *vista de árbol.*

Ilustración 6-46. Password Management (Gestión de contraseñas)



La página **Password Management** (Gestión de contraseñas) contiene los siguientes campos:

Password Minimum Length (8-64 Characters) (Longitud mínima de contraseña [8-64 caracteres]: indica la longitud mínima de la contraseña cuando se selecciona esta opción. Por ejemplo, el administrador puede definir que todas las contraseñas de línea tengan un mínimo de 10 caracteres.

Enable Password Aging (1-365) (Activar caducidad de la contraseña [1-365]): indica la cantidad de tiempo que pasa antes de que la contraseña caduque cuando se selecciona esta opción. El valor del campo es entre 1 y 365 días.

Consecutive Passwords Before Reuse (Contraseñas consecutivas antes de reutilizarlas): indica el número de veces que se puede cambiar una contraseña antes de poder reutilizarla. Los valores posibles del campo son 1 - 10.

NOTA: Se notifica al usuario que debe cambiar la contraseña antes de que caduque. Los usuarios web no ven esta notificación.

Enable Login Attempts (1-5) (Activar intentos de inicio de sesión [1-5]): si se selecciona esta opción, se activa el bloqueo de un usuario y se impide que acceda al dispositivo cuando una contraseña defectuosa se utiliza un número determinado de veces. Por ejemplo, si el número de intentos de inicio de sesión se ha definido en cinco y el usuario intenta iniciar la sesión cinco veces con una contraseña incorrecta, el dispositivo bloquea al usuario en el sexto intento. El intervalo del campo es de 1 a 5 intentos.

Definición de las restricciones de la contraseña

1. Abra la página **Password Management** (Gestión de contraseñas).
2. Defina los campos pertinentes.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Las restricciones de la contraseña se definen y el dispositivo se actualiza.

Definición de las restricciones de la contraseña mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar las contraseñas en la página **Password Management** (Gestión de contraseñas).

Tabla 6-33. Comandos de la CLI para la gestión de contraseñas

Comando de la CLI	Descripción
password min-length *length*	Define la longitud mínima necesaria para las contraseñas.
passwords aging *days*	Define la fecha de caducidad de las contraseñas en la base de datos local.
passwords history *number*	Define el número de modificaciones obligatorias de la contraseña antes de poder reutilizar una contraseña de la base de datos local.
passwords lock-out *number*	Bloquea una cuenta de usuario después de un número especificado de intentos de inicio de sesión fallidos.
show password configuration	Muestra información sobre la gestión de contraseñas.

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

```
Console (config)# password min-length 8

Console (config)# password aging 120

Console (config)# passwords history 2

Console (config)# passwords lock-out 3

Console (config)# exit

Console# show passwords configuration

Minimal length: 8

Aging: 120 days

History: 2

Lock-out: Disabled
```

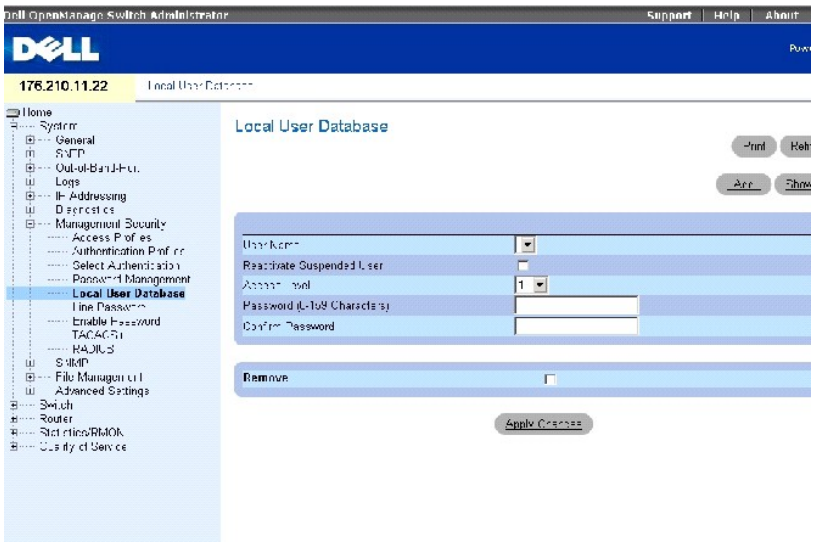
Definición de las bases de datos de usuarios locales

Utilice la página **Local User Database** (Base de datos de usuarios locales) para definir las contraseñas, los derechos de acceso de los usuarios y para reactivar los usuarios cuyas cuentas se han suspendido.

Para abrir la página **Local User Database** (Base de datos de usuarios locales), haga clic en **System**→ **Management Security**→ **Local User Database**

(Sistema→ Gestión de seguridad→ Base de datos de usuarios locales) en la *vista de árbol.*

Ilustración 6-47. Local User Database (Base de datos de usuarios locales)



La página **Local User Database** (Base de datos de usuarios locales) contiene los siguientes campos:

User Name (Nombre de usuario): lista de usuarios.

Reactivated Suspended User (Usuario suspendido reactivado): seleccione esta opción para reactivar los derechos de acceso del usuario especificado. Los derechos de acceso se pueden suspender después de intentar iniciar sesión sin conseguirlo.

Access Level (1-15) (Nivel de acceso [1-15]): el nivel de acceso del usuario. El nivel más bajo de acceso del usuario es **1** y **15** es el nivel más alto de acceso del usuario.

Password (Contraseña): la contraseña definida por el usuario.

Confirm Password (Confirmar contraseña): confirma la contraseña definida por el usuario.

Remove (Eliminar): si esta opción está seleccionada, se eliminan usuarios de la lista **User Name** (Nombre de usuario).

Asignación de derechos de acceso a un usuario

1. Abra la página **Local User Database** (Base de datos de usuarios locales).
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 del usuario, y el dispositivo se actualiza.

Adición de un usuario a una base de datos local

1. Abra la página **Local User Database** (Base de datos de usuarios locales).

2. Haga clic en **Add** (Agregar) para visualizar la página **Add User** (Agregar un usuario).
3. Complete los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define el nuevo usuario y el dispositivo se actualiza.

NOTA: Puede definir hasta 30 usuarios en el dispositivo.

Reactivación de un usuario suspendido

1. Abra la página **Local User Database** (Base de datos de usuarios locales).
2. Haga clic en **Show All** (Mostrar todo) para abrir la página **Local User Table** (Tabla de usuarios locales).
3. Seleccione una entrada de **nombre de usuario**.
4. Seleccione la casilla de verificación Reactivate Suspended User (Reactivar usuario suspendido).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los derechos de acceso del usuario se reactivan y el dispositivo se actualiza.

Supresión de usuarios de la base de datos de usuarios locales

1. Abra la página **Local User Database** (Base de datos de usuarios locales).
2. Haga clic en **Show All** (Mostrar todo) para abrir la **Local User Table** (Tabla de usuarios locales).
3. Seleccione un **nombre de usuario**.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se suprime el usuario y el dispositivo se actualiza.

Asignación de usuarios mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver los campos que se muestran en la página **Local User Database** (Base de datos de usuarios locales).

Tabla 6-34. Comandos de la CLI para bases de datos de usuarios locales

Comando de la CLI	Descripción
`username` *`nombre`* [`password` *`contraseña`*] [`privilege` *`nivel`*] [`encrypted`]	Establece un sistema de autenticación basado en el nombre de usuario.
`set username name active`	Reactiva una cuenta de usuario que está bloqueada.

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

```
Console (config)#username bob password lee privilege 15
```

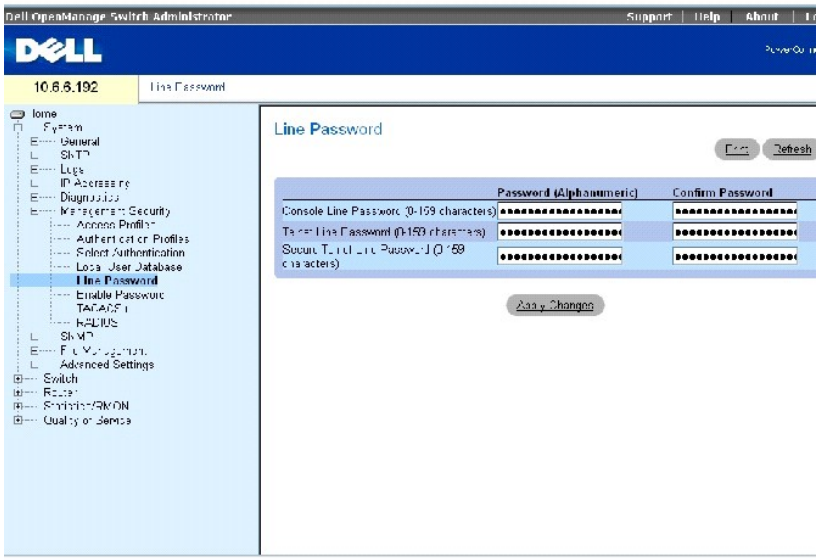
```
Console# set username bob active
```

Definición de las contraseñas de línea

Utilice la página **Line Password** (Contraseña de línea) para definir las contraseñas de línea de los métodos de gestión.

Para abrir la página **Line Password** (Contraseña de línea), haga clic en **System**→ **Management Security**→ **Line Password** (Sistema→ Seguridad de gestión→ Contraseña de línea) en la *vista de árbol.*

Ilustración 6-48. Line Password (Contraseña de línea)



La página **Line Password** (Contraseña de línea) contiene los siguientes campos:

Line Password for Console/Telnet/Secure Telnet (Contraseña de línea para consola/Telnet/Telnet seguro): la contraseña de línea para acceder al dispositivo a través de una sesión de consola, Telnet, o Telnet seguro.

Confirm Password (Confirmar contraseña): confirma la nueva contraseña de línea. La contraseña se muestra como *****.

Definición de las contraseñas de línea

1. Abra la página **Line Password** (Contraseña de línea).
2. Defina el campo **Line Password** (Contraseña de línea) según el tipo de sesión que utilice para conectarse al dispositivo.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la contraseña de línea según el tipo de sesión y el dispositivo se actualiza.

Asignación de contraseñas de línea mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir las contraseñas de línea.

Tabla 6-35. Comandos de la CLI para las contraseñas de línea

Comando de la CLI	Descripción
	Especifica una contraseña en una línea.

password *contraseña* [encrypted]	

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

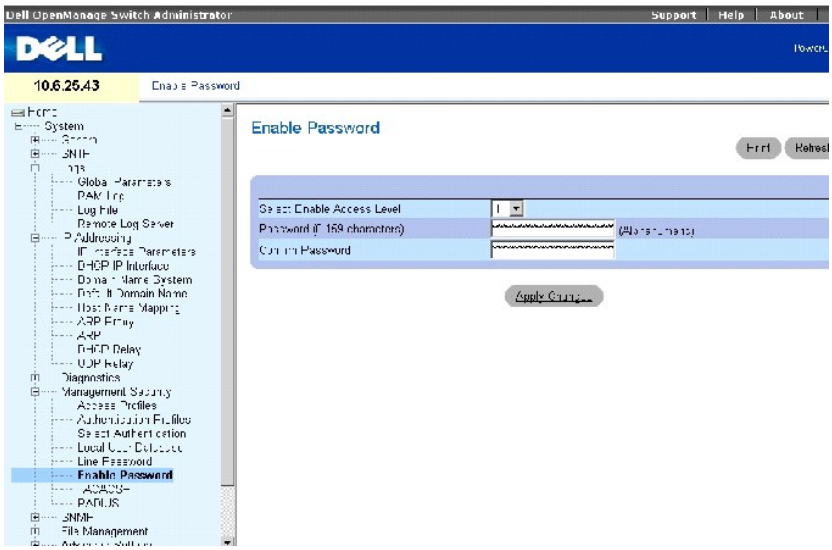
```
Console (config-line)# password ****
```

Definición de la contraseña de activación

La página **Modify Enable Password** (Modificar contraseña de activación) establece una contraseña local para controlar el acceso a los diferentes niveles de privilegio (1-15).

Para abrir la página **Modify Enable Password** (Modificar contraseña de activación), haga clic en **System**→ **Management Security**→ **Enable Password** (Sistema→ Seguridad de gestión→ Contraseña de activación) en la *vista de árbol.*

Ilustración 6-49. Modify Enable Password (Modificar contraseña de activación)



La página **Modify Enable Password** (Modificar contraseña de activación) contiene los siguientes campos:

Select Enable Access Level (Seleccionar nivel de acceso de activación): nivel de acceso asociado a la contraseña de activación. Los valores de campo posibles son 1-15.

Password (Contraseña): la contraseña de activación actual.

Confirm Password (Contraseña de activación): confirma la nueva contraseña de activación. La contraseña se muestra como *****.

Definición de una nueva contraseña de activación

1. Abra la página **Modify Enable Password** (Modificar contraseña de activación).
2. Complete los campos del cuadro de diálogo.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la nueva contraseña y el dispositivo se actualiza.

Asignación de contraseñas de activación mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los campos que se muestran en la página **Modify Enable Password** (Modificar contraseña de activación).

Tabla 6-36. Comandos de la CLI para las contraseñas de activación

Comando de la CLI	Descripción
`enable password [level` *`nivel`*`]` *`contraseña`* `[encrypted]`	Establece una contraseña local para controlar el acceso a niveles de privilegio y usuario.
`show users accounts`	Muestra información sobre la base de datos de usuarios local.

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

```
Console (config)# enable password level 15 dell

Console# show users accounts

Username   Privilege

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

Bob        15

Jim        15

Dell       1515
```

Configuración de los valores de TACACS+

El dispositivo proporciona asistencia de Sistema de Control de Acceso al Controlador de Acceso a la Terminal (TACACS+) al cliente. TACACS+ proporciona seguridad centralizada para la validación de usuarios que acceden al dispositivo.

TACACS+ proporciona un sistema de gestión de usuarios centralizado al mismo tiempo que mantiene la coherencia con RADIUS y otros procesos de autenticación. TACACS+ proporciona los siguientes servicios:

- **Authentication** (Autenticación): proporciona autenticación durante el inicio de sesión y a través de nombres de usuario y contraseñas definidas por el usuario.
- **Authorization** (Autorización): otorgada en el inicio de sesión. Cuando la sesión de autenticación se haya completado, se iniciará una sesión de autorización mediante el nombre de usuario autenticado. El servidor TACACS+ comprobará los privilegios del usuario.

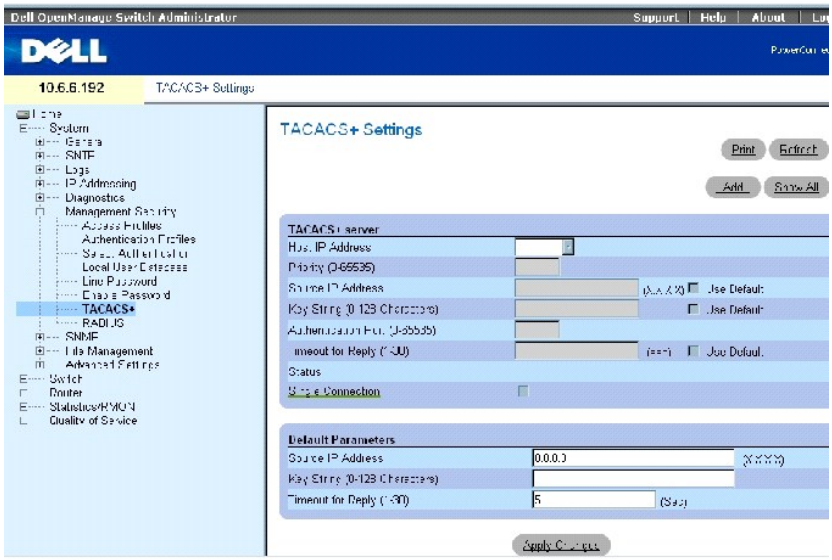
El protocolo TACACS+ garantiza la integridad de la red a través de intercambios de protocolo codificado entre el dispositivo y el servidor TACACS+.

La página **TACACS+ Settings** (Configuración de TACACS) contiene tanto la configuración de TACACS+ predeterminada como la definida por el usuario para el

puerto de gestión en banda.

Para abrir la página **TACACS+ Settings** (Configuración de TACACS+), haga clic en **System**→ **Management Security**→ **TACACS+** (Sistema→ Seguridad de gestión→ TACACS+) en la vista de árbol.

Ilustración 6-50. TACACS+ Settings (Configuración de TACACS+)



La página **TACACS+ Settings** (Configuración de TACACS+) contiene los siguientes campos:

Host IP Address (Dirección IP del sistema principal): especifica la dirección IP del servidor TACACS+.

Priority (0-65535) (Prioridad [0 - 65535]): especifica 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 de TACACS+ entre el dispositivo y el servidor TACACS+.

Key String (0-128 Characters) (Cadena de clave [0 - 128 caracteres): define la autenticación y la clave de codificación para las comunicaciones de TACACS+ entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con la codificación usada en el servidor TACACS+.

Authentication Port (0-65535) (Puerto de autenticación [0 - 65535]): número del puerto a través del cual se lleva a cabo la sesión de TACACS+. El puerto predeterminado es el 49.

Timeout for Reply (1-30) (Tiempo de espera para respuesta [1-30]): tiempo que transcurre antes de que caduque la conexión entre el dispositivo y el servidor TACACS+. El intervalo de este campo es de 1 a 30 segundos.

Status (Estado): estado de conexión entre el dispositivo y el servidor TACACS+. Los valores de campo posibles son:

Connected (Conectado): actualmente existe una conexión entre el dispositivo y el servidor TACACS+.

Not Connected (No conectado): actualmente no existe ninguna conexión entre el dispositivo y el servidor TACACS+.

Single Connection (Conexión única): si esta opción está seleccionada, se mantiene una única conexión abierta entre el dispositivo y el servidor TACACS+.

Los parámetros predeterminados de TACACS+ están definidos por el usuario. La configuración predeterminada se aplica a los servidores TACACS+ recientemente definidos. Si los valores predeterminados no están definidos, los valores predeterminados del sistema se aplican a los nuevos servidores TACACS+. Los valores que se muestran a continuación son los valores predeterminados de TACACS+:

Source IP Address (Dirección IP de origen): dirección IP de origen del dispositivo predeterminado utilizada para la sesión de TACACS+ entre el dispositivo y el servidor TACACS+.

Key String (0-128 Characters) (Cadena de clave [0 - 128 caracteres]): autenticación predeterminada y clave de codificación para la comunicación de TACACS+ entre el dispositivo y el servidor TACACS+.

Timeout for Reply (1-30) (Tiempo de espera para repuesta [1 - 30]): tiempo predeterminado que transcurre antes de que caduque la conexión entre el dispositivo y TACACS+.

NOTA: Los valores predeterminados mencionados anteriormente también se aplican a la página **OOB TACACS+ Settings** (Configuración de TACACS+ OOB) (**System**→ **Out-of- Band-Port**→ **TACACS+**) (Sistema→ Puerto de fuera de banda→ TACACS+).

Definición de los parámetros de TACACS+

1. Abra la página **TACACS+ Settings** (Configuración de TACACS+).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de TACACS+ se actualiza en el dispositivo.

Adición de un servidor TACACS+

1. Abra la página **TACACS+ Settings** (Configuración de TACACS+).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add TACACS+ Host** (Agregar sistema principal de TACACS+):

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

El servidor TACACS+ se agregará y el dispositivo se actualizará.

Supresión de un servidor TACACS+ de la lista de servidores TACACS+

1. Abra la página **TACACS+ Settings** (Configuración de TACACS+).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **TACACS+ Table** (Tabla de TACACS+).

3. Seleccione una entrada de la **TACACS+ Table** (Tabla de TACACS+).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor TACACS+ se eliminará y el dispositivo se actualizará.

Definición de los servidores TACACS+ mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los campos que se muestran en la página **TACACS+ Settings** (Configuración de TACACS+).

Tabla 6-37. Comandos de la CLI para la configuración de TACACS+

Comando de la CLI	Descripción
tacacs-server host {*dirección-ip* | *nombrehost*} [single-connection] [**port** port-number] [timeout timeout] [**key** key-string] [source source] [priority priority]	Especifica el sistema principal de un servidor TACACS+.
no tacacs-server host {*dirección-ip* | *nombrehost*}	Suprime el sistema principal de un servidor TACACS+ concreto.
tacacs-server key [key- string]	Especifica la autenticación y la clave de codificación utilizada para todas las comunicaciones de TACACS entre el enrutador y el servidor TACACS+. Esta clave debe coincidir con la codificación utilizada en el daemon de TACACS. (Intervalo: 0-128 caracteres)
no tacacs-server key	Vuelve al valor predeterminado.
tacacs-server timeout *tiempo de espera*	Especifica el valor del tiempo de espera en segundos. (Intervalo: 1-30)
no tacacs-server timeout	Vuelve al valor predeterminado.
tacacs-server source-ip ip-address	Especifica la dirección IP de origen. (Intervalo: dirección IP válida)
no tacacs-server source-ip ip-address	Vuelve al valor predeterminado.
show tacacs+ [*dirección_ip*]	Muestra la configuración y las estadísticas para un servidor TACACS+.

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

```
Console (config)# tacacs-server host 171.16.8.1 port 49 key abc

Console (config)# end

Console# show tacacs

                                                                                

Device Configuration

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

IP address  Status      Port  Single Connection  TimeOut  Source IP  Priority

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

171.16.8.1  Not Connected  49  No                 Global   Global     0

                                                                                
```

OOB Host Configuration

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
----------	---------	----	----------	-------	------	--------

No TACACS server is configured.

Device Configuration

Source IP: 0.0.0.0

OOB host Configuration

Source IP : 0.0.0.0

Configuración de los valores de RADIUS

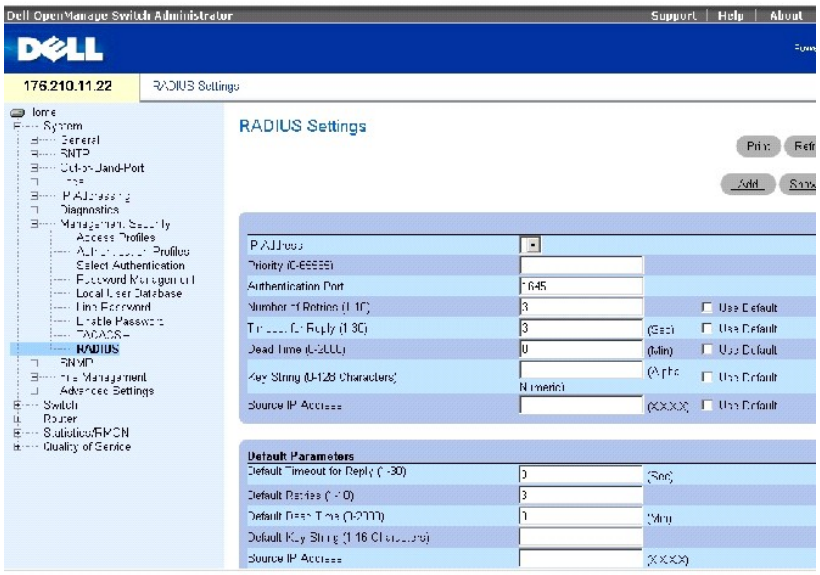
Los servidores de servicio de usuario de marcación de entrada de autorización remota (RADIUS) proporcionan seguridad adicional a las redes. El servidor RADIUS mantiene una base de datos de usuarios, que contiene información sobre la autenticación por usuario. Los servidores RADIUS proporcionan un método de autenticación centralizado para:

- Acceso a Telnet
- Acceso a web
- El acceso de la consola al conmutador

La página **RADIUS Settings** (Configuración de RADIUS) contiene la configuración de RADIUS predeterminada así como la definida por el usuario.

Para abrir la página **RADIUS Settings** (Configuración de RADIUS), haga clic en **System**→ **Management Security**→ **RADIUS** (Sistema→ Gestión de seguridad→ RADIUS) en la *vista de árbol.*

Ilustración 6-51. RADIUS Settings (Configuración de RADIUS)



La página **RADIUS Settings** (Configuración de RADIUS) contiene los siguientes campos:

IP Address (Dirección IP): la dirección IP del puerto de autenticación.

Priority (0-65535) (Prioridad [0-65535]): indica la prioridad del puerto. Los valores posibles son 0-65535.

Authentication Port (Puerto de autenticación): identifica el puerto de autenticación que se utiliza para comprobar la autenticación del servidor RADIUS.

Number of Retries (1-10) (Número de reintentos [1-10]): número de peticiones transmitidas que se envían al servidor RADIUS antes de que se produzca un fallo. Los valores posibles son 1 - 10. Tres es el valor predeterminado. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales. Haga clic en **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado.

Timeout for Reply (1-30) (Tiempo de espera para respuesta [1-30]): cantidad de tiempo en segundos que el dispositivo espera una respuesta del servidor RADIUS antes de expirar. Los valores posibles son 1 - 30. Tres es el valor predeterminado. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales. Haga clic en **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado.

Dead Time (0-2000) (Tiempo muerto [0-2000]): cantidad de tiempo (en minutos) durante el que no se envían peticiones de servicio a un servidor RADIUS. El intervalo es 0-2000. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales. Haga clic en **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado.

Key String (0-128 Characters) (Cadena de clave [1-128 caracteres]): cadena de clave utilizada para autenticar y codificar todas las comunicaciones de RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la codificación RADIUS. Si no se especifica ningún valor específico del sistema principal, se aplica el valor global a cada uno de los sistemas principales.

Source IP Address (Dirección IP de origen): dirección IP del dispositivo que accede al servidor RADIUS.

NOTA: Los parámetros predeterminados de esta página están definidos por el usuario.

Default Retries (1-10) (Reintentos predeterminados [1-10]): número predeterminado de peticiones transmitidas que se envían al servidor RADIUS antes de que se produzca un fallo.

Default Timeout for Reply (1-30) (Tiempo de espera predeterminado para respuesta [1-30]): el número predeterminado de peticiones transmitidas que se envían al servidor RADIUS antes de que se produzca un fallo. Los valores de campo posibles son 1 - 30.

Default Dead Time (0-2000) (Tiempo muerto predeterminado [0-2000]): especifica la cantidad de tiempo predeterminada (en minutos) durante el que no se envían peticiones de servicio a un servidor RADIUS. El intervalo es 0-2000.

Default Key String (0-128 characters) (Cadena de clave predeterminada [0-128 caracteres]): cadena de clave predeterminada que se utiliza para autenticar y cifrar todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la codificación RADIUS.

Source IP Address (Dirección IP de origen): dirección IP predeterminada de un dispositivo que accede al servidor RADIUS.

Adición de un servidor RADIUS

1. Abra la página **RADIUS Settings** (Configuración de RADIUS).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add RADIUS Server** (Agregar un servidor RADIUS).
3. Defina los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El nuevo servidor RADIUS se agrega y el dispositivo se actualiza.

Definición de los parámetros de RADIUS

1. Abra la página **RADIUS Settings** (Configuración de RADIUS).
2. Defina los campos del cuadro de diálogo.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de RADIUS se actualiza en el dispositivo.

Modificación de la configuración del servidor RADIUS

1. Abra la página **RADIUS Settings** (Configuración de RADIUS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la **RADIUS Servers List** (Lista de servidores RADIUS).
3. Modifique los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración del servidor RADIUS se modifica y el dispositivo se actualiza.

Supresión de un servidor RADIUS de la lista de servidores RADIUS

1. Abra la página **RADIUS Settings** (Configuración de RADIUS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la **RADIUS Servers List** (Lista de servidores RADIUS).
3. Seleccione un servidor RADIUS y marque la casilla de verificación **Remove** (Eliminar).

Se elimina el servidor RADIUS de la lista.

Definición de los servidores RADIUS mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **RADIUS Settings** (Configuración de RADIUS).

Tabla 6-38. Comandos de la CLI para los servidores RADIUS

Comando de la CLI	Descripción
`radius-server timeout tiempo de espera`	Establece el intervalo durante el cual un enrutador espera la respuesta del sistema principal de un servidor.
`radius-server retransmit reintentos`	Especifica el número de veces que el software realiza búsquedas en la lista de sistemas principales de servidores RADIUS.
`radius-server deadtime tiempo muerto`	Configura los servidores no disponibles que deben omitirse.
`radius-server key cadena_clave`	Establece la clave de autenticación y codificación para todas las comunicaciones de RADIUS entre el enrutador y el entorno de RADIUS.
`radius-server host dirección_ip [auth-port número_puerto_autenticación] [timeout timeout] [retransmit reintentos] [deadtime tiempo muerto] [key cadena_clave] [source origen] [priority prioridad]`	Especifica el sistema principal de un 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 **SNMP** (Simple Network Management Protocol) proporciona un método para administrar dispositivos en una red. El dispositivo es compatible con SNMP versión 1, SNMP versión 2 y SNMP versión 3.

NOTA: De manera predeterminada, SNMPv2 se activa automáticamente en el dispositivo. Para activar SNMPv3, hay que definir un ID de motor local para el dispositivo. El ID de motor local puede ser una cadena especificada por el usuario o una cadena predeterminada generada en función de la dirección MAC del dispositivo. Para obtener información sobre cómo configurar el ID de motor local, consulte el apartado **Definición de parámetros globales de SNMP**.

SNMP v1 y v2

El agente SNMP mantiene una lista de variables que se utilizan para administrar el dispositivo. Las 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 obtener acceso a la información por la red. Las cadenas de acceso controlan los derechos de acceso al agente SNMP.

SNMP v3

SNMP v3 también aplica el control de acceso y un nuevo mecanismo de capturas a las PDU de SNMPv1 y SNMPv2. Además, el modelo de seguridad de usuarios (USM) se define para SNMP v3 e incluye:

- **Autenticación**: proporciona la autenticación del origen de datos y la integridad de los datos.
- **Privacidad**: impide la divulgación del contenido del mensaje. Para la codificación se utiliza CBC (Cipher-Bock-Chaining). En un mensaje de SNMP se puede activar la autenticación o bien tanto la autenticación como la privacidad. Sin embargo, la privacidad no se puede activar sin la autenticación.
- **Puntualidad**: impide que el mensaje se retrase o sea redundante. El agente de SNMP compara el mensaje de entrada con la información de la hora del mensaje.
- **Gestión de claves**: define la generación de claves, las actualizaciones de las claves y su utilización.

El dispositivo es compatible con los filtros de notificación de SNMP en función de los ID de objeto (OID). El sistema utiliza los OID para gestionar las funciones del dispositivo. SNMP v3 es compatible con las siguientes funciones:

- Seguridad
- Control de acceso a las funciones
- Capturas

Las claves de privacidad o autenticación se modifican en el **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]).

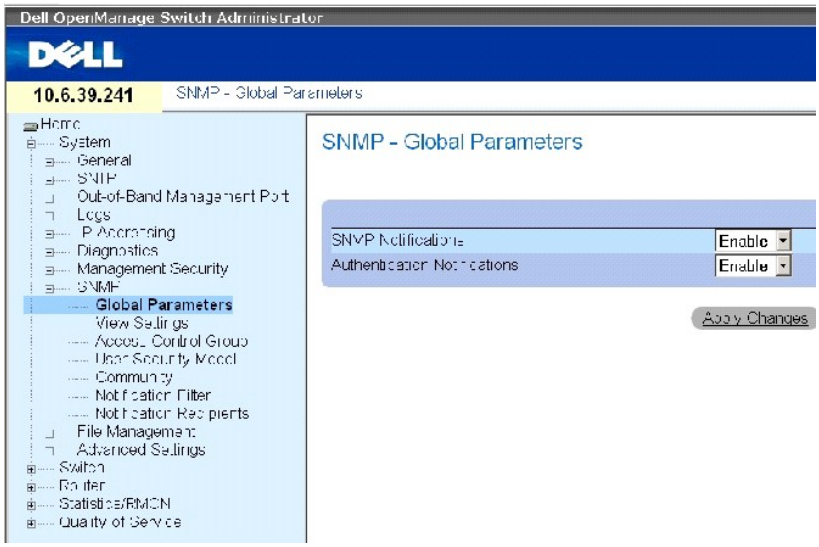
Utilice la página SNMP para definir los parámetros SNMP. Para abrir la página SNMP, haga clic en **System**→ **SNMP** (Sistema→ SNMP) en la *vista de árbol.*

Definición de los parámetros globales de SNMP

Utilice la página **Global Parameters** (Parámetros globales) para activar las notificaciones de autenticación y SNMP.

Para abrir la página **Global Parameters** (Parámetros globales), haga clic en **System**→ **SNMP**→ **Global Parameters** (Sistema→ SNMP→ Parámetros globales) en la *vista de árbol*.

Ilustración 6-52. Global Parameters (Parámetros globales)



La página **Global Parameters** (Parámetros globales) contiene los siguientes parámetros:

SNMP Notifications (Notificaciones de SNMP): activa o desactiva el envío de notificaciones SNMP por parte del dispositivo.

Authentication Notifications (Notificaciones de autenticación): activa o desactiva el envío de capturas SNMP por parte del dispositivo cuando se ha producido un error en la autenticación.

Activación de notificaciones SNMP

1. Abra la página **Global Parameters** (Parámetros globales).
2. Seleccione **Enable** (Activar) en el campo **SNMP Notifications** (Notificaciones SNMP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Las notificaciones SNMP se activan y el dispositivo se actualiza.

Activación de notificaciones de autenticación

1. Abra la página **Global Parameters** (Parámetros globales).
2. Seleccione **Enable** (Activar) en el campo **Authentication Notifications** (Notificaciones de autenticación).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Las notificaciones de autenticación se activan y el dispositivo se actualiza.

Activación de las notificaciones SNMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **Global Parameters** (Parámetros globales).

Tabla 6-39. Comandos de la CLI para las notificaciones SNMP

Comando de la CLI	Descripción

snmp-server engineID local {*ID motor_cadena* | default}	Especifica el ID de motor SNMP en el dispositivo local.
show snmp	Muestra la configuración del dispositivo SNMP.

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 (config)# end

Console# show snmp
```

Community-String	Community-Access	IP address
------------	-----------------	-----------------
public	read only	All
private	read write	172.16.1.1
private	read write	172.17.1.1
OOB management stations		
Community-String	Community-Access	IP address
------------	-----------------	-----------------
private	read write	176.16.8.9
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
192.122.173.42	public	2

OOB trap receivers		
Trap-Rec-Address	Trap-Rec-Community	Version
176.16.8.9	public	2
System Contact: Robert		
System Location: Marketing		

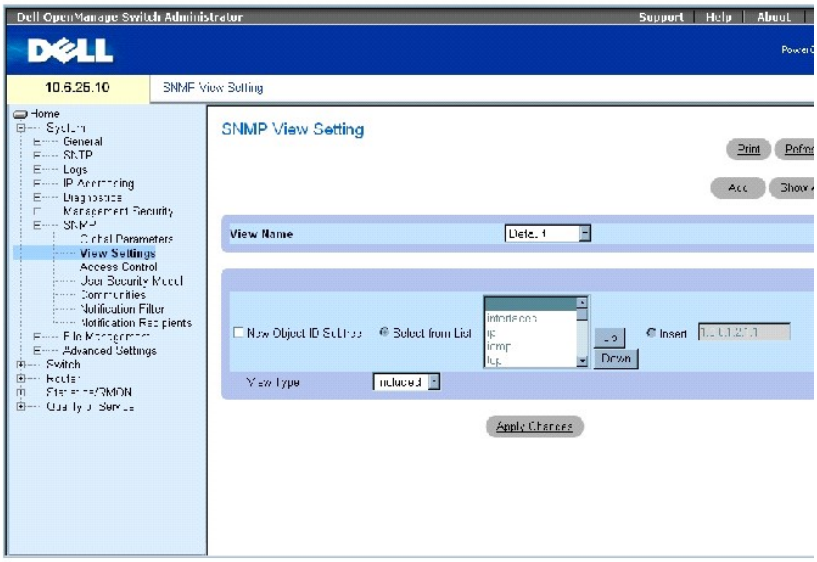
Definición de las vistas SNMP

Las vistas SNMP proporcionan o bloquean el acceso a las funciones del dispositivo o a aspectos de las funciones. Por ejemplo, se puede definir una vista que determine que el grupo SNMP A tenga acceso de sólo lectura al encaminamiento, mientras que el grupo SNMP B tenga acceso de lectura y escritura al encaminamiento. El acceso a las funciones se otorga a través del nombre de MIB o del ID de objeto de MIB.

Utilice la página **SNMP View Setting** (Configuración de vistas SNMP) para definir las vistas SNMP.

Para abrir la página **SNMP View Setting** (Configuración de vistas SNMP), haga clic en **System**→ **SNMP**→ **View Settings** (Sistema→ SNMP→ Configuración de vistas) en la *vista de árbol.*

Ilustración 6-53. SNMP View Setting (Configuración de vistas SNMP)



La página **SNMP View Setting** (Configuración de vistas SNMP) contiene los siguientes campos:

View Name (Nombre de vista): contiene una lista de las vistas definidas por el usuario. Un nombre de vista puede contener un máximo de 30 caracteres alfanuméricos.

New Object ID Subtree (Subárbol de nuevo ID de objeto): especifica el OID de la función del dispositivo que se incluye o excluye de la vista SNMP.

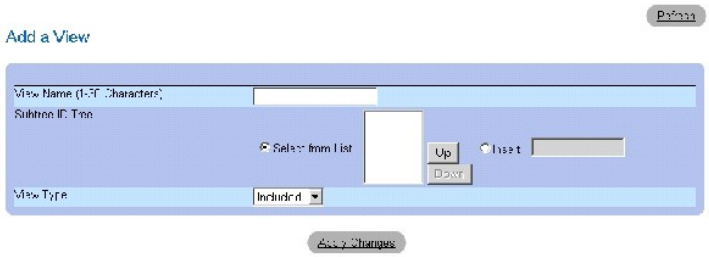
View Type (Tipo de vista): si se selecciona esta opción, se activa el acceso a una función seleccionada o a un aspecto de la función en la vista SNMP.

Adición de una vista

1. Abra la página **SNMP View Setting** (Configuración de vistas SNMP).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add A View** (Agregar una vista):

Ilustración 6-54. Add A View (Agregar una vista)



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

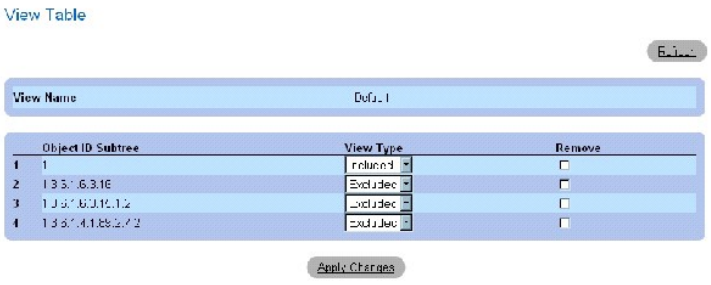
Se agrega la vista SNMP y el dispositivo se actualiza.

Visualización de la tabla de vistas

1. Abra la página **SNMP View Setting** (Configuración de vistas SNMP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **View Table** (Ver tabla):

Ilustración 6-55. View Table (Ver tabla)



Eliminación de vistas SNMP

1. Abra la página **SNMP View Setting** (Configuración de vistas SNMP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **View Table** (Ver tabla):

3. Seleccione una vista SNMP.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La vista SNMP se elimina y el dispositivo se actualiza.

Definición de las vistas SNMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **SNMP View Setting** (Configuración de vistas SNMP).

Tabla 6-40. Comandos de la CLI para las vistas SNMP

Comando de la CLI	Descripción
show snmp views [*nombre_vista*]	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

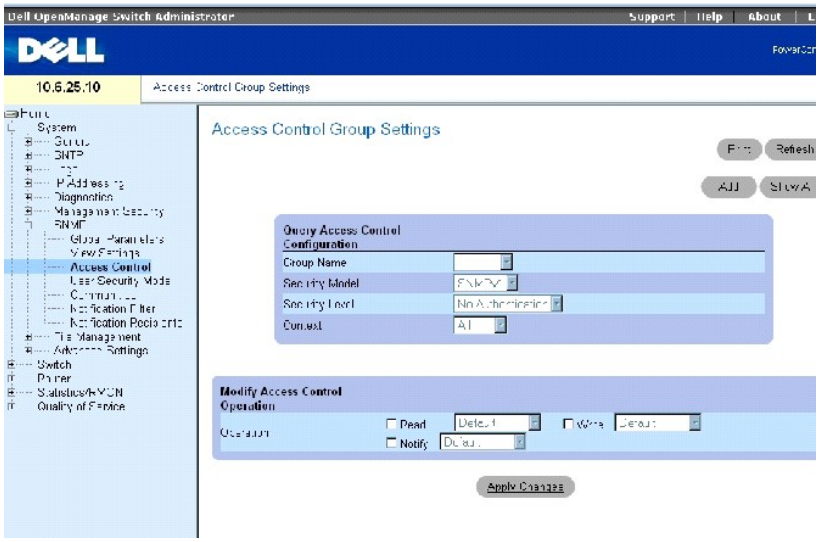
Definición del control de acceso de SNMP

La página **Access Control Group** (Grupo de control de acceso) ofrece información para la creación de grupos SNMP y la asignación de privilegios de acceso SNMP. Los grupos permiten a los administradores de red asignar derechos de acceso a funciones específicas del dispositivo o a aspectos de las funciones.

El puerto fuera de banda se trata como un dispositivo independiente cuando se utilizan las funciones de SNMP. Las vistas se pueden limitar a las MIB fuera de banda, a las MIB del dispositivo o a todas las MIB.

Para abrir la página **Access Control Group** (Grupo de control de acceso), haga clic en **System**→ **SNMP**→ **Access Control** (Sistema→ SNMP→ Control de acceso) en la vista de árbol.

Ilustración 6-56. Access Control Group (Grupo de control de acceso)



La página **Access Control Group** (Grupo de control de acceso) contiene los siguientes campos:

Group Name (Nombre del grupo): contiene una lista de los grupos definidos por el usuario a los que se aplican reglas de control de acceso. Un nombre de grupo puede contener un máximo de 30 caracteres alfanuméricos.

Security Model (Modelo de seguridad): define la versión de SNMP asignada al grupo. Los valores de campo posibles son:

SNMPv1: se define SNMPv1 para el grupo.

SNMPv2: se define SNMPv2 para el grupo.

SNMPv3: se define SNMPv3 para el grupo.

Security Level (Nivel de seguridad): el nivel de seguridad asignado al grupo. Los niveles de seguridad sólo se aplican a los grupos SNMPv3. Los valores de campo posibles son:

No Authentication (Sin autenticación): no se asignan ni niveles de seguridad de privacidad ni de autenticación al grupo.

Authentication (Autenticación): autentica los mensajes de SNMP sin cifrarlos.

Privacy (Privacidad): autentica los mensajes de SNMP y los cifra.

Operation (Funcionamiento): define los derechos de acceso del grupo. Los valores de campo posibles son:

Read (Leer): seleccione una vista que restrinja el acceso de gestión a la visualización del contenido del agente. Si no se selecciona ninguna vista, se pueden visualizar todos los objetos excepto la tabla de comunidad, el usuario de SNMPv3 y las tablas de acceso.

Write (Escribir): seleccione una vista que permita el acceso de lectura-escritura de gestión al contenido del agente pero no a la comunidad.

Notify (Notificar): seleccione una vista que permita el envío de informes o capturas SNMP.

Context (Contexto): contexto para el que se configura el grupo de acceso. Los valores de campo posibles son:

Router (Enrutador): el grupo de acceso se configura para la gestión en banda.

OOB: el grupo de acceso se configura para la gestión fuera de banda.

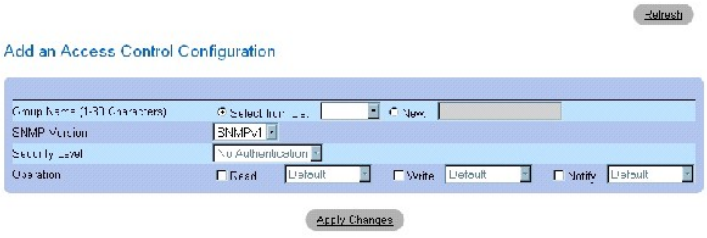
All (Todo): el grupo de acceso se configura tanto para la gestión en banda como fuera de banda

Definición de grupos SNMP

1. Abra la página **Access Control Group** (Grupo de control de acceso).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add an Access Control Group** (Agregar un grupo de control de acceso):

Ilustración 6-57. Add an Access Control Group (Agregar un grupo de control de acceso)



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

Se agrega el grupo y el dispositivo se actualiza.

Visualización de la tabla de acceso

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 acceso):

Ilustración 6-58. Access Table (Tabla de acceso)

Supresión de un grupo

1. Abra la página **Access Control Group** (Grupo de control de acceso).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Access Table** (Tabla de acceso):

3. Seleccione un grupo.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El grupo se suprime y el dispositivo se actualiza.

Definición del control de acceso de SNMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **Access Control Group** (Grupo de control de acceso).

Tabla 6-41. Comandos de la CLI para el control de acceso de SNMP

Comando de la CLI	Descripción
snmp-server group *nombre_grupo* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**}} [**read** *vista_leer*] [**write** *vista_escribir*] [**notify** *vista_notificar*]	Configure un grupo nuevo de SNMP (Simple Network Management Protocol) o una tabla que asigne usuarios de SNMP a vistas de SNMP.
show snmp groups [*nombre_grupo*]	Muestra la configuración de los grupos.

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

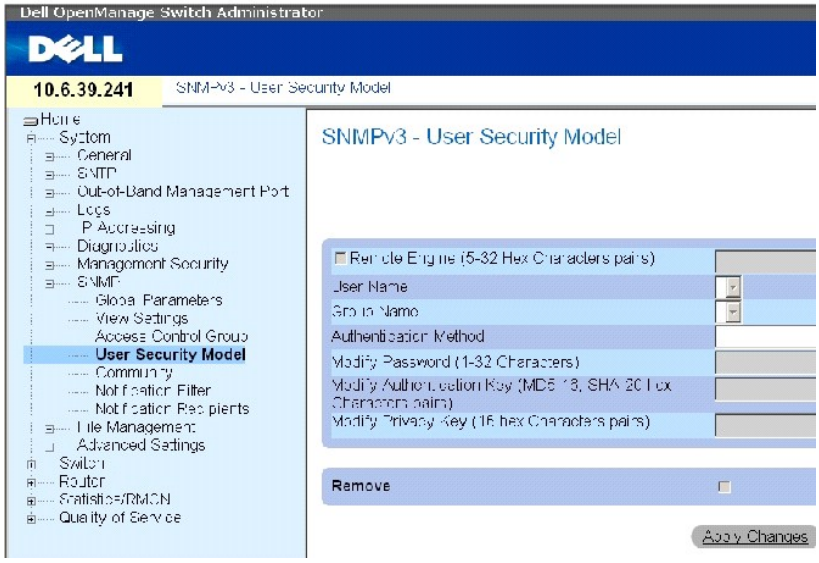
```
Console (config)# snmp-server group user-group v3 priv read user- view
```

Asignación de seguridad de usuarios SNMP

La página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]) activa la asignación de usuarios del sistema a grupos SNMP además de definir el método de autenticación de usuarios.

Para abrir la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]), haga clic en **System**→ **SNMP**→ **User Security Model** (Sistema→ SNMP→ Modelo de seguridad de usuarios) en la *vista de árbol*.

Ilustración 6-59. SNMPv3 User Security Model (USM) (Modelo de seguridad de usuarios de SNMPv3 [USM])



La página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]) contiene los siguientes campos:

Engine ID (ID de motor): identifica el dispositivo activado SNMPv3 remoto al que se conecta el usuario seleccionado.

Remote Engine ID (ID de motor remoto): indica que el usuario está configurado en un dispositivo activado SNMPv3 remoto. Si se define el ID de motor, los dispositivos remotos reciben mensajes de información.

User Name (Nombre de usuario): contiene una lista de nombres de usuario definidos por el usuario.

Group Name (Nombre del 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): especifica el método de autenticación utilizado para autenticar a los usuarios. Los valores de campo posibles son:

None (Ninguna): no se realiza ninguna autenticación de usuario.

MD5 Password (Contraseña MD5): los usuarios se autentican con el nivel de autenticación HMAC-MD5-96. El usuario debe especificar una contraseña.

SHA Password (Contraseña SHA): los usuarios se autentican con el nivel de autenticación HMAC-SHA-96. El usuario debe introducir una contraseña.

MD5 Key (Clave MD5): los usuarios se autentican con el nivel de autenticación HMAC-MD5-96. El usuario debe introducir las claves de privacidad y autenticación.

SHA Key (Clave SHA): los usuarios se autentican con el nivel de autenticación HMAC-SHA-96. El usuario debe introducir las claves de privacidad y autenticación.

Password (0-32 Characters) (Contraseña [0-32 caracteres]): modifica la contraseña definida por el usuario para el grupo. Las contraseñas pueden contener un máximo de 32 caracteres. Las contraseñas sólo se definen si el método de autenticación es contraseña SHA o MD5.

Authentication Key (MD5-16; SHA-20 hexa chars) (Clave de autenticación [caracteres hexa SHA-20; MD5-16]): especifique la clave de autenticación. Una clave de autenticación sólo se define si el método de autenticación es clave MD5 o clave SHA.

Privacy Key (16 hexa chars) (Clave de privacidad [16 caracteres hexa]): especifique una contraseña para autenticar y generar una clave DES de privacidad. Una clave de privacidad sólo se define si el método de autenticación es clave MD5 o clave SHA.

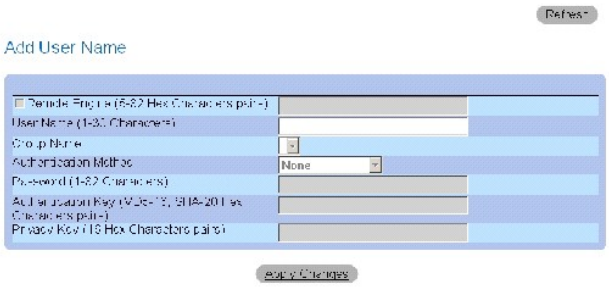
Remove (Eliminar): si se selecciona esta opción, se elimina el usuario especificado del grupo especificado.

Adición de usuarios de SNMPv3 a un grupo

1. Abra la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add SNMPv3 User Name** (Agregar nombre de usuario de SNMPv3):

Ilustración 6-60. Add SNMPv3 User Name (Agregar nombre de usuario de SNMPv3)



3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. El usuario se agrega al grupo y el dispositivo se actualiza.

Visualización de la tabla de modelos de seguridad de usuarios

1. Abra la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **SNMPv3 User Security Model Table** (Tabla de modelos de seguridad de usuarios de SNMPv3):

Ilustración 6-61. SNMPv3 User Security Model Table (Tabla de modelos de seguridad de usuarios de SNMPv3)

Supresión de una entrada de la tabla de modelos de seguridad de usuarios

1. Abra la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]).

2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **SNMPv3 User Security Model Table** (Tabla de modelos de seguridad de usuarios de SNMPv3):

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

La entrada se suprime y el dispositivo se actualiza.

Definición de los usuarios de SNMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad de usuarios de SNMPv3 [USM]).

Tabla 6-42. Comandos de la CLI para los usuarios de SNMP

Comando de la CLI	Descripción
show snmp users [*nombre_usuario*]	Muestra la configuración de los usuarios.

```
Console (config)# snmp-server user John auth-md5 1234

Console (config)# end

Console (config)# show snmp users
```

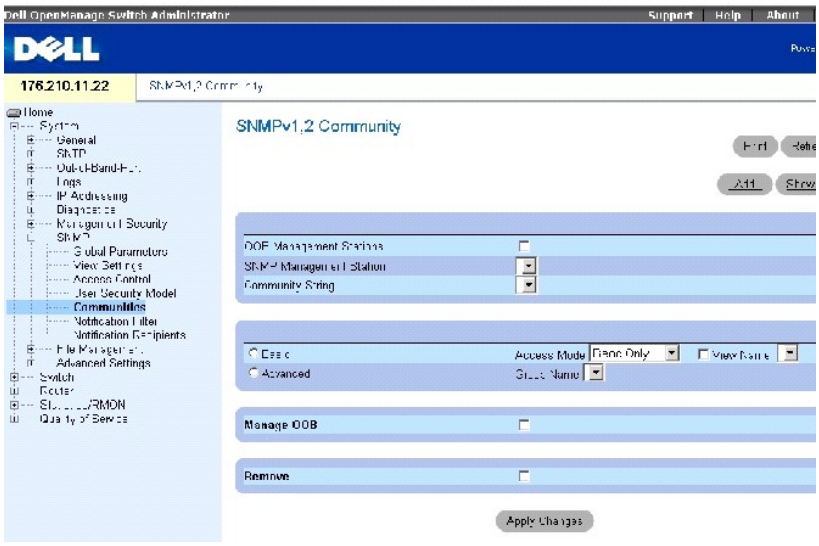
Name	Group Name	Auth Method	Remote
-------	----------	----------	------
John	user-group	md5	

Definición de las comunidades

Los derechos de acceso se gestionan mediante la definición de comunidades en la página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2). Cuando se cambian los nombres de las comunidades, los derechos de acceso también cambian. Las comunidades SNMP sólo se definen para SNMP v1 y SNMP v2.

Para abrir la página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2), haga clic en **System**→ **SNMP**→ **Communities** (Sistema→ SNMP→ Comunidades) en la *vista de árbol.*

Ilustración 6-62. SNMPv1, 2 Community (Comunidad SNMPv1, 2)



La página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2) contiene los siguientes campos:

OOB Management Station (Estación de gestión OOB): seleccione esta casilla de verificación para crear una comunidad SNMP independiente para el puerto fuera de banda. Si no se selecciona esta casilla de verificación, se accede al dispositivo mediante la estación de gestión a través de los puertos en banda.

SNMP Management Station (Estación de gestión de SNMP): contiene una lista de direcciones IP de la estación de gestión para la que se han definido cadenas de comunidad.

NOTA: Sólo los superusuarios pueden utilizar la misma comunidad para configurar puertos en banda y fuera de banda.

Community String (Cadena de comunidad): contiene una lista de cadenas de comunidad definidas por el usuario que funcionan como una contraseña y se utilizan para autenticar la estación de gestión de SNMP para el dispositivo. Una cadena de comunidad puede contener un máximo de 20 caracteres.

Basic (Básico): activa el modo básico de SNMP para la comunidad seleccionada. Los valores de campo posibles son:

Access Mode (Modo de acceso): define los derechos de acceso de la comunidad. Los valores de campo posibles son:

Read-Only (Sólo lectura): el acceso de gestión está restringido a sólo lectura y no se pueden realizar cambios en la comunidad.

Read-Write (Lectura-Escritura): el acceso de gestión es de lectura y escritura y se pueden 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 derechos para modificar la comunidad.

View Name (Nombre de vista): contiene una lista de las vistas de SNMP definidas por el usuario.

Advanced (Avanzado): contiene una lista de grupos definidos por el usuario. Si 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 los grupos SNMP para comunidades SNMP específicas. El modo avanzado de SNMP sólo se define con SNMPv3.

Manage OOB (Gestionar OOB): si se selecciona esta casilla de verificación, se facilita la gestión de SNMP a las estaciones de gestión fuera de banda conectadas al dispositivo únicamente a través del puerto fuera de banda.

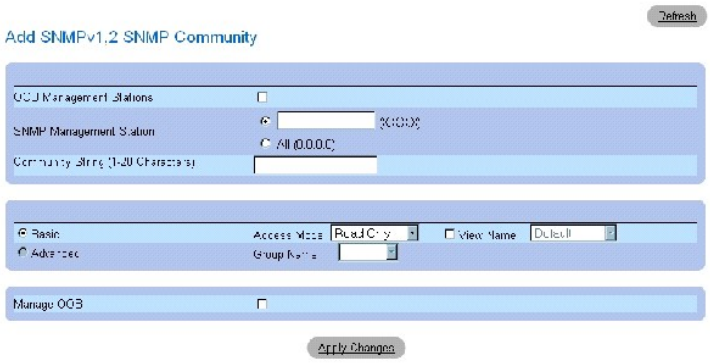
Remove (Eliminar): si se selecciona esta opción, se elimina una comunidad.

Definición de una nuevo comunidad

1. Abra la página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add SNMPv1, 2 Community** (Agregar comunidad SNMPv1, 2):

Ilustración 6-63. Add SNMPv1, 2 Community (Agregar comunidad SNMPv1, 2)



3. Complete los campos pertinentes.

Además de los campos de la página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2), la página **Add SNMPv1, 2 Community** (Agregar comunidad SNMPv1, 2) contiene el campo **All (0.0.0.0)** (Todo [0.0.0.0]), que indica si se ha definido una comunidad SNMP para una determinada estación de gestión o para todas las estaciones de gestión.

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

La comunidad nueva se guarda y el dispositivo se actualiza.

Supresión de comunidades

1. Abra la página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **SNMPv1, 2 Community Tables** (Tablas de comunidad SNMPv1, 2).

3. Seleccione una comunidad y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la comunidad se suprime y el dispositivo se actualiza.

Configuración de comunidades mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **SNMPv1, 2 Community** (Comunidad SNMPv1, 2).

Tabla 6-43. Comandos de la CLI para la comunidad SNMP

Comando de la CLI	Descripción
snmp-server community community [**ro** | **rw** | **su**] [*dirección_ip*] [view view-name][type {router | oob}]	Configura la cadena de acceso a la comunidad para permitir el acceso al protocolo SNMP.
snmp-server community-group community group-name [*dirección_ip*] [type {router | oob}]	Configura la cadena de acceso a la comunidad para permitir el acceso limitado al protocolo SNMP en función de los derechos de acceso del grupo.
show snmp	Muestra la configuración actual del dispositivo SNMP.

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

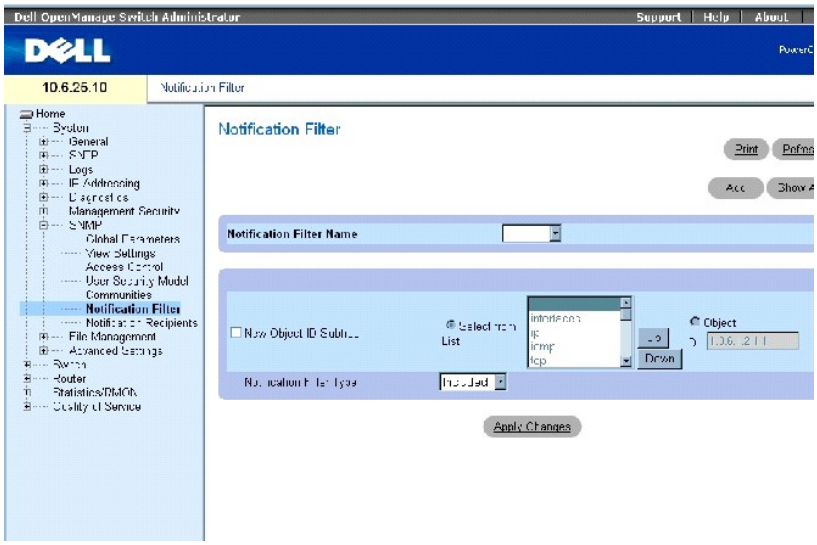
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Definición de filtros de notificación SNMP

La página **Notification Filter** (Filtro de notificación) permite filtrar capturas en función de OID. Cada OID está vinculado con una función del dispositivo o un aspecto de la función. La página **Notification Filter** (Filtro de notificación) también permite a los administradores de red filtrar las notificaciones.

Para abrir la página **Notification Filter** (Filtro de notificación), haga clic en **System**→ **SNMP**→ **Notification Filters** (Sistema→ SNMP→ Filtros de notificación) en la *vista de árbol*.

Ilustración 6-64. Notification Filter (Filtro de notificación)



La página **Notification Filter** (Filtro de notificación) contiene los siguientes campos:

Notification Filter Name (Nombre del filtro de notificación): contiene una lista de filtros de notificación definidos por el usuario. Un nombre de filtro de notificación puede contener un máximo de 30 caracteres.

New Object Identifier Subtree (Subárbol de nuevo identificador de objetos): el OID por el cual se envían o bloquean las notificaciones. Si se asigna un filtro a un OID, se generan capturas o informes y se envían a los destinatarios de la captura. Los ID de objeto se seleccionan en el cuadro *Select from List* (Seleccionar de la lista) o en el campo *Object ID* (ID de objeto) especificado.

Notification Filter Type (Tipo de filtro de notificación): indica si se envían los informes o capturas referentes al OID a los destinatarios de la captura.

Excluded (Excluido): restringe el envío de informes o capturas de OID.

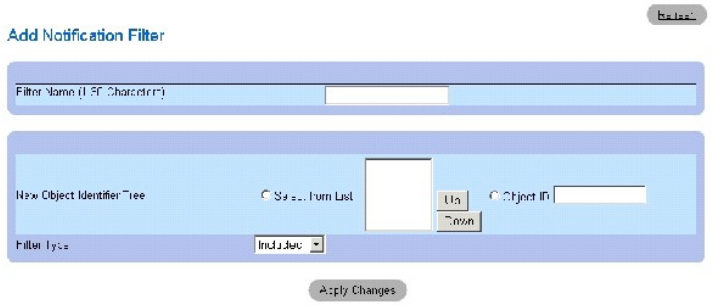
Included (Incluido): envía informes o capturas de OID.

Adición de filtros SNMP

1. Abra la página **Notification Filter** (Filtro de notificación).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add Filter** (Agregar filtro):

Ilustración 6-65. Add Filter (Agregar filtro)



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

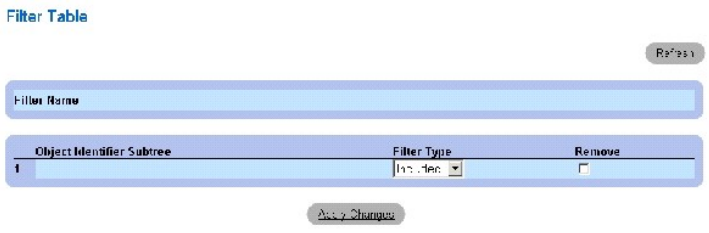
Se agrega el nuevo filtro y el dispositivo se actualiza.

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):

Ilustración 6-66. Filter Table (Tabla de filtros)



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 de la **Filter Table** (Tabla de filtros).
4. Marque la casilla de verificación **Remove** (Eliminar).

   La entrada del filtro se suprime y el dispositivo se actualiza.

Configuración de filtros de notificación mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **Notification Filter** (Filtro de notificación).

Tabla 6-44. Comandos de la CLI para los filtros de notificación SNMP

Comando de la CLI	Descripción
snmp-server filter filter-name oid-tree {**included** | excluded}	Crea o actualiza un filtro de notificación SNMP.
show snmp filters [filtername]	Muestra la configuración de los filtros de notificación SNMP.

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

```
Console (config)# snmp-server filter user1 1 included

Console (config)# end

Console # show snmp filters

Name          OID Tree       Type
-----------   ------------   --------
user1         iso            Included
```

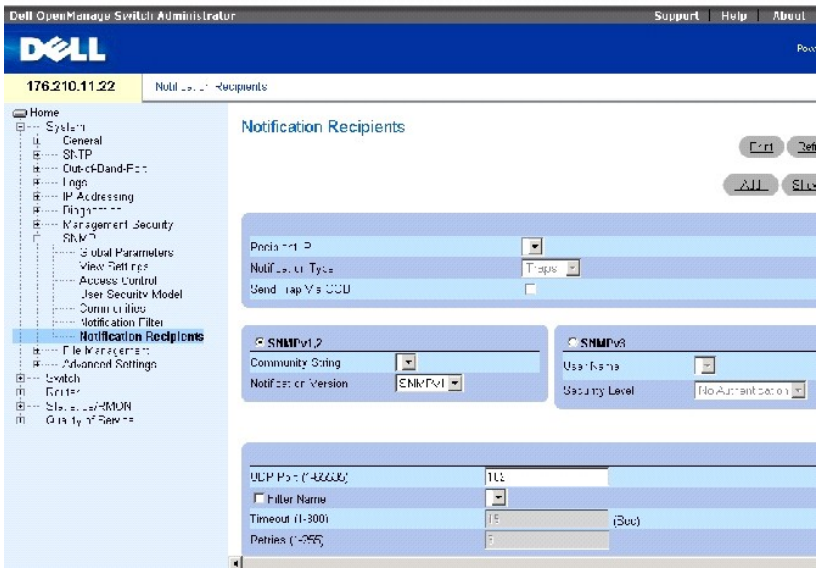
Definición de destinatarios de notificaciones SNMP

La página **Notification Recipients** (Destinatarios de notificaciones) contiene información para definir los filtros que determinan si las capturas se envían a usuarios específicos y el tipo de captura que se envía. Los filtros de notificaciones SNMP ofrecen los siguientes servicios:

- Identificación de los destinos de capturas de gestión
- Filtrado de capturas
- Selección de los parámetros de generación de capturas
- Suministro de comprobaciones de control de acceso

Para abrir la página **Notification Recipients** (Destinatarios de notificaciones), haga clic en **System**→ **SNMP**→ **Notification Recipient** (Sistema→ SNMP→ Destinatario de notificaciones) en la *vista de árbol.*

Ilustración 6-67. Notification Recipients (Destinatarios de notificaciones)



La página **Notification Recipients** (Destinatarios de notificaciones) contiene los siguientes campos:

Recipient IP (IP de destinatario): contiene una lista definida por el usuario de las direcciones IP de los destinatarios de notificaciones.

Notification Type (Tipo de notificación): el tipo de notificación enviada. Los valores de campo posibles son:

Trap (Captura): se envían capturas.

Inform (Informe): se envían informes.

SNMPv1, 2: las versiones 1 o 2 de SNMP se activan para el destinatario seleccionado. Los valores de campo posibles son:

Community String (Cadena de comunidad): contiene una lista de cadenas de comunidad. Seleccione una que se enviará con la notificación.

Notification Version (Versión de la notificación): determina la versión de la notificación. Los valores de campo posibles son:

SNMP V1: se envían capturas de SNMP versión 1.

SNMP V2: se envían capturas o informes de SNMP versión 2.

SNMPv3: se activa SNMP versión 3 para el destinatario seleccionado. Los valores de campo posibles son:

User Name (Nombre de usuario): contiene una lista de usuarios. Seleccione uno para generar notificaciones.

Security Level (Nivel de seguridad): el nivel de seguridad asignado a las notificaciones. Los valores de campo posibles son:

No Authentication (Sin autenticación): el paquete ni se autentica ni se codifica.

Authentication (Autenticación): el paquete se autentica.

Privacy (Privacidad): el paquete se autentica y se codifica.

UDP Port (1-65535) (Puerto UDP [1-65535]): puerto UDP que se utiliza para enviar notificaciones. El valor predeterminado es 162.

Filter Name (Nombre de filtro): marque esta casilla de verificación para aplicar un filtro SNMP definido por el usuario a las notificaciones y seleccionar un filtro SNMP de la lista.

Timeout (1-300) (Tiempo de espera [1-300]): cantidad de tiempo (segundos)que el dispositivo espera antes de reenviar informes. El valor predeterminado es 15 segundos.

Retries (1-255) (Reintentos [1-255]): número máximo de veces que el dispositivo reenvía una petición de informe. El valor predeterminado es 3.

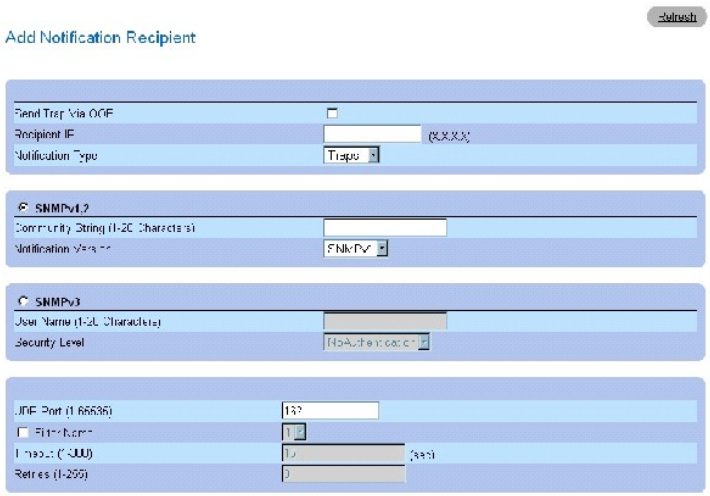
Remove Notification Recipient (Eliminar destinatario de notificaciones): si se selecciona esta opción, se elimina el destinatario de notificaciones seleccionado.

Adición de un nuevo destinatario de notificaciones

1. Abra la página **Notification Recipients** (Destinatarios de notificaciones).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add Notification Recipient** (Agregar destinatario de notificaciones):

Ilustración 6-68. Add Notification Recipient (Agregar destinatario de notificaciones)



3. Defina los campos pertinentes.

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

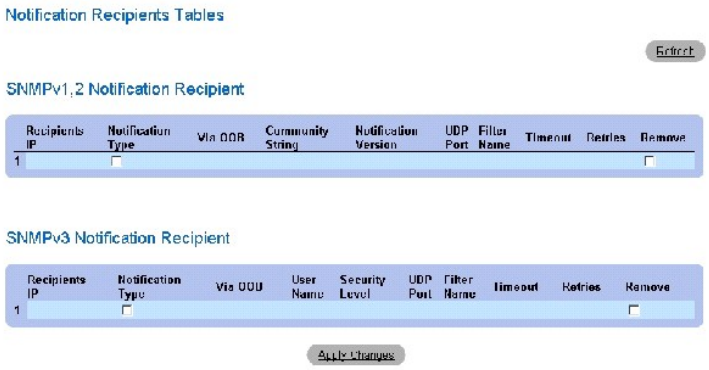
Se agrega el destinatario de notificaciones y el dispositivo se actualiza.

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):

Ilustración 6-69. Notification Recipients Table (Tabla de destinatarios de notificaciones)



Supresión 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 uno o varios destinatarios de notificaciones en **SNMPv1, 2 Notification Recipient** (Destinatario de notificaciones de SNMPv1, 2) y/o en **SNMPv3 Notification Recipient Tables** (Tablas de destinatarios de notificaciones SNMPv3).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se suprimen los destinatarios y el dispositivo se actualiza.

Definición de los destinatarios de notificaciones SNMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **Notification Recipients** (Destinatarios de notificaciones).

Tabla 6-45. Comandos de la CLI para los destinatarios de notificaciones

Comando de la CLI	Descripción
snmp-server host {*dirección_ip* | hostname} community-string [traps | informs] [1 | 2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]	Crea o actualiza un destinatario de notificaciones que recibe notificaciones en SNMP versión 1 o 2.
	Crea o actualiza un destinatario de notificaciones que recibe notificaciones en SNMP versión 3.

snmp-server v3-host {ip-address | hostname} username [traps | informs] {noauth | auth | priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]

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

```
Console (config)# snmp-server host 12.1.1.1 Dell-community

Console (config)# end

Console# show snmp

Community-String  Community-Access  View name  IP address  Type
----------------  ----------------  ---------  ----------  ----

Community-String  Group name  IP address  Type

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

OOB management stations

Community-String  Community-Access  View name  IP address  Type
----------------  ----------------  ---------  ----------  ----

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
--------------  ----  ---------  -------  --------  -----------  ------  -------
```

12.1.1.1	Trap	Dell_community	2	162		1500	3
OOB Notification Receivers							
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
--------	----	--------	-------	----	-------	---	-------
OOB Notification Receivers							
Target Address	Type	Username	Security Level	Udp Port	Filter name	To Sec	Retries
--------	----	--------	-------	----	-------	---	-------

Gestión de archivos

Utilice la página **File Management** (Gestión de archivos) para gestionar el software del dispositivo, el archivo de imagen y los archivos de configuración. Los archivos se pueden descargar o cargar mediante un servidor TFTP.

Visión general de los archivos de gestión

La estructura de los archivos de gestión se compone de los siguientes archivos:

- **Startup configuration file** (Archivo de configuración de inicio): conserva la configuración exacta del dispositivo cuando se apaga o se reinicia el dispositivo. El archivo de inicio conserva los comandos de configuración, y los comandos de configuración del archivo de configuración en ejecución pueden guardarse en el archivo de inicio.
- **Running configuration file** (Archivo de configuración en ejecución): contiene todos los comandos del archivo de inicio, así como todos los comandos especificados durante la sesión actual. Después de 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 inicio se copian en el archivo de configuración en ejecución y se aplican al dispositivo. Durante la sesión, todos los comandos nuevos que se han especificado se agregan a los comandos ya existentes del archivo de configuración en ejecución. Los comandos no se sobrescriben. Para actualizar el archivo de inicio, antes de apagar el dispositivo, hay que copiar el archivo de configuración en ejecución en el archivo de configuración de inicio. La próxima vez que se reinicie el dispositivo, los comandos se vuelven a copiar en el archivo de configuración en ejecución desde el archivo de configuración de inicio
- **Backup Configuration File** (Archivo de configuración de copia de seguridad): contiene una copia de seguridad de la configuración del dispositivo. El archivo de copia de seguridad cambia cuando los archivos de configuración en ejecución o inicio se copian en el archivo de copia de seguridad. Los comandos copiados en el archivo reemplazan los comandos existentes guardados en el archivo de copia de seguridad. El contenido del archivo de copia de seguridad puede copiarse en el archivo de configuración en ejecución o en el archivo de configuración de inicio.
- **Image Files** (Archivos de imagen): las imágenes del sistema se guardan en dos sectores Flash llamados imágenes (Imagen 1 e Imagen 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 se inicia automáticamente desde la imagen no activa. Se trata de una función de seguridad contra fallos que se producen durante el proceso de actualización de inicio.

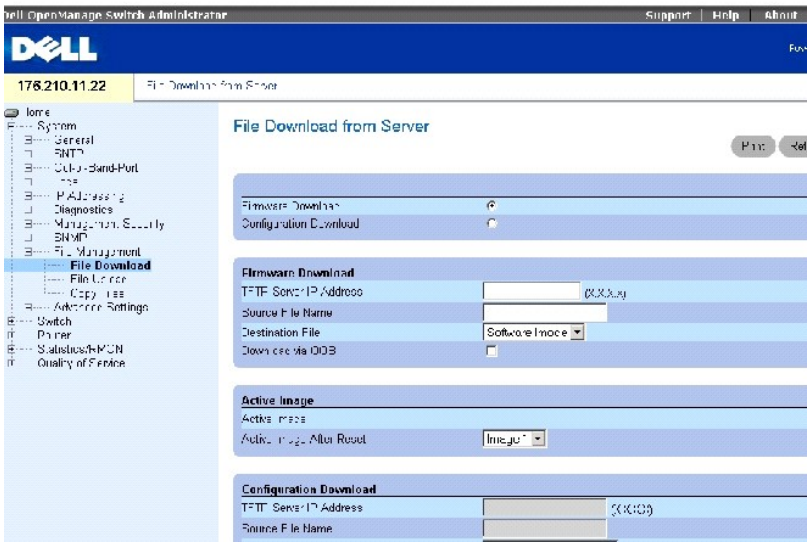
Para abrir la página **File Management** (Gestión de archivos), haga clic en **System**→ **File Management** (Sistema→ Gestión de archivos) en la *vista de árbol.*

Descarga de archivos

La página **File Download From Server** (Descarga de archivos del servidor) contiene campos para descargar el software del servidor TFTP en el dispositivo. El archivo de imagen también se puede descargar desde la página **File Download from Server** (Descarga de archivos del servidor).

Para abrir la página **File Download From Server** (Descarga de archivos del servidor), haga clic en **System**→ **File Management**→ **File Download** (Sistema→ Gestión de archivos→ Descarga de archivos) en la *vista de árbol.*

Ilustración 6-70. File Download From Server (Descarga de archivos del servidor)



La página **File Download From Server** (Descarga de archivos del servidor) contiene los siguientes campos:

Firmware Download (Descarga de firmware): cuando se selecciona esta opción, indica que se ha descargado el archivo de firmware. Si se selecciona esta opción, los campos de **Configuration Download** (Descarga de configuración) aparecen atenuados.

Configuration Download (Descarga de configuración): cuando se selecciona esta opción, indica que se ha descargado el archivo de configuración. Si la opción **Configuration Download** (Descarga de configuración) está seleccionada, los campos de **Firmware Download** (Descarga de firmware) aparecen atenuados.

Firmware TFTP Server IP Address (Dirección IP del servidor TFTP de firmware): la dirección IP del servidor TFTP desde el que se descargan los archivos.

Firmware Source File Name (Nombre de archivo de origen de firmware): el archivo de firmware que se va a descargar.

Firmware Destination File (Archivo de destino de firmware): determina si el archivo se descarga en el archivo de imagen o en el archivo de inicio.

Firmware Download via OOB (Descarga de firmware mediante OOB): descarga el archivo de firmware a través del puerto de gestión fuera de banda.

Active Image (Imagen activa): el archivo de imagen que está actualmente activo.

Active Image After Reset (Imagen activa después de restablecer): el archivo de imagen que está activo después de restablecer el dispositivo. Los valores

posibles son los siguientes:

Image 1 (Imagen 1): el archivo Image 1 está activo después de restablecer el dispositivo.

Image 2 (Imagen 2): el archivo Image 2 está activo después de restablecer el dispositivo.

Configuration File TFTP Server IP Address (Dirección IP del servidor TFTP del archivo de configuración): la dirección IP del servidor TFTP desde donde se descargan los archivos de configuración.

Configuration File Source File Name (Nombre de archivo de origen del archivo de configuración): el archivo de configuración que se va a descargar.

Configuration File Destination (Destino del archivo de configuración): el archivo de destino en el que se van a descargar los archivos de configuración. Los valores posibles son:

Running Configuration (Configuración en ejecución): descarga los archivos de configuración en ejecución.

Startup Configuration Configuración de inicio): descarga los archivos de configuración de inicio.

Backup Configuration (Configuración de copia de seguridad): descarga los archivos de configuración de copia de seguridad.

Configuration Download via OOB (Descarga de configuración mediante OOB): descarga el archivo de configuración a través del puerto de gestión fuera de banda.

Descarga de archivos

1. Abra la página **File Download From Server** (Descarga de archivos del servidor).
2. compruebe la dirección IP del servidor TFTP y asegúrese de que la imagen de software o el archivo de inicio que se van a descargar estén disponibles en el servidor TFTP.
3. Complete los campos **TFTP Server IP Address** (Dirección IP del servidor TFTP), **Source File Name** (Nombre de archivo de origen) (ruta de acceso completa sin la dirección IP del servidor TFTP), y **Destination File** (Archivo de destino) (inicio o imagen de software).

NOTA: La imagen del archivo de imagen sobrescribe la imagen no activa. Se recomienda designar que la imagen no activa se convierta en la imagen activa después de restablecer y, a continuación, restablecer el dispositivo después de la descarga.

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

El software se descarga en el dispositivo.

Activación de los archivos de imagen

1. Abra la página **File Download From Server** (Descarga de archivos del servidor).
2. Seleccione la imagen que se va a activar en el menú descendente **Active Image After Reset** (Imagen activa después de restablecer).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona el archivo de imagen.

NOTA: Para activar el archivo de imagen seleccionado, restablezca el dispositivo. Para obtener información sobre el restablecimiento del dispositivo, consulte el apartado Restablecimiento del dispositivo .

Descarga de archivos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **File Download From Server** (Descarga de archivos del servidor).

Tabla 6-46. Comandos de la CLI para la descarga

Comando de la CLI	Descripción
copy *url_origen url_destino*	Copia un archivo de un origen en un destino.

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

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...

Loading file1 from 172.16.101.101:

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

[OK]

Copy took 0:01:11 [hh:mm:ss]
```

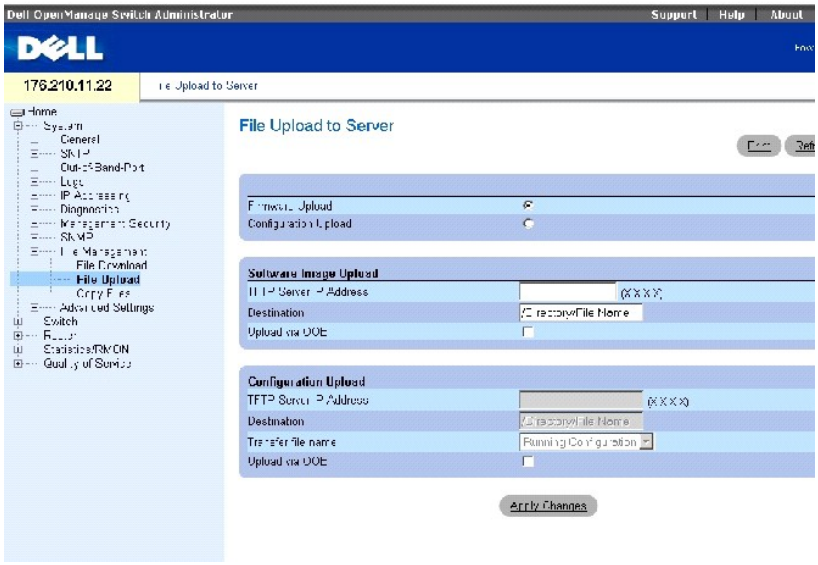
NOTA: Cada uno de los signos ! indica que la descarga de archivos progresa correctamente.

Carga de archivos

La página **File Upload to Server** (Carga de archivos en el servidor) contiene campos para cargar los archivos del servidor TFTP en el dispositivo. El archivo de imagen también se puede cargar desde la página **File Upload to Server** (Carga de archivos en el servidor).

Para abrir la página **File Upload to Server** (Carga de archivos en el servidor), haga clic en **System→ File Management→ File Upload** (Sistema→ Gestión de archivos→ Carga de archivos) en la *vista de árbol.*

Ilustración 6-71. File Upload to Server (Carga de archivos en el servidor)



La página **File Upload to Server** (Carga de archivos en el servidor) contiene los siguientes campos:

Firmware Upload (Carga de firmware): indica que se ha cargado el archivo de firmware. Si la opción **Firmware Upload** (Carga de firmware) está seleccionada, los campos de **Configuration Upload** (Carga de configuración) aparecen atenuados.

Configuration Upload (Carga de configuración): indica que se ha cargado el archivo de configuración. Si la opción **Configuration Upload** (Carga de configuración) está seleccionada, los campos de **Firmware Upload** (Carga de firmware) aparecen atenuados.

Software Image Upload TFTP Server IP Address (Dirección IP del servidor TFTP de carga de imagen de software): la dirección IP del servidor TFTP en la que se carga la imagen de software.

Software Image Upload Destination (Destino de carga de imagen de software): la ruta de acceso del archivo de imagen de software en la que se carga el archivo.

Software Image Upload via OOB (Carga de imagen de software mediante OOB): indica que la imagen de software se carga a través del puerto de gestión fuera de banda.

Configuration Upload TFTP Server IP Address (Dirección IP del servidor TFTP de carga de configuración): la dirección IP del servidor TFTP en la que se carga el archivo de configuración.

Configuration Upload Destination (Destino de carga de configuración): la ruta de acceso del archivo de configuración en la que se carga el archivo.

Configuration Upload Transfer File Name (Nombre de archivo de transferencia de carga de configuración): el archivo de software que se carga. Los valores posibles del campo son:

Running Configuration (Configuración en ejecución): carga el archivo de configuración en ejecución.

Startup Configuration(Configuración de inicio): carga los archivos de configuración de inicio.

Backup Configuration (Configuración de copia de seguridad): carga los archivos de configuración de copia de seguridad.

Configuration Upload via OOB (Carga de configuración mediante OOB): indica que el archivo de configuración se carga a través del puerto de gestión fuera de banda.

Carga de archivos

1. Abra la página **File Upload to Server** (Carga de archivos en el servidor).
2. Defina los campos aplicables en la página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

El software se carga en el servidor.

Carga de archivos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **File Upload to Server** (Carga de archivos en el servidor).

Tabla 6-47. Comandos de la CLI para cargar

Comando de la CLI	Descripción
`copy source-url destination-url`	Copia un archivo de un origen en un destino.

A continuación se muestra un ejemplo del comando de la CLI:

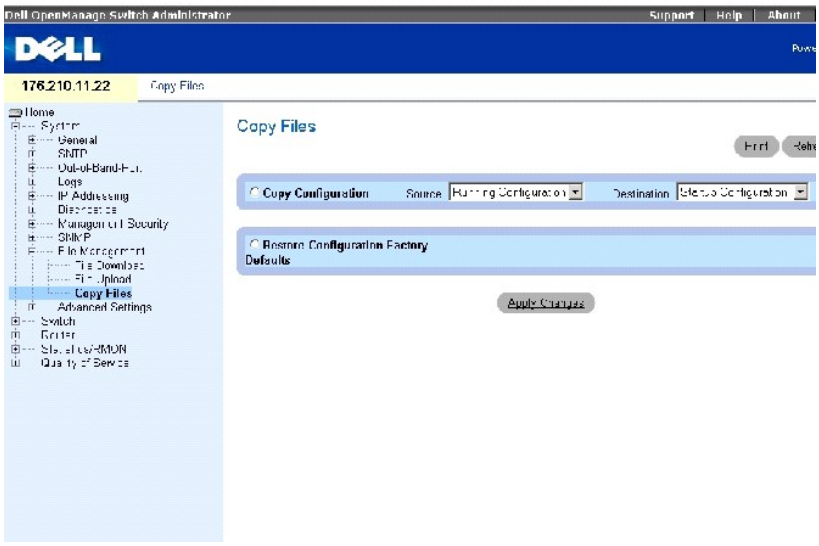
```
---------------------------------------------------


Console# copy image tftp:16.1.1.200/file1
```

Copia de archivos

Utilice la página **Copy Files** (Copiar archivos) para copiar y restaurar los valores predeterminados de la configuración.

Para abrir la página **Copy Files** (Copiar archivos), haga clic en **System**→ **File Management**→ **Copy** (Sistema→ Gestión de archivos→ Copiar) en la *vista de árbol.*

Ilustración 6-72. Copy Files (Copiar archivos)



La página **Copy Files** (Copiar archivos) contiene los siguientes campos:

Copy Configuration (Copiar configuración): especifica que se debe copiar un archivo de configuración.

Source (Origen): el archivo de origen de configuración (en ejecución, de inicio, de copia de seguridad) del que se copia el archivo.

Destination (Destino): archivo de configuración de destino (en ejecución, de inicio o configuración) en el que se copia el archivo.

Restore Configuration Factory Defaults (Restaurar valores predeterminados de configuración de fábrica): si se selecciona esta opción, se especifica que los archivos predeterminados de configuración de fábrica se deben restablecer. Si no se selecciona, se mantienen los valores actuales de configuración.

NOTA: Si se copian archivos en el archivo de configuración en ejecución sólo se agregan datos de configuración; no se sustituye el archivo.

Copia de archivos

1. Abra la página **Copy Files** (Copiar archivos).
2. Seleccione **Copy** (Copiar) o **Restore** (Restaurar) y complete los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se copia el archivo.

Copia de archivos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en la página **Copy Files** (Copiar archivos).

Tabla 6-48. Comandos de la CLI para copiar archivos

Comando de la CLI	Descripción
copy *url_origen url_destino*	Copia un archivo de un origen en un destino.
	Suprime el archivo de configuración de inicio.

`delete startup-config`	

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

```
Console# delete startup-config
```

Definición de la configuración avanzada

Utilice la configuración avanzada para establecer otros atributos globales del dispositivo. Los cambios realizados en estos atributos sólo se aplican después de restablecer el dispositivo. Haga clic en **System**→ **Advanced Settings** (Sistema→ Configuración avanzada) en la vista de árbol para abrir la página **Advanced Settings** (Configuración avanzada).

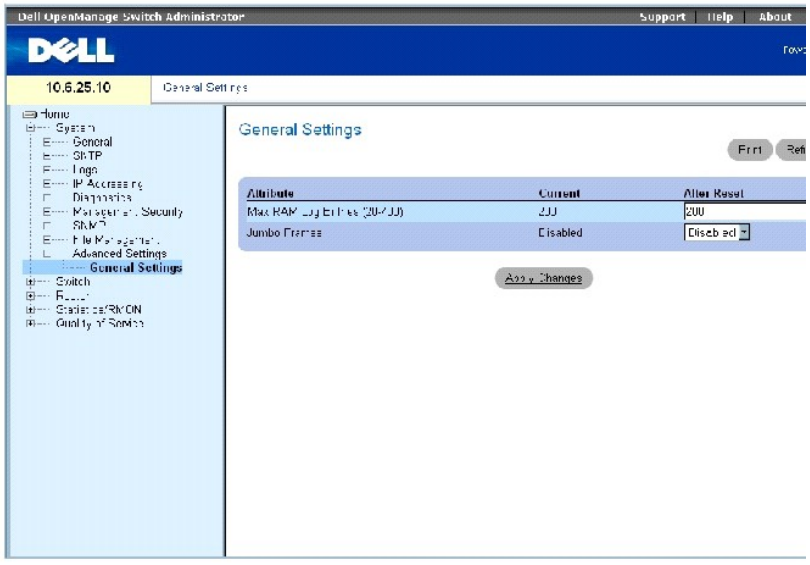
La página **Advanced Settings** (Configuración avanzada) contiene un enlace para configurar los valores generales.

Configuración de los valores generales

Utilice la página **General Settings** (Configuración general) para definir los parámetros generales del dispositivo.

Para abrir la página **General Settings** (Configuración general), haga clic en **System**→ **Advanced Settings**→ **General** (Sistema→ Configuración avanzada→ General) en la *vista de árbol.*

Ilustración 6-73. General Settings (Configuración general)



La página **General Settings** (Configuración general) contiene los siguientes campos:

Current (Actual): número máximo de entradas.

After Reset (Después del restablecimiento): número máximo de entradas después de restablecer el dispositivo. Si se introduce un valor en esta columna,se asigna la memoria a la tabla de campos.

Max RAM Log Entries (20-400) (Entradas máximas de registros RAM [20-400]): número máximo de entradas de la tabla de registros RAM. El valor predeterminado es 200 entradas.

Jumbo Frames (Tramas gigantes): activa el transporte de datos idénticos en menos tramas. De este modo se garantiza un menor coste, un tiempo de procesamiento inferior y menos interrupciones. Las tramas internas pueden verse afectadas por la activación de las tramas gigantes.

Activación de paquetes gigantes

1. Abra la página **General Settings** (Configuración general).
2. Seleccione **Enabled** (Activado) en el campo **Jumbo packets** (Paquetes gigantes).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se activan los paquetes gigantes en el dispositivo.

Visualización de la configuración general mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los campos que se muestran en 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 del registro del sistema almacenados en el búfer interno (RAM).
`port jumbo-frame`	Activa los paquetes gigantes para el dispositivo.

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

```
Console (config)# logging buffered size 300
```

```
Console (config)# port jumbo-frame
```

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la información del conmutador

Sistemas Dell PowerConnect 6024/6024F

En esta sección se proporciona toda la información general y de funcionamiento del sistema para configurar la seguridad de la red, los puertos, las tablas de direcciones, GARP, VLAN, el árbol extensible, el agregado de puertos y la compatibilidad de multidifusión.

Configuración de la seguridad de la red

Utilice la página **Network Security** (Seguridad de la red) para establecer la seguridad de la red a través de las listas de control de acceso y de puertos bloqueados. Para abrir la página **Network Security** (Seguridad de la red), seleccione **Switch**→ **Network Security** (Conmutador→ Seguridad de la red).

La página **Network Security** (Seguridad de la red) proporciona enlaces que le permiten configurar la autenticación basada en puerto, la seguridad del puerto, las listas de control de acceso (ACL) basadas en IP, las ACL basadas en MAC y los enlaces a ACL.

Autenticación basada en puerto (802.1x)

La autenticación basada en puerto permite la autenticación de los usuarios del sistema por puerto a través de un servidor externo. Sólo los usuarios del sistema autenticados y aprobados pueden transmitir y recibir datos. Los puertos se autentican a través del servidor RADIUS mediante el protocolo de autenticación extensible (EAP).

La red 802.1x tiene tres componentes:

- **Autenticadores**: Especifican el puerto que se autentica antes de permitir el acceso al sistema.
- **Solicitantes**: Especifican el sistema principal conectado al puerto autenticado que solicita acceder a los servicios del sistema.
- **Servidor de autenticación**: Especifica el servidor externo, por ejemplo, el servidor RADIUS que realiza la autenticación en nombre del autenticador, e indica si el usuario está autorizado para acceder a los servicios del sistema.

La autenticación basada en puerto crea dos estados de acceso:

- **Acceso controlado**: Permite la comunicación entre el usuario y el sistema, si el usuario está autorizado.
- **Acceso no controlado**: Permite la comunicación no controlada independientemente del estado del puerto.

Actualmente el dispositivo admite la autenticación basada en puerto a través de los servidores RADIUS.

Autenticación avanzada basada en puerto

La autenticación avanzada basada en puerto permite que varios sistemas principales se conecten a un solo puerto. La autenticación avanzada basada en puerto sólo requiere que se autorice un sistema principal para que todos los sistemas principales tengan acceso al sistema. Si el puerto no está autorizado, se negará el acceso a la red a todos los sistemas principales conectados.

La autenticación avanzada basada en puerto también permite la autenticación basada en VLAN. En el conmutador siempre hay disponibles unas VLAN

específicas, incluso si determinados puertos conectados a la VLAN no están autorizados. Por ejemplo, la tecnología de voz sobre IP no necesita la autenticación, mientras que el tráfico de datos sí que la necesita. Se pueden definir las VLAN para las que no es necesaria autorización. Las VLAN no autenticadas están disponibles para los usuarios, aunque los puertos conectados a la VLAN se definan como autorizados.

La autenticación avanzada basada en puerto se implementa en los siguientes modos:

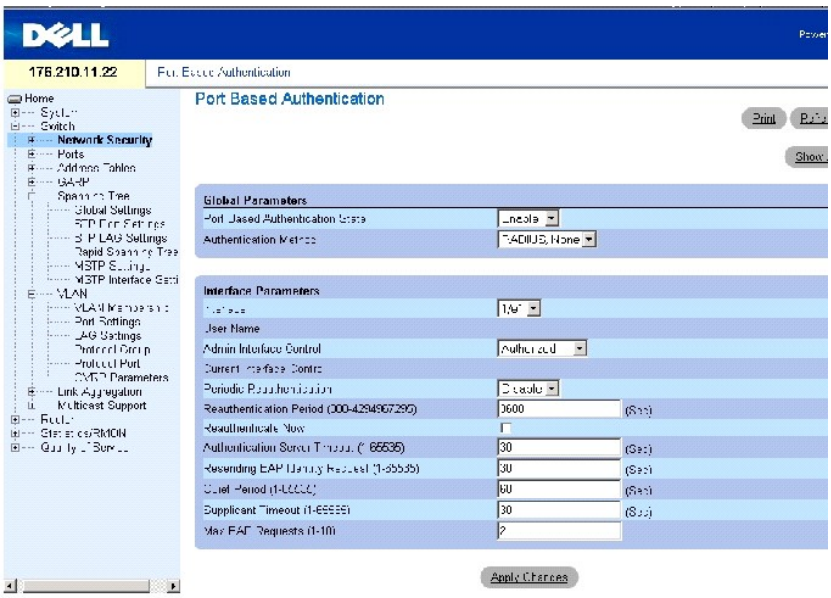
- **Modo de sistema principal único**: Sólo permite que el sistema principal autorizado acceda al puerto.
- **Modo de varios sistemas principales**: Permite que varios sistemas principales se conecten a un solo puerto. Sólo hay que autorizar a un sistema principal para que todos los sistemas principales accedan a la red. Si la autenticación del sistema principal falla o se recibe un mensaje de cierre de sesión-EAPOL, se negará el acceso a la red a todos los clientes conectados.

Configuración de la autenticación basada en puerto

La página **Port Based Authentication** (Autenticación basada en puerto) contiene campos para configurar la autenticación basada en puerto.

Para abrir la página **Port Based Authentication** (Autenticación basada en puerto), haga clic en **Switch→ Network Security→ Port Based Authentication** (Conmutador→ Seguridad de la red→ Autenticación basada en puerto).

Ilustración 7-1. Port Based Authentication (Autenticación basada en puerto)



La página **Port Based Authentication** (Autenticación basada en puerto) contiene los siguientes campos:

Port Based Authentication State (Estado de autenticación basada en puerto): Permite la autenticación basada en puerto del dispositivo. Los valores de campo posibles son:

Enable (Activar): Activa la autenticación basada en puerto del dispositivo.

Disable (Desactivar): Desactiva la autenticación basada en puerto del dispositivo.

Authentication Method (Método de autenticación): El método de autenticación utilizado. Los valores de campo posibles son:

RADIUS, None (RADIUS, Ninguno): Indica que la autenticación del puerto se realiza primero a través del servidor RADIUS. Si la autenticación no se puede alcanzar, el servidor RADIUS autentica el método de gestión utilizado. Sin embargo, si se produce un error, el puerto continúa sin tener autorización y no se permite el acceso.

RADIUS: Indica que la autenticación se realiza en el servidor RADIUS.

None (Ninguno): Indica que no se utiliza ningún método de autenticación.

Interfaz: Contiene una lista de interfaces que se deben autenticar.

User Name (Nombre de usuario): El nombre de usuario tal como se configura en el servidor RADIUS.

Admin Interface Control (Control de interfaz de administración): Define el estado de autorización del puerto. Los valores de campo posibles son:

Auto (Automático): Activa la autenticación basada en puerto por puerto. La interfaz se mueve entre un estado autorizado o no autorizado basado en el intercambio de autenticaciones entre dispositivo y el cliente.

Authorized (Autorizado): Coloca la interfaz en un estado autorizado sin ser autenticada. La interfaz envía y recibe tráfico normal sin autenticación basada en puerto del cliente.

Unauthorized: (No autorizado): Deniega el acceso al sistema de interfaces seleccionado moviendo la interfaz a un estado no autorizado. El dispositivo no puede proporcionar servicios de autenticación al cliente a través de la interfaz.

Current Interface Control (Control de la interfaz actual): El estado de autorización del puerto actual. Un asterisco muestra si el puerto está actualmente desactivado.

Periodic Reauthentication (Reautenticación periódica): Vuelve a autenticar el puerto seleccionado de manera periódica cuando está activado.

Reauthentication Period (300-4294967295) (Período de reautenticación [300-4294967295]): Indica el período de tiempo en el que se vuelve a autenticar el puerto seleccionado. El valor del campo se expresa en segundos. El valor predeterminado del campo es 3600 segundos.

Reauthenticate Now (Reautenticar ahora): Si se selecciona esta opción, se fuerza la reautenticación inmediata del puerto.

Authentication Server Timeout (1-65535) (Tiempo de espera del servidor de autenticación [1-65535]): Define la cantidad de tiempo que pasa antes de que el dispositivo vuelva a enviar una solicitud 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 solicitud de identidad EAP [1-65535]): Define la cantidad de tiempo que pasa antes de volver a enviar solicitudes de EAP. El valor del campo se expresa en segundos. El valor predeterminado del campo es 30 segundos.

Quiet Period (1-65535) (Período pasivo [0-65535]): Define la cantidad de tiempo que el dispositivo permanece en un estado pasivo después de un intercambio de autenticación que no ha salido bien. El intervalo posible del campo es 0-65535. El valor del campo está establecido en segundos. El valor predeterminado del campo es 60 segundos.

Supplicant Timeout (1-65535) (Tiempo de espera del solicitante [1-65535]): Define la cantidad de tiempo que pasa antes de que las solicitudes de EAP se reenvíen al usuario. El valor del campo se expresa en segundos. El valor predeterminado del campo es 30 segundos.

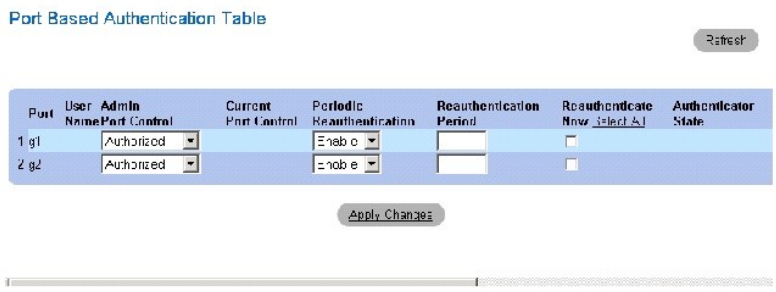
Máximo de solicitudes de EAP (1-10): El número máximo de veces que un dispositivo puede enviar una solicitud de EAP antes de reiniciar el proceso de autenticación si no recibe una respuesta. El intervalo posible de campo es de 1 a 10. El valor predeterminado del campo son dos reintentos.

Visualización de la tabla de autenticación basada en puerto

1. Abra la página **Port Based Authentication** (Autenticación basada en puerto).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Port Based Authentication Table** (Tabla de autenticación basada en puerto):

Ilustración 7-2. Port Based Authentication Table (Tabla de autenticación basada en puerto)



La **Port Based Authentication Table** (Tabla de autenticación basada en puerto) contiene los siguientes campos:

Copy Parameters From Port No. (Copiar parámetros del número de puerto): El puerto del que se copian los parámetros.

Termination Cause (Motivo de la terminación): El motivo por el que ha finalizado la autenticación del puerto.

Copy To (Copiar en): Copia los parámetros de puerto desde un puerto a los puertos seleccionados.

Select All (Seleccionar todo): Selecciona todos los puertos de **Port Based Authentication Table** (Tabla de autenticación basada en puerto).

Copia de los parámetros de Port Based Authentication Table (Tabla de autenticación basada en puerto)

1. Abra la página **Port Based Authentication** (Autenticación basada en puerto).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Port Based Authentication Table** (Tabla de autenticación basada en puerto).

3. Seleccione la interfaz en el campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que se copian los parámetros de autenticación basada en puerto.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian en el puerto seleccionado de **Port Based Authentication Table** (Tabla de autenticación basada en puerto) y el dispositivo se actualiza.

Habilitación de la autenticación basada en puerto mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para habilitar la autenticación basada en puerto tal como aparecen en la página **Port Based Authentication** (Autenticación basada en 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 varios métodos de autenticación, autorización y contabilidad (AAA) para su utilización en interfaces que ejecutan IEEE 802.1X.
dot1x system-auth- control	Activa la red 802.1X globalmente.
dot1x port-control {auto | force- authorized | force- unauthorized}	Controla manualmente el estado de autorización del puerto.
dot1x max-req *recuento*	Establece el número máximo de veces que el dispositivo envía un 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 de un puerto específico habilitado para 802.1X.
dot1x re- authentication	Activa la reautenticación periódica del cliente.
dot1x timeout quiet-period segundos	Establece el número de segundos que el dispositivo permanece en el estado pasivo después de un intercambio de autenticación que no ha salido bien.
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 solicitud de EAP al cliente.
dot1x timeout tx-period *segundos*	Establece el número de segundos que el dispositivo espera una respuesta a una trama de identidad/solicitud - EAP, del cliente, antes de reenviar la solicitud.
show dot1x [**ethernet** *interfaz*]	Muestra el estado de 802.1X para el dispositivo o para la interfaz especificada.
show dot1x users [username nombreusuario]	Muestra los usuarios de 802.1X para el dispositivo.
show dot1x statistics ethernet interfaz	Muestra las estadísticas 802.1X de la interfaz especificada.

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

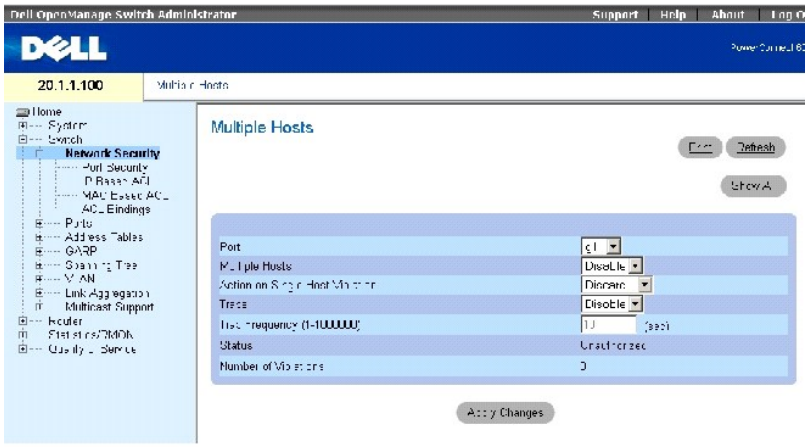
```
Console# show dot1x

Port  Admin Mode  Oper Mode     Reauth Control  Reauth Period  Username
----  ----------  ----------    -------         ------         --------
g11   Auto        Authorized    Ena             3600           Bob
g12   Auto        Authorized    Ena             3600           John
g13   Auto        Unauthorized  Ena             3600           Clark
g14   Force-auth  Authorized    Dis             3600           n/a
```

Configuración de la autenticación avanzada basada en puerto

La página **Multiple Hosts** (Varios sistemas principales) proporciona información para definir la configuración de la autenticación avanzada basada en puerto para puertos específicos.

Para abrir la página **Multiple Hosts** (Varios sistemas principales), haga clic en **Switch**→ **Network Security**→ Multiple Hosts (Conmutador→ Seguridad de la red→ Varios sistemas principales).

Ilustración 7-3. Multiple Hosts (Varios sistemas principales)



La página **Multiple Hosts** (Varios sistemas principales) contiene los siguientes campos:

Port (Puerto): El número de puerto para el que se habilita la autenticación avanzada basada en puerto.

Multiple Hosts (Varios sistemas principales): Activa o desactiva un solo sistema principal para que autorice el acceso al sistema a varios sistemas principales. Este parámetro tiene que estar activado para desactivar el filtrado de entrada o utilizar la seguridad de bloqueo de puerto en el puerto seleccionado.

Action on Single Host Violation (Acción tras la infracción de un solo sistema principal): Define la acción que hay que aplicar a los paquetes que llegan en modo de un solo sistema principal, desde un sistema principal cuya dirección MAC no es la dirección MAC del cliente (solicitante). Los valores de campo posibles son:

Forward (Reenviar): Reenvía los paquetes de origen desconocido aunque no se obtiene la dirección MAC.

Discard (Descartar): Descarta los paquetes procedentes de un origen no obtenido. Éste es el valor predeterminado.

Discard Shutdown (Descartar apagado): Descarta el paquete procedente de cualquier origen no obtenido y bloquea el puerto. Los puertos permanecen apagados hasta que se activan o se restablece el dispositivo.

Traps (Capturas): Activa o desactiva el envío de capturas al sistema principal si se produce una infracción.

Trap Frequency (1-1000000) (Frecuencia de las capturas [1-1000000] [seg]): Define el período de tiempo por el que se envían capturas al sistema principal. El valor predeterminado es 10 segundos.

Status (Estado): El estado del sistema principal. Los valores de campo posibles son:

Unauthorized (No autorizado): Indica que el control del puerto está *Force Unauthorized* (No autorizado forzado), la conexión de puerto desactivada o que el control de puerto es Auto (Automático), pero que un cliente no se ha autenticado a través del puerto.

Not in auto mode (Modo no automático): Indica que el control del puerto es *Forced Authorized* (Autorizado Forzado) y que los clientes tienen acceso de puerto completo.

Single-host Lock (Bloqueo de un único sistema principal): Indica que el control de puerto es *Auto* (Automático) y que un único cliente se ha autenticado a través del puerto.

No Single Host (Sin un único sistema principal): Indica que se ha activado Multiple Host (Varios sistemas principales).

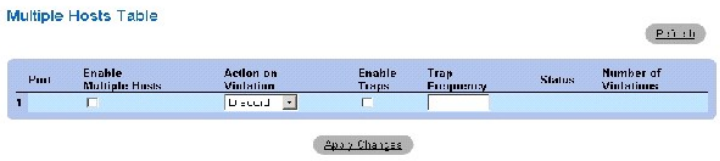
Number of Violations (Número de infracciones): El número de paquetes que llegan a la interfaz en modo de sistema principal único, desde un sistema principal cuya dirección MAC no es la dirección MAC del cliente (solicitante).

Visualización de la tabla de varios sistemas principales

1. Abra la página **Multiple Hosts** (Varios sistemas principales).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Multiple Hosts Table** (Tabla de varios sistemas principales).

Ilustración 7-4. Multiple Hosts Table (Tabla de varios sistemas principales)



Habilitación de varios sistemas principales mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para habilitar la autenticación avanzada basada en puerto tal como aparecen en la página **Multiple Hosts** (Varios sistemas principales).

Tabla 7-2. Comandos de la CLI para varios sistemas principales

Comando de la CLI	Descripción
`dot1x multiple-hosts`	Permite varios sistemas principales (clientes) en un puerto autorizado por 802.1X que tenga el comando de configuración de interfaces de control de puertos dot1x establecido en auto.
`dot1x single-host- violation {forward |discard |discard- shutdown}[trap seconds]`	Configura la acción que se debe realizar cuando una estación, cuya dirección MAC no es la dirección MAC del cliente (solicitante), intenta acceder a la interfaz.

A continuación se muestra un ejemplo del comando de la CLI.

```
Console (config)# interface ethernet g11
```

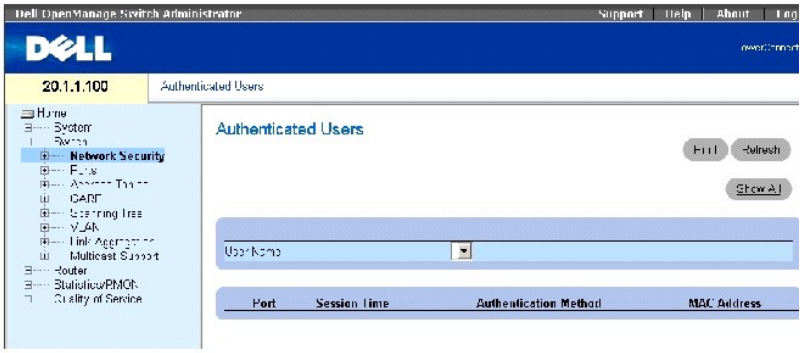
```
Console (config-if)# dot1x multiple-hosts
```

Autenticación de usuarios

La página **Authenticated Users** (Usuarios autenticados) muestra las listas de acceso al puerto del usuario.

Para abrir la página **Authenticated Users** (Usuarios autenticados), haga clic en **Switch**→ **Network Security**→ **Authenticated Users** (Conmutador→ Seguridad de la red→ Usuarios autenticados).

Ilustración 7-5. Authenticated Users (Usuarios autenticados)



La página **Authenticated Users** (Usuarios autenticados) contiene los siguientes campos:

User Name (Nombre de usuario): Lista de los usuarios autorizados a través del servidor RADIUS.

Puerto: Lista los números de puerto utilizados para la autenticación. Los puertos se listan por nombre de usuario.

Session Time (Tiempo de sesión): La cantidad de tiempo que el usuario lleva conectado al dispositivo. El formato de este campo es **Día:Hora:Minuto:Segundos**, por ejemplo, 3 días: 2 horas: 4 minutos: 39 segundos.

Authentication Method (Método de autenticación): El método por el que se autenticó la última sesión. Los valores de campo posibles son:

Remote (Remoto): El usuario se ha autenticado desde un servidor remoto.

None (Ninguno): No se ha autenticado al usuario.

MAC Address (Dirección MAC): La dirección MAC del solicitante.

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 **Authenticated Users Table** (Tabla de usuarios autenticados):

Ilustración 7-6. Authenticated Users Table (Tabla de usuarios autenticados)

Visualización de la autenticación de usuarios mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para autenticar usuarios tal como aparecen en la página **Authenticated Users** (Usuarios autenticados).

Tabla 7-3. Comandos de la CLI para agregar nombres de usuarios

Comando de la CLI	Descripción
show dot1x users [username 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
----    --------    ------------    -----------    -----------------
g12     bob         00:09:27        Remote         00:80:c8:b9:dc:1d
```

Configuración de la seguridad de los puertos

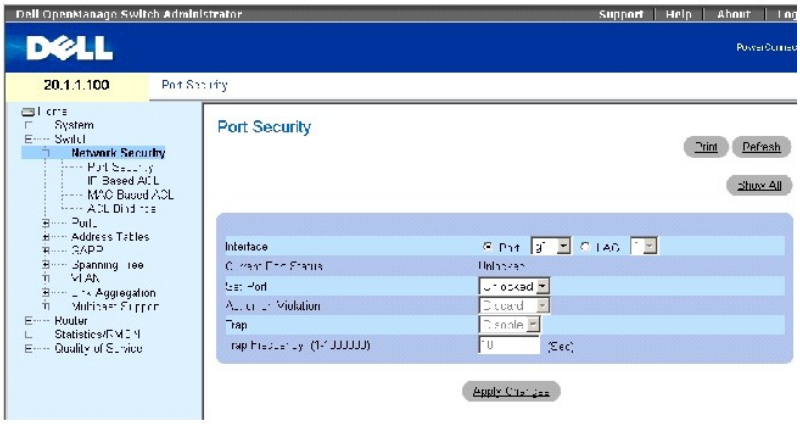
La seguridad de la red puede aumentarse limitando el acceso a un puerto específico sólo a los usuarios que dispongan de direcciones MAC específicas. Las direcciones MAC pueden obtenerse dinámicamente, hasta dicho punto, o pueden configurarse estáticamente. La seguridad de los puertos bloqueados supervisa tanto los paquetes recibidos como los obtenidos que se reciben en puertos específicos. El acceso a los puertos bloqueados está restringido a aquellos usuarios que tengan direcciones MAC específicas. Dichas direcciones se definen manualmente en el puerto o se obtienen en dicho puerto hasta el punto en que 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 (ya sea porque se ha obtenido en un puerto distinto o bien porque resulta desconocida para el sistema), se llama al mecanismo de protección y se pueden proporcionar varias opciones. Los paquetes no autorizados que llegan a un puerto bloqueado se reenvían, de descartan sin captura o se desactiva el puerto de ingreso.

La seguridad del puerto bloqueado también habilita el almacenamiento de una lista de direcciones MAC en el archivo de configuración. Esta lista puede restaurarse una vez restablecido el dispositivo.

Los puertos desactivados sólo se pueden activar desde la página **Port Configuration** (Configuración de puertos).

Para abrir la página **Port Security** (Seguridad del puerto), seleccione **Switch**→ **Network Security**→ **Port Security** (Conmutador→ Seguridad de la red→ Seguridad del puerto).

Ilustración 7-7. Port Security (Seguridad del puerto)



Interfaz: Indica si la seguridad del puerto bloqueado está habilitada en un puerto o LAG.

Current Port Status (Estado actual del puerto): Indica si el puerto está actualmente bloqueado y desactivado o si está desbloqueado.

Set Port (Establecer puerto): Habilita el bloqueo del puerto. Cuando un puerto está bloqueado, todas las direcciones actuales que el conmutador haya obtenido dinámicamente en dicho puerto se transformarán en direcciones MAC estáticas. Cuando el puerto se desbloquea, se eliminan de la lista estática.

Action on Violation (Acción tras infracción): Acción que se aplica a los paquetes que llegan al puerto. El campo aparece atenuado si el puerto está desbloqueado. Los valores posibles son:

Discard (Descartar): Descarta los paquetes procedentes de un origen no obtenido. Éste es el valor predeterminado.

Forward (Reenviar): Reenvía los paquetes procedentes de un origen desconocido. La dirección MAC no se obtiene.

Shutdown (Apagar): Descarta el paquete procedente de cualquier origen no obtenido y envía una captura. Además, el puerto de entrada está desactivado.

Trap (Captura): Habilita o inhabilita el envío de una captura cuando se recibe un paquete en un puerto bloqueado.

Trap Frequency (Frecuencia de capturas): Cantidad de tiempo (en segundos) que transcurre entre capturas.

Definición de un puerto bloqueado

1. Abra la página **Port Security** (Seguridad del puerto).
2. Seleccione un tipo de interfaz y un número.
3. Seleccione **Locked** (Bloqueado) en el menú descendente **Set Port** (Establecer puerto).
4. Complete los campos restantes:
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto bloqueado se agrega a la tabla **Port Security** (Seguridad de puertos) y el dispositivo se actualiza.

Copia de los parámetros de la tabla de puertos bloqueados

1. Abra la página **Port Security** (Seguridad del puerto).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **Port Security Table** (Tabla de seguridad de puertos).

   Los campos de **Port Security Table** (Tabla de seguridad de puertos) son los mismos que los campos de la página **Port Security** (Seguridad de puertos).
3. En el campo **Copy Parameters from** (Copiar parámetros de), seleccione una interfaz en el menú descendente **Port** (Puerto) o **LAG**.

   Las definiciones de la seguridad del puerto referentes a esta interfaz se copian a las interfaces seleccionadas. Consulte el Paso 5.
4. Marque la casilla de verificación **Copy to** (Copiar a) para seleccionar las interfaces a las que se copiarán las definiciones de la seguridad del puerto.

   O bien:

   Haga clic en **Select All** (Seleccionar todo) para copiar las definiciones a todos los puertos o LAG.
5. Haga clic en **Apply Changes** (Aplicar cambios).

   Los parámetros se copian en los puertos o LAG seleccionados en **Port Security Table** (Tabla de seguridad de puertos) y el dispositivo se actualiza.

Configuración de la seguridad de los puertos bloqueados mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar la seguridad de los puertos bloqueados tal como aparecen en la página **Port Security** (Seguridad del puerto).

Tabla 7-4. Comandos de la CLI para la seguridad de puertos bloqueados

Comando de la CLI	Descripción
`port security [forward | discard | discard-shutdown] [trap segundos]`	Inhabilita la obtención de nuevas direcciones en una interfaz.
`show ports security [ethernet interfaz | port-channel port- número_canal]`	Muestra el estado de bloqueo de los puertos.

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

```
Console (config)# interface ethernet g1

Console (config-if)# port security forward trap 100

Console (config-if)# exit

Console (config)# exit

Console# show ports security
```

Port	status	Action	Trap	Frequency	Counter

----	------	------	----	---------	-------
g1	Locked	Forward	Enabled	100	0
g2	Unlocked	-	-	-	-
...					
g24	Unlocked	-	-	-	-
ch1	Unlocked	-	-	-	-
...					
ch7	Unlocked	-	-	-	-

Definición de ACL basadas en IP

Las listas de control de acceso (ACL) permiten a los administradores de red definir acciones y reglas de clasificación para puertos de entrada específicos. El conmutador admite hasta 1.024 ACL. Los paquetes que entran en un puerto de entrada, con una ACL activa, son admitidos o bien se les deniega la entrada y se inhabilita el puerto de entrada. Si se les deniega la entrada, el usuario puede inhabilitar el puerto.

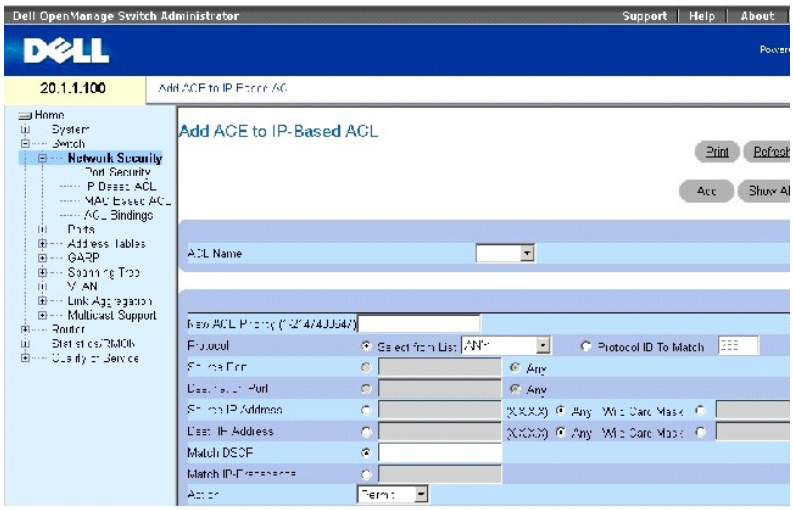
Por ejemplo, un administrador de red define una regla de ACL que dice que el puerto número 20 puede recibir paquetes TCP, aunque si se recibe un paquete UDP, éste se elimina.

Las ACL constan de entradas de control de acceso (ACE) que están compuestas de filtros que determinan las clasificaciones del tráfico. El número total de ACE que puede definirse en todas las ACL es de 1024.

Utilice la página **Add ACE to IP Based ACL** (Agregar ACE a ACL basada en IP) para definir ACE basadas en IP.

Para abrir la página **Add ACE to IP Based ACL** (Agregar ACE a ACL basada en IP), seleccione **Switch**→ **Network Security**→ **IP Based ACL** (Conmutador→ Seguridad de la red→ ACL basada en IP).

Ilustración 7-8. Add ACE to IP Based ACL (Agregar ACE a ACL basada en IP)



La página **Add ACE to IP Based ACL** (Agregar ACE a ACL basada en IP) contiene los siguientes campos:

ACL Name (Nombre de ACL): ACL definidas por el usuario.

New ACE Priority (Nueva prioridad de ACE): La prioridad de ACE que determina qué ACE coincide con un paquete en función de la primera coincidencia.

Protocol (Protocolo): Habilita la creación de una ACE de acuerdo con un protocolo específico.

Select from List (Seleccionar de la lista): Haga clic en esta opción para seleccionar entre una lista de protocolos en los que la ACE se puede basar.

Protocol ID To Match (ID de protocolo para coincidir): Haga clic en esta opción para agregar un protocolo definido por el usuario mediante el cual los paquetes coincidan con la ACE.

NOTA: Utilice any (cualquiera) para seleccionar todos los protocolos IP.

Source Port (Puerto de origen): El puerto de origen TCP/UDP. Este campo sólo está activo si se ha seleccionado la opción **800/6-TCP** o **800/17-UDP** del menú descendente **Select from List** (Seleccionar de la lista).

Destination Port (Puerto de destino): El puerto de destino TCP/UDP. Este campo sólo está activo si se ha seleccionado la opción **800/6-TCP** o **800/17-UDP** del menú descendente **Select from List** (Seleccionar de la lista).

Source IP Address (Dirección IP de origen): Hace coincidir la dirección IP de origen hacia la cual se direccionan los paquetes con la ACE.

Wild Card Mask (Máscara comodín): Máscara comodín de dirección IP de origen. Las máscaras comodín especifican qué bits se utilizan y cuáles se ignoran. Una máscara comodín de 255.255.255.255 indica que ningún bit es importante. Un comodín de 0.0.0.0 indica que todos los bits son importantes.

Dest. IP Address (Dirección IP de destino): Hace coincidir la dirección IP del puerto de destino hacia la cual se direccionan los paquetes con la ACE.

Wild Card Mask (Máscara comodín): La máscara comodín de la dirección IP de destino. Seleccione **Match DSCP** (Coincidencia con DSCP) o **Match IP Precedence** (Coincidencia con precedencia de IP):

Match DSCP (Coincidencia con DSCP): Hace coincidir el valor del paquete DSCP con la ACE. Para hacer coincidir paquetes con las ACL se utiliza el valor

de DSCP o el de precedencia de IP.

Match IP Precedence (Coincidencia con precedencia de IP): Hace coincidir el valor del paquete de precedencia de IP con la ACE. Para hacer coincidir paquetes con las ACL se utiliza el valor de DSCP o el de precedencia de IP.

Action (Acción): Acción de reenvío de ACL. Los valores posibles son:

Permit (Permitir): Reenvía los paquetes que cumplen los criterios de ACL.

Deny (Denegar): Rechaza los paquetes que cumplen los criterios de ACL.

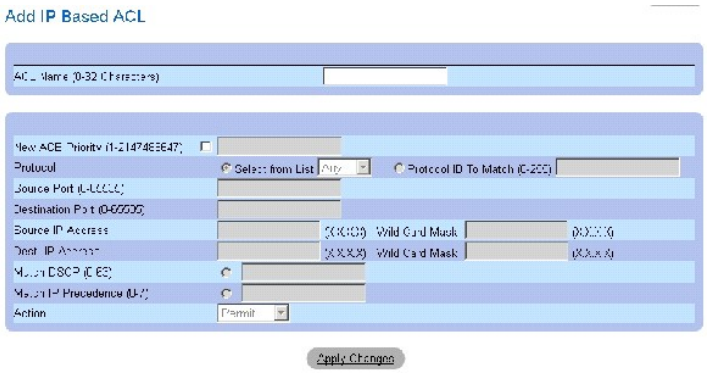
Shutdown (Apagado): Rechaza los paquetes que cumplen con los criterios de ACL y desactiva el puerto al que se dirigía el paquete. Los puertos se vuelven a activar desde la página **Ports Configuration** (Configuración de puertos), consulte el apartado **Definición de la configuración de puertos** .

Para ver todas las ACE conectadas a la ACE, haga clic en **Show All** (Mostrar todo).

Adición de una ACL basada en IP

1. Abra la página **Add ACE to IP Based ACL** (Agregar ACE a ACL basada en IP).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add IP Based ACL** (Agregar ACL basada en IP).

Ilustración 7-9. Add IP Based ACL (Agregar ACL basada en IP)



3. Escriba el **ACL Name** (Nombre de ACL).
4. Marque la casilla de verificación **New ACE Priority** (Nueva prioridad de ACE) y defina todos los campos de la página.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la ACL basada en IP y el dispositivo se actualiza.

Modificación de una ACE basada en IP

NOTA: Las ACE sólo pueden modificarse cuando la ACL a la que pertenecen no está vinculada a una interfaz.

1. Abra la página **Add ACE to IP Based ACL** (Agregar ACE a ACL basada en IP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar todas las ACE de la ACL.
3. Seleccione una ACL del campo **ACL Name** (Nombre de ACL).
4. Modifique los campos según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la ACE basada en IP y el dispositivo se actualiza.

Adición de nuevas ACE a una ACL basada en IP

1. Abra la página **Add ACE to IP Based ACL** (Agregar ACE a ACL basada en IP).
2. Seleccione una ACL del campo **ACL Name** (Nombre de ACL).
3. Defina los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La ACE se asigna a la ACL basada en IP.

5. Haga clic en **Apply Changes** (Aplicar cambios) y rellene los parámetros de la nueva ACE de las ACE adicionales respecto a una ACE existente.

Reclasificación de las ACE de una ACL

1. Abra la página **Add ACE to IP Based ACL** (Agregar ACE a la ACL basada en IP) y seleccione la ACL que debe utilizarse en el menú descendente **ACL Name** (Nombre de ACL).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **ACEs Associated with IP-ACL** (ACE asociadas con ACL basada en IP).

3. Escriba un número de prioridad que clasifique las ACE según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La ACE se reclasifica y el dispositivo se actualiza.

Eliminación de ACL

1. Abra la página **Add ACE to IP Based ACL** (Agregar ACE a la ACL basada en IP) y seleccione la ACL que debe utilizarse en el menú descendente **ACL Name** (Nombre de ACL).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **ACEs Associated with IP-ACL** (ACE asociadas con ACL basada en IP).

3. Marque la casilla de verificación **Remove ACL** (Eliminar ACL).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la ACL basada en IP y el dispositivo se actualiza.

Asignación de ACE basadas en IP a ACL mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar las ACE basadas en IP a las ACL tal como aparecen en la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).

Tabla 7-5. Comandos de la CLI para asignar ACE basadas en IP a ACL

Comando de la CLI	Descripción
ip access-list *nombre*	Crea ACL de IP y entra en la modalidad de configuración de lista de acceso basada en IP.
permit {**any** | *protocolo*} {**any** | source *comodín_origen*} {**any** | destination *comodín_destino*} [dscp *número dscp* | ip-precedence *prioridad_ip*]	Permite el tráfico si las condiciones definidas en la declaración de permiso coinciden.

deny [disable-port] {**any** | *protocolo*} {**any** | source *comodín_origen*} {**any** | destination *comodín_destino*} [dscp *número dscp* | ip-precedence *prioridad_ip*]	Deniega el tráfico si las condiciones definidas en la declaración de negación coinciden.
show access-lists [*nombre*]	Muestra las listas de control de acceso definidas en el conmutador.

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

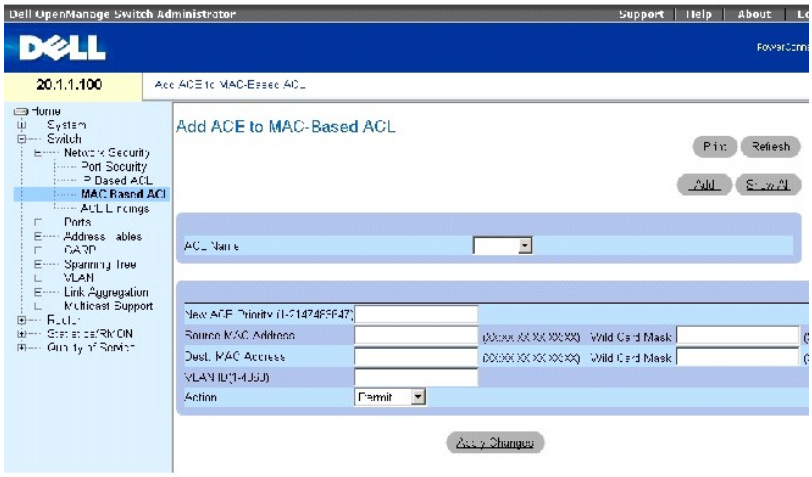
```
Console (config)# ip access-list Dell

Console (config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56

Console (config-ip-al)# deny any 192.1.1.10 0.0.0.255 any

Console# show access-lists

IP access list one

permit ip host 12.1.1.1 any

permit rsvp host 176.30.40.1 any

Console# show access-lists

IP access list Dell

permit rsvp 12.1.1.1 0.0.0.0 any dscp 56

deny any 192.1.1.10 0.0.0.255 any
```

Definición de ACL basadas en MAC

En la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC) los administradores de red pueden definir una ACL basada en MAC. Para obtener una explicación de las ACL, consulte el apartado **Definición de ACL basadas en IP** .

Para abrir la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC), seleccione **Switch→ Network Security→ MAC based ACL** (Conmutador→ Seguridad de la red→ ACL basada en MAC).

Ilustración 7-10. Add ACE to MAC Based ACL (Agregar ACE a ACL basada en MAC)



La página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC) contiene los siguientes campos:

ACL Name (Nombre de ACL): ACL definida por el usuario.

New ACE Priority (Nueva prioridad de ACE): La prioridad de ACE que determina qué ACE coincide con un paquete en función de la primera coincidencia.

Source MAC Address (Dirección MAC de origen): Hace coincidir la dirección MAC de origen desde la cual se direccionan los paquetes con la ACE.

Wild Card Mask (Máscara comodín): La máscara comodín de la dirección MAC de origen. Los comodines se utilizan para enmascarar toda una dirección MAC de origen o parte de la misma. Las máscaras comodín especifican qué bits se utilizan y cuáles se ignoran. Una máscara comodín de FF:FF:FF:FF:FF:FF indica que ningún bit es importante. Un comodín de 00.00.00.00.00.00 indica que todos los bits son importantes.
Por ejemplo, si la dirección MAC de origen es E0:3B:4A:C2:CA:E2 y la máscara comodín es 00:3B:4A:C2:CA:FF, se utilizan los primeros dos bits de la MAC, mientras que se ignoran los dos últimos.

Destination MAC Address (Dirección MAC de destino): Hace coincidir la dirección MAC de destino hacia la cual se direccionan los paquetes con la ACE.

Wild Card Mask (Máscara comodín): La máscara comodín de la dirección MAC de destino. Los comodines se utilizan para enmascarar toda una dirección MAC de destino o parte de la misma.

VLAN ID (ID de VLAN): Hace coincidir el ID de VLAN del paquete con la ACE. Los valores posibles son 1-4094.

Action (Acción): Indica la acción de reenvío de ACL. Los valores posibles del campo son:

Permit (Permitir): Reenvía los paquetes que cumplen los criterios de ACL.

Deny (Denegar): Rechaza los paquetes que cumplen los criterios de ACL.

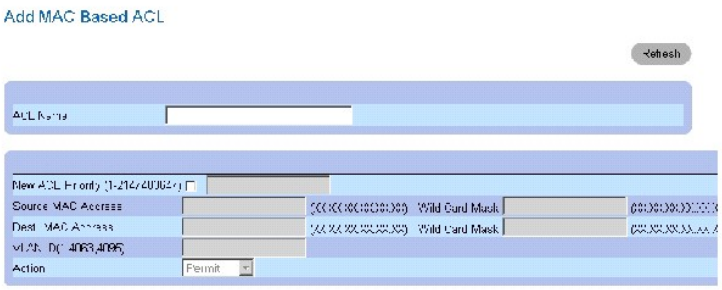
Shutdown (Apagado): Rechaza el paquete que cumple los criterios de ACL y desactiva el puerto al que se dirigía el paquete. Los puertos se vuelven a activar desde la página **Ports Configuration** (Configuración de puertos, consulte el apartado **Definición de la configuración de puertos** .

Adición de una ACL basada en MAC

1. Abra la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).

2. Haga clic en **Add** (Agregar) para abrir la página **Add MAC Based ACL** (Agregar ACL basada en MAC).

Ilustración 7-11. Add MAC Based ACL (Agregar ACL basada en MAC)



3. Escriba el **ACL Name** (Nombre de ACL).
4. Para agregar una nueva ACE a la ACL creada recientemente, marque la casilla de verificación **New ACE Priority** (Nueva prioridad de ACE) y defina los campos **Source MAC Address** (Dirección MAC de origen) y **Dest MAC Address** (Dirección MAC de destino), **VLAN ID** (ID de VLAN) y **Action** (Acción).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la ACL basada en MAC y el dispositivo se actualiza.

Modificación de una ACE basada en MAC

1. Abra la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).
2. Seleccione una ACL del campo **ACL Name** (Nombre de ACL).
3. Modifique los campos obligatorios.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los campos se modifican y el dispositivo se actualiza.

Adición de ACE a una ACL basada en MAC

NOTA: Las ACE sólo pueden agregarse si la ACL no está vinculada a una interfaz.

1. Abra la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).
2. Seleccione una ACL del campo **ACL Name** (Nombre de ACL).
3. Defina los campos **New ACE Priority** (Nueva prioridad de ACE), **Source MAC Address** (Dirección MAC de origen) y **Dest MAC Address** (Dirección MAC de destino), **VLAN ID** (ID de VLAN) y **Action** (Acción).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La ACE se asigna a la ACL basada en MAC.

NOTA: Para agregar más de una ACE a una ACL existente, haga clic en **Apply Changes** (Aplicar cambios) y complete los parámetros de la nueva ACE.

Visualización de ACE específicas de ACL

1. Abra la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **ACEs Associated with MAC ACL** (ACE asociadas con ACL basada en MAC).

Eliminación de ACL

NOTA: Las ACL sólo pueden eliminar si no están vinculadas a una interfaz.

1. Seleccione una ACL.
2. Abra la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).
3. Haga clic en **Show All** (Mostrar todo) para visualizar la página **ACEs Associated with MAC ACL** (ACE asociadas con ACL basada en MAC).
4. Marque la casilla de verificación **Remove ACL** (Eliminar ACL).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la ACL basada en MAC y el dispositivo se actualiza.

Eliminación de ACE de una ACL

1. Seleccione una ACL.
2. Abra la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).
3. Haga clic en **Show All** (Mostrar todo) para visualizar la página **ACEs Associated with MAC ACL** (ACE asociadas con ACL basada en MAC).
4. Marque la casilla de verificación **Remove ACE** (Eliminar ACE) de la fila de la ACE que debe eliminarse.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la ACL basada en MAC y el dispositivo se actualiza.

Asignación de ACE basadas en MAC a ACL mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar las ACE basadas en IP a las ACL tal como aparecen en la página **Add ACE to MAC Based ACL** (Agregar ACE a ACL basada en MAC).

Tabla 7-6. Comandos de la CLI para ACE basada en MAC

Comando de la CLI	Descripción
mac access-list *nombre*	Crea ACL de MAC de nivel 2 y entra en la modalidad de configuración de lista de acceso basada en MAC.
permit {any | host source *comodín_origen*} {any | destination *comodín_destino*}[vlan *id_vlan*]	Permite el tráfico si las condiciones definidas en la declaración de permiso coinciden.
deny [disable-port] {any | source *comodín_origen*} {any | destination *comodín_destino*}[vlan *id_vlan*]	Deniega el tráfico si las condiciones definidas en la declaración de negación coinciden.
show access-lists [*nombre*]	Muestra las listas de control de acceso configuradas en el conmutador.

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

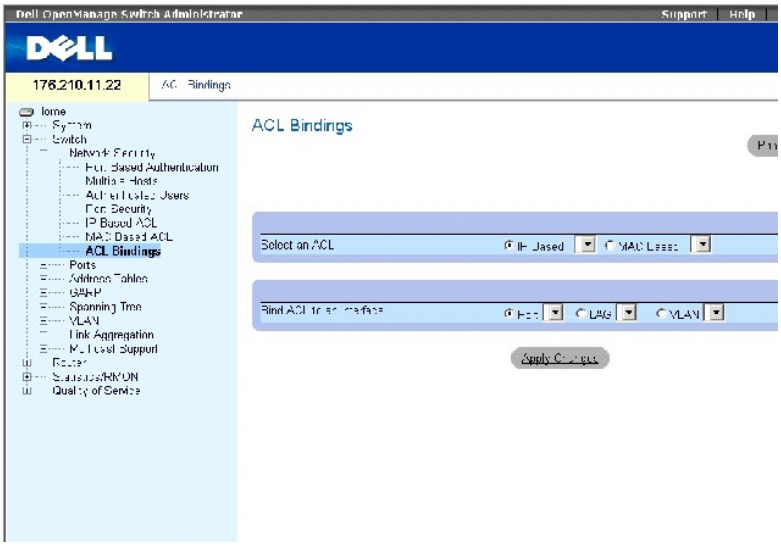
```
Console (config)# mac access-list dell

Console (config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 4

Console (config-mac-al)# deny 6:6:6:6:6:6 0:0:255:255:255:255
```

Configuración de la vinculación de ACL

Cuando se vincula una ACL a una interfaz, todas las reglas de ACE que se hayan definido se aplican a la interfaz seleccionada. Utilice las páginas **ACL Bindings** (Vinculaciones de ACL) para asignar listas de ACL a interfaces y métodos de clasificación.

Para abrir la página **ACL Bindings** (Vinculaciones de ACL), seleccione **Switch**→ **Network Security**→ **ACL Binding** (Conmutador→ Seguridad de la red→ Vinculaciones de ACL).

Ilustración 7-12. ACL Bindings (Vinculaciones de ACL)



La página **ACL Bindings** (Vinculaciones de ACL) contiene los siguientes campos:

Select an ACL (Seleccionar una ACL): El tipo de ACL con el que coinciden los paquetes entrantes. Los paquetes pueden coincidir con ACL basadas en IP o ACL basadas en direcciones MAC.

Bind ACL to Interface (Vincular ACL a interfaz): La interfaz y el tipo de interfaz al cual se conecta la ACL. Puede conectar la ACL a un puerto, LAG o una VLAN.

Asignación de una ACL a una interfaz

1. Abra la página **ACL Bindings** (Vinculaciones de ACL).
2. Seleccione el tipo de ACL del campo **Select ACL** (Seleccionar ACL).
3. Seleccione la interfaz a la que se conecta la ACL en el campo **Bind ACL to an Interface** (Vincular ACL a una interfaz).

NOTA: Siempre que una ACL esté asignada a un puerto, LAG o VLAN, los flujos procedentes de dicha interfaz de entrada que no coincidan con la ACL se hacen coincidir con la regla predeterminada, que es rechazar los paquetes que no coincidan.

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

La ACL se conecta a la interfaz.

Eliminación de una entrada de ACL Bindings Table (Tabla de vinculaciones de ACL)

1. Abra la página **ACL Bindings** (Vinculaciones de ACL).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **ACL Bindings Table** (Tabla de vinculaciones de ACL).
3. Marque la casilla de verificación **Remove** (Eliminar) de la entrada que desee eliminar.

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

La entrada seleccionada se elimina de la tabla y el dispositivo se actualiza.

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 visualizar **ACL Bindings Table** (Tabla de vinculaciones de ACL).

Los campos de **ACL Bindings Table** (Tabla de vinculaciones de ACL) 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) para visualizar **ACL Bindings Table** (Tabla de vinculaciones de ACL).
3. Seleccione una interfaz del campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione un puerto/tronco del menú descendente **Port / LAG** (Puerto/LAG) o **VLAN**.

Las definiciones de esta interfaz se copiarán a los puertos/troncos de destino seleccionados.

5. Marque la casilla de verificación **Copy to** (Copiar en) de la entrada que deba editarse o, para copiar las definiciones a todos los puertos/troncos disponibles, haga clic en **Select All** (Seleccionar todo).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian a los puertos/troncos de destino a **ACL Bindings Table** (Tabla de vinculaciones de ACL) y el dispositivo se actualiza.

Asignación de pertenencia a ACL mediante comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar la pertenencia a ACL tal como aparecen en la página **ACL Bindings** (Vinculaciones de la ACL).

Tabla 7-7. Comandos de la CLI para la vinculación de la ACL

Comando de la CLI	Descripción
`class-map class-map-name [match-all | match-any]`	Crea asignaciones de clase y entra en el modo de configuración de asignación de clases.
`match access-group` *`nombre_acl`*	Define los criterios de coincidencia para clasificar el tráfico.
`show class-map [`*`nombre_asignación_clase`*`]`	Muestra todas las asignaciones de clases configuradas en el dispositivo.

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

```
Console (config)# class-map class1 match-all

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit
```

```
Console (config)# exit


Console> exit


Console> show class-map class1


Class Map match-all class1 (id4)
```

Configuración de los puertos

En la página **Ports** (Puertos) se proporcionan enlaces para configurar la funcionalidad de los puertos, incluidas varias funciones avanzadas como, por ejemplo, el control de tormentas y la duplicación de puertos y para poder efectuar pruebas con puertos virtuales.

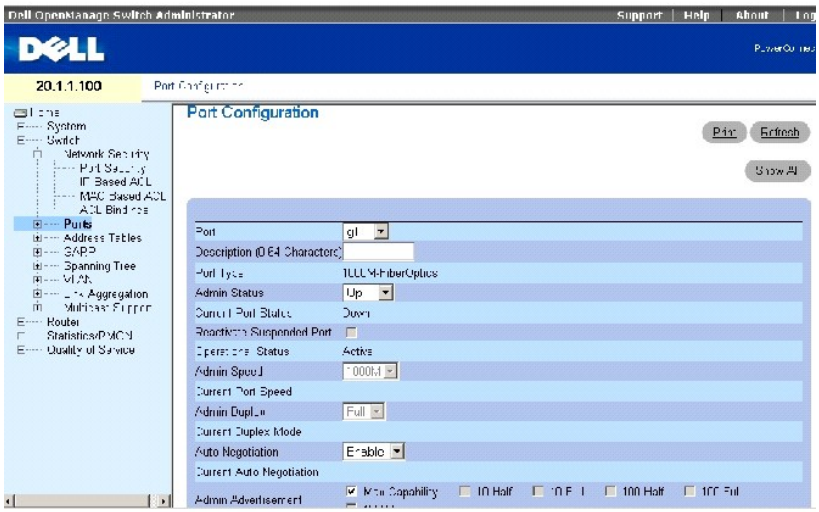
Para abrir la página **Ports** (Puertos), seleccione **Switch**→ **Ports** (Conmutador→ Puertos).

Definición de la configuración de puertos

Utilice la página **Port Configuration** (Configuración de puertos) para definir los parámetros del puerto.

Para abrir la página **Port Configuration** (Configuración de puertos), haga clic en **Switch**→ **Ports**→ **Port Configuration** (Conmutador→ Puertos→ Configuración de puertos) en la vista de árbol.

Ilustración 7-13. Port Configuration (Configuración de puertos)



La página **Port Configuration** (Configuración de puertos) contiene los siguientes campos:

Port (Puerto): El número de puerto para el que se definen los parámetros de puerto.

Description (0-64 Characters) (Descripción [0-64 caracteres]): Una breve descripción de la interfaz como, por ejemplo, Ethernet.

Port Type (Tipo de puerto): El tipo de puerto.

Admin Status (Estado admin): Activa o desactiva el reenvío de tráfico a través del puerto.

Current Port Status (Estado actual del puerto): Especifica si el puerto está actualmente operativo o no.

Reactivate Suspended Port (Reactivar puerto suspendido): Reactiva un puerto si el puerto 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 posibles del campo son:

- **Suspended** (Suspendido): El puerto está activo actualmente y no recibe ni transmite tráfico.
- **Active** (Activo): El puerto está activo actualmente y recibe y transmite tráfico.
- **Disable** (Desactivado): El puerto está actualmente desactivado y no recibe ni transmite tráfico.

Admin Speed (Velocidad admin): La velocidad configurada del puerto. El tipo de puerto determina qué opciones de configuración de velocidad hay disponibles. Puede designar la velocidad de administración sólo cuando el puerto está inhabitado.

Current Port Speed (Velocidad actual del puerto): Velocidad del puerto sincronizado (en bps).

Admin Duplex (Admin. dúplex): El modo dúplex de puerto en bps. **Full** (Completo) indica que la interfaz admite la transmisión entre el dispositivo y el cliente en ambas direcciones simultáneamente. **Half** (Medio) 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): 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 partes del enlace que permite que un puerto comunique su velocidad de transmisión, modo dúplex y capacidades de control de flujo a la otra parte.

Current Auto Negotiation (Negociación automática actual): La configuración actual de la negociación automática.

Admin Advertisement (Aviso de administración): Especifica las funciones que debe anunciar el puerto. Los valores de campo posibles son:

- **Max Capability** (Capacidad máxima): Indica que se pueden aceptar todas las velocidades del puerto y los valores de Duplex mode (Modo dúplex).
- **10 Half** (10 Medio): Indica que el puerto anuncia una velocidad de 10 Mbps y modalidad de dúplex medio.
- **10 Full** (10 Completo): Indica que el puerto anuncia una velocidad de 10 Mbps y modalidad de dúplex completo.
- **100 Half** (100 Medio): Indica que el puerto anuncia una velocidad de 100 Mbps y modalidad de dúplex medio.

100 Full (100 Completo): Indica que el puerto anuncia una velocidad de 100 Mbps y modalidad de dúplex completo.

1000 Full (1000 Completo): Indica que el puerto anuncia una velocidad de 1000 Mbps y modalidad de dúplex completo.

Current Advertisement (Aviso actual): El puerto comunica su velocidad al puerto adyacente para iniciar el proceso de negociación. Los valores de campo posibles son los especificados en el campo Admin Advertisement (Aviso de administración).

Neighbor Advertisement (Aviso adyacente): El puerto adyacente (el puerto al que está conectada la interfaz seleccionada) anuncia sus funciones al puerto para iniciar el proceso de negociación. Los valores posibles son los especificados en el campo Admin Advertisement (Aviso de administración).

Back Pressure (Contrapresión): Habilita el modo de contrapresión en el puerto. El modo de contrapresión se utiliza con el modo dúplex medio para inhabilitar la recepción de mensajes en los puertos. La contrapresión no es compatible con los puertos fuera de banda.

Current Back Pressure (Contrapresión actual): La configuración de la contrapresión actual.

Flow Control (Control de flujo): Habilita o inhabilita el control de flujo o habilita la negociación automática del control de flujo en el puerto.

Current Flow Control (Control de flujo actual): La configuración del control de flujo actual.

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 utilizar 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 asegurar que se conecten los pares correctos. La MDIX automática no funciona en los puertos FE cuando la negociación. MDIX no es compatible con los puertos fuera de banda.

Los valores posibles son:

MDIX (Media Dependent Interface with Crossover) (MDIX [Interfaz dependiente de los soportes con cable cruzado]): Se utiliza para concentradores y conmutadores.

MDI (Media Dependent Interface) (MDI [Interfaz dependiente de los soportes]): Se utiliza para estaciones finales.

Current MDI/MDIX (MDI/MDIX actual): Indica la configuración de MDIX del dispositivo actual. Los valores posibles del campo son:

MDI: La configuración actual de MDI es MDI.

MDIX: La configuración actual de MDI es MDIX.

Auto (Automático): El valor se establece automáticamente.

LAG: Especifica si el puerto forma parte de un LAG.

PVE: Habilita un puerto como puerto PVE (Private VLAN Edge). Cuando se define un puerto como PVE, éste evita la base de datos de reenvío (FDB) y reenvía todo el tráfico de unidifusión, de multidifusión y de difusión a un enlace ascendente (excepto a los paquetes MAC para mí). Los enlaces ascendentes pueden ser un puerto o un LAG. El tráfico de los enlaces ascendentes se distribuye a todas las interfaces.

Definición de los parámetros de puerto

1. Abra la página **Port Configuration** (Configuración de puertos).
2. Seleccione un puerto en el campo **Port** (Puerto).
3. Defina las variables en el cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del 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) para visualizar **Port Security Tabla** (Tabla de seguridad de puertos).

Configuración de los puertos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los puertos tal como aparecen en la página **Ports Configuration** (Configuración de puertos).

Tabla 7-8. Comandos de la CLI para la configuración de puertos

Comando de la CLI	Descripción
`interface ethernet` *interfaz*	Entra en el modo de configuración de interfaz para configurar una interfaz de tipo Ethernet.
`description` *cadena*	Agrega una descripción a una configuración de interfaz.
`shutdown`	Inhabilita las interfaces que forman parte del contexto establecido actualmente.
`set interface active {ethernet` *interfaz* `| port- channel` *número_canal_puerto*`}`	Reactiva una interfaz que está apagada por motivos de seguridad.
`speed {10 | 100 | 1000}`	Configura la velocidad de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
`duplex {half | full}`	Configura el funcionamiento dúplex completo o dúplex medio de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
`negotiation`	Habilita el funcionamiento con negociación automática para los parámetros de velocidad y dúplex de una interfaz determinada.
`back-pressure`	Habilita la contrapresión en una interfaz determinada.
`flowcontrol {auto | on | off}`	Configura el control de flujo en una interfaz determinada.
`mdix {on | auto}`	Habilita el cable cruzado automático en una interfaz o un canal de puertos determinados.
`show interfaces configuration [ethernet` *interfaz* `| port-channel` *número_canal_puerto* `oob- eth` *interfaz*`]`	Muestra el estado de la configuración de todas las interfaces configuradas.
`show interfaces status [ethernet` *interfaz* `| port- channel` *número_canal_puerto* `oob-eth` *interfaz*`]`	Muestra el estado de todas las interfaces configuradas.
`show interfaces description [ethernet` *interfaz* `| port-channel` *número_canal_puerto* `oob- eth` *interfaz*`]`	Muestra la descripción de todas las interfaces configuradas.

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

```
Console (config)# interface ethernet g18

Console (config-if)# description RD_SW#3

Console (config-if)# speed 100

Console (config-if)# shutdown

Console (config-if)# no shutdown

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)# exit

Console (config)# exit

Console> set interface active ethernet g9

Console> show interfaces status
```

					Flow	Link	Back	Mdix
Port	Type	Duplex	Speed	Neg	ctrl	State	Pressure	Mode
---	------	----	---	---	-----	-----	-----	-----
g1	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Off
g2	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Off
g3	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Off

					Flow	Link	Back
Ch	Type	Duplex	Speed	Neg	control	State	Pressure
---	--------	-----	----	----	------	------	-------
ch1	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch2	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch3	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch4	Unknown	Unknown		Unknown	Off	Not Present	Unknown

```
Console# show interfaces configuration
```

					Flow	Admin	Back
Ch	Type	Duplex	Speed	Neg	control	State	Pressure
---	-------	---	---	----	-------	-----	--------
ch1	Unknown			Enabled	Off	Up	Disabled
ch2	Unknown			Enable d	Off	Up	Disabled
ch3	Unknown			Enable d	Off	Up	Disabled

```
Console# show interfaces description ethernet 1
```

Port	Description
-----	-----------------
g1	connect_to_server

Definición de la configuración de LAG

Los conmutadores de múltiples niveles admiten la agrupación de varias conexiones en una única conexión lógica de capacidad agregada denominada grupo de agregado de conexiones (LAG). A menudo, se denomina a los LAG como troncos o conexiones agregadas.

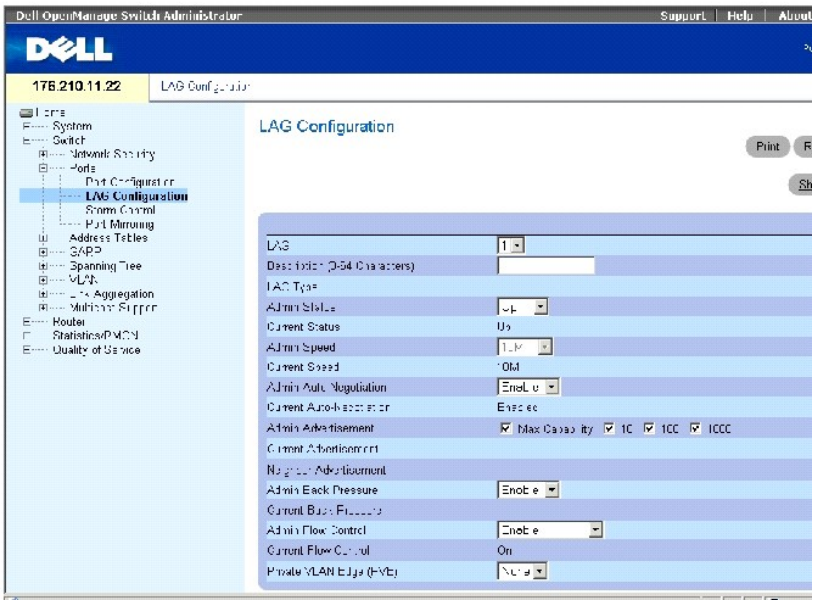
Utilice la página **LAG Configuration** (Configuración de LAG) para configurar los parámetros de LAG. El conmutador admite hasta siete puertos por LAG y siete LAG por sistema. Si la configuración del puerto se modifica mientras éste es miembro de un LAG, el cambio de configuración sólo se hace efectivo una vez que se ha eliminado el puerto del LAG.

Para obtener información sobre adición y la asignación de puertos a los LAG, consulte el apartado **Agregación de puertos** .

Para abrir la página **LAG Configuration** (Configuración de LAG), haga clic en **Switch**→ **Ports**→ **LAG Configuration** (Conmutador→ Puertos→ Configuración de

LAG) en la vista de árbol.

Ilustración 7-14. LAG Configuration (Configuración de LAG)



La página **LAG Configuration** (Configuración de LAG) contiene los siguientes campos:

LAG: Contiene una lista de números de LAG.

Description (0-64 Characters) (Descripción [0-64 caracteres]): Descripción del puerto.

LAG Type (Tipo de LAG): Los tipos de puerto de que consta el LAG.

Admin Status (Estado admin): Habilita o inhabilita el reenvío de tráfico a través del LAG seleccionado.

Current Status (Estado actual): Indica si el LAG está operativo actualmente.

Admin Speed (Velocidad admin): La velocidad a la cual está funcionando el LAG.

Current Speed (Velocidad actual): La velocidad actual a la cual está funcionando el LAG.

Admin Auto Negotiation (Negociación automática admin): Habilita o inhabilita la negociación automática en el LAG. La negociación automática es un protocolo entre dos partes del enlace que permite que un LAG comunique su velocidad de transmisión, modo dúplex y capacidades de control de flujo (el valor predeterminado es inhabilitado) a la otra parte.

Current Auto Negotiation (Negociación automática actual): La configuración actual de la negociación automática.

Admin Advertisement (Aviso de administración): Especifica las funciones que debe anunciar el LAG. Los valores de campo posibles son:

Max Capability (Capacidad máxima): Indica que se pueden aceptar todas las velocidades del LAG y los valores de Duplex mode (Modo dúplex).

10: Indica que el LAG anuncia una velocidad de 10 Mbps y modalidad de dúplex completo.

100: Indica que el LAG anuncia una velocidad de 100 Mbps y modalidad de dúplex completo.

1000: Indica que el LAG anuncia una velocidad de 1000 Mbps y modalidad de dúplex completo.

Current Advertisement (Aviso actual): El LAG comunica sus funciones al LAG adyacente para iniciar el proceso de negociación. Los valores de campo posibles son los especificados en el campo Admin Advertisement (Aviso de administración).

Neighbor Advertisement (Aviso adyacente): El LAG adyacente (el LAG al que está conectada la interfaz seleccionada) anuncia sus funciones al LAG para iniciar el proceso de negociación. Los valores posibles son los especificados en el campo Admin Advertisement (Aviso de administración).

Admin Back Pressure (Admin. contrapresión): Habilita o inhabilita el modo de contrapresión en el dispositivo. El modo de contrapresión se utiliza con el modo dúplex medio para inhabilitar la recepción de mensajes en los puertos.

Current Back Pressure (Contrapresión actual): Indica si el modo de contrapresión está habilitado o inhabilitado.

Admin Flow Control (Control de flujo admin): Habilita o inhabilita el control de flujo o habilita la negociación automática del control de flujo en el LAG.

Current Flow Control (Control de flujo actual): La configuración del control de flujo designada por el usuario.

Definición de los parámetros del LAG

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Seleccione un LAG en el campo **LAG**.
3. Defina los campos disponibles.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG se guardan en el dispositivo.

Visualización de la tabla de configuración de LAG

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **LAG Configuration Table** (Tabla de configuración de LAG).

Configuración de LAG con comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los LAG tal como aparecen en la página **LAG Configuration** (Configuración de LAG).

Tabla 7-9. Comandos de la CLI para la configuración de LAG

Comando de la CLI	Descripción
`interface port-channel` *`número_canal_puerto`*	Entra en el modo de configuración de interfaz de un canal de puertos específico.
	Asocia un puerto con un canal de puertos.

channel-group *número_canal_puerto* mode {on | auto}	
show interfaces port- channel [*número_canal_puerto*]	Muestra información de canal de puertos (qué puertos son miembros de dicho 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 ethernet g5

Console (config-if)# channel-group 1 mode on

Console (config-if)# exit

Console# show interfaces port-channel

Channel     Port

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

Ch 1        Active   g1, g2, g5   Inactive g3

Ch 2        Active   g2

Ch 3        Inactive g8
```

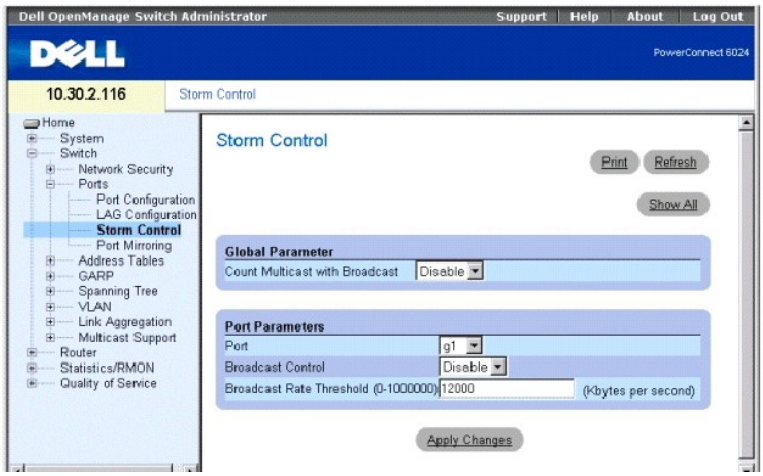
Habilitación del control de tormentas

Una tormenta de difusión 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 cargan en la red, lo que provoca una tensión en los recursos de ésta o que se agote el tiempo de espera.

El sistema mide la velocidad de difusión y de multidifusión entrantes por separado en cada puerto y descarta los paquetes cuando la velocidad supera un valor definido por el usuario. El control de tormentas se habilita por dispositivo, al definir el tipo de paquete y la velocidad a la que se transmiten los paquetes. Los grupos de puertos proporcionan protección contra tormentas a todo un grupo de puertos.

Utilice la página **Storm Control** (Control de tormentas) para habilitar y configurar el control de tormentas. Para abrir la página **Storm Control** (Control de tormentas), haga clic en **Switch**→ **Ports**→ **Storm Control** (Conmutador→ Puertos→ Control de tormentas) en la vista de árbol.

Ilustración 7-15. Página Storm Control (Control de tormentas)



Count Multicast with Broadcast (Contar multidifusión con difusión): **Enable** (Habilitar) efectúa un recuento del tráfico de difusión y de multidifusión; **Disable** (Inhabilitar) sólo efectúa un recuento del tráfico de difusión.

Port (Puerto): El puerto desde el cual se habilita el control de tormentas.

Broadcast Control (Control de difusión): Habilita o inhabilita el reenvío de tipos de paquetes desconocidos en el dispositivo.

Broadcast Rate Threshold (Umbral de velocidad de difusión): La velocidad máxima (kilobytes por segundo) a la que se reenvían los paquetes desconocidos. El intervalo es 0-148.800. El valor predeterminado es 12000. Todos los valores se redondean a los 64 Kbps más próximos. Si el valor del campo se encuentra por debajo de 64 Kbps, el valor se redondea hasta los 64 Kbps.

Modificación de los parámetros del puerto de control de tormentas

1. Abra la página **Storm Control** (Control de tormentas).
2. Complete los campos de esta página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del puerto de control de tormentas se guardan en el dispositivo.

Copia de los parámetros de la tabla de configuración del control de tormentas

1. Abra la página **Storm Control** (Control de tormentas).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **Storm Control Settings Table** (Tabla de configuración del control de tormentas).
3. Seleccione el puerto desde el que desee copiar la configuración que aparece en el campo **Copy Parameters from Port** (Copiar parámetros del puerto).
4. Marque la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que se copian las definiciones del control de tormentas, o bien haga clic en **Select All** (Seleccionar todo) para copiar las definiciones a todos los puertos.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian a los puertos seleccionados de **Storm Control Settings Table** (Tabla de configuración del control de tormentas) y el dispositivo se actualiza.

Configuración del control de tormentas mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar el control de tormentas tal como se muestran en la

página **Storm Control** (Control de tormentas).

Tabla 7-10. Comandos de la CLI para el control de tormentas

Comando de la CLI	Descripción
`port storm-control include-multicast`	Habilita al dispositivo para que pueda contar paquetes de multidifusión junto con los paquetes de difusión.
`port storm-control broadcast enable`	Habilita el control de tormentas de difusión.
`port storm-control broadcast rate` *`velocidad`*	Configura la velocidad de difusión máxima.
`show ports storm-control` *`puerto`*	Muestra la configuración del 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 g1

Console (config-if)# port storm-control broadcast enable

Console (config-if)# port storm-control broadcast rate 100000

Console (config-if)# exit
```

Port	Broadcast and Multicast Storm Control [Kbytes/sec]	
----	----------	
g1		100000
g2		Disabled
...		
g24		Disabled

Definición de sesiones de duplicación de puertos

La duplicación de puertos supervisa y duplica el tráfico de red mediante el reenvío de copias de paquetes entrantes y salientes desde un puerto a un puerto de supervisión. La duplicación de puertos puede utilizarse como herramienta de diagnóstico o como función de depuración de errores. También activa la supervisión del rendimiento del conmutador.

Los administradores de red configuran la duplicación de puertos seleccionando un puerto específico para copiar todos los paquetes y diferentes puertos desde los que se copian los paquetes. Antes de configurar la duplicación de puertos, tenga en cuenta lo siguiente:

- Los puertos supervisados no pueden funcionar más rápido que los puertos supervisores.

- El número máximo de puertos de origen es ocho.
- Sólo se puede configurar una sesión de duplicación cada vez.

Las restricciones siguientes se aplican a los puertos configurados como puertos de destino:

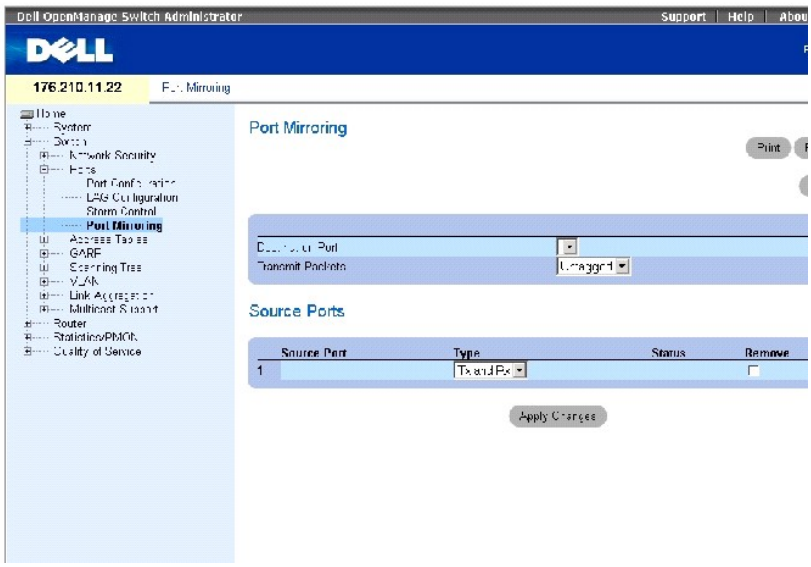
- Los puertos no pueden estar configurados como puertos de origen.
- Los puertos no pueden ser miembros de un LAG.
- Las interfaces IP no se configuran en el puerto.
- El GVRP no se activa en el puerto.
- El puerto no es miembro de una VLAN.
- Sólo se puede definir un puerto de destino.

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.
- Todos los paquetes deben tener una etiqueta cuando se transmiten desde el puerto de destino.
- Todos los paquetes RX/TX deben supervisarse para el mismo puerto.

Para abrir la página **Port Mirroring** (Duplicación de puertos), haga clic en **Switch**→ **Ports**→ **Port Mirroring** (Conmutador→ Puertos→ Duplicación de puertos) en la vista de árbol.

Ilustración 7-16. Port Mirroring (Duplicación de puertos)



La página **Port Mirroring** (Duplicación de puertos) contiene los siguientes campos:

Destination Port (Puerto de destino): Contiene una lista de los números de puerto desde los que se puede copiar el tráfico de puerto.

Transmit Packets (Transmisión de paquetes): Especifica si los paquetes se transmiten con o sin etiqueta desde el puerto de destino.

Source Port (Puerto de origen): Número de puerto para el que se duplica el tráfico de puerto.

Type (Tipo): Especifica el tipo de tráfico supervisado. Los valores posibles del campo son:

TX: Sólo supervisa los paquetes transmitidos.

RX: Sólo supervisa los paquetes recibidos.

TX y RX: Supervisa los paquetes transmitidos y los paquetes recibidos.

Status (Estado): Indica si el puerto está supervisado actualmente (**Active**) o no está supervisado (**Not Ready**).

Remove (Eliminar): Si se selecciona esta opción, se 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** (Agregar) para visualizar la página **Add Source Port** (Agregar puerto de origen).
3. Seleccione el puerto de origen en el menú descendente **Source Port** (Puerto de origen).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los campos de la sesión de duplicación de puertos se habilita para el puerto y el dispositivo se actualiza.

Modificación de una sesión de duplicación de puertos

1. Abra la página **Port Mirroring** (Duplicación de puertos).
2. Modifique los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los campos de la sesión de duplicación se modifican y el dispositivo se actualiza.

Supresión de una sesión de duplicación de puertos

1. Abra la página **Port Mirroring** (Duplicación de puertos).
2. Marque la casilla de verificación **Remove** (Eliminar).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La sesión de duplicación se suprime y el dispositivo se actualiza.

Configuración de una sesión de duplicación de puertos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar una sesión de duplicación de puertos tal como se muestra en la página **Port Mirroring** (Duplicación de puertos).

Tabla 7-11. Comandos de la CLI para la duplicación de puertos

Comando de la CLI	Descripción
port monitor *interfaz_src* [rx | tx]	Inicia una sesión de supervisión de puertos.
	Muestra el estado de la supervisión de puertos.

`show ports monitor`	

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

```
Console (config-if)# port monitor g2
```

Configuración de las tablas de direcciones

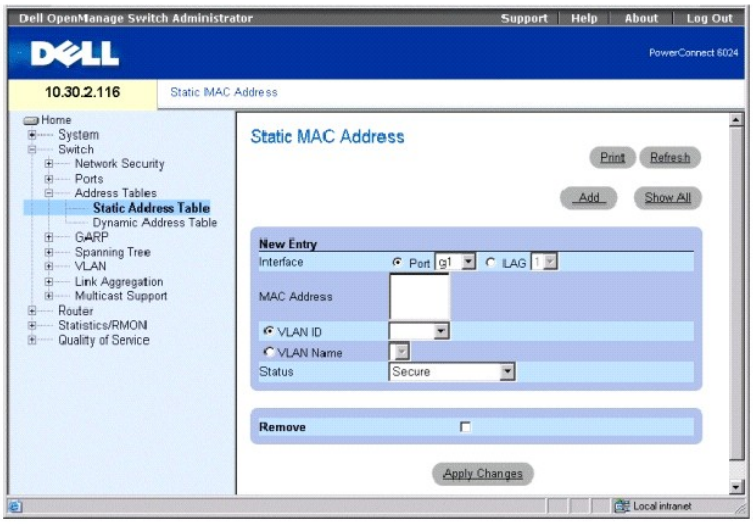
Las direcciones MAC se almacenan en bases de datos de direcciones estáticas o de direcciones dinámicas. Las direcciones estáticas las define el usuario. Las dinámicas las obtiene el sistema y se borran tras agotarse un tiempo de espera concreto. Un paquete direccionado hacia un destino almacenado en una de las bases de datos se reenvía de inmediato a los puertos. Las tablas de direcciones estáticas y dinámicas se pueden ordenar por interfaz, por VLAN y por tipo de interfaz. Además, las direcciones pueden agregarse a las tablas de direcciones estáticas y dinámicas.

Para abrir la página **Address Table** (Tabla de direcciones), haga clic en **Switch**→ **Address Table** (Conmutador→ Tabla de direcciones) en la vista de árbol.

Definición de direcciones estáticas

La página **Static Address** (Dirección estática) contiene una lista de direcciones MAC estáticas. Éstas se pueden agregar y eliminar en **Static MAC Address Table** (Tabla de dirección MAC estática). Para abrir la página **Static Address** (Dirección estática), haga clic en **Switch**→ **Address Table**→ **Static Address** (Conmutador→ Tabla de direcciones→ Dirección estática) en la vista de árbol.

Ilustración 7-17. Página Static MAC Address (Dirección MAC estática)



Interface (Interfaz): El puerto o LAG específico al que se aplica la dirección MAC estática.

MAC Address (Dirección MAC): La dirección MAC indicada en la lista de direcciones estáticas actuales.

NOTA: Sólo se visualizan las direcciones MAC asignadas a la interfaz y VLAN específicas. Para ver las direcciones MAC asignadas a una VLAN distinta, elija la VLAN del selector de VLAN.

VLAN ID (ID de VLAN): El valor del ID de la VLAN conectada a la dirección 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 (Segura): Garantiza que no se suprima una dirección MAC de puerto bloqueado.

Permanent (Permanente): La dirección MAC es permanente.

Delete on Reset (Suprimir al restablecer): La dirección MAC se suprime al restablecer el dispositivo.

Delete on Timeout (Suprimir al agotarse el tiempo de espera): La dirección MAC se suprime cuando transcurre el tiempo de espera especificado.

Adición de una dirección MAC estática

1. Abra la página **Static MAC Address** (Dirección MAC estática).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add Static MAC Address** (Agregar dirección MAC estática).
3. Complete los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva dirección estática se agrega a **Static MAC Address Table** (Tabla de dirección MAC estática) y el dispositivo se actualiza.

Modificación de una dirección estática de la tabla de direcciones MAC estáticas

1. Abra la página **Static MAC Address** (Dirección MAC estática).
2. Modifique los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección estática MAC se modifica y el dispositivo se actualiza.

Eliminación de una dirección estática de la tabla de direcciones estáticas

1. Abra la página **Static MAC Address** (Dirección MAC estática).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **Static MAC Address Table** (Tabla de dirección MAC estática).
3. Seleccione una entrada de la tabla.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección estática se suprime y el dispositivo se actualiza.

Configuración de los parámetros de direcciones estáticas mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los parámetros de direcciones estáticas tal como aparecen en la página **Static MAC Address** (Dirección MAC estática).

Tabla 7-12. Comandos de la CLI para las direcciones estáticas

Comando de la CLI	Descripción
	Agrega una dirección de origen de estación de nivel MAC

bridge address mac-address {ethernet *interfaz* | port- channel *número_canal_puerto*} [permanent | delete-on-reset | delete- on-timeout | secure]	estática a la tabla de puentes.
show bridge address-table static [vlan *vlan*] [ethernet *interfaz* | port- channel *número_canal_ puerto*]	Muestra clases de entradas creadas de manera estática en la base de datos de reenvío de puente.

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

```
Console (config)# interface vlan 1 console

(config-vlan)# bridge address 3aa2.64b3.a245 ethernet g8 permanent....



Console (config-vlan)# exit

Console (config)#exit

Console> show bridge address-table static



Aging time is 300 sec



Vlan  Mac Address           Port   Type

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

1     3a:a2:64:b3:a2:45     g8     permanent
```

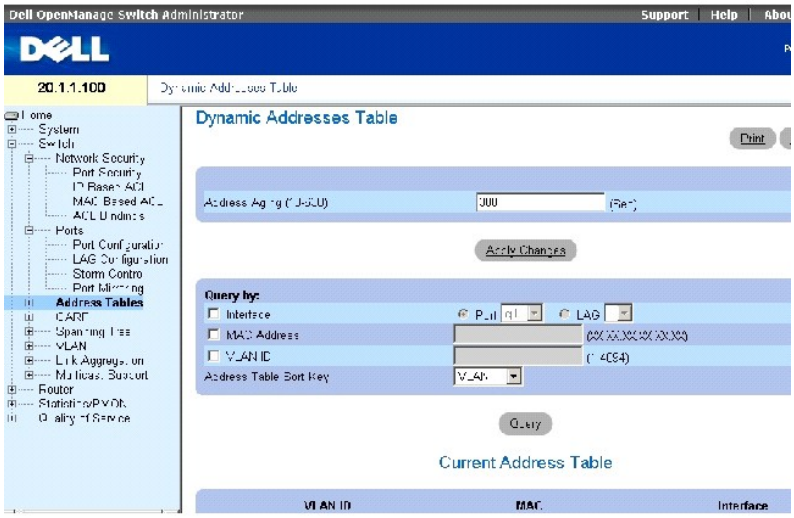
Visualización de direcciones dinámicas

Dynamic Addresses Table (Tabla de direcciones dinámicas) contiene campos para consultar información en la tabla de direcciones dinámicas, incluidos el tipo de interfaz, las direcciones, VLAN y la clave de ordenación de tablas. Los paquetes reenviados a una dirección almacenada en la tabla de direcciones se reenvían directamente a esos puertos.

Dynamic Address Table (Tabla de direcciones dinámicas) también contiene información sobre el tiempo de duración antes de que se elimine una dirección MAC dinámica de la tabla.

Para abrir **Dynamic Address Table** (Tabla de direcciones dinámicas), haga clic en **Switch→ Address Tables→ Dynamic Addresses Table** (Conmutador→ Tablas de direcciones→ Tabla de direcciones dinámicas) en la vista de árbol.

Ilustración 7-18. Dynamic Address Table (Tabla de direcciones dinámicas)



Dynamic Address Table (Tabla de direcciones dinámicas) contiene los campos siguientes:

Address Aging (10-630) (Duración de las direcciones [10-630]): Especifica el tiempo de duración en segundos que tarda en borrarse una dirección MAC dinámica. El valor predeterminado es 300 segundos.

La **Dynamic Address Table** (Tabla de direcciones dinámicas) se puede consultar por:

Port (Puerto): Interfaz consultada para obtener una dirección.

MAC Address (Dirección MAC): Dirección MAC consultada para obtener una dirección.

VLAN ID (ID de VLAN): Número de la VLAN (al que se conecta la dirección MAC) consultada para obtener una dirección.

Address Table Sort Key (Clave de clasificación de la tabla de direcciones): Especifica si la tabla de direcciones dinámicas se ordena por dirección, VLAN o interfaz.

Definición del tiempo de duración

1. Abra la página **Dynamic Address Table** (Tabla de direcciones dinámicas).
2. Defina el campo **Address Aging** (Caducidad de dirección).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El tiempo de caducidad se modifica y el dispositivo se actualiza.

Consulta de la tabla de direcciones dinámicas

1. Abra la página **Dynamic Address Table** (Tabla de direcciones dinámicas).
2. Defina el parámetro por el que se consultará **Dynamic Address Table** (Tabla de direcciones dinámicas).

Las *entradas* de la tabla de direcciones dinámicas se pueden consultar por **Port** (Puerto), **MAC Address** (Dirección MAC) o **VLAN ID** (ID de VLAN).

3. Haga clic en **Query** (Consultar).

Se consulta la tabla de direcciones dinámicas.

Clasificación de la tabla de direcciones dinámicas

1. Abra la página **Dynamic Address Table** (Tabla de direcciones dinámicas).
2. En el menú descendente **Address Table Sort Key** (Clave de clasificación de la tabla de direcciones), seleccione si las direcciones deben clasificarse por dirección, ID de VLAN o interfaz.
3. Haga clic en **Query** (Consultar).

Se clasifica la tabla de direcciones dinámicas.

Tabla de direcciones actuales

La tabla de direcciones actuales contiene parámetros de direcciones dinámicas que se utilizan para reenviar directamente los paquetes a los puertos. La tabla de direcciones actuales contiene los campos siguientes:

- **VLAN ID** (ID de VLAN): Indica el valor de la etiqueta de la VLAN.
- **MAC**: Indica la dirección MAC.
- **Port** (Puerto): Indica el número de puerto.

Consulta y clasificación de direcciones dinámicas mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para consultar y clasificar direcciones dinámicas tal como aparecen en **Dynamic Address Table** (Tabla de direcciones dinámicas).

Tabla 7-13. Comandos de la CLI para consultar y clasificar

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 300

Console (config)# exit

Console# show bridge address-table

Aging time is 300 sec

vlan   mac address      port    type

----   --------------   -----   -----
```

```
1       0060.704C.73FF   g8      dynamic

1       0060.708C.73FF   g8      dynamic

200     0010.0D48.37FF   g9      static
```

Configuración de GARP

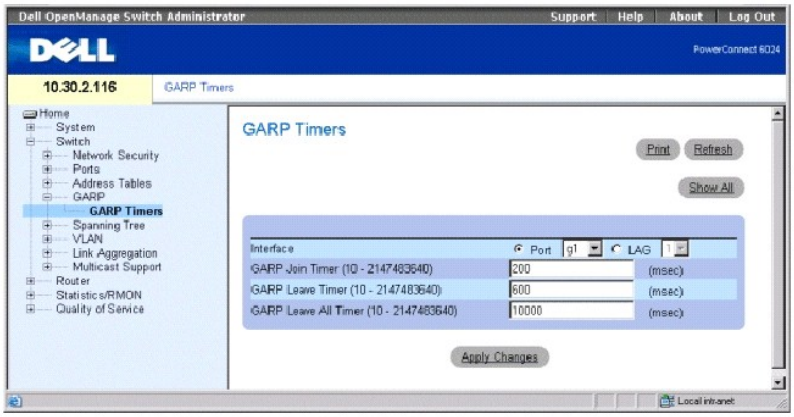
El protocolo genérico de registro de atributos (GARP) es un protocolo de propósitos generales que registra cualquier información de conectividad de red o de estilo de pertenencia. GARP define un conjunto de dispositivos interesados en un atributo de red determinado, como VLAN o dirección de multidifusión.

Para abrir la página **GARP**, haga clic en **Switch→ GARP** (Conmutador→ GARP) en la vista de árbol.

Definición de temporizadores de GARP

La página **GARP Timers** (Temporizadores de GARP) contiene parámetros para activar GARP en el dispositivo. Para abrir la página **GARP Timers** (Temporizadores de GARP), haga clic en **Switch→ GARP→ GARP Timers** (Conmutador→ GARP→ Temporizadores de GARP) en la vista de árbol.

Ilustración 7-19. GARP Timers (Temporizadores de GARP)



La página **GARP Timers** (Temporizadores de GARP) contiene los siguientes campos:

Interface (Interfaz): Determina si se habilita en un puerto o en un LAG.

GARP Join Timer (10 - 2147483640) (Temporizador de unión GARP [10 - 2147483640]): Indica el tiempo en milisegundos en que se transmiten las PDU. Los valores posibles son 10-2147483640. El valor predeterminado es 200 ms.

GARP Leave Timer (10 - 2147483640) (Temporizador de cese GARP [10 - 2147483640]): 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 posible del campo es 0-2147483640. El valor predeterminado es 600 ms.

GARP Leave All Timer (10 - 2147483640) (Temporizador de cese de todos GARP [10 - 2147483640]): Indica el tiempo en milisegundos durante el que todos los dispositivos esperan antes de abandonar el estado GARP. El tiempo de cese de todos debe ser mayor que el tiempo de cese. El valor posible del campo es 0-2147483640. El valor predeterminado es 10.000 ms.

Definición de temporizadores de GARP

1. Abra la página **GARP Timers** (Temporizadores de GARP).
2. Complete los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de GARP se guardan en el dispositivo.

Copia de los parámetros de la tabla de temporizadores de GARP

1. Abra la página **GARP Timers** (Temporizadores de GARP).
2. Haga clic en **Show All** (Mostrar todo) para ver **GARP Timers Table** (Tabla de temporizadores de GARP).
3. Seleccione una interfaz en el campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione una interfaz en el menú descendente **Port** (Puerto) o **LAG**.
5. Las definiciones de esta interfaz se copiarán en las interfaces seleccionadas. Véase el paso 6.
6. Marque la casilla de verificación **Copy to** (Copiar en) para definir las interfaces a las que deban copiarse las definiciones de los temporizadores de GARP, o bien haga clic en **Select All** (Seleccionar todo) para copiar las definiciones a todos los puertos o LAG.
7. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian a los puertos o LAG de **GARP Timers Table** (Tabla de temporizadores de GARP) y el dispositivo se actualiza.

Definición de los temporizadores de GARP mediante los comandos de la CLI

En la Tabla 7-14 se muestra un resumen de los comandos de la CLI equivalentes para definir los temporizadores de GARP tal como aparecen en la página **Garp Timers** (Temporizadores de GARP).

Tabla 7-14. Comandos de la CLI para los temporizadores de GARP

Comando de la CLI	Descripción
`garp timer {join | leave | leaveall} valor_temporizador`	Establece 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 g8
```

```
Console (config-if)# garp timer leave 900
```

Configuración del protocolo de árbol extensible

El protocolo de árbol extensible (STP) proporciona una topología de árbol para cualquier disposición de puentes. STP también proporciona una vía de comunicación entre las estaciones finales de una red, eliminando los bucles.

Los bucles se producen cuando existen rutas alternativas entre los sistemas principales. En una red extendida, los bucles 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 extensible: Classic STP (STP clásico), Rapid STP (STP rápido) y Multiple STP (STP múltiple).

Classic STP (STP clásico) proporciona una sola ruta de acceso entre la estación final, evitando y eliminando los bucles. Si desea obtener más información sobre la configuración de Classic STP (STP clásico), consulte el apartado **Definición de la configuración global de STP**.

Rapid STP (STP rápido [RSTP]) detecta y utiliza las topologías de red que proporcionan una convergencia más rápida del árbol extensible son crear bucles de reenvío. Si desea obtener más información sobre la configuración de RSTP, consulte el apartado **Definición del árbol extensible rápido**.

Multiple STP (STP múltiple [MSTP]) proporciona una conectividad completa para paquetes asignados a cualquier VLAN. MSTP se basa en RSTP. Además, MSTP transmite paquetes asignados a VLAN diferentes a través de regiones MST diferentes. Las regiones MST actúan como un único puente. MSTP aumenta la tolerancia de fallas del sistema y habilita el equilibrado de carga. Si desea obtener más información sobre la configuración de MSTP, consulte el apartado **Definición del árbol extensible múltiple**.

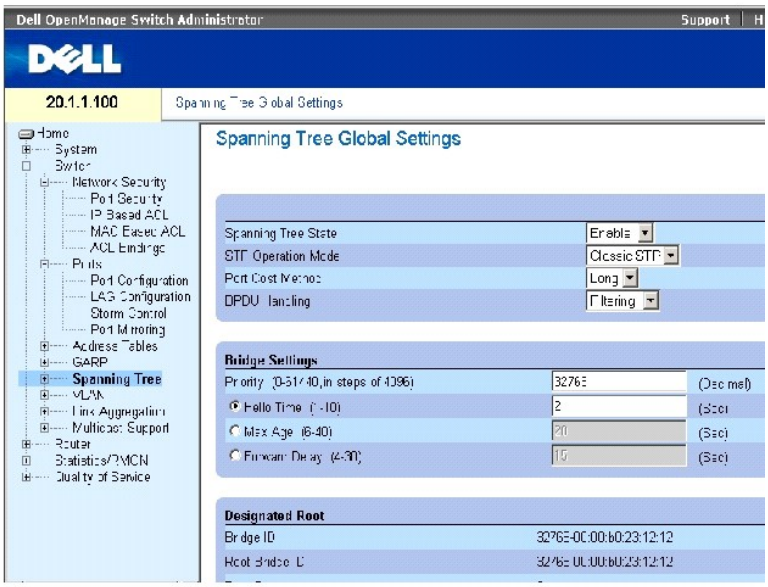
Para abrir la página **Spanning Tree** (Árbol extensible), haga clic en **Switch**→ **Spanning Tree** (Conmutador→ Árbol extensible) en la vista de árbol.

Definición de la configuración global de STP

La página **Spanning Tree Global Settings** (Configuración global del árbol extensible) contiene parámetros para habilitar el funcionamiento de STP en el dispositivo.

Para abrir la página **Spanning Tree Global Settings** (Configuración global del árbol extensible), haga clic en **Switch**→ **Spanning Tree**→ **Global Settings** (Conmutador→ Árbol extensible→ Configuración global) en la vista de árbol.

Ilustración 7-20. Spanning Tree Global Settings (Configuración global del árbol extensible)



La página **Spanning Tree Global Settings** (Configuración global del árbol extensible) contiene los siguientes campos:

Spanning Tree State (Estado del árbol extensible): Habilita o inhabilita el STP, el RSTP o el MSTP en el dispositivo.

STP Operation Mode (Modo STP de funcionamiento): El modo STP mediante el cual se habilita el STP en el dispositivo. Los valores posibles del campo son: **Classic STP** (STP clásico), **Rapid STP** (STP rápido) y **Multiple STP** (STP múltiple).

Path Cost Method (Método de coste de la ruta de acceso): Especifica el método utilizado para asignar costes de rutas de acceso predeterminados a puertos STP. Los valores de campo posibles son:

Long (Largo): Método de coste de ruta de acceso con un rango de 1-200.000.000.

Short (Corto): Método de coste de ruta de acceso con un rango de 1-65.535. Este es el método predeterminado.

Los costes de ruta de acceso predeterminados que se asignan a una interfaz varían en función del método seleccionado:

Interface	Long	Short
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

BPDU Handling (Manejo de BPDU): Especifica el manejo de paquetes BPDU cuando el árbol extensible está desactivado en una interfaz. Los valores de campo posibles son Filtering (Filtrado) y Flooding (Desbordamiento). El valor predeterminado es Flooding (Desbordamiento).

Priority (0-65535) (Prioridad [0-65535]): El valor de la prioridad del puente. Cuando los conmutadores o puentes ejecutan el STP, se asigna una prioridad a cada uno. Después de intercambiar BPDU, el conmutador con el menor valor de prioridad se transforma en el puente raíz. El valor predeterminado es 32768.

Hello Time (1-10) (Tiempo de saludo [1-10]): El tiempo de saludo del conmutador, que indica la cantidad de tiempo en segundos que espera un puente raíz entre los mensajes de configuración. El valor predeterminado es 2.

Max Age (6-40) (Duración máxima [6-40]): El tiempo máximo de duración del conmutador, que indica la cantidad de tiempo en segundos que espera un puente antes de implementar un cambio topológico. El valor predeterminado es 20.

Forward Delay (4-30) (Retraso de envío [4-30]): El tiempo de retraso de envío del conmutador, que indica la cantidad de tiempo en segundos que permanece un puente en estado de escucha y de obtención antes de reenviar los paquetes. El valor predeterminado es 15.

Bridge ID (ID de puente): El ID de puente.

Root Bridge ID (ID de puente raíz): El ID de puente raíz.

Root Port (Puerto raíz): El número de puerto que ofrece la ruta de acceso de menor coste desde este puente hasta el puente raíz. Es significativo cuando el puente no es la raíz. El valor predeterminado es cero.

Root Port Cost (Coste de la ruta a la raíz): Coste de la ruta de acceso desde este puente hasta la raíz.

Topology Changes Counts (Recuentos de cambios de topología): La cantidad total de cambios de estado de STP que se han producido.

Last Topology Change (Último cambio de topología): Cantidad total de tiempo que ha transcurrido desde el último cambio topográfico. El tiempo aparece en formato de horas, minutos y segundos; por ejemplo, 5 horas 10 minutos y 4 segundos.

Definición de los parámetros globales de STP

1. Abra la página **Spanning Tree Global Settings** (Configuración global del árbol extensible).
2. Seleccione el puerto que desee habilitar en el menú **Select a Port** (Seleccionar un puerto).
3. Seleccione **Enable** (Habilitar) en el campo **Spanning Tree State** (Estado del árbol extensible).

4. Seleccione el modo **STP** en el campo **STP Operation Mode** (Modo de funcionamiento de STP) y defina la configuración del puente.
5. Haga clic en **Apply Changes** (Aplicar cambios).

STP se habilita en el dispositivo.

Modificación de los parámetros globales de STP

1. Abra la página **Spanning Tree Global Settings** (Configuración global del árbol extensible).
2. Defina los campos del cuadro de diálogo.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de STP se modifican y el dispositivo se actualiza.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los parámetros globales de STP tal como aparecen en la página **Spanning Tree Global Settings** (Configuración global del árbol extensible).

Tabla 7-15. Comandos de la CLI para la configuración global de STP

Comando de la CLI	Descripción
spanning-tree	Habilita la funcionalidad del árbol extensible.
spanning-tree mode {stp | rstp}	Configura el modo de protocolo de árbol extensible.
spanning-tree pathcost method {long | short}	Configura el método de coste de la ruta de acceso del árbol extensible.
spanning-tree bpdu {filtering | flooding}	Configura el manejo de paquetes BPDU cuando el árbol extensible está desactivado en una interfaz.
spanning-tree priority *prioridad*	Configura la prioridad del árbol extensible.
spanning-tree hello-time *segundos*	Configura el tiempo de saludo del puente del árbol extensible, que es la frecuencia con la que el conmutador transmite mensajes de saludo a otros conmutadores.
spanning-tree max-age *segundos*	Configura la duración máxima del puente del árbol extensible.
spanning-tree forward-time *segundos*	Configura el tiempo de reenvío del puente del árbol extensible, 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*]	Muestra la configuración del árbol extensible.

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 10

Console (config)# spanning-tree forward-time 25

Console (config)# exit

Console# show spanning-tree

Spanning tree enabled mode RSTP

Root ID Priority 32768

Address 0001.4297.e000

Cost 57

Port g1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address 0002.4b29.7a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 8 last change occurred 00:37:24 ago

Times: hold 1, topology change 35, notification 2

hello 2, max age 20, forward delay 15
```

Inter face	Port ID				Designated		Port ID
Name	Prio	Sts	Enb	Cost	Cost	Bridge Id	Prio.Nbr

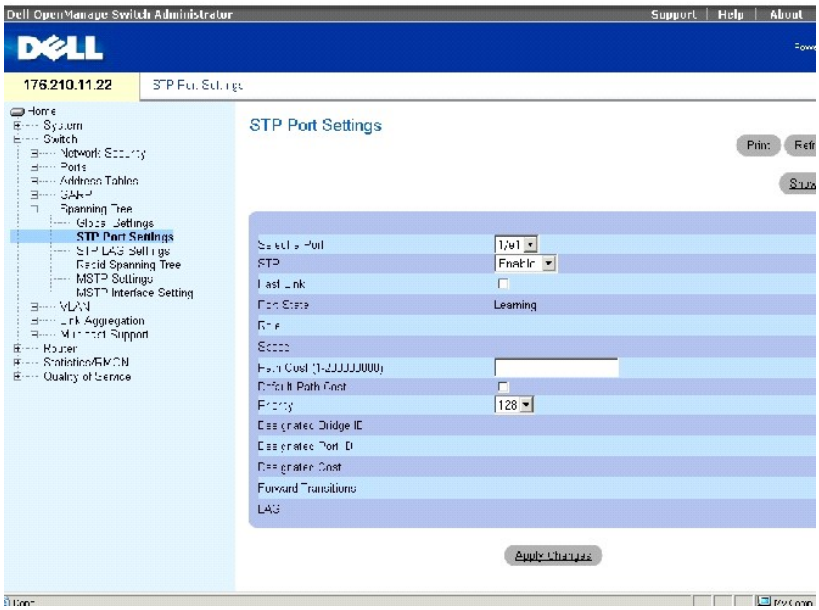
| ---- | ---- | ---- | --- | ---- | ---- | ---- | --------- | --- | --- |
g1	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	001
g2	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	002
g3	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	003
ch1	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	019
ch2	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	01a
ch3	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	01b

Definición de la configuración del puerto STP

Utilice la página **STP Port Settings** (Configuración del puerto STP) para asignar propiedades STP a puertos individuales.

Para abrir la página **STP Port Settings** (Configuración del puerto STP), haga clic en **Switch**→ **Spanning Tree**→ **Port Settings** (Conmutador→ Árbol extensible→ Configuración del puerto) en la vista de árbol.

Ilustración 7-21. STP Port Settings (Configuración del puerto STP)



La página **STP Port Settings** (Configuración del puerto STP) contiene los siguientes campos:

Select a Port (Seleccionar un puerto): Puerto en el que se ha habilitado STP.

STP: Habilita o inhabilita STP en el puerto.

Fast Link (Enlace rápido): Si se selecciona esta opción, se habilita 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 de puerto) pasa automáticamente al estado **Forwarding** (Reenvío) cuando se activa la conexión del puerto. El modo de enlace rápido optimiza el tiempo que tarda el protocolo STP en hacer la convergencia. La convergencia de STP puede tardar de 30 a 60 segundos en redes extensas.

Port State (Estado de puerto): Indica el estado STP actual de un puerto.Si está habilitado, el estado del puerto determina qué acción de reenvío se realiza con el tráfico. Los valores de puerto posibles son:

Disabled (Inhabilitado): STP está inhabilitado actualmente en el puerto. El puerto reenvía el tráfico a medida que obtiene las direcciones MAC.

Blocking (Bloqueo): El puerto está bloqueado actualmente y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC.

Listening (Escucha): El puerto está actualmente en el modo de escucha. El puerto no puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): El puerto está actualmente en el modo de obtención. El puerto no puede reenviar tráfico, pero sí obtener direcciones MAC nuevas.

Forwarding (Reenvío): El puerto está actualmente en el modo de reenvío. El puerto puede reenviar tráfico y obtener direcciones MAC nuevas.

Speed (Velocidad): La velocidad del funcionamiento del puerto.

Path Cost (1-200,000,000) (Coste de la ruta de acceso [1-200.000.000]): La contribución de este puerto al coste de la ruta de acceso hasta la raíz. El coste de la ruta se puede ajustar a un valor mayor o menor y se utiliza para reenviar tráfico cuando se redirecciona una ruta.

Default Path Cost (Coste de la ruta de acceso predeterminada): Indica que el coste de la ruta de acceso predeterminada se asigna en función del método seleccionado en la página **Spanning Tree Global Settings** (Configuración global del árbol extensible).

Priority (0-240) (Prioridad [0-240]): Valor de la prioridad del puerto. El valor de prioridad puede utilizarse para influir en la elección del puerto cuando un puente tiene dos puertos conectados en un bucle.

Designated Bridge ID (ID de puente designado): El ID del puente designado.

Designated Port ID (ID de puerto designado): El ID del puerto seleccionado.

Designated Cost (Coste designado): Coste del puerto designado que participa en la topología STP. Los puertos cuyo coste es menor tienen menos probabilidades de bloquearse si STP detecta bucles.

Forward Transitions (Transiciones de reenvío): Número de veces que el puerto ha cambiado del estado **Forwarding** (Reenvío) al estado **Disabled** (Desactivado).

LAG: El LAG al que está conectado el puerto.

Habilitación de STP en un puerto

1. Abra la página **STP Port Settings** (Configuración del puerto STP).
2. Seleccione **Enabled** (Habilitado) en el campo **STP Port Status** (Estado del puerto STP).
3. Defina los campos **Fast Link** (Enlace rápido), **Path Cost** (Coste de la ruta) y **Priority** (Prioridad).
4. Haga clic en **Apply Changes** (Aplicar cambios).

STP está habilitado en el puerto.

Modificación de las propiedades del puerto STP

1. Abra la página **STP Port Settings** (Configuración del puerto STP).
2. Modifique los campos **Priority** (Prioridad), **Fast Link** (Conexión rápida), **Path Cost** (Coste de la ruta) y **Fast Link** (Conexión rápida).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del puerto STP se modifican y el dispositivo se actualiza.

Visualización de la tabla del puerto STP

1. Abra la página **STP Port Settings** (Configuración del puerto STP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **STP Port Table** (Tabla del puerto STP).

Definición de la configuración del puerto STP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los parámetros del puerto STP tal como aparecen en la página **STP Port Settings** (Configuración del puerto STP).

Tabla 7-16. Comandos de la CLI para la configuración del puerto STP

Comando de la CLI	Descripción
`spanning-tree disable`	Inhabilita el árbol extensible en un puerto específico.
`spanning-tree cost` *`coste`*	Configura el coste de la ruta de acceso del árbol extensible para un puerto.
`spanning-tree port-priority` *`prioridad`*	Configura la prioridad del puerto.
`show spanning-tree [ethernet interface | port-channel` *`número_canal_puerto`*`]`	Muestra la configuración del árbol extensible.
`spanning-tree portfast`	Habilita el modo rápido de puerto.

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

```
Console (config)# interface ethernet g5

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 g1
```

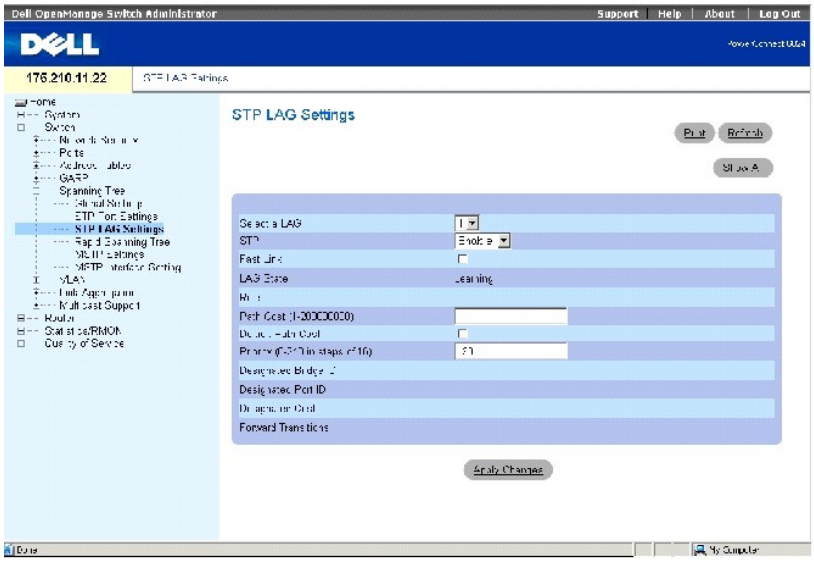
Interface	Port ID	Designated			Port ID
Name	Prio.Nbr	Cost	Sts	Cost Bridge ID	Prio.Nbr
--------	-------	---	--	-------------------	------
g1	128.1	19	FWD	38 32768 0030.9441.62c1	128.25

```
Spanning tree enabled

Type: point-to-point (configured

: auto)

Port Fast: no (configured: no)
```

Definición de la configuración STP de LAG

Utilice la página **STP LAG Settings** (Configuración STP de LAG) para asignar parámetros de puerto de adición STP. Para abrir la página **STP LAG Settings** (Configuración STP de LAG), haga clic en **Switch**→ **Spanning Tree**→ **LAG Settings** (Conmutador→ Árbol extensible→ Configuración de LAG) en la vista de árbol.

Ilustración 7-22. STP LAG Settings (Configuración STP de LAG)



La página **STP LAG Settings** (Configuración STP de LAG) contiene los siguientes campos:

Select a LAG (Seleccionar un LAG): El número de LAG para el que desee modificar la configuración de STP.

STP: Habilita o inhabilita STP en el LAG.

Fast Link (Conexión rápida): Habilita el modo de conexión rápida para el LAG. Si se habilita la conexión rápida para un LAG, el valor de **LAG State** (Estado de LAG) pasa automáticamente al estado **Forwarding** (Reenvío) cuando el LAG está activo. El modo de conexión rápida optimiza el tiempo que tarda el protocolo STP en hacer la convergencia. La convergencia de STP puede tardar de 30 a 60 segundos en redes extensas.

LAG State (Estado de LAG): El estado STP actual de un LAG. Si está habilitado, el estado de LAG determina qué acción de reenvío se realiza con el tráfico. Si el puente descubre un LAG cuyo funcionamiento es defectuoso, lo coloca en estado **Broken** (Averiado). Los posibles estados de LAG son:

- **Disabled** (Inhabilitado): STP está inhabilitado actualmente en el LAG. El LAG reenvía el tráfico a medida que obtiene las direcciones MAC.
- **Blocking** (Bloqueo): El LAG está bloqueado y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC.
- **Listening** (Escucha): El LAG se encuentra en el modo de escucha y no puede reenviar tráfico ni obtener direcciones MAC.
- **Learning** (Obtención): El LAG está actualmente en el modo de obtención y no puede reenviar tráfico pero sí obtener direcciones MAC nuevas.
- **Forwarding** (Reenvío): El LAG está actualmente en el modo de reenvío, y puede reenviar tráfico y obtener direcciones MAC nuevas.
- **Broken** (Averiado): Actualmente, el funcionamiento del LAG es defectuoso y no puede utilizarse para reenviar tráfico.

Path Cost (1-200000000) (Coste de la ruta de acceso [1-200000000]): La cantidad con la que el LAG contribuye al coste de la ruta de acceso hasta la raíz. El coste de la ruta se puede ajustar a un valor mayor o menor, y se utiliza para reenviar tráfico cuando se redirecciona una ruta.

Default Path Cost (Coste de la ruta de acceso predeterminada): Indica que el coste de la ruta de acceso predeterminada se asigna en función del método seleccionado en la página **Spanning Tree Global Settings** (Configuración global del árbol extensible).

Priority (0-240) (Prioridad [0-240]): Valor de la prioridad del LAG. El valor de prioridad puede utilizarse para influir en la elección del LAG cuando un puente tiene dos puertos en bucle. El valor de la prioridad oscila entre 0-240, en saltos de 16.

Designated Bridge ID (ID de puente designado): El ID del puente designado.

Designated Port ID (ID del puerto designado): El ID del puerto designado.

Designated Cost (Coste designado): Coste del puerto designado que participa en la topología STP. Los puertos cuyo coste es menor tienen menos probabilidades de bloquearse si STP detecta bucles.

Forward Transitions (Transiciones de reenvío): Número de veces que el valor de **LAG State** (Estado de LAG) ha cambiado de **Forwarding** (Reenvío) a **Disabled** (Inhabilitado).

Modificación de los parámetros STP de LAG

1. Abra la página **STP LAG Settings** (Configuración STP de LAG).
2. Seleccione un LAG del menú descendente **Select a LAG** (Seleccionar un LAG).
3. Modifique los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros STP de LAG se modifican y el dispositivo se actualiza.

Definición de la configuración STP de LAG mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir la configuración STP de LAG.

Tabla 7-17. Comandos de la CLI para la configuración STP de LAG

Comando de la CLI	Descripción
`spanning-tree disable`	Habilita el árbol extensible.
`spanning-tree cost` *`coste`*	Configura el coste de la ruta de árbol extensible para un puerto.
`spanning-tree port-priority` *`prioridad`*	Configura la prioridad del puerto.
`show spanning-tree [ethernet interface | port-channel` *`número_canal_puerto`*`]`	Muestra la configuración del árbol extensible.
`spanning-tree portfast`	Habilita el modo rápido de puerto.

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
```

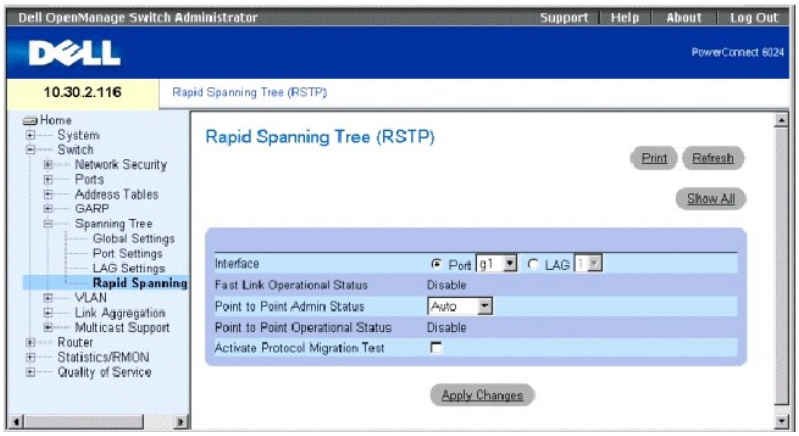
```
Console (config-if)# spanning-tree port-priority 96

Console (config-if)# spanning-tree portfast

Console (config-if)# exit

Console (config)# exit

Console# show spanning-tree port-channel 1

Interface Port ID Designated Port ID

Name   Prio  Sts    Enb    Cost   Cost   Bridge Id               Prio.Nbr

------ ----  ------ -----  ------ ------ ----------------------  ----------------
ch1    96    DSBL   FALSE  35000  0      32768 00:00:b0:11:00:00  96

Spanning tree disabled

Port Fast: yes (configured: yes)

Type: point-to-point (configured: auto)

Number of transitions to forwarding state: 0
```

Definición de árbol extensible rápido

El árbol extensible clásico impide que el nivel 2 reenvíe bucles en una topología de red general. Sin embargo, la convergencia puede tardar hasta 30-60 segundos. El retardo permite disponer de tiempo suficiente para detectar posibles bucles y propagar los cambios del estado.

El protocolo de árbol extensible rápido (RSTP) detecta y utiliza topologías de red que proporcionan una convergencia más rápida del árbol extensible sin crear bucles de reenvío. Para abrir la página **Rapid Spanning Tree (RSTP)** (Árbol extensible rápido [RSTP]), haga clic en **Switch**→ **Spanning Tree**→ **Rapid Spanning Tree** (Conmutador→ Árbol extensible→ Árbol extensible rápido) en la vista de árbol.

Ilustración 7-23. Página Rapid Spanning Tree (RSTP) (Árbol extensible rápido [RSTP])



Interface (Interfaz): Puerto o LAG en el que se ha habilitado el STP rápido.

Fast Link Operational Status (Estado operativo de la conexión rápida): Indica si la conexión rápida está habilitada o inhabilitada para el puerto o el LAG. Si se ha habilitado para un puerto, éste se coloca automáticamente en el estado de reenvío.

Point-to-Point Admin Status (Estado admin punto a punto): Habilita o inhabilita al dispositivo para que pueda establecer una conexión punto a punto, o bien especifica que el dispositivo establezca automáticamente una conexión punto a punto.

Para establecer comunicaciones a través de una conexión punto a punto, el PPP originario envía primero paquetes LCP (Protocolo de control de conexiones) para configurar y comprobar la conexión de los datos. Tras establecerse una conexión y una vez negociadas las capacidades opcionales en función de las necesidades del LCP, el PPP originario envía paquetes NCP (Protocolo de control de red) para seleccionar y configurar uno o más protocolos de nivel de red. Una vez configurados cada uno de los protocolos de nivel de red, ya se pueden enviar sus paquetes a través de la conexión. La conexión permanecerá configurada para las comunicaciones hasta que paquetes LCP o NCP explícitos cierren la conexión, o bien hasta que se genere algún evento externo. Éste es el tipo real de conexión del puerto de conmutador. Puede ser distinto del tipo del estado administrativo.

Point-to-Point Operational Status (Estado operativo punto a punto): El estado operativo de la conexión punto a punto.

Activate Protocol Migrational Test (Activar prueba de migración de protocolo): Si se selecciona esta opción, SE habilita el PPP para que pueda enviar paquetes LCP (Protocolo de control de conexiones) para configurar y probar la conexión de los datos.

Habilitación de RSTP

1. Abra la página Rapid Spanning Tree (RSTP) (Árbol extensible rápido).
2. Defina los campos **Point-to-Point Admin** (Admin. punto a punto), **Point-to-Point Oper** (Oper. punto a punto) y **Activate Protocol Migration** (Activar migración de protocolo).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del STP rápido se habilitan y el dispositivo se actualiza.

Visualización de la tabla del árbol extensible rápido

1. Abra la página Rapid Spanning Tree (RSTP) (Árbol extensible rápido).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Rapid Spanning Tree Tabla (RSTP)** (Tabla del árbol extensible rápido).

Definición de los parámetros globales de STP rápido mediante los comandos de la CLI

La siguiente tabla muestra un resumen de los comandos de la CLI equivalentes para definir los parámetros del STP rápido tal como aparecen en la página **RSTP**.

Tabla 7-18. Comandos de la CLI para la configuración de RSTP

Comando de la CLI	Descripción
spanning-tree link-type {point-to-point | shared}	Hace prevalecer la configuración predeterminada del tipo de conexión.

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

```
Console (config)# interface ethernet g5

Console (config-if)# spanning-tree link-type shared
```

Definición del árbol extensible múltiple

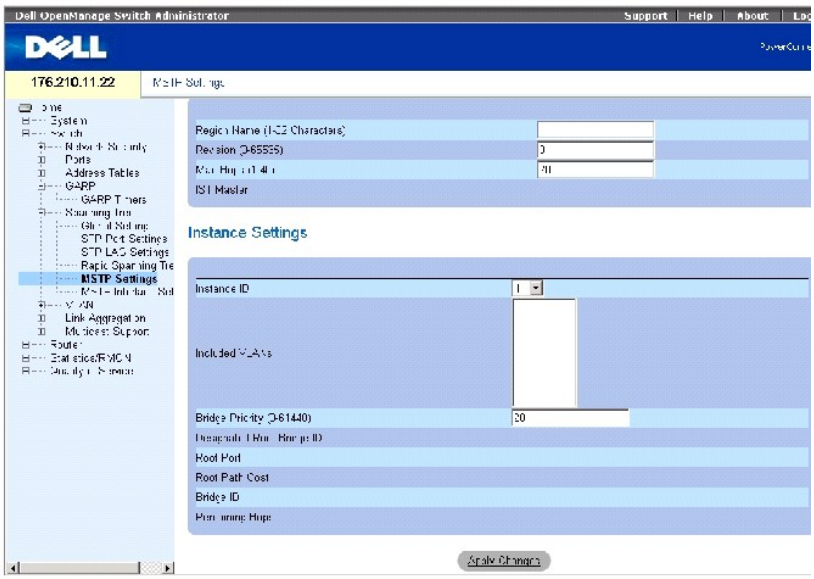
El funcionamiento de MSTP (Protocolo del árbol extensible múltiple) asigna las VLAN a las instancias STP.

MSTP proporciona un escenario de equilibrio de carga diferente. Por ejemplo, mientras el puerto A está bloqueado en una instancia STP, el mismo puerto se coloca en estado Forwarding (Reenvío) en otra instancia STP. La página **MSTP Settings** (Configuración de MSTP) permite definir hasta dieciséis instancias MSTP para el dispositivo.

Además, los paquetes asignados a varias VLAN se transmiten por diferentes rutas de acceso en las regiones de árboles extensibles múltiples (Regiones MST). Las regiones son uno o más puentes interconectados de árbol extensible múltiple con una configuración de MSTP idéntica. Al configurar un MST, se define la región MST a la que pertenece el dispositivo. La configuración consta del nombre, la revisión y la región a la que pertenece el dispositivo.

Para abrir la página **MSTP Settings** (Configuración de MSTP), haga clic en **Switch**→ **Spanning Tree**→ **MSTP Region Configuration** (Conmutador→ Árbol extensible→ Configuración de la región MSTP) en la vista de árbol.

Ilustración 7-24. MSTP Settings (Configuración de MSTP)



La página **MSTP Settings** (Configuración de MSTP) contiene los siguientes campos que se dividen en dos secciones:

Region Name (1-32) (Nombre de región [1-32]): Especifica un nombre de región MST definido por el usuario.

Revision (0-65535) (Revisión [0-65535]): Especifica el número de 16 bits no firmado que identifica la revisión de la configuración del MST actual. El número de revisión es necesario para la configuración de MST.

Max Hops (1-40) (Máximo de saltos [1-40]): Especifica el número total de saltos que se producen en una región específica antes de que se descarte la BPDU. Una vez que se ha descartado la BPDU, caduca la información del puerto. El valor predeterminado del campo es 20.

IST Master (Principal de IST): Indica el ID principal del árbol extensible interno. El IST Master (Principal de IST) es la raíz de la instancia especificada y su instancia es 0.

Instance ID (ID de instancia): Especifica el ID de la instancia del árbol extensible. El intervalo de este campo es de 1 a 15.

Included VLANs (VLAN incluidas): Asigna las VLAN seleccionadas a la instancia seleccionada. Cada VLAN pertenece a una sola instancia.

Bridge Priority (0-61440) (Prioridad del puente [0-61440]): Especifica la prioridad del dispositivo para la instancia del árbol extensible seleccionado.

Designated Root Bridge ID (ID del puente raíz designado): Indica el ID del puente con el menor coste de ruta de acceso a la raíz de la instancia.

Root Port (Puerto raíz): Indica el puerto raíz de la instancia seleccionada.

Root Path Cost (Coste de la ruta de acceso raíz): Indica el coste de la ruta de acceso de la instancia seleccionada hasta la raíz regional.

Bridge ID (ID de puente): Indica el ID de puente de la instancia seleccionada.

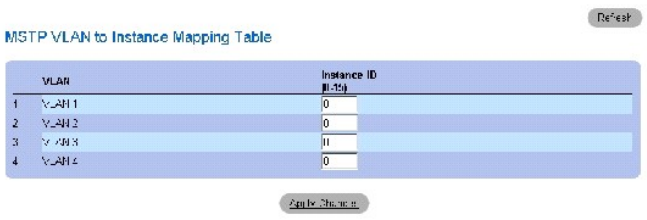
Remaining Hops (Saltos restantes): Indica el número de saltos que faltan hasta el siguiente destino.

Visualización de la tabla de asignación de la VLAN de MSTP a instancias

1. Abra la página **MSTP Settings** (Configuración de MSTP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **MSTP VLAN to Instance Mapping Table** (Tabla de asignación de la VLAN de MSTP a instancias):

Ilustración 7-25. MSTP VLAN to Instance Mapping Table (Tabla de asignación de la VLAN de MSTP a instancias)



Definición de las instancias del MST mediante comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir grupos de instancia de MST tal como aparecen en la página **MSTP Settings** (Configuración de MSTP).

Tabla 7-19. Comandos de la CLI para instancias del MSTP

Comando de la CLI	Descripción
`spanning-tree mst configuration`	Entra en el modo de configuración de MST.
`instance instance-id {add | remove} vlan vlan-range`	Asigna VLAN a la instancia del MST.
`name string`	Establece el nombre de la configuración.
`revision value`	Establece el número de revisión de la configuración.
`spanning-tree mst instance-id port-priority priority`	Establece la prioridad del puerto.
`spanning-tree mst instance-id priority priority`	Establece la prioridad del dispositivo para la instancia del árbol extensible especificado.
`spanning-tree mst max- hops hop-count`	Establece el número de saltos en una región del MST antes de descartar la BPDU y de que caduque la información guardada para un puerto.
`spanning-tree mst instance-id cost cost`	Establece el coste de la ruta de acceso del puerto para los cálculos del MST.
`exit`	Sale del modo de configuración de MST y aplica los cambios de la configuración.
`anular`	Sale del modo de configuración sin aplicar los cambios de la configuración.
`show {current | pending}`	Muestra la configuración de la región 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
```

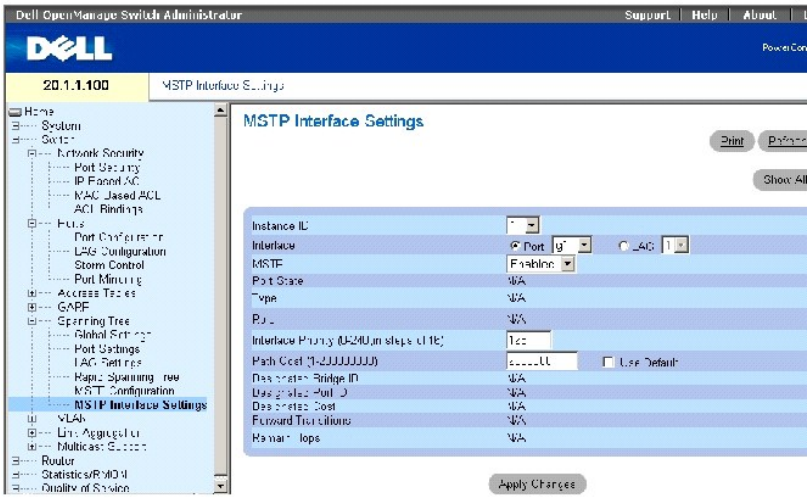
Pending MST configuration	
Name: Region1	
Revision: 1	
Instance	Vlans Mapped
--------	------------
0	1-9,31-4094
1	10-20
2	21-30

Definición de la configuración de la interfaz del MSTP

Utilice la página **MSTP Interface Setting** (Configuración de la interfaz del MSTP) para asignar la configuración de MSTP a interfaces específicas.

Para abrir la página **MSTP Interface Setting** (Configuración de la interfaz del MSTP), haga clic en **Switch**→ **Spanning Tree**→ **MSTP Interface Setting** (Conmutador→ Árbol extensible→ Configuración de la interfaz del MSTP) en la vista de árbol.

Ilustración 7-26. MSTP Interface Setting (Configuración de la interfaz del MSTP)



La página **MSTP Interface Setting** (Configuración de la interfaz del MSTP) contiene los siguientes parámetros:

Instance ID (ID de instancia): Lista las instancias del MSTP que están configuradas en el dispositivo. El intervalo posible del campo es de 0 a 15.

Interface (Interfaz): Asigna puertos o LAG a la instancia del 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 al puerto como un puerto punto a punto o un puerto conectado a un concentrador y si el puerto está dentro de la región del MST o es un puerto fronterizo. Si el puerto es un puerto fronterizo, también indica si el dispositivo situado al otro lado del enlace está funcionando en modalidad RSTP o STP.

Role (Rol): Indica el rol de puerto que asignó el algoritmo STP para proporcionar las rutas de acceso STP. Los valores de campo posibles son:

- **Root** (Raíz): Proporciona la ruta de acceso de menor coste para reenviar paquetes al dispositivo raíz.
- **Designated** (Designado): Indica el puerto o LAG a través del cual el dispositivo designado se conecta a la LAN.
- **Alternate** (Alternativa): Proporciona una ruta de acceso alternativa al dispositivo raíz desde la interfaz.
- **Backup** (Copia de seguridad): Proporciona una ruta de acceso de seguridad para la red LAN designada. Los puertos de seguridad sólo se producen cuando dos puertos están conectados a un bucle mediante un enlace punto a punto. También se produce cuando una LAN tiene dos o más conexiones conectadas con un segmento compartido.
- **Disabled** (Inhabilitado): Indica que el puerto no participa en el árbol extensible.

Interface Priority (Prioridad de la interfaz): Define la prioridad de la interfaz para la instancia específica. El intervalo de prioridad está comprendido entre 0 y 240 en saltos de 16. El valor predeterminado es 128.

Path Cost (Coste de la ruta de acceso): Indica la contribución del puerto a la instancia del árbol extensible. El intervalo está entre 1 y 200.000.000.

Default Path Cost (Coste de la ruta de acceso predeterminada): Indica que el coste de la ruta de acceso predeterminada se asigna en función del método seleccionado en la página **Spanning Tree Global Settings** (Configuración global del árbol extensible).

Designated Bridge ID (ID de puente designado): El número de identificación del puente que conecta el enlace o la red LAN compartida a la raíz.

Designated Port ID (ID de puerto designado): El número de identificación del puerto en el puente designado que conecta el enlace o la red LAN compartida a la raíz.

Designated Cost (Coste designado): Coste de la ruta de acceso desde el enlace o la red LAN compartida hasta la raíz.

Forward Transitions (Transiciones de reenvío): Número de veces que el puerto cambió al estado **Forwarding** (Reenvío).

Remain Hops (Saltos restantes): Indica el número de saltos que faltan hasta el siguiente destino.

Visualización de la tabla de la interfaz del MSTP

1. Abra la página **MSTP Interface Setting** (Configuración de la interfaz del MSTP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **MSTP Interface Table** (Tabla de la interfaz del MSTP):

Ilustración 7-27. MSTP Interface Table (Tabla de la interfaz del MSTP)

Definición de las interfaces del MSTP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir interfaces del MSTP tal como aparecen en la página **MSTP Interface Setting** (Configuración de la interfaz del MSTP).

Tabla 7-20. Comandos de la CLI para la interfaz del MSTP

Comando de la CLI	Descripción
spanning-tree mst *instancia-id* **cost** *coste*	Establece el coste de la ruta de acceso del puerto para los cálculos MST.
spanning-tree mst *instancia-id* **priority** *prioridad*	Establece la prioridad del dispositivo para la instancia del ST especificada.
show spanning-tree mst-configuration	Muestra la configuración de MST.

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

```
Console (config) # interface ethernet g9

Console (config-if) # spanning-tree mst 1 cost 4

Console (config-if)# spanning-tree mst 1 port-priority 142

Console (config-if)# end

Console# show spanning-tree

Spanning tree enabled mode MSTP

Default port cost method: long
```

```
###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID Priority 32768

Address 00:01:42:97:e0:00

Path Cost 20000

Root Port 1 (ig)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master ID Priority 32768

Address 00:02:4b:19:7a:00

Path Cost 10000

Rem hops 19

Bridge ID Priority 32768

Address 00:02:4b:29:7a:00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Max hops 20
```

Configuración de VLAN

Las VLAN son subgrupos lógicos de una LAN creados utilizando software en lugar de una definición de solución de hardware. Combinan estaciones de usuario y dispositivos de red en un dominio único, 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, adiciones y movimientos de la red.

Las VLAN se basan en software y no se definen por atributos físicos. En consecuencia, las VLAN tienen no tienen un número mínimo de puertos y pueden crearse por unidad, por dispositivo, por pila o cualquier otra combinación de conexión lógica.

Las VLAN funcionan en el nivel 2. Dado que aíslan el tráfico dentro de la VLAN, se requiere un enrutador funcional de nivel de 3 para permitir que el tráfico fluya 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 donde se genera el tráfico.

La asignación de etiquetas a VLAN proporciona un método para transferir información de la VLAN entre grupos de la 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 VLAN y GVRP permite a los administradores de red definir nodos de red en dominios de difusión. El tráfico de difusión y multidifusión se confina dentro del grupo de origen.

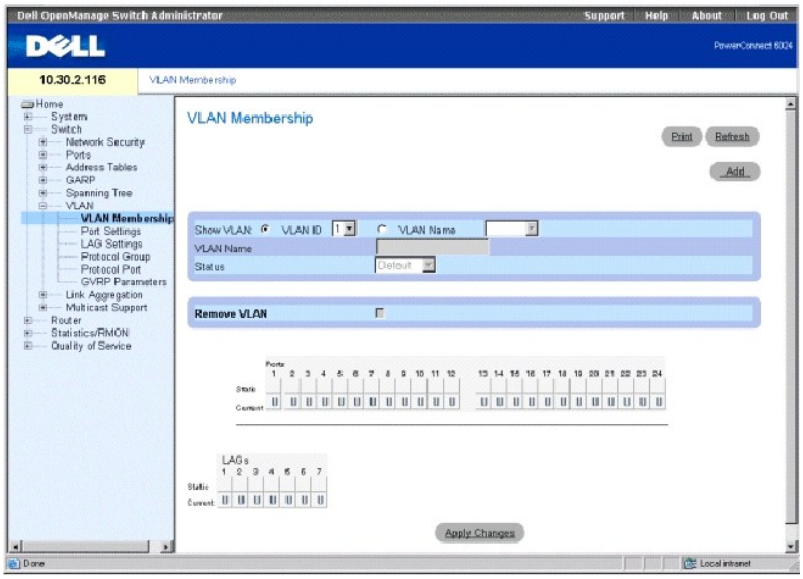
Para visualizar la página **VLAN**, haga clic en **Switch**→ **VLAN** (Conmutador→ VLAN) en la vista de árbol.

Definición de la pertenencia a VLAN

Utilice la página **VLAN Membership** (Pertenencia a la VLAN) para definir grupos de VLAN.

Para abrir la página de pertenencia a VLAN, haga clic en **Switch**→ **VLAN**→ **VLAN Membership** (Conmutador→ VLAN→ Pertenencia a VLAN) en la vista de árbol.

Ilustración 7-28. Página VLAN Membership (Pertenencia a VLAN)



La página **VLAN Membership** (Pertenencia a VLAN) se divide en **VLAN Membership Table** (Tabla de pertenencia a VLAN) y **VLAN Port Membership Table** (Tabla de pertenencia al puerto de VLAN).

Tabla de pertenencia a VLAN

La **VLAN Membership Table** (Tabla de pertenencia a VLAN) contiene parámetros para asignar pertenencias a la VLAN para los puertos. El conmutador admite hasta 4095 VLAN. No obstante, realmente puede crear sólo 4062 VLAN porque:

- El dispositivo reserva las VLAN que van de la 4064 a la 4094 para uso de funcionamiento interno,
- la VLAN 1 es la VLAN predeterminada a la que pertenecen, por defecto, todos los puertos, y
- la VLAN 4095 es la VLAN descartada .

Show VLAN (Mostrar VLAN): Muestra una lista y visualiza información de VLAN específica de acuerdo con el ID o el nombre de VLAN.

VLAN Name (Nombre de VLAN): Indica el nombre de la VLAN definida 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.

Remove VLAN (Eliminar VLAN): Si se selecciona esta opción, se elimina la VLAN de la tabla de pertenencia a VLAN.

Adición de nuevas VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Haga clic en **Add** (Agregar) para visualizar la página **Create New VLAN** (Crear nueva VLAN).
3. Escriba el ID y el nombre de VLAN.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva VLAN se agrega y el dispositivo se actualiza.

Modificación de grupos de pertenencia a VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN del menú descendente **Show VLAN** (Mostrar VLAN).
3. Modifique los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La información de pertenencia a la VLAN se modifica y el dispositivo se actualiza.

Supresión de grupos de pertenencia a la VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN del campo **Show VLAN** (Mostrar VLAN).
3. Marque la casilla de verificación **Remove VLAN** (Eliminar VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La VLAN servidor se suprime y el dispositivo se actualiza.

Definición de grupos de pertenencia a la VLAN mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir grupos de pertenencia a la VLAN tal como aparecen en la página **VLAN Membership** (Pertenencia a la VLAN).

Tabla 7-21. Comandos de la CLI para el grupo de pertenencia a la VLAN

Comando de la CLI	Descripción
`vlan database`	Entra en el modo de configuración de interfaz (VLAN).
`vlan {`*`intervalo_vlan`*`}`	Crea una VLAN.
	Agrega un nombre a una VLAN.

name *cadena*	

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

```
Console (config)#interface vlan 1972

Console (config-if)#name Marketing
```

Tabla de pertenencia al puerto de VLAN

La **VLAN Port Membership Table** (Tabla de pertenencia al puerto de VLAN) contiene una **Port Table** (Tabla del puerto) para asignar puertos a las VLAN. A los puertos se les asigna la pertenencia a la VLAN mediante la configuración de **Port Control** (Control de puerto). Los puertos pueden tener los valores siguientes:

Tabla 7-22. VLAN Port Membership Table (Tabla de pertenencia al puerto de VLAN)

Control de puerto	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 miembro de una 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 miembro de una VLAN. Los paquetes asociados con la interfaz no se reenvían.

En la **VLAN Port Membership Table** (Tabla de pertenencia al puerto de VLAN) se muestran los puertos y los estados de los puertos, así como los LAG.

Asignación de los 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 del menú descendente.
3. Seleccione un puerto en **Port Membership Table** (Tabla de pertenencia al puerto) y asigne un valor al puerto.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se asigna al grupo de VLAN y el dispositivo se actualiza.

Supresión 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 del menú descendente.
3. Marque la casilla de verificación **Remove VLAN** (Eliminar VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La VLAN servidor se suprime y el dispositivo se actualiza.

Asignación de puertos a grupos de VLAN mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para asignar puertos a los grupos de VLAN.

Tabla 7-23. Comandos de la CLI para asignar puertos a grupos de VLAN

Comando de la CLI	Descripción
`switchport general acceptable-frame-types tagged-only`	Rechaza tramas sin etiqueta en la entrada.
`switchport forbidden vlan {add` *`lista_vlan`* `| remove` *`lista_vlan`*`}`	Prohibe la adición de VLAN específicas al puerto.

A continuación figuran ejemplos de comando de la CLI:

```
Console (config)# interface ethernet g1
```

```
Console (config-if)# switchport general acceptable-frame-types tagged-only
```

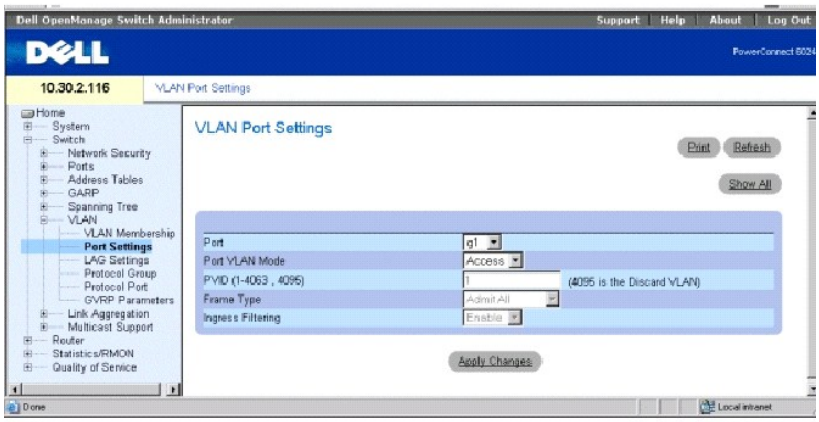
```
Console (config-if)# switchport forbidden vlan add 234-256
```

Definición de la configuración de puertos de VLAN

Utilice la página **VLAN Port Settings** (Configuración de puertos de VLAN) para proporcionar parámetros para administrar puertos que forman parte de una VLAN. El ID de VLAN predeterminado del puerto (PVID) se configura en la página **VLAN Port Settings** (Configuración de puertos de VLAN). Todos los paquetes sin etiquetar que lleguen al dispositivo se etiquetan con los PVID de los puertos.

Para abrir la página **VLAN Port Settings** (Configuración de puertos de VLAN), haga clic en **Switch**→ **VLAN**→ **Port Settings** (Conmutador→ VLAN→ Configuración del puerto) en la vista de árbol.

Ilustración 7-29. Página VLAN Port Settings (Configuración de puertos de VLAN)



Port (Puerto): El número de puerto incluido en la VLAN.

Port VLAN Mode (Modo VLAN de puerto): Indica el modo del puerto. Los valores posibles son:

General: El puerto pertenece a las VLAN y cada una de las VLAN está definida por el usuario como con etiqueta o sin etiqueta (modo 802.1Q completo).

Access (Acceso): El puerto pertenece a una única VLAN sin etiqueta. Cuando un puerto se encuentra en el modo de acceso, los tipos de paquete que se aceptan en el puerto (tipo de paquete) no pueden designarse. Tampoco se puede habilitar/inhabilitar el filtrado de entrada en un puerto de acceso.

Trunk (Combinación de puertos): El puerto pertenece a una VLAN en la que todos los puertos tienen etiqueta (excepto en el caso de una VLAN nativa única opcional).

PVID (1-4063, 4095): Asigna un ID de VLAN a paquetes sin etiqueta. Los valores posibles son 1-4063 y 4095. En el sector industrial, el valor estándar de la VLAN 4095 es definirla como la VLAN descartada; los paquetes clasificados para esta VLAN se eliminan.

Frame Type (Tipo de trama): El tipo de trama aceptado en el puerto. Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): Indica que en el puerto sólo se aceptan tramas con etiqueta.

Admit All (Admitir todos): Indica que en el puerto se aceptan tramas con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): Habilita o inhabilita el filtrado de entrada en el puerto. El filtrado de entrada descarta las tramas cuya etiqueta de VLAN no coincide con ninguna VLAN de puerto.

Asignación de la configuración de puertos

1. Abra la página **VLAN Port Settings** (Configuración de puertos de VLAN).
2. Seleccione el puerto al que desee asignar la configuración del menú descendente **Port** (Puerto).
3. Complete los campos restantes de la página y haga clic en **Apply Changes** (Aplicar cambios).

La configuración de puertos de VLAN se define y el dispositivo se actualiza.

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) para visualizar **VLAN Port Table** (Tabla de puertos de VLAN).

NOTA: Si se elige un puerto de tipo **Access** (Acceso), los tipos de paquete que se aceptan en el puerto (tipo de paquete) no pueden designarse. Tampoco se puede habilitar o inhabilitar el filtrado de entrada en un puerto de acceso.

Asignación de puertos a grupos de VLAN mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para asignar puertos a los grupos de VLAN.

Tabla 7-24. Comandos de la CLI para los puertos de VLAN

Comando de la CLI	Descripción
`switchport mode { access | trunk | general}`	Configura un modo de pertenencia a la VLAN de puertos.
`switchport trunk native vlan id_vlan`	Define el puerto como miembro de la VLAN especificada y el ID de VLAN como el ID de VLAN predeterminado del puerto (PVID) .
`switchport general pvid id_vlan`	Configura el ID de VLAN de puerto (PVID) cuando la interfaz está en modo general.
	Agrega o elimina redes VLAN de un puerto general.

switchport general allowed vlan add *lista_vlan* [tagged | untagged]	
switchport general acceptable-packet- types tagged-only	Rechaza las tramas sin etiqueta en la entrada.
switchport general ingress-filtering disable	Inhabilita el filtrado de entrada del puerto.
shutdown	Inhabilita interfaces.
set interface active {ethernet *interfaz* | port-channel *número_ canal_puerto*}	Reactiva una interfaz que está apagada por motivos de seguridad.

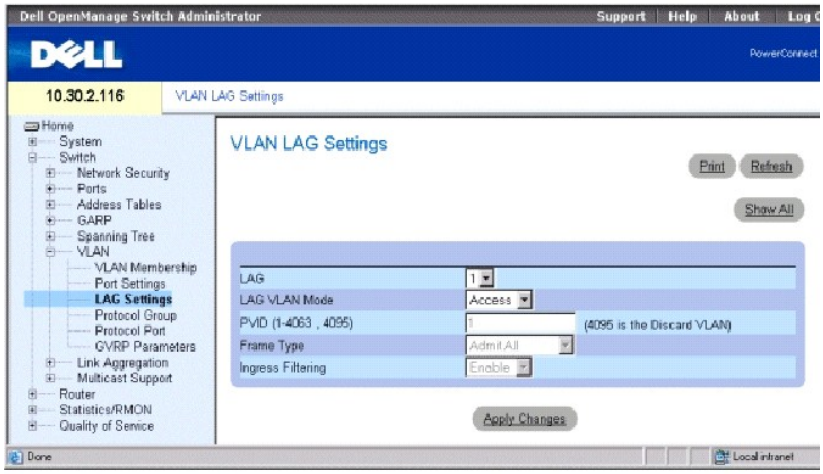
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport trunk native vlan 123

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged

Console (config-if)# switchport general acceptable-packet-types tagged-only
```

Definición de la configuración de LAG de la VLAN

En la página **VLAN LAG Settings** (Configuración de LAG de la VLAN) se proporcionan parámetros para gestionar los LAG que forman parte de una VLAN. Las VLAN pueden constar de puertos individuales o de LAG. Los paquetes sin etiquetar que entren en el conmutador se etiquetan con el ID de LAG especificado por el PVID. Para abrir la página **VLAN LAG Settings** (Configuración de LAG de la VLAN), haga clic en **Switch**→ **VLAN**→ **LAG Settings** (Conmutador→ VLAN→ Configuración de LAG) en la vista de árbol.

Ilustración 7-30. Página VLAN LAG Setting (Configuración de LAG de la VLAN)



LAG: El número de LAG incluido en la VLAN.

LAG VLAN Mode (Modo VLAN de LAG): Indica el modo VLAN de LAG. Los valores posibles son:

General: El LAG pertenece a las VLAN y cada una de las VLAN está definida por el usuario como con etiqueta o sin etiqueta (modo 802.1Q completo).

Access (Acceso): El LAG pertenece a una única VLAN sin etiqueta.

Trunk (Troncal): El LAG pertenece a VLAN en las que todos los puertos están etiquetados (excepto por una sola VLAN nativa opcional).

PVID (1-4063, 4095): Asigna un ID de VLAN a paquetes sin etiqueta. Los valores posibles del campo son 1-4063 y 4095. En el sector industrial, el valor estándar de la VLAN 4095 es definirla como la VLAN descartada; los paquetes clasificados para esta VLAN se eliminan.

Frame Type (Tipo de trama): El 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): Habilita o inhabilita el filtrado de entrada por el LAG. El filtrado de entrada descarta los paquetes cuya etiqueta de VLAN no coincide con ningún LAG de VLAN.

Asignación de la configuración de VLAG

1. Abra la página **VLAN LAG Settings** (Configuración de LAG de la VLAN).
2. Seleccione un LAG en el menú descendente **LAG** y complete los campos de la página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG de la VLAN se definen y el dispositivo se actualiza.

Visualización de la tabla LAG de VLAN

1. Abra la página **VLAN LAG Settings** (Configuración de LAG de la VLAN).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **VLAN LAG Table** (Tabla LAG de VLAN).

Asignación de LAG a grupos de VLAN mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar LAG a grupos de VLAN tal como aparecen en la página **VLAN LAG Settings** (Configuración de LAG de la VLAN).

Tabla 7-25. Comandos de la CLI para asignar LAG a la VLAN

Comando de la CLI	Descripción
`switchport mode {access | trunk | general}`	Configura un modo de pertenencia a la VLAN de puertos.
`switchport trunk native vlan id_vlan`	Define el puerto como miembro de la VLAN especificada y el ID de VLAN como el ID de VLAN predeterminado del puerto (PVID).
`switchport general pvid id_vlan`	Configura el ID de VLAN de puerto (PVID) cuando la interfaz está en modo general.
`switchport general allowed vlan add lista_vlan [tagged | untagged]`	Agrega o elimina redes VLAN de un puerto general.
`switchport general acceptable-frame-type tagged-only`	Rechaza los paquetes sin etiqueta en la entrada.
`switchport general ingress-filtering disable`	Inhabilita el filtrado de entrada del puerto.

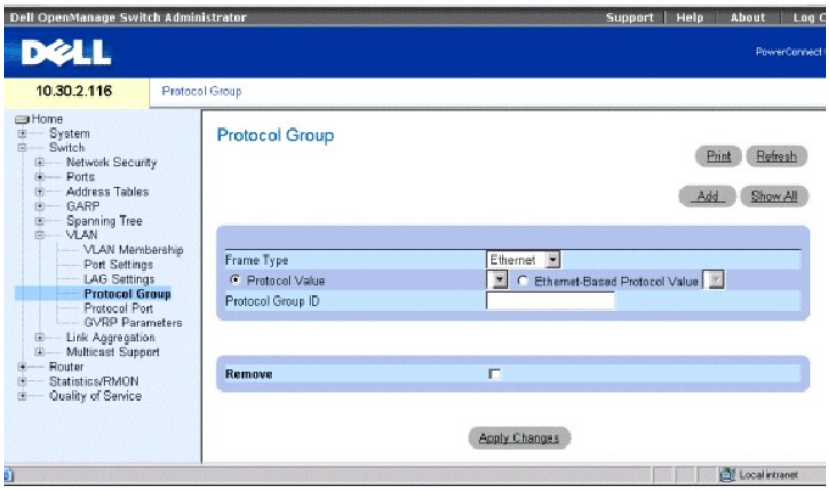
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config-if)# switchport mode access

Console (config-if)# switchport trunk native vlan 123

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged

Console (config-if)# switchport general acceptable-frame-type tagged-only
```

Definición de los grupos de protocolos de la VLAN

La página **Protocol Group** (Grupo de protocolos) contiene información relativa a los nombre de protocolos y el tipo de Ethernet de la VLAN. Las interfaces pueden clasificarse como una interfaz basada en un protocolo específico. La clasificación coloca la interfaz en un grupo de protocolos. Para abrir la página **Protocol Group** (Grupo de protocolos), haga clic en **Switch→ VLAN→ Protocol Group** (Conmutador→ VLAN→ Grupo de protocolos) en la vista de árbol.

Ilustración 7-31. Protocol Group Table (Tabla grupo de protocolos)



Frame Type (Tipo de trama): El tipo de paquete. Los valores posibles del campo son **Ethernet**, **RFC1042** y **LLC Other** (LLC Otros).

Protocol Value (Valor del protocolo): Nombre del protocolo definido por el usuario.

Ethernet-Based Protocol Value (Valor del protocolo basado en Ethernet): El tipo de grupo de protocolos de Ethernet.

Protocol Group ID (ID de grupo de protocolos): El número de ID del grupo de VLAN.

Adición de un grupo de protocolos

1. Abra la página **Protocol Group** (Grupo de protocolos).
2. Haga clic en **Add** (Agregar) para visualizar la página **Assign Protocol to Group** (Asignar protocolo al grupo).
3. Complete los campos de la página y haga clic en **Apply Changes** (Aplicar cambios).

El grupo de protocolos se asigna y el dispositivo se actualiza.

Asignación de la configuración del grupo de protocolos de la VLAN

1. Abra la página **Protocol Group** (Grupo de protocolos).
2. Complete los campos de la página y haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del grupo de protocolos de la VLAN se definen y el dispositivo se actualiza.

Eliminación de protocolos de la tabla de grupos de protocolos

1. Abra la página **Protocol Group** (Grupo de protocolos).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **Protocol Group Table** (Tabla de grupo de protocolos).
3. Marque la casilla de verificación **Remove** (Eliminar) correspondiente a los grupos de protocolos que desee eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el protocolo y el dispositivo se actualiza.

Definición de grupos de protocolos de VLAN mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar los grupos de protocolos.

Tabla 7-26. Comando de la CLI para los grupos de protocolos de VLAN

Comando de la CLI	Descripción
`map protocol` *`protocolo`* `[`*`encapsulación`*`]` `protocols- group` *`grupo`*	Agrega un protocolo especial a un grupo de protocolos especificado, que puede utilizarse para la asignación de VLAN basada en protocolos.

En el ejemplo siguiente se asigna un protocolo ARP de IP al grupo 213 :

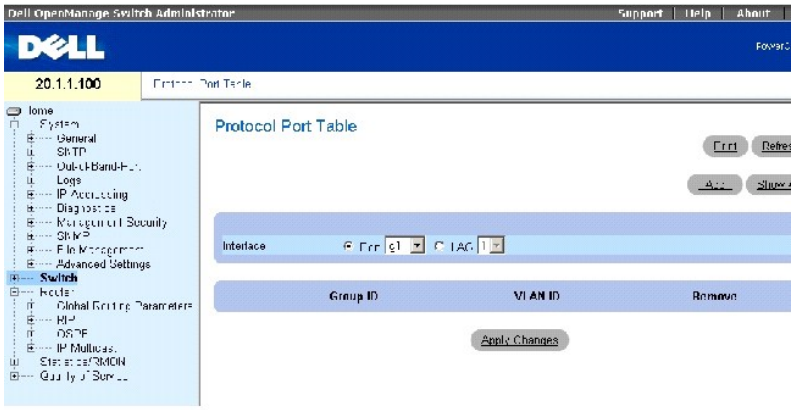
```
Console (config)# vlan database

Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Adición de puertos de protocolo

La página **Protocol Port** (Puerto de protocolo) agrega interfaces a los grupos de protocolos.

Para abrir la página **Protocol Port** (Puerto de protocolo), haga clic en **Switch**→ **VLAN**→ **Protocol Port** (Conmutador→ VLAN→ Puerto de protocolo) en la vista de árbol.

Ilustración 7-32. Página Protocol Port (Puerto de protocolos)



Interface (Interfaz): Número de puerto o LAG que se agrega a un grupo de protocolos.

Protocol Group ID (ID de grupo de protocolos): El ID del grupo de protocolos al que se agrega la interfaz. Los ID de grupo de protocolos se definen en la tabla de grupos de protocolos.

VLAN ID (ID de VLAN): Conecta la interfaz a un ID de VLAN definido por el usuario. El ID de VLAN se define en la página **Create a New VLAN** (Crear nueva VLAN). Los puertos de los protocolos bien pueden conectarse a un ID de VLAN o a un nombre de VLAN.

VLAN Name (Nombre de VLAN): Conecta la interfaz a un nombre de VLAN definido por el usuario. El nombre de VLAN se define en la página **Create a New VLAN** (Crear nueva VLAN). Este campo sólo está disponible en la página **Add Protocol Port** (Agregar puerto de protocolos).

Remove (Eliminar): Si selecciona esta opción, se elimina la asignación del puerto de una VLAN o un grupo de protocolos.

Adición de nuevo puerto de protocolos

1. Abra la página **Protocol Port Table** (Tabla de puertos de protocolos).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add Protocol Port** (Agregar protocolo de origen).
3. Complete los campos del cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

Se agrega el nuevo grupo de protocolos de VLAN a **Protocol Port Table** (Tabla de puertos de protocolos) y el dispositivo se actualiza.

Definición de puertos de protocolo mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir los puertos de los protocolos.

Tabla 7-27. Comandos de la CLI para el puerto de protocolos

Comando de la CLI	Descripción
`switchport general map protocols-group` *`grupo`* `vlan` *`id_vlan`*	Establece una regla de clasificación basada en protocolos.

En el ejemplo siguiente se establece una regla de clasificación basada en protocolo del grupo de protocolos 1 a la VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

Configuración 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 registrar la pertenencia a la VLAN.

Para minimizar los requisitos de memoria cuando se ejecuta el protocolo GVRP, se han agregado dos variables de ajuste de propietario a las variables estándar:

- **Maximum number of GVRP VLANs** (Número máximo de VLAN GVRP): El número de VLAN GVRP que pueden participar en el funcionamiento de GVRP.
- **Maximum number of GVRP VLANs after Reset** (Número máximo de VLAN GVRP después de restablecer): Número máximo de VLAN GVRP después de utilizar la opción de restablecimiento para realizar ajustes. Este valor sólo se hace efectivo tras el restablecimiento.

El número máximo de VLAN GVRP incluye todas las VLAN que participan en el funcionamiento de GVRP, independientemente de si son estáticas o dinámicas.

Al especificar el número máximo de VLAN que participan en GVRP fijando el valor del número máximo de VLAN GVRP tras el restablecimiento, debe tenerse en cuenta lo siguiente:

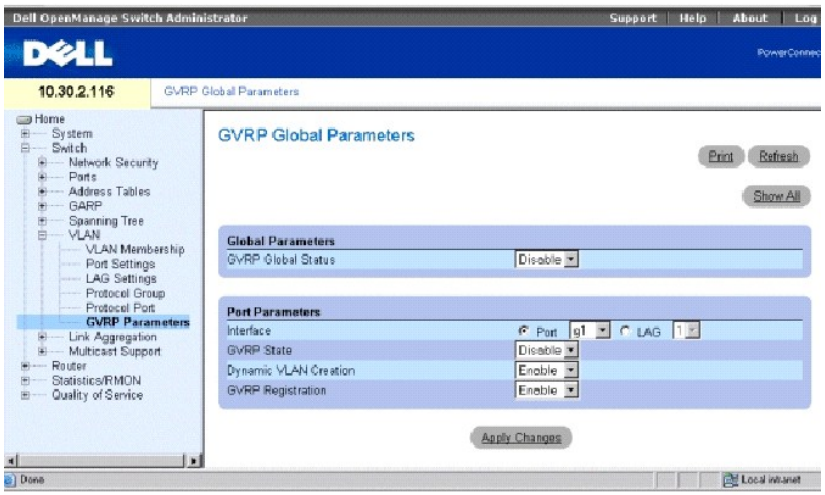
- El número máximo predeterminado de VLAN GVRP es igual a 255.
- El número máximo de VLAN (administrado a través de la variable Max VLANs MIB) limita el número máximo de VLAN GVRP.

Para garantizar el funcionamiento correcto del protocolo GVRP, se aconseja a los usuarios que fijen el número máximo de VLAN GVRP con un valor que supere significativamente la suma de:

- El número de todas las VLAN estáticas, tanto las configuradas actualmente como las que se prevé que se configurarán.
- El número de todas las VLAN dinámicas que participan en GVRP, tanto las configuradas actualmente (el número inicial de VLAN GVRP dinámicas es 255) como las que se prevé que se configurarán.

La página **GVRP Global Parameters** (Parámetros globales de GVRP) habilita el GVRP globalmente. También puede habilitar el GVRP en función de cada interfaz. Para abrir la página **GVRP Global Parameters** (Parámetros globales de GVRP), haga clic en **Switch**→ **VLAN**→ **GVRP Parameters** (Conmutador→ VLAN→ Parámetros de GVRP) en la vista de árbol.

Ilustración 7-33. Página GVRP Global Parameters (Parámetros globales de GVRP)



GVRP Global Status (Estado global de GVRP): Habilita o inhabilita GVRP en el dispositivo. De forma predeterminada, el GVRP está inhabilitado.

Interface (Interfaz): El puerto o LAG para el que se activa GVRP.

GVRP State (Estado de GVRP): Habilita o inhabilita GVRP en una interfaz.

Dynamic VLAN Creation (Creación de VLAN dinámica): Habilita o inhabilita la creación de VLAN a través del GVRP.

GVRP Registration (Registro de GVRP): Muestra el estado de registro del GVRP.

Habilitación 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).

GVRP se habilita en el dispositivo.

Habilitación 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) para la interfaz pertinente.
3. Seleccione **Enable** (Activar) en el campo **GVRP Registration** (Registro de GVRP).

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

Se habilita el registro de VLAN GVRP en el puerto y el dispositivo se actualiza.

Configuración de GVRP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar GVRP tal como aparecen en la página **GVRP Global Parameters** (Parámetros globales de GVRP).

Tabla 7-28. Comandos de la CLI para los parámetros globales de GVRP

Comando de la CLI	Descripción
`gvrp enable (global)`	Habilita el GVRP globalmente.
`gvrp enable (interface)`	Habilita el GVRP en una interfaz.
`gvrp vlan-creation-forbid`	Habilita o inhabilita la creación de VLAN dinámica.
`gvrp registration-forbid`	Extrae todas las VLAN del registro e impide la creación o el registro de 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 dinámica 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 interface | port-channel` *`número-canal-puerto`*`]`	Borra toda la información de estadísticas del GVRP.

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

```
Console (config)# gvrp enable

Console (config)# interface ethernet g8

Console (config-if)# gvrp enable

Console (config-if)# gvrp vlan-creation-forbid

Console (config-if)# gvrp registration-forbid

Console> show gvrp configuration
```

```
GVRP Feature is currently Enabled on the device.

Maximum VLANs: 4063, Maximum VLANs after reset: 4063.


Port(s)  GVRP-Status Registration Dynamic VLAN Timers(milliseconds)

                                 Creation      Join      Leave      Leave All

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

g1       Disabled    Normal       Enabled       200       600        10000

...

g7       Disabled    Normal       Enabled       200       600        10000

g8       Enabled     Forbidden    Disabled      200       600        10000

g9       Disabled    Normal       Enabled       200       600        10000

...

g24       Disabled    Normal       Enabled       200       600        10000

ch1       Disabled    Normal       Enabled       200       600        10000

...

ch7       Disabled    Normal       Enabled       200       600        10000

...

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
g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

Console# clear gvrp statistics ethernet g8

Agregado de puertos

El agregado de conexiones optimiza la utilización de los puertos al conectar un grupo de puertos para que formen un único LAG (grupo agregado de conexiones). El agregado de conexiones multiplica la amplitud de banda entre los dispositivos, aumenta la flexibilidad de los puertos y proporciona redundancia de la conexión.

Su conmutador admite LAG estáticos y LACP (Protocolo de control de adición de enlaces). Los LAG de LACP negocian las conexiones de los puertos agregados con otros puertos LACP ubicados en un dispositivo distinto. Si los demás puertos de dispositivo también son puertos LACP, los dispositivos establecen un LAG entre ellos.

Deben seguirse las directrices siguientes durante la configuración del agregado de puertos:

- Todos los puertos de un LAG deben ser del mismo tipo de soporte.
- No se ha configurado ninguna VLAN en el puerto.
- El puerto no se ha asignado a un LAG distinto.
- Existe una dirección MAC disponible que puede asignarse a un puerto.
- No se ha configurado el modo de negociación automática en el puerto.
- El puerto se encuentra en el modo dúplex completo.
- Todos los puertos del LAG tienen los mismos modos de etiquetado y filtro de entrada.
- Todos los puertos del LAG tienen los mismos modos de control de flujo y contrapresión.
- Todos los puertos del LAG tienen la misma prioridad.
- Todos los puertos del LAG tienen el mismo tipo de transceptor.
- PowerConnect 6024/6024F admite hasta siete LAG.
- Los puertos sólo se pueden configurar como puertos LACP si no forman parte de un LAG configurado previamente.

Los puertos agregados a un LAG pierden su configuración de puerto individual. Cuando los puertos se eliminan del LAG, se les aplica la configuración de puerto original.

El conmutador utiliza una función hash para determinar qué tramas se transportan en qué miembro de la conexión agregada. La función hash equilibra estadísticamente la carga de los miembros de la conexión agregada. El conmutador considera la conexión agregada como un puerto lógico único.

Para abrir la página **Link Aggregation** (Agregado de conexiones), haga clic en **Switch**→ **Link Aggregation** (Conmutador→ Agregado de conexiones) en la vista de árbol.

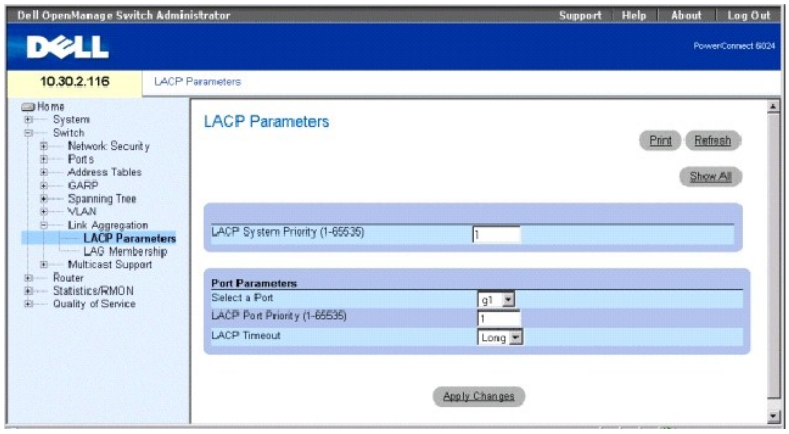
Definición de los parámetros del LACP

Los puertos agregados se pueden conectar en grupos de puertos de agregado de conexiones. Cada grupo consta de puertos con la misma velocidad, establecida en el modo dúplex completo.

Los puertos de un grupo de agregado de conexiones (LAG) pueden contener diferentes tipos de soportes si los puertos funcionan a la misma velocidad. Las conexiones agregadas se pueden configurar manual o automáticamente habilitando el protocolo de control de adición de enlaces (LACP) en las conexiones pertinentes.

Utilice la página **LACP Parameters** (Parámetros de LACP) para configurar grupos LAG de LACP. Para abrir la página **LACP Parameters** (Parámetros de LACP), haga clic en **Switch**→ **Link Aggregation**→ **LACP Parameters** (Conmutador→ Agregado de conexiones→ Parámetros de LACP) en la vista de árbol.

Ilustración 7-34. Página LACP Parameters (Parámetros de LACP)



La página **LACP Parameters** (Parámetros de LACP) contiene secciones para definir parámetros globales y parámetros de puertos.

LACP System Priority (1-65535) (Prioridad del sistema de LACP [1-65535]): Indica el valor de prioridad de LACP para la configuración global. El valor predeterminado es 1.

Select a Port (Seleccionar un puerto): El número de puerto al que se asignan los valores de tiempo de espera y de prioridad.

LACP Port Priority (1-65535) (Prioridad del puerto de LACP [1-65535]): El valor de prioridad de LACP para el puerto.

LACP Timeout (Tiempo de espera de LACP): El tiempo de espera administrativo de LACP. Los valores 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 agregado de conexiones

1. Abra la página **LACP Parameters** (Parámetros de LACP).
2. Complete los campos **LACP System Priority** (Prioridad del sistema de LACP) y **LACP Timeout** (Tiempo de espera de LACP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se definen y el dispositivo se actualiza.

Definición de parámetros de puertos de agregado de conexiones

1. Abra la página **LACP Parameters** (Parámetros de LACP).
2. Desplácese hasta la tabla **Port Parameters** (Parámetros de puerto).
3. Seleccione el puerto para el que desee definir parámetros.
4. Defina los campos **LACP System Priority** (Prioridad del sistema de LACP) y **LACP Timeout** (Tiempo de espera de LACP).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se definen y el dispositivo se actualiza.

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) para visualizar **LACP Parameters Table** (Tabla de parámetros de LACP).

Configuración de los parámetros de LACP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar parámetros de LACP tal como aparecen en la página **Link Aggregation** (Agregado de conexiones).

Tabla 7-29. Comandos de la CLI para los parámetros de LACP

Comando de la CLI	Descripción
`lacp system-priority` *valor*	Configura la prioridad del sistema.
	Configura el valor de prioridad para los puertos físicos.

`lacp port-priority valor`	
`lacp timeout {long | short}`	Asigna un tiempo de espera de LACP administrativo.
`show lacp ethernet interfaz [parameters | statistics | protocol- state]`	Muestra información sobre LACP relativa a los puertos Ethernet.

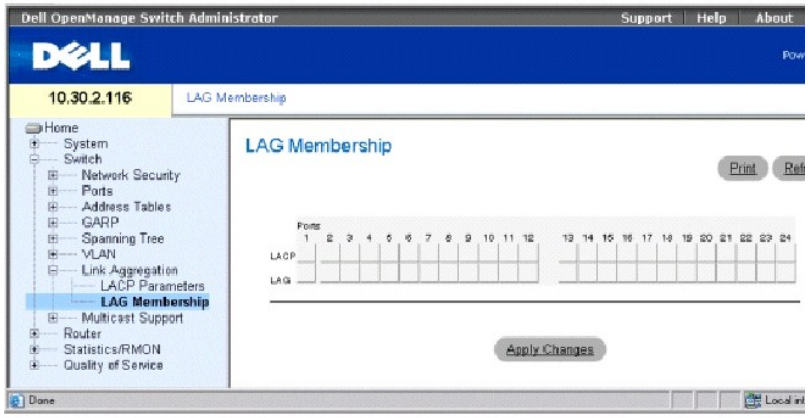
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet g8

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console (config-if)# exit

Console# show lacp ethernet g1 statistics

Port 1 LACP Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

Definición de la pertenencia a LAG

El conmutador admite hasta siete LAG por sistema y siete puertos por LAG. Utilice la página **LAG Membership** (Pertenencia a LAG) para asignar puerto a los LAG. Para abrir la página **LAG Membership** (Pertenencia a LAG), haga clic en **Switch**→ **Link Aggregation**→ **LAG Membership** (Conmutador→ Agregado de conexiones→ Pertenencia a LAG) en la vista de árbol.

Ilustración 7-35. Página LAG Membership (Pertenencia a LAG)



LACP: Agrega el puerto a un LAG, mediante LACP.

LAG: Agrega un puerto a un LAG e indica el LAG especifico al que pertenece el puerto.

Adición de un puerto a un LAG

1. Abra la página **LAG Membership** (Pertenencia a LAG).
2. Cambie la posición del botón ubicado debajo del número de puerto para asignar la configuración estática y el número de LAG.
3. Coloque el botón ubicado en la fila LACP en la posición **L** para agregar el puerto a un LAG con LACP
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se agrega al LAG y el dispositivo se actualiza.

Asignación de puertos a LAG mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar puertos a LAG tal como aparecen en la página **LAG Membership** (Pertenencia a LAG).

Tabla 7-30. Comandos de la CLI para la pertenencia a LAG

Comando de la CLI	Descripción
`interface port-channel` *`número_canal_puerto`*	Entra en el modo de configuración de interfaz de un canal de puertos específico.
`channel-group` *`número_canal_puerto`* `mode {on | auto}`	Asocia un puerto con un canal de puertos. Utilice la variedad no form de este comando para eliminar la configuración del grupo de canales de la interfaz.
`show interfaces port- channel [`*`número_canal_puerto`*`]`	Muestra información del canal de puertos.

```
Console (config)# interface port-channel 1
```

```
Console (config-if)# channel-group 1 mode on
```

```
Console# show interfaces port-channel

Channel       Port

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

Ch 1          Active    g1, g2    Inactive g3

Ch 2          Active    g2

Ch 3          Inactive  g8
```

Compatibilidad con el reenvío de multidifusión

El reenvío de multidifusión permite reenviar un solo paquete a varios destinos. El servicio de multidifusión de nivel 2 se basa en el conmutador de nivel 2 que recibe un solo paquete direccionado a una dirección de multidifusión específica. El reenvío de multidifusión crea copias del paquete, y transmite los paquetes a los puertos pertinentes.

Este 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 está activado por defecto y el usuario no lo puede configurar.

NOTA: El sistema admite el filtrado de multidifusión para 256 grupos de multidifusión.

- **Filtering L2 Multicast Packets** (Filtrado de paquetes de multidifusión L2): Reenvía paquetes de nivel 2 a las interfaces. Si el filtrado de multidifusión está inhabilitado, los paquetes de multidifusión se acumulan en los puertos pertinentes.

Para abrir la página **Multicast Support** (Compatibilidad con multidifusión), haga clic en **Switch**→ **Multicast Support** (Conmutador→ Compatibilidad con multidifusión) en la vista de árbol.

Definición de los parámetros globales de multidifusión

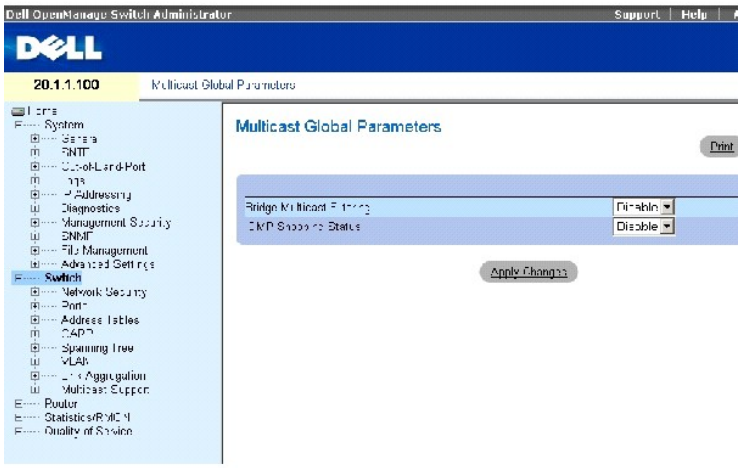
La conmutación de nivel 2 reenvía paquetes de multidifusión a todos los puertos de VLAN pertinentes de manera predeterminada, gestionando el paquete como un paquete de transmisión de multidifusión. Aunque el reenvío de tráfico de multidifusión es efectivo, no es óptimo, ya que los puertos que no son importantes también reciben los paquetes de multidifusión. Los paquetes sobrantes provocan el aumento del tráfico de red. Los filtros de reenvío de multidifusión habilitan el reenvío de paquetes de nivel 2 a los subconjuntos de los puertos.

Cuando la inspección IGMP está activada globalmente, todos los paquetes IGMP se reenvían a la CPU. La CPU analiza los paquetes entrantes y determina qué puertos quieren unirse a qué grupos de multidifusión, qué puertos tienen enrutadores de multidifusión que generan consultas de IGMP y qué protocolos enrutadores reenvían paquetes y tráfico de multidifusión.

Los puertos que solicitan la unión a un grupo de multidifusión específico emiten un informe IGMP en el que se especifica que el grupo de multidifusión acepta miembros. Así se crea una base de datos de filtros de multidifusión.

Utilice la página **Multicast Global Parameters** (Parámetros globales de multidifusión) para habilitar la inspección IGMP en el dispositivo. Para abrir la página **Multicast Global Parameters** (Parámetros globales de multidifusión), haga clic en **Switch**→ **Multicast Support**→ **Global Parameters** (Conmutador→ Compatibilidad con multidifusión→ Parámetros globales) en la vista de árbol.

Ilustración 7-36. Multicast Global Parameters (Parámetros globales de multidifusión)



La página **Multicast Global Parameters** (Parámetros globales de multidifusión) contiene los siguientes campos:

Bridge Multicast Filtering (Filtrado de multidifusión de puente): Habilita o inhabilita el filtrado de multidifusión de puente. El valor predeterminado es **Disabled** (Inhabilitado).

IGMP Snooping Status (Estado de inspección IGMP): Habilita o inhabilita la inspección IGMP en el dispositivo. El valor predeterminado es **Disabled** (Inhabilitado).

Habilitación del filtrado de multidifusión de puente en el dispositivo

1. Abra la página **Multicast Global Parameters** (Parámetros globales de multidifusión).
2. Seleccione **Enable** (Activar) en el campo **Bridge Multicast Filtering** (Filtrado de multidifusión de puente).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La multidifusión de puente se habilita en el dispositivo.

Habilitación de la inspección IGMP en el dispositivo

1. Abra la página **Multicast Global Parameters** (Parámetros globales de multidifusión).
2. Seleccione **Enable** (Activar) en el campo **IGMP Snooping Status** (Estado de inspección IGMP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La inspección IGMP se habilita en el dispositivo.

Habilitación del reenvío de multidifusión y la inspección IGMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para habilitar el reenvío de multidifusión y la inspección IGMP tal como aparecen en la página **Multicast Support** (Compatibilidad con multidifusión).

Tabla 7-31. Comandos de la CLI para el reenvío de multidifusión y la inspección

Comando de la CLI	Descripción
`bridge multicast filtering`	Habilita el filtrado de direcciones de multidifusión.

`ip igmp snooping`	Habilita la inspección IGMP (Internet Group Membership Protocol).

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

```
Console (config)# bridge multicast filtering
```

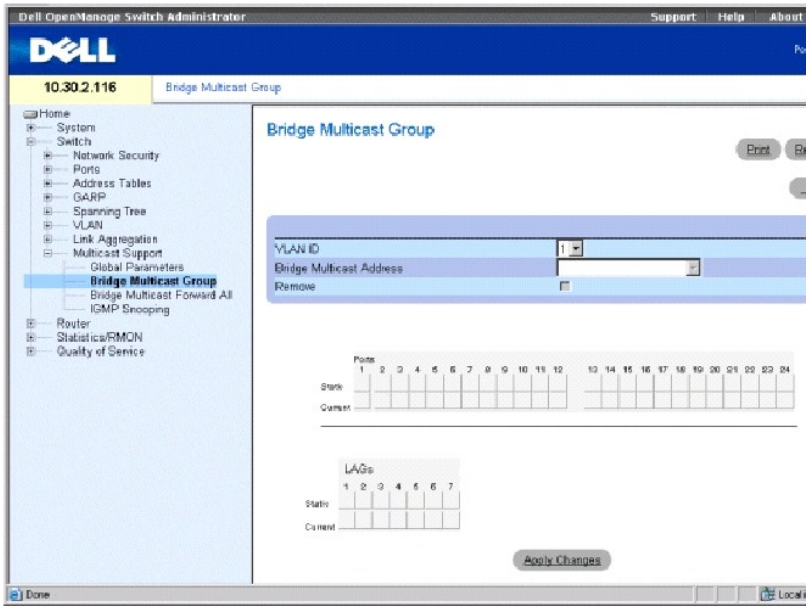
```
Console (config)# ip igmp snooping
```

Adición de miembros de dirección de multidifusión de puente

En la página **Bridge Multicast Group** (Grupo de multidifusión de puente) se muestran los puertos y los LAG conectados al grupo de servicio de multidifusión de las tablas **Ports** (Puertos) y **LAGs** (LAG). En las tablas de puertos y LAG también se refleja el modo en que el puerto o los LAG se han unido al grupo de multidifusión. Los puertos pueden agregarse bien a los grupos existentes o a grupos de servicio de multidifusión. La página **Bridge Multicast Group** (Grupo de multidifusión de puente) permite la creación de nuevos grupos de servicio de multidifusión. La página **Bridge Multicast Group** (Grupo de multidifusión de puente) también asigna puertos a un grupo específico de direcciones de servicio de multidifusión.

Para abrir la página **Bridge Multicast Group** (Grupo de multidifusión de puente), haga clic en **Switch**→ **Multicast Support**→ **Bridge Multicast Address** (Conmutador→ Compatibilidad con multidifusión→ Dirección de multidifusión de puente) en la vista de árbol.

Ilustración 7-37. Página Bridge Multicast Group (Grupo de multidifusión de puente)



VLAN ID (ID de VLAN): Identifica una VLAN y contiene información sobre la dirección de 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): El puerto que se puede agregar a un servicio de multidifusión.

LAGs (LAG): Los LAG que se pueden agregar a un servicio de multidifusión.

La siguiente tabla contiene los valores para la gestión del puerto IGMP y los miembros de LAG.

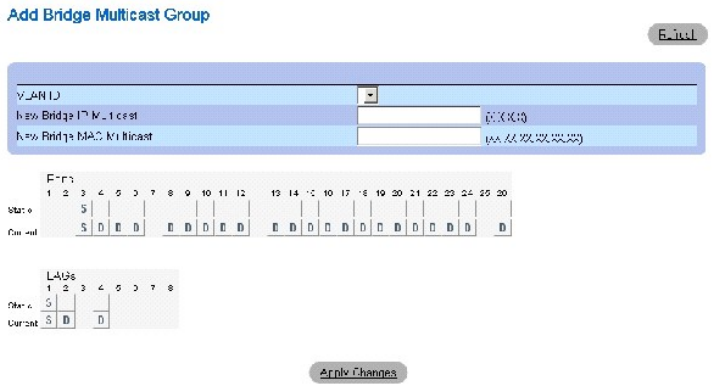
Tabla 7-32. Valores de control de la tabla de los miembros de LAG/puerto IGMP

Control de puerto	Definición
D	Indica que el puerto/LAG se ha unido al grupo de multidifusión dinámicamente 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/LAG se ha unido al grupo de multidifusión estáticamente en la fila **Current** (Actual).
F	Indica que el puerto/LAG tiene prohibida la entrada al grupo de multidifusión.
En blanco	Indica que el puerto no está conectado a un 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** (Agregar) para visualizar la página **Add Bridge Multicast Group** (Agregar grupo de multidifusión de puente).

Ilustración 7-38. Página Add Bridge Multicast Group (Agregar grupo de multidifusión de puente)



3. Defina los campos **VLAN ID** (ID de VLAN) y **New Bridge Multicast Address** (Nueva dirección de multidifusión de puente).
4. Conmute un puerto a la posición **S** para que éste se pueda unir al grupo de multidifusión seleccionado.
5. Conmute un puerto a la posición **F** para prohibir que se puedan agregar direcciones de multidifusión específicas a un puerto específico.
6. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección de multidifusión se asigna al grupo de multidifusión y el dispositivo se actualiza.

Definición de puertos para que reciban el 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. Conmute un puerto a la posición **S** para que éste se pueda unir al grupo de multidifusión seleccionado.
4. Conmute un puerto a la posición **F** para prohibir que se puedan agregar direcciones de multidifusión específicas a un puerto específico.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se asigna al grupo de multidifusión y el dispositivo se actualiza.

Asignación de LAG para que reciban el 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. Conmute el LAG a la posición **S** para que éste se pueda unir al grupo de multidifusión seleccionado.
4. Conmute el LAG a la posición **F** para prohibir que se puedan agregar direcciones de multidifusión específicas a un LAG específico.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El LAG se asigna al grupo de multidifusión y el dispositivo se actualiza.

Administración de miembros de servicio de multidifusión mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes administrar miembros del servicio de multidifusión tal como aparecen en la página **Bridge Multicast Group** (Grupo de multidifusión de puente).

Tabla 7-33. Comandos de la CLI para los miembros del servicio de multidifusión

Comando de la CLI	Descripción
`bridge multicast address {`*`dirección_multidifusión_mac`* `| `*`dirección_ip_multidifusión`*`} [add | remove] {ethernet `*`lista_interfaz`* `| port-channel `*`lista_número_canal_puerto`*`}`	Registra las direcciones de multidifusión de nivel MAC en la tabla puente y agrega puertos estáticos al grupo.
`bridge multicast forbidden address {`*`dirección_multidifusión_mac`* `| `*`dirección_multidifusión_ip`*`} [add | remove] {ethernet interface-list | port-channel port-channel- number-list}`	Prohibe la adición de una dirección de multidifusión específica a puertos específicos. Use la variedad no form de este comando para volver al valor predeterminado.
`show bridge multicast address-table [vlan vlan- id] [address mac-multicast-address | `*`dirección_multidifusión_ip`*`] [format ip | mac]`	Muestra la información de la tabla de direcciones MAC de multidifusión.

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

```
Console# config

Console (config)# vlan database

Console (config-if)# vlan 8

Console (config-if)# exit

Console (config)# interface range ethernet g1-9

Console (config-if)# switchport mode general

Console (config-if)# switchport general allow vlan add 8

Console (config)# interface vlan 8
```

```
Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# exit

Console# show bridge multicast address-table

Vlan   MAC Address      type      Ports

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

1      0100.5e02.0203   static    g1, g2

19     0100.5e02.0208   static    g1-8

19     0100.5e02.0208   dynamic   g9-11

Forbidden ports for multicast addresses:

Vlan   MAC Address      Ports

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

1      0100.5e02.0203   g8

19     0100.5e02.0208   g8

Console# configuration

Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

Console (config-if)# bridge multicast forbidden address 0100.5e02.0203 add ethernet g9
```

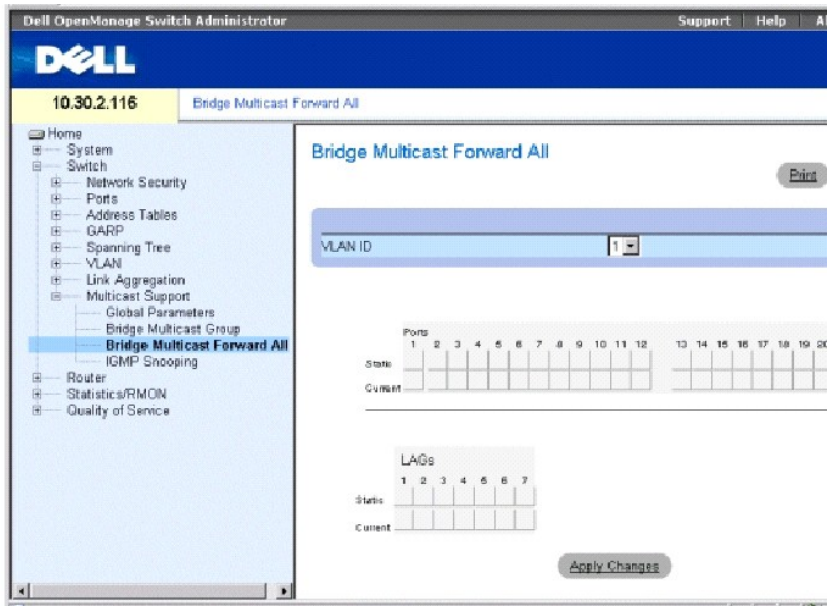
Asignación de parámetros de multidifusión reenviar todos

Utilice la página **Bridge Multicast Forward All** (Multidifusión de puente reenviar todos) para habilitar la conexión de puertos o LAG a un conmutador

conectado a un enrutador/conmutador de multidifusión adyacente. Una vez habilitada la inspección IGMP, los paquetes de multidifusión se reenvían al puerto o VLAN correspondiente.

Para abrir la página **Bridge Multicast Forward All** (Multidifusión de puente reenviar todos), haga clic en **Switch**→ **Multicast Support**→ **Bridge Multicast**→ **Bridge Multicast Forward All** (Conmutador→ Compatibilidad con multidifusión→ Multidifusión de puente→ Multidifusión de puente reenviar todos) en la vista de árbol.

Ilustración 7-39. Página Bridge Multicast Forward All (Multidifusión de puente reenviar todos)



VLAN ID (ID de VLAN): Identifica una VLAN de paquetes y contiene información sobre la dirección de grupo de multidifusión.

Ports (Puertos): Los puertos que se puede agregar a un servicio de multidifusión.

LAGs (LAG): Los LAG que se pueden agregar a un servicio de multidifusión.

La siguiente tabla contiene la configuración necesaria para administrar la configuración del enrutador y del puerto.

Tabla 7-34. Control de puerto/enrutador de multidifusión de puente Reenviar todos

Control de puerto	Definición
D	Conecta el puerto al conmutador o enrutador de multidifusión como un puerto dinámico.
S	Conecta el puerto al conmutador o enrutador de multidifusión como un puerto estático.
F	Prohibido.
En blanco	Indica que el puerto no está conectado a un conmutador o enrutador de multidifusión.

Conexión de un puerto a un conmutador o direccionador 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 asigne un valor al puerto.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto está conectado al conmutador o enrutador de multidifusión.

Conexión de un LAG a un conmutador o direccionador 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 no está conectado al conmutador o enrutador de multidifusión.

Administración de LAG y puertos conectados a enrutadores de multidifusión mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para administrar los LAG y puertos conectados a enrutadores de multidifusión tal como aparecen en la página **Bridge Multicast Forward All** (Multidifusión de puente reenviar todos).

Tabla 7-35. Comandos de la CLI para gestionar 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_interfaz`* `| port- channel` *`lista_número_canal_puerto`*`}`	Habilita el reenvío de todos los paquetes de multidifusión en un puerto. Use la variedad no form de este comando para volver al valor predeterminado.

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

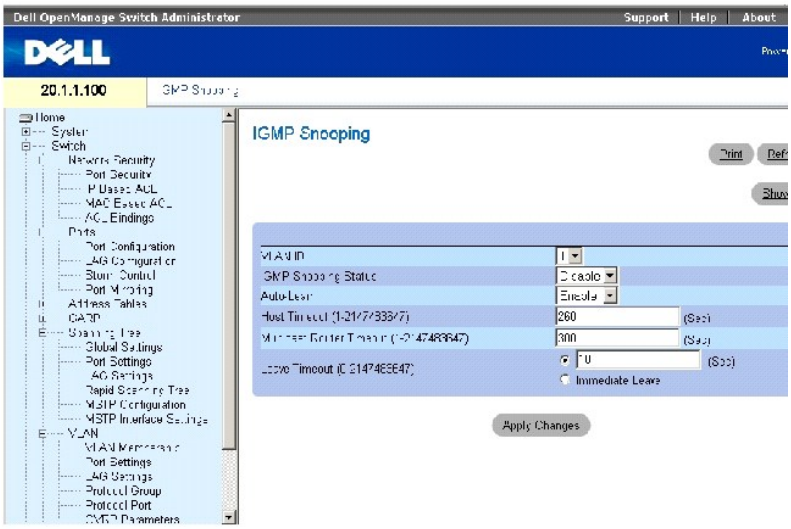
```
Console# show bridge multicast filtering 1

Filtering: Disabled

VLAN: 1

Forward-All

Port      Static      Status

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

g1        -           Filter

g2        -           Filter

...

Console# config
```

```
Console (config)# vlan database

Console (config-if)# vlan 8

Console (config-vlan)# exit

Console (config)# interface range ethernet g1-9

Console (config-if)# switchport mode general

Console (config-if)# switchport general allow vlan add 8

Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# exit

Console# configuration

Console (config)# interface VLAN 1

Console (config-if)# bridge multicast forward-all add ethernet g8
```

Inspección IGMP

Utilice la página **IGMP Snooping** (Inspección IGMP) para agregar miembros de IGMP. Para abrir la página **IGMP Snooping** (Inspección IGMP), haga clic en **Switch**→ **Multicast Support**→ **IGMP Snooping** (Conmutador→ Compatibilidad con multidifusión→ Inspección IGMP) en la vista de árbol.

Ilustración 7-40. IGMP Snooping (Inspección IGMP)



VLAN ID (ID de VLAN): Especifica el ID de VLAN.

IGMP Snooping Status (Estado de inspección IGMP): Habilita o inhabilita la inspección IGMP en la VLAN.

Auto Learn (Obtención automática): Habilita o inhabilita la obtención automática en el dispositivo.

Host Timeout (1-2147483647) (Tiempo de espera de sistema principal [1-2147483647]): El tiempo que transcurre antes de que caduque una entrada de inspección IGMP. El valor predeterminado es 260 segundos.

Multicast Router Timeout (1-2147483647) (Tiempo de espera del enrutador de multidifusión [1-2147483647]): El tiempo que transcurre antes de que caduque una entrada del enrutador de multidifusión. El valor predeterminado es 300 segundos.

Leave Timeout (0-2147483647) (Tiempo de espera de cese [0-2147483647]): El tiempo en segundos que transcurre después que se recibe un mensaje de cese del puerto hasta que la entrada caduca. **User-defined** (Definido por el usuario) le permite establecer el período de tiempo de espera. El **Immediate Leave** (Cese inmediato) especifica un período de tiempo de espera inmediato. El tiempo de espera predeterminado es 10 segundos.

Habilitación de la inspección IGMP en el dispositivo

1. Abra la página **IGMP Snooping** (Inspección IGMP).
2. Seleccione el ID de VLAN del dispositivo en el que desee habilitar la inspección IGMP.
3. Seleccione **Enable** (Activar) en el campo **IGMP Snooping Status** (Estado de inspección IGMP).
4. Complete los campos de esta página.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La inspección IGMP se habilita en el dispositivo.

Visualización de la tabla de inspección IGMP

1. Abra la página **IGMP Snooping** (Inspección IGMP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **IGMP Snooping Table** (Tabla de inspección IGMP).

Configuración de la inspección IGMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para configurar la seguridad de los puertos bloqueados tal como aparecen en la página **IGMP Snooping** (Inspección IGMP).

Tabla 7-36. Comandos de la CLI para la inspección IGMP

Comando de la CLI	Descripción
`ip igmp snooping`	Habilita la inspección IGMP (Internet Group Membership Protocol).
`ip igmp snooping mrouter learn-pim-dvmrp`	Habilita la obtención automática de los puertos de enrutador de multidifusión en el contexto de una VLAN específica.
`ip igmp snooping host-time- out` *`tiempo de espera`*	Configura el tiempo de espera del sistema principal.
`ip igmp snooping mrouter- time-out` *`tiempo de espera`*	Configura el tiempo de espera del enrutador de multidifusión.
`ip igmp snooping leave-time- out {`*`tiempo de espera`* `| immediate- leave}`	Configura el tiempo de espera de cese.
`show ip igmp snooping interface` *`id_vlan`*	Muestra la configuración de inspección IGMP.
`show ip igmp snooping mrouter [interface` *`id_vlan`*`]`	Muestra información sobre las interfaces del enrutador de multidifusión obtenidas dinámicamente.

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

```
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)# exit

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show ip igmp snooping interface 1000
```

```
IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1000

IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast router ports is enabled

Console> show igmp-snooping mrouter

VLAN      Ports

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

2         g9
```

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del encaminamiento

Sistemas Dell PowerConnect 6024/6024F

Visión general del encaminamiento

Los dispositivos de diferentes subredes se comunican entre ellos mediante un enrutador de nivel 3 entre las VLAN. El encaminamiento está habilitado de manera predeterminada en el conmutador. Sin embargo, se debe configurar como mínimo una interfaz IP para que el conmutador inicie el tráfico de red de encaminamiento. Las rutas se configuran estadísticamente o bien mediante el protocolo RIP (Routing Information Protocol) o el protocolo OSPF (Open Shortest Path First).

Para obtener más información sobre RIP, consulte el apartado Configuración de RIP .

Para obtener más información sobre OSPF, consulte el apartado Configuración de parámetros y filtros de OSPF .

Configuración del encaminamiento IP global

La página **Global Routing Parameters** (Parámetros de encaminamiento global) contiene enlaces para configurar el encaminamiento. El encaminamiento siempre está activado, pero sólo se habilita si el sistema tiene una o varias direcciones IP. Para abrir la página **Global Routing Parameters** (Parámetros de encaminamiento global), haga clic en **Router**→ **Global Routing Parameters** (Enrutador→ Parámetros de encaminamiento global) en la vista de árbol.

Esta página **Global Routing Parameters** contiene enlaces que le permiten realizar los siguientes procedimientos:

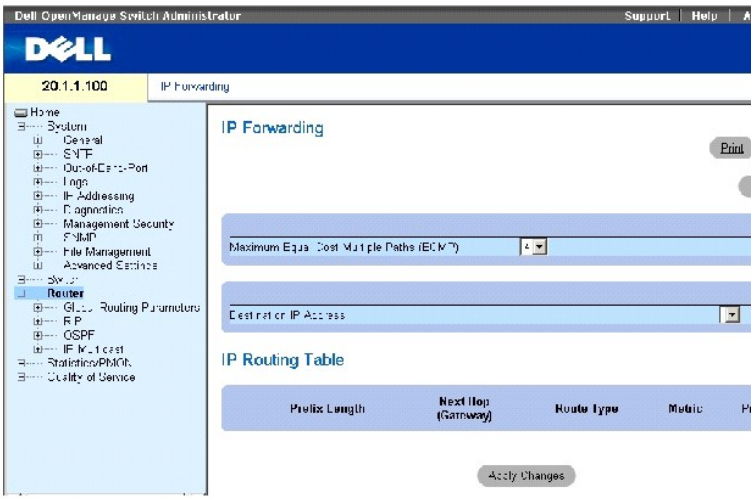
- Configuración de la tabla de reenvío IP
- Configuración de las rutas IP estáticas
- Configuración de VRRP
- Configuración de la autenticación del encaminamiento por MD5
- Configuración de los valores de la cadena de claves MD5

Configuración de la tabla de reenvío IP

Utilice la página **IP Forwarding** (Reenvío IP) para ver los parámetros de encaminamiento por los que se reenvía el tráfico IP. En esta página se proporciona una lista de rutas IP para las direcciones IP de destino seleccionadas, incluidas las rutas IP que se definen de manera estática o dinámica. Las rutas IP se basan en máscaras de red, próximos saltos, métrica y protocolos de reenvío. Estos parámetros determinan cómo se reenvían o eliminan paquetes específicos. Cuando se configura una dirección IP en una interfaz, se incluye en la tabla de reenvío IP.

Para abrir la página **IP Forwarding** (Reenvío IP), haga clic en **Router**→ **Global Routing Parameters**→ **IP Forwarding** (Enrutador→ Parámetros de encaminamiento global→ Reenvío IP) en la vista de árbol.

Ilustración 8-1. Página IP Forwarding (Reenvío IP)



Maximum Equal Cost Multipaths (ECMP) (Máximo de múltiples rutas de acceso del mismo coste [ECMP]): El valor ECMP, que se debe definir cuando se reenvían paquetes IP. El valor ECMP indica cuántas rutas de acceso hay disponibles desde el enrutador hasta una red. El intervalo de valores posibles es de 1 a 4. Por ejemplo, un valor de 1 indica que sólo hay una ruta de acceso a la red. Cuanto mayor sea el valor, más recursos de memoria se necesitarán. Las modificaciones realizadas en este campo sólo son efectivas después de restablecer el dispositivo.

Destination IP Address (Dirección IP de destino): La red IP de destino.

Prefix Length (Longitud del prefijo): El número de bits que componen el prefijo de la dirección IP de destino. La longitud oscila entre 1 y 32 bits.

Next Hop (Gateway) (Próximo salto [Puerta de enlace]): La dirección del próximo enrutador en la ruta hacia la red de destino.

Route Type (Tipo de ruta): Especifica cómo se realiza el encaminamiento remoto. Los valores posibles son:

Remote (Remoto): El paquete se reenvía.

Reject (Rechazar): El paquete se elimina.

Local: El paquete se envía a una red local.

Metric (Métrica): El número de saltos efectuados hasta llegar a la red de destino.

Protocol (Protocolo): El protocolo de encaminamiento mediante el que se ha agregado esta ruta.

Visualización de la tabla de reenvío IP

En la **IP Forwarding Table** (Tabla de reenvío IP) se proporciona una lista de todas las rutas IP del sistema.

1. Abra la página **IP Forwarding** (Reenvío IP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **IP Forwarding Table** (Tabla de reenvío IP).

Visualización del reenvío IP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver el reenvío IP.

Tabla 8-1. Comandos de la CLI para el reenvío IP

Comando de la CLI	Descripción
show ip route [address]<*dirección_ip*>	Muestra el estado actual de la tabla de encaminamiento.
ip maximum-paths number-paths	Controla el número máximo de rutas paralelas instaladas en una tabla de encaminamiento.

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

```
Console (config)# interface ip 10.10.10.2

Console (config-ip)# ip maximum-paths 2

Console (config-ip)# exit

Console (config)# exit

Console# exit

Console> show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, E - OSPF external

R 10.0.0.0/8 is rejected

C 10.0.1.1/32 is directly connected, Loopback0

C 10.0.1.0/24 is directly connected, Ethernet g1

C 10.0.2.0/24 is directly connected, Ethernet g2

R 10.8.2.0/24 [230/50] via 10.0.2.2, 00:17:19, Ethernet g2

S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Ethernet g1

S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active

O 10.8.1.0/24 [30/2000] via 10.0.1.2, 00:39:08, Ethernet g1

S 172.1.0.0/16 [5/3] via 10.0.1.1, 18:21:58, Ethernet g1
```

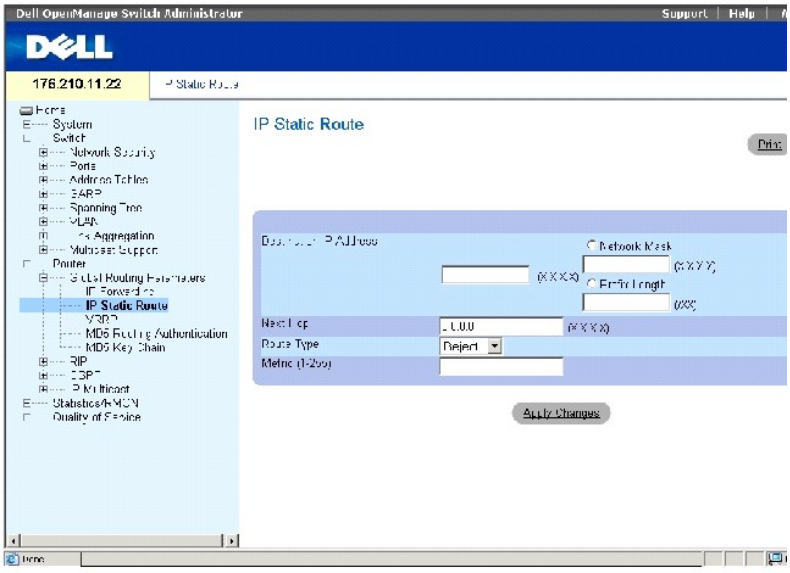
```
S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1

S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet g1

Maximum Parallel Paths: 2
```

Configuración de las rutas IP estáticas

Utilice la página **IP Static Route** (Ruta IP estática) para definir las rutas estáticas.

Para abrir la página **IP Static Route** (Ruta IP estática), haga clic en **Router**→ **Global Routing Parameters**→ **IP Static Route** (Enrutador→ Parámetros de encaminamiento global→ Ruta IP estática) en la vista de árbol.

Ilustración 8-2. Página IP Static Route (Ruta IP estática)



Destination IP Address (Dirección IP de destino): La red IP de destino de la ruta estática.

Network Mask (Máscara de red): La máscara de red de destino para esta ruta.

Prefix Length (Longitud del prefijo): El número de bits que componen el prefijo de la dirección IP de destino. La longitud oscila entre 1 y 32 bits.

Next Hop (Próximo salto): Indica la dirección del próximo sistema en la ruta.

Route Type (Tipo de ruta): Especifica cómo se realiza el encaminamiento remoto. Los valores de campo posibles son:

Remote (Remoto): El paquete se reenvía.

Reject (Rechazar): El paquete se elimina.

Local: El paquete se envía a una red local.

Metric (1-255) (Métrica [1-255]): Número de saltos hasta la red de destino.

Adición de rutas IP estáticas

NOTA: Sólo un enrutador conectado directamente se puede definir como puerta de enlace.

1. Abra la página **IP Static Route** (Ruta IP estática).
2. Defina los campos de la página.

NOTA: Si selecciona **Reject** (Rechazar) en la opción **Route Type** (Tipo de ruta) todas las rutas a la red designada serán inaccesibles.

Si desea definir una ruta estática para un sistema principal situado en una red remota, seleccione **Remote** (Remoto) en la opción **Route Type** (Tipo de ruta).

Si desea definir una ruta estática para un sistema principal situado en la red local, seleccione **Local** en la opción **Route Type** (Tipo de ruta).

Las opciones **Destination IP Address** (Dirección IP de destino) y **Network Mask** (Máscara de red) designan la dirección de red remota. La opción **Next Hop** (Próximo salto) indica la dirección de un enrutador conectado directamente al conmutador.

La opción **Destination IP Address** (Dirección IP de destino) indica la dirección del sistema principal. La opción **Next Hop** (Próximo salto) se debe rellenar como 0.0.0.0.

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

La nueva ruta estática se agrega y el dispositivo se actualiza.

Eliminación de una ruta IP estática

1. Abra la página **IP Static Route** (Ruta IP estática).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **IP Static Route Table** (Tabla de ruta estática IP).
3. Marque la opción **Remove for the Destination IP address** (Eliminar la dirección IP de destino) de la ruta estática que desee eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La ruta estática se suprime y el dispositivo se actualiza.

Configuración de la tabla estática IP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar la tabla estática IP.

Tabla 8-2. Comandos de la CLI para la tabla de ruta IP estática

Comando de la CLI	Descripción
`ip route prefix {`*`máscara`* `|` *`longitud_prefijo`*`} `*`puerta de enlace`* `[metric `*`distancia`*`] [reject- route]`	Establece las rutas IP estáticas.

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

```
Console (config)# ip route 172.16.0.0 255.255.0.0 131.16.1.1
```

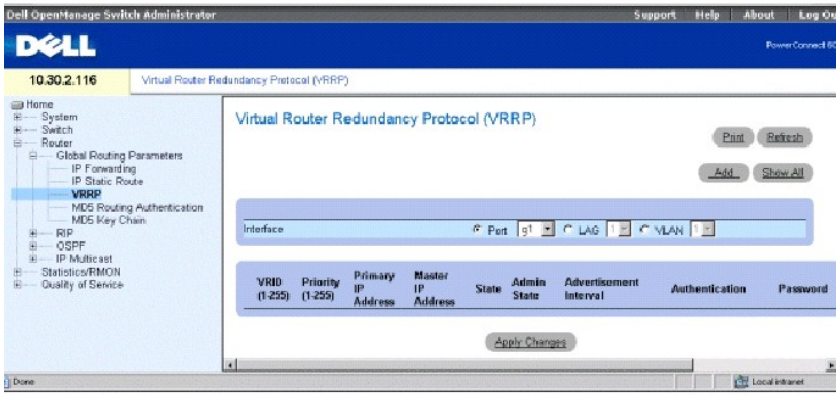
Configuración de VRRP

El protocolo de redundancia de enrutador virtual (VRRP) especifica un protocolo de elección que asigna de manera dinámica la responsabilidad del encaminamiento a uno de los enrutadores VRRP de la LAN (el enrutador principal). El proceso de elección permite realizar una conmutación por errores dinámica en la responsabilidad de encaminamiento si el enrutador maestro no está disponible.

La ventaja de VRRP es que elimina el fenómeno de error de un solo punto inherente al entorno de encaminamiento al proporcionar una ruta de acceso predeterminada de mayor disponibilidad, a la vez que elimina la necesidad de configuración de protocolos de encaminamiento dinámico o de detección de encaminamiento en cada sistema principal final.

La página **Virtual Router Redundancy Protocol (VRRP)** (Protocolo de redundancia de enrutador virtual [VRRP]) establece los parámetros de encaminamiento VRRP del conmutador. Para abrir la página **Virtual Router Redundancy Protocol (VRRP)** (Protocolo de redundancia de enrutador virtual [VRRP]), haga clic en **Router→ Global Routing Parameters→ VRRP** (Enrutador→ Parámetros de encaminamiento global→ VRRP) en la vista de árbol.

Ilustración 8-3. Página Virtual Router Redundancy Protocol (VRRP) (Protocolo de redundancia de enrutador virtual [VRRP])



Interface (Interfaz): El tipo de interfaz y el número conectado al enrutador VRRP.

VRID (1-255): El identificador virtual del enrutador.

Priority (1-255) (Prioridad [1-255]): La prioridad del enrutador que se utiliza en el proceso de elección del enrutador virtual. El valor puede determinar si un enrutador VRRP de mayor prioridad suprime un enrutador VRRP de menor prioridad.

Primary IP Address (Dirección IP principal): La dirección IP virtual identificada con el enrutador virtual. La dirección IP principal se selecciona a partir de direcciones de interfaz reales configuradas en un enrutador VRRP.

Master IP Address (Dirección IP maestra): El enrutador VRRP que es actualmente maestro de este enrutador virtual.

State (Estado): El estado actual del enrutador. Los valores posibles son:

Master (Maestro): El enrutador funciona como el enrutador de reenvío de las direcciones IP asociadas con el enrutador virtual. El enrutador maestro responde a las peticiones de ARP con direcciones IP asociadas en el destino ARP, reenvía los paquetes con una dirección MAC virtual (VMAC) como MAC de destino, y acepta paquetes asociados con las direcciones IP virtuales (sólo si el enrutador es propietario de la dirección IP asociada).

Initialize (Inicializar): El enrutador espera un evento de inicio. Cuando se recibe el evento de inicio, el enrutador pasa al estado adecuado.

Backup (Copia de seguridad): El enrutador realiza una copia de seguridad del enrutador maestro. El enrutador supervisa de manera continua si el enrutador maestro está disponible mediante los anuncios periódicos que envía el maestro o mediante anuncios específicos que se envían desde el maestro y anuncian que se está desactivando.

Admin State (Estado de administración): Indica si el enrutador está activo o no.

Advertisement Interval (Intervalo de anuncio): Indica la frecuencia con la que se envían anuncios cuando el enrutador es el maestro.

Authentication (Autenticación): Especifica si no se realiza ningún proceso de autenticación o si se utilizan contraseñas para autenticar los intercambios de protocolo VRRP.

Password (Contraseña): La contraseña que se utiliza para autenticar los intercambios de protocolo VRRP.

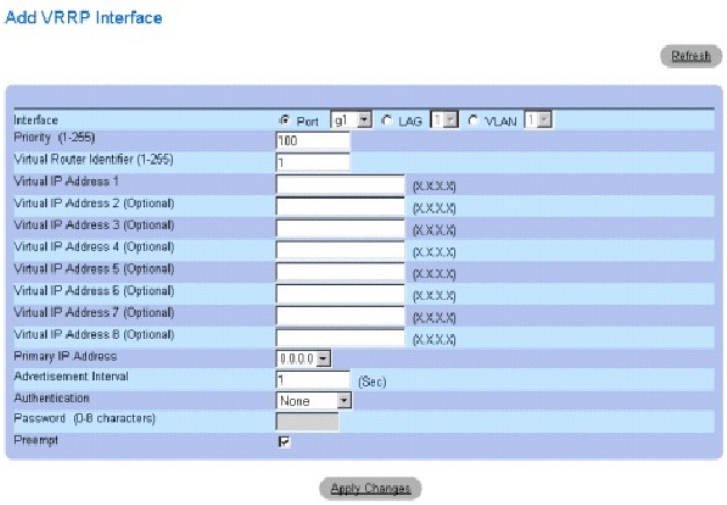
Preempt (Anular): Si se selecciona esta opción, los enrutadores VRRP de mayor prioridad pueden suprimir los enrutadores de menor prioridad.

Remove (Eliminar): Si se selecciona esta opción, se eliminan las entradas de VRRP de la tabla de VRRP.

Adición de enrutadores a un grupo de VRRP

1. Abra la página **Virtual Router Redundancy Protocol (VRRP)** (Protocolo de redundancia de enrutador virtual [VRRP]).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add VRRP Interface** (Agregar una interfaz de VRRP).

Ilustración 8-4. Add VRRP Interface (Agregar una interfaz de VRRP)



3. Defina los campos.

Consulte el apartado Configuración de VRRP para obtener información sobre los campos.

NOTA: Hay que definir las interfaces de VRRP antes de que el estado de administración pueda estar *habilitado*.

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

La nueva interfaz de VRRP se agrega y el dispositivo se actualiza.

NOTA: Si se especifica una dirección IP virtual ilícita, aparecerá una advertencia, pero el enrutador virtual se agregará. Se recomienda que suprima esta entrada de la tabla de enrutadores virtuales.

Modificación de enrutadores de VRRP

1. Abra la página **Virtual Router Redundancy Protocol (VRRP)** (Protocolo de redundancia de enrutador virtual [VRRP]).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).
3. Defina los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Supresión de una entrada de VRRP

1. Abra la página **Virtual Router Redundancy Protocol (VRRP)** (Protocolo de redundancia de enrutador virtual [VRRP]).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **VRRP Table** (Tabla de VRRP).
3. Seleccione una entrada de la tabla.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada de VRRP se suprime y el dispositivo se actualiza.

Configuración de VRRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar el VRRP.

Tabla 8-3. Comandos de la CLI para VRRP

Comando de la CLI	Descripción
vrrp *enrutador_virtual ip dirección_ip* [*dirección_ip2...dirección_ip8*]	Define el protocolo de redundancia de enrutador virtual (VRRP) de una interfaz.
vrrp *enrutador_virtual* up	Activa el protocolo de redundancia de enrutador virtual (VRRP) en una interfaz.
vrrp *enrutador_virtual* timer *segundos*	Configura el intervalo de tiempo que transcurre entre el envío de mensajes de anuncio.
vrrp *enrutador_virtual* priority *prioridad*	Configura la prioridad del protocolo de redundancia de enrutador virtual (VRRP) en una interfaz.
vrrp *enrutador_virtual* source-ip *dirección_ip*	Define la dirección IP de origen (dirección IP principal) que se utiliza para los mensajes del protocolo de redundancia de enrutador virtual (VRRP) en una interfaz.
vrrp *enrutador_virtual* authentication *texto*	Habilita la autenticación del protocolo de redundancia de enrutador virtual (VRRP) en una interfaz.
vrrp *enrutador_virtual* preempt	Habilita la anulación del protocolo de redundancia de enrutador virtual (VRRP) en una interfaz.
show vrrp configuration [ethernet *número_* interfaz | *vlan id_vlan* | *número_canal_puerto*]	Muestra la configuración del protocolo de redundancia de enrutador virtual (VRRP).
show vrrp status [ethernet *número_interfaz* | *vlan id-vlan* |	Muestra el estado del protocolo de redundancia de enrutador virtual (VRRP).

número_canal_puerto]	

Configuración de VRRP mediante los comandos de la CLI

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

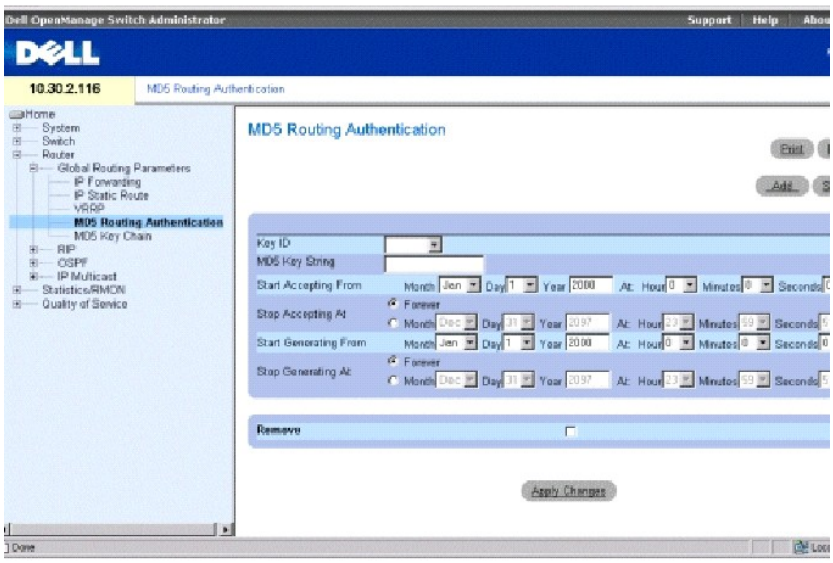
```
Console (config)# interface ethernet g8

Console (config-if)# vrrp 45 ip 172.16.1.1 172.16.2.1

Console (config-if)# vrrp 45 up

Console (config-if)# vrrp 45 timer 100

Console (config-if)# vrrp 45 priority 150

Console (config-if)# vrrp 45 source-ip 168.192.1.1

Console (config-if)# vrrp 45 authentication Dell

Console (config-if)# vrrp 45 preempt

Console (config-if)# exit

Console (config)# exit
```

Configuración de la autenticación del encaminamiento por MD5

Las claves MD5 las utiliza el algoritmo de autenticación MD5. Se pueden definir las horas de inicio y final, tanto para enviar como para recibir, de cada clave. Se pueden configurar las claves que están activas y caducan a las horas restablecidas. Las interfaces que se comunican entre ellas deben tener el mismo ID de clave. Si las horas de las claves se solapan en el extremo de envío, el dispositivo utiliza la clave con la hora de inicio más reciente. Cuando se reciben paquetes, la interfaz utiliza la clave que indica el valor **Key ID** (ID de clave) en el paquete.

Utilice la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5) para definir y gestionar las claves. Para abrir la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5), haga clic en **Router**→ **Global Routing Parameters**→ **MD5 Routing Authentication** (Enrutador→ Parámetros de encaminamiento global→ Autenticación del encaminamiento por MD5) en la vista de árbol.

Ilustración 8-5. MD5 Routing Authentication (Autenticación del encaminamiento por MD5)



Key ID (ID de clave): Especifica el ID de clave.

MD5 Key String (Cadena de clave MD5): Indica la contraseña que se utiliza para la autenticación del encaminamiento.

Start Accepting From (Empezar a aceptar desde): La fecha y la hora en que la clave MD5 empieza a aceptar tráfico con la clave MD5 especificada. El formato del campo **Start Accept** (Empezar a aceptar) es **Mes:Día:Año: Hora:Minuto:Segundo**.

Stop Accepting At (Dejar de aceptar a las): La fecha y la hora en que la clave MD5 empieza a no aceptar ya más tráfico con la clave MD5 especificada. El formato de campo **Stop Accept** (Dejar de aceptar) es **Mes:Día:Año: Hora:Minuto:Segundo**. Si selecciona **Forever** (Para siempre), no se establecerá ningún límite para aceptar tráfico con claves MD5.

Start Generating From (Empezar a generar desde): La fecha y la hora en que los paquetes del protocolo se reenvían con las claves MD5. El formato del campo **Start Generate** (Empezar a generar) es **Mes:Día:Año: Hora:Minuto:Segundo**.

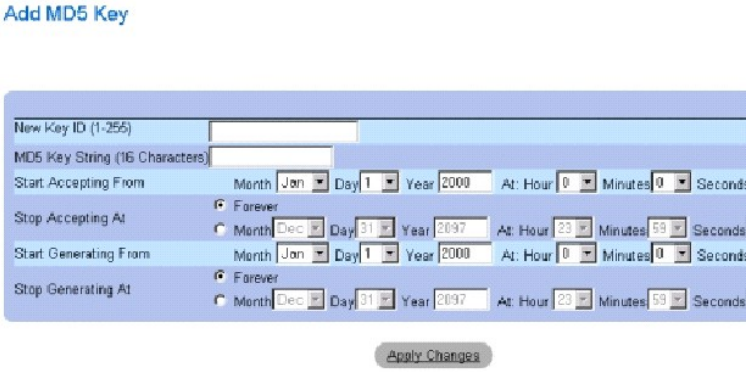
Stop Generating At (Dejar de generar a las): La fecha y la hora en que los paquetes de protocolos dejan de reenviarse con claves MD5. El formato del campo **Stop Generate** (Dejar de generar) es **Mes:Día:Año: Hora:Minuto:Segundo**. Si selecciona **Forever** (Para siempre), no se establecerá ningún límite para aceptar tráfico con claves MD5.

Remove (Eliminar): Si selecciona esta opción, se elimina la clave MD5.

Adición de una clave MD5

1. Abra la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add MD5 Key** (Agregar una clave MD5).

Ilustración 8-6. Add MD5 Key (Agregar una clave MD5)



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

La nueva clave MD5 se agrega a **MD5 Key Table** (Tabla de clave MD5) y el dispositivo se actualiza.

Modificación de una clave MD5

1. Abra la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).
2. En el menú descendente **Entry No.** (Número de entrada), seleccione la clave MD5 que desee modificar.
3. Modifique los campos del cuadro de diálogo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los nueva clave MD5 se modifica y el dispositivo se actualiza.

Supresión de una clave MD5

1. Abra la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **MD5 Key Table** (Tabla de clave MD5).
3. Seleccione una entrada en el campo **Key ID** (ID de clave).
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los clave MD5 se suprime y el dispositivo se actualiza.

Configuración de la autenticación por MD5 mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar la autenticación por MD5.

Tabla 8-4. Comandos de la CLI para la autenticación por MD5

Comando de la CLI	Descripción
key *id_clave*	Crea una clave de autenticación.
	Establece el período de tiempo durante el que se puede recibir la clave de

accept-lifetime { duration time-to-start day-of-the-month *día_del_mes* year-to- start key-lifetime-duration-in-seconds } | { infinite time-to- start day-of-the-month *día_del_mes* year- to-start } | { time- to-start day-of-the- month *día_del_mes* year-to-start time-to- stop day-of-the-month *día_del_mes* year- to-stop }	autenticación en una cadena de claves.
send-lifetime { duration time-to-start day-of-the-month *día_del_mes* year-to- start key-lifetime-duration-in-seconds } | { infinite time-to- start day-of-the-month *día_del_mes* year- to-start } | { time- to-start day-of-the- month *día_del_mes* year-to-start time-to- stop day-of-the-month *día_del_mes* year- to-stop }	Establece el período de tiempo durante el que se puede enviar una clave de autenticación en una cadena de claves.

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

```
Console (config)# key 3
```

```
Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200
```

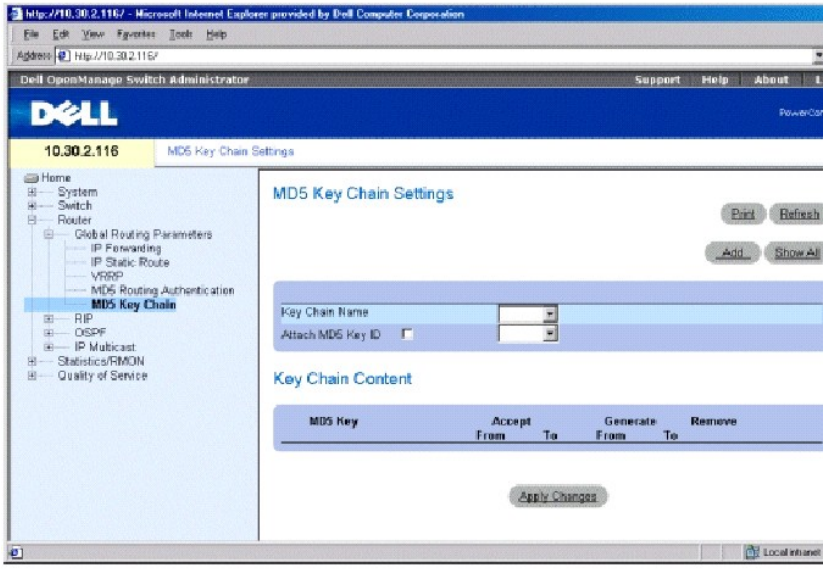
```
Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600
```

Configuración de los valores de la cadena de claves MD5

Después de definir las claves, éstas se agrupan en lo que se denomina una cadena de claves . Se pueden asignar varias claves a la vez a cada interfaz del enrutador. Las claves se pueden agrupar en cadenas de claves para asignarlas de forma cómoda a las interfaces. Cada clave se puede incluir en varias cadenas de claves. Las cadenas de claves se asignan a las interfaces en los parámetros de interfaz RIP u OSPF. Las claves MD5 se agregan a una cadena de claves MD5 para generar la cadena de claves.

Utilice la página **MD5 Key Chain Settings** (Valores de la cadena de claves MD5) para definir las cadenas de claves y asignarles claves. Para abrir la página **MD5 Key Chain Settings** (Valores de la cadena de claves MD5), haga clic en **Router**→ **Global Routing Parameters**→ **MD5 Key Chain** (Enrutador→ Parámetros de encaminamiento global→ Cadena de claves MD5) en la vista de árbol.

Ilustración 8-7. MD5 Key Chain Settings (Valores de la cadena de claves MD5)



Key Chain Name (Nombre de la cadena de claves): Nombres de la cadena de claves definidas por el usuario.

Attach MD5 Key ID (Adjuntar ID de clave MD5): Indica el ID de cadena de clave que se adjunta a la cadena de claves.

MD5 Key (Clave): La clave que es miembro de una cadena de claves.

Accept From (Aceptar desde): La fecha y la hora en que la clave MD5 seleccionada empieza a aceptar tráfico con la clave MD5 especificada. El formato del campo **Accept From** (Aceptar desde) es **Mes:Día:Año: Hora:Minuto:Segundo**. El campo **Accept From** (Aceptar desde) es la clave que se define en la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).

Accept To (Aceptar hasta): La fecha y la hora a partir de la cual la clave MD5 seleccionada ya no acepta tráfico con la clave MD5 especificada. El formato del campo es **Mes:Día:Año: Hora:Minuto:Segundo**. El campo **Accept To** (Aceptar hasta) es la clave que se define en la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).

Generate From (Generar desde): La fecha y la hora en que la clave MD5 empieza a reenviar tráfico. El formato del campo **Generate From** (Generar desde) es **Mes:Día:Año: Hora:Minuto:Segundo**. El campo **Generate From** (Generar desde) es la clave que se define en la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).

Generate To (Generar hasta): La fecha y la hora en que la clave MD5 seleccionada deja de reenviar tráfico. El formato del campo **Generate To** (Generar para) es **Mes:Día:Formato: Hora:Minuto:Segundo**. El campo **Generate To** (Generar para) es la clave que se define en la página **MD5 Routing Authentication** (Autenticación del encaminamiento por MD5).

Remove (Eliminar): Si se selecciona esta opción, se elimina la clave MD5 de la tabla de cadena de claves MD5.

Adición de una cadena de claves MD5

1. Abra la página **MD5 Key Chain Settings** (Configuración de la cadena de claves MD5).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add Key Chain** (Agregar una cadena de claves).
3. Complete los campos **New Key Chain Name** (Nuevo nombre de cadena de claves) y **Attach MD5 Key No.** (Adjuntar número de clave MD5).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva cadena de claves MD5 se agrega a la tabla de cadena de claves MD5 y el dispositivo se actualiza.

Modificación de una cadena de claves MD5

1. Abra la página **MD5 Key Chain Settings** (Configuración de la cadena de claves MD5).
2. Modifique los campos **Name** (Nombre) o **Key Chain ID** (ID de cadena de claves).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los nueva cadena de claves MD5 se modifica y el dispositivo se actualiza.

Eliminación de una cadena de claves MD5:

1. Abra la página **MD5 Key Chain Settings** (Configuración de la cadena de claves MD5).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **MD5 Key Chain Table** (Tabla de cadena de claves MD5).
3. Seleccione una entrada en el campo **Key Chain Name** (Nombre de cadena de claves).
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La cadena de claves MD5 se elimina y el dispositivo se actualiza.

Configuración de las cadenas de claves mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar las cadenas de claves.

Tabla 8-5. Comandos de la CLI para las cadenas de claves

Comando de la CLI	Descripción
key-chain *nombre_ de_cadena*	Identifica un grupo de claves de autenticación.
key *id_clave*	Identifica una clave de autenticación en una cadena de claves.
key-string *texto*	Especifica una cadena de caracteres de autenticación para una clave.
accept-lifetime *tiempo_inicio tiempo_fin* | {infinite | *tiempo_inicio* | duration *tiempo_inicio segundos*} no accept-lifetime	Establece el período de tiempo durante el cual la clave de autenticación es válida para autenticar los paquetes entrantes.
send-lifetime *tiempo_inicio tiempo_fin* | {infinite | *tiempo_inicio* | duration *tiempo_inicio segundos*}no send-lifetime	Establece el período de tiempo durante el cual una clave de autenticación es válida para generar una autenticación por MD5 implícita para los paquetes salientes.
show key-chains [*nombre_de_cadena*]	Muestra información de la cadena de claves.

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

```
Console (config)# key chain M

Console (config-key-chain)# key 1

Console (config-key)# key-string mountain

Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200

Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600

Console (config-key)# exit

Console (config)# exit

Console# show key-chains

key chain internal

key 1

accept: 13:30:00 Jan 25 2002 duration 7200

send: 14:00:00 Jan 25 2002 duration 3600
```

```
key 2

accept: 14:30:00 Jan 25 2002 duration 7200

send: 15:00:00 Jan 25 2002 duration 3600

key chain external

key 1

accept: 13:30:00 Jan 25 2002 until 15:30:00 Jan 25 2002

send: 14:00:00 Jan 25 2002 until 15:00:00 Jan 25 2002

key 2

accept: 14:30:00 Jan 25 2002 until 16:30:00 Jan 25 2002

send: 15:00:00 Jan 25 2002 until 16:00:00 Jan 25 2002

25 2002
```

Configuración de RIP

El Protocolo de información de encaminamiento (RIP) es el estándar de Internet más utilizado para protocolos de puertas de enlace interiores. El protocolo transmite la información de encaminamiento para determinar cuál es la ruta más rápida hasta el próximo destino. RIP es un protocolo de encaminamiento del vector de distancia que se utiliza preferentemente en redes pequeñas. Las rutas se determinan mediante el recuento de saltos más pequeño. Las actualizaciones de encaminamiento contienen pares de valores formados por una dirección IP y la distancia hasta el nodo.

RIP versión 2 hace lo siguiente:

- Admite máscaras de subredes.
- Proporciona métodos de autenticación.
- Admite protocolos de encaminamiento.
- Proporciona requisitos de actividad general de amplitud de banda menores y de distribución mayores.

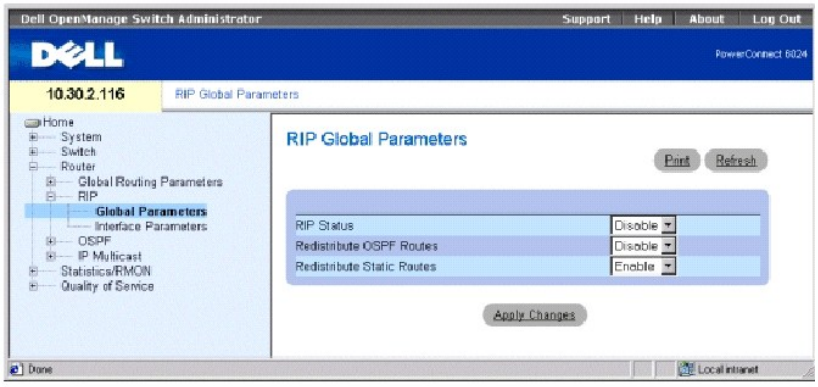
Puede configurar RIP en la página **RIP**. Para abrir la página **RIP**, haga clic en **Router**→ **RIP** (Enrutador→ RIP) en la vista de árbol.

Definición de los parámetros globales de RIP

En la página **RIP Global Parameters** (Parámetros globales de RIP) se proporcionan los campos para habilitar RIP en el dispositivo, con lo que se establece la redistribución de OSPF y la redistribución de rutas estáticas.

Haga clic en **Router→ RIP→ Global Parameters** (Enrutador→ RIP→ Parámetros globales) en la vista de árbol para visualizar la página **RIP Global Parameters** (Parámetros globales de RIP).

Ilustración 8-8. Página RIP Global Parameters (Parámetros globales de RIP)



RIP Status (Estado de RIP): Habilita o inhabilita RIP en el dispositivo.

Redistribute OSPF Routes (Redistribuir rutas de OSPF): Si se habilita esta opción, se redistribuyen las rutas de OSPF a RIP. La redistribución de las rutas conlleva la importación de interfaces de encaminamiento externas en el protocolo RIP.

Redistribute Static Routes (Redistribuir rutas estáticas): Si se habilita esta opción, se redistribuyen las rutas de rutas estáticas a RIP.

Habilitación de RIP, redistribución de rutas de OSPF, redistribución de rutas estáticas

1. Abra la página **RIP Global Parameters** (Parámetros globales de RIP).
2. Seleccione **Enabled** (Habilitado) en el campo de parámetros globales de RIP que desee habilitar.
3. Haga clic en **Apply Changes** (Aplicar cambios).

RIP se habilita en el dispositivo.

Configuración de los parámetros globales de RIP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar los parámetros globales de RIP.

Tabla 8-6. Comandos de la CLI para los parámetros globales de RIP

Comando de la CLI	Descripción
`router rip enable`	Habilita el protocolo de información de encaminamiento (RIP) en el dispositivo.
`no router rip enable`	Inhabilita el protocolo de información de encaminamiento (RIP) en el dispositivo.
`router rip redistribute ospf`	Anuncia las rutas obtenidas por OSPF en el proceso RIP.
`no router rip redistribute ospf`	Deja de anunciar las rutas obtenidas por OSPF en el proceso RIP.

`router rip redistribute static`	Anuncia las rutas configuradas estadísticamente en el proceso RIP.
`no router rip redistribute static`	Deja de anunciar las rutas configuradas estáticamente en el proceso RIP.

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

```
Console (config)# router rip enable

Console (config)# router rip redistribute ospf

Console (config)# router rip redistribute static

Console (config)# no router rip enable

Console (config)# no router rip redistribute ospf

Console (config)# no router rip redistribute static
```

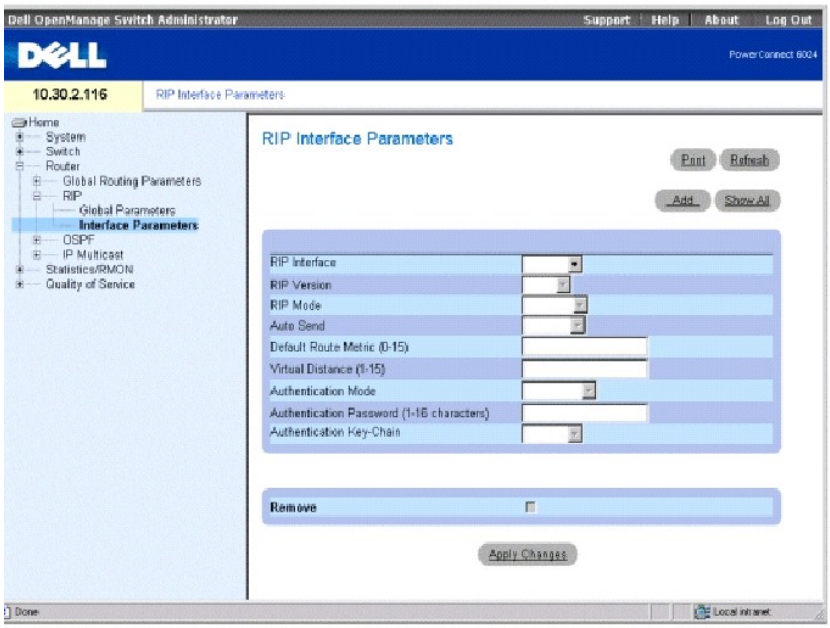
Definición de los parámetros de la interfaz RIP

Utilice la página **RIP Interface Parameters** (Parámetros de la interfaz RIP) para definir las direcciones IP en las que RIP está activado, definir la métrica de encaminamiento, activar el envío automático, definir la distancia virtual y definir el estado IP.

NOTA: Para definir una interfaz RIP, es necesario que RIP esté habilitado. Consulte el apartado Habilitación de RIP, redistribución de rutas de OSPF, redistribución de rutas estáticas para obtener más información.

Para abrir la página **RIP Interface Parameters** (Parámetros de la interfaz RIP), haga clic en **Router**→ **RIP**→ **RIP Interface Parameters** (Enrutador→ RIP→ Parámetros de la interfaz RIP) en la vista de árbol.

Ilustración 8-9. Página RIP Interface Parameters (Parámetros de la interfaz RIP)



RIP Interface (Interfaz RIP): La dirección IP de la interfaz actual.

RIP Version (Versión RIP): El tipo de RIP que se transmite. Los valores posibles son:

Ver. 1 (Versión 1): Transmite las actualizaciones de RIP compatibles con RFC 1058.

Ver. 2 (Versión 2): Indica que el dispositivo está transmitiendo actualizaciones de RIP 2.

RIP Mode (Modo RIP): El tipo de operación RIP. Los valores posibles son:

RX (Receptor): Las difusiones de recepción de RIP se reciben en el dispositivo.

RX & TX (Receptor y transmisor): Las difusiones de recepción y transmisión de RIP se reciben en el dispositivo.

Auto Send (Envío automático): Habilita al dispositivo para que anuncie mensajes de RIP sólo en la métrica predeterminada, lo que permite que las estaciones obtengan la dirección predeterminada del enrutador. Como resultado, se evita que el enrutador envíe demasiadas actualizaciones de RIP a enlaces en los que no existen enrutadores para recibirlas. Mientras la opción **Auto Send** (Envío automático) está activa, se envía una actualización de RIP de pequeño formato, lo que permite a las estaciones escuchar a RIP para que realice un descubrimiento de enrutadores y envíe una actualización de RIP a los enrutadores que se agregarán a la red posteriormente.

Si se recibe una actualización de RIP en una interfaz, se inhabilita la opción **Auto Send** (Envío automático) en esa interfaz y se envían actualizaciones de RIP completas. Si el dispositivo detecta otro mensaje de RIP, la opción **Auto Send** (Envío automático) se inhabilita.

Default Route Metric (1-16) (Métrica de ruta predeterminada): La métrica de entrada de ruta predeterminada en las actualizaciones de RIP que se originan en esta interfaz. Cero indica que no se ha originado ninguna ruta predeterminada.

Virtual Distance (1-16) (Distancia virtual [1-16]): Número virtual de saltos asignados a la interfaz. Así se ajusta el algoritmo de encaminamiento RIP.

Authentication Mode (Modo de autenticación): El tipo de autenticación de la interfaz, contraseña o MD5, que se utiliza para autenticar los mensajes de RIP versión. 2.

Authentication Password (Contraseña de autenticación): La contraseña de autenticación.

Authentication Key-Chain (Cadena de claves de autenticación): La cadena de claves de autenticación.

Remove (Eliminar): Si se selecciona esta opción, se elimina la interfaz RIP.

Adición de una interfaz RIP

1. Abra la página **RIP Interface Parameters** (Parámetros de la interfaz RIP).
2. Haga clic en **Add** (Agregar) para visualizar la página **New RIP Interface** (Nueva interfaz RIP).
3. Complete los campos de esta página.

   Los campos de esta página son los mismos que los de la página **RIP Interface Parameters** (Parámetros de la interfaz RIP).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Modificación de los parámetros de la interfaz RIP

1. Abra la página **RIP Interface Parameters** (Parámetros de la interfaz RIP).
2. Modifique los campos según convenga.
3. Haga clic en **Apply Changes** (Aplicar cambios).

   Los parámetros de la interfaz RIP se modifican y el dispositivo se actualiza.

Supresión de una interfaz RIP

1. Abra la página **RIP Interface Parameters** (Parámetros de la interfaz RIP).
2. Utilice el menú descendente **RIP Interface** (Interfaz RIP) para seleccionar una interfaz RIP.
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

   Se elimina la interfaz RIP y el dispositivo se actualiza.

Configuración de interfaces RIP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar los parámetros globales de RIP.

Tabla 8-7. Comandos de la CLI para la configuración de RIP

Comando de la CLI	Descripción
`rip`	Activa RIP en una interfaz.
`rip version {1 | 2}`	Especifica una versión de RIP.
`rip passive-interface`	Inhabilita el envío de actualizaciones de encaminamiento en una interfaz.
`rip auto-send`	Detecta automáticamente si es necesario que la información RIP se envíe a la interfaz.

`rip offset` *diferencia*	Agrega un desplazamiento a una métrica obtenida a través de RIP antes de agregarla a la tabla de la interfaz.
`rip default-route offset` *diferencia*	Genera una ruta predeterminada en RIP mediante la aplicación de un valor de desplazamiento.
`rip authentication {text` *texto* `|` *nombre_de_cadena* *md5*`}`	Habilita la autenticación para los paquetes de RIP versión 2 y especifica el tipo de autenticación.
`show ip rip`	Muestra información del RIP de IP.
`show ip rip md5`	Muestra información MD5 del RIP de IP.

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

```
Console (config)# router rip enable

Console (config)# interface ip 100.1.1.1

Console (config-ip)# rip

Console (config-ip)# rip version 1

Console (config-ip)# rip passive interface

Console (config-ip)# rip auto-send

Console (config-ip)# rip offset 5

Console (config-ip)# rip default-route offset 5

Console (config-ip)# rip authorization text dell

Console (config-ip)# exit

Console (config)# exit

Console# show ip rip

RIP is enabled.

OSPF leaking is enabled.

Static leaking is enabled.
```

```
Interface State Ver Offset Default Route Passive Auto Send Auth

176.16.0.0/16 Enabled 2 1 Disabled No Yes MD5

192.168.0.0/16 Enabled 2 1 Disabled No No Text
```

Configuración de parámetros y filtros de OSPF

El protocolo de puerta de enlace interna OSPF (Open Shortest Path First) permite que los enrutadores intercambien mensajes sobre el estado de la conexión mediante la recopilación de información de red y la determinación de la mejor ruta de acceso de encaminamiento según la distancia del nodo.

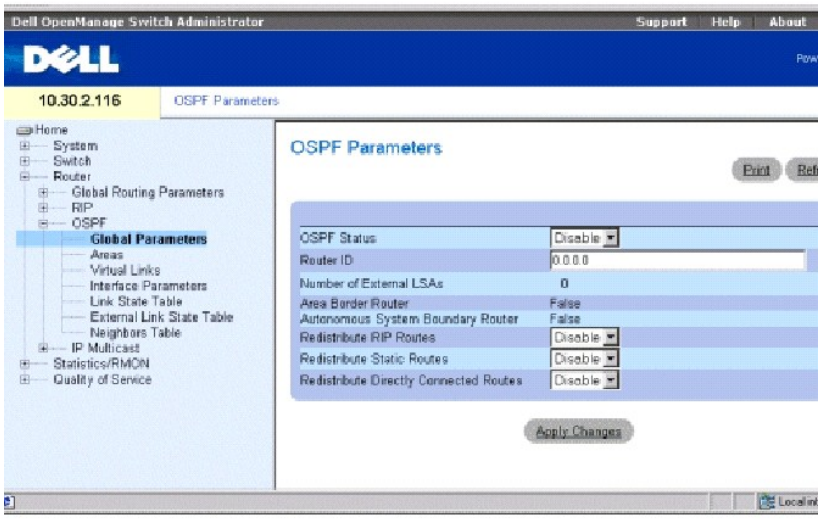
OSPF es un protocolo de estado de la conexión en vez de un protocolo de vector de distancia y, por tanto, necesita menos amplitud de banda que RIP. OSPF se habilita y define mediante:

- Configuración de parámetros OSPF
- Configuración de áreas OSPF
- Configuración de los enlaces virtuales de OSPF
- Visualización de la tabla de estado de enlace
- Visualización de la tabla de estado de enlace externo
- Visualización de la tabla de elementos adyacentes de OSPF

Configuración de parámetros OSPF

OSPF descubre la mejor ruta de acceso de encaminamiento según el nodo de distancia. OSPF está habilitado en la página **OSPF Parameters** (Parámetros OSPF). Para abrir la página **OSPF Parameters** (Parámetros OSPF), haga clic en **Router**→ **OSPF**→ **Global Parameters** (Enrutador→ OSPF→ Parámetros globales) en la vista de árbol.

Ilustración 8-10. Página OSPF Global Parameters (Parámetros globales de OSPF)



OSPF Status (Estado de OSPF): Habilita OSPF en una interfaz como mínimo o inhabilita OSPF para todas las interfaces.

Router ID (ID de enrutador): El número de identificación del enrutador. De manera predeterminada, el ID de enrutador es una dirección IP del dispositivo. **Router ID** (ID de enrutador) es un campo opcional, con un valor predeterminado de la interfaz IP del dispositivo más pequeño.

Number of External LSAs (Número de LSA externos): El número de anuncios externos del estado de los enlaces (LSA) de la base de datos de estado de enlace.

Area Border Router (ABR) (Enrutador de límite de área [ABR]): Indica si el dispositivo es un enrutador de límite de área. Si el dispositivo está configurado como un ABR, está conectado a dos o más áreas. Un área es el área de red troncal.

Autonomous System Boundary Router (ASBR) (Enrutador de límite de sistema autónomo [ASBR]): Indica si el dispositivo está configurado como un ASBR. Si el dispositivo está configurado como un ASBR, importa datos de encaminamiento de protocolos distintos al protocolo de encaminamiento OSPF.

Redistribute RIP Routes (Redistribuir rutas RIP): Habilita o inhabilita la redistribución de rutas insertadas en la tabla de encaminamiento IP por el protocolo RIP para anunciar OSPF como rutas externas.

Redistribute Static Routes (Redistribuir rutas estáticas): Habilita todas las rutas configuradas estáticamente para que se anuncien como rutas externas OSPF o inhabilita la redistribución de rutas estáticas.

Redistribute Directly Connected Routes (Redistribuir rutas conectadas directamente): Habilita todas las rutas externas para anunciar a OSPF como rutas externas o inhabilita la redistribución de rutas directas externas.

Habilitación de OSPF

1. Abra la página **OSPF Parameters** (Parámetros de OSPF).
2. Defina los campos **OSPF Status** (Estado de OSPF), **Router ID** (ID de enrutador), **Redistribute RIP Routes** (Redistribuir rutas RIP), **Redistribute Static Routes** (Redistribuir rutas estáticas), y **Redistribute Directly Connected Routes** (Redistribuir rutas conectadas directamente).
3. Haga clic en **Apply Changes** (Aplicar cambios).

OSPF se habilita en el dispositivo.

NOTA: Los procesos OSPF sólo se pueden borrar utilizando el comando de la CLI **clear ip ospf process**.

Habilitación de OSPF mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para habilitar OSPF.

Tabla 8-8. Comandos de la CLI para OSPF

Comando de la CLI	Descripción
`router ospf enable`	Habilita el proceso de encaminamiento de OSPF.
`router ospf router-id` *`dirección_ip`*	Configura un ID de enrutador de OSPF.
`router ospf redistribute rip`	Habilita las rutas de anuncio, que se obtienen por el proceso RIP, en el proceso de encaminamiento de OSPF.
`router ospf redistribute static`	Rutas de anuncio, configuradas estáticamente, en el proceso de encaminamiento de OSPF.
`outer ospf redistribute connected`	Rutas de anuncio conectadas directamente.

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

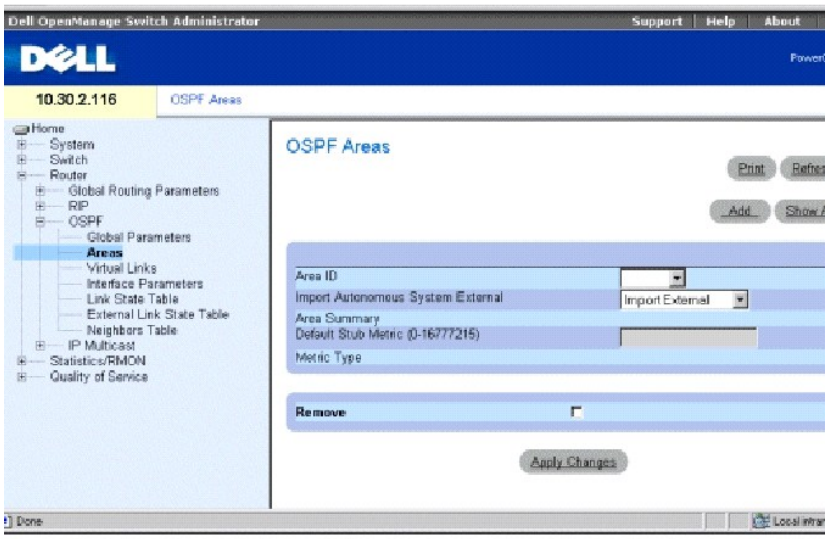
```
Console (config)# router ospf enable

Console (config)# router ospf router-id 196.127.2.1

Console (config)# router ospf redistribute rip

Console (config)# router ospf redistribute static
```

Configuración de áreas OSPF

La página **OSPF Areas** (Áreas OSPF) contiene información para definir y mantener áreas OSPF dentro de las cuales se definen las interfaces y los enlaces virtuales. Después de crear un área OSPF, OSPF se habilita automáticamente en todas las interfaces IP.

Para visualizar la página **OSPF Areas** (Áreas OSPF), haga clic en **Router**→ **OSPF**→ **Areas** (Enrutador→ OSPF→ Áreas) en la vista de árbol.

Ilustración 8-11. Página OSPF Areas (Áreas OSPF)



Area ID (ID de área): El ID de área. El formato es una dirección IP.

Import Autonamous System External (Importar AS externos): Indica si se trata de un área de rutas internas. Los valores posibles son:

Import External (Importar externos): Los anuncios de estado de enlace (LSA) externo del sistema autónomo se pueden importar en el área.

Import No External (Importar no externos): Los LAS externos no se pueden importar al área; por lo tanto, se trata de un área de rutas internas.

Area Summary (Resumen de área): Controla la importación de LSA de resumen en áreas de rutas internas. Esta variable no tiene ninguna repercusión en otras áreas. Los valores posibles son:

No Area Summary (Sin resumen de área): Especifica que se trata en su totalidad de un área de rutas internas.

Send Area Summary (Enviar resumen de área): Especifica que no se trata en su totalidad de un área de rutas internas.

Un área de rutas internas es un área a la que no se dirigen LSA externos de AS. Las áreas que se componen en su totalidad de rutas internas utilizan una ruta predeterminada para llegar no sólo a destinos externos del sistema autónomo, sino también a todos los destinos externos del área. Para aprovechar el soporte al área de rutas internas OSPF, se debe utilizar el encaminamiento predeterminado en el área de rutas internas.

Default Stub Metric (0-16777216) (Métrica predeterminada para el área de rutas internas [0-16777215]): La métrica de la ruta predeterminada creada para el área de rutas internas. Las áreas de rutas internas no importan AS externos. Por lo tanto, el enrutador de límite de área crea un ruta predeterminada para el área de rutas internas.

Metric Type (Tipo de métrica): El tipo de métrica del protocolo.

Remove (Eliminar): Si se selecciona esta opción, se elimina la dirección IP de la tabla de áreas OSPF.

Definición de una nueva área OSPF

1. Abra la página **OSPF Areas** (Áreas OSPF).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add an OSPF Area** (Agregar un área OSPF).
3. Complete los campos del cuadro de diálogo.

NOTA: El campo **Stub Metric** (Métrica de etiqueta) se define para los enrutadores de límite de área.

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

La nueva área se agrega a la tabla de áreas OSPF.

Modificación de los parámetros del área OSPF

1. Abra la página **OSPF Areas** (Áreas OSPF).
2. Seleccione un **Area ID** (ID de área).

Se muestran los parámetros del área OSPF.

3. Modifique los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del área se modifican y el dispositivo se actualiza.

Supresión de un área OSPF

1. Abra la página **OSPF Areas** (Áreas OSPF).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la tabla del área OSFP.
3. Seleccione un área OSPF y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El área OSPF se elimina de la tabla y el dispositivo se actualiza.

Definición de áreas OSPF mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir las áreas OSPF.

Tabla 8-9. Comandos de la CLI para el área OSPF

Comando de la CLI	Descripción
`router ospf area` *`id_área`* `stub`	Define un área como un área de rutas internas. Para inhabilitar esta función, utilice la forma no de este comando.
`router ospf area` *`id_área coste_predeterminado coste`*	Especifica un coste para la ruta de resumen predeterminada que se envía a un área de rutas internas.

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

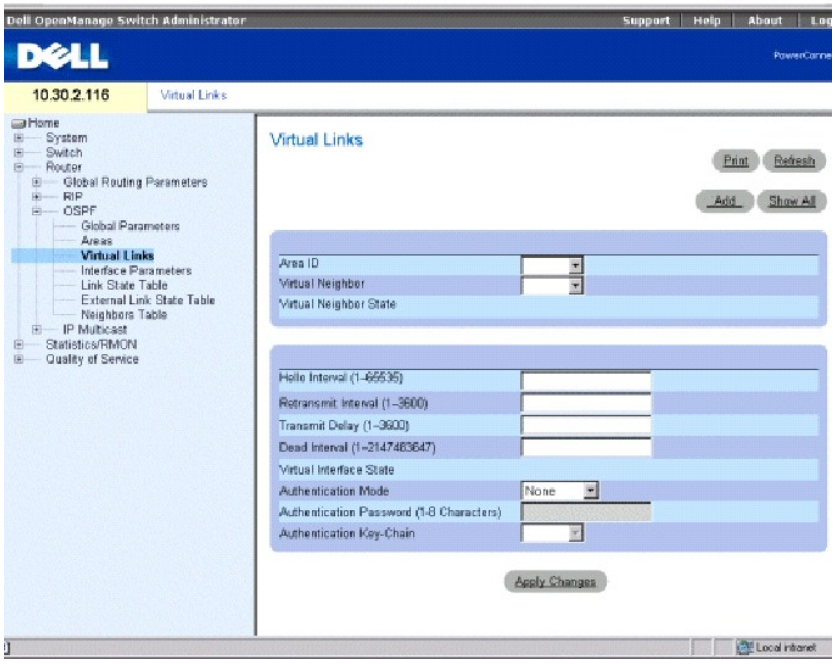
```
Console (config)# router ospf enable

Console (config)# router ospf area 7.7.7.7 stub

Console (config)# router ospf area 192.168.3.1 default-cost 10000
```

Configuración de los enlaces virtuales de OSPF

OSPF requiere que todas las áreas estén conectadas mediante un área de red troncal. Sin embargo, si un área no está conectada a una red troncal, se pueden conectar dos enrutadores de límite de área mediante un enlace virtual. Los enlaces virtuales se definen mediante la configuración de un elemento adyacente virtual. Los enlaces virtuales no se pueden configurar mediante un área de rutas internas.

Defina los enlaces virtuales en la página **Virtual Links** (Enlaces virtuales). Para visualizar la página **Virtual Links** (Enlaces virtuales), haga clic en **Router**→ **OSPF**→ **Virtual Links** (Enrutador→ OSPF→ Enlaces virtuales) en la vista de árbol.

Ilustración 8-12. Página Virtual Links (Enlaces virtuales)



Area ID (ID de área): El ID de área de la interfaz OSPF del área de tránsito.

Virtual Neighbor (Elemento adyacente virtual): El ID del enrutador del elemento adyacente virtual.

Virtual Neighbor State (Estado del elemento adyacente virtual): El estado del elemento adyacente virtual.

Hello Interval (1-65535) (Intervalo de saludo [1-65535]): El tiempo (segundos) entre los paquetes de saludo. Todos los dispositivos conectados a una red común deben tener el mismo intervalo de saludo. El valor predeterminado es 10 segundos.

Retransmit Interval (0-3600) (Intervalo de retransmisión): Tiempo (segundos) que transcurre entre las retransmisiones de anuncio de estado de enlaces (LSA) para adyacencias que pertenecen a la interfaz. El valor debe ser superior a la demora de ida y vuelta prevista entre dos enrutadores de la red conectada. El valor predeterminado es 5 segundos.

Transmit Delay(0-3600) (Demora de transmisión [0-3600]): Tiempo estimado (segundos) necesario para enviar un paquete de actualización de estado de enlace en la interfaz. Los LSA del paquete de actualización incrementan su antigüedad por esta cantidad antes de la transmisión. El valor predeterminado es 1 segundo.

Dead Interval (0-2147483647) (Intervalo de caducidad [1-2147483647]): El tiempo (segundos) durante el cual no se han detectado paquetes de saludo del enrutador y en el que el enrutador caduca. El valor debe ser un múltiplo del valor de **Hello Interval** (Intervalo de saludo). Todos los enrutadores conectados a una red común deben tener un valor especificado para este parámetro. El valor predeterminado es 60 segundos.

Virtual Interface State (Estado de la interfaz virtual): Indica el estado de la interfaz virtual.

Authentication Mode (Modo de autenticación): El tipo de autenticación de la interfaz, contraseña o MD5, que se utiliza para autenticar los mensajes del estado de enlace de OSPF.

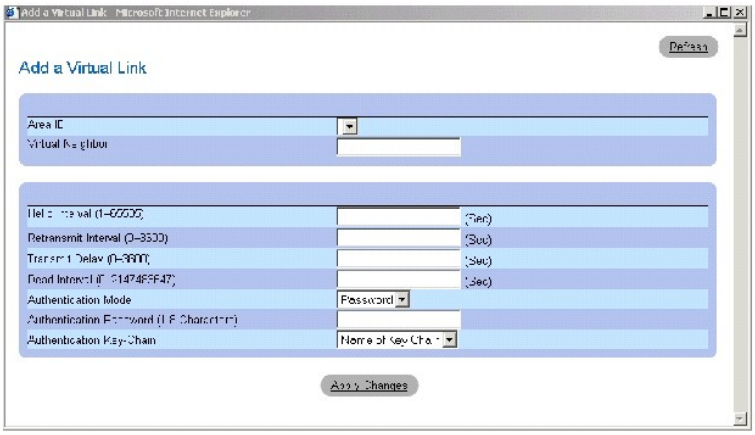
Authentication Password (1-8 Characters) (Contraseña de autenticación [1-8 caracteres]): La contraseña (ocho caracteres o menos) que se utiliza para autenticar los mensajes del estado de enlace de OSPF.

Authentication Key-Chain (Cadena de claves de autenticación): La cadena de claves MD5 que se utiliza para autenticar los mensajes del estado de enlace de OSPF.

Adición de un enlace virtual

1. Abra la página **Virtual Links** (Enlaces virtuales).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add a Virtual Link** (Agregar un enlace virtual).

Ilustración 8-13. Página Add a Virtual Link (Agregar un enlace virtual)



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

Se agrega el nuevo enlace virtual de OSPF.

Modificación de enlaces virtuales

1. Abra la página **Virtual Links** (Enlaces virtuales).
2. Seleccione un ID de área en el menú descendente **Area ID** (ID de área).

Se visualizan los parámetros del campo.

3. Modifique los campos que desee.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del enlace virtual de OSPF se modifican y se guardan en el dispositivo.

Supresión de un enlace virtual de OSPF

1. Abra la página **Virtual Links** (Enlaces virtuales).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **Virtual Links Table** (Tabla de enlaces virtuales).
3. Seleccione un enlace virtual.

Se visualizan los parámetros del campo de la entrada de la tabla.

4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el enlace virtual y el dispositivo se actualiza.

Visualización de los enlaces virtuales de OSPF mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir las áreas OSPF.

Tabla 8-10. Comandos de la CLI para el enlace virtual de OSPF

Comando de la CLI	Descripción
`show ip ospf virtual-links [area id_área] [router id_enrutador]`	Muestra los parámetros y el estado actual de los enlaces virtuales de OSPF.
`router ospf area id_área enlace_virtual id_enrutador`	Agrega un enlace virtual.

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

```
Console (config)# show ip ospf virtual-links

Virtual Link to router 192.168.101.2 is up

Virtual link has simple password authentication

Transit area 0.0.0.1

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Adjacency State FULL

Console (config)#router ospf area 176.16.1.0 virtual-link 176.16.8.7

Console (config)#router ospf area 176.16.1.0 virtual-link 176.16.8.7
```

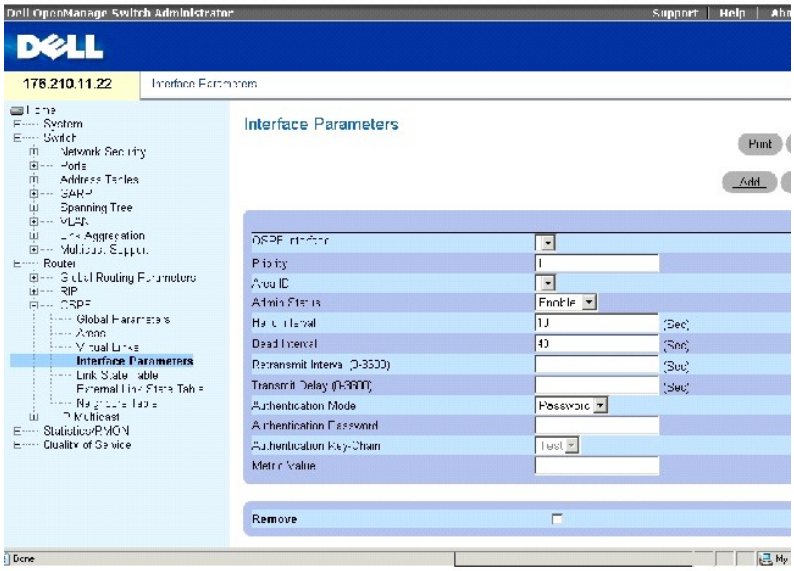
Configuración de los parámetros de la interfaz OSPF

Después de definir las áreas y los parámetros globales de OSPF, puede configurar OSPF en cada interfaz.

La creación automática permite que OSPF se configure automáticamente en cada interfaz después de definir un área. Las interfaces OSPF también pueden ser definidas por el usuario. La tabla de interfaces OSPF habilita el encaminamiento IP utilizando información específica de OSPF.

Para visualizar la página **Interface Parameters** (Parámetros de la interfaz), haga clic en **Router**→ **OSPF**→ **Interface Parameters** (Enrutador→ OSPF→ Parámetros de la interfaz) en la vista de árbol.

Ilustración 8-14. Página Interface Parameters (Parámetros de la interfaz)



OSPF Interface (Interfaz OSPF): La dirección IP de la interfaz OSPF.

Priority (Prioridad): La prioridad de la interfaz. El valor 0 indica que el dispositivo no se puede definir como el dispositivo designado en la red actual. Si más de un dispositivo tiene la misma prioridad, se utiliza el ID del enrutador. El intervalo de valores posibles es 0-255. El valor predeterminado es 1.

Area ID (ID de área): El ID de área de la interfaz OSPF.

Admin Status (Admin. estado): Habilita o inhabilita el proceso OSPF.

Hello Interval (Intervalo de saludo): El tiempo (segundos) entre los paquetes de saludo. Todos los dispositivos conectados a una red común deben tener el mismo intervalo de saludo. El intervalo posible de valores del campo es 1-65535. El valor predeterminado es 10 segundos.

Dead Interval (Intervalo de caducidad): El intervalo de tiempo (en segundos) antes de que el enrutador caduque tras no haber detectado los paquetes de saludo. El valor debe ser un múltiplo del valor de **Hello Interval** (Intervalo de saludo). Todos los enrutadores conectados a una red común deben tener un valor especificado para este parámetro. El intervalo posible de valores del campo es **1-2147483647.** El valor predeterminado es cuatro veces el valor de **Hello Interval** (Intervalo de saludo).

Retransmit Interval (0-3600) (Intervalo de retransmisión [1-3600]): El intervalo de tiempo (en segundos) entre las retransmisiones de anuncio de estado de enlaces (LSA) para adyacencias pertenecientes a la interfaz. El valor debe ser superior a la demora de ida y vuelta prevista entre dos enrutadores de la red conectada. El valor predeterminado es 5 segundos.

Transmit Delay (0-3600) (Demora de transmisión [1-3600]): La cantidad de tiempo estimada (en segundos) necesaria para enviar un paquete de actualización de estado de enlace en la interfaz. Los LSA del paquete de actualización incrementan su antigüedad por esta cantidad antes de la transmisión. El valor predeterminado es 1 segundo.

Authentication Mode (Modo de autenticación): El tipo de autenticación de la interfaz, contraseña o MD5, que se utiliza para autenticar los mensajes del estado de enlace de OSPF.

Authentication Password (Contraseña de autenticación): Contraseña que se utiliza para autenticar los mensajes del estado de enlace de OSPF. La longitud máxima de la contraseña es de ocho caracteres.

Authentication Key-Chain (Cadena de claves de autenticación): La cadena de claves MD5 que se utiliza para autenticar los mensajes del estado de enlace de OSPF.

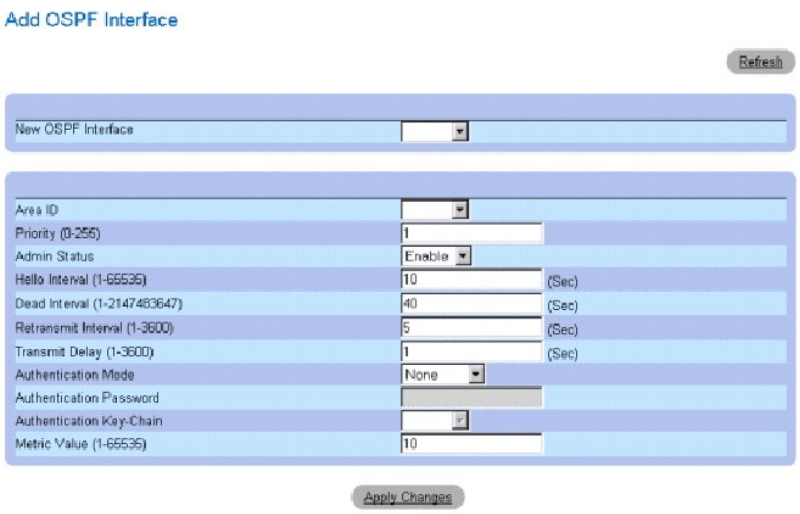
Metric Value (Valor métrico [1-65535]): La métrica de este tipo de servicio en la interfaz. El intervalo posible de valores del campo es **1-65535.**

Remove (Eliminar): Si se selecciona esta opción, se elimina una interfaz OSPF.

Adición de una interfaz OSPF

1. Abra la página **Interface Parameters** (Parámetros de la interfaz).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add OSPF Interface** (Agregar una interfaz OSPF).

Ilustración 8-15. Add OSPF Interface (Agregar una interfaz OSPF)



3. Complete los campos de esta página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva interfaz OSPF se agrega y el dispositivo se actualiza.

Modificación de los parámetros de OSPF

1. Abra la página **Interface Parameters** (Parámetros de la interfaz).
2. Seleccione una interfaz OSPF para visualizar los parámetros de campo de la entrada de la tabla.
3. Modifique los parámetros que desee.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de la interfaz OSPF se modifican y se guardan en el dispositivo.

Eliminación de una interfaz OSPF

1. Abra la página **Interface Parameters** (Parámetros de la interfaz).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **OSPF Interface Table** (Tabla de interfaz OSPF).
3. Seleccione una interfaz OSPF.

4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La interfaz OSPF se elimina.

Definición de interfaces OSPF

La siguiente tabla contiene los comandos de la CLI para definir las interfaces OSPF.

Tabla 8-11. Comandos de la CLI para la interfaz OSPF

Comando de la CLI	Descripción
`ospf`	Crea un proceso de encaminamiento OSPF en una interfaz.
`ospf area` *`id_área`*	Define el ID de área de una interfaz.
`ospf enable`	Activa OSPF en una interfaz.
`ospf priority number- value`	Establece la prioridad del enrutador, que se utiliza al elegir el enrutador designado de la red.
`ospf hello-interval seconds`	Especifica el intervalo de tiempo entre los paquetes de saludo que el software envía en una interfaz.
`ospf dead-interval seconds`	Establece el intervalo de tiempo durante el cual los paquetes de saludo no se deben enviar antes de que los elementos adyacentes declaren que el enrutador está inactivo.
`ospf retransmit-interval seconds`	Especifica el intervalo de tiempo entre las retransmisiones de anuncio de estado de enlaces (LSA) para adyacencias pertenecientes a la interfaz.
`ospf transmit-delay seconds`	Establece el tiempo estimado necesario para enviar un paquete de actualización de estado de enlace en una interfaz.
`ospf authentication {text text | md5 name-of-chain}`	Habilita la autenticación para los paquetes de OSPF y especifica el tipo de autenticación.
`clear ip ospf process [`*`interfaz`*`]`	Borra la redistribución basándose en el encaminamiento OSPF.
`show ip ospf interface [`*`interfaz`*`]`	Muestra información de la interfaz relacionada con OSPF.

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

```
Console (config)# interface ip 1.100.100.100

Console (config-ip)# ospf

Console (config-ip)# ospf area 192.168.2.1

Console (config-ip)# ospf enable

Console (config-ip)# ospf priority 100
```

```
Console (config-ip)# ospf hello-interval 100

Console (config-ip)# ospf dead-interval 100

Console (config-ip)# ospf retransmit-interval 60

Console (config-if)# ospf retransmit-delay 60

Console (config-ip)# ospf authentication text abab

Console (config-ip)# ospf authentication md5 mychain

Console (config-ip)# exit

Console (config)# exit

Console# clear ip ospf process 192.168.3.1

Console# exit

Console# show ip ospf interface 192.168.1.1

IP interface 192.168.1.1/16 is up, OSPF is enabled

Area 0.0.0.0, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10

Interface has simple password authentication

Transmit Delay is 1 sec, State OTHER, Priority 1

Designated Router id 192.168.1.11, Interface address 192.168.1.11

Backup Designated router id 192.168.1.28, Interface addr 192.168.1.28

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

Neighbor Count is 8, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.1.28 (Backup Designated Router)
```

Visualización de la tabla de estado de enlace

La página **OSPF Link State Table** (Tabla de estado de enlace OSPF) contiene información de anuncio de estado de enlace para áreas a las que el dispositivo está conectado. Haga clic en **Router**→ **OSPF**→ **Link State Table** (Enrutador→ OSPF→ Tabla de estado de enlace) en la vista de árbol.

Ilustración 8-16. OSPF Link State Table (Tabla de estado de enlace OSPF)

Area ID (ID de área): El ID de área.

Link Type (Tipo de enlace): Indica el tipo de enlace del área.

Link ID (ID de enlace): La pieza de dominio de encaminamiento descrito por el anuncio. Se trata de un ID de enrutador o de una dirección IP.

Router ID (ID de enrutador): El enrutador de origen en el sistema autónomo.

Sequence Number (Número de secuencia): El número de secuencia del enlace. El número de secuencia detecta tanto anuncios de estado de enlace antiguos como duplicados. Cuanto mayor sea el número de secuencia, más reciente será el anuncio.

Age (Antigüedad): Indica el anuncio del estado de la antigüedad del enlace en segundos.

Checksum (Suma de comprobación): La suma de comprobación del contenido completo del anuncio, sin incluir el valor de **Age** (Antigüedad).

Visualización de la tabla de estado del enlace de OSPF mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de estado de enlace de OSPF.

Tabla 8-12. Comandos de la CLI para el estado de enlace de OSPF

Comando de la CLI	Descripción
`show ip OSPF [id_área] database`	Muestra listas de información relacionadas con la base de datos OSPF de un enrutador específico.

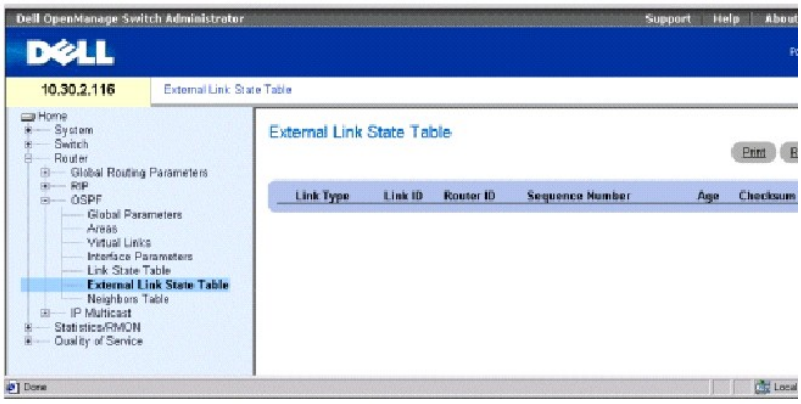
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console> show ip ospf database

OSPF Router with ID 200.1.1.11

Router Link States(Area 0)

Link ID ADV Router Age Seq# Checksum Link count

200.1.1.8 200.1.1.8 1381 0x8000010D 0xEF60 2

200.1.1.11 200.1.1.11 1460 0x800002FE 0xEB3D 4

200.1.1.12 200.1.1.12 2027 0x80000090 0x875D 3

200.1.1.27 200.1.1.27 1323 0x800001D6 0x12CC 3



Net Link States(Area 0)

Link ID ADV Router Age Seq# Checksum

140.1.1.27 200.1.1.27 1323 0x8000005B 0xA8EE

141.1.1.11 200.1.1.11 1461 0x8000005B 0x7AC
```

Visualización de la tabla de estado de enlace externo

La tabla de estado de enlace externo contiene información de los anuncios de estado de enlace externo. La información de la tabla de estado de enlace externo se obtiene de fuentes distintas a las rutas OSPF. Para visualizar la página de la tabla de estado de enlace externo, haga clic en **Router**→ **OSPF**→ **External Link State Table** (Enrutador→ OSPF→ Tabla de estado de enlace externo) en la vista de árbol.

Ilustración 8-17. External Link State Table (Tabla de estado del enlace externo)



Link Type (Tipo de enlace): El tipo de enlace externo. Cada anuncio de estado de enlace tiene un formato específico. Este campo es siempre un enlace externo.

Link ID (ID de enlace): La pieza de dominio de encaminamiento descrito por el anuncio. Se trata de un ID de enrutador o de una dirección IP.

Router ID (ID de enrutador): El enrutador de origen en el sistema autónomo.

Sequence Number (Número de secuencia): El número de secuencia del enlace externo. El número de secuencia detecta tanto anuncios de estado de enlace antiguos como duplicados. Cuanto mayor sea el número de secuencia, más reciente será el anuncio.

Age (Antigüedad): Indica el anuncio del estado de la antigüedad del enlace externo en segundos.

Checksum (Suma de comprobación): La suma de comprobación del contenido completo del anuncio, sin incluir el valor de **Age** (Antigüedad).

Visualización de la tabla de ruta externa OSPF mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de ruta externa OSPF.

Tabla 8-13. Comandos de la CLI para la tabla de ruta externa OSPF

Comando de la CLI	Descripción
show ip OSPF [*id_área*] database [external] [*id_estado_enlace*]	Muestra información relacionada con la base de datos OSPF de un enrutador específico.

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

```
Console> show ip ospf database
```

Visualización de la tabla de elementos adyacentes de OSPF

En la tabla de elementos adyacentes de OSPF se describen todos los elementos adyacentes de la localidad del enrutador del sujeto. Para abrir la página

Neighbor Table (Tabla de elementos adyacentes), haga clic en **Router**→ **OSPF**→ **Neighbors Table** (Enrutador→ OSPF→ Tabla de elementos adyacentes) en la vista de árbol.

Ilustración 8-18. Neighbors Table (Tabla de elementos adyacentes)

IP Address (Dirección IP): La dirección IP que utiliza este elemento adyacente en su dirección IP de origen.

Network Mask (Máscara de red): La máscara de red de la interfaz adyacente.

Neighbor Selection (Selección de elementos adyacentes): Especifica qué información adyacente del dispositivo hay que mostrar.

Neighbor's Address (Dirección del elemento adyacente): La dirección IP del elemento adyacente.

Priority (Prioridad): La prioridad del elemento adyacente.

Router ID (ID de enrutador): El ID de enrutador del elemento adyacente.

State (Estado): El estado actual del elemento adyacente.

Visualización de la lista de elementos adyacentes

1. Abra la página **OSPF Neighbors Table** (Tabla de elementos adyacentes de OSPF).
2. En la columna **Neighbor Selection** (Selección de elementos adyacentes), haga clic en el botón de opción del elemento adyacente cuya información desea ver.
3. Haga clic en **Show Neighbor's Info** (Mostrar información del elemento adyacente).

La información del elemento adyacente se muestra en la parte inferior de la página.

Visualización de la tabla de todos los elementos adyacentes

1. Abra la página **Neighbors Table** (Tabla de elementos adyacentes).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **All Neighbors Table** (Tabla de todos los elementos adyacentes).

Visualización de la información sobre el elemento adyacente de OSPF mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de información de elementos adyacentes de OSPF.

Tabla 8-14. Comandos de la CLI para los elementos adyacentes de OSPF

Comando de la CLI	Descripción
`show ip ospf neighbor [`*`interfaz`*`]`	Muestra información del elemento adyacente de OSPF por interfaz.

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

```
Console> show ip ospf neighbor

ID            Pri  State         Address       IP interface

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

192.168.1.11  1    FULL          /DR           192.168.1.11 192.168.1.1

192.168.1.12  2    FULL          /DROTHER      192.168.1.12 192.168.1.1

192.168.2.11  1    FULL          /DR           192.16 8.2.11 192.168.2.1

192.168.2.12  2    FULL          /DROTHER      192.168.2.12 192.168.2.1

Console> show ip ospf neighbor 192.168.1.1

Neighbor 192.168.1.11, Address 192.168.1.11

In the area 0.0.0.0

Neighbor priority is 1, State is FULL

Options 2

Neighbor 192.168.1.12, Address 192.168.1.12

In the area 0.0.0.0

Neighbor priority is 2, State is FULL

Options 2
```

Configuración del encaminamiento de multidifusión IP

El encaminamiento de multidifusión maximiza los recursos de la red. Un sistema principal envía datos a un grupo de sistemas principales (en vez de a un único sistema principal) dentro de la red IP, mediante la dirección del grupo de multidifusión IP. El encaminamiento de multidifusión IP se implementa en el conmutador PowerConnect 6024/6024F mediante los siguientes protocolos:

- **Internet Group Member Protocol** (IGMP) (Protocolo de miembros del grupo de Internet [IGMP]): Proporciona un método para descubrir qué clientes están interesados en recibir transmisiones específicas.
- **Distance Vector Multicast Routing Protocol** (DVMRP) (Protocolo de encaminamiento de multidifusión de vectores de distancia [DVMRP]): Permite que los enrutadores establezcan un árbol de transmisión y copien los paquetes a lo largo del árbol de encaminamiento de la transmisión.

Definición de los parámetros globales de IPM

El encaminamiento de multidifusión IP se habilita en la página **IPM Global Parameters** (Parámetros globales de IPM). Para visualizar la página **IPM Global Parameters** (Parámetros globales de IPM), haga clic en **Router**→ **IP Multicast**→ **Global Parameters** (Enrutador→ Multidifusión IP→ Parámetros globales) en la vista de árbol.

Ilustración 8-19. IPM Global Parameters (Parámetros globales de IPM)

IP Multicast Status (Estado de multidifusión IP): Habilita o inhabilita el encaminamiento IPM en el dispositivo.

Habilitación del encaminamiento IPM en el dispositivo

1. Abra la página **IPM Global Parameters** (Parámetros globales de IPM).
2. Seleccione **Enable** (Habilitar) en el campo **IPM Multicast Status** (Estado de multidifusión IPM).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El encaminamiento de multidifusión IP se habilita en el dispositivo.

Habilitación del encaminamiento de multidifusión mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para habilitar el encaminamiento de multidifusión.

Tabla 8-15. Comandos de la CLI para el encaminamiento de multidifusión

Comando de la CLI	Descripción

`ip multicast- routing`	Habilita el encaminamiento de multidifusión IP.

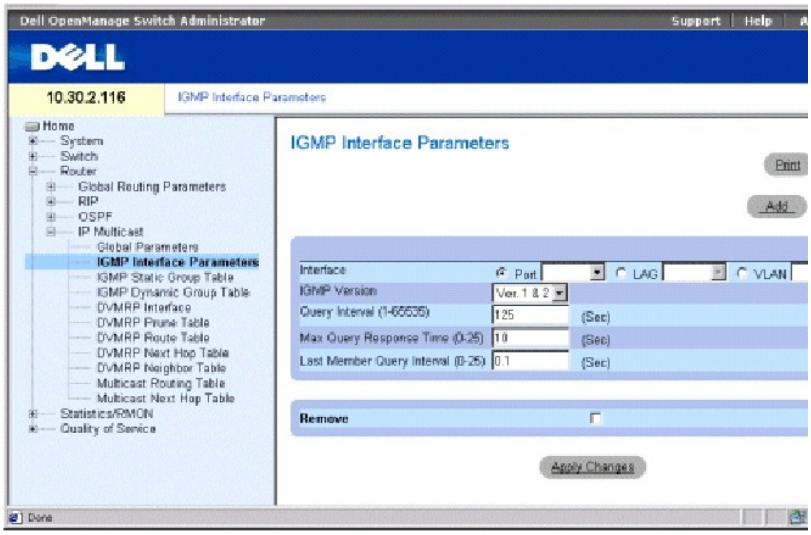
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# ip multicast-routing
```

Definición de parámetros de la interfaz de IGMP

Internet Group Membership Protocol (IGMP) (Protocolo de pertenencia a grupos de Internet [IGMP]): Establece los miembros del sistema principal en un grupo de multidifusión. IGMP permite que los sistemas principales notifiquen a los enrutadores que pueden recibir paquetes de multidifusión dirigidos a grupos de multidifusión específicos. Para abrir la página **IGMP Interface Parameters** (Parámetros de la interfaz IGMP), haga clic en **Router→ IP Multicast→ IGMP Interface Parameters** (Enrutador→ Multidifusión IP→ Parámetros de la interfaz IGMP) en la vista de árbol.

Ilustración 8-20. IGMP Interface Parameters (Parámetros de la interfaz de IGMP)



Interface (Interfaz): Contiene una lista de direcciones IP de interfaces para las que se ha habilitado IGMP.

IGMP Version (Versión de IGMP): La versión de software actual de IGMP. El valor predeterminado es **Ver. (Versión) 1 y 2**.

Query Interval (1-65535) (Intervalo de consulta [1-65535]): Cantidad de tiempo en segundos durante el que se transmiten los mensajes de consulta. Puede ajustar la cantidad de mensajes de IGMP que se envían en subredes ajustando el valor del intervalo de consulta. Cuanto mayor sea el valor, con menos frecuencia se enviarán mensajes de IGMP. El valor predeterminado es 125 segundos.

Max Query Response Time (0-25) (Tiempo máximo de respuesta de consulta [0-25]): El tiempo de respuesta máximo para anunciar consultas de IGMP. El tiempo de respuesta ajusta la cantidad de tráfico por subred. Si se varía el tiempo de respuesta se influye en la transmisión en bloques del tráfico de la red. Cuanto mayor sea el valor, más tiempo pasará entre las respuestas de los sistemas principales. El valor predeterminado es 10 segundos.

Last Member Query Interval (0-25) (Intervalo de consulta de último miembro): Modifica la latencia de cese de la red. Un valor reducido reduce la cantidad de tiempo necesaria para detectar la pérdida del último miembro del grupo. El valor predeterminado es 0.1.

Remove (Eliminar): Si se selecciona esta opción, se elimina la interfaz IGMP.

Adición de una interfaz IGMP

1. Abra la página **IGMP Interface Parameters** (Parámetros de la interfaz IGMP).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add an IGMP Interface** (Agregar una interfaz IGMP).
3. Seleccione una interfaz en el menú descendente **New Interface** (Nueva interfaz).
4. Complete los campos de esta página.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva interfaz IGMP se agrega al dispositivo.

Modificación de una interfaz IGMP

1. Abra la página **IGMP Interface Parameters** (Parámetros de la interfaz IGMP).
2. Seleccione la interfaz que desea modificar.
3. Modifique los campos que desee.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de la interfaz IGMP se modifican y se guardan en el dispositivo.

Supresión de una interfaz IGMP

1. Abra la página **IGMP Interface Parameters** (Parámetros de la interfaz IGMP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **IGMP Interface Table** (Tabla de interfaz IGMP).
3. Seleccione una interfaz IGMP y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La interfaz IGMP se elimina.

Configuración de los parámetros de la interfaz IGMP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar los parámetros de la interfaz IGMP.

Tabla 8-16. Comandos de la CLI para los parámetros de la interfaz IGMP

Comando de la CLI	Descripción
`ip igmp`	Crea IGMP en una interfaz.
`ip igmp query-interval` *segundos*	Configura la frecuencia con la que el software envía mensajes de consulta al sistema principal IGMP.
`ip igmp query-max-response- time` *segundos* [*décimas_de_segundo*]	Configura el tiempo máximo de respuesta que se anuncia en las consultas de IGMP.
`ip igmp last-member-query- interval` *segundos* [*décimas_de_segundos*]	Configura la frecuencia con la que el enrutador envía mensajes de consulta al sistema principal específico del grupo IGMP.
`show ip igmp interface [ethernet` *número_interfaz* `| vlan` *id_vlan* `|` *número_canal_puerto*`]`	Muestra información relacionada con IGMP sobre una interfaz.

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

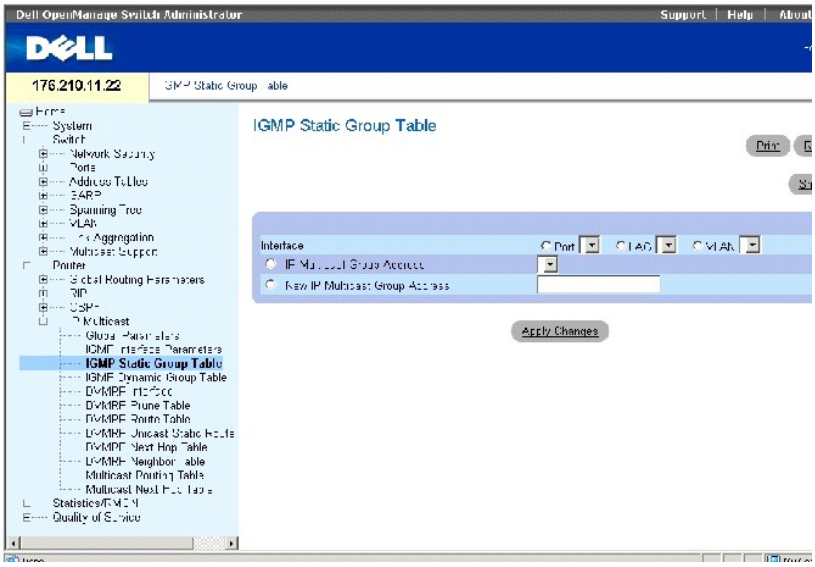
```
Console (config)# interface ethernet g1

Console (config-if)# ip igmp

Console (config-if)# ip igmp query-interval 60

Console (config-if)# ip igmp query-max-response-time 20

Console (config-if)# ip igmp last-member-query-interval 200

Console (config-if)# exit

Console (config)# exit

Console# disable

Console> show ip igmp interface

Interface Version Query Last Max Querier Interval Member response router

[sec] [mSec] [Sec]

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

eth g1 2 60 1000 10 198.92.37.33

eth g2 60 1000 10 198.92.36.131
```

Definición de grupos de interfaces estáticas IGMP

IGMP Static Group Table (Tabla de grupos estáticos IGMP): Habilita la definición estática de grupos IGMP en interfaces específicas.

Para abrir la página **IGMP Static Group Table (Tabla de grupos estáticos IGMP)**, haga clic en **Router→ IP Multicast→ IGMP Static Group Table** (Enrutador→ Multidifusión IP→ Tabla de grupos estáticos IGMP) en la vista de árbol.

Ilustración 8-21. IGMP Static Group Table (Tabla de grupos estáticos IGMP)



Interface (Interfaz): Especifica el puerto, VLAN o LAG al que se asigna el grupo de multidifusión específico.

IP Multicast Group Address (Dirección del grupo de multidifusión IP): La dirección del grupo de multidifusión IP que se asigna a una interfaz.

New IP Multicast Group Address (Nueva dirección del grupo de multidifusión IP): La nueva dirección del grupo de multidifusión IP que se asigna a una interfaz.

Asignación de una interfaz a un grupo de multidifusión

1. Abra la **IGMP Static Group Table** (Tabla de grupos estáticos IGMP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).
3. Seleccione una dirección IP en el campo **Multicast Group Address** (Dirección del grupo de multidifusión) o defina una nueva dirección del grupo de multidifusión en el campo **New Multicast Group Address** (Nueva dirección del grupo de multidifusión).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Visualización de la tabla de grupos de interfaces estáticas

1. Abra **IGMP Static Group Table** (Tabla de grupos estáticos IGMP).
2. Haga clic en **Show All** (Mostrar todo) para visualizar **Static Interface Grouping Table** (Tabla de grupos de interfaces estáticas).

La página contiene los siguientes campos:

- **Interface** (Interfaz): La dirección del grupo de multidifusión IP de la que es miembro el puerto.
- **IP Multicast Group** (Grupo de multidifusión IP): El grupo de multidifusión IP del que es miembro esta interfaz.
- **Group Up Time** (Tiempo de actividad del grupo): Indica en tics la cantidad de tiempo que ha pasado desde que se creó la entrada. El formato de la hora es hora/minuto/segundo.
- **Last Reporter** (Último informador): El último miembro que se une al grupo de multidifusión IP. Si no se especifica ningún miembro en el grupo de multidifusión IP, el valor es 0.0.0.0.
- **Remove** (Eliminar): Si se selecciona esta opción, se elimina una interfaz IGMP.

Configuración de los grupos de interfaces estáticas mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI de los grupos de interfaces estáticas.

Tabla 8-17. Comandos de la CLI para el grupo de interfaces estáticas

Comando de la CLI	Descripción
`ip igmp static- group` *dirección_grupo*	Configura el enrutador para que sea un miembro conectado estáticamente del grupo especificado en la interfaz.

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

```
Console (config)# interface ethernet g5
```

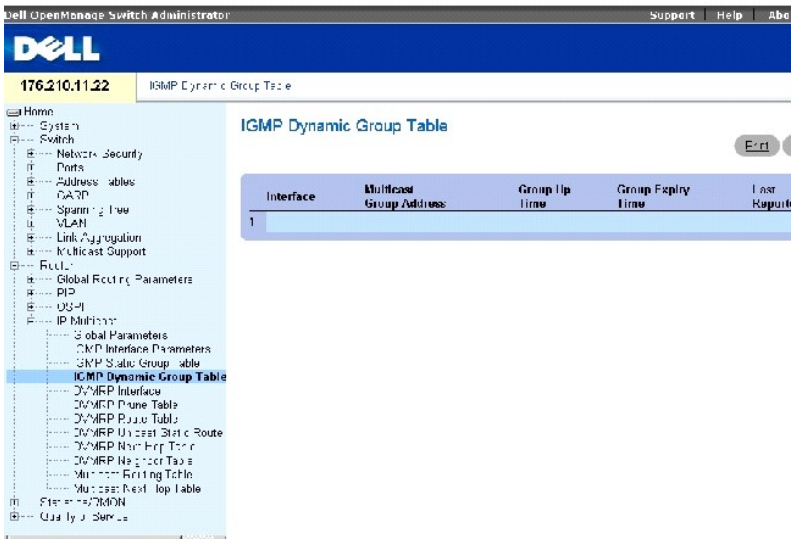
```
Console (config-if)# ip igmp static-group 192.168.4.1
```

Visualización de la tabla de grupos dinámicos IGMP

La página **IGMP Dynamic Group Table** (Tabla de grupos dinámicos IGMP) muestra información referente a cada uno de los grupos de multidifusión IP cuyos miembros se han asignado dinámicamente a una interfaz en un puerto físico.

Para abrir la página **Static Interface Grouping** (Grupos de interfaces estáticas), haga clic en **Router**→ **IP Multicast**→ **IGMP Static Group Table** (Enrutador→ Multidifusión IP→ Tabla de grupos estáticos IGMP) en la vista de árbol.

Ilustración 8-22. IGMP Dynamic Group Table (Tabla de grupos dinámicos IGMP)



Interface (Interfaz): Especifica una interfaz que pertenece al grupo de multidifusión IP.

Multicast Group Address (Dirección del grupo de multidifusión): La dirección IP del grupo de multidifusión de IGMP.

Group Up Time (Tiempo de actividad del grupo): Indica en tics la cantidad de tiempo que ha pasado desde que se creó la entrada. El formato de la hora es hora/minuto/segundo.

Group Expiry Time (Tiempo de caducidad del grupo): Cantidad de tiempo antes de que la entrada dinámica caduque. El formato de la hora es hora/minuto/segundo.

Last Reporter (Último informador): El último miembro que se une al grupo de multidifusión IP. Si no se especifica ningún miembro en el grupo de multidifusión IP, el valor es 0.0.0.0.

Visualización de grupos IGMP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver los grupos IGMP.

Tabla 8-18. Comandos de la CLI para los grupos IGMP

Comando de la CLI	Descripción
show ip igmp groups [*dirección_ip grupo*] [ethernet interface- *número* | *vlan id_vlan* | *número_canal_puerto*]	Muestra los grupos de multidifusión con receptores que están directamente conectados al enrutador y que se obtuvieron mediante el Protocolo de pertenencia a grupos de Internet (IGMP).

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

```
Console> show ip igmp groups

Group Address Interface Uptime Expires Last Reporter

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

239.255.255.254 eth g1 1w0d 00:02:19 172.21.200.159

224.0.1.40 eth g3 1w0d 00:02:15 172.21.200.1

224.0.1.40 eth g3 1w0d 00:02:1 static

224.0.1.1 eth g1 1w0d 00:02:11 172.21.200.11

224.9.9.2 eth g1 1w0d 00:02:17 172.21.200.155

232.1.1.1 eth g1 5d21h 00:02:11 172.21.200.206
```

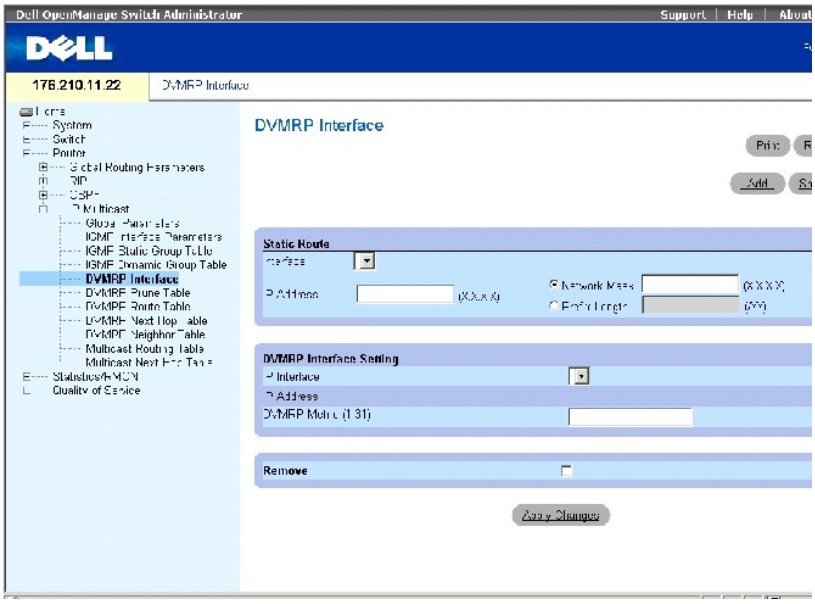
Configuración de interfaces DVMRP

El protocolo de encaminamiento de multidifusión de vectores de distancia (DVMRP) utiliza el algoritmo de multidifusión de reenvío de ruta inversa (RPF) para crear árboles de entrega de multidifusión basados en origen. DVMRP es un protocolo de comprobación RPF que se basa en la información de encaminamiento DVMRP. La información de encaminamiento se recopila durante el encaminamiento del intercambio.

La página **DVMRP Interface** (Interfaz DVMRP) contiene información sobre las configuraciones de la interfaz DVMRP.

Para abrir la página **DVMRP Interface** (Interfaz DVMRP), haga clic en **Router**→ **IP Multicast**→ **DVMRP Interface** (Enrutador→ Multidifusión IP→ Interfaz DVMRP) en la vista de árbol.

Ilustración 8-23. DVMRP Interface (Interfaz DVMRP)



La página **DVMRP Interface** (Interfaz DVMRP) contiene los siguientes campos divididos en dos áreas:

STATIC ROUTE (RUTA ESTÁTICA)

Interface (Interfaz): Especifica el número de la interfaz en la que está habilitado DVMRP.

IP Address (X.X.X.X) (Dirección IP [X.X.X.X]): Especifica la dirección IP de origen del puerto en que está habilitado DVMRP.

Network Mask (X.X.X.X) (Máscara de red [X.X.X.X]): Especifica la máscara de subred de la dirección IP de origen.

Prefix Length /XX) (Longitud del prefijo [/XX]): Especifica el número de bits que componen el prefijo de la IP de origen o la máscara de red de la dirección IP de origen.

DVMRP INTERFACE SETTING (CONFIGURACIÓN DE LA INTERFAZ DVMRP)

IP Interface (Interfaz IP): Especifica el número de la interfaz en el que está habilitado DVMRP.

IP Address (Dirección IP): Indica la dirección IP de origen del puerto en el que está habilitado DVMRP.

DVMRP Metric (1-31) (Métrica CVMRP [1-31]): Indica la distancia que se utiliza para calcular el vector de distancia. La métrica DVMRP es la distancia de interfaz que existe entre el enrutador que origina el informe y la red de origen. El valor predeterminado es 1.

Remove (Eliminar): Si se selecciona esta opción, se elimina una interfaz DVMRP.

Adición de una nueva interfaz DVMRP

1. Abra la página **DVMRP Interface** (Interfaz DVMRP).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add a DVMRP Interface** (Agregar una interfaz DVMRP).
3. Defina el número de interfaz y la métrica de DVMRP.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se agrega la interfaz DVMRP a la **IP Interface List** (Lista de interfaces IP) y el dispositivo se actualiza.

Modificación de una interfaz DVMRP

1. Abra la página **DVMRP Interface** (Interfaz DVMRP).
2. Seleccione una interfaz en la lista **IP Interface** (Interfaces IP).
3. Modifique los campos que desee.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se agrega la interfaz DVMRP seleccionada a la **DVMRP Interface List** (Lista de interfaces DVMRP) y el dispositivo se actualiza.

Supresión de una interfaz DVMRP

1. Abra la página **DVMRP Interface** (Interfaces DVMRP).
2. Seleccione una interfaz en la lista **IP Interface** (Interfaces IP).
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se suprime la interfaz DVMRP modificada de **IP Interface List** (Lista de interfaces IP) y se actualiza el dispositivo.

Configuración de las interfaces DVMRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar y ver las interfaces DVMRP.

Tabla 8-19. Comandos de la CLI para DVMRP

Comando de la CLI	Descripción
`ip dvmrp`	Habilita DVRMP en una interfaz.
`no ip dvmrp`	Inhabilita DVRMP en una interfaz.
`ip dvmrp metric` *`métrica`*	Configura la métrica de interfaz para DVMRP. La métrica puede ser 1-31.
`no ip dvmrp metric`	Habilita la métrica de interfaz para DVMRP.
`show ip dvmrp interface [ethernet` *`número_interfaz`* `| vlan` *`id_vlan`* `| port-channel` *`número`*`]`	Muestra la tabla de la interfaz.

A continuación se muestra un ejemplo del comando de la CLI:

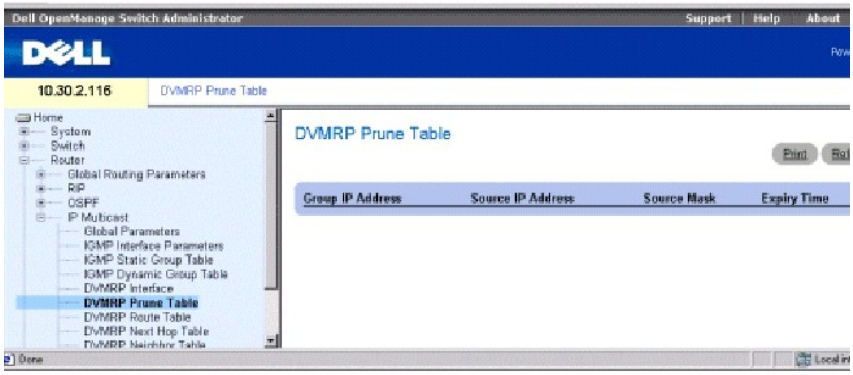
```
Console (config-if)# interface ethernet g5
```

```
Console (config-if)# ip dvmrp

Console (config-if)# ip dvmrp metric 15

Console (config-if)# exit

Console (config)# exit

Console> show ip dvmrp interface

Multicast routing enabled.

Multicast routing protocol is DVMRP.

Interface IP address Metric RCV Bad RCV Bad Sent Packets Routes Routes

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

eth g1 172.16.1.1 10 0 12
```

Tabla de eliminación DVMRP

En la página **DVMRP Prune Table** (Tabla de eliminación DVMRP) se lista el estado de eliminación en dirección ascendente del enrutador. Para abrir la página **DVMRP Prune Table** (Tabla de eliminación DVMRP), haga clic en **Router**→ **IP Multicast**→ **DVMRP Prune Table** (Enrutador→ Multidifusión IP→ Tabla de eliminación DVMRP) en la vista de árbol.

Ilustración 8-24. DVMRP Prune Table (Tabla de eliminación de DVMRP)



Group IP Address (Dirección IP de grupo): Dirección IP del grupo de eliminación.

Source IP Address (Dirección IP de origen): La dirección IP de origen que debe eliminarse.

Source Mask (Máscara de origen): Máscara de la IP de origen que se ha eliminado.

Expiry Time (Tiempo de caducidad): El tiempo restante antes de que se elimine el flujo en dirección ascendente.

Visualización de la tabla de supresión de DVMRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de supresión.

Tabla 8-20. Comandos de la CLI para la tabla DVRMP

Comando de la CLI	Descripción
`show ip dvmrp prune [group` *`dirección_grupo`*`] [`*`dirección_origen`*`]`	Muestra la tabla.

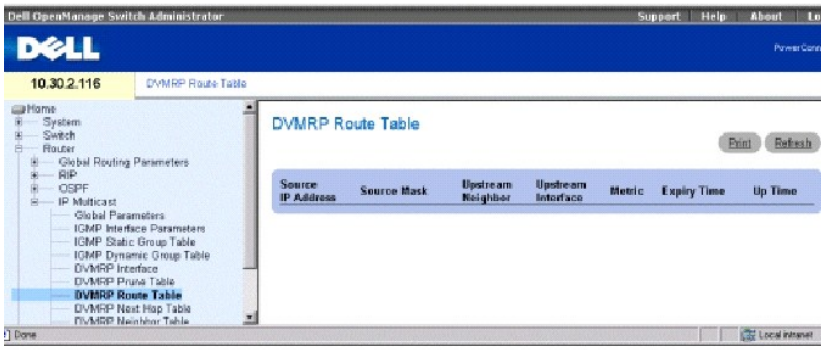
A continuación se muestra un ejemplo del comando de la CLI:

```
Console> show ip dvmrp prune

Group Source Expiry Time

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

224.192.78.88 171.68.0.0/16 00:02:52

224.192.78.89 171.68.0.0/16 00:08:52
```

Tabla de ruta DVMRP

La página **DVMRP Route Table** (Tabla de ruta DVMRP) contiene información sobre las rutas obtenidas a través del intercambio de enrutador DVMRP. Para abrir la página **DVMRP Route Table** (Tabla de ruta DVMRP), haga clic en **Router**→ **IP Multicast**→ **DVMRP Route Table** (Enrutador→ Multidifusión IP→ Tabla de ruta DVMRP) en la vista de árbol.

Ilustración 8-25. DVMRP Route Table (Tabla de ruta DVMRP)



Source IP Address (Dirección IP de origen): La dirección IP del origen de la información de encaminamiento de multidifusión.

Source Mask (Máscara de origen): La máscara de red de la dirección IP de origen.

Upstream Neighbor (Elemento adyacente en dirección ascendente): Dirección IP del elemento adyacente RPF en dirección ascendente, del cual proceden los datagramas de IP de origen que se reciben.

Upstream Interface (Interfaz en dirección ascendente): La dirección IP de la interfaz en dirección ascendente.

Metric (Métrica): Distancia que existe entre saltos hasta la subred de origen.

Expiry Time (Tiempo de caducidad): Cantidad de tiempo antes de que la entrada caduque.

Up Time (Tiempo de actividad): Cantidad de tiempo que ha transcurrido desde que el enrutador ha obtenido el enrutador.

Visualización de la tabla de ruta DVMRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para configurar y ver la tabla de ruta DVMRP.

Tabla 8-21. Comando de la CLI para la tabla de ruta DVRMP

Comando de la CLI	Descripción
`show ip dvmrp route [`*`dirección_ip`*`] [`*`dirección_ip`*`]`	Muestra la tabla de ruta DVMRP.

A continuación se muestra un ejemplo del comando de la CLI:

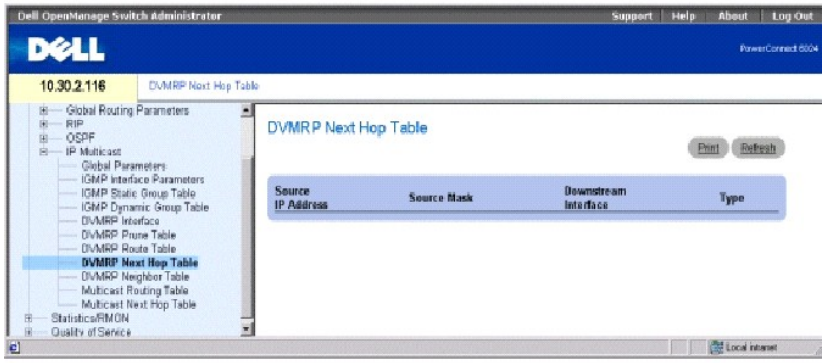
```
Console> show ip dvmrp route

Source Neighbor Interface Metric Expiry Up Time Time
```

```
-----------------------------------------------------


171.68.0.0/16 192.168.1.2816 eth g116 11016 100:02:5216 107:55:50
```

Tabla de próximo salto DVMRP

La página **DVMRP Next Hop Table** (Tabla de próximo salto DVMRP) contiene información relativa al próximo salto de interfaz saliente para los paquetes de multidifusión IP. Para abrir la página **DVMRP Next Hop Table** (Tabla de próximo salto DVMRP), haga clic en **Router→ IP Multicast→ DVMRP Next Hop Table** (Enrutador→ Multidifusión IP→ Tabla de próximo salto DVMRP) en la vista de árbol.

Ilustración 8-26. DVMRP Next Hop Table (Tabla de próximo salto DVMRP)



Source IP Address (Dirección IP de origen): La dirección IP de origen para el próximo salto de una interfaz de salida.

Source Mask (Máscara de origen): La máscara de origen para el próximo salto de una interfaz de salida.

Downstream Interface (Interfaz en dirección descendente): La interfaz de salida del próximo salto.

Type (Tipo): Especifica el tipo del próximo salto. Los valores posibles son:

Branch (Rama): Indica que existe otro salto después de éste.

Leaf (Hoja): Indica que éste es el último salto de la ruta.

Visualización de la tabla de próximo salto DVMRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de próximo salto DVMRP.

Tabla 8-22. Comandos de la CLI para la tabla de próximo salto DVMRP

Comando de la CLI	Descripción
`show ip dvmrp next-hop [ethernet` *`número_interfaz`* `| vlan` *`id_vlan`* `| port-channel` *`número`*`]`	Muestra la tabla de próximo salto DVMRP.

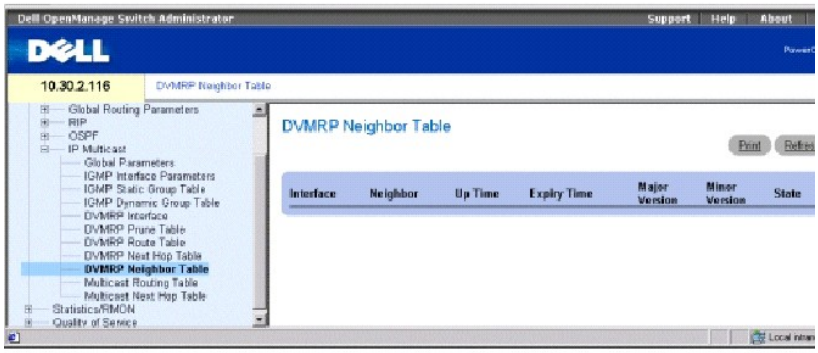
A continuación se muestra un ejemplo del comando de la CLI:

```
Console> show ip dvmrp next-hop

Source Interface Hop Type

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

198.92.37.100/32 eth g2 Leaf
```

Tabla de elementos adyacentes DVMRP

La página **DVMRP Neighbor Table** (Tabla de elementos adyacentes DVMRP) contiene información sobre las interfaces de puertos adyacentes. Los elementos adyacentes DVMRP se descubren mediante los mensajes DVMRP. Para abrir la página **DVMRP Neighbor Table** (Tabla de elementos adyacentes DVMRP), haga clic en **Router**→ **IP Multicast**→ **DVMRP Neighbor Table** (Enrutador→ Multidifusión IP→ Tabla de elementos adyacentes DVMRP) en la vista de árbol.

Ilustración 8-27. DVMRP Neighbor Table (Tabla de elementos adyacentes DVMRP)



Interface (Interfaz): El número de la interfaz en la que se habilita DVMRP.

Neighbor (Elemento adyacente): Dirección IP de la interfaz adyacente.

Up Time (Tiempo de actividad): Cantidad de tiempo transcurrido desde que la interfaz vecina se convirtió en adyacente.

Expiry Time (Tiempo de caducidad): Indica la cantidad de tiempo mínima antes de que la interfaz caduque.

Major Version (Versión mayor): El número de versión mayor del enrutador del elemento adyacente.

Minor Version (Versión menor): El número de versión menor del enrutador del elemento adyacente.

State (Estado): El estado del dispositivo adyacente.

Visualización de la tabla de elementos adyacentes DVMRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de elementos adyacentes DVMRP.

Tabla 8-23. Comandos de la CLI para la tabla de elementos adyacentes DVMRP

Comando de la CLI	Descripción
show ip dvmrp neighbor [ethernet *número_interfaz* | vlan *id_vlan* | port-channel *número*]	Muestra la tabla de elementos adyacentes DVMRP.

A continuación se muestra un ejemplo del comando de la CLI:

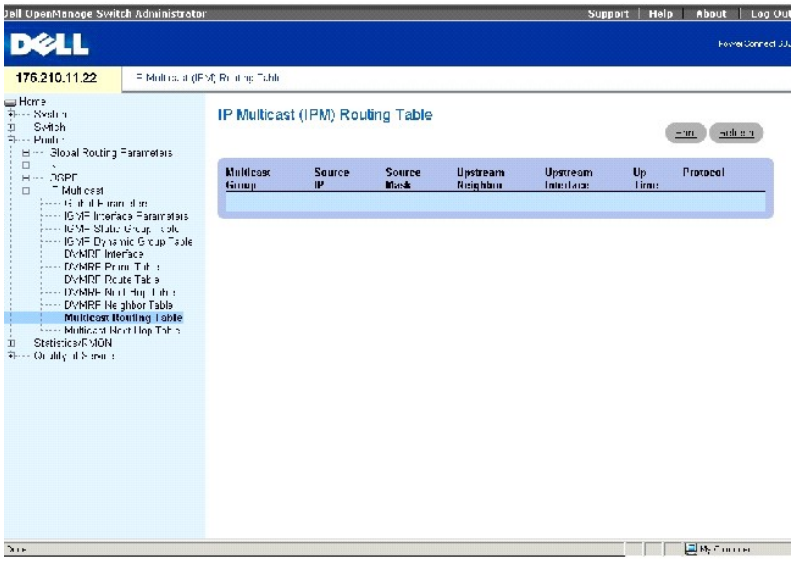
```
Console> show ip dvmrp neighbor ethernet g1

Interface Neighbor Up Expiry Version Capabilities RCV Bad State Time Time Routes Routes

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

eth g1 192.168.1.28 2 0:20:00 0:02:55 3.255 L,P,G,M 11 0 Active

eth g1 192.168.1.10 2 0:20:00 0:02:55 3.255 L,P,G,M 18 0 Active

eth g2 192.168.1.28 2 0:20:00 0:02:55 3.255 L,P,G,M 11 0 Active

eth g2 192.168.1.89 2 0:20:00 0:02:55 3.255 L,P,G,M 18 0 Active
```

Visualización de la tabla de encaminamiento de multidifusión IP

IP Multicast (IPM) Routing Table (Tabla de encaminamiento de multidifusión IP) contiene información de encaminamiento de multidifusión de paquetes IP enviados desde un origen específico a los grupos de multidifusión IP conocidos al encaminamiento de multidifusión IP.

Para abrir **IP Multicast (IPM) Routing Table** (Tabla de encaminamiento de multidifusión IP), haga clic en **Router→ IP Multicast→ Multicast Routing Table** (Enrutador→ Multidifusión IP→ Tabla de encaminamiento de multidifusión) en la vista de árbol.

Ilustración 8-28. IP Multicast (IPM) Routing Table (Tabla de encaminamiento de multidifusión IP)



La **IP Multicast (IPM) Routing Table** (Tabla de encaminamiento de multidifusión IP) contiene los siguientes campos:

Multicast Group (Grupo de multidifusión): Dirección IP del grupo de multidifusión.

Source IP (IP de origen): Dirección IP de origen del dispositivo al cual se aplica la información de multidifusión.

Source Mask (Máscara de origen): Enmascara todas las partes de la dirección IP de origen.

Upstream Neighbor (Elemento adyacente en dirección ascendente): Dirección IP del siguiente dispositivo en dirección ascendente del cual proceden los paquetes recibidos en la dirección IP.

Upstream Interface (Interfaz en dirección ascendente): Número del puerto en el que se reciben los paquetes de multidifusión enviados.

Up Time (Tiempo de actividad): Indica el lapso de tiempo transcurrido desde que el enrutador ha obtenido la información de multidifusión.

Protocol (Protocolo): Identifica el tipo de protocolo utilizado para obtener la información de multidifusión. Para este proyecto, el único valor posible es **DVMRP**, que indica que se ha utilizado el protocolo de encaminamiento de multidifusión de vector de distancia se ha utilizado para obtener la información de multidifusión.

Visualización de la tabla de encaminamiento de multidifusión IP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de encaminamiento de multidifusión IP.

Tabla 8-24. Comandos de la CLI para la tabla de encaminamiento de multidifusión IP

Comando de la CLI	Descripción
`show ip mroute [group` *dirección_grupo*`] [source` *dirección_origen*`] [ethernet` *número_interfaz* `|` *vlan id_vlan* `|` *número_canal_puerto*`]`	Visualiza el contenido de la tabla de encaminamiento de multidifusión IP.

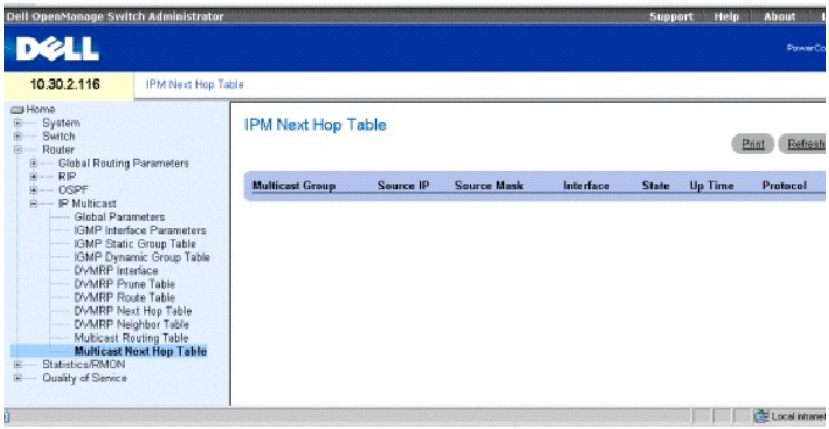
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console> show ip mroute

Group Source Upstream Interface Up Time Expiry Time Owner

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

224.0.255.1 198.92.37.100/32 10.20.37.33 eth g1 20:20:00 0:02:55 dvmrp

224.0.255.1 199.92.37.100/32 10.20.37.33 eth g1 1d:4h:20m 0:02:55 dvmrp

224.1.255.1 198.92.37.100/32 10.20.37.33 eth g1 21:20:00 0:02:55 dvmrp

224.1.255.1 199.92.37.100/32 10.20.37.33 eth g1 1d:5h:20m 0:02:55 dvmrp

224.8.255.1 179.82.17.200/32 10.20.37.33 vlan 127 1w:1d:2h 0:02:55 dvmrp

224.8.255.1 179.82.17.200/32 10.20.37.33 vlan 128 3m:2w:2d 0:02:55 dvmrp

224.8.255.1 179.82.17.200/32 10.20.37.33 vlan 129 1y:2m:2w 0:02:55 dvmrp

224.9.255.1 179.82.17.200/32 10.20.37.33 p-c 7 1d:5h:20m 0:02:55 dvmrp
```

Visualización de la tabla de próximo salto de multidifusión IP

La página **IPM Next Hop Table** (Tabla de próximo salto de multidifusión IP) contiene información del próximo salto de multidifusión. Para abrir la página, haga clic en **Router**→ **IP Multicast**→ **Multicast Next Hop Table** (Enrutador→ Multidifusión IP→ Tabla de próximo salto de multidifusión) en la vista de árbol.

Ilustración 8-29. IPM Next Hop Table (Tabla de próximo salto de multidifusión IP)



Multicast Group (Grupo de multidifusión): Dirección IP del grupo de multidifusión.

Source IP (IP de origen): Dirección IP de origen del dispositivo al cual se aplica la información de multidifusión.

Source Mask (Máscara de origen): Enmascara todas las partes de la dirección IP de origen.

Interface (Interfaz): Número del puerto en el que se reciben los paquetes de multidifusión enviados.

State (Estado): Indica si el puerto y el próximo salto se utilizan para reenviar paquetes de multidifusión. Los valores posibles son:

Pruned (Eliminado): El puerto y el próximo salto no se utilizan para reenviar paquetes de multidifusión.

Forwarding (Reenvío): El puerto y el próximo salto se están utilizando actualmente para reenviar paquetes de multidifusión.

Up Time (Tiempo de actividad): El lapso de tiempo transcurrido desde que el enrutador ha obtenido la información de multidifusión.

Protocol (Protocolo): El tipo de protocolo utilizado para obtener la información de multidifusión. Para este producto, el único valor posible es **DVMRP**, que indica que el protocolo de encaminamiento de multidifusión de vector de distancia se ha utilizado para obtener la información de multidifusión.

Visualización de la tabla de próximo salto de multidifusión IP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver la tabla de próximo salto de multidifusión IP.

Tabla 8-25. Comandos de la CLI para el próximo salto de multidifusión IP

Comando de la CLI	Descripción
`show ip mroute-next-hop [group` *`dirección_grupo`*`] [source` *`dirección_origen`*`]`	Visualiza el contenido de la tabla de próximo salto de multidifusión IP.

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

```
Console> show ip mroute-next-hop

Group Source Interface Up Time Expiry Time State Owner

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

224.0.255.1 198.92.37.100/32 eth g2 2 0:20:00 0:02:55 Forward igmp

224.0.255.1 199.92.37.100/32 eth g2 1 :4d:20m 0:02:55 Forward igmp

224.1.255.1 198.92.37.100/32 eth g2 2 1:20:00 0:02:55 Forward dvmrp

224.1.255.1 199.92.37.100/32 eth g2 1 :4d:20m 0:02:55 Forward dvmrp
```

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de QoS

Sistemas Dell PowerConnect 6024/6024F

La página **Quality of Service** (Calidad de servicio) contiene enlaces a las principales páginas de configuración de la calidad de servicio. Para abrir la página, haga clic en **Quality of Service** (Calidad de servicio) en la vista de árbol.

Visión general de la calidad de servicio

Normalmente, el tráfico de la red es impredecible, y la única garantía básica que un administrador de red puede ofrecer es la entrega del tráfico de mejor esfuerzo. Para poder afrontar este reto, los administradores de red aplican el concepto de calidad de servicio (QoS) en toda la red. Esto garantiza que el tráfico de la red se priorice en función de criterios específicos y que dicho tráfico específico reciba un trato preferente. QoS, cuando se aplica a una red, optimiza el rendimiento de ésta y conlleva dos características básicas:

- La clasificación del tráfico entrante en clases de manejo, en función de un atributo, que incluye lo siguiente:
  - La interfaz de entrada
  - Contenido del paquete
  - Una combinación de dichos atributos
- La proporción de varios mecanismos para poder determinar la asignación de los recursos de la red a diferentes clases de manejo como, por ejemplo:
  - La asignación del tráfico de red a una cola de hardware concreta
  - La asignación de los recursos internos
  - Moldeado del tráfico

En este documento, los términos Clase de servicio (CoS) y Calidad de servicio (QoS) se utilizan en el siguiente contexto:

- CoS proporciona varios servicios de tráfico de nivel 2. El término CoS hace referencia a la clasificación de tráfico en clases de tráfico, que se manejan como un agregado entero, sin configuración en base al flujo. Normalmente, CoS guarda relación con el servicio 802.1p, que clasifica los flujos en función de su prioridad de nivel 2, tal como se establece en el encabezado de la VLAN.
- QoS hace referencia al tráfico de nivel 2 y posterior. QoS maneja la configuración en base al flujo, incluso dentro de una única clase de tráfico.

El recurso QoS implica los elementos siguientes:

- **Access Control Lists (ACLs)** (Listas de control de acceso [ACL]): Se utiliza para decidir a qué tráfico se le permite entrar en el sistema y cuál debe eliminarse. Sólo el tráfico que cumpla estos criterios está sujeto a la configuración de CoS o QoS. Las ACL se utilizan en QoS y la seguridad de la red.
- **Traffic Classification** (Clasificación del tráfico): Clasifica cada paquete entrante como perteneciente a una clase de tráfico determinada, en función del contenido del paquete o del contexto.
- **Assignment to Hardware Queues** (Asignación a colas de hardware): Asigna los paquetes entrantes a las colas de reenvío. Los paquetes se envían a una cola concreta para su manejo como función de la clase de tráfico a la que pertenecen, tal como se ha definido mediante el mecanismo de clasificación.
- **Traffic Class-Handling Attributes** (Atributos de manejo de clase de tráfico): Aplica los mecanismos de QoS/CoS a clases diferentes como, por ejemplo:
  - Gestión de amplitud de banda
  - Moldeado
  - Utilización de políticas

Listas de control de acceso

Las ACL inspeccionan los paquetes entrantes y los clasifican en grupos lógicos, según diferentes criterios. Los grupos de ACL tienen acciones específicas que se llevan a cabo en cada paquete que se clasifica en el grupo. Las ACL permiten realizar acciones como, por ejemplo:

- Reenviar

- Denegar
- Denegar e inhabilitar el puerto

Las ACL se utilizan para los objetivos principales siguientes:

- Como mecanismo de seguridad, bien permitiendo o denegando la entrada de paquetes en un grupo. Este mecanismo se describe en la sección Seguridad de la red.
- Como mecanismo para clasificar paquetes en clases de tráfico para los que se ejecutan varias acciones de manejo de CoS/QoS.

Las ACL contienen varias acciones y reglas de clasificación. Un elemento de control de acceso (ACE) consta de una única regla de clasificación y su acción. Una ACL puede contener uno o más ACE.

El orden de los ACE dentro de una ACL es importante, ya que se aplican en función del primero que se ajuste a los criterios especificados. Los ACE se procesan de forma secuencial, comenzando por el primer ACE. Cuando un paquete coincide con una clasificación de ACE, se lleva a cabo la acción de ACE y el proceso de ACL termina. Si debe procesarse más de una ACL, la acción de supresión predeterminada sólo se aplica una vez procesadas todas las ACL. Esta acción de supresión predeterminada requiere que el usuario acepte de forma explícita todo el tráfico que se haya permitido, incluido el tráfico de gestión como, por ejemplo, telnet, HTTP o SNMP, que se dirija explícitamente al enrutador.

Se han definido dos tipos de ACL:

- **IP ACL** (ACL de IP): Se aplica sólo a los paquetes de IP. Todos los campos de clasificación hacen referencia a los paquetes de IP.
- **MAC ACL** (ACL de MAC): Se aplica a cualquier paquete, incluidos los paquetes que no sean de tipo IP. Los campos de clasificación se basan solamente en el nivel 2.

Existen dos métodos para aplicar las ACL a una interfaz:

- **Policy** (Política): Con este formato, las ACL se agrupan en una estructura más compleja llamada política. La política puede contener tanto reglas de QoS como ACL. El usuario puede aplicar la política a una interfaz (consulte el apartado Modo avanzado de QoS).
- **Simple**: En el formato simple, se aplica una única ACL (de MAC o IP) ACL a una interfaz. Aunque no se puede aplicar una política a una interfaz, es posible aplicar reglas básicas de QoS que clasifiquen los paquetes en las colas de salida (consulte el apartado Modo básico de QoS).

Asignación a colas

Puede seleccionarse un comportamiento de confianza o los campos de servicio de salida, entre los que se incluyen:

- **VLAN Priority Tags (VPT)** (Etiquetas de prioridad VLAN [VPT]): Las VPT se asignan a colas de salida que se basen en la VPT. Mientras que el usuario puede configurar la asignación de colas, la asignación de VPT predeterminada en la cola de salida es la que se indica a continuación. En la asignación de VPT predeterminada, la cola 1 tiene la prioridad más baja, tal como se muestra en la tabla siguiente:

Tabla 10-1. Tabla de asignación predeterminada de VPT

Valor de VPT	Número de cola
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

NOTA: La asignación de la VPT a la cola de salida se lleva a cabo en todo el sistema, y puede habilitarse o inhabilitarse por puerto.

- **802.1p Port-Based** (Basados en puerto 802.1p): Los paquetes que llegan sin etiquetar se asignan a una VPT predeterminada, que puede establecer el usuario por puerto. Una vez asignada la VPT, el paquete se trata como si hubiera llegado con esta etiqueta. La asignación de VPT a la cola de salidas se basa en las mismas definiciones basadas en etiqueta 802.1p establecidas por el usuario.
- **Layer 3 Predefined Field** (Campo predefinido de nivel 3): El usuario puede configurar el sistema para que utilice DSCP de IP del paquete entrante para las colas de prioridad de salida. La asignación de DSCP de IP en la cola de prioridad se establece en función del sistema. Si este modo está activo, un paquete que no sea de tipo IP se clasificará siempre en la cola de mejor esfuerzo. En la tabla siguiente se muestra la asignación predeterminada:

Tabla 10-2. Tabla de asignación predeterminada de DSCP

Valor de DSCP	Número de cola
0-7	q1 (Prioridad más baja)
8-15	q2
16-23	q3
24-31	q4
32-39	q5
40-47	q6
48-55	q7
55-63	q8 (Prioridad más alta)

NOTA: Los valores de DSCP 3, 11, 19, 27, 35, 43, 51 y 59 se asignan a q1, q2... q8. Esta configuración no se puede cambiar.

- **Layer 4 Predefined Fields** (Campos predefinidos de nivel 4): Configura el sistema para que utilice el puerto TCP/UDP de destino del paquete entrante para asignar el paquete a las colas de prioridad de salida. La asignación del puerto de TCP/UDP de destino a una cola de prioridad se establece por sistema, en dos tablas separadas. Puede habilitarse o inhabilitarse por puerto.
- **None** (Ninguno): Todo el tráfico se clasifica en el servicio del mejor esfuerzo.

Una vez asignados los paquetes a una cola específica, se puede utilizar el método de clasificación elegido para aplicar varios servicios. La planificación de las colas de salida puede configurarse, que incluye lo siguiente:

- Prioridad estricta.
- Turno rotativo ponderado (WRR).
- Una combinación de dichos métodos.

Los esquemas de planificación se especifican por sistema. Las ponderaciones de WRR para las colas pueden asignarse en cualquier orden. La configuración de la ponderación está disponible por puerto.

Para cada interfaz o cola, también puede configurarse el moldeado de salida:

- Tamaño de transmisión en bloques.
- Velocidad de información convenida (CIR).
- Acciones para el trafico que supere el límite.

Modos de QoS

QoS está habilitado en PowerConnect 6024/6024F bien en modo básico o avanzado de QoS.

Modo básico de QoS

En el modo básico de QoS, se puede activar uno o más de los modos Trust, entre los que se incluyen:

- VPT
- DSCP
- TCP
- UDP
- Ninguno

Además, una sola ACL basada en MAC o en IP se puede conectar directamente a la interfaz (consulte el apartado **Configuración de la seguridad de la red** para obtener más información). Sólo los paquetes que tengan una acción **Forward** (Reenviar) se asignan a la cola de salida, en función de la clasificación especificada.

Si configura las colas de salida correctamente, podrá establecer los siguientes servicios del modo básico:

- **Minimum Delay** (Demora mínima): La cola se asigna a una política de prioridad estricta, y el tráfico se asigna a la cola de prioridad más alta.
- **Best Effort** (Mejor esfuerzo): El tráfico se asigna a la cola de prioridad más baja.
- **Bandwidth Assignments** (Asignaciones de amplitud de banda): Si configura el esquema de planificación de WRR y elige las ponderaciones adecuadas, podrá asignar amplitudes de banda.

Modo avanzado de QoS

El modo avanzado de QoS proporciona reglas para especificar la clasificación del flujo y asignar las acciones de regla que se relacionan con la gestión de la amplitud de banda. Las reglas se definen en las listas de control de la clasificación (CCL).

Las CCL se establecen de acuerdo con la clasificación definida en la ACL y no se pueden definir hasta que se haya definido una ACL válida. Cuando las CCL están definidas, puede agrupar las ACL y las CCL en una estructura más compleja, llamada política. Las políticas se pueden aplicar a una interfaz. Las ACL/CCL de la política se aplican en el orden en que aparecen en la política. Sólo se puede adjuntar una política a cada puerto.

En el modo avanzado de QoS, las ACL se pueden aplicar directamente a una interfaz. No obstante, no pueden aplicarse simultáneamente una política y una ACL a una interfaz.

Tras asignar los paquetes a una cola específica, puede aplicar servicios como, por ejemplo, configurar colas de salida para el esquema de planificación, o bien configurar el moldeado de la salida para el tamaño de transmisión en bloques, CIR o CBS por interfaz o por cola.

Configuración de los servicios - Ejemplos

Puede utilizar la configuración del modo avanzado de QoS para aplicar los servicios siguientes al tráfico de la red:

- **Best Effort** (Mejor esfuerzo): El tráfico se asigna a la cola de prioridad más baja.
- **802.1p**: El valor de VPT se establece en función de la clasificación.
- **IP DSCP** (DSCP de IP): El valor se establece en función de la clasificación.
- **Minimum Delay** (Demora mínima): La cola se asigna a una política de prioridad estricta, y el tráfico se asigna a la cola de prioridad más alta.
- **Ingress Metering/Rate Limiting** (Medición de entradas/Límite de velocidad): Se especifica un valor máximo de amplitud de banda más allá del cual se elimina todo el tráfico. Esto puede llevarse a cabo colocando un contador en la entrada para la amplitud de banda máxima y estableciendo le política de exceso para la supresión. Para poder configurar este servicio de forma eficaz, la amplitud de banda total en un puerto de entrada específico no puede exceder la velocidad del puerto.

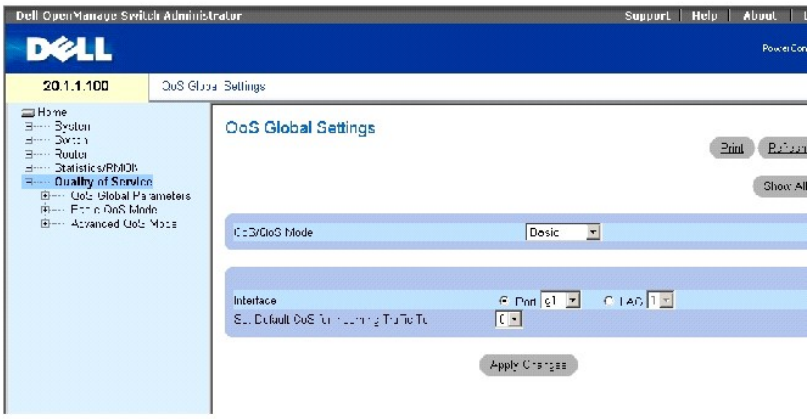
Configuración de los parámetros globales de QoS

La página **QoS Global Parameters** (Parámetros globales de QoS) contiene enlaces a las páginas de QoS en las que se habilita QoS, se reasigna la configuración y los valores de DSCP, el tráfico de la red se coloca en la cola y se define la clasificación del tráfico. Para abrir la página, haga clic en **Quality of Service→ QoS Global Parameters** (Calidad de servicio→ Parámetros globales de QoS) en la vista de árbol.

Definición de la configuración de QoS

Utilice la página **QoS Global Settings** (Configuración global de QoS) para seleccionar el modo de QoS y configurar el CoS predeterminado del tráfico entrante en una interfaz seleccionada. Para abrir la página, haga clic en **Quality of Service→ QoS Global Parameters→ QoS Settings** (Calidad de servicio→ Parámetros globales de QoS→ Configuración de QoS) en la vista de árbol.

Ilustración 10-1. Página QoS Global Settings (Configuración global de QoS)



QoS Mode (Modo de QoS): Inhabilita o habilita el modo básico o avanzado de QoS. El modo básico está habilitado de forma predeterminada.

NOTA: Es posible que al conmutar entre los modos básico y avanzado de QoS se pierda cierta información de configuración.

Interface (Interfaz): El puerto o LAG para el que se ha definido la política de CoS predeterminada.

Set Default CoS for Incoming Traffic To (Establecer CoS como predeterminado para tráfico entrante en): Determina el valor predeterminado de CoS para los paquetes entrantes para los que no se haya definido ninguna etiqueta de VLAN. Los valores posibles son **0**-**7**. El valor predeterminado de CoS es **0**.

Selección de un modo de servicio

1. Abra la página **QoS Settings** (Configuración de QoS).
2. Seleccione un modo de servicio en el campo **CoS/QoS Mode** (Modo de CoS/QoS).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona el modo de QoS y el dispositivo se actualiza.

Establecimiento del valor predeterminado de CoS para el tráfico entrante de una interfaz

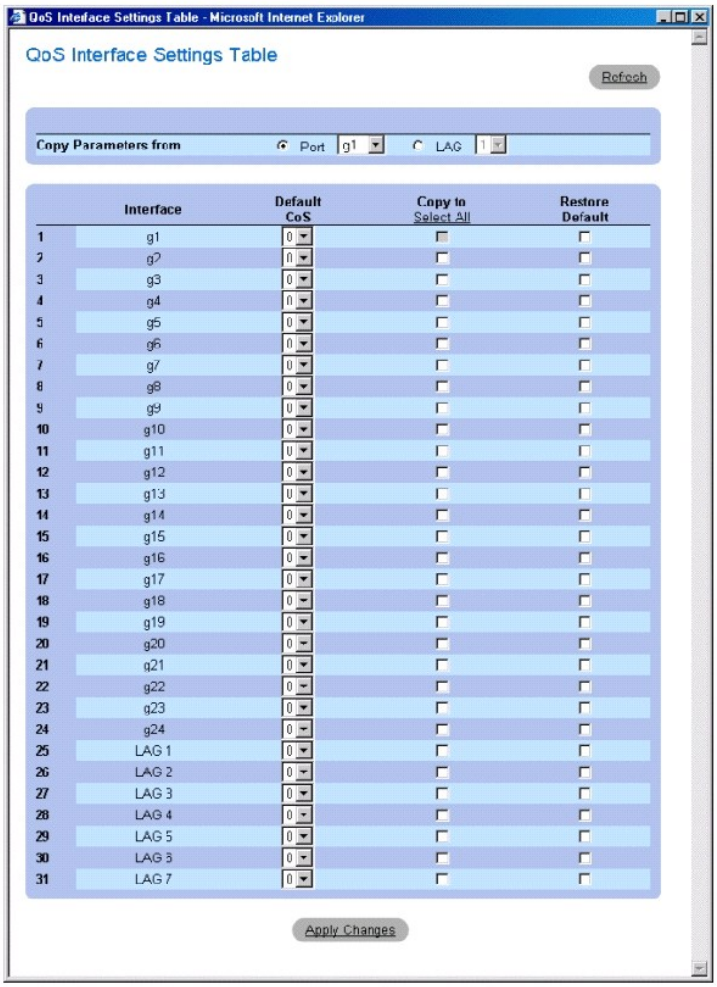
1. Abra la página **QoS Settings** (Configuración de QoS).
2. Seleccione una interfaz y establezca el valor predeterminado de CoS para el tráfico entrante mediante el menú descendente.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona el valor predeterminado de CoS para el tráfico entrante en la interfaz y el dispositivo se actualiza.

Copia de la configuración de la interfaz QoS

1. Abra la página **QoS Settings** (Configuración de QoS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **QoS Interface Settings Table** (Tabla de configuración de la interfaz QoS).
3. Seleccione una interfaz de la que copiar la configuración de QoS en todas o alguna de las interfaces que figuran en la página QoS Interface Settings Table (Tabla de configuración de la interfaz QoS).
4. Marque la casilla de verificación **Copy to** (Copiar en) para cada una de las interfaces en las que deba copiarse la configuración de QoS, o bien haga clic en **Select All** (Seleccionar todo) para copiar la configuración de QoS en todas las interfaces de la lista.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Ilustración 10-2. Página QOS Interface Settings Table (Tabla de configuración de la interfaz QoS)



Definición de la configuración de QoS mediante los comandos de la CLI

Tabla 10-3. Comandos de la CLI para definir la configuración de QoS

Comando de la CLI	Descripción
`qos [avanzado]`	Habilita/inhabilita el modo básico/avanzado de QoS para todo el dispositivo.
`show qos`	Muestra el modo de QoS para todo el dispositivo.
`qos cos default- cos`	Configura el valor predeterminado de CoS para la interfaz.

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

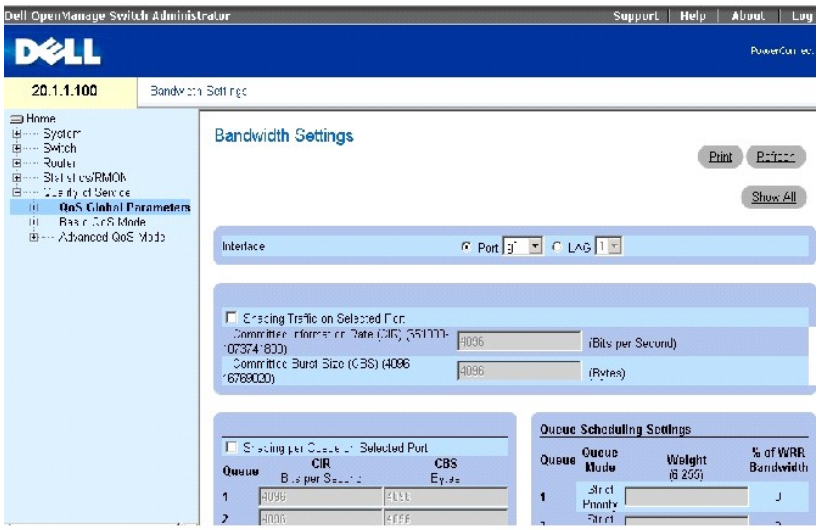
```
Console (config)# qos

Console (config)# interface ethernet g5
```

```
Console (config-if)# qos cos 3


Console (config-if)# exit


Console (config)#exit


Console# show qos


QoS: basic


Basic trust: vpt
```

Definición de la configuración de la amplitud de banda

Utilice la página **Bandwidth Settings** (Configuración de la amplitud de banda) para definir la configuración de la amplitud de banda para una interfaz de entrada especificada. La modificación de la planificación de la cola afecta globalmente a la configuración de la cola. Para abrir la página, haga clic en **Quality of Service→ QoS Global Parameters→ Bandwidth Settings** (Calidad de Servicio→ Parámetros globales de QoS→ Configuración de la amplitud de banda) en la vista de árbol.

Ilustración 10-3. Bandwidth Settings (Configuración de la amplitud de banda)



La página **Bandwidth Settings** (Configuración de la amplitud de banda) contiene los siguientes campos:

Interface (Interfaz): El puerto o LAG al que se aplica la configuración de la amplitud de banda.

Shaping Traffic on Selected Port (Moldeado del tráfico en el puerto seleccionado): Configura la velocidad de información convenida (CIR) y el tamaño de transmisión en bloques convenido (CBS) en la interfaz. Es posible especificar el moldeado por cola y por interfaz simultáneamente. El moldeado se determina mediante el valor especificado más bajo.

Shaping per Queue on Selected Port (Moldeado por cola en el puerto seleccionado): Configura CIR y CBS por cola. Es posible especificar el moldeado por cola

y por interfaz simultáneamente. El moldeado se determina mediante el valor especificado más bajo.

Queue Scheduling Settings (Configuración de la planificación de colas): Configura la ponderación para cada cola de turno rotativo ponderado.

WRR Weight (0-255) (Ponderación de WRR): Asigna ponderaciones a cada cola del turno rotativo ponderado. Las colas WRR se definen por puerto y tiene un rango de 6-255. Se puede asignar un peso de 0 a cada cola, en cuyo caso la cola no será operativa y se cerrará eficazmente.

Moldeado del tráfico en una interfaz seleccionada

1. Abra la página **Bandwidth Settings** (Configuración de la amplitud de banda).
2. Seleccione una interfaz.
3. Marque **Shaping Traffic on Selected Port** (Moldeado del tráfico en el puerto seleccionado).
4. Escriba los valores de CIR y CBS para la interfaz.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se configuran CIR y CBS para la interfaz seleccionada y el dispositivo se actualiza.

Moldeado del tráfico por cola de puerto

1. Abra la página **Bandwidth Settings** (Configuración de la amplitud de banda).
2. Seleccione una interfaz.
3. Marque **Shaping Traffic on Selected Port** (Moldeado por cola en el puerto seleccionado).
4. Escriba los valores de CIR y CBS para cada cola.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se configuran CIR y CBS para cada cola de la interfaz seleccionada y el dispositivo se actualiza.

Configuración de la planificación de colas por puerto

1. Abra la página **Bandwidth Settings** (Configuración de la amplitud de banda).

NOTA: Utilice la página **Global Queue Settings** (Configuración global de las colas) para modificar de forma global la configuración de la planificación de colas.

2. Para cada una de las ocho colas, configure el valor **Strict Priority** (Prioridad estricta) o escriba un valor para **Weight** (Ponderación).
3. Para cada una de las colas que se haya establecido en todo el sistema como una cola WRR, escriba una ponderación.

El intervalo de ponderación especifica la frecuencia con la que el planificador de paquetes extrae de cada cola los paquetes. El intervalo de cada cola se define mediante la ponderación de cola dividida por la suma de todas las ponderaciones de cola (ponderación normalizada); de esta forma se establece la asignación de la amplitud de banda de cada cola.

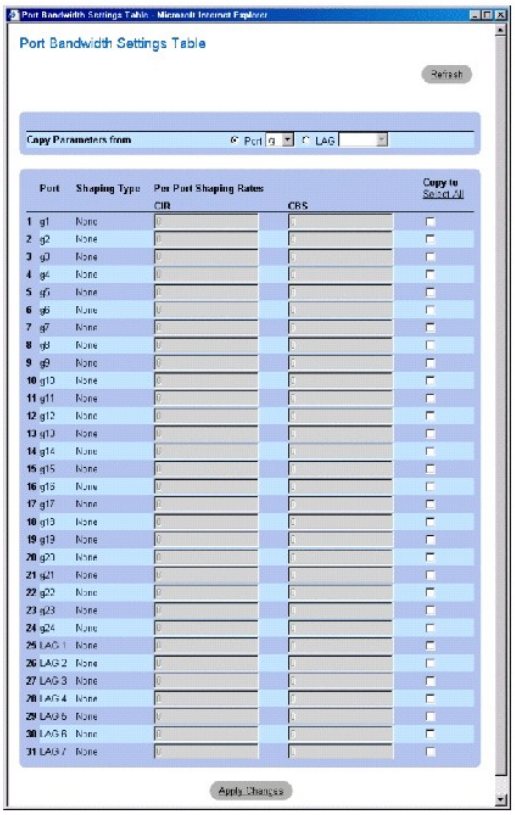
4. Haga clic en **Apply Changes** (Aplicar cambios).

El dispositivo se actualiza.

Visualización de la tabla de configuración de la amplitud de banda de los puertos

1. Abra la página **Bandwidth Settings** (Configuración de la amplitud de banda).
2. Haga clic en **Show All** (Mostrar todo) para visualizar al página **Port Bandwidth Settings Table** (Tabla de configuración de la amplitud de banda de los puertos).

Ilustración 10-4. Port Bandwidth Settings Table (Tabla de configuración de la amplitud de banda del puerto)



Shaping Type (Tipo de moldeado): Puede ser por puerto, por cola, ambos tipos o ninguno.

Per Port Shaping Rates (Intervalos de moldeado por puerto): El tipo de intervalo para CIR y CBS es por puerto. Para ver el moldeado de cola, utilice la página de edición.

Copia de la configuración de la amplitud de banda de los puertos

1. Abra la página **Bandwidth Settings** (Configuración de la amplitud de banda).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Port Bandwidth Settings Table** (Tabla de configuración de la amplitud de banda de los puertos).
3. Seleccione una interfaz de la que copiar la configuración de la amplitud de banda de los puertos en todas o alguna de las interfaces que figuran en la página Port Bandwidth Settings Table (Tabla de configuración de la amplitud de banda de los puertos).
4. Marque la casilla de verificación **Copy to** (Copiar en) de cada una de las interfaces en las que deba copiarse la configuración de la amplitud de banda de los puertos, o bien haga clic en **Select All** (Seleccionar todo) para copiar dicha configuración en todas las interfaces de la lista.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Definición de la configuración de la amplitud de banda mediante los comandos de la CLI

Tabla 10-4. Comandos de la CLI para la configuración de amplitud de banda

Comando de la CLI	Descripción
`traffic-shape {`*`velocidad_convenida transmisión en bloques_convenida`*`} [`*`id_cola`*`]`	Establece el moldeador en el puerto o cola de salida.
`wrr-queue bandwidth` *`ponderación1 ponderación2... ponderación_n`*	Asigna las ponderaciones de turno rotativo ponderado (WRR) en las colas de salida.
	Configura el número de colas de prioridad estricta.

priority-queue out num- of-queues *número_de_ colas*	
show qos interface [ethernet *número_interfaz* | vlan *id_vlan* | port-channel *número*] [buffers | queuing | policers | shapers]	Muestra la información de interfaz QoS.

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

```
Console (config)# interface ethernet g5

Console (config-if)# traffic-shape 124000 96000

Console (config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8

Console (config-if)# exit

Console (config)# priority-queue out num-of-queues 2

Console (config)# exit

Console> show qos interface ethernet g1 buffers

Ethernet g1

Notify Q depth:

qid-size

1 - 125

2 - 125

3 - 125

4 - 125

5 - 125

6 - 125

7 - 125

8 - 125
```

qid WRED thresh0 thresh1 thresh2

1 dis 100 100 100

2 dis 100 100 100

3 dis 100 100 100

4 dis 100 100 100

5 Ena N/A N/A N/A

6 Ena N/A N/A N/A

7 Ena N/A N/A N/A

8 Ena N/A N/A N/A

qid MinDP0 MaxDP0 ProbDP0 MinDP1 MaxDP1 ProbDP1 MinDP2 MaxDP2 ProbDP2 weight

1 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

2 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

3 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

4 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

5 50 60 13 65 80 6 85 95 4 2

6 50 60 13 65 80 6 85 95 4 2

7 50 60 13 65 80 6 85 95 4 2

8 50 60 13 65 80 6 85 95 4 2

Console> show qos interface ethernet g1 queueing

Ethernet g1

wrr bandwidth weights and EF priority:

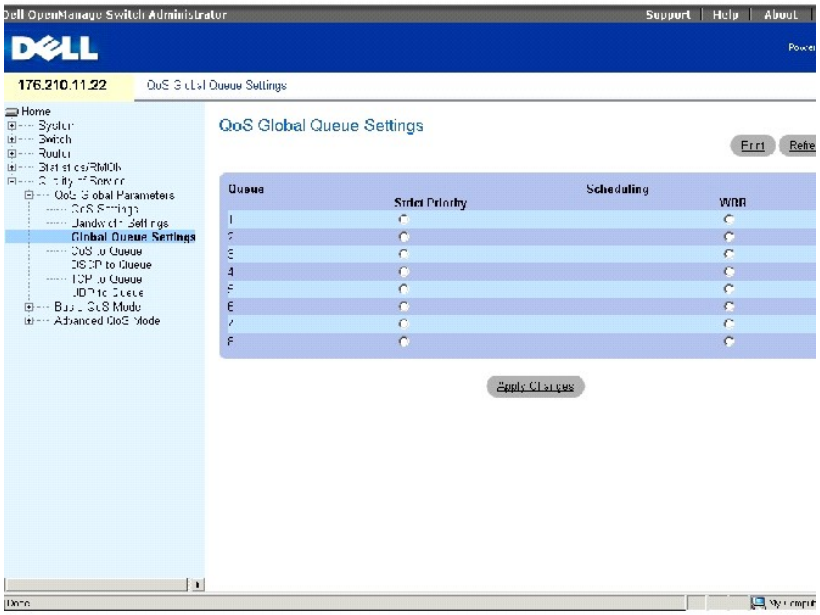
```
qid-weights Ef - Priority

1 - 125 dis- N/A

2 - 125 dis- N/A

3 - 125 dis- N/A

4 - 125 dis- N/A

5 - N/A ena- 5

6 - 125 dis- N/A

7 - 125 dis- N/A

8 - N/A ena- 8

Cos-queue map:

cos-qid

0 - 3

1 - 1

2 - 2

3 - 4

4 - 5

5 - 6

6 - 7
```

Definición de la configuración global de las colas

Utilice la página **Global Queue Settings** (Configuración global de las colas) para modificar las planificaciones de las colas de forma global.

Para abrir la página, haga clic en **Quality of Service**→ **QoS Global Parameters**→ **Queue Settings** (Calidad de servicio→ Parámetros globales de QoS→ Configuración de colas) en la vista de árbol.

Ilustración 10-5. Global Queue Settings (Configuración global de las colas)



La página **Global Queue Settings** (Parámetros globales de las colas) contiene los siguientes campos:

Queue (Cola): Indica el número de cola.

Strict Priority (Prioridad estricta): Especifica si la planificación del tráfico se basa en la prioridad de la cola. Es el valor predeterminado para las colas.

WRR: Especifica si la planificación del tráfico se basa en las ponderaciones de turno rotativo ponderado (WRR) asignadas a las colas de salida. Las ponderaciones de WRR se definen en la página **Bandwidth Settings** (Configuración de la amplitud de banda).

Configuración global de la planificación de colas

1. Abra la página **Global Queue Settings** (Configuración global de las colas).
2. Para cada una de las colas, haga clic en **Strict Priority** (Prioridad estricta) o **WRR** (turno rotativo ponderado).

   La configuración real de WRR se establece por puerto, en la página **Bandwidth Settings** (Configuración de la amplitud de banda).

   Al marcar un botón de opción para cualquier cola se selecciona automáticamente el tipo de planificación para las colas que aparecen después de dicha cola. Las colas que aparecen antes de la cola seleccionada utilizan el tipo contrario de planificación de prioridad. Por ejemplo, si hace clic en **Strict Priority** (Prioridad estricta) para la cola 6, también se seleccionan las colas 7 y 8 como **Strict Priority** (Prioridad estricta); las colas 1 a 5 se seleccionan como WRR.

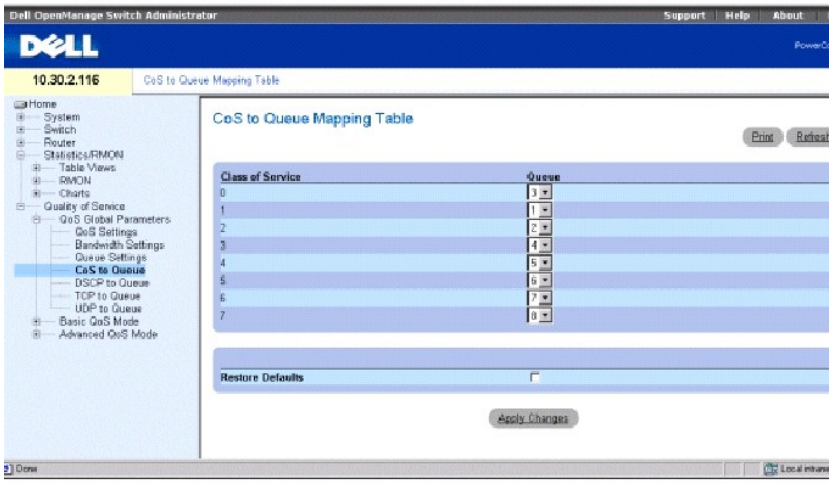
NOTA: Deben configurarse como colas WRR un mínimo de dos colas.

3. Haga clic en **Apply Changes** (Aplicar cambios) para actualizar el dispositivo.

Definición de la asignación de CoS a colas

En la página **CoS to Queue Mapping Table** (Tabla de asignación de CoS a colas) puede asignar valores de CoS a colas específicas. Para abrir la página, haga clic en **Quality of Service→ QoS Global Parameters→ CoS to Queue** (Calidad de servicio→ Parámetros globales de QoS→ CoS a cola) en la vista de árbol.

Ilustración 10-6. Página CoS to Queue Mapping Table (Tabla de asignación de CoS a colas)



Class of Service (Clase de servicio): La etiqueta de prioridad de VLAN 802.1Q del paquete entrante.

Queue (Cola): Asigna CoS a la cola seleccionada. Los valores posibles para la cola son **1-8**.

Los paquetes entrantes que tienen el valor de CoS especificado se asignan a la cola definida, si se ha habilitado **Trust** (Confianza) para CoS.

Restore Defaults (Restaurar valores predeterminados): Restaura todas las colas a la configuración de clase de servicio predeterminada.

Asignación de CoS a colas

1. Abra la página **CoS to Queue Mapping Table** (Tabla de asignación de CoS a colas).
2. Seleccione una cola para cada entrada de **Class of Service** (Clase de servicio).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna CoS a las colas y el dispositivo se actualiza.

Restablecimiento de la asignación de CoS a las colas predeterminadas:

1. Abra la página **CoS to Queue Mapping Table** (Tabla de asignación de CoS a colas).
2. Marque **Restore Defaults** (Restaurar valores predeterminados).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La asignación de CoS a colas se restablece en el valor predeterminado y el dispositivo se actualiza.

Asignación de CoS a las colas mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para asignar CoS a las colas.

Tabla 10-5. Comandos de la CLI para la asignación de CoS a colas

Comando de la CLI	Descripción
`wrr-queue cos-map` *`id_cola cos1... cos8`*	Utiliza los valores CoS asignados para seleccionar una de las colas de salida.
`show qos map [dscp- queue | tcp-port- queue | udp-port- queue | dscp-policed | dscp-mutation]`	Muestra todas las asignaciones para QoS.

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

```
Console (config)# wrr-queue cos-map 7 246

Console (config)# show qos map dscp-queue

Dscp-queue map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

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

0 : 01 01 01 01 01 01 01 02 02

1 : 02 02 02 02 02 02 03 03 03 03

2 : 03 03 03 03 04 04 04 04 04 04

3 : 04 04 05 05 05 05 05 05 05 05

4 : 06 06 06 06 06 06 06 06 07 07

5 : 07 07 07 07 07 07 08 08 08 08

6 : 08 08 08 08

Console (config)# show qos map tcp-port-queue

Tcp port-queue map:

Port queue

----- ------

6000 1
```

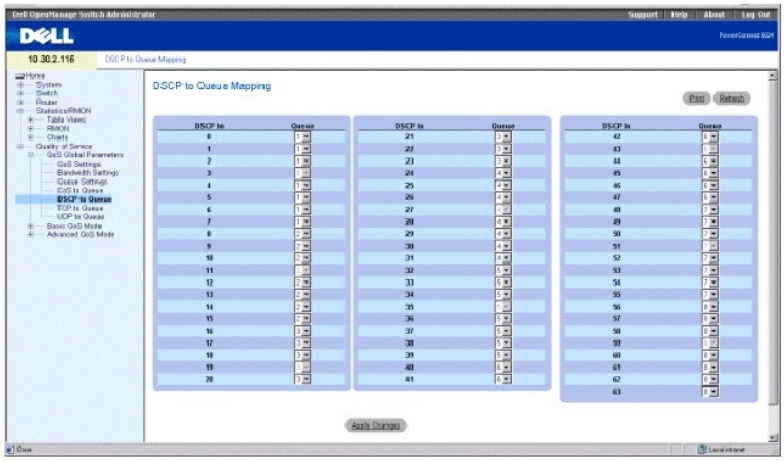
```
6001 2

6002 3

Console (config)# show qos map udp-port-queue

Udp port-queue map:

Port queue

----- -----

8000 1

8001 2

Console (config)# show qos map dscp-policed

Policed-dscp map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

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

0 : 00 01 02 03 04 05 06 07 08 09

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 60 61 62 63

Console (config)# show qos map dscp-mutation

Dscp-dscp mutation map:
```

```
d1 :d2 0 1 2 3 4 5 6 7 8 9

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

0 : 00 01 02 03 04 05 06 07 08 09

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 60 61 62 63
```

Definición de la asignación de DSCP a colas

En la página **DSCP to Queue Mapping** (Asignación de DSCP a colas) se puede habilitar la asignación de valores de DSCP a colas específicas. Para abrir la página, haga clic en **Quality of Service→ QoS Global Parameters→ DSCP to Queue** (Calidad de servicio→ DSCP a cola) en la vista de árbol.

Ilustración 10-7. Página DSCP to Queue Mapping (Asignación de DSCP a colas)



DSCP In (Entrada DSCP): Indica el valor de punto de código diferenciado de servicios en el paquete entrante.

Queue (Cola): Asigna el valor de DSCP a la cola seleccionada.

Los paquetes entrantes que tengan el valor de DSCP especificado se asignan a la cola designada, si se habilitado el modo **Trust** (Confianza) para el DSCP.

Los valores de DSCP 3, 11, 19, 27, 35, 43, 51 y 59 se asignan a q1, q2... q8. Esta configuración no puede cambiarse.

Asignación de DSCP a colas

1. Abra la página **DSCP to Queue Mapping** (Asignación de DSCP a colas).
2. Seleccione una cola para cada nivel de DSCP.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna el DSCP a las colas y el dispositivo se actualiza.

Asignación de DSCP a las colas mediante los comandos de la CLI

Tabla 10-6. Comandos de la CLI para asignar DSCP a las colas

Comando de la CLI	Descripción
`qos map dscp-queue` *`lista_dscp`* `to` *`id_cola`*	Modifica la asignación de DSCP a CoS.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Muestra todas las asignaciones para QoS.

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

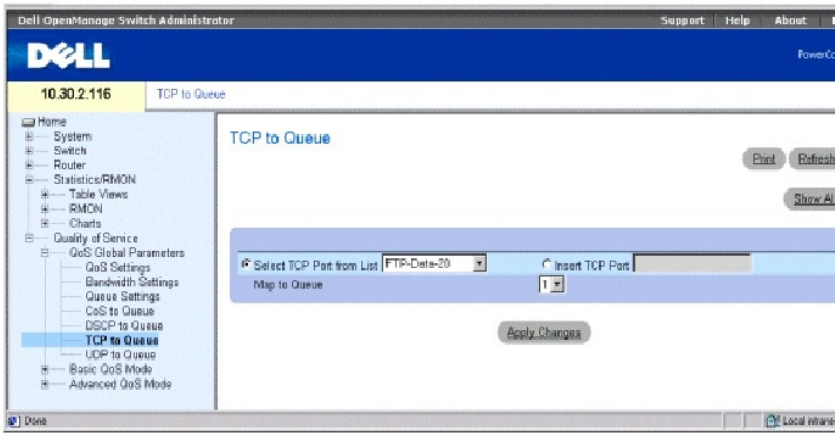
```
Console (config)# qos map dscp-queue 33 40 41 to 1

Console (config)# exit

Console # show qos map dscp-queue

Dscp-queue Map

d1: d2 0 1 2 3 4 5 6 7 8 9

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

0: 01 01 01 01 01 01 02 02

1: 02 02 02 02 02 03 03 03

2: 03 03 03 04 04 04 04 04

3: 04 04 05 05 05 05 05 05

4: 06 06 06 06 06 06 07 07

5: 07 07 07 07 08 08 08 08
```

6: 08 08 08 08

Definición de la asignación de TCP de QoS a cola

En la página **QoS TCP to Queue** (TCP de QoS a cola) se habilita la asignación del puerto TCP a una cola. Para abrir la página, haga clic en **Quality of Service**→ **QoS Global Parameters**→ **TCP to Queue** (Calidad de servicio→ Parámetros globales de QoS→ TCP a cola) en la vista de árbol.

Ilustración 10-8. Página QoS TCP to Queue (TCP de QoS a cola)



Select TCP Port from List (Seleccionar puerto TCP de la lista): Selecciona un puerto TCP conocido para asignarlo a una cola.

Insert TCP Port (Insertar puerto TCP): Habilita manualmente la especificación de un puerto TCP para asignarlo a una cola.

Map to Queue (Asignar a cola): Indica la cola a la que se asigna el puerto TCP especificado.

Asignación de un puerto TCP conocido a una cola

1. Abra la página **TCP to Queue** (TCP a cola).
2. Seleccione la opción **Select TCP Port from List** (Seleccionar puerto TCP de la lista).
3. Seleccione un puerto TCP.
4. Seleccione una cola de la lista **Map to Queue** (Asignar a cola).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto TCP se asigna a la cola especificada,y el dispositivo se actualiza.

Asignación de un puerto TCP no listado a una cola

1. Abra la página **QoS TCP to Queue** (TCP de QoS a cola).
2. Seleccione la opción **Insert TCP Port** (Insertar puerto TCP).
3. Escriba el número de puerto TCP y la descripción en el campo **Insert TCP Port** (Insertar puerto TCP).
4. Seleccione una cola de la lista **Map to Queue** (Asignar a cola).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto TCP se asigna a la cola especificada,y el dispositivo se actualiza.

Eliminación de la asignación TCP a cola

1. Abra la página **QoS TCP to Queue** (TCP de QoS a cola).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **TCP to Queue Mapping Table** (Tabla de asignación de TCP a colas).
3. Marque la casilla de verificación **Remove** (Eliminar) de cada uno de los puertos TCP de los que desee eliminar la asignación de colas.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Definición de TCP para la asignación de colas mediante los comandos de la CLI

Tabla 10-7. Comandos de la CLI para la asignación de TCP a colas

Comando de la CLI	Descripción
`qos map tcp-port- queue` *`puerto1... puerto 8 a id_cola`*	Modifica la asignación del puerto TCP a una cola.
`show qos map [dscp- queue | tcp-port- queue | udp-port- queue | dscp-policed | dscp-mutation]`	Muestra todas las asignaciones para QoS.

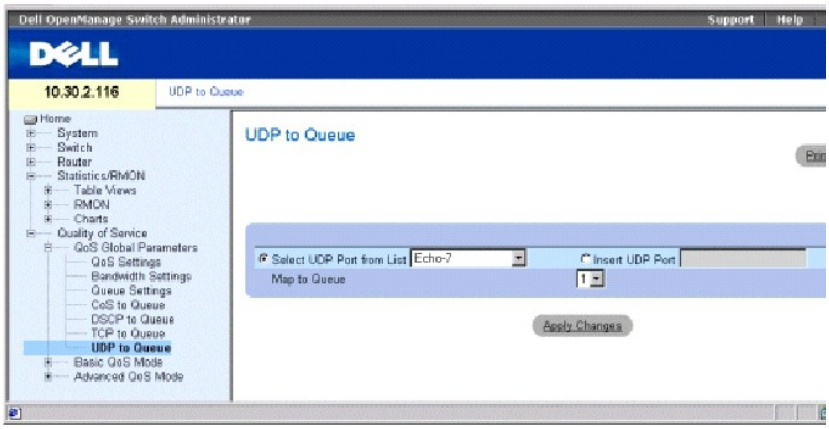
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# qos map tcp-port-queue 2000 80 to 2

Console (config)# exit

Console# show qos map tcp-port-queue

Tcp port - queue map

Port queue

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

6000 1

6001 2

6002 3
```

Definición de la asignación de UDP de QoS a cola

En la página **QoS UDP to Queue** (UDP de QoS a cola) se habilita la asignación del puerto UDP a una cola. Para abrir la página, haga clic en **Quality of Service→ QoS Global Parameters→ UDP to Queue** (Calidad de servicio→ Parámetros globales de QoS→ UDP a cola) en la vista de árbol.

Ilustración 10-9. Página UDP to Queue (UDP a cola)



Select UDP Port from List (Seleccionar puerto UDP de la lista): Selecciona un puerto UDP conocido para asignarlo a una cola.

Insert UDP Port (Insertar puerto UDP): Habilita manualmente la especificación de un puerto UDP para asignarlo a una cola.

Map to Queue (Asignar a cola): La cola a la que se asigna el puerto UDP especificado.

Asignación de un puerto UDP conocido a una cola

1. Abra la página **UDP to Queue** (UDP a cola).
2. Seleccione la opción **Select UDP Port from List** (Seleccionar puerto UDP de la lista).
3. Seleccione un puerto UDP.
4. Seleccione una cola de la lista **Map to Queue** (Asignar a cola).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto UDP se asigna a la cola especificada,y el dispositivo se actualiza.

Asignación de un puerto UDP no listado a una cola

1. Abra la página **UDP to Queue** (UDP a cola).
2. Seleccione la opción **Insert UDP Port** (Insertar puerto UDP).
3. Especifique el número de puerto UDP del campo **Insert UDP Port** (Insertar puerto UDP).
4. Seleccione una cola de la lista **Map to Queue** (Asignar a cola).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto UDP se asigna a la cola especificada, y el dispositivo se actualiza.

Eliminación de la asignación UDP a cola

1. Abra la página **UDP to Queue** (UDP a cola).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **UDP to Queue Mapping Table** (Tabla de asignación de UDP a colas).
3. Haga clic en **Remove** (Eliminar) en cada uno de los puertos UDP de los que desee eliminar la asignación de colas.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Definición de UDP para la asignación de colas mediante los comandos de la CLI

Tabla 10-8. Comandos de la CLI para la asignación de UDP a las colas

Comando de la CLI	Descripción
`qos map udp-port-queue` *`puerto1... puerto 8 a id_cola`*	Modifica la asignación del puerto UDP a una cola.
`show qos map [dscp-queue | tcp-port-queue | udp-port- queue | dscp-policed | dscp-mutation]`	Muestra todas las asignaciones para QoS.

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

```
Console (config)# qos map udp-port-queue 68 to 1

Console (config)# exit

Console# show qos map udp-port-queue

Udp port-queue map:

Port queue

----- -----

8000 1

8001 2
```

Configuración del modo básico de QoS

La página **Basic QoS Mode** (Modo básico de QoS) contiene enlaces a las páginas de QoS en las que se configura el modo **Trust** (Confianza) y la reescritura de DSCP. Para abrir la página **Basic QoS Mode** (Modo básico de QoS), haga clic en **Quality of Service**→ **Basic QoS Mode** (Calidad de servicio→ Modo Básico de QoS) en la vista de árbol.

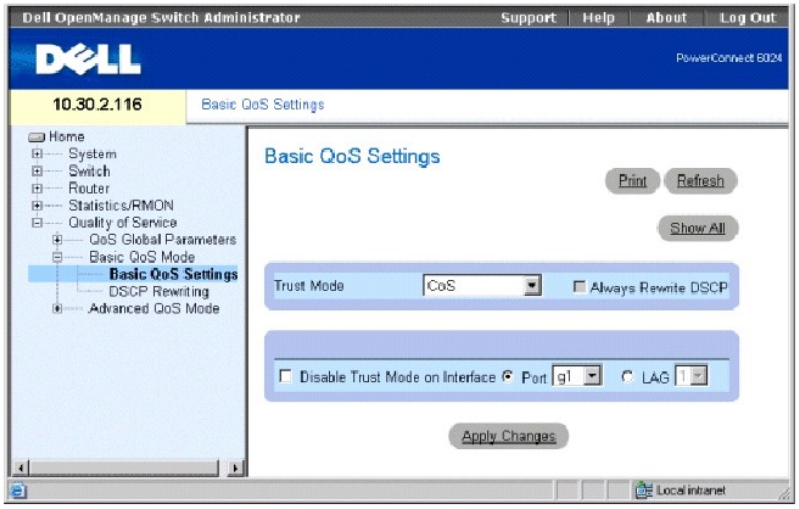
Definición de la configuración básica de QoS

Utilice la página **Basic QoS Settings** (Configuración básica de QoS) para configurar el modo **Trust** (Confianza) global, que se establece en interfaces especificadas. Los paquetes que entra en un dominio de QoS se clasifican en el límite del dominio de QoS. Cuando los paquetes se clasifican en el límite, el modo **Trust** (Confianza) puede configurarse en los puertos.

Los valores de DSCP pueden reescribirse en el límite de dominio administrativo de QoS. Si dos dominios de QoS tiene definiciones DSCP diferentes, los valores de DSCP pueden reescribirse. La asignación de DSCP se aplica sólo a puertos de confianza DSCP.

Para abrir la página **Basic QoS Settings** (Configuración básica de QoS), haga clic en **Quality of Service**→ **Basic QoS Mode**→ **Basic QoS Settings** (Calidad de servicio→ Modo básico de QoS→ Configuración básica de QoS) en la vista de árbol.

Ilustración 10-10. Página Basic QoS Settings (Configuración básica de QoS)



Trust Mode (Modo Confianza): Selecciona el modo de confianza. Si la etiqueta CoS, la etiqueta DSCP y la asignación de TCP/UDP de un paquete se asignan a colas distintas, el **Trust Mode** (Modo Confianza) determina la cola a la que se asigna el paquete. Los valores posibles son:

CoS: Establece el modo de confianza en CoS en el dispositivo. La asignación de CoS determina la cola del paquete.

DSCP: Establece el modo de confianza en DSCP en el dispositivo. La asignación de DSCP determina la cola del paquete.

TCP/UDP Port (Puerto TCP/UDP): Establece el modo de confianza en TCP/UDP Port (Puerto TCP/UDP) en el dispositivo. La asignación del puerto TCP/UDP determina la cola del paquete.

Always Rewrite DSCP (Reescribir siempre DSCP): Reescribe la etiqueta DSCP del paquete de acuerdo con la configuración de la reescritura DSCP de QoS. **Always Rewrite DSCP** (Reescribir siempre DSCP) sólo puede marcarse si el valor de **Trust Mode** (Modo Confianza) es **DSCP**.

Disable Trust Mode on Interface (Desactivar modo Trust en la interfaz): Inhabilita el modo de confianza para el puerto o LAG seleccionado.

Interface (Interfaz): Puerto o LAG en el que se ha inhabilitado el modo de confianza.

Establecimiento del modo de confianza

1. Abra la página **Basic Global Settings** (Configuración básica de QoS).
2. Seleccione un valor para **Trust Mode** (Modo Confianza).
3. Si el valor de **Trust Mode** (Modo Confianza) es **DSCP**, marque la opción **Always Rewrite DSCP** (Reescribir siempre DSCP) de forma que todas las etiquetas DSCP se reescriban como asignadas.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se selecciona el modo de confianza y el dispositivo se actualiza.

Inhabilitación del modo de confianza para las interfaces:

1. Abra la página **Basic Global Settings** (Configuración básica de QoS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Basic QoS Interface Settings Table** (Tabla de configuración básica de QoS).
3. Marque **Disable Trust Mode** (Desactivar modo Trust) para todas las interfaces en las que deba inhabilitarse el modo de confianza.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Definición de la configuración básica de QoS mediante los comandos de la CLI

Tabla 10-9. Comandos de la CLI para la configuración básica de QoS

Comando de la CLI	Descripción
`qos trust cos | dscp | tcp-udp-port`	En el contexto global, este comando se utiliza para configurar el sistema en el modo básico y el estado de confianza.
`qos trust`	En el contexto de configuración de interfaces, este comando se utiliza para habilitar el estado de confianza de cada puerto.
`qos dscp-mutation`	Aplica la asignación de mutación DSCP a un puerto de confianza DSCP del sistema (reescribe DSCP siempre en este puerto).

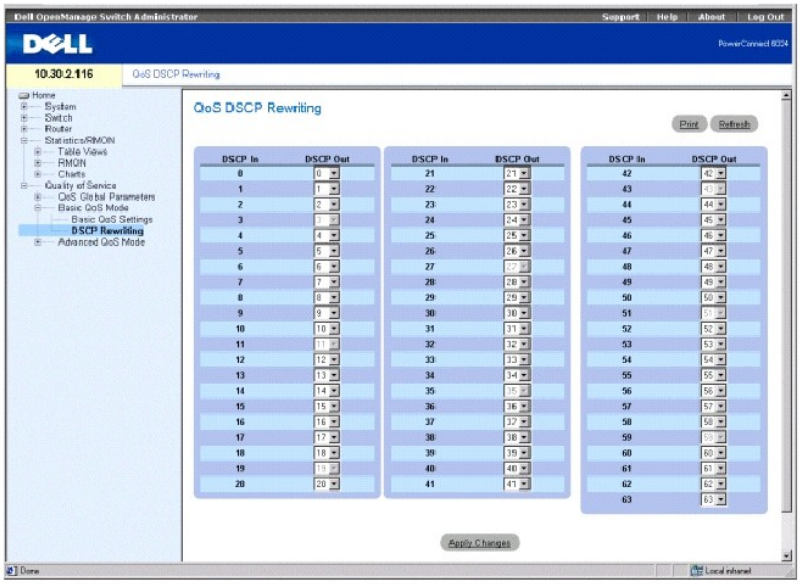
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# qos trust dscp

Console (config)# qos dscp-mutation

Console (config)# interface ethernet g5

Console (config-if) qos trust
```

Definición de la configuración de la reescritura DSCP de QoS

Utilice la página **QoS DSCP Rewriting** (Reescritura DSCP de QoS) para configurar el método de reescritura de etiquetas DSCP. Para abrir la página, haga clic en **Quality of Service**→ **Basic QoS Settings**→ **DSCP Rewriting** (Calidad de servicio→ Configuración básica de QoS→ Reescritura DSCP) en la vista de árbol.

Ilustración 10-11. Página QoS DSCP Rewriting (Reescritura DSCP de QoS)



DSCP In (Entrada DSCP): Etiqueta DSCP en un paquete entrante.

DSCP Out (Salida de DSCP): Etiqueta DSCP en los paquetes salientes.

Configuración de la reescritura DSCP

1. Abra la página **QoS DSCP Rewriting** (Reescritura DSCP de QoS).
2. Para cada una de las etiquetas de **DSCP In** (Entrada DSCP), seleccione un valor de **DSCP Out** (Salida de DSCP) en la lista descendente.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se configura la reescritura de DSCP y el dispositivo se actualiza.

Configuración de la reescritura de DSCP mediante los comandos de la CLI

Tabla 10-10. Comandos de la CLI para la reescritura DSCP

Comando de la CLI	Descripción
qos map dscp- mutation *dscp_entrada* to *dscp_salida*	Modifica la asignación de mutación de DSCP a DSCP.

A continuación se muestra un ejemplo de los comandos de la CLI para definir la asignación de mutación de DSCP:

```
Console (config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

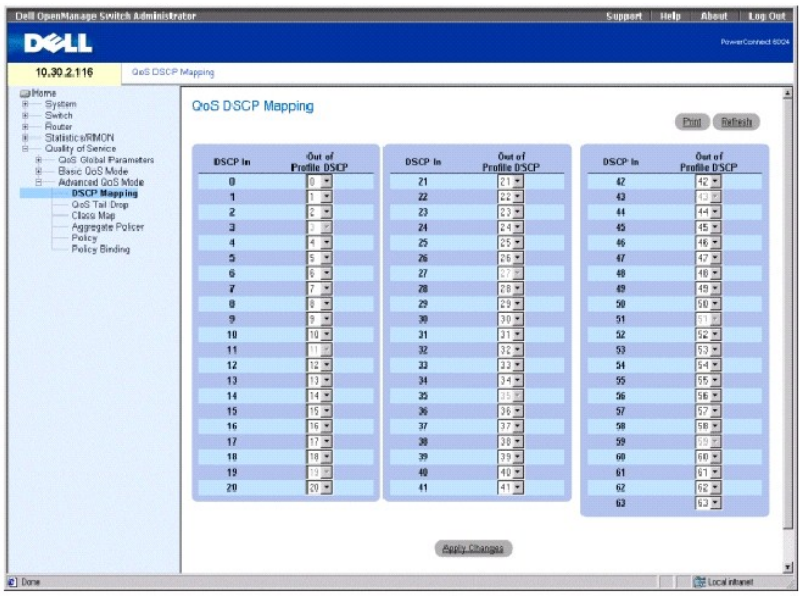
Configuración del modo avanzado de QoS

La página **Advanced QoS Mode** (Modo avanzado de QoS) contiene enlaces a páginas de QoS para poder configurar valores avanzados. Para abrir la página, haga clic en **Quality of Service**→ **Advanced QoS Mode** (Calidad de servicio→ Modo avanzado de QoS) en la vista de árbol.

Definición de la configuración de DSCP de QoS

Cuando el tráfico supere los límites definidos por el usuario, utilice la página **QoS DSCP Mapping** (Asignación de DSCP de QoS) para configurar la etiqueta DSCP para que se utilice en lugar de las etiquetas DSCP entrantes. Para abrir la página, haga clic en **Quality of Service**→ **Advanced QoS Mode**→ **DSCP Mapping** (Calidad de servicio→ Modo avanzado de QoS→ Asignación de DSCP) en la vista de árbol.

Ilustración 10-12. Página QoS DSCP Mapping (Asignación de DSCP de QoS)



DSCP In (Entrada DSCP): Etiqueta DSCP en un paquete entrante.

Out of Profile DSCP (DSCP fuera del perfil): Establece una etiqueta nueva DSCP para la etiqueta entrante.

Configuración de la asignación de DSCP

1. Abra la página **QoS DSCP Mapping** (Asignación de DSCP de QoS).
2. Seleccione un valor del menú descendente **DSCP fuera de perfil**.

   Este valor sustituye al valor de etiqueta **DSCP In** (Entrada DSCP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

   Se configura la asignación de DSCP y el dispositivo se actualiza.

Configuración de la asignación de DSCP mediante los comandos de la CLI

Tabla 10-11. Comandos de la CLI para la asignación de DSCP

Comando de la CLI	Descripción
`qos map policed- dscp lista_dscp a marcado_dscp`	Modifica la asignación DSCP a la que se aplica el control de políticas para su remarcado.

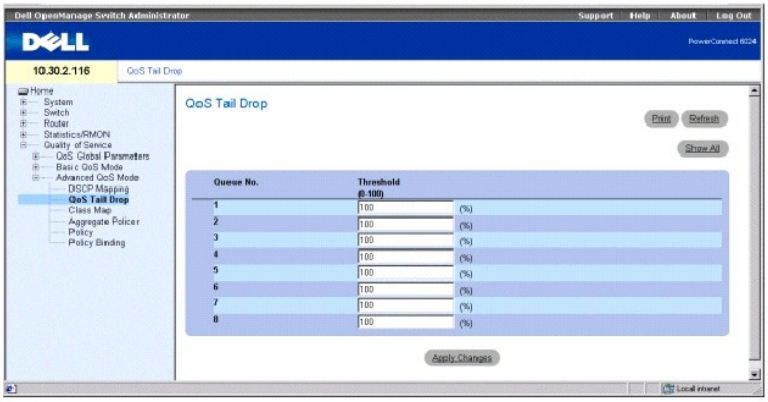
A continuación se muestra un ejemplo de los comandos de CLI para asignar valores DSCP 12 y 18 al valor 56, cuando se encuentra fuera del perfil:

```
Console (config)# qos map policed-dscp 12 18 to 56
```

Definición de la configuración de la eliminación de colas de QoS

La eliminación de colas se produce cuando una transmisión en bloques de paquetes satura un búfer. Se eliminan los últimos paquetes de la transmisión en bloques, debido a la falta de espacio en el búfer. Utilice la página **QoS Tail Drop** (Eliminación de colas de QoS) para definir la configuración de eliminación de colas para cada cola. Para abrir la página **QoS Tail Drop** (Eliminación de colas de QoS), haga clic en **Quality of Service→ Advanced QoS Mode→ QoS Tail Drop** (Calidad de servicio→ Modo avanzado de QoS→ Eliminación de colas de QoS) en la vista de árbol.

Ilustración 10-13. Página QoS Tail Drop (Eliminación de colas de QoS)



Queue No. (Nº de cola): Especifica la cola para la que se aplica la configuración de la eliminación.

Threshold (1-100) (Umbral [1-100]): El porcentaje de umbral de eliminación de colas para la cola. El paquete hace referencia a este umbral, y si se supera, los paquetes se eliminan hasta que no se exceda.

Establecimiento de un umbral de eliminación de colas

1. Abra la página **QoS Tail Drop** (Eliminación de colas de QoS).
2. Seleccione un umbral para cada cola.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se configura el umbral de eliminación y el dispositivo se actualiza.

Establecimiento de los parámetros de eliminación de colas para una interfaz:

1. Abra la página **QoS Tail Drop** (Eliminación de colas de QoS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Tail Drop Table** (Tabla de eliminación de colas).
3. Seleccione un estado para cada interfaz.
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. Se define el estado de la eliminación de colas para las interfaces.

Definición de la configuración de eliminación de colas QoS mediante los comandos de la CLI

Tabla 10-12. Comandos de la CLI para la configuración de la eliminación de colas

Comando de la CLI	Descripción
`qos wrr-queue threshold id_cola id porcentaje_umbral`	Asigna umbrales de eliminación de colas.

A continuación se muestra un ejemplo de los comandos de la CLI para definir la configuración de eliminación de colas:

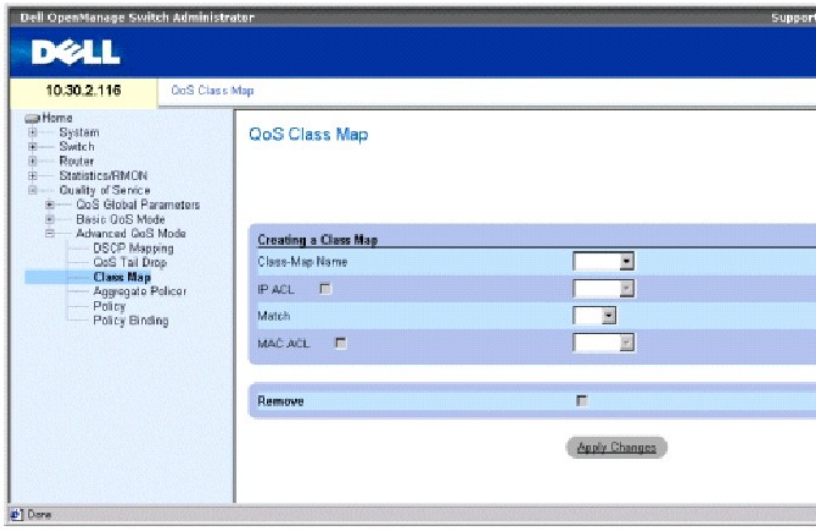
```
Console (config)# qos wrr-queue threshold 8 80
```

Definición de las asignaciones de clase de QoS

Una ACL de IP o una ACL de MAC consta de una asignación de clase. Las asignaciones de clases se configuran para que coincidan con los criterios de los paquetes, y coinciden con la primera regla a la que se ajusten. Por ejemplo, la asignación de clase A se asigna a los paquetes que se basen solamente en una ACL basada en IP o en MAC. La asignación de clase B se asigna a los paquetes que se basen tanto en una ACL basada en IP como en una basada en MAC.

Utilice la página **Class Map** (Asignación de clase) para habilitar la asignación y la edición de asignaciones de clase. Para abrir la página, haga clic en **Quality of Service→ Advanced QoS Mode→ Class Map** (Calidad de servicio→ Modo avanzado de QoS→ Asignación de clase) en la vista de árbol.

Ilustración 10-14. Página QoS Class Map (Asignación de clase de QoS)



Class-Map Name (Nombre de asignación de clase): El nombre, definido por el usuario, de la asignación de clase.

IP ACL (ACL de IP): La ACL de IP de la lista de control de acceso (ACL) de IP. Para obtener más información sobre cómo definir las ACL basadas en IP, consulte el apartado Definición de ACL basadas en IP .

Match (Coincidir): Criterios utilizados para encontrar coincidencias con direcciones IP o MAC que tengan una dirección de ACL. Los valores posibles son:

And (Y): Tanto la ACL basada en MAC como la basada en IP deben coincidir con un paquete.

Or (O): Tanto la ACL basada en MAC como la basada en IP deben coincidir con un paquete.

MAC ACL (ACL de MAC): La ACL de MAC procedente de la lista de control de acceso MAC. Para obtener información acerca de la definición de ACL basadas en MAC, consulte el apartado Definición de ACL basadas en MAC .

Remove (Eliminar): Si se selecciona esta opción, se elimina la asignación de clase de la tabla de asignación de clases.

Adición de una asignación de clase

1. Abra la página **QoS Class Map** (Asignación de clase de QoS).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add a Class-Map** (Agregar una asignación de clase).
3. Escriba un nombre (de 16 caracteres como máximo) para la asignación de clase en el campo **Class-Map Name** (Asignación de clase).
4. Realice uno de los siguientes pasos.
   - Para conectar una ACL de IP a la asignación de clase, marque **IP ACL** (ACL de IP) y seleccione una ACL de IP en el menú descendente.
   - Para conectar una ACL de MAC a la asignación de clase, marque **MAC ACL** (ACL de MAC) y seleccione una ACL de MAC en el menú descendente.
5. Seleccione **And** (Y) u **Or** (O) en el menú descendente **Match** (Coincidir) si se han seleccionado tanto la casilla de verificación **IP ACL** (ACL de IP) como la casilla de verificación **MAC ACL** (ACL de MAC).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se crea la asignación de clase y el dispositivo se actualiza.

Edición de una asignación de clase

1. Abra la página **QoS Class Map** (Asignación de clase de QoS).
2. Seleccione una asignación de clase del menú **Class-Map Name** (Nombre de asignación de clase).
3. Edite los campos restantes de la página según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. Se edita la asignación de clase y se actualiza el dispositivo.

Supresión de una asignación de clase

1. Abra la página **QoS Class Map** (Asignación de clase de QoS).
2. Seleccione una asignación de clase del menú **Class-Map Name** (Nombre de asignación de clase).
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se suprime la asignación de clase y el dispositivo se actualiza.

Visualización de la tabla de asignaciones de clase

1. Abra la página **QoS Class Map** (Asignación de clase de QoS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Class Map Table** (Tabla de asignación de clase).

Definición de las asignaciones de clases de QoS mediante los comandos de la CLI

Tabla 10-13. Comandos de la CLI para la asignación de clases de QoS

Comando de la CLI	Descripción
`class-map class-map- name [match-all | match-any]`	Crea una asignación de clase y entra en el modo de configuración de asignación de clases.

`match access-group acl- name`	Define el criterio de coincidencia para clasificar el tráfico; sólo permanece activo en el modo de configuración de asignación de clase.
`show class-map [class- map-name]`	Muestra todas las asignaciones de clase.

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

```
Console (config)# class-map class1 match-all

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit

Console (config)# exit

Console> show class-map class1

Class Map match-all class1 (id4)
```

Definición de los controladores de políticas agregados de QoS

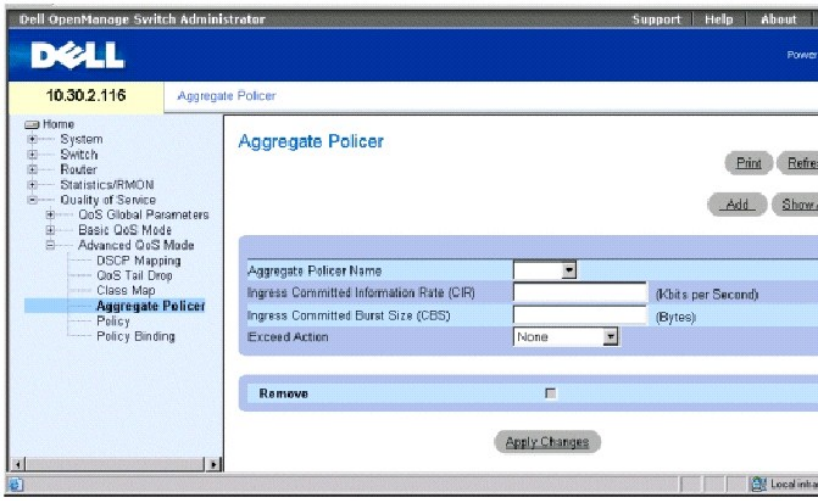
Tras clasificarse un paquete, comienza el proceso de control de políticas. Un controlador de políticas especifica el límite de la amplitud de banda para el tráfico entrante en el flujo clasificado, y las acciones se definen para los paquetes que excedan los límites. Estas acciones incluyen el reenvío, la eliminación o el remarcado de paquetes con un nuevo valor DSCP.

El conmutador admite controlador de políticas agregados y por flujo.

Los controladores de políticas agregados fuerzan los límites de un grupo de flujos. Un controlador de políticas agregado no puede suprimirse si se está utilizando en una asignación de políticas. Primero suprima el controlador de políticas agregado de todas las asignaciones de política mediante el comando **no police aggregate** antes de utilizar el comando **no qos aggregate-policer**.

Utiliza la página **QoS Aggregate Policer** (Controlador de políticas agregado de QoS) para especificar los límites de la amplitud de banda y definir las acciones que deben efectuarse en los paquetes que no cumplen los requisitos. Para abrir la página, haga clic en **Quality of Service→ Advanced QoS Mode→ Aggregate Policer** (Calidad de servicio→ Modo avanzado de QoS→ Controlador de políticas agregado) en la vista de árbol.

Ilustración 10-15. Página QoS Aggregate Policer (Controlador de políticas agregado de QoS)



Aggregate Policer Name (Nombre de controlador de políticas agregado): Especifica el nombre del controlador de políticas agregado.

Ingress Committed Information Rate (CIR) (Velocidad de información convenida de entrada [CIR]): CIR en bits por segundo.

Ingress Committed Burst Size (CBS) (Tamaño de transmisión en bloques convenido de entrada [CBS]): CBS en bytes por segundo.

Exceed Action (Acción excedida): Acción asignada a la información entrante que excede los límites del tráfico. Los valores posibles son:

Drop (Eliminar): Se eliminan los paquetes que exceden los límites.

Remark DSCP (Remarcar DSCP): Los paquetes que exceden los límites se reenvían con un valor DSCP con etiqueta o que se ha remarcado.

None (Ninguno): Los paquetes que exceden los límites se reenvían.

Remove (Eliminar): Si se selecciona esta opción, se elimina el controlador de políticas agregado de la tabla del controlador de políticas agregado.

Adición de un controlador de políticas agregado

1. Abra la página **QoS Aggregate Policer** (Controlador de políticas agregado de QoS).
2. Haga clic en **Add** (Agregar) para visualizar la página **Add Aggregate Policer** (Agregar controlador de políticas agregado).
3. Complete los campos del diálogo y haga clic en **Apply Changes** (Aplicar cambios).

Se crea el controlador de políticas agregado y el dispositivo se actualiza.

Supresión de un controlador de políticas agregado

1. Abre la página **QoS Aggregate Policer** (Controlador de políticas agregado de QoS).
2. Seleccione un controlador de políticas agregado en el menú descendente.
3. Haga clic en **Remove** (Eliminar) y, a continuación, en **Apply Changes** (Aplicar cambios).

Se suprime el controlador de políticas agregado y el dispositivo se actualiza.

Edición de un controlador de políticas agregado:

1. Abra la página **QoS Aggregate Policer** (Controlador de políticas agregado de QoS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Aggregate Policer Table** (Tabla de controlador de políticas agregado).
3. Edite la información de la tabla relativa a los controladores de políticas que desee editar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Definición de controladores de políticas agregados mediante los comandos de la CLI

Tabla 10-14. Comandos de la CLI para los controladores de políticas agregados

Comando de la CLI	Descripción
qos aggregate- policer *nombre_controlador_políticas_agregado velocidad_convenida_bps byte_transmisión en bloques_excedido acción_excedida* {drop | policed-dscp- transmit}	Define los parámetros que pueden aplicarse a varias clases de tráfico dentro de la misma asignación de política.
show qos aggregate police [*nombre_controlador_políticas_agregado*]	Muestra el parámetro del controlador de políticas agregado.

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

```
Console# qos aggregate policer policer1 124000 96000 exceed-action drop

Console> show qos aggregate police policer1

aggregate-policer policer1 96000 4800 exceed-action drop

not used by any policy map
```

Definición de políticas

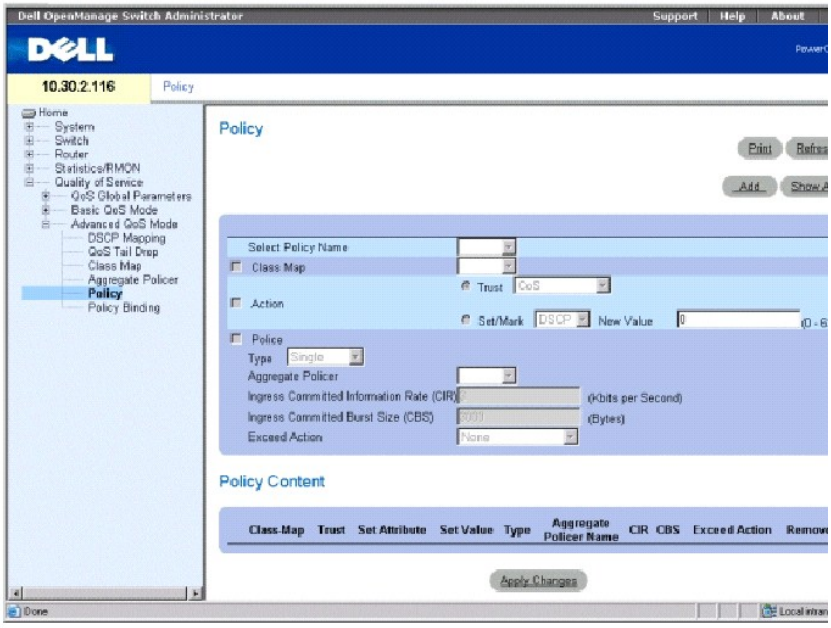
Una política es una recopilación de clases, cada una de las cuales es una combinación de asignación de clase y acción de QoS que debe aplicarse al tráfico coincidente. Las clases se aplican con la primera regla que se ajuste dentro de una política.

Antes de configurar las políticas para clases cuyos criterios de coincidencia se definan en una asignación de clase, debe definir una asignación de clase o bien especificar el nombre de la asignación de política que debe crearse, agregarse o modificarse. Las políticas de clase sólo pueden configurarse en una asignación de política si se han definido criterios de coincidencia para las mismas.

Un controlador de políticas agregado puede aplicarse a varias clases de la misma asignación de política, pero no se puede utilizar un controlador de políticas agregado en diferentes asignaciones de políticas diferentes. Defina un controlador de políticas agregado si el controlador de políticas se comparte entre varias clases. Los controladores de políticas de un puerto no pueden compartirse con otros controladores de políticas de otro dispositivo. El tráfico de dos puertos diferentes puede agregarse a efectos de control de políticas.

Para abrir la página Política de QoS, haga clic en **Quality of Service**→ **Advanced QoS Mode**→ **Policy** (Calidad de servicio→ Modo avanzado de QoS→ Política) en la vista de árbol.

Ilustración 10-16. Página QoS Policy (Política de QoS)



Select Policy Name (Seleccionar nombre de política): Selecciona un nombre de política.

Class Map (Asignación de clase): Selecciona una asignación de clase para la clase.

Action (Acción): Acción opcional para la clase. Los valores posibles son:

Trust (Confianza): Habilita el modo de confianza para la clase. Este comando se utiliza para distinguir el comportamiento de confianza de QoS para el tráfico especificado. Cuando se confía en un tipo especificado, el mecanismo de QoS asigna un paquete a una cola mediante el valor recibido o predeterminado y la asignación pertinente, tal como se define en la página **QoS Global Parameters** (Parámetros globales de QoS). Al designar la confianza, cabe la posibilidad de confiar solamente en el tráfico entrante con ciertos valores DSCP.

Set/Mark (Establecer/marcar): Configura manualmente la confianza.

New Value (Nuevo valor): Valor del método **Set/Mark** (Establecer/marcar) seleccionado.

Police Type (Tipo de política): Tipo de controlador de políticas para la clase. Los valores posibles son:

Aggregate (Agregado): Configura la clase que debe utilizar un controlador de políticas agregado seleccionado en el menú descendente. Se define un controlador de políticas agregado si el controlador de políticas se comparte con varias clases. El tráfico de puertos diferentes puede configurarse a efectos de control de políticas. Un controlador de políticas agregado puede aplicarse a varias clases de la misma asignación de política, pero no puede utilizarse en asignaciones de política diferentes.

Single (Único): Configura la clase para que utilice acciones excedidas y velocidades de información configuradas manualmente.

Aggregate Policer (Controlador de políticas agregado): Controladores de políticas agregados definidos por el usuario.

Ingress Committed Information Rate (CIR) (Velocidad de información convenida de entrada [CIR]): CIR en bits por segundo. Este campo sólo es importante cuando el valor de **Police** (Control de políticas) es **Single** (Único).

Ingress Committed Burst Size (CBS) (Tamaño de transmisión en bloques convenido de entrada [CBS]): CBS en bytes por segundo. Este campo sólo es importante cuando el valor de **Police** (Control de políticas) es **Single** (Único).

Exceed Action (Acción excedida): Acción asignada a los paquetes entrantes que excedan el valor de CIR. Este campo sólo es importante cuando el valor de **Police** (Control de políticas) es **Single** (Único). Los valores posibles son:

Drop (Eliminar): Elimina los paquetes que exceden el valor de CIR.

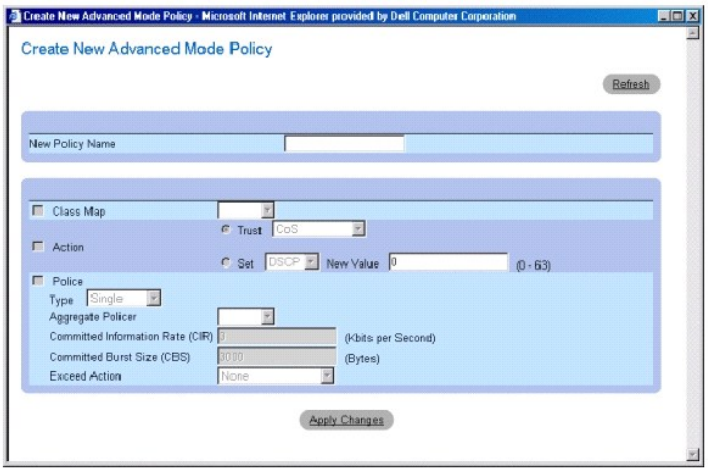
Remark DSCP (Remarcar DSCP): Vuelve a marcar los valores DSCP de los paquetes que excedan el valor de CIR que se haya definido.

None (Ninguno): Reenvía los paquetes que exceden el valor de CIR que se haya definido.

Adición de una política y su primera clase

1. Abra la página **QoS Policy** (Política de QoS).
2. Haga clic en **Add** (Agregar) para visualizar la página **Create New Advanced Mode Policy** (Crear nueva política de modo avanzado).

Ilustración 10-17. Página Create New Advanced Mode Policy (Crear nueva política de modo avanzado)



3. Escriba un nombre para la política en el campo **New Policy Name** (Nombre de nueva política).
4. Realice uno de los siguientes pasos:
   - Para configurar una asignación de clase para la clase, haga clic en **Class Map** (Asignación de clase) y seleccione una de las que aparecen en el menú descendente.
   - Para configurar una acción de confianza para la clase, haga clic en **Action** (Acción), en **Trust** (Confianza) y seleccione un método de confianza en el menú descendente.
   - Para configurar la opción de establecer/marcar acciones, haga clic en **Set** (Establecer), seleccione un método en el menú descendente y escriba un valor en el campo **New Value** (Nuevo valor).
5. Si desea configurar el control de políticas para la clase, haga clic en **Police** (Control de políticas) y seleccione un tipo de controlador de políticas en el menú descendente.
   - Para un controlador de políticas agregado, seleccione uno de los que aparecen en el menú descendente **Aggregate Policer** (Controlador de políticas agregado).
   - Para un controlador de políticas único, complete la información de los campos **Committed Information Rate (CIR)** (Velocidad de información convenida [CIR]), **Committed Burst Size (CBS)** (Tamaño de transmisión en bloques convenido [CBS]) y **Exceed Action** (Acción excedida).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se crean la política y su primera clase y el dispositivo se actualiza.

Adición de una clase

1. Abra la página **QoS Policy** (Política de QoS).
2. En el menú descendente, seleccione una política.
3. Edite la información de los campos de la página y haga clic en **Apply Changes** (Aplicar cambios).

Se agrega la clase a la política y el dispositivo se actualiza.

Supresión de políticas

1. Abra la página **QoS Policy** (Política de QoS).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Policy Table** (Tabla de políticas).
3. Haga clic en **Remove** (Eliminar) para cada una de las políticas que deban suprimirse y, a continuación, haga clic en **Apply Changes** (Aplicar cambios).

Se suprimen las políticas del sistema y el dispositivo se actualiza.

Definición de políticas mediante los comandos de la CLI

Tabla 10-15. Comandos de la CLI para las políticas

Comando de la CLI	Descripción
`policy-map` *nombre_asignación_política*	Crea una asignación de política y entra en el modo de configuración de asignación de políticas.
`class` *nombre_asignación_clase* [`access-group` *nombre_acl*]	Define la clasificación del tráfico y entra en el modo de configuración de clase de asignación de políticas.
`trust [cos | dscp | tcp-udp-port]`	Configura el estado de confianza, que selecciona el valor que QoS utiliza como origen del valor DSCP interno.
`set {dscp` *dscp_nuevo* `| queue` *id_cola* `| cos` *cos_nuevo*`}`	Establece nuevos valores en el paquete de IP. Nota: Este comando y el comando trust se excluyen mutuamente.
`police` *velocidad_convenida_bps transmisión en bloques_convenida_ byte* [`exceed-action {drop | policed-dscp- transmit}`]	Define un controlador de políticas único para el tráfico clasificado.
`qos aggregate-policer` *nombre_controlador_políticas_agregado velocidad_convenida_bps transmisión en bloques_convenida_byte* `exceed-action {drop | policed-dscp-transmit}`	Define los parámetros que pueden aplicarse a varias clases de tráfico dentro de la misma asignación de política.

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

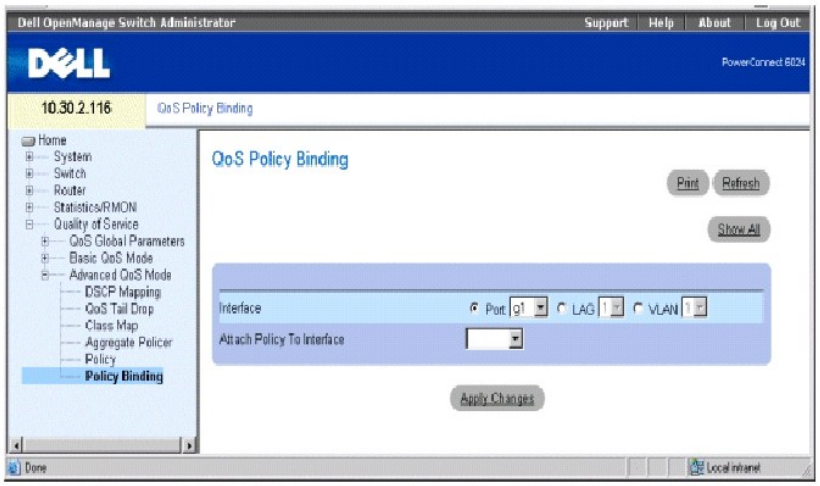
```
Console (config)# policy map policy1

Console (config-pmap)# class class1 access-group dell

Console (config-pmap)# trust cos

Console (config-pmap)# set dscp 56

Console (config-pmap)# police 124000 96000 exceed-action drop
```

```
Console (config-pmap)# exit


Console (config)# qos aggregate-policer policer1 124000 96000 exceed-action drop
```

Aplicación de las políticas a las interfaces

Utilice la página **QoS Policy Binding** (Vinculación de políticas de QoS) para implementar políticas en las interfaces. Para abrir la página, haga clic en **Quality of Service→ Advanced QoS Mode→ Policy Binding** (Calidad de servicio→ Modo avanzado de QoS→ Vinculación de políticas) en la vista de árbol.

Ilustración 10-18. Página QoS Policy Binding (Vinculación de políticas de QoS)



Interface (Interfaz): Selecciona una interfaz.

Attach Policy to Interface (Conectar política a interfaz): La política implementada en la interfaz.

NOTA: Una asignación de política que contiene un comando de configuración de clase de asignación de política `set` o `trust`, o que tiene una clasificación ACL que no se puede conectar a una interfaz de salida.

Conexión de una política a una interfaz

1. Abra la página **QoS Policy Binding** (Vinculación de políticas de QoS).
2. Seleccione un tipo de interfaz.

   Sólo se admite una asignación de política por interfaz por dirección. No obstante, puede aplicarse la misma asignación de política a varias interfaces y direcciones.
3. Seleccione el número de puerto, LAG o VLAN en el menú descendente adecuado.
4. Seleccione una política en el menú descendente **Attach Policy to Interface** (Conectar política a interfaz).
5. Haga clic en **Apply Changes** (Aplicar cambios).

   Se implementa la política seleccionada en la interfaz seleccionada y el dispositivo se actualiza.

Eliminación de políticas de las interfaces

1. Abra la página **QoS Policy Binding** (Vinculación de políticas de QoS).

2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **PTI Reference Table** (Tabla de referencia de PTI).
3. Haga clic en **Remove** (Eliminar) para cada una de las interfaces cuyas políticas desee eliminar y haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la política del puerto, pero permanece en el sistema.

Aplicación de las políticas a las interfaces mediante los comandos de la CLI

Tabla 10-16. Comandos de la CLI para aplicar políticas a interfaces

Comando de la CLI	Descripción
`service-policy input` *`nombre-asignación-política`*	Aplica una asignación de política a la entrada o salida de una interfaz concreta.

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

```
Console (config-if)# service-policy input policy1
```

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del conmutador

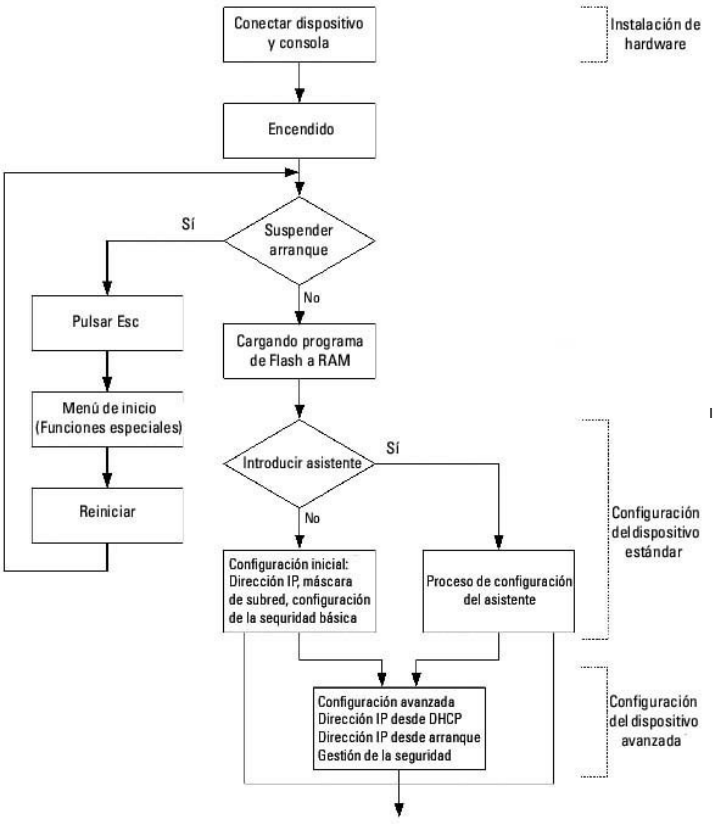
Sistemas Dell PowerConnect 6024/6024F

En esta sección se describe la configuración inicial del dispositivo.

Tras efectuar todas las conexiones externas, debe conectar un terminal al dispositivo para poder supervisar el arranque y demás procedimientos. El orden de instalación y los procedimientos de configuración se ilustran en la Ilustración 5-1. Para la configuración inicial, se lleva a cabo la configuración de dispositivo estándar. Puede realizar otras funciones, pero ello implica suspender el proceso de instalación y provoca que el sistema se reinicie. La realización de otras funciones se describe más adelante en esta misma sección.

AVISO: Antes de continuar, lea las notas de la versión de este producto. Puede descargar estas notas del sitio web **support.dell.com**.

Ilustración 5-1. Flujo de trabajo de configuración e instalación



Información general sobre la configuración

El conmutador tiene una configuración de la instalación y características predefinidas.

Negociación automática

La negociación automática permite a un dispositivo anunciar los modos de funcionamiento y compartir información con otro dispositivo que comparta un segmento de conexión punto a punto. Esto configura automáticamente ambos dispositivos para que saquen el máximo provecho de sus posibilidades.

La negociación automática se lleva a cabo totalmente dentro de las capas físicas durante la iniciación de la conexión, sin que ello represente ningún aumento adicional de la actividad general en las capas de protocolo MAC o superiores. La negociación automática permite a los puertos realizar las acciones siguientes:

- Anunciar sus posibilidades
- Confirmar la recepción y la comprensión de los modos comunes de funcionamiento que comparten ambos dispositivos
- Rechazar la utilización de los modos de funcionamiento que no compartan ambos dispositivos
- Configurar cada puerto para el nivel de modo de funcionamiento más alto que admitan ambos puertos

Si conecta un puerto del conmutador a la NIC (Tarjeta de interfaz de red) de una estación de trabajo o de un servidor que no admitan la negociación automática o que no estén establecidos en la negociación automática, tanto el puerto de conmutación como la NIC deberán establecerse manualmente, mediante la interfaz del explorador de la web o los comandos de la CLI, en la misma velocidad y el mismo modo dúplex.

AVISO: Si la estación del otro lado de la conexión intenta realizar la negociación automática con un puerto que se haya configurado manualmente en dúplex completo, la estación intentará funcionar en modo dúplex medio como resultado de la negociación automática. La discrepancia resultante puede producir una pérdida significativa de tramas. Esto es inherente a la norma de negociación automática.

Configuración predeterminada del puerto de conmutación

En la tabla siguiente se describe la configuración predeterminada del puerto del conmutador.

Tabla 5-1. Configuración predeterminada del puerto

Función	Configuración predeterminada
Velocidad y modo del puerto	Negociación automática de 1000M
Estado de reenvío del puerto	Activado
Prevención del bloqueo de la cabecera de línea	Activada
Control de flujo	Desactivado
Contrapresión	Desactivada

En el ejemplo siguiente se describe cómo cambiar la velocidad del puerto g1 utilizando comandos de la CLI:

```
Console (config)# interface ethernet g1

Console (config-if)# speed 100
```

En el ejemplo siguiente se describe cómo habilitar el control de flujo del puerto g1 utilizando comandos de la CLI:

```
Console (config)# interface ethernet g1

Console (config-if)# flowcontrol on
```

En el ejemplo siguiente se describe cómo habilitar la contrapresión del puerto g1 utilizando comandos de la CLI: La contrapresión sólo funciona para el modo de funcionamiento de 10 Mbps.

```
Console (config)# interface ethernet g1

Console (config-if)# speed 10

Console (config-if)# back-pressure
```

Configuración de la conexión de terminales

La configuración del conmutador requiere los parámetros de conexión de terminal siguientes:

- no parity (sin paridad)
- one stop bit (un bit de parada)
- 8 data bits (8 bits de datos)

Velocidad en baudios

Las velocidades en baudios pueden cambiarse manualmente por cualquiera de los valores siguientes:

- 2400
- 4800
- 9.600
- 19200
- 115,200

NOTA: La velocidad en baudios predeterminada es de 115.200.

NOTA: El cierre del dispositivo no devuelve la velocidad en baudios predeterminada. Debe configurarse específicamente.

NOTA: El valor de la velocidad en baudios de la consola no se guarda en el archivo de configuración general del conmutador. Se almacena directamente en el dispositivo de memoria no volátil del conmutador.

A continuación figura un ejemplo de configuración en el que se cambia la velocidad en baudios predeterminada mediante comandos de la CLI:

```
Console# configure

Console (config)# line console

Console (config-line)# speed 115200
```

Otros requisitos de la configuración

Para la descarga y del software incorporado y la configuración del dispositivo se requiere lo siguiente:

- Terminal ASCII (o emulación) conectada al puerto serie (cable cruzado) de la parte frontal de la unidad.

- Dirección IP asignada al conmutador a efectos de control remoto de dispositivos mediante Telnet, SSH, etc.

NOTA: El proceso de configuración sólo define un puerto.

Inicio del conmutador

Cuando se activa la alimentación y el terminal local ya está conectado, en el conmutador se ejecuta la autoprueba de encendido (POST). POST se ejecuta cada vez que el dispositivo se inicia y comprueba los componentes de hardware para determinar si el dispositivo está completamente operativo antes de iniciarse por completo.

Si se detecta un problema grave, el flujo del programa se detiene. Si POST se pasa correctamente, se carga una imagen ejecutable válida en la RAM.

Los mensajes de POST se muestran en el terminal e indican si la prueba ha finalizado con éxito o no.

Realice los pasos siguientes para iniciar el conmutador:

1. Asegúrese de que el cable ASCII esté conectado a la terminal.
2. Conecte el suministro de energía al conmutador.
3. Encienda el conmutador.

Mientras se inicia el conmutador, la prueba de arranque efectúa en primer lugar un recuento de la memoria disponible del dispositivo y, a continuación, prosigue con el arranque. En la pantalla que figura a continuación se muestra un ejemplo de la POST que se puede ver en el terminal:

```
Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

Testing CPU PCI Bus Device Configuration.........PASS



BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31



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

El proceso de inicio dura aproximadamente 30 segundos.

El mensaje de autoarranque que aparece al final de la POST (véanse las últimas líneas) indica que no se ha encontrado ningún problema durante el arranque.

Durante el arranque, puede utilizar el menú **Inicio**, si fuera necesario, para ejecutar procedimientos especiales. Para entrar en el menú **Inicio**, pulse <Esc> o <Intro> en los dos primeros segundos posteriores a la aparición del mensaje de autoarranque. Para obtener información sobre el menú **Inicio**, consulte el apartado Funciones del menú de inicio.

Si no interrumpe el inicio del sistema pulsando <Esc> o <Intro>, el sistema sigue funcionando y descomprime y carga el código en la RAM. El código se inicia ejecutándose desde la RAM y se muestra una lista numerada de los puertos del sistema y sus estados (activo o inactivo).

NOTA: La siguiente pantalla es un ejemplo de configuración. Algunos elementos, como direcciones, versiones y fechas, pueden diferir para cada dispositivo.

```
Preparing to decompress...



Decompressing SW from image-1

d04000

OK

Running from RAM...



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

** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 **

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



HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18
```

```
Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed


Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

Console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2
```

Tras arrancar completamente el conmutador, aparece un indicador del sistema (Console>) y, a continuación, puede utilizar el terminal local para empezar a configurar el conmutador. No obstante, antes de configurar el conmutador, compruebe que la versión de software instalada en el dispositivo sea la última. En caso contrario, descargue e instale la última versión. Consulte el apartado Descarga del software y reinicio .

Descripción general de la configuración

El conmutador es compatible con el puerto de gestión OOB (Fuera de banda) Ethernet a 10/100 Mbps que está conectado directamente al dispositivo. Este puerto admite aplicaciones de gestión del sistema. El sistema considera el puerto fuera de banda como una interfaz IP y a través del mismo se puede acceder a todas las interfaces de gestión. El puerto de fuera de banda no admite tráfico del usuario. Los paquetes no se conmutan ni se direccionan desde ningún puerto en banda (puerto Ethernet distinto de OOB) hasta el puerto fuera de banda.

Antes de configurar el dispositivo, obtenga la siguiente información del administrador de red.

- La dirección IP del puerto fuera de banda
- La máscara de subred IP de la red
- La dirección IP de la puerta de enlace predeterminada (enrutador de siguiente salto) para configurar la ruta predeterminada

Existen dos tipos de configuración: La configuración inicial consta de funciones de configuración con consideraciones de seguridad básica, mientras que la configuración avanzada incluye configuración IP dinámica y más consideraciones de seguridad avanzadas.

AVISO: Después de realizar cualquier cambio en la configuración, debe guardarse la configuración nueva antes de reiniciar. Para guardar la configuración, escriba:

```
Console# copy running-config startup-config
```

Configuración inicial

La configuración inicial se puede llevar a cabo mediante el uso del Asistente para la instalación o la CLI. El Asistente para la instalación se inicia automáticamente cuando el archivo de configuración del dispositivo está vacío. La CLI se puede invocar pulsando [ctrl+z].

En esta guía se muestra cómo utilizar el Asistente para la instalación para la configuración inicial del dispositivo. El Asistente para la instalación configura los campos siguientes:

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

Después de que el dispositivo haya completado la POST y se haya iniciado, aparecerá la siguiente información:

```
Welcome to Dell Easy Setup Wizard (Bienvenido al Asistente para la instalación fácil de Dell)

The Setup Wizard guides you through the initial switch configuration, and gets you up and running easily and quickly (El Asistente para
la instalación le muestra los pasos de la configuración inicial del conmutador y le permite empezar a trabajar de manera fácil y rápida).
You can also skip the setup wizard, and enter CLI mode to manually configure the switch if you prefer (También puede omitir el Asistente
para la instalación y entrar en el modo CLI para configurar el conmutador manualmente si lo desea).

You can exit the Setup Wizard at any time by entering [ctrl+Z] (Puede salir del Asistente para la instalación en cualquier momento
pulsando [ctrl+Z]).

The system will prompt you with a default answer; by pressing enter, you accept the default (El sistema le solicitará una respuesta
predeterminada; si pulsa Intro, aceptará el valor predeterminado).

After you configure basic settings using the Setup Wizard, you can manage the device from the Out-of-band management port. (Después de
configurar los parámetros básicos mediante el Asistente para la instalación, podrá gestionar el dispositivo desde el puerto de gestión
fuera de banda).

Would you like to enter the setup wizard? (¿Desea entrar en el asistente para la instalación?) [Y/N] Y (S/N [S])
```

1. Si escribe [N], saldrá del Asistente para la instalación. Si no responde nada en un plazo de 60 segundos, el Asistente para la instalación se cerrará automáticamente y aparecerá el indicador de la consola de la CLI. Si escribe [Y], el Asistente para la instalación le guiará de manera interactiva por todo el proceso de configuración inicial del dispositivo.

NOTA: Si no hay ninguna respuesta en el plazo de 60 segundos, y hay un servidor BootP en la red, se recuperará una dirección del servidor BootP.

NOTA: El usuario puede salir del Asistente para la instalación en cualquier momento pulsando [ctrl+z].

Paso 1 del asistente

Si escribe [Y], aparece el siguiente mensaje:

The system is not setup for SNMP management by default (El sistema no está configurado de manera predeterminada para la gestión SNMP). To manage the switch using SNMP (required for Dell Network Manager) you can: (Para gestionar el conmutador con SNMP (obligatorio para Dell Network Manager) puede:)

- Setup the initial SNMP version 2 account now (Configurar ahora la cuenta inicial de SNMP versión 2).
- Return later and setup the SNMP version 2 account. (Volver después y configurar la cuenta de SNMP versión 2). (For more information on setting up a SNMP version 2 account, see the user documentation) (Para obtener más información sobre la configuración de una cuenta de SNMP versión 2, consulte la documentación del usuario).

Would you like to setup the SNMP management interface now? (¿Desea configurar ahora la interfaz de gestión SNMP?) [Y/N] Y (S/N [S])

2. Escriba [N] para pasar al paso 2 o [Y] para continuar con el Asistente para la instalación. Si escribe [Y], aparecerá el siguiente mensaje:

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. (Para configurar la cuenta de gestión SNMP, debe especificar la dirección IP del sistema de gestión y la "cadena de comunidad" o contraseña que el sistema de gestión en concreto utilizar para acceder al conmutador). The wizard automatically assigns the highest access level [Privilege Level 15] to this account (El asistente asigna automáticamente el nivel de acceso más alto [Nivel de privilegio 15] a esta cuenta). You can use Dell Network Manager or other management interfaces to change this setting later, and to add additional management system later (Puede utilizar Dell Network Manager u otras interfaces de gestión para modificar este valor más tarde así como para agregar un sistema de gestión adicional posteriormente). For more information on adding management systems, see the user documentation (Si desea obtener más información sobre cómo agregar sistemas de gestión, consulte la documentación del usuario).

To add a management station: (Para agregar una estación de gestión:)

Please enter the SNMP community string to be used (Introduzca la cadena de comunidad SNMP que vaya a utilizar):

Please enter the Management System IP address(A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station (Introduzca la dirección IP del sistema de gestión (A.B.C.D.) o el comodín (0.0.0.0) para gestionar desde cualquier estación de gestión):

3. Escriba lo siguiente:
   - La cadena de comunidad SNMP del usuario como, por ejemplo, MYSETUPWIZARD .
   - La dirección IP del sistema de gestión como, por ejemplo, 0.0.0.0 .
4. Pulse Intro.

Paso 2 del asistente

Aparece el siguiente mensaje:

Now we need to setup your initial privilege (Level 15) user account (Ahora es necesario configurar su cuenta de usuario de privilegio inicial (Nivel 15). This account is used to login to the CLI and Web interface (Esta cuenta se utiliza para iniciar la sesión de la CLI y la interfaz web). You may setup other accounts and change privilege levels later (Podrá configurar otras cuentas y cambiar los niveles de privilegio más tarde). For more information on setting up user accounts and changing privilege levels, see the user documentation (Si desea obtener más información sobre la configuración de las cuentas de usuario y la modificación de los niveles de privilegio, consulte la documentación del usuario).

To setup a user account: (Para configurar una cuenta de usuario:)

Please enter the user name: (Introduzca el nombre del usuario:)

Please enter the user password: (Introduzca la contraseña del usuario:)

Please reenter the user password: (Vuelva a introducir la contraseña del usuario:)

5. Escriba lo siguiente:

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

NOTA: Si la primera y la segunda contraseña que escribe no son idénticas, se le pide que introduzca contraseñas idénticas.

6. Pulse la tecla **Intro**.

Paso 3 del asistente

7. Aparece el siguiente mensaje:

```
Next, an IP address is setup (A continuación, se configura una dirección IP). The IP address is defined on the OOB port (La dirección IP
se define en el puerto OOB). This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch (Ésta es
la dirección IP que se utiliza para acceder a la CLI, la interfaz web o la interfaz SNMP del conmutador).

To setup an IP address: (Para configurar una dirección IP:)

Please enter the device IP address(A.B.C.D) (Introduzca la dirección IP del dispositivo (A.B.C.D.):

Please enter the IP subnet mask (A.B.C.D or /nn): (Introduzca la máscara de subred IP (A.B.C.D o /nn):)
```

8. Especifique la dirección IP y la máscara de subred, por ejemplo, 192.168.1.100 como dirección IP y 255.255.255.0 como máscara de subred IP.

NOTA: Cada parte de la dirección IP debe empezar con un número distinto de cero. Por ejemplo, las direcciones IP 001.100.192.6 y 192.001.10.3 no son válidas.

9. Pulse la tecla INTRO.

Paso 4 del asistente

Aparece el siguiente mensaje:

```
Finally, setup the default gateway (Por último, configure la puerta de enlace predeterminada). Please enter the gateway IP address from
which this network is reachable (e.g. 192.168.1.1): (Introduzca la dirección IP de la puerta de enlace desde la que se puede acceder a
esta red (por ejemplo, 192.168.1.1):)
```

10. Especifique la puerta de enlace predeterminada.
11. Pulse Intro. Aparece la siguiente información (según los parámetros descritos en el ejemplo):

```
This is the configuration information that has been collected: (Ésta es la información de configuración que se ha recopilado:)

SNMP Interface = MYSETUPWIZARD@0.0.0.0 (Interfaz SNMP = MYSETUPWIZARD@0.0.0.0)

User Account setup = admin (Configuración de la cuenta de usuario = admin)

Password = ********** (Contraseña = **********)

Management IP address = 192.168.1.100 255.255.255.0 (Dirección IP de gestión = 192.168.1.100 255.255.255.0)

Default Gateway = 192.168.1.1 (Puerta de enlace predeterminada = 192.168.1.1)
```

Paso 5 del asistente

Aparece el siguiente mensaje:

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file (Si la
información es correcta, seleccione (S) para guardar la configuración y copiarla en el archivo de configuración de inicio). If the
information is incorrect, select (N) to discard configuration and restart the wizard: (Si la información no es correcta, seleccione (N)
para rechazar la configuración y reiniciar el asistente:) [Y/N] ([S/N])
```

12. Escriba [N] para omitir el reinicio del Asistente para la instalación o [Y] para completar el asistente para la instalación. Si escribe [Y]. aparecerá el siguiente mensaje:

```
Configuring SNMP management interface (Configurando la interfaz de gestión SNMP).

Configuring user account....... (Configurando la cuenta de usuario.......)

Configuring IP and subnet...... (Configurando IP y la subred......)

.............................

Thank you for using Dell Easy Setup Wizard (Gracias por utilizar el Asistente para la instalación fácil de Dell). You will now enter CLI
mode (Ahora entrará en el modo CLI).
```

Paso 6 del asistente

Aparece el siguiente indicador de la CLI.

Ahora, el dispositivo se puede gestionar desde el puerto de la consola ya conectado o remotamente, a través de la interfaz fuera de banda definida durante la configuración inicial.

Configuración avanzada

En esta sección se proporciona información sobre la asignación dinámica de direcciones IP y la gestión de seguridad basada en el mecanismo de autenticación, autorización y contabilidad (AAA).

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

Recuperación de una dirección IP desde un servidor DHCP

Cuando se usa el protocolo DHCP para recuperar una dirección IP, el dispositivo actúa como un cliente DHCP.

Para recuperar una dirección IP desde un servidor DHCP, lleve a cabo los pasos siguientes:

1. Seleccione y conecte un puerto cualquiera a un servidor DHCP o a una subred que disponga de un servidor DHCP, para poder recuperar la dirección IP.
2. Escriba 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 (en un puerto en banda):

```
Console# configure

Console (config)# interface ethernet g1

Console (config-if)# ip address dhcp hostname <string>

Console (config-if)# exit
```

- Asignación de direcciones IP dinámicas (en un puerto fuera de banda):

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address dhcp hostname dell

Console (config-oob)# exit

Console (config)# exit
```

La interfaz recibe la dirección IP automáticamente.

3. Para verificar la dirección IP, escriba el comando **show ip interface** en el indicador del sistema, tal como se muestra en el ejemplo siguiente.

```
Console# show ip interface

IP Address I/F Type Directed Broadcast

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

100.1.1.1/24 vlan 1 static disable



OOB ip interfaces



Gateway IP Address Activity status

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

10.6.12.1 active
```

```
IP Address I/F Type

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

10.6.12.20/24 Oob-eth 1 dhcp
```

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

NOTA: Cuando copie archivos de configuración, evite utilizar un archivo de configuración que contenga una instrucción para habilitar DHCP en una interfaz que se conecte al mismo servidor DHCP, o que contenga una configuración idéntica. En esta instancia, el conmutador recupera el nuevo archivo de configuración y arranca desde el mismo. A continuación, el conmutador habilita DHCP, tal como se indica en el nuevo archivo de configuración y DHCP le da instrucciones para que recargue de nuevo el mismo archivo.

Recepción de una dirección IP desde un servidor BOOTP

Se admite el protocolo BOOTP estándar y permite al conmutador descargar automáticamente su configuración de sistema principal IP desde cualquier servidor BOOTP estándar en la red. En este caso, el dispositivo actúa como un cliente BOOTP.

Para recuperar una dirección IP desde un servidor BOOTP:

1. Seleccione y conecte un puerto cualquiera a un servidor BOOTP o a una subred que disponga de uno, para poder recuperar la dirección IP.
2. En el indicador del sistema escriba el comando **delete startup configuration** para suprimir de la flash la configuración de inicio.

   El dispositivo se reinicia sin configuración alguna y 60 segundos después empieza a emitir solicitudes BOOTP.

   El dispositivo recibe la dirección IP automáticamente.

NOTA: Cuando comienza el reinicio del dispositivo, cualquier entrada que se efectúe en el terminal ASCII o mediante el teclado cancela, automáticamente, el proceso de BOOTP antes de que finalice y el dispositivo no recibe ninguna dirección IP del servidor BOOTP.

En el ejemplo siguiente se ilustra el 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, escriba el comando **show ip interface**.

En este punto, el dispositivo está configurado con una dirección IP.

Configuración de contraseñas y gestión de la seguridad

La seguridad del sistema se maneja a través del mecanismo de autenticación, autorización y contabilidad (AAA) que gestiona los derechos de acceso de usuarios, privilegios y métodos de gestión. El método AAA utiliza bases de datos de usuarios tanto locales como remotas. El cifrado de datos se lleva a cabo a través del mecanismo SSH.

El sistema se entrega sin que se haya configurado la contraseña predeterminada; todas las contraseñas son contraseñas definidas por el usuario. Si se pierde una contraseña definida por el usuario, puede invocarse un procedimiento de recuperación de contraseña desde el menú **Startup** (Inicio). El procedimiento sólo puede aplicarse al terminal local y permite un sólo acceso al dispositivo desde éste sin que deba escribirse ninguna contraseña.

Configuración de contraseñas de seguridad

Es posible configurar las contraseñas de seguridad para los servicios siguientes:

- Consola
- Telnet
- SSH
- HTTP
- HTTPS

NOTA: Las contraseñas están definidas por el usuario.

NOTA: Al crear un nombre de usuario, la prioridad predeterminada es 1 , que otorga acceso pero no derechos de configuración. Debe establecerse una prioridad de 15 para otorgar acceso y derechos de configuración del dispositivo. Aunque es posible asignar el nivel de privilegio 15 a los nombres de usuario sin definir ninguna contraseña, es recomendable asignar siempre una contraseña. Si no se especifica ninguna contraseña, los usuarios privilegiados pueden acceder a la interfaz web sin contraseña.

Configuración de una contraseña inicial de consola

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

```
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 george
```

- Cuando se conecte inicialmente a un dispositivo a través de una sesión de consola, escriba **george** cuando se le pida la contraseña.
- Cuando cambie el modo de un dispositivo a enable (habilitado), escriba george cuando se le pida la contraseña.

Configuración de una contraseña inicial Telnet

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

```
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 bob
```

- Cuando se conecte inicialmente a un dispositivo a través de una sesión de Telnet, escriba bob cuando se le pida la contraseña.
- Cuando cambie el modo de un dispositivo a `enable`, escriba bob.

Configuración de una contraseña inicial SSH

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

```
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.
```

- Cuando se conecte inicialmente a un dispositivo a través de una sesión de SSH, escriba jones cuando se le pida la contraseña.
- Cuando cambie el modo de un dispositivo a `enable`, escriba jones.

Configuración de una contraseña inicial HTTP

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

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

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

Configuración de una contraseña inicial HTTPS:

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

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

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

NOTA: Deberá generar un nuevo certificado criptográfico cada vez que actualice (instale una nueva versión) la aplicación del software de control en el dispositivo.

Escriba los comandos siguientes una vez cuando configure la utilización de una sesión de consola, Telnet o SSH para poder utilizar una sesión HTTPS.

En el explorador de la web habilite SSL 2.0 o posterior para que pueda visualizarse el contenido de la página.

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

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

Al habilitar inicialmente una sesión HTTP o HTTPS, escriba `admin` como nombre de usuario y `user1` como contraseña.

NOTA: Los servicios http y https requieren el acceso de nivel 15 y conectarse directamente al acceso de nivel de configuración.

Descarga del software y reinicio

Descarga del software mediante XModem

Esta sección contiene instrucciones para descargar software del dispositivo (imágenes del sistema y de arranque) mediante XModem, que es un protocolo de transferencia de datos para actualizar archivos de configuración de copia de seguridad.

Para descargar un archivo de arranque mediante XModem:

1. Escriba el comando **console# xmodem: boot**.

   El conmutador ya está preparado para recibir el archivo mediante el protocolo XModem y aparece un texto parecido al siguiente:

   ```
   Console# copy xmodem: boot
   ```

   ```
   Please download program using XMODEM. (Descargue el programa utilizando un XMODEM.)
   ```

   ```
   Console#
   ```

2. Especifique la ruta de acceso del archivo fuente en 20 segundos.

   Si no especifica la ruta de acceso en 20 segundos, se agota el tiempo de espera del comando.

Para descargar una imagen de software mediante XModem:

1. Escriba el comando **console# xmodem: image**.

   El conmutador ya está preparado para recibir el archivo mediante el protocolo XModem.

2. Especifique la ruta de acceso del archivo fuente para comenzar el proceso de transferencia.

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

```
Console# copy xmodem: image

Please download program using XMODEM. (Descargue el programa utilizando un XMODEM.)

Console#
```

Descarga del software a través de un servidor TFTP

Esta sección contiene instrucciones para descargar software del conmutador (imágenes del sistema y arranque) a través de un servidor TFTP. El servidor TFTP se debe configurar antes de descargar el software.

El conmutador se inicia y se activa tras descomprimir la imagen del sistema del área de la memoria flash en la que se ha almacenado una copia de la imagen del sistema. Cuando se descarga una nueva imagen, se guarda en la otra área asignada para la copia adicional de la imagen del sistema.

En el próximo arranque, el conmutador descomprime y ejecuta la imagen actual activa actualmente a menos que se especifique lo contrario.

Para descargar una imagen a través del servidor TFTP:

1. Compruebe que se haya configurado una dirección IP en uno de los puertos de dispositivo y que un comando ping ejecutado contra un servidor TFTP obtenga una respuesta satisfactoria.
2. Asegúrese de que el archivo que deba descargarse (el archivo de DOS) se guarde en el servidor TFTP.
3. Escriba el comando **console# show version** para verificar qué versión de software se está ejecutando actualmente en el dispositivo.

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

```
Console# show version
SW version 3.31.42 (date 22-Jul-2003 time 13:42:41)
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20)
HW version
```

4. Escriba el comando **console# show bootvar** para verificar qué imagen del sistema está 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. Escriba el comando **console# copy tftp://{tftp address}/{file name} image** para copiar una nueva imagen del sistema al dispositivo.

   Cuando se descarga una nueva imagen, se guarda en la otra área asignada para la copia de la imagen del sistema (image-2, tal como se indica en el ejemplo). A continuación se muestra un ejemplo de la información que aparece:

```
Console# copy tftp://176.215.31.3/file1 image
Accessing file file1 on 176.215.31.3...



Loading file1 from
176.215.31.3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Los signos de admiración indican que hay en curso un proceso de copia. Un punto indica que se ha agotado el tiempo de espera del proceso de copia. Si aparecen muchos puntos en una fila, significa que el proceso de copia ha fallado.

6. Seleccione la imagen para el siguiente inicio escribiendo el comando del sistema **boot**. Después de este comando, escriba el comando **console# show bootvar** para verificar que la copia indicada como parámetro en el comando del sistema boot esté seleccionada para el arranque siguiente.

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

```
Console# boot system image-2
console# sh bootvar
Images currently available on the Flash
Image-1 active
Image-2 not active (selected for next boot)
```

   Si la imagen para el siguiente arranque se selecciona mediante el comando del sistema boot, el sistema se arranca desde la imagen que esté activa actualmente (image-1, tal como se indica en el ejemplo).

7. Escriba el comando **reload**. Aparece el siguiente mensaje:

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

8. Escriba **Y** para reiniciar el conmutador.

Descarga de la imagen de inicio

La imagen de inicio de la memoria flash se actualiza al cargar y programar en ella una nueva imagen de inicio procedente del servidor TFTP. La imagen de arranque se carga al encender el conmutador.

Para descargar un archivo de arranque a través del servidor TFTP:

1. Compruebe que se haya configurado una dirección IP en uno de los puertos del dispositivo y que un comando ping ejecutado contra un servidor TFTP obtenga una respuesta satisfactoria.
2. Asegúrese de que el archivo que deba descargarse (el archivo **.rfb**) se guarde en el servidor TFTP.
3. Escriba el comando **console# show version** para verificar qué versión de arranque se está ejecutando actualmente en el dispositivo.

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

```
Console# show version
SW version 3.31.42 (date 22-Jul-2003 time 13:42:41)
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20)
HW version 00.00.01 (date 01-May-2003 time 12:12:20)
```

4. Escriba el comando **console# copy tftp://{tftp address}/{file name} boot** para copiar la imagen de arranque en el conmutador.

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

```
Console# copy tftp://176.215.31.3/6024_boot-10013.rfb
Erasing
file...done. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 393232 bytes copied in 00:00:05 [hh:mm:ss]
```

5. Escriba el comando **reload**.

   Aparece el siguiente mensaje:

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

6. Escriba **Y** para reiniciar el conmutador.

Proceso de configuración de ejemplo

En esta sección se proporcionan los pasos básicos para establecer una conexión de administración de red con el conmutador. En esta sección no se explican las diferentes configuraciones disponibles en el conmutador ni los comandos pertinentes.

En ella también se describe cómo acceder a un conmutador por primera vez con la configuración y las definiciones predeterminadas. Si una configuración especificada previamente provoca problemas, deberá borrar el archivo de configuración de inicio (que es la configuración del dispositivo al encenderse) y reiniciar el dispositivo. Para obtener más información, consulte el apartado Configuración predeterminada del dispositivo .

Requisitos de configuración del dispositivo

En este ejemplo se presupone que se dispone de los componentes siguientes:

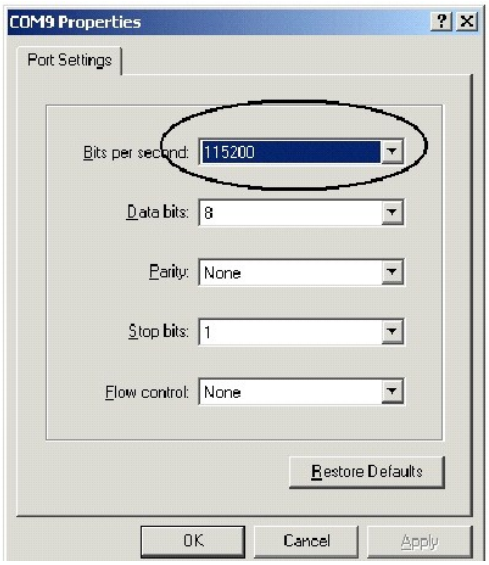
- Conmutador PowerConnect 6024/6024F.
- Una estación de trabajo en la que se han instalado los componentes siguientes:
  - Tarjeta de adaptador de red.
  - Aplicación de terminal ASCII (por ejemplo, hiperterminal de Microsoft® Windows® o terminal de Procomm Plus).
  - Una aplicación de explorador.
- Un cable F2F de módem nulo.
- Cables UTP (categoría 5) directos o cruzados.

Conexión inicial

1. Mediante el puerto RS-232, conecte el conmutador a la estación de trabajo.
2. Establezca el terminal ASCII con la configuración siguiente y seleccione el puerto COM adecuado.

   En la pantalla de ejemplo se utiliza la aplicación HyperTerminal.

Ilustración 5-2. Ventana de las propiedades del hiperterminal



NOTA: 115.200 es la velocidad en baudios predeterminada del nuevo dispositivo. El dispositivo puede otra velocidad en baudios. Si utiliza la velocidad en baudios de 115.200 pero no logra ver el terminal del dispositivo, pruebe con otra velocidad.

3. Utilice un cable de módem nulo F2F para conectarse a la estación de trabajo a través del conmutador.
4. Conecte el cable de alimentación del dispositivo y encienda el dispositivo.

Aparece la pantalla siguiente:

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

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

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


Booting...


Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

Testing CPU PCI Bus Configuration...............PASS


BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31
```

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

En este punto, puede entrar en el menú **Startup** (Inicio) si fuera necesario, para ejecutar procedimientos especiales. Si no entra en el menú **Startup** (Inicio), el sistema continúa con sus procesos y descomprime el código en la RAM. El código se inicia ejecutándose desde la RAM y se muestra una lista con los números de los puertos disponibles y sus estados (activo o inactivo).

NOTA: La pantalla que se muestra a continuación ejemplifica una configuración. Algunos elementos, como direcciones, versiones y fechas, pueden diferir para cada dispositivo.

```
Preparing to decompress...



Decompressing SW from image-1

d04000

OK

Running from RAM...



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

*** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 ***

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



HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M
```

```
Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed




Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

Console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2
```

El dispositivo ya está preparado para la configuración.

Configuración predeterminada del dispositivo

Para restablecer la configuración predeterminada del dispositivo, utilice el comando `delete startup-config` en el indicador de modo privilegiado (#) y reinicie el dispositivo. Tras cargarse de nuevo el dispositivo, se establece con la configuración predeterminada.

```
Console>

Console> enable

Console# delete startup-config

Startup file was deleted

Console# reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?

y



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

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

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

.

.

.

.
```

Habilitación de la gestión remota

1. Escriba el comando **enable** en la consola para acceder al modo de pantalla Privileged EXEC (Ejecución privilegiada) tal como se indica a continuación:

```
Console> enable

Console#
```

2. Conecte la estación de gestión (PC) al dispositivo a través de uno de los puertos Ethernet o a través de una red conectada al dispositivo, mediante un cable CAT5.

   En este ejemplo se utilizará el puerto g1.

3. Asegúrese (en el terminal ASCII) de que el estado de la interfaz haya cambiado a `up` (activo) y que el estado de STP sea `forwarding` (transcurridos 30 segundos) tal como se muestra a continuación:

```
Console#


01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1


01-Jan-2000 01:43:03 %LINK-I-Up: g1


01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port g1: STP status Forwarding
```

4. Escriba el comando **config** en la consola para acceder al modo de pantalla de configuración, tal como se indica a continuación:

```
Console# config
```

5. Escriba el comando **interface vlan** en la consola para entrar el modo de pantalla de configuración de VLAN a través del valor predeterminado VLAN 1 (tag = 1), tal como se indica a continuación:

```
Console (config)# interface vlan 1


Console (config-if)#
```

6. Defina una dirección IP en el dispositivo asignando una dirección IP (en este ejemplo 50.1.1.1) a la VLAN que contenga la interfaz conectada a la estación de gestión. Si la estación de gestión está conectada directamente a la interfaz, la dirección IP de la VLAN debe tener la misma subred que la estación de gestión.

```
Console (config)#


Console (config-if)#ip address 50.1.1.1 225.0.0.0


Console (config-if)#
```

7. Si la estación de gestión es miembro de una red remota y no está conectada directamente a la interfaz, configure una ruta estática.

   La dirección IP configurada debe pertenecer a la misma subred que una de las interfaces IP del dispositivo. En este ejemplo, la dirección estática es 50.1.1.100.

```
Console (config-if)# exit


Console (config)# ip route 0.0.0.0.0.0.0.0 50.1.1.100


Console (config)#
```

8. Ejecute un comando ping desde el conmutador contra la estación de gestión para comprobar si la conexión funciona correctamente.

   Permita que el puerto se coloque en el estado de reenvío STP; para ello, espere 30 segundos antes de ejecutar el comando ping contra la estación de gestión. La dirección estática es (en este ejemplo) 50.1.1.2:

```
Console (config)#

Console (config)# exit

Console# ping 50.1.1.2

64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms



----50.1.1.2 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

Console#
```

9. Defina un nombre de usuario y una contraseña para permitir el acceso de dispositivo de nivel 15 privilegiado para un usuario remoto (HTTP y HTTPS).

En este ejemplo, el nombre del usuario y la contraseña son Dell y el nivel de privilegio es 15. Los niveles de privilegio oscilan entre 1 y 15; 15 incida el nivel más alto. El acceso de nivel 15 es el único nivel de acceso para la interfaz web.

```
Console# config

Console (config)# username Dell password Dell privilege 15

Console (config)# ip http authentication local

Console (config)# ip https authentication local

Console (config)# crypto certificate generate key_generate

Generating RSA private key, 1024 bit long modulus

Console (config)# ip https server
```

10. Defina un nombre de usuario y una contraseña para permitir el acceso a un usuario local (por ejemplo, consola, Telnet, servidor de la web).

En este ejemplo, el nombre de usuario y la contraseña son Dell , y el nivel de privilegio es 15.

```
Console (config)# username Dell password Dell privilege 15

Console (config)#

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 tom

Console (config-line)# exit

Console (config)# line telnet

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password bob

Console (config-line)# exit

Console (config)# line ssh

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password jones

Console (config-line)# exit
```

11. Guarde el archivo **running-config** en el archivo **startup-config**.

De esta forma, se asegura de que la configuración que se acaba de completar sea la misma si se reinicia el dispositivo.

```
Console (config-line)# exit

Console (config)# exit

Console# copy running-config startup-config
```

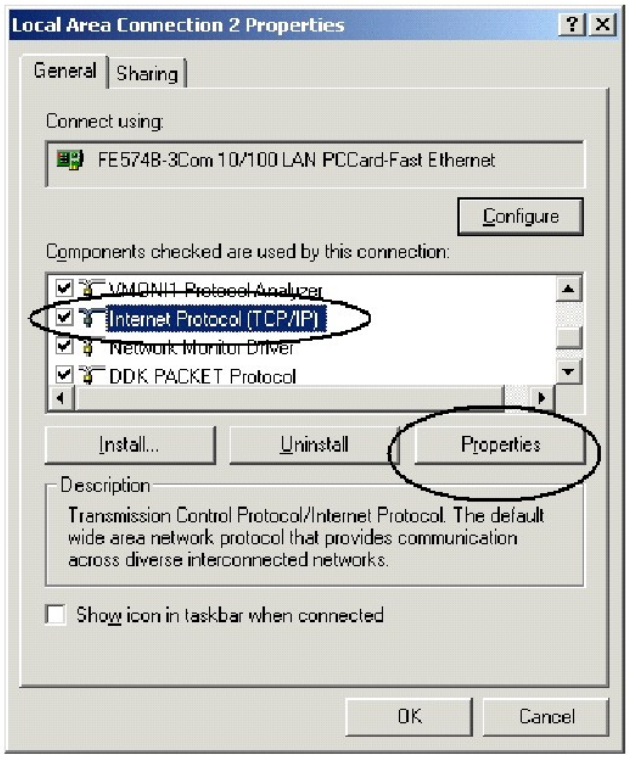
El dispositivo que se ha configurado ahora, puede gestionarse a través de las diferentes opciones como, por ejemplo, Telnet, interfaz de servidor web y otras.

Establecimiento de la dirección IP de la estación de gestión

1. En la estación de gestión, haga clic en **Inicio**→ **Configuración**→ **Conexiones de red y de acceso telefónico**.
2. Haga clic con el botón derecho del ratón en la conexión de red que se utilice para la gestión y seleccione **Propiedades**.

Aparece la ventana de propiedades de la conexión.

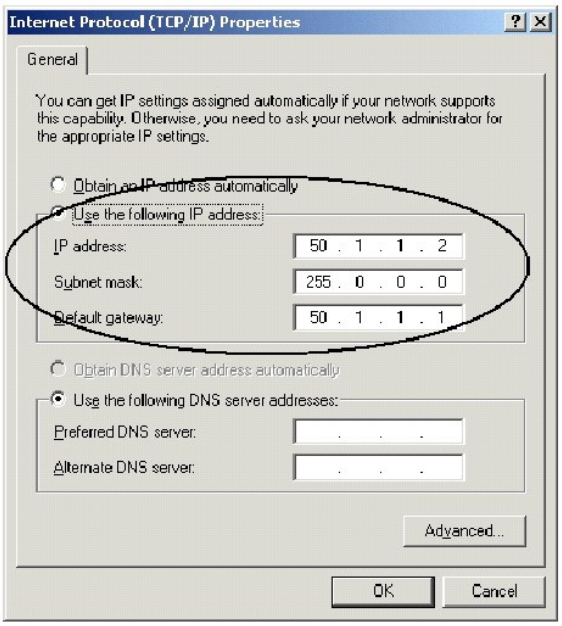
Ilustración 5-3. Ventana Propiedades de Conexión de área local



3. Haga clic en **Protocolo Internet (TCP/IP)** y, a continuación, en **Propiedades**.

Aparecerá la ventana **Propiedades de Protocolo Internet (TCP/IP)**.

Ilustración 5-4. Ventana Propiedades de Protocolo Internet (TCP/IP)



4. Haga clic en **Usar la siguiente dirección IP**.
5. Escriba las direcciones adecuadas de la estación de gestión en los campos **Dirección IP**, **Máscara de subred** y **Puerta de enlace predeterminada**.

NOTA: Si la estación de gestión está conectada a un enrutador, en lugar de estar directamente conectada al conmutador 6024/6024F, la puerta de enlace predeterminada se debe configurar como la dirección IP de la interfaz del enrutador conectada a la estación de gestión (que dirige la conexión hacia el conmutador 6024/6024F).

Habilitación del acceso Telnet

Utilice la línea de comandos de Windows/DOS o bien una aplicación Telnet para acceder al dispositivo vía Telnet. Recuerde que debe especificar la contraseña adecuada. La conexión se realiza con la dirección IP definida en el dispositivo.

Cuando se otorga el acceso, la utilización de los comandos es la misma que la de la gestión de dispositivo directa:

1. En la estación de gestión, haga clic en **Inicio→ Ejecutar**.
2. En la ventana **Ejecutar**, escriba cmd y haga clic en **Aceptar**.

   Aparece la línea de comandos estándar de Windows.
3. Escriba el comando **Telnet** y la dirección IP del dispositivo, tal como se indica a continuación:

```
Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 50.1.1.1

11-Aug-20 03 11:14:06 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

Password:***
```

```
Console> enable

Password:***

Console# show ip interface

Proxy ARP is disabled

IP Address I/F Type Directed Broadcast

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

100.1.1.1/24 vlan 1 static disable



OOB ip interfaces

Gateway IP Address Activity status

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

10.6.12.1 active



IP Address I/F Type

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

10.6.12.20/24 Oob-eth 1 dhcp
```

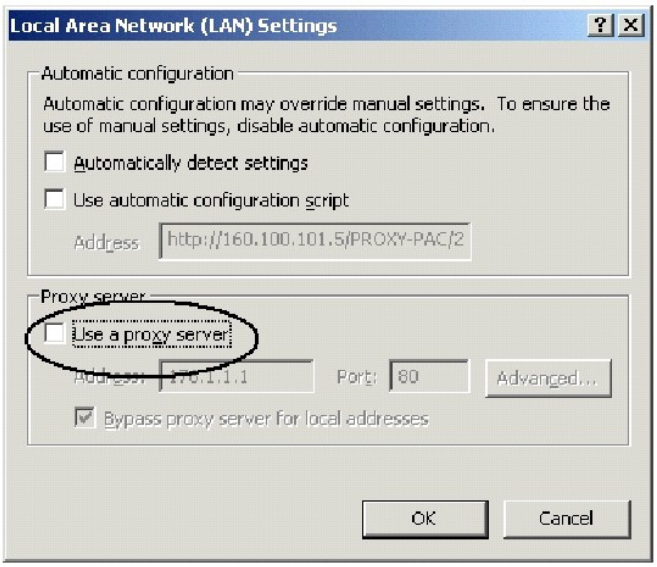
El conmutador indica el estado de la sesión Telnet:

```
Console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection from 50.1.1.2 terminated
```

Habilitación del acceso web (servidor HTTP)

1. Para evitar los problemas que puedan surgir al utilizar un servidor proxy HTTP, inhabilite (desmarque) la opción proxy del explorador.
   a. En Microsoft Internet Explorer, haga clic en **Herramientas**→ **Opciones de Internet**.
   b. Haga clic en la ficha **Conexiones** y, a continuación, en **Configuración de LAN** para que aparezca la ventana **Configuración de la red de área local (LAN)**.
   c. Compruebe que la casilla de verificación **Utilizar un servidor proxy** esté desmarcada y, a continuación, haga clic en **Aceptar**.

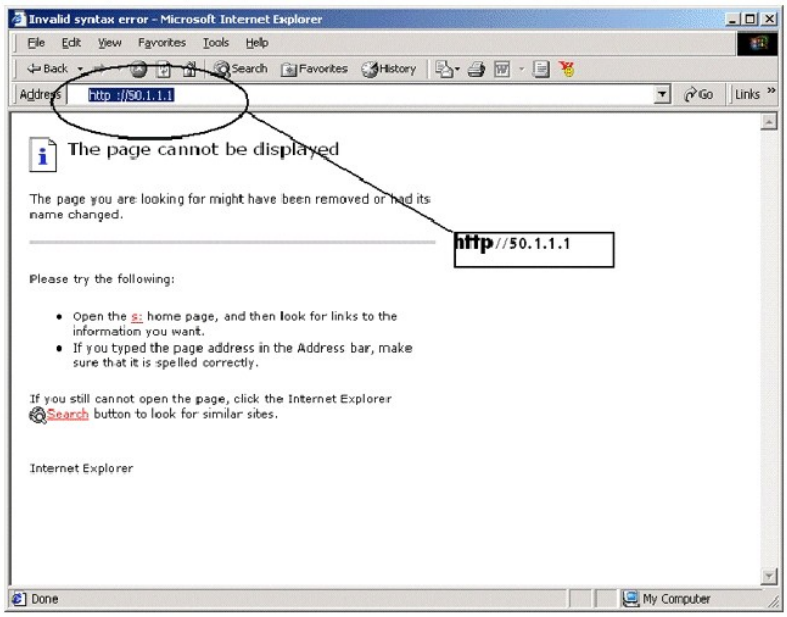
Ilustración 5-5. Ventana Configuración de la red de área local (LAN)



d. Haga clic en **Aceptar** para cerrar la ventana **Opciones de Internet**.

2. En la ventana del explorador escriba la IP configurada previamente en el dispositivo (con o sin el prefijo http://).

Ilustración 5-6. Conexión a la interfaz de la web



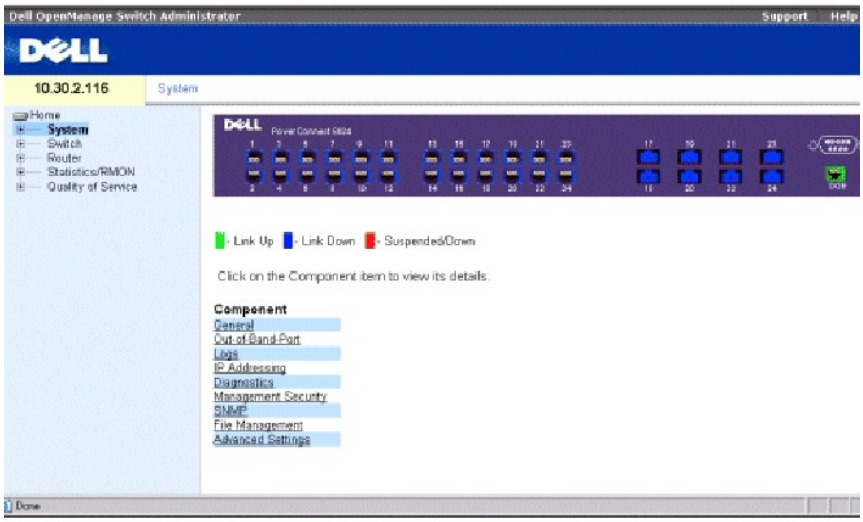
Aparece la ventana de autenticación de la contraseña.

3. Escriba el nombre de usuario y la contraseña asignados.

Aparece el administrador del conmutador de Dell OpenManage.

NOTA: si no se ha definido ninguna contraseña, se acepta cualquier contraseña.

Ilustración 5-7. Página Dell OpenManage Switch Administrator (Administrador del conmutador Dell OpenManage)



Configuración del acceso de gestión seguro (HTTPS)

Cuando se gestiona el dispositivo de forma segura a través del navegador web estándar, se utiliza el protocolo de seguridad SSL (Secure Socket Layer).

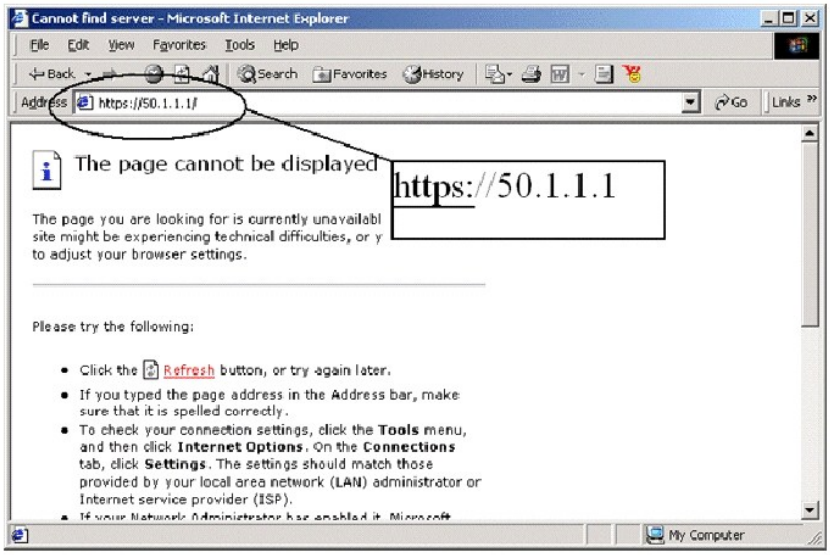
Para gestionar el dispositivo de forma segura a través del navegador web estándar, efectúe los pasos siguientes:

1. Configure el conmutador para que habilite el servidor HTTPS. Cree una clave de seguridad mediante los comandos **ip https server** y **crypto certificate generate key-generate**:

```
Console# configure

Console (config)# ip https server

Console (config)# crypto certificate generate key-generate

Generating RSA private key, 1024 bit long modulus

Console (config)#
```

2. Configure la estación de gestión como si se tratara de una conexión HTTP normal (consulte el apartado Habilitación del acceso web (servidor HTTP)) .
3. Conecte el dispositivo vía HTTPS escribiendo la dirección `https://<dirección_ip_dispositivo>` en la ventana del navegador (deberá escribir https):

Figure 5-8. Conexión a la interfaz de la web con una conexión segura



Aparece la ventana **Alerta de seguridad**.

4. Haga clic en **Sí** para confirmar que acepta el certificado de seguridad (si no lo autentica un tercero).
5. Aparece la ventana **Escribir contraseña de red**.
6. Escriba el nombre de usuario y la contraseña asignados.

Aparece el administrador del conmutador de Dell OpenManage del dispositivo.

Funciones del menú Startup (Inicio)

Desde el menú **Startup** (Inicio) puede realizar funciones adicionales de configuración.

Para ver el menú **Startup** (Inicio):

1. Durante el proceso de arranque, tras completarse la primera parte de la POST, pulse <Esc> o <Intro> en los dos segundos siguientes a la aparición del mensaje siguiente:

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

Aparece el menú **Startup** (Inicio), que contiene las funciones de configuración siguientes:

```
[1] Download Software (Descargar software)

[2] Erase Flash File (Borrar archivo de memoria flash)

[3] Erase Flash Sectors (Borrar sectores de la memoria flash)

[4] Password Recovery Procedure (Procedimiento de recuperación de contraseña)
```

```
[5] Enter Diagnostic Mode (Entrar en el modo de diagnósticos)

[6] Back Enter your choice or press 'ESC' to exit (Elija una opción o pulse 'ESC' para salir):
```

En las secciones siguientes se describen las opciones del menú **Startup** (Inicio). Si no efectúa ninguna selección en los 25 segundos siguientes (valor predeterminado), se agota el tiempo de espera del conmutador.

Sólo el personal de soporte técnico puede utilizar el modo de diagnósticos. Por este motivo la opción **Enter Diagnostic Mode** (Entrar en el modo de diagnósticos) del menú **Startup** (Inicio) no se describe en esta guía.

Download Software (Descargar software)

Utilice la opción de descarga de software cuando deba descargarse una nueva versión de software para sustituir a los archivos dañados o actualizar el software del sistema.

Para descargar software desde el menú **Startup** (Inicio):

1. En el menú **Startup** (Inicio), pulse <1>.

   Aparece el siguiente mensaje:

   ```
   Downloading code using XMODEM (Descargando el código mediante XMODEM)
   ```

2. Si utiliza HyperTerminal, haga clic en **Transferir** de la barra de menús de **HyperTerminal**.
3. En el menú **Transferir**, haga clic en **Enviar archivo...**.

   Aparece la ventana **Enviar archivo**.

4. Escriba la ruta de acceso del archivo que deba descargarse.
5. Asegúrese de que el protocolo esté definido como Xmodem.
6. Haga clic en **Send** (Enviar).

   El software se descarga. La descarga del software puede durar varios minutos. La aplicación de emulación de terminal, como HyperTerminal, puede mostrar el curso del proceso de carga.

   Una vez descargado el software, el dispositivo se reinicia automáticamente.

Borrar archivo de memoria flash

En algunos casos, la configuración del dispositivo debe borrarse. Si se borra, se deben reconfigurar todos los parámetros configurados a través de CLI, EWS o SNMP.

Para borrar la configuración del dispositivo:

1. En el menú **Startup**, pulse <2> en los 6 segundos posteriores para borrar el archivo de memoria flash.

   Aparece el siguiente mensaje:

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

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

2. Pulse <Y> (Sí).

NOTA: no pulse <Intro>.

Aparece el siguiente mensaje:

```
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 de memoria FLASH.

Se borra la configuración y el dispositivo se reinicia.

4. Lleve a cabo la configuración inicial del conmutador.

Erase FLASH Sectors (Borrar sectores de la memoria flash)

A efectos de solución de problemas, es posible que deba borrar los sectores flash. Si borra la memoria FLASH, se deben descargar y volver a instalar todos los archivos del software.

Para borrar la memoria FLASH:

1. En el menú **Startup**, pulse <3> en los 6 segundos posteriores.

Aparece el siguiente mensaje:

```
Warning! About to erase Flash Memory! FLASH size = 16252928. blocks = 64 Are you sure (Y/N)
```

2. Confirme pulsando <Y> (Sí).

Aparece el siguiente mensaje:

```
Enter First flash block (1 - 63):
```

3. Escriba el primer bloque de FLASH que se borrará y pulse <Intro>.

El intervalo de valores es 1-64. Aparece el siguiente mensaje:

```
Enter Last flash block (1 - 63):
```

4. Escriba el último bloque de FLASH que se borrará y pulse <Intro>.
5. Aparece el siguiente mensaje:

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

6. Confirme pulsando <Y> (Sí).

Aparece el siguiente mensaje:

```
Erasing flash blocks 1 - 63: Done.
```

Recuperación de contraseña

Si se pierde una contraseña, utilice la opción **Password Recovery** (Recuperación de contraseña) del menú **Startup** (Inicio). El procedimiento permite al usuario especificar el dispositivo una vez sin contraseña.

Para recuperar una contraseña perdida para el terminal local solamente:

1. En el menú **Startup** (Inicio), seleccione **[4]** y pulse <Intro>.

   La contraseña se suprime.

2. Para garantizar la seguridad del dispositivo, reconfigure las contraseñas para los métodos de gestión aplicables.

Puerto de gestión fuera de banda

El puerto de gestión fuera de banda (OOB) es un puerto Ethernet a 10/100 Mbps que se puede utilizar para conectarse directamente al conmutador con el objetivo de trabajar con funciones de gestión de administrador del sistema. El sistema considera a este puerto como una interfaz IP normal y a través del mismo se puede acceder a todas las interfaces de gestión.

A través del puerto fuera de banda no se puede acceder a las interfaces en banda. De forma parecida, no se puede acceder al puerto fuera de banda a través de los puertos en banda. Puesto que la funcionalidad de la administración de red puede llevarse a cabo mediante OOB, debe utilizar el puerto OOB para todas las funciones de administración de la red, incluida la gestión web; descarga/carga de imagen, arranque y configuración; Telnet; administración de SNMP, etc.

Al contrario de lo que ocurre en los puertos en banda, OOB no se utiliza a efectos de encaminamiento ni conmutación. La utilización del puerto fuera de banda (OOB) en lugar de un puerto en banda para la administración de la red garantiza que un puerto en banda adicional de 1 Gbyte permanezca activo para el encaminamiento.

En la secciones siguientes aparecen ejemplos de comandos OOB.

Asignación de direcciones IP dinámicas (en un puerto fuera de banda)

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address dhcp hostname dell

Console (config-oob)# exit

Console (config)# exit

Console#
```

Asignación de direcciones IP estáticas (en un puerto fuera de banda)

```
Console> enable

Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.1.1.1 255.0.0.0

Console (config-oob)# exit

Console (config)# ip default-gateway 10.1.1.10

Console (config)# exit

Console#
```

Asignación de la puerta de enlace predeterminada IP

```
Console>

Console> enable

Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.0.0.1 /8

Console (config-oob)# ip default-gateway 10.1.1.1

Console (config-oob)#
```

Ping a través del puerto fuera de banda

```
Console# ping oob/10.6.12.25
```

Copia de la imagen / arranque

```
copy tftp://oob/10.6.12.25/ves_115.dos image
```

```
copy tftp://oob/10.6.12.25/boot_013.rfb boot
```

Puerta de enlace IP predeterminada de fuera de banda

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip default-gateway 10.1.1.10
```

Información adicional

Para obtener más información sobre la configuración de los puertos fuera de banda, consulte el apartado Configuración de los puertos de gestión fuera de banda (OOB) .

Regresar a la página de contenido

Regresar a la página de contenido

Obtención de ayuda

Sistemas Dell™ PowerConnect™ 6024/6024F

Asistencia técnica

Si necesita ayuda con un problema técnico, utilice la amplia gama de servicios en línea de Dell disponibles en el sitio web Dell Support en **support.dell.com**, para obtener ayuda sobre la instalación y los procedimientos de solución de problemas. Para obtener más información, consulte el apartado "Servicios en línea".

Si no puede resolver el problema con los servicios en línea, llame a Dell para obtener asistencia técnica. Consulte el apartado "Cómo ponerse en contacto con Dell".

NOTA: Llame al servicio de asistencia técnica desde un teléfono que esté cerca del sistema, de manera que el personal de soporte pueda ayudarle con los procedimientos necesarios.

NOTA: Es posible que el sistema de código de servicio urgente de Dell no esté disponible en todos los países.

Cuando el sistema telefónico automatizado de Dell lo solicite, marque el código de servicio rápido para dirigir su llamada directamente al personal de servicio que corresponda. Si no tiene un código de servicio urgente, abra la carpeta **Dell Accessories** (Accesorios Dell), haga doble clic en el icono **Express Service Code** (Código de servicio rápido) y siga las instrucciones.

Para obtener instrucciones sobre cómo usar el servicio de asistencia técnica, consulte los apartados "Servicio de asistencia técnica" y "Antes de llamar".

NOTA: Algunos de los servicios que se describen a continuación no siempre están disponibles en todos los lugares fuera de la parte continental de EE.UU. Póngase en contacto con su representante local de Dell para obtener información sobre su disponibilidad.

Servicios en línea

Puede acceder al sitio web Dell Support en la dirección **support.dell.com**. Seleccione su región en la página **WELCOME TO DELL SUPPORT** (Bienvenido al servicio de asistencia de Dell) y rellene los datos que se solicitan para acceder a las herramientas y a la información de la Ayuda.

Puede ponerse en contacto con Dell en las siguientes direcciones electrónicas:

- Red mundial

  www.dell.com/

  www.dell.com/ap/ (únicamente para países asiáticos y del Pacífico)

  www.dell.com/jp (únicamente para Japón)

  www.euro.dell.com (únicamente para Europa)

www.dell.com/la (para países de Latinoamérica)

www.dell.ca (únicamente para Canadá)

- FTP (File Transfer Protocol, Protocolo de transferencia de archivos) anónimo

ftp.dell.com/

Inicie la sesión como user: anonymous y use su dirección de correo electrónico como su contraseña.

- Servicio electrónico de asistencia (Electronic Support Service)

support@us.dell.com

apsupport@dell.com (únicamente para países asiáticos y del Pacífico)

support.jp.dell.com (únicamente para Japón)

support.euro.dell.com (únicamente para Europa)

- Electronic Quote Service (Servicio electrónico de cotizaciones)

sales@dell.com

apmarketing@dell.com (sólo para países asiáticos y del Pacífico)

sales_canada@dell.com (únicamente para Canadá)

- Electronic Information Service (Servicio electrónico de información)

info@dell.com

Servicio AutoTech

El servicio de asistencia técnica automatizada de Dell, AutoTech, proporciona respuestas grabadas a las preguntas más frecuentes que los clientes de Dell hacen acerca de sus ordenadores portátiles y de sobremesa.

Cuando llame a AutoTech, utilice un teléfono de tonos para seleccionar los temas correspondientes a sus preguntas.

El servicio AutoTech está disponible las 24 horas del día, 7 días a la semana. También puede acceder a este servicio a través del servicio de asistencia técnica. Consulte la información de contacto para su región.

Servicio automatizado para averiguar el estado de un pedido

Para comprobar el estado de un pedido de cualquier producto Dell™ que haya solicitado, puede dirigirse a **support.dell.com** o llamar al servicio automatizado de estado de pedidos. Un contestador automático le pedirá los datos necesarios para buscar el pedido e informarle sobre su estado. Consulte la información de contacto para su región.

Servicio de asistencia técnica

Dell pone a su disposición un servicio de asistencia técnica, disponible las 24 horas del día y todos los días de la semana, para dar respuesta a todas sus preguntas sobre el hardware de Dell. Nuestro personal de asistencia técnica usa diagnósticos basados en PC para proporcionar respuestas rápidas y precisas.

Para ponerse en contacto con el servicio de asistencia técnica de Dell, consulte el apartado "Antes de llamar" y, a continuación, lea la información de contacto de su región.

Formación y certificación Dell Enterprise

El servicio Dell Enterprise Training and Certification se encuentra disponible; visite **www.dell.com/training** para obtener más información. Es posible que este servicio no esté disponible en todas los lugares.

Problemas con su pedido

Si tiene algún problema con un pedido (por ejemplo, falta algún componente, hay componentes equivocados o la factura es incorrecta), póngase en contacto con el departamento de atención al cliente de Dell. Al llamar, tenga a la mano su factura o lista de embalaje. Consulte la información de contacto para su región.

Información sobre productos

Si necesita información sobre otros productos de Dell disponibles o si desea hacer un pedido, visite el sitio web de Dell en la dirección **www.dell.com**. Para obtener un número de teléfono al que llamar y hablar con un especialista en ventas, consulte la información de contacto para su región.

Devolución de artículos para su reparación bajo garantía o para recibir crédito

Prepare todos los artículos que vaya a devolver, ya sea para su reparación bajo garantía o para que le devuelvan el importe, de la manera siguiente:

1. Llame a Dell para obtener un RMA (número de autorización para devolución de material) y anótelo de forma clara y evidente en la parte exterior de la caja.

   Para obtener un número de teléfono al que llamar, consulte la información de contacto para su región.

2. Incluya una copia de la factura y una carta que describa la razón de la devolución.
3. Incluya una copia de la información de diagnóstico de que disponga.
4. Incluya todos los accesorios relacionados con los artículos que desea devolver (por ejemplo, cables de alimentación, soportes como CD y discos, y guías) si la devolución es para recibir crédito.
5. Empaquete el equipo que vaya a devolver en el embalaje original (o uno equivalente).

   El usuario se responsabiliza de los gastos de envío. Asimismo, tiene la obligación de asegurar el producto devuelto y asumir el riesgo en caso de pérdida durante el envío a Dell. Los paquetes enviados a pago contra entrega no serán aceptados.

Cualquier devolución que no satisfaga los requisitos indicados no será aceptada en nuestro departamento de recepción y le será devuelta.

Antes de llamar

NOTA: Tenga a mano el código de servicio rápido cuando llame. Este código contribuirá a que el sistema de soporte telefónico automatizado de Dell gestione de manera más eficiente su llamada.

Si es posible, encienda el sistema antes de llamar a Dell y haga la llamada desde un teléfono que esté cerca del equipo. Es posible que se le pida que introduzca algunos comandos con el teclado, que proporcione información detallada durante el funcionamiento o que intente otros pasos de solución de problemas que únicamente pueden realizarse con el equipo. Asegúrese de tener a la mano la documentación de su equipo.

PRECAUCIÓN: Antes de intentar reparar cualquiera de los componentes del interior de su equipo, consulte la *Guía de información del sistema* para obtener información de seguridad importante.

Cómo ponerse en contacto con Dell

Para ponerse en contacto con Dell de forma electrónica, puede acceder a los siguientes sitios web:

- **www.dell.com**
- **support.dell.com** (asistencia técnica)
- **premiersupport.dell.com** (asistencia técnica para clientes del ámbito educativo, del gobierno, de la sanidad y de negocios a mediana y a gran escala, incluidos clientes de las categorías Premier, Platinum y Gold)

Para obtener las direcciones web de su país, busque la sección correspondiente en la siguiente tabla.

NOTA: Los números de teléfono gratuitos son para uso dentro del país para el que aparecen.

Cuando necesite ponerse en contacto con Dell, utilice las direcciones electrónicas, los números de teléfono y los códigos que se incluyen en la siguiente tabla. Si necesita ayuda para averiguar los códigos que debe utilizar, póngase en contacto con un operador de telefonía local o internacional.

País (ciudad) **Código de acceso internacional** **Código del país** **Código de ciudad**	**Nombre de departamento o área de servicio,** **Sitio web y Dirección de correo electrónico**	**Prefijo,** **Números locales y** **Números de teléfono gratuitos**
Alemania (Langen) Código de acceso internacional: **00** Código del país: **49** Código de la ciudad: **6103**	Página web: **support.euro.dell.com**	
	Correo electrónico: tech_support_central_europe@dell.com	
	Asistencia técnica	06103 766-7200
	Atención a clientes particulares y pequeñas empresas	0180-5-224400
	Atención global al cliente según segmentos	06103 766-9570
	Atención a clientes de cuentas preferentes	06103 766-9420
	Atención a clientes de cuentas grandes	06103 766-9560
	Atención a clientes de cuentas públicas	06103 766-9555
	Centralita	06103 766-7000
Anguila	Asistencia general	gratuito: 800-335-0031
Antigua y Barbuda	Asistencia general	1-800-805-5924
Antillas Neerlandesas	Asistencia general	001-800-882-1519
Argentina (Buenos Aires) Código de acceso internacional: **00** Código del país: **54** Código de la ciudad: **11**	Página web: **www.dell.com.ar**	
	Asistencia técnica y atención al cliente	gratuito: 0-800-444-0733
	Ventas	0-810-444-3355
	Fax de asistencia técnica	11 4515 7139
	Fax de atención al cliente	11 4515 7138
Aruba	Asistencia general	gratuito: 800-1578
Australia (Sydney) Código de acceso internacional: **0011** Código del país: **61** Código de la ciudad: **2**	Correo electrónico (Australia): au_tech_support@dell.com	
	Correo electrónico (Nueva Zelanda): nz_tech_support@dell.com	
	Residencias y empresas pequeñas	1-300-65-55-33
	Gobierno y empresas	gratuito: 1-800-633-559
	División de cuentas preferentes (PAD)	gratuito: 1-800-060-889
	Atención al cliente	gratuito: 1-800-819-339
	Ventas corporativas	gratuito: 1-800-808-385
	Transacciones de venta	gratuito: 1-800-808-312
	Fax	gratuito: 1-800-818-341

Austria (Viena) Código de acceso internacional: **900** Código del país: **43** Código de la ciudad: **1**	Página web: **support.euro.dell.com**	
	Correo electrónico: tech_support_central_europe@dell.com	
	Ventas a particulares y pequeñas empresas	0820 240 530 00
	Fax para particulares y pequeñas empresas	0820 240 530 49
	Atención a clientes particulares y pequeñas empresas	0820 240 530 14
	Atención a clientes con cuentas preferentes y de empresas	0820 240 530 16
	Asistencia técnica a clientes particulares y pequeñas empresas	0820 240 530 14
	Asistencia técnica a cuentas preferentes y de empresas	0660 8779
	Centralita	0820 240 530 00
Bahamas	Asistencia general	gratuito: 1-866-278-6818
Barbados	Asistencia general	1-800-534-3066
Bélgica (Bruselas) Código de acceso internacional: **00** Código del país: **32** Código de la ciudad: **2**	Página web: **support.euro.dell.com**	
	Correo electrónico: tech_be@dell.com	
	Correo electrónico para clientes francófonos: **support.euro.dell.com/be/fr/emaildell/**	
	Asistencia técnica	02 481 92 88
	Atención al cliente	02 481 91 19
	Ventas corporativas	02 481 91 00
	Fax	02 481 92 99
	Centralita	02 481 91 00
Bermuda	Asistencia general	1-800-342-0671
Bolivia	Asistencia general	gratuito: 800-10-0238
Brasil Código de acceso internacional: **00** Código del país: **55** Código de la ciudad: **51**	Página web: **www.dell.com/br**	
	Servicio al cliente, asistencia técnica	0800 90 3355
	Fax de asistencia técnica	51 481 5470
	Fax de atención al cliente	51 481 5480
	Ventas	0800 90 3390
Brunei Código del país: **673**	Asistencia técnica al cliente (Penang, Malasia)	604 633 4966
	Servicio al cliente (Penang, Malasia)	604 633 4949
	Transacciones de venta (Penang, Malasia)	604 633 4955
Canadá (North York, Ontario) Código de acceso internacional: **011**	Estado de los pedidos en línea: **www.dell.ca/ostatus**	
	AutoTech (asistencia técnica automatizada)	gratuito: 1-800-247-9362
	TechFax	gratuito: 1-800-950-1329
	Atención al cliente (ventas a particulares y pequeñas empresas)	gratuito: 1-800-847-4096
	Atención al cliente para empresas medianas y grandes, y del gobierno	gratuito: 1-800-326-9463
	Asistencia técnica (ventas a particulares y pequeñas empresas)	gratuito: 1-800-847-4096
	Asistencia técnica para empresas medianas y grandes, y del gobierno	gratuito: 1-800-387-5757
	Ventas (ventas a particulares y pequeñas empresas)	gratuito: 1-800-387-5752
	Ventas (medianas y grandes empresas, instituciones gubernamentales)	gratuito: 1-800-387-5755
	Ventas de repuestos y ventas por extensión de servicio	1 866 440 3355
Colombia	Asistencia general	980-9-15-3978
Corea (Seúl) Código de acceso internacional: **001** Código del país: **82** Código de la ciudad: **2**	Asistencia técnica	gratuito: 080-200-3800
	Ventas	gratuito: 080-200-3600
	Servicio al cliente (Seúl, Corea)	gratuito: 080-200-3800
	Servicio al cliente (Penang, Malasia)	604 633 4949
	Fax	2194-6202
	Centralita	2194-6000
Costa Rica	Asistencia general	0800-012-0435
Chile (Santiago) Código del país: **56** Código de la ciudad: **2**	Asistencia técnica, servicio al cliente y ventas	gratuito: 1230-020-4823
China (Xiamén) Código del país: **86** Código de la ciudad: **592**	Sitio web de asistencia técnica: **support.ap.dell.com/china**	
	Dirección de correo electrónico de asistencia técnica: cn_support@dell.com	
	Fax de asistencia técnica	818 1350
	Asistencia técnica a particulares y pequeñas empresas	gratuito: 800 858 2437
	Asistencia técnica para las cuentas corporativas	gratuito: 800 858 2333
	Servicio al cliente	gratuito: 800 858 2060
	Particulares y pequeñas empresas	gratuito: 800 858 2222

	División de cuentas preferentes	gratuito: 800 858 2557
	Grandes cuentas corporativas: GCP	gratuito: 800 858 2055
	Grandes cuentas corporativas: Cuentas clave	gratuito: 800 858 2628
	Grandes cuentas corporativas: Norte	gratuito: 800 858 2999
	Grandes cuentas corporativas: Norte (instituciones gubernamentales y educativas)	gratuito: 800 858 2955
	Grandes cuentas corporativas: Este	gratuito: 800 858 2020
	Grandes cuentas corporativas: Este (instituciones gubernamentales y educativas)	gratuito: 800 858 2669
	Grandes cuentas corporativas: Equipo Queue	gratuito: 800 858 2222
	Grandes cuentas corporativas: Sur	gratuito: 800 858 2355
	Grandes cuentas corporativas: Oeste	gratuito: 800 858 2811
	Grandes cuentas corporativas: Recambios	gratuito: 800 858 2621
Dinamarca (Copenhague) Código de acceso internacional: **00** Código del país: **45**	Página web: **support.euro.dell.com**	
	Asistencia por correo electrónico (equipos portátiles): den_nbk_support@dell.com	
	Asistencia por correo electrónico (equipos de sobremesa): den_support@dell.com	
	Asistencia por correo electrónico (servidores): Nordic_server_support@dell.com	
	Asistencia técnica	7023 0182
	Atención al cliente (relacional)	7023 0184
	Atención a clientes particulares y pequeñas empresas	3287 5505
	Centralita (relacional)	3287 1200
	Centralita de fax (relacional)	3287 1201
	Centralita (particulares y pequeñas empresas)	3287 5000
	Centralita de fax (particulares y pequeñas empresas)	3287 5001
Dominica	Asistencia general	gratuito: 1-866-278-6821
Ecuador	Asistencia general	gratuito: 999-119
EE.UU. (Austin, Texas) Código de acceso internacional: **011** Código del país: **1**	Servicio automatizado para averiguar el estado de un pedido	gratuito: 1-800-433-9014
	AutoTech (equipos portátiles y de sobremesa)	gratuito: 1-800-247-9362
	Consumidor (particulares y oficinas domésticas)	
	Asistencia técnica	gratuito: 1-800-624-9896
	Servicio al cliente	gratuito: 1-800-624-9897
	Servicio y soporte DellNet™	gratuito: 1-877-DellNet (1-877-335-5638)
	Clientes del programa de compras para empleados (EPP)	gratuito: 1-800-695-8133
	Página web de servicios financieros: **www.dellfinancialservices.com**	
	Servicios financieros (arrendamiento/préstamo)	gratuito: 1-877-577-3355
	Servicios financieros (cuentas preferentes de Dell, DPA)	gratuito: 1-800-283-2210
	Empresas	
	Servicio al cliente y asistencia técnica	gratuito: 1-800-822-8965
	Clientes del programa de compras para empleados (EPP)	gratuito: 1-800-695-8133
	Asistencia técnica para proyectores	gratuito: 1-877-459-7298
	Público (gobierno, centros educativos y sanitarios)	
	Servicio al cliente y asistencia técnica	gratuito: 1-800-456-3355
	Clientes del programa de compras para empleados (EPP)	gratuito: 1-800-234-1490
	Ventas Dell	gratuito: 1-800-289-3355 o gratuito: 1-800-879-3355
	Tienda de productos de ocasión de Dell (equipos reacondicionados de Dell)	gratuito: 1-888-798-7561
	Ventas de software y periféricos	gratuito: 1-800-671-3355
	Ventas de repuestos	gratuito: 1-800-357-3355
	Ventas de servicio y garantía extendidos	gratuito: 1-800-247-4618
	Fax	gratuito: 1-800-727-8320
	Servicios de Dell para personas sordas, con discapacidades auditivas o problemas del habla	gratuito: 1-877-DELLTTY (1-877-335-5889)
El Salvador	Asistencia general	01-899-753-0777
España (Madrid) Código de acceso internacional: **00**	Página web: **support.euro.dell.com**	
	Correo electrónico: **support.euro.dell.com/es/es/emaildell/**	
	Particulares y pequeñas empresas	

Código del país: **34** Código de la ciudad: **91**	Asistencia técnica	902 100 130
	Atención al cliente	902 118 540
	Ventas	902 118 541
	Centralita	902 118 541
	Fax	902 118 539
	Corporativa	
	Asistencia técnica	902 100 130
	Atención al cliente	902 118 546
	Centralita	91 722 92 00
	Fax	91 722 95 83
Finlandia (Helsinki) Código de acceso internacional: **990** Código del país: **358** Código de la ciudad: **9**	Página web: **support.euro.dell.com**	
	Correo electrónico: fin_support@dell.com	
	Asistencia por correo electrónico (servidores): Nordic_support@dell.com	
	Asistencia técnica	09 253 313 60
	Fax para obtener asistencia técnica	09 253 313 81
	Asistencia de relaciones al cliente	09 253 313 38
	Atención a clientes particulares y pequeñas empresas	09 693 791 94
	Fax	09 253 313 99
	Centralita	09 253 313 00
Francia (París) (Montpellier) Código de acceso internacional: **00** Código del país: **33** Códigos de la ciudad: **(1) (4)**	Página web: **support.euro.dell.com**	
	Correo electrónico: **support.euro.dell.com/fr/fr/emaildell/**	
	Particulares y pequeñas empresas	
	Asistencia técnica	0825 387 270
	Atención al cliente	0825 823 833
	Centralita	0825 004 700
	Centralita (llamadas desde fuera de Francia)	04 99 75 40 00
	Ventas	0825 004 700
	Fax	0825 004 701
	Fax (llamadas desde fuera de Francia)	04 99 75 40 01
	Corporativa	
	Asistencia técnica	0825 004 719
	Atención al cliente	0825 338 339
	Centralita	01 55 94 71 00
	Ventas	01 55 94 71 00
	Fax	01 55 94 71 01
Granada	Asistencia general	gratuito: 1-866-540-3355
Grecia Código de acceso internacional: 00 Código del país: 30	Página web: **support.euro.dell.com**	
	Correo electrónico: support.euro.dell.com/fr/fr/emaildell/	
	Asistencia técnica	080044149518
	Asistencia técnica de categoría Gold	08844140083
	Centralita	2108129800
	Ventas	2108129800
	Fax	2108129812
Guatemala	Asistencia general	1-800-999-0136
Guayana	Asistencia general	gratuito: 1-877-270-4609
Hong Kong Código de acceso internacional: **001** Código del país: **852**	Página web: **support.ap.dell.com**	
	Correo electrónico: ap_support@dell.com	
	Asistencia técnica (Dimension™ e Inspiron™)	2969 3189
	Asistencia técnica (OptiPlex™, Latitude™ y Dell Precision™)	2969 3191
	Asistencia técnica (PowerApp™ y PowerVault™)	2969 3196
	Teléfono de soporte del EEC de Gold Queue	2969 3187
	Defensa del consumidor	3416 0910
	Grandes cuentas corporativas	3416 0907
	Programas para clientes globales	3416 0908
	División de empresas medianas	3416 0912
	División de particulares y pequeñas empresas	2969 3105
India	Asistencia técnica	1600 33 8045
	Ventas	1600 33 8044
Irlanda (Cherrywood)	Página web: **support.euro.dell.com**	

Código de acceso internacional: **16** Código del país: **353** Código de la ciudad: **1**	Correo electrónico: dell_direct_support@dell.com	
	Asistencia técnica	1850 543 543
	Asistencia técnica para el Reino Unido (sólo llamadas dentro del Reino Unido)	0870 908 0800
	Atención al cliente para usuarios particulares	01 204 4014
	Atención al cliente para pequeñas empresas	01 204 4014
	Atención al cliente en el Reino Unido (sólo llamadas dentro del Reino Unido)	0870 906 0010
	Atención al cliente de corporaciones	1850 200 982
	Atención al cliente de corporaciones (sólo llamadas dentro del Reino Unido)	0870 907 4499
	Ventas para Irlanda	01 204 4444
	Ventas para el Reino Unido (sólo llamadas dentro del Reino Unido)	0870 907 4000
	Fax/Fax para ventas	01 204 0103
	Centralita	01 204 4444
Islas Caimán	Asistencia general	1-800-805-7541
Islas Turks y Caicos	Asistencia general	gratuito: 1-866-540-3355
Islas Vírgenes Americanas	Asistencia general	1-877-673-3355
Islas Vírgenes Británicas	Asistencia general	gratuito: 1-866-278-6820
Italia (Milán) Código de acceso internacional: **00** Código del país: **39** Código de la ciudad: **02**	Página web: **support.euro.dell.com**	
	Correo electrónico: **support.euro.dell.com/it/it/emaildell/**	
	Particulares y pequeñas empresas	
	Asistencia técnica	02 577 826 90
	Atención al cliente	02 696 821 14
	Fax	02 696 821 13
	Centralita	02 696 821 12
	Corporativa	
	Asistencia técnica	02 577 826 90
	Atención al cliente	02 577 825 55
	Fax	02 575 035 30
	Centralita	02 577 821
Jamaica	Asistencia general (sólo llamadas dentro de Jamaica)	1-800-682-3639
Japón (Kawasaki) Código de acceso internacional: **001** Código del país: **81** Código de la ciudad: **44**	Página web: **support.jp.dell.com**	
	Asistencia técnica (servidores)	gratuito: 0120-198-498
	Asistencia técnica fuera de Japón (servidores)	81-44-556-4162
	Asistencia técnica (Dimension™ e Inspiron™)	gratuito: 0120-198-226
	Asistencia técnica fuera de Japón (Dimension e Inspiron)	81-44-520-1435
	Asistencia técnica (Dell Precision™, OptiPlex™ y Latitude™)	gratuito: 0120-198-433
	Asistencia técnica fuera de Japón (Dell Precision, OptiPlex y Latitude)	81-44-556-3894
	Asistencia técnica (Axim™)	gratuito: 0120-981-690
	Asistencia técnica fuera de Japón (Axim)	81-44-556-3468
	Servicio Faxbox	044-556-3490
	Servicio de pedidos automatizado las 24 horas del día	044-556-3801
	Atención al cliente	044-556-4240
	División de ventas corporativas (hasta 400 empleados)	044-556-1465
	Ventas de la división de cuentas preferentes (más de 400 empleados)	044-556-3433
	Ventas de grandes cuentas corporativas (más de 3.500 empleados)	044-556-3430
	Ventas públicas (organismos gubernamentales, instituciones educativas e instituciones sanitarias)	044-556-1469
	Segmento global de Japón	044-556-3469
	Usuario particular	044-556-1760
	Centralita	044-556-4300
Latinoamérica	Asistencia técnica a clientes (Austin, Texas, EE.UU.)	512 728-4093
	Servicio al cliente (Austin, Texas, EE.UU.)	512 728-3619
	Fax (Asistencia técnica y Servicio al cliente) (Austin, Texas, EE.UU.)	512 728-3883
	Ventas (Austin, Texas, EE.UU.)	512 728-4397
	Ventas por fax (Austin, Texas, EE.UU.)	512 728-4600 o 512 728-3772
Luxemburgo Código de acceso internacional: **00**	Página web: **support.euro.dell.com**	
	Correo electrónico: tech_be@dell.com	
	Asistencia técnica (Bruselas, Bélgica)	3420808075

Código del país: **352**	Ventas a particulares y pequeñas empresas (Bruselas, Bélgica)	gratuito: 080016884
	Ventas corporativas (Bruselas, Bélgica)	02 481 91 00
	Atención al cliente (Bruselas, Bélgica)	02 481 91 19
	Fax (Bruselas, Bélgica)	02 481 92 99
	Centralita (Bruselas, Bélgica)	02 481 91 00
Macao Código del país: **853**	Asistencia técnica	gratuito: 0800 582
	Servicio al cliente (Penang, Malasia)	604 633 4949
	Transacciones de venta	gratuito: 0800 581
Malasia (Penang) Código de acceso internacional: **00** Código del país: **60** Código de la ciudad: **4**	Asistencia técnica	gratuito: 1 800 888 298
	Servicio al cliente	04 633 4949
	Transacciones de venta	gratuito: 1 800 888 202
	Ventas corporativas	gratuito: 1 800 888 213
México Código de acceso internacional: **00** Código del país: **52**	Asistencia técnica al cliente	001-877-384-8979 o 001-877-269-3383
	Ventas	50-81-8800 o 01-800-888-3355
	Servicio al cliente	001-877-384-8979 o 001-877-269-3383
	Central	50-81-8800 o 01-800-888-3355
Montserrat	Asistencia general	gratuito: 1-866-278-6822
Nicaragua	Asistencia general	001-800-220-1006
Noruega (Lysaker) Código de acceso internacional: **00** Código del país: **47**	Página web: **support.euro.dell.com**	
	Asistencia por correo electrónico (equipos portátiles): nor_nbk_support@dell.com	
	Asistencia por correo electrónico (equipos de sobremesa): nor_support@dell.com	
	Asistencia por correo electrónico (servidores): nordic_server_support@dell.com	
	Asistencia técnica	671 16882
	Asistencia de relaciones al cliente	671 17514
	Atención a clientes particulares y pequeñas empresas	23162298
	Centralita	671 16800
	Centralita de fax	671 16865
Nueva Zelanda Código de acceso internacional: **00** Código del país: **64**	Correo electrónico (Nueva Zelanda): nz_tech_support@dell.com	
	Correo electrónico (Australia): au_tech_support@dell.com	
	Particulares y pequeñas empresas	0800 446 255
	Gobierno y empresas	0800 444 617
	Ventas	0800 441 567
	Fax	0800 441 566
Países Bajos (Amsterdam) Código de acceso internacional: **00** Código del país: **31** Código de la ciudad: **20**	Página web: **support.euro.dell.com** Correo electrónico (Asistencia técnica): (Enterprise): nl_server_support@dell.com (Latitude): nl_latitude_support@dell.com (Inspiron): nl_inspiron_support@dell.com (Dimension): nl_dimension_support@dell.com (OptiPlex): nl_optiplex_support@dell.com (Dell Precision): nl_workstation_support@dell.com	
	Asistencia técnica	020 674 45 00
	Fax para obtener asistencia técnica	020 674 47 66
	Atención a clientes particulares y pequeñas empresas	020 674 42 00
	Asistencia de relaciones al cliente	020 674 4325

	Ventas a particulares y pequeñas empresas	020 674 55 00
	Ventas relacionales	020 674 50 00
	Fax de ventas a particulares y pequeñas empresas	020 674 47 75
	Fax de ventas relacionales	020 674 47 50
	Centralita	020 674 50 00
	Centralita de fax	020 674 47 50
Países del sureste asiático y del Pacífico	Asistencia técnica al cliente, servicio al cliente y ventas (Penang, Malasia)	604 633 4810
Panamá	Asistencia general	001-800-507-0962
Perú	Asistencia general	0800-50-669
Polonia (Varsovia) Código de acceso internacional: **011** Código del país: **48** Código de la ciudad: **22**	Página web: **support.euro.dell.com**	
	Correo electrónico: pl_support@dell.com	
	Teléfono de servicio al cliente	57 95 700
	Atención al cliente	57 95 999
	Ventas	57 95 999
	Fax de servicio al cliente	57 95 806
	Fax del mostrador de recepción	57 95 998
	Centralita	57 95 999
Portugal Código de acceso internacional: **00** Código del país: **351**	Página web: **support.euro.dell.com**	
	Correo electrónico: **support.euro.dell.com/pt/en/emaildell/**	
	Asistencia técnica	707200149
	Atención al cliente	800 300 413
	Ventas	800 300 410 ó 800 300 411 ó 800 300 412 ó 21 422 07 10
	Fax	21 424 01 12
Puerto Rico	Asistencia general	1-800-805-7545
Reino Unido (Bracknell) Código de acceso internacional: **00** Código del país: **44** Código de la ciudad: **1344**	Página web: **support.euro.dell.com**	
	Página web de atención al cliente: **support.euro.dell.com/uk/en/ECare/Form/Home.asp**	
	Correo electrónico: dell_direct_support@dell.com	
	Asistencia técnica (Cuentas corporativas/preferentes/PAD [más de 1.000 empleados])	0870 908 0500
	Asistencia técnica (directo/PAD y general)	0870 908 0800
	Atención a clientes de cuentas globales	01344 373 186
	Atención al cliente para particulares y pequeñas empresas	0870 906 0010
	Atención al cliente de corporaciones	01344 373 185
	Atención al cliente para cuentas preferentes (de 500 a 5.000 empleados)	0870 906 0010
	Atención a clientes que son parte de gobiernos centrales	01344 373 193
	Atención al cliente para gobiernos locales y centros educativos	01344 373 199
	Atención al cliente para instituciones sanitarias	01344 373 194
	Ventas a particulares y pequeñas empresas	0870 907 4000
	Ventas a sectores corporativos/públicos	01344 860 456
	Fax para particulares y pequeñas empresas	0870 907 4006
República Checa (Praga) Código de acceso internacional: **00** Código del país: **420** Código de la ciudad: **2**	Página web: **support.euro.dell.com**	
	Correo electrónico: czech_dell@dell.com	
	Asistencia técnica	02 2186 27 27
	Atención al cliente	02 2186 27 11
	Fax	02 2186 27 14
	TechFax	02 2186 27 28
	Centralita	02 2186 27 11
República Dominicana	Asistencia general	1-800-148-0530
San Kitts y Nevis	Asistencia general	gratuito: 1-877-441-4731
San Vicente y las Granadinas	Asistencia general	gratuito: 1-877-270-4609
Santa Lucía	Asistencia general	1-800-882-1521
Singapur (Singapur) Código de acceso internacional: **005** Código del país: **65**	Asistencia técnica	gratuito: 800 6011 051
	Servicio al cliente (Penang, Malasia)	604 633 4949
	Transacciones de venta	gratuito: 800 6011 054
	Ventas corporativas	gratuito: 800 6011 053
Sudáfrica (Johannesburg)	Página web: **support.euro.dell.com**	

Código de acceso internacional: **09/091** Código del país: **27** Código de la ciudad: **11**	Correo electrónico: dell_za_support@dell.com	
	Asistencia técnica	011 709 7710
	Atención al cliente	011 709 7707
	Ventas	011 709 7700
	Fax	011 706 0495
	Centralita	011 709 7700
Suecia (Upplands Vasby) Código de acceso internacional: **00** Código del país: **46** Código de la ciudad: **8**	Página web: **support.euro.dell.com**	
	Correo electrónico: swe_support@dell.com	
	Asistencia por correo electrónico para Latitude e Inspiron: Swe-nbk_kats@dell.com	
	Asistencia por correo electrónico para OptiPlex: Swe_kats@dell.com	
	Asistencia por correo electrónico para servidores: Nordic_server_support@dell.com	
	Asistencia técnica	08 590 05 199
	Asistencia de relaciones al cliente	08 590 05 642
	Atención a clientes particulares y pequeñas empresas	08 587 70 527
	Soporte EPP (Programa de Compras para Empleados)	20 140 14 44
	Asistencia técnica por fax	08 590 05 594
	Ventas	08 590 05 185
Suiza (Ginebra) Código de acceso internacional: **00** Código del país: **41** Código de la ciudad: **22**	Página web: **support.euro.dell.com**	
	Correo electrónico: swisstech@dell.com	
	Correo electrónico para clientes HSB y corporativos francófonos: **support.euro.dell.com/ch/fr/emaildell/**	
	Asistencia técnica (particulares y empresas pequeñas)	0844 811 411
	Asistencia técnica (Corporativa)	0844 822 844
	Atención al cliente (particulares y pequeñas empresas)	0848 802 202
	Atención al cliente (corporativo)	0848 821 721
	Fax	022 799 01 90
	Centralita	022 799 01 01
Tailandia Código de acceso internacional: **001** Código del país: **66**	Asistencia técnica	gratuito: 0880 060 07
	Servicio al cliente (Penang, Malasia)	604 633 4949
	Ventas	gratuito: 0880 060 09
Taiwán Código de acceso internacional: **002** Código del país: **886**	Asistencia técnica (equipos portátiles y de sobremesa)	gratuito: 00801 86 1011
	Asistencia técnica (servidores)	gratuito: 0080 60 1256
	Transacciones de venta	gratuito: 0080 651 228
	Ventas corporativas	gratuito: 0080 651 227
Trinidad y Tobago	Asistencia general	1-800-805-8035
Uruguay	Asistencia general	gratuito: 000-413-598-2521
Venezuela	Asistencia general	8001-3605

Regresar a la página de contenido

Regresar a la página de contenido

Utilización del administrador del conmutador Dell OpenManage

Sistemas Dell™ PowerConnect™ 6024/6024F

Inicio de la aplicación

1. Abra un explorador de la web.
2. Escriba la dirección IP del conmutador (tal como se define en la CLI) en la barra de direcciones y pulse <Intro>.

   Para obtener información sobre cómo asignar una dirección IP a un conmutador, consulte el apartado "Configuración inicial".
3. Cuando aparezca la ventana **Escriba la contraseña de red**, escriba un nombre de usuario y una contraseña.

NOTA: El conmutador no está configurado con una contraseña predeterminada, y puede configurarlo sin introducir ninguna contraseña. Para obtener información sobre la recuperación de una contraseña perdida, consulte el apartado "Recuperación de contraseña".

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

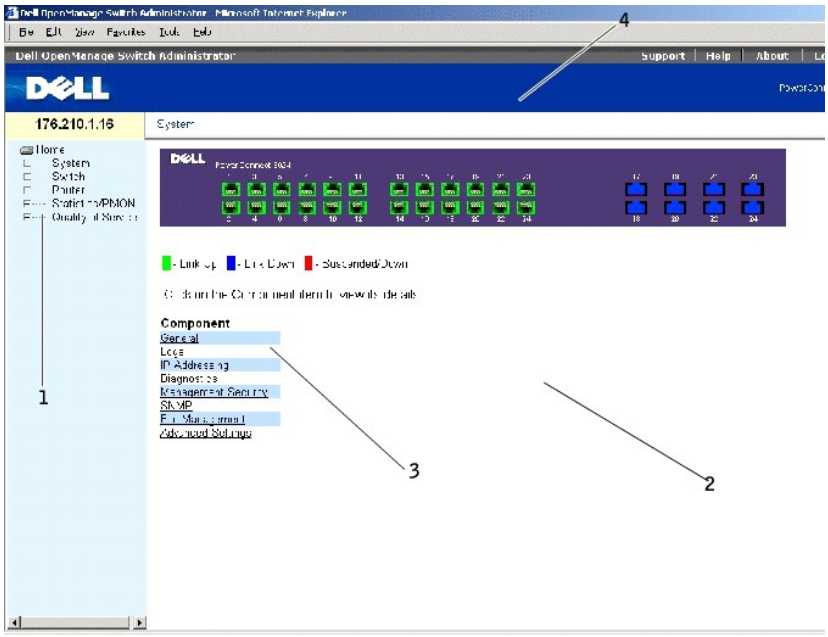
4. Haga clic en **Aceptar**.
5. Aparece la página principal de **Dell OpenManage Switch Administrator** (Administrador del conmutador Dell OpenManage).

Descripción de la interfaz

La página principal (consulte la Ilustración 4-1) contiene las siguientes vistas:

- **Vista de árbol**: situada en la parte izquierda de la página principal, la vista de árbol proporciona una vista ampliable de las funciones y sus componentes.
- **Vista de dispositivo**: situada en la parte derecha de la página principal, la vista de dispositivo proporciona una vista del dispositivo, un área de información o tabla, e instrucciones de configuración.

Ilustración 4-1. Componentes del administrador del conmutador



En la Tabla 4-1 aparecen los componentes de la interfaz con sus correspondientes números.

Tabla 4-1. Componentes de la interfaz

Componente	Nombre
1	La vista de árbol contiene una lista de las diferentes funciones del dispositivo. Las ramas de la vista de árbol se pueden expandir para ver todos los componentes de una determinada función, o se pueden retraer para ocultar los componentes de la función. Si se arrastra la barra vertical a la derecha, se puede expandir el área del árbol para ver el nombre completo de un componente.
2	La vista de dispositivo proporciona información sobre los puertos del dispositivo, el estado y la configuración actuales, información sobre la tabla, y los componentes de las funciones. El color del puerto indica si un puerto está actualmente activo. Verde indica que el puerto está activado, rojo indica que se ha producido un error en el puerto, y azul indica que la conexión se ha desactivado. **NOTA:** Los LED no aparecen en la vista de dispositivo. Sólo se puede determinar el estado de los LED observando el conmutador. Para obtener información sobre los LED, consulte el apartado "Definiciones de los LED". Según la opción que seleccione, el área situada en la parte inferior de la vista de dispositivo muestra más información sobre el dispositivo y/o los cuadros de diálogo para configurar los parámetros.
3	La lista de componentes contiene una lista de los componentes de las funciones. También puede ver los componentes si amplía una función en la vista de árbol.
4	Los botones de información proporcionan acceso a información sobre el conmutador así como acceso a la página Dell Support. Para obtener más información, consulte el apartado "Botones de información".

Utilización de los botones del administrador del conmutador

Botones de información

Tabla 4-2. Botones de información

Botón	Descripción
Support (Asistencia técnica)	Abre la página Dell Support que se encuentra en **support.dell.com**.
Help (Ayuda)	Ayuda en línea que contiene información para ayudarle a configurar y gestionar el conmutador. Las páginas de ayuda en

	línea enlazan directamente con las páginas. Por ejemplo, si la página **IP Addressing** (Direccionamiento IP) está abierta y hace clic en **Help** (Ayuda) aparecerá el tema de ayuda de esa página.
About (Acerca de)	Contiene el número de versión y compilación e información de copyright de Dell.
Log Out (Salir)	Sale de la aplicación y cierra la ventana del explorador.

Botones de gestión del dispositivo

Tabla 4-3. Botones de gestión del dispositivo

Botón	Descripción
Apply Changes (Aplicar cambios)	Aplica los cambios establecidos en el dispositivo.
Add (Agregar)	Agrega información a las tablas o cuadros de diálogo.
Telnet	Inicia una sesión de Telnet.
Query (Consulta)	Hace consultas en las tablas.
Show All (Mostrar todos)	Muestra las tablas de dispositivos.
Left arrow / Right arrow (Flecha izquierda/Flecha derecha)	Desplaza información entre las listas.
Refresh (Actualizar)	Actualiza la información sobre el dispositivo.
Reset All Counters (Restablecer todos los contadores)	Pone a cero los contadores de estadísticas.
Print (Imprimir)	Imprime la página **Network Management System** (Sistema de gestión de redes) y, o también, la información de la tabla.
Show Neighbor's Info (Mostrar información del elemento adyacente)	Muestra la **Neighbors List** (Lista de elementos adyacentes) de la página **Neighbors Table** (Tabla de elementos adyacentes).
Draw (Trazar)	Crea gráficas de estadísticas al momento.
Clear Log (Borrar registro)	Borra los mensajes de registro del búfer de registro.
Reset (Restablecer)	Restablece el conmutador.
Test Now (Probar ahora)	Ejecuta las pruebas de diagnóstico de los cables de cobre.

Definición de los campos

Los campos definidos por el usuario pueden contener de 1 a 159 caracteres, a no ser que se indique lo contrario en la página web de Dell OpenManage Switch Administrator (Administrador del conmutador Dell OpenManage).

Se pueden utilizar todos los caracteres excepto los siguientes:

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

Acceso al conmutador mediante la CLI

El conmutador se puede gestionar a través de una conexión directa con el puerto de consola o a través de una conexión Telnet. Para obtener información sobre los puertos de gestión fuera de banda, consulte el apartado "Puerto de gestión fuera de banda".

Utilizar la CLI es parecido a especificar comandos en un sistema Linux. Si el acceso es a través de una conexión Telnet, asegúrese de que el dispositivo tiene una dirección IP definida y que la estación de trabajo que se utiliza para acceder al dispositivo está conectada al dispositivo antes de empezar a usar los comandos de la CLI.

Para obtener información sobre cómo configurar una dirección IP inicial, consulte el apartado "Configuración inicial".

NOTA: Asegúrese de que el cliente está cargado antes de utilizar la CLI.

Conexión de la consola

1. Encienda el conmutador y espere hasta que se haya iniciado completamente.
2. Cuando aparezca la petición Console>, escriba enable y pulse <Intro>.
3. Configure el dispositivo y especifique los comandos necesarios para realizar las tareas requeridas.
4. Cuando haya acabado, salga de la sesión con el comando quit o exit.

NOTA: Si un usuario diferente se conecta al sistema en el modo de comando Privileged EXEC, el usuario actual se desconecta y el nuevo usuario inicia sesión.

Conexión Telnet

Telnet es un protocolo TCP/IP de emulación de terminal. Los terminales ASCII se pueden conectar de manera virtual al dispositivo local mediante una red de protocolo TCP/IP. Telnet es una alternativa a un terminal de conexión local cuando sea necesario realizar un inicio de sesión remoto.

Su conmutador admite hasta cuatro sesiones simultáneas de Telnet. Se pueden utilizar todos los comandos de la CLI en una sesión de Telnet.

Para iniciar una sesión de Telnet:

1. Seleccione **Inicio**→ **Ejecutar**.
2. En la ventana **Ejecutar**, escriba Telnet <*dirección IP*> en el campo **Abrir**.
3. Haga clic en **Aceptar** para iniciar la sesión de Telnet.

Utilización de la CLI

Visión general del modo de comando

La CLI está dividida en dos modos de comando. Cada uno de los modos de comando tiene un conjunto de comandos específicos. Si se introduce un signo de interrogación en la petición de consola, se muestra una lista de los comandos disponibles para ese determinado modo de comando.

En cada modo, se utiliza un comando específico para navegar de un modo de comando a otro.

Durante el inicio de la sesión de la CLI, el modo de la CLI es el modo User EXEC o modo de ejecución de usuario. En el modo User EXEC sólo hay disponibles un subconjunto limitado de comandos. Este nivel se reserva para tareas que no cambian la configuración de la consola y se utiliza para acceder a subsistemas de configuración como la CLI. Para pasar al siguiente nivel, el modo Privileged EXEC o modo de ejecución privilegiado, es necesaria una contraseña (si está configurada).

El modo Privileged EXEC proporciona acceso a la configuración global del dispositivo. Para realizar configuraciones globales específicas dentro del dispositivo, pase al siguiente nivel, el modo Global Configuration o modo de configuración global. No es necesaria ninguna contraseña.

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

El modo Interface Configuration o modo de configuración de interfaz configura el dispositivo en el nivel de interfaz física. Los comandos de interfaz que requieren subcomandos tienen otro nivel denominado modo Subinterface Configuration o modo de configuración de subinterfaz. No es necesaria ninguna contraseña.

Modo User EXEC

Después de conectarse al dispositivo, se activa el modo de comando User EXEC. La petición de nivel de usuario está formada por el nombre del sistema principal seguido del paréntesis angular (>). Por ejemplo,

```
Console>
```

NOTA: El nombre del sistema principal predeterminado es console a no ser que se haya modificado durante la configuración inicial.

Los comandos User EXEC permiten conectarse con dispositivos remotos, cambiar la configuración del terminal de manera temporal, realizar pruebas básicas y enumerar la información del sistema.

Para obtener una lista de los comandos User EXEC, introduzca un signo de interrogación en la petición de comando.

Modo Privileged EXEC

El acceso privilegiado se puede proteger para impedir el acceso no autorizado y asegurar los parámetros de funcionamiento. Las contraseñas aparecen en la pantalla y distinguen entre mayúsculas y minúsculas.

Para acceder y ver una lista de los comandos del modo Privileged EXEC:

1. En la petición escriba enable y pulse <Intro>.
2. Cuando aparezca una petición de contraseña, introduzca la contraseña y pulse <Intro>.

La petición del modo Privileged EXEC aparece como el nombre de sistema principal del dispositivo seguido del símbolo #. Por ejemplo,

```
Console#
```

Para obtener una lista de los comandos Privileged EXEC, escriba un signo de interrogación en el símbolo del sistema y pulse <Intro>.

Para pasar del modo Privileged EXEC al modo User EXEC utilice uno de los siguientes comandos: disable, exit/end o <Ctrl><Z>.

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 a un modo anterior. Por ejemplo, puede pasar del modo Interface Configuration al modo Global Configuration, y del modo Global Configuration al modo Privileged EXEC.

Modo Global Configuration

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

Para acceder al modo Global Configuration, en la petición del modo Privileged EXEC, escriba `configure` y pulse <Intro>. El modo Global Configuration aparece como el nombre del sistema principal del dispositivo seguido de (config) y el símbolo de la almohadilla #.

```
Console (config)#
```

Para obtener una lista de los comandos Global Configuration, introduzca un signo de interrogación en la petición de comando.

Para volver del modo Global Configuration al modo Privileged EXEC, escriba el comando `exit` o utilice el comando <Ctrl><Z>.

En el ejemplo siguiente se muestra cómo acceder al modo Global Configuration y volver al modo Privileged EXEC:

```
Console#

Console# configure

Console (config)# exit

Console#
```

Modo Interface Configuration

Los comandos de configuración de la interfaz modifican la configuración específica de la dirección IP, incluido el grupo de puentes, la descripción, etc. Los modos Interface Configuration son:

- **VLAN**: contiene los comandos para crear y configurar una VLAN como un todo, por ejemplo, para crear una VLAN y aplicarle una dirección IP.
- **Port Channel** (Canal de puerto): contiene los comandos para configurar grupos de agregados de conexiones (LAG).
- **IP**: contiene los comandos para gestionar las interfaces IP.
- **Out-of-Band-Ethernet** (Ethernet fuera de banda): contiene los comandos para gestionar y configurar las conexiones de gestión.

Ejemplos de la CLI

Los comandos de la CLI se proporcionan como ejemplos de configuración. Para obtener una descripción completa de los comandos de la CLI, incluidos ejemplos, consulte la publicación "CLI Reference Guide" (Guía de referencia CLI) del conmutador.

Regresar a la página de contenido

Regresar a la página de contenido

Descripción del hardware

Sistemas Dell™ PowerConnect™ 6024/6024F

Esta sección contiene información sobre las características de los dispositivos y las configuraciones del hardware del módulo.

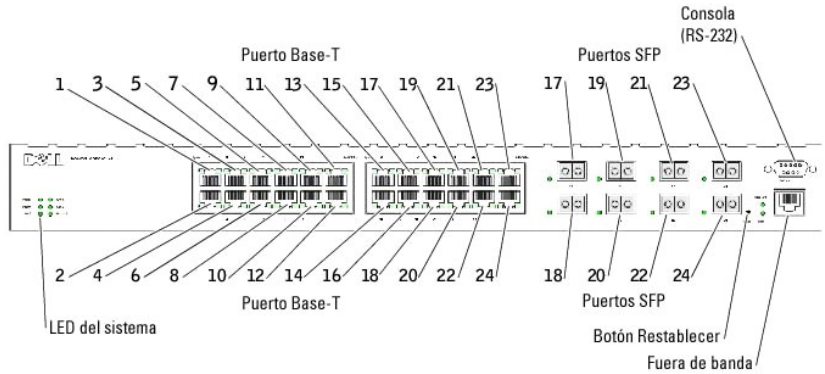
Descripción de los puertos

PowerConnect 6024

Los puertos del 1 al 16 se han designado como puertos 10/100/1000, y los puertos del 17 al 24 se han designado como puertos combinados. Los números de puerto se muestran en la siguiente ilustración:

Un puerto combinado es un único puerto lógico con dos conexiones físicas (una conexión RJ-45 y una conexión SFP). Cuando se inserta un conector en el puerto SFP, éste se activa a menos que el conector de cobre del puerto Base-T del mismo número esté insertado y haya establecido una conexión.

Ilustración 2-1. PowerConnect 6024 con 24 puertos Base-T 10/100/1000



El conmutador detecta automáticamente las diferencias entre los cables cruzados y directos conectados a los puertos RJ-45. Los puertos SFP admiten tanto los módulos SX como LX.

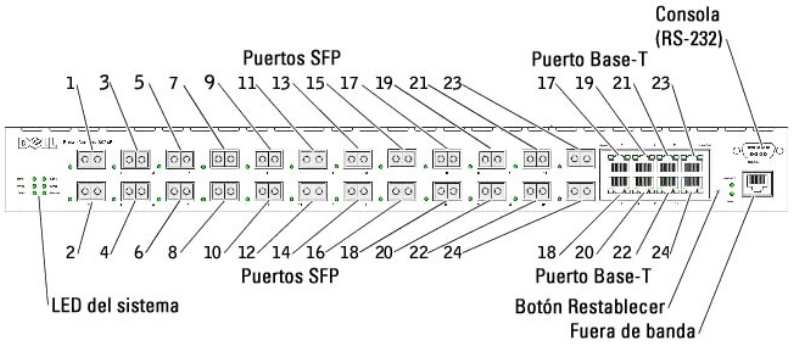
Los puertos RJ-45 admiten las transferencias en modo dúplex medio y dúplex completo de 10/100/1000 Mbps.

PowerConnect 6024F

Los puertos PowerConnect 6024F difieren de los puertos PowerConnect 6024 sólo en la designación del puerto: Los puertos del 1 al 16 se han designado como puertos SFP y los puertos del 17 al 24 como puertos combinados. Los números de puerto se muestran en la siguiente ilustración:

Para obtener información sobre cómo funcionan los puertos, consulte la descripción de los puertos para el modelo PowerConnect 6024.

Ilustración 2-2. PowerConnect 6024F con 24 puertos SFP



Puerto de gestión fuera de banda

El puerto de gestión OOB (Fuera de banda) es un puerto Ethernet a 10/100 Mbps que se puede conectar directamente al conmutador para trabajar con aplicaciones de gestión de administrador del sistema. El sistema considera al puerto fuera de banda como una interfaz IP y a través del mismo se puede acceder a todas las interfaces de gestión.

Para obtener más información sobre la configuración fuera de banda, consulte el apartado "Puerto de gestión fuera de banda".

Puerto de consola (RS-232)

El puerto (RS-232) de la consola se utiliza solamente a efectos de gestión a través de una interfaz serie. Este puerto es una conexión directa al conmutador, que se utiliza para acceder a la CLI desde un terminal de consola conectado a un puerto EIA/TIA-232.

El puerto de la consola admite ocho bits de datos sincrónicos, un bit de parada y ningún bit de paridad. La velocidad en baudios predeterminada es de 115.200 bps.

Componentes de hardware

Dimensiones físicas

El conmutador tiene las siguientes dimensiones físicas:

- 440 x 460 x 44 mm (A x P x A).
- 17,32 x 18,11 x 1,73 pulgadas (A x P x A).

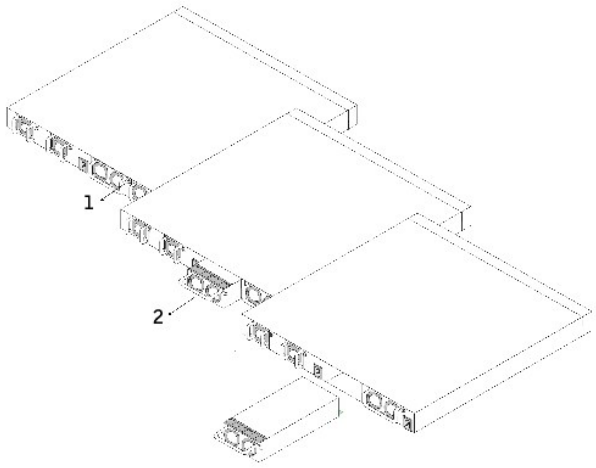
Fuentes de alimentación

El conmutador se suministra con dos fuentes de alimentación internas. Puede verificar su funcionamiento a través de los LED. Consulte el apartado "LED del sistema" para obtener información.

Para sustituir una fuente de alimentación:

1. Retire la unidad de la fuente de alimentación defectuosa; para ello, afloje el tornillo correspondiente en el panel posterior y extráigala.
2. Inserte una fuente de alimentación nueva en la ranura y asegúrese de que se haya insertado completamente en el conmutador.

Ilustración 2-3. Inserción de la fuente de alimentación



3. Inserte y apriete el tornillo de la fuente de alimentación.
4. Conecte las fuentes de alimentación a tomas de corriente externas distintas.

   Cuando se conecta a una toma de alimentación distinta, se reduce la probabilidad de que el conmutador deje de funcionar a causa de un corte del suministro eléctrico.

Botón de restablecimiento

El botón de restablecimiento, situado en el panel anterior, restablece manualmente el conmutador.

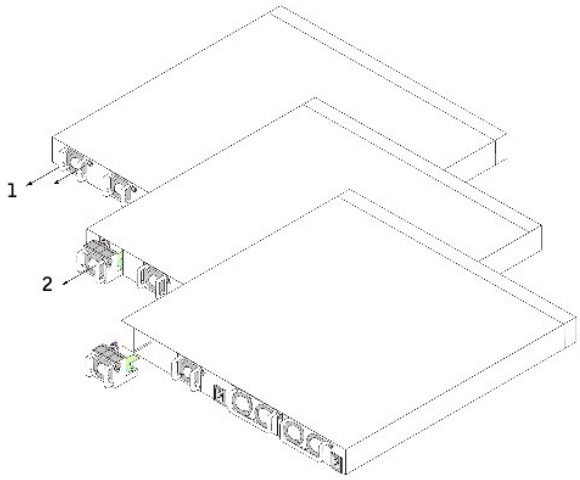
Sistema de ventilación

En el sistema hay dos ventiladores. Puede verificar su funcionamiento a través de los LED. Consulte el apartado "LED del sistema" para obtener información.

Para sustituir un ventilador:

1. Retire los dos tornillos y, suavemente, extraiga el ventilador que se haya estropeado.
2. Inserte con cuidado el nuevo ventilador en la ranura.

Ilustración 2-4. Instalación/sustitución del ventilador



3. Inserte y apriete el tornillo del ventilador.

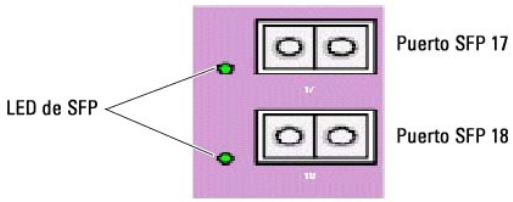
Definiciones de los LED

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

LED del puerto SFP

En la Ilustración 2-5 se muestran los LED del puerto SFP que están ubicados junto a cada puerto SFP.

Ilustración 2-5. LED del puerto SFP



La Tabla 2-1 contiene las definiciones de los LED del puerto SFP:

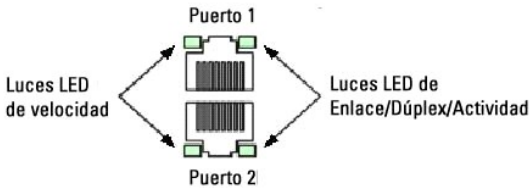
Tabla 2-1. Definiciones de los LED del puerto SFP

LED	Color	Definición
SFP	Verde	El puerto está vinculado actualmente.
	Verde parpadeante	El puerto está enviando o recibiendo tráfico de red actualmente.
	Desactivado	El puerto no está vinculado actualmente.

LED del puerto Base-T 10/100/1000

Cada puerto Base-T 10/100/1000 tiene dos LED. El LED de velocidad está ubicado en el lado izquierdo del puerto, mientras que el LED de conexión/dúplex/actividad está ubicado en el derecho. En la siguiente ilustración se muestran los LED del puerto Base-T 10/100/1000:

Ilustración 2-6. LED del puerto Base-T 10/100/1000



La Tabla 2-2 contiene las definiciones de los LED del puerto Base-T 10/100/1000.

Tabla 2-2. Definiciones del puerto Base-T 10/100/1000

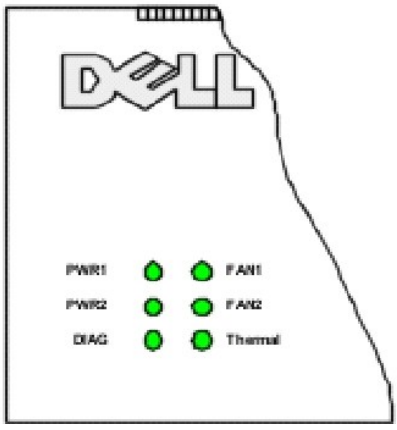
LED	Color	Definición
Velocidad		
	Verde	El puerto está funcionando a 1000 Mbps.
	Ámbar	El puerto está funcionando a 100 Mbps.
	Desactivado	El puerto está funcionando a 10 Mbps.
Enlace		
	Verde	El puerto está funcionando, y el modo dúplex completo está activo.
	Verde parpadeante	El puerto está enviando o recibiendo paquetes y está funcionando en el modo dúplex completo.
	Ámbar	El puerto está funcionando, y el modo dúplex medio está activo.
	Ámbar parpadeante	El puerto está enviando o recibiendo paquetes y está funcionando en el modo dúplex medio.
	Desactivado	El puerto no está vinculado.

LED del sistema

Los LED del sistema, ubicados en la parte izquierda del panel anterior, proporcionan información sobre las fuentes de alimentación, ventiladores, condiciones térmicas y diagnósticos.

En la Ilustración 2-7 se muestran los LED del sistema.

Ilustración 2-7. LED del sistema



La Tabla 2-3 contiene las definiciones de los LED del sistema.

Tabla 2-3. Definiciones de los LED del sistema

LED	Color	Definición
Fan 1 (Ventilador 1)		
	Verde	El ventilador 1 está presente y en funcionamiento.
	Rojo	El ventilador 1 está presente, pero no funciona.
	Desactivado	El ventilador 1 no está presente.
Fan 2 (Ventilador 2)		
	Verde	El ventilador 2 está presente y en funcionamiento.
	Rojo	El ventilador 2 está presente, pero no funciona.
	Desactivado	El ventilador 2 no está presente.
PWR1 (Fuente alim. 1)		
	Verde	La fuente de alimentación 1 está presente y en funcionamiento.
	Rojo	La fuente de alimentación 1 está presente, pero no funciona.
	Desactivado	La fuente de alimentación 1 no está presente.
PWR2 (Fuente alim. 2)		
	Verde	La fuente de alimentación 2 está presente y en funcionamiento.
	Rojo	La fuente de alimentación 2 está presente, pero no funciona.
	Desactivado	La fuente de alimentación 2 no está presente.
Dia (Diagnóstico)		
	Verde parpadeante	Actualmente hay en curso una prueba de diagnósticos.
	Verde	La prueba de diagnósticos ha finalizado correctamente.
	Rojo	La prueba de diagnósticos ha fallado.
Thermal (Temperatura)		
	Rojo	El sistema ha excedido la temperatura máxima.
	Desactivado	La temperatura del sistema es normal.

Regresar a la página de contenido

Regresar a la página de contenido

Introducción

Sistemas Dell™ PowerConnect™ 6024/6024F

AVISO: Antes de continuar, lea las notas de la versión de este producto. Puede descargar estas notas del sitio web **support.dell.com**.

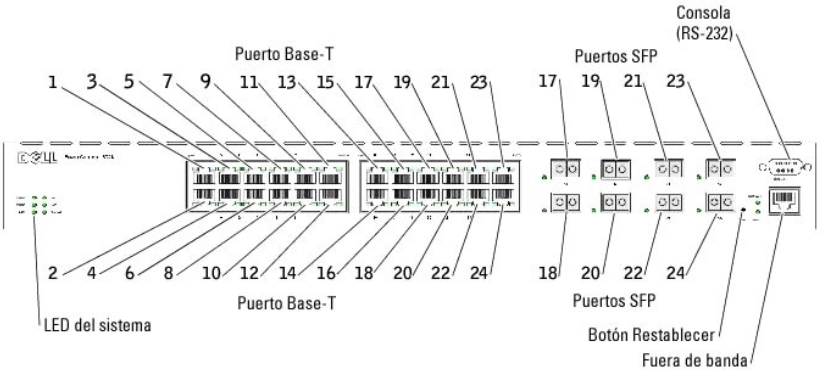
El conmutador Dell™ PowerConnect™ 6024/6024F es un conmutador independiente de nivel 3 que amplía la gama de productos de conmutación LAN Dell PowerConnect. Este conmutador presenta las características siguientes:

- Diseño de chasis montable en estante con formato de 1U.
- Puerto de gestión fuera de banda para conexiones RJ-45 y RS-232.
- Compatibilidad con todos los requisitos de comunicación de datos de un conmutador de múltiples niveles, incluida una amplia gama de funciones de nivel 2, nivel 3+, seguridad y gestión.
- Alta disponibilidad con fuentes de alimentación de intercambio dinámico y ventiladores de enfriamiento.

PowerConnect 6024

El conmutador PowerConnect 6024 proporciona 24 puertos Base-T 10/100/1000 RJ-45 con ocho puertos combinados SFP que disponen de un modo de detección automática de la velocidad, el control del flujo y el modo dúplex. Los transceptores SFP se venden por separado.

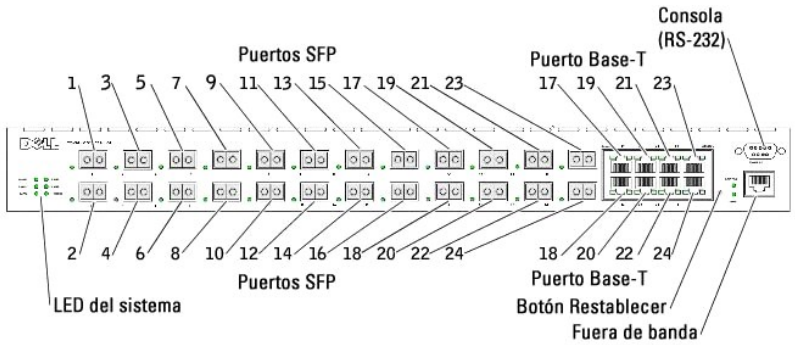
Ilustración 1-1. PowerConnect 6024



PowerConnect 6024F

El conmutador PowerConnect 6024F proporciona 24 puertos SFP con 8 puertos combinados 10/100/1000 Base-T RJ-45 que disponen de un modo de detección automática de la velocidad, el control del flujo y el modo dúplex. Los transceptores SFP se venden por separado.

Ilustración 1-2. PowerConnect 6024F



Documentación de la CLI

La publicación *CLI Reference Guide* (Guía de referencia CLI) proporciona información acerca de los comandos de la CLI que se utilizan para configurar el conmutador. En este documento se ofrecen los valores predeterminados, la sintaxis y las descripciones de la CLI.

Funciones

En este apartado se describen las funciones del conmutador que puede configurar el usuario. Para obtener una lista de todas las funciones, consulte las notas de la versión del software.

Funciones basadas en el puerto

Pruebas virtuales de cable (VCT)

Las VCT sirven para detectar e informar sobre los posibles problemas de los cables de conexión de cobre, como cables desconectados o cortocircuitos.

Compatibilidad con tramas gigantes

Las tramas gigantes permiten transportar datos idénticos en menos tramas para garantizar un menor coste, un tiempo de procesamiento inferior y menos interrupciones.

Compatibilidad con MDI/MDIX

El conmutador admite la autodetección entre cables de red cruzados y directos.

El cableado estándar para las estaciones terminales es MDI (Interfaz dependiente de los soportes) y el cableado estándar para los concentradores y conmutadores se conoce como MDIX (Interfaz dependiente de los soportes con cable cruzado).

Para obtener información sobre la configuración de MDI/MDI para puertos o LAG, consulte el apartado "Definición de la configuración de puertos" o "Definición de la configuración de LAG".

Compatibilidad con la vigilancia de hardware

El conmutador utiliza la vigilancia de hardware para detectar problemas y tomar medidas correctivas cuando el software deja de responder.

Negociación automática

La negociación automática permite al dispositivo dar a conocer los modos de funcionamiento. La función de negociación automática proporciona los medios para intercambiar información entre dos dispositivos que comparten un segmento de enlace punto a punto y para configurar automáticamente ambos dispositivos con el objetivo de sacar el máximo partido a las posibilidades de transmisión que ofrecen.

El sistema PowerConnect 6024/6024F amplía la negociación automática mediante el anuncio de los puertos. El hecho de dar a conocer los puertos permite al administrador del sistema configurar las velocidades de los puertos anunciadas.

Para obtener información sobre la negociación automática, consulte el apartado "Definición de la configuración de puertos" o "Definición de la configuración de LAG".

Compatibilidad con el control de flujo (IEEE 802.3X)

El control de flujo permite que dispositivos de menor velocidad se comuniquen con dispositivos de mayor velocidad al solicitar que el dispositivo de velocidad superior se abstenga de enviar paquetes. Las transmisiones se detienen temporalmente para evitar que se produzcan desbordamientos del búfer.

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

Prevención de bloqueo de la cabecera de línea

El bloqueo de HOL (Cabecera de línea) evita que se produzcan retrasos en el tráfico y que se pierda la trama debido a que el tráfico compite por los mismos recursos del puerto de salida. El bloqueo HOL pone en cola los paquetes, y los paquetes situados al principio de la cola se envían antes que los paquetes situados al final de la cola.

Compatibilidad con la contrapresión

En las conexiones de dúplex medio, un receptor puede evitar que se produzcan desbordamientos de búfer ocupando el enlace de modo que éste no esté disponible al tráfico adicional.

Para obtener información sobre la configuración de la contrapresión para los puertos o LAG, consulte el apartado "Definición de la configuración de puertos" o "Definición de la configuración de LAG".

Funciones compatibles con las direcciones MAC

Compatibilidad con las direcciones MAC

El conmutador admite direcciones MAC de hasta 16K y reserva direcciones MAC específicas para que las utilice el sistema.

Obtención automática de direcciones MAC

El conmutador permite que se obtengan automáticamente las direcciones MAC de los paquetes entrantes.

Caducidad automática de las direcciones MAC

Las direcciones MAC en las que no ha habido tráfico durante un período de tiempo determinado caducan, lo que impide que la tabla de direcciones se desborde.

Para obtener información sobre la configuración del período de caducidad de las direcciones MAC, consulte el apartado "Visualización de direcciones dinámicas".

Entradas MAC estáticas

Las entradas MAC definidas por el usuario se almacenan en la tabla de direcciones con las direcciones obtenidas automáticamente.

Para obtener información sobre la configuración de las direcciones MAC estáticas, consulte el apartado "Definición de direcciones estáticas".

Conmutación basada en MAC compatible con VLAN

Los paquetes que llegan de una dirección de origen desconocido se envían a la CPU y se agregan a la tabla de hardware. Los paquetes que en el futuro se envíen a esta dirección o desde esta dirección se reenvían de manera más eficaz.

Compatibilidad con la multidifusión de MAC

El servicio de multidifusión es un servicio de difusión limitado que permite conexiones de uno a varios y de varios a varios. En los servicios de multidifusión de nivel 2, se recibe una sola trama dirigida a una dirección de multidifusión específica, y se crean copias de la trama que se va a transmitir en cada puerto relevante.

Para obtener información sobre la configuración de la compatibilidad con la multidifusión de MAC, consulte el apartado "Compatibilidad con el reenvío de multidifusión".

Funciones del nivel 2

Inspección IGMP

La inspección IGMP examina el contenido de las tramas IGMP cuando el conmutador las reenvía desde estaciones a un enrutador de multidifusión que precede en la cadena. La inspección permite que el conmutador identifique las estaciones interesadas en sesiones de multidifusión y qué enrutadores de multidifusión envían tramas de multidifusión.

Para obtener información sobre la configuración de la inspección IGMP, consulte el apartado "Inspección IGMP".

Duplicación de puertos

La duplicación de puertos supervisa y duplica el tráfico de red mediante el reenvío de copias de paquetes entrantes y salientes desde un puerto a un puerto de supervisión.

Para obtener información sobre la configuración de la duplicación de puertos, consulte el apartado "Definición de sesiones de duplicación de puertos".

Control de tormentas de difusión

Cuando se reenvían las tramas de nivel 2, las tramas de difusión y multidifusión se desbordan en todos los puertos de la VLAN relevante. El desbordamiento ocupa la amplitud de banda, y carga todos los nodos conectados en todos los puertos. El control de tormentas limita la cantidad de tramas de multidifusión y difusión que el conmutador acepta y reenvía.

Para obtener información sobre la configuración del control de tormentas, consulte el apartado "Habilitación del control de tormentas".

Funciones compatibles con VLAN

Compatibilidad con VLAN

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

Para obtener información sobre la configuración de VLAN, consulte el apartado "Configuración de VLAN".

VLAN basadas en puertos

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

Para obtener información sobre la configuración de las VLAN, consulte el apartado "Configuración de VLAN".

VLAN basadas en el protocolo IEEE802.1V

Las normas de clasificación de VLAN se definen según la identificación del protocolo de nivel de enlace de datos (nivel 2). Las VLAN basadas en protocolos se utilizan para aislar el tráfico de nivel 2 de forma que se diferencie de los protocolos de nivel 3.

Para obtener información sobre la definición de VLAN basadas en protocolos, consulte el apartado "Definición de grupos de protocolos de VLAN".

Cumplimiento absoluto con el estándar de etiquetado 802.1Q VLAN

El estándar IEEE 802.1Q define una arquitectura para las LAN con puentes virtuales, los servicios proporcionados en las VLAN, y los protocolos y algoritmos que participan en la oferta de estos servicios.

Un requisito de este estándar es la posibilidad de marcar tramas con el valor de etiqueta (0-7) CoS (Clase de servicio) que desee.

Compatibilidad con GVRP

El GVRP (Protocolo de registro VLAN GARP) proporciona la creación dinámica de VLAN y la eliminación de VLAN de acuerdo con el estándar IEEE 802.1Q en los puertos troncales 802.1Q. Cuando se habilita GVRP, el conmutador registra y propaga la pertenencia a VLAN a todos los puertos que forman parte de la topología activa subyacente del protocolo de árbol de expansión.

Para obtener información sobre la configuración de GVRP, consulte el apartado "Configuración de GVRP".

PVE (Private VLAN Edge)

Los puertos PVE son una función de seguridad de nivel 2 que proporciona seguridad basada en puertos entre los puertos contiguos de una VLAN. Es una extensión de la VLAN común. El tráfico de los puertos protegidos se envía únicamente a los puertos de enlace ascendente y no se puede enviar a otros puertos de la VLAN.

Para obtener información sobre la configuración de los puertos PVE, consulte el apartado "Configuración de puertos".

Funciones del protocolo de árbol extensible

STP (Protocolo de árbol extensible) por dispositivo

El STP 802.1d es un requisito estándar de los conmutadores de nivel 2 que permite a los puentes impedir y solucionar automáticamente los bucles de reenvío de nivel 2. Los conmutadores intercambian mensajes de configuración, utilizando tramas formateadas específicamente, y habilitan e inhabilitan de manera selectiva el reenvío en los puertos.

Para obtener información sobre la configuración de STP, consulte el apartado "Configuración del protocolo de árbol extensible".

Conexión rápida

STP puede tardar entre 30 y 60 segundos en converger mientras detecta posibles bucles y permite que los cambios de estado se propaguen y que los dispositivos relevantes respondan. Esta duración se considera excesiva para muchas aplicaciones. Fast Link omite este retraso sin necesidad de varias rutas de datos para la resistencia de la red.

Para obtener información sobre la habilitación de Fast Link para puertos y LAG, consulte el apartado "Definición de la configuración de puertos" o "Definición de la configuración de LAG".

Árbol extensible rápido compatible con el estándar IEEE 802.1w

RSTP (Rapid Spanning Tree Protocol) detecta las topologías de red para permitir una convergencia más rápida, sin crear bucles de reenvío.

Para obtener información sobre la habilitación de RSTP, consulte el apartado "Definición del árbol extensible rápido".

Árbol extensible múltiple

La operación MSTP (Árbol extensible múltiple) asigna VLAN a las instancias ST. MSTP proporciona un escenario de equilibrio de carga diferente. Los paquetes asignados a varias VLAN se transmiten por diferentes rutas de acceso dentro de las regiones MSTP (regiones de árboles extensibles múltiples). Las regiones son uno o más puentes MSTP interconectados con una configuración MSTP idéntica. El estándar permite a los administradores asignar tráfico de VLAN a rutas de acceso únicas.

Para obtener más información sobre MSTP, consulte el apartado "Definición del árbol extensible múltiple".

Agregado de conexiones

Agregado de conexiones

Se pueden combinar hasta siete puertos para que formen un solo LAG (Grupo agregado de conexiones). Esto permite la protección con tolerancia de fallos contra la interrupción de conexiones físicas, unas conexiones con mayor amplitud de banda y una resolución de amplitud de banda mejorada.

Un LAG está compuesto por puertos de la misma velocidad, establecidos para funcionar en dúplex completo.

Para obtener información sobre la configuración de LAG, consulte el apartado "Definición de la configuración de LAG".

Agregado de conexiones y LACP

LACP utiliza intercambios de igual a igual entre enlaces para determinar, de manera continua, la capacidad de adición de diferentes enlaces, y proporciona el máximo nivel de capacidad de adición posible entre un par determinado de sistemas. LACP determina, configura, enlaza y supervisa automáticamente el enlace de puertos con agregadores dentro del sistema.

Para obtener información acerca de LACP, consulte el apartado "Definición de los parámetros del LACP".

Funciones de encaminamiento

Encaminamiento IP

El encaminamiento IP envía a un dispositivo de próximo salto todos los paquetes que se dirigen a las direcciones MAC del sistema pero no a una dirección IP del sistema.

Para obtener información sobre la configuración del encaminamiento IP, consulte el apartado "Configuración del encaminamiento IP global".

Versiones 1 y 2 de RIP

RIP (Protocolo de información de encaminamiento) es un protocolo de encaminamiento del vector de distancia. RIP selecciona las rutas según el recuento de saltos hasta el destino. RIP 2 mejora la eficacia, el uso y los métodos de autenticación del protocolo RIP.

Para obtener información sobre la configuración de RIP, consulte el apartado "Configuración de RIP".

Versión 2 de OSPF

OSPF (Protocolo de encaminamiento Abrir primero la ruta de acceso más corta) es un protocolo interno de encaminamiento de puerta de enlace. En las redes que cuentan con un gran número de enrutadores interconectados, OSPF es más eficaz que RIP puesto que OSPF utiliza menos amplitud de banda de conexión y converge más rápidamente.

Para obtener información sobre la configuración de OSPF, consulte el apartado "Configuración de parámetros y filtros de OSPF".

Protocolo de resolución de direcciones (ARP)

En el encaminamiento IP, los enrutadores y los conmutadores de nivel 3 utilizan diferentes protocolos de encaminamiento para descubrir la topología de red y definir las tablas de encaminamiento. ARP determina automáticamente las direcciones MAC de próximo salto del dispositivo de los sistemas, incluidos los sistemas finales conectados directamente. Los usuarios pueden hacer prevalecer esto y complementarlo mediante la definición de más entradas de la tabla ARP.

Para obtener información sobre la configuración de ARP, consulte el apartado "Definición de la configuración de ARP".

Mensajes ICMP

Los mensajes ICMP (Protocolo de mensajes de control de Internet) se utilizan para los mensajes fuera de banda relacionados con el fallo o el funcionamiento

de la red.

IGMPv2

IGMP permite que el enrutador envíe consultas IGMP en forma de difusiones de nivel 2 en cada interfaz. Cuando se envía un paquete de multidifusión, y tiene una dirección MAC de destino de multidifusión, todos los sistemas principales en esa interfaz de enrutador reciben una copia. Los sistemas principales escuchan todos los informes IGMP. Si cualquier estación de la misma interfaz ya ha solicitado grupos de multidifusión interesados, las estaciones restantes no envían peticiones duplicadas.

Para obtener información sobre la configuración de IGMP, consulte el apartado "Definición de parámetros de la interfaz de IGMP".

Compatibilidad con las coincidencias de prefijo más largo

Las coincidencias de prefijo más largo se utilizan principalmente para determinar la mejor ruta de próximo salto para un paquete basándose solamente en la dirección de destino que contiene el encabezado del paquete. Puesto que las direcciones IP normalmente se asignan de manera que reflejen la topología de la red, el resultado de una coincidencia de prefijo más largo refleja la ruta más corta hasta el destino.

DVMRP

DVMRP (Protocolo de encaminamiento de multidifusión de vector de distancia) anuncia las rutas más cortas a las redes de origen de multidifusión con sistemas principales que pueden transmitir tráfico IP de multidifusión.

Para obtener información sobre la configuración de DVMRP, consulte el apartado "Configuración de interfaces de DVMRP".

VRRP

VRRP (Protocolo de redundancia de enrutador virtual) elimina puntos únicos de fallo en el entorno del encaminamiento. VRRP utiliza un protocolo de elección que asigna de manera dinámica la responsabilidad del enrutador virtual a uno de los enrutadores VRRP de la LAN.

El proceso de elección proporciona una conmutación por errores dinámica en la responsabilidad de reenvío, si el maestro no está disponible. Los sistemas principales finales pueden utilizar cualquier dirección IP del enrutador virtual como enrutador de primer salto predeterminado.

Para obtener información sobre la configuración de VRRP, consulte el apartado "Configuración de VRRP".

Funciones del nivel 3

TCP

Las conexiones del protocolo de control de transmisiones (TCP) están definidas entre 2 puertos por un intercambio de sincronización inicial. Los puertos TCP se identifican mediante una dirección IP y un número de puerto de 16 bits. Las secuencias de octetos se dividen en paquetes TCP, cada uno de los cuales lleva un número de secuencia.

Relé UDP

El relé UDP permite que el dispositivo reenvíe difusiones UDP específicas de una interfaz a otra. Los paquetes de difusión IP de una interfaz no suelen reenviarse a otra interfaz. Sin embargo, algunas aplicaciones utilizan la difusión UDP para detectar la disponibilidad de un servicio. Otros servicios requieren que los paquetes de difusión UDP se encaminen para proporcionar servicios a los clientes de otra subred.

Clientes de BootP y DHCP

DHCP permite que se reciban parámetros de configuración adicional de un servidor de red al iniciar el sistema. El servicio DHCP es un proceso continuo. DHCP es una ampliación de BootP.

Para obtener información acerca de DHCP, consulte el apartado "Definición de los parámetros de interfaz IP DHCP".

Relé BootP

BootP permite a un dispositivo solicitar y recibir datos de configuración de los servidores. Si el servidor BootP previsto no está directamente conectado a un dominio de difusión del cliente, un servicio de relé BootP permite que el cliente llegue al servidor.

Relé DHCP

DHCP permite a un dispositivo solicitar y recibir datos de configuración de los servidores. Si el servidor DHCP previsto no está directamente conectado a un dominio de difusión del cliente, un servicio de relé DHCP permite que el cliente llegue al servidor.

Para obtener información sobre la configuración de los parámetros del relé DHCP, consulte el apartado "Definición de los parámetros del relé DHCP".

Funciones de QoS

Compatibilidad con QoS

Para superar el tráfico de red impredecible y optimizar el rendimiento, puede aplicar QoS (Calidad de servicio) en toda la red para garantizar que el tráfico de red se prioriza de acuerdo con criterios específicos. El conmutador admite dos modos de QoS: básico y avanzado.

Compatibilidad con la clase de servicio 802.1p

La técnica de señalización IEEE 802.1p es un estándar OSI de nivel 2 para etiquetar y priorizar el tráfico de red en el subnivel MAC/enlace de datos. El tráfico de 802.1p se clasifica y se envía al destino; no se establecen ni aplican límites o reservas de amplitud de banda. El estándar 802.1p establece ocho niveles de prioridad, similar al campo de bits IP Precedence IP Header.

Modo básico de QoS

En el modo básico de QoS, se puede activar un modo de confianza (para confiar en VPT, DSCP, TCP/UDP o en ninguno). Además, se puede adjuntar una sola lista de control de acceso a una interfaz.

Para obtener información sobre la habilitación del modo básico de QoS, consulte el apartado "Configuración del modo básico de QoS".

Modo avanzado de QoS

El modo avanzado de QoS especifica la clasificación del flujo y asigna acciones de regla que se relacionan con la gestión de la amplitud de banda. Estas reglas se pueden agrupar en una política, que se puede aplicar a una interfaz.

Para obtener información acerca de la habilitación del modo avanzado de QoS, consulte el apartado "Configuración del modo avanzado de QoS".

Funciones de gestión del dispositivo

Registros de capturas y alarmas de SNMP

El sistema registra eventos con códigos de gravedad y marcas de hora. Los eventos se envían como capturas SNMP a una lista de destinatarios de capturas.

Para obtener información sobre capturas y alarmas SNMP, consulte el apartado "Definición de los parámetros de SNMP".

Gestión basada en web

Puede gestionar cualquier sistema desde cualquier explorador de la web. El conmutador contiene un servidor web incorporado que ejecuta páginas HTML que puede utilizar para supervisar y configurar el sistema.

Descarga de los archivos de configuración

El archivo de configuración del conmutador incluye datos de configuración de dispositivos específicos del puerto y de todo el sistema. Puede visualizar los archivos de configuración mediante los comandos CLI.

Para obtener información sobre la descarga de archivos de configuración, consulte el apartado "Descarga de archivos".

Descarga de software

La descarga de software permite el almacenamiento de imágenes de firmware de copia de seguridad. Para obtener información sobre la descarga del software, consulte el apartado "Descarga del software y reinicio".

TFTP (Trivial File Transfer Protocol)

PowerConnect 6024/6024F admite imágenes de inicio, firmware y carga /descarga de configuración a través del protocolo TFTP.

Supervisión remota

RMON (Supervisión remota) es una ampliación del protocolo SNMP que proporciona funciones completas de supervisión del *tráfico* de la red (a diferencia de SNMP, que permite gestionar y supervisar *dispositivos* de la red). 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 a lo largo de toda la red.

Para obtener información sobre RMON, consulte el apartado "Visualización de las estadísticas de RMON".

SNMP versión 1, 2 y 3

Para controlar 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 sus privilegios de acceso. Hay tres niveles de seguridad SNMP: sólo lectura, lectura/escritura y super. Sólo un superusuario puede acceder a la tabla de comunidad.

Interfaz de línea de comandos

La sintaxis y la semántica de la interfaz de línea de comandos (CLI) se ajustan tanto como es posible a las prácticas habituales del sector. CLI se compone de elementos obligatorios y opcionales. La ayuda relativa al contexto proporciona el formato y los intervalos de valores permitidos para los comandos actuales, y el intérprete de comandos CLI proporciona la realización de comandos y palabras clave.

Syslog

Syslog es un protocolo que permite que las notificaciones de eventos se envíen a un conjunto de servidores remotos específicos donde se pueden almacenar, examinar y actuar en consecuencia.

Para obtener información sobre Syslog, consulte el apartado "Gestión de registros".

SNTP

El protocolo SNTP garantiza una sincronización precisa del tiempo del reloj del conmutador de red en milisegundos. La sincronización del tiempo la realiza un servidor SNTP en red.

Para obtener más información sobre SNTP, consulte el apartado "Configuración de los valores de SNTP".

Traceroute

Traceroute permite descubrir cuáles eran las rutas IP a las que se reenviaban los paquetes durante el proceso de reenvío. La utilidad Traceroute de la CLI se puede ejecutar desde los modos User EXEC o Privileged EXEC.

Compatibilidad con el puerto de gestión fuera de banda

Un puerto de gestión fuera de banda es un puerto Ethernet externo que sólo lleva tráfico entre el administrador del sistema y las aplicaciones de gestión. El puerto de gestión fuera de banda proporciona una conexión físicamente segura y también ofrece tolerancia de fallos.

Funciones de seguridad

ACL (Listas de control de acceso)

ACL proporciona normas para enviar o bloquear el tráfico de red. Puede definir ACL para reforzar las mejoras de seguridad al definir normas de clasificación y asignar una acción por norma. Puede asignar una ACL a una interfaz de entrada (puerto o VLAN).

Para obtener información sobre la definición de ACL, consulte el apartado "Definición de ACL basadas en IP" y "Definición de ACL basadas en MAC".

Autenticación basada en puerto (802.1x)

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

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

Compatibilidad con el puerto bloqueado

Un puerto bloqueado limita el acceso a un puerto sólo a los usuarios con direcciones MAC específicas. Estas direcciones se aprenden o definen manualmente en dicho puerto. Cuando se ve una trama en un puerto bloqueado y la dirección MAC de origen de la trama no está vinculada a ese puerto, se invoca el mecanismo de protección.

Para obtener información sobre la habilitación de la seguridad de puertos bloqueados, consulte el apartado "Configuración de la seguridad de los puertos".

Seguridad de la gestión de contraseñas

La gestión de contraseñas ofrece una mayor seguridad de la red y un mejor control de las contraseñas. Las contraseñas para el acceso a SSH, Telnet, HTTP, HTTPS y SNMP tienen asignadas funciones de seguridad.

Para obtener más información sobre la gestión de contraseñas, consulte el apartado "Gestión de contraseñas".

TACACS+

TACACS+ proporciona seguridad centralizada para validar a usuarios que acceden al conmutador. TACACS+ proporciona un sistema de gestión de usuarios centralizado al mismo tiempo que mantiene la coherencia con RADIUS y otros procesos de autenticación.

Para obtener información sobre la definición de la configuración de TACACS+, consulte el apartado "Configuración de los servidores TACACS+ fuera de banda" y "Configuración de los valores de TACACS+".

Cliente de RADIUS

RADIUS es un protocolo basado en cliente/servidor en el que el servidor mantiene una base de datos de usuarios, que contiene información de autenticación por usuario como, por ejemplo, el nombre del usuario, la contraseña e información de cuentas.

Para obtener información sobre la definición de la configuración de RADIUS, consulte el apartado "Configuración de los valores de RADIUS".

SSH

Shell seguro (SSH) es un protocolo que proporciona una conexión segura y remota a un dispositivo. Esta conexión proporciona unas funciones parecidas a una conexión de telnet entrante.

Regresar a la página de contenido

Regresar a la página de contenido

Sistemas Dell™ PowerConnect™ 6024/6024F

NOTA: Una NOTA proporciona información importante que le ayuda a utilizar su equipo de la mejor manera posible.

AVISO: Un AVISO indica la posibilidad de daños en el hardware o pérdida de datos, y le explica cómo evitar el problema.

PRECAUCIÓN: Una PRECAUCIÓN indica un posible daño material, lesión corporal o muerte.

Enero 2005

Regresar a la página de contenido

Regresar a la página de contenido

Visualización de estadísticas

Sistemas Dell PowerConnect 6024/6024F

Esta sección contiene estadísticas sobre la utilización de la interfaz, GVRP, Etherlike, RMON y el dispositivo.

NOTA: Los comandos de la CLI no están disponibles para todas las páginas Statistics (Estadísticas).

Visualización de tablas

La página **Table Views** (Vistas de tabla) contiene enlaces para visualizar estadísticas en un formato de gráfico.

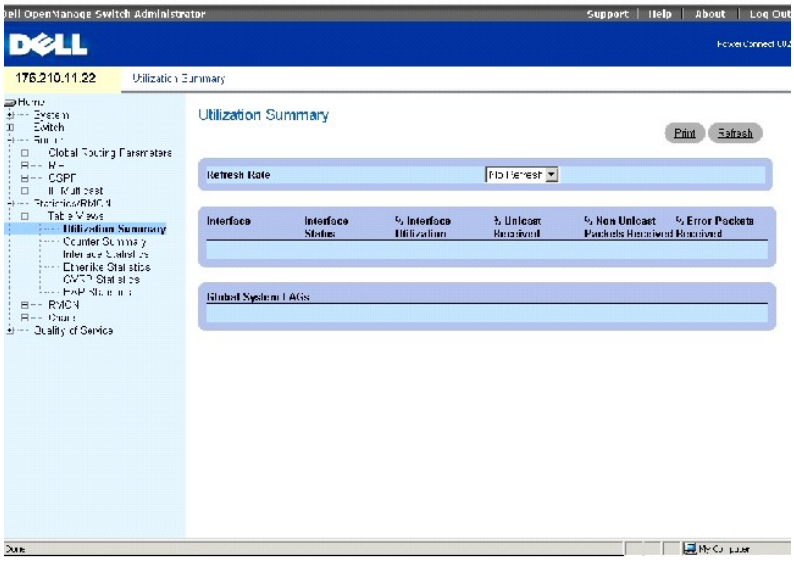
Para abrir la página, haga clic en **Statistics/RMON**→ **Table Views** (Estadísticas/RMON→ Vistas de tablas) en la vista de árbol.

Visualización del resumen de utilización

La página **Utilization Summary** (Resumen de utilización) contiene estadísticas para la utilización de la interfaz.

Para abrir la página, haga clic en **Statistics/RMON**→ **Table Views**→ **Utilization Summary** (Estadísticas/RMON→ Vistas de tablas→ Resumen de utilización) en la vista de árbol.

Ilustración 9-1. Utilization Summary (Resumen de utilización)



La página **Utilization Summary** (Resumen de utilización) contiene los siguientes campos:

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Interface (Interfaz): el número de la interfaz.

Interface Status (Estado de la interfaz): el estado de la interfaz.

% Interface Utilization (% de utilización de la interfaz): el porcentaje de utilización de la interfaz de red en función del modo dúplex de la interfaz. El rango de esta lectura está comprendido entre 0 y 200 %. La lectura máxima de 200% en una conexión de dúplex completo indica que el flujo de datos que pasa por la interfaz utiliza el 100% de la amplitud de banda de las conexiones de entrada y salida. La lectura máxima en una conexión de dúplex medio es del 100%.

% Unicast Received (% de paquetes de difusión única recibidos): el porcentaje de paquetes de difusión única recibidos en la interfaz.

% Non Unicast Packets Received (% de paquetes recibidos sin difusión única): el porcentaje de paquetes sin difusión única recibidos en la interfaz.

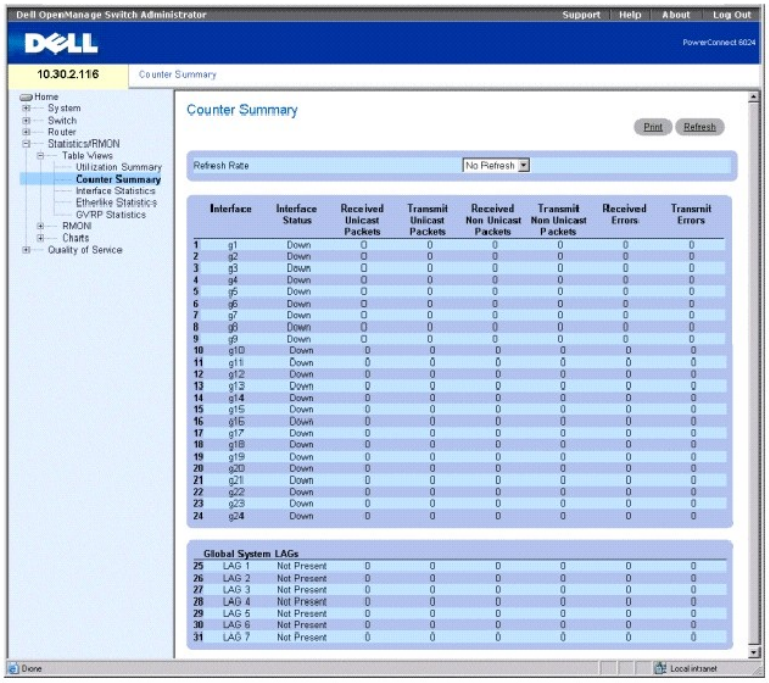
% Error Packets Received (% de paquetes con errores recibidos): el número de paquetes con errores recibidos en la interfaz.

Visualización del resumen de contador

La página **Counter Summary** (Resumen de contador) contiene estadísticas para la utilización del puerto en sumas numéricas en lugar de porcentajes.

Para abrir la página, haga clic en **Statistics/RMON**→ **Table Views**→ **Counter Summary** (Estadísticas/RMON→ Vistas de tablas→ Resumen de contador) en la vista de árbol.

Ilustración 9-2. Página Counter Summary (Resumen de contador)



Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Interface (Interfaz): el número de la interfaz.

Interface Status (Estado de la interfaz): el estado de la interfaz.

Received Unicast Packets (Paquetes de difusión única recibidos): el número de paquetes de difusión única recibidos en la interfaz.

Transmit Unicast Packets (Paquetes de difusión única transmitidos): número de paquetes de difusión única transmitidos desde la interfaz.

Received non-Unicast Packets (Paquetes recibidos sin difusión única): número de paquetes sin difusión única recibidos en la interfaz.

Transmit non-Unicast Packets (Paquetes sin difusión única transmitidos): número de paquetes sin difusión única transmitidos desde la interfaz.

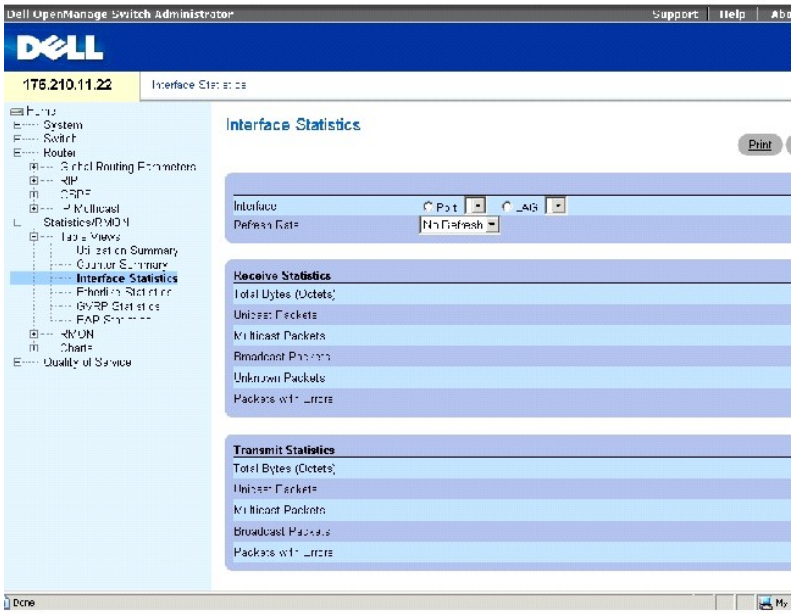
Received Errors (Errores recibidos): número de errores recibidos en la interfaz.

Transmit Errors (Errores transmitidos): número de errores transmitidos desde la interfaz.

Visualización de las estadísticas de la interfaz

La página **Interface Statistics** (Estadísticas de la interfaz) contiene las estadísticas de los paquetes recibidos y transmitidos. Los campos para los paquetes recibidos y transmitidos son exactamente iguales. Para abrir la página, haga clic en **Statistics/RMON→ Table Views→ Interface Statistics** (Estadísticas/RMON→ Vistas de tablas→ Estadísticas de la interfaz) en la vista de árbol.

Ilustración 9-3. Página Interface Statistics (Estadísticas de la interfaz)



Interface (Interfaz): especifica si se muestran las estadísticas para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Estadísticas de recepción

Total Bytes (Octets) (Total de bytes [octetos]): cantidad de octetos recibidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): cantidad de paquetes de difusión única recibidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): cantidad de paquetes de multidifusión recibidos en la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): cantidad de paquetes de difusión recibidos en la interfaz seleccionada.

Unknown Packets (Paquetes desconocidos): cantidad de paquetes desconocidos recibidos en la interfaz seleccionada.

Packets with Errors (Paquetes con errores): cantidad de errores transmitidos desde la interfaz seleccionada.

Estadísticas de transmisión

Total Bytes (Octets) (Total de bytes [octetos]): cantidad de octetos transmitidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): cantidad de paquetes de difusión única transmitidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): cantidad de paquetes de multidifusión transmitidos en la interfaz seleccionada.

Broadcast Packets (paquetes de difusión): cantidad de paquetes de difusión transmitidos en la interfaz seleccionada.

Packets with Errors (Paquetes con errores): cantidad de errores transmitidos desde la interfaz seleccionada.

Visualización de las estadísticas de la interfaz

1. Abra la página **Interface Statistics** (Estadísticas de la interfaz).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Restablecimiento de los contadores de las estadísticas de la interfaz

1. Abra la página **Interface Statistics** (Estadísticas de la interfaz).
2. Haga clic en el botón **Reset All Counters** (Restablecer todos los contadores).

Visualización de las estadísticas de la interfaz mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver las estadísticas de la interfaz.

Tabla 9-1. Comandos de la CLI para ver las estadísticas de la interfaz

Comando de la CLI	Descripción
`show interfaces counters [ethernet` *`interfaz`* `| port- channel` *`número_canal_puerto`*`]`	Muestra la pantalla de tráfico desde el punto de vista de una interfaz física.

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

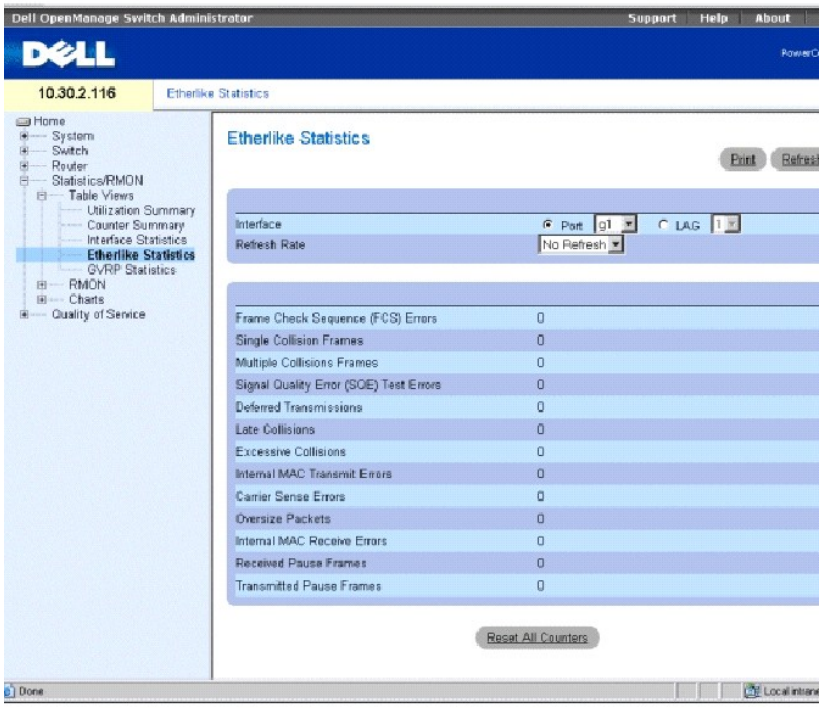
```
Console> show interfaces counters

Port    InOctets InUcastPkts InMcastPkts InBcastPkts

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

g1          0         0          0          0

g2          0         0          0          0

g3          0         0          0          0

g4          0         0          0          0

g5          0         0          0          0

g6          0         0          0          0

g7          0         0          0          0

g8          0         0          0          0

g9          0         0          0          0

g10         0         0          0          0

g11         0         0          0          0

g12         10        685        290        32

g13         0         0          0          0

g14         0         0          0          0

g15         0         0          0          0
```

g16	0	0	0	0
g17	0	0	0	0
g18	0	0	0	0
g19	0	0	0	0
g20	0	0	0	0
g21	0	0	0	0
g22	0	0	0	0
g23	0	0	0	0
g24	0	0	0	0

Visualización de las estadísticas de Etherlike

La página **Etherlike Statistics** (Estadísticas de Etherlike) contiene las estadísticas de la interfaz. Para abrir la página, haga clic en **Statistics / RMON→ Table Views→ Etherlike Statistics** (Estadísticas/RMON→ Vistas de tablas→ Estadísticas de Etherlike) en la vista de árbol.

Ilustración 9-4. Página Etherlike Statistics (Estadísticas de Etherlike)



Interface (Interfaz): especifica si se muestran las estadísticas para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Frame Check Sequence (FCS) Errors (Errores de secuencia de comprobación 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.

Multiple Collision Frames (Tramas de colisión múltiple): número de errores de tramas de colisión múltiple recibidos en la interfaz seleccionada.

Signal Quality Error (SQE) Test Errors (Errores de prueba de calidad de la señal [SQE]): número de errores de prueba SQE recibidos en la interfaz seleccionada.

Deferred Transmissions (Transmisiones diferidas): número de transmisiones diferidas en la interfaz seleccionada.

Late Collisions (Colisiones tardías): número de colisiones tardías recibidas en la interfaz seleccionada.

Excessive Collisions (Colisiones excesivas): número de colisiones excesivas recibidas en la interfaz seleccionada.

Internal MAC Transmit Errors (Errores de transmisión MAC internos): número de errores de transmisión MAC internos en la interfaz seleccionada.

Carrier Sense Errors (Errores de detección de comunicación): número de errores de detección de comunicación en la interfaz seleccionada.

Oversize Packets (Paquetes demasiado grandes): número de errores de paquetes demasiado grandes en la interfaz seleccionada.

Internal MAC Receive Errors (Errores de recepción MAC internos): número de errores MAC internos en la interfaz seleccionada.

Receive Pause Frames (Tramas de pausa recibidas): número de errores de pausa recibidos en la interfaz seleccionada.

Transmitted Paused Frames (Tramas de pausa transmitidas): número de errores de pausa transmitidos en la interfaz seleccionada.

Visualización de las estadísticas de Etherlike para una interfaz

1. Abra la página **Etherlike Statistics** (Estadísticas de Etherlike).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).
3. Haga clic en **Query** (Consulta) para mostrar las estadísticas de Etherlike de la interfaz.

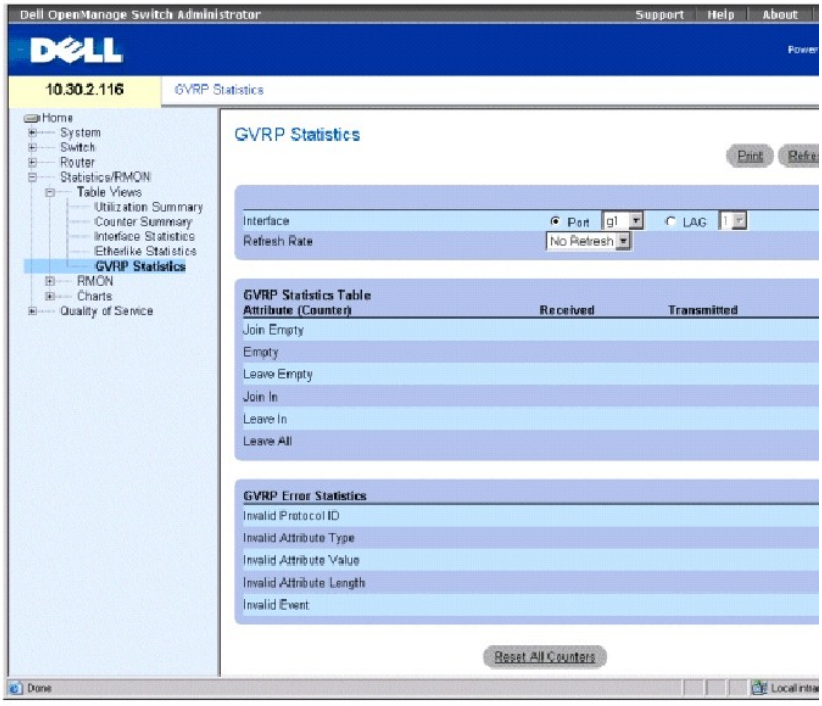
Restablecimiento de las estadísticas de Etherlike

1. Abra la página **Etherlike Statistics** (Estadísticas de Etherlike).
2. Haga clic en el botón **Reset All Counters** (Restablecer todos los contadores).

Visualización de las estadísticas de GVRP

La página **GVRP Statistics** (Estadísticas de GVRP) contiene estadísticas del dispositivo de GVRP. Para abrir la página, haga clic en **Statistics/RMON→ Table Views→ GVRP Statistics** (Estadísticas/RMON→ Vistas de tabla→ Estadísticas de GVRP) en la vista de árbol.

Ilustración 9-5. Página GVRP Statistics (Estadísticas de GVRP)



Interface (Interfaz): especifica si se muestran las estadísticas para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Join Empty (Unir vacíos): muestra las estadísticas de Join Empty (Unir vacíos) de GVRP del dispositivo.

Empty (Vacíos): muestra las estadísticas de Empty (Vacíos) de GVRP del dispositivo.

Leave Empty (Dejar vacío): muestra las estadísticas de Leave Empty (Dejar vacío) de GVRP del dispositivo.

Join In (Unir): muestra las estadísticas de Join In (Unir) de GVRP del dispositivo.

Leave In (Dejar): muestra las estadísticas de Leave In (Dejar) de GVRP del dispositivo.

Leave All (Dejar todos): muestra las estadísticas de Leave All (Dejar todos) de GVRP del dispositivo.

Invalid Protocol ID (ID de protocolo no válido): estadísticas de IP de protocolo no válido GVRP del dispositivo.

Invalid Attribute Type (Tipo de atributo no válido): estadísticas de ID de atributo no válido GVRP del dispositivo.

Invalid Attribute Value (Valor del atributo no valido): estadísticas de valor del atributo no válido GVRP del dispositivo.

Invalid Attribute Length (Longitud de atributo no válida): estadísticas de longitud de atributo no válida GVRP del dispositivo.

Invalid Event (Evento no válido): estadísticas de eventos no válidos de GVRP del dispositivo.

Visualización de las estadísticas de GVRP para un puerto:

1. Abra la página **GVRP Statistics** (Estadísticas de GVRP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Restablecimiento de las estadísticas de GVRP

1. Abra la página **GVRP Statistics** (Estadísticas de GVRP).
2. Haga clic en el botón **Reset All Counters** (Restablecer todos los contadores).

Visualización de las estadísticas de GVRP mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver las estadísticas de GVRP.

Tabla 9-2. Comandos de la CLI para ver las estadísticas de GVRP

Comando de la CLI	Descripción
`show gvrp statistics [ethernet` *`interfaz`* `| port-channel` *`número_canal_puerto`*`]`	Muestra las estadísticas de GVRP.
	Muestra las estadísticas de error de GVRP.

show gvrp error- statistics [ethernet *interfaz* | port-channel *número_canal_puerto*]

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

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

g1    0    0    0    0   0   0   0   0   0    0   0   0

g2    0    0    0    0   0   0   0   0   0    0   0   0

g3    0    0    0    0   0   0   0   0   0    0   0   0

g4    0    0    0    0   0   0   0   0   0    0   0   0

g5    0    0    0    0   0   0   0   0   0    0   0   0

g6    0    0    0    0   0   0   0   0   0    0   0   0

g7    0    0    0    0   0   0   0   0   0    0   0   0
```

```
g8    0    0    0    0   0   0   0   0   0    0   0   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

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

g1      0       0       0       0       0       0

g2      0       0       0       0       0       0

g3      0       0       0       0       0       0

g4      0       0       0       0       0       0

g5      0       0       0       0       0       0

g6      0       0       0       0       0       0

g7      0       0       0       0       0       0

g8      0       0       0       0       0       0
```

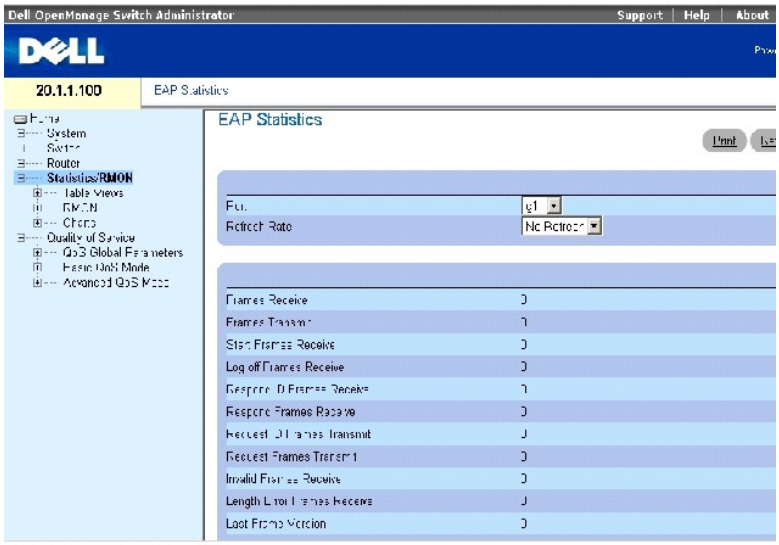
Visualización de estadísticas de EAP

La página **EAP Statistics** (Estadísticas de EAP) contiene información sobre los paquetes EAP recibidos en un puerto específico. Para obtener más información sobre EAP, consulte el apartado Autenticación basada en puertos (802.1x) .

Para abrir la página **EAP Statistics** (Estadísticas de EAP), haga clic en **Statistics / RMON**→ **Table Views**→ **EAP Statistics** (Estadísticas/RMON→ Vistas de tabla→

Estadísticas de EAP) en la vista de árbol.

Ilustración 9-6. EAP Statistics (Estadísticas de EAP)



La página **EAP Statistics** (Estadísticas de EAP) contiene los siguientes campos:

Port (Puerto): el puerto que se sondea para obtener las estadísticas.

Refresh Rate (Frecuencia de actualización): tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Frames Receive (Tramas recibidas): el número de tramas de EAPOL válidas recibidas en el puerto.

Frames Transmit (Tramas transmitidas): el número de tramas EAPOL válidas transmitidas a través del puerto.

Start Frames Receive (Tramas de inicio recibidas): el número de tramas de EAPOL de inicio recibidas en el puerto.

Log off Frames Receive (Tramas de cierre de sesión recibidas): el número de tramas de cierre de sesión de EAPOL que se han recibido en el puerto.

Respond ID Frames Receive (Tramas de ID de respuesta recibidas): el número de tramas de ID de respuesta de EAP que se han recibido en el puerto.

Respond Frames Receive (Tramas de respuesta recibidas): el número de tramas de respuesta de EAP válidas recibidas en el puerto.

Request ID Frames Transmit (Tramas de ID de solicitud transmitidas): el número de tramas de ID de solicitud de EAP transmitidas a través del puerto.

Request Frames Transmit (Tramas de solicitud transmitidas): el número de tramas de solicitud de EAP transmitidas a través del puerto.

Invalid Frames Receive (Tramas no válidas no recibidas): el número de tramas de EAPOL no reconocidas recibidas en este puerto.

Length Error Frames Receive (Tramas con longitud errónea recibidas): el número de tramas de EAPOL con una longitud de cuerpo de paquete no válida recibidas en este puerto.

Last Frame Version (Versión de la última trama): el número de versión del protocolo que va unido a la trama de EAPOL que se haya recibido más recientemente.

Last Frame Source (Origen de la última trama): la dirección MAC de origen que va unida a la trama de EAPOL que se haya 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 de la interfaz.

Visualización de las estadísticas de EAP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de EAP.

Tabla 9-3. Comandos de la CLI para ver las estadísticas de EAP

Comando de la CLI	Descripción
`show dot1x statistics ethernet` *interfaz*	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 g11

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

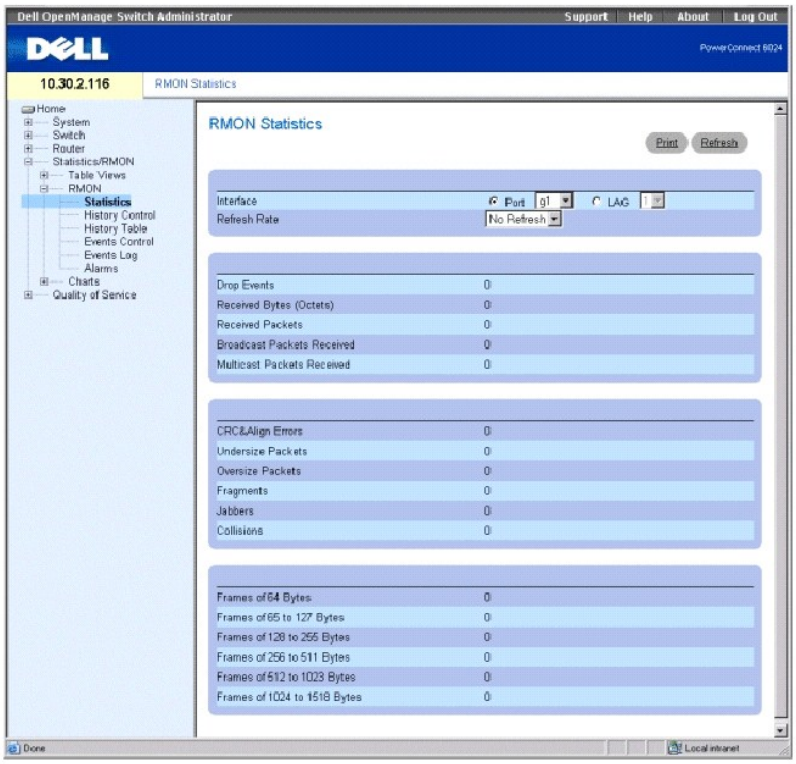
La supervisión remota (RMON) permite a los administradores de red ver la información de red desde una ubicación remota. Para abrir la página **RMON**, haga clic en **Statistics / RMON**→ **RMON** (Estadísticas/RMON→ RMON) en la vista de árbol.

Visualización del grupo de estadísticas de RMON

Utilice la página **RMON Statistics Group** (Grupo de estadísticas de RMON) para visualizar información acerca de la utilización del dispositivo y los errores producidos en el mismo.

Para abrir la página, haga clic en **Statistics / RMON**→ **RMON**→ **Statistics** (Estadísticas/RMON→ RMON→ Estadísticas) en la vista de árbol.

Ilustración 9-7. Página RMON Statistics Group (Grupo de estadísticas de RMON)



Interface (Interfaz): especifica el puerto o LAG para el que se muestran las estadísticas.

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Drop Events (Eventos descartados): número de eventos descartados que se han producido en la interfaz desde que se actualizó por última vez el dispositivo.

Received Bytes (Octets) (Bytes recibidos [octetos]): número de octetos recibidos en la interfaz desde que se actualizó por última vez el dispositivo. Este número incluye paquetes erróneos y octetos FCS, pero excluye los bits de la trama.

Received Packets (Paquetes recibidos): número de paquetes recibidos en la interfaz, incluidos los paquetes erróneos y los paquetes de difusión, desde que se actualizó por última vez el dispositivo.

Broadcast Packets Received (Paquetes de difusión recibidos): número de paquetes de difusión correctos recibidos en la interfaz desde que se actualizó por última vez el 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 que se actualizó por última vez el dispositivo.

CRC & Align Errors (Errores de alineación y de CRC): número de errores de alineación y de CRC que se han producido en la interfaz desde que se actualizó por última vez el dispositivo.

Undersize Packets (Paquetes demasiado pequeños): número de paquetes demasiado pequeños (inferiores a los 64 octetos) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Oversize Packets (Paquetes demasiado grandes): número de paquetes demasiado grandes (superiores a los 1.518 octetos) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Fragments (Fragmentos): número de fragmentos (paquetes de menos de 64 octetos, excluidos los bits de trama e incluidos los octetos FCS) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Jabbers: número de paquetes recibidos de más de 1.518 octetos de longitud y que han tenido una FCS durante la sesión de muestreo.

Collisions (Colisiones): número de colisiones recibidas en la interfaz desde que se actualizó por última vez el dispositivo.

Frames of *xx* Bytes (Tramas de xx bytes): número de tramas de *xx* bytes recibidas en la interfaz desde que se actualizó por última vez el dispositivo.

Visualización de las estadísticas de la interfaz

1. Abra la página **RMON Statistics Group** (Grupo de estadísticas de RMON).
2. Seleccione un tipo y un número de interfaz en el campo **Interface** (Interfaz).

Visualización de las estadísticas de RMON mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver las estadísticas de RMON.

Tabla 9-4. Comandos de la CLI para ver las estadísticas de RMON

Comando de la CLI	Descripción
	Muestra las estadísticas de Ethernet de RMON.

show rmon statistics {ethernet *interfaz* | port-channel *número_canal_puerto*}

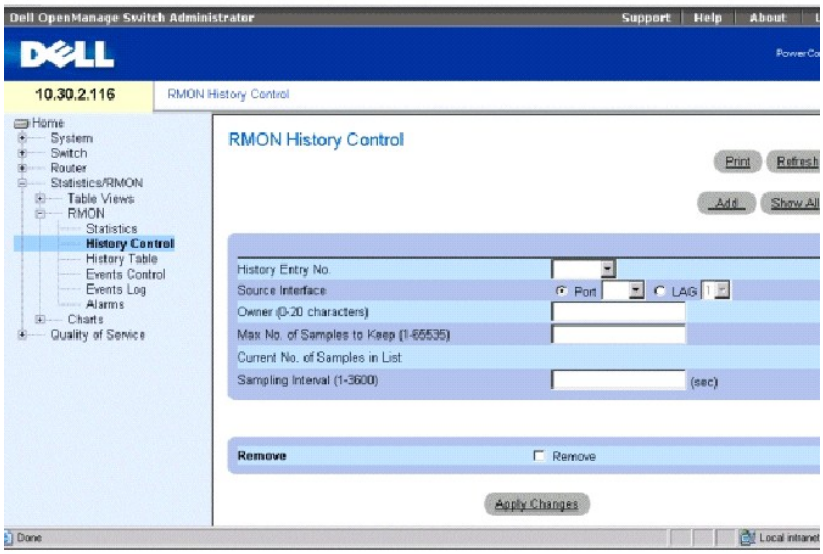
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console# show rmon statistics ethernet g1

Port g1

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: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Visualización de estadísticas del control del historial de RMON

La página **RMON History Control** (Control del historial de RMON) contiene información acerca de muestras de datos obtenidos desde los puertos. Por ejemplo, las muestras pueden incluir definiciones de la interfaz o períodos de encuesta. Para abrir la página, haga clic en **Statistics / RMON→ RMON→ RMON History Control** (Estadísticas/RMON→ RMON→ Control del historial de RMON) en la vista de árbol.

Ilustración 9-8. Página RMON History Control (Control del historial de RMON)



History Entry No. (Nº de entrada del historial): número de entrada en la tabla de **RMON History Control** (Control del historial de RMON).

Source Interface (Interfaz de origen): el puerto o LAG desde los que se han obtenido las muestras del historial.

Owner (Propietario): estación de RMON o usuario que ha solicitado la información de RMON.

Max No. of Samples to Keep (1-65535) (Número máximo de muestras que se deben conservar [1-65535]): número de muestras que se van a guardar. El valor predeterminado es 50.

Current No. of Samples in List (Nº 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, transcurrido 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 1800 segundos (30 minutos).

Remove (Eliminar): si se selecciona esta opción, se elimina la entrada de la tabla **RMON History Control** (Control del historial de RMON).

Adición de una entrada de control del historial

1. Abra la página **RMON History Control** (Control del historial de RMON).
2. Haga clic en **Add** (Agregar) para mostrar la página **Add History Entry** (Agregar entrada del historial).
3. Complete los campos del cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

La entrada se agrega a la tabla **RMON History Control** (Control del historial de RMON).

Modificación de una entrada de la tabla de control del historial de RMON

1. Abra la página **RMON History Control** (Control del historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).
3. Modifique los campos como desee y haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la tabla se modifica y el dispositivo se actualiza.

Supresión de una entrada de la tabla de control del historial

1. Abra la página **RMON History Control** (Control del historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).
3. Haga clic en **Remove** (Eliminar) y, a continuación, haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la tabla se suprime y el dispositivo se actualiza.

Visualización del control del historial de RMON mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver las estadísticas de GVRP.

Tabla 9-5. Comandos de la CLI para ver el historial de RMON

Comando de la CLI	Descripción
rmon collection *índice_historial* [owner *nombre_propietario* | buckets *número_sector_almacenamiento*] [interval *segundos*]	Activa y configura RMON en una interfaz.
show rmon collection history [ethernet *interfaz* | port-channel *número_canal_puerto*]	Muestra las estadísticas del historial de recopilación de RMON.

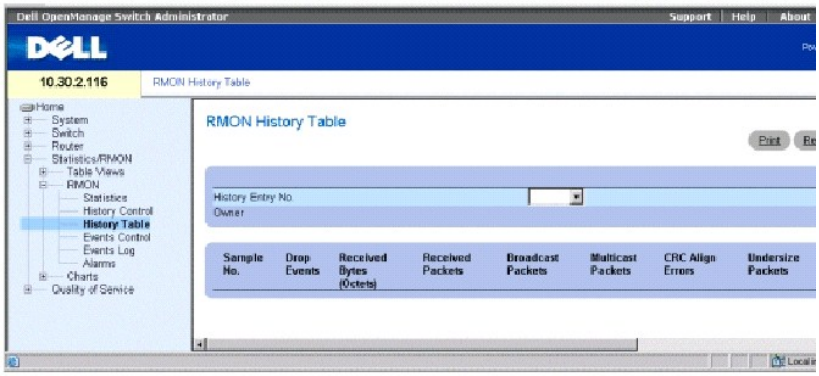
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# interface ethernet g8

Console (config-if)# rmon collection history 1 interval 2400

Console (config-if)# exit

Console (config)#exit

Console# disable

Console> show rmon collection history

Index Interface Interval Requested Samples  Granted Samples   Owner

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

1         1        10        0        50           50         CLI
```

Visualización de la tabla del historial de RMON

La página RMON History Table (Tabla del historial de RMON) contiene muestreos estadísticos de red específicos de la interfaz. Cada entrada de la tabla representa a todos los valores del contador compilados durante una única muestra. Para abrir la página **RMON History Table** (Tabla del historial de RMON), haga clic en **Statistics / RMON→ RMON→ History Table** (Estadísticas/RMON→ RMON→ Tabla del historial) en la vista de árbol.

Ilustración 9-9. RMON History Table (Tabla del historial de RMON)



NOTA: En la RMON History Table (Tabla del historial de RMON) no se muestran todos los campos.

History Entry No. (Nº de entrada del historial): contiene una lista de los números de entrada de la tabla **RMON History Control** (Control del historial de RMON).

Owner (Propietario): si está disponible, el nombre del propietario del grupo de estadísticas de RMON.

Sample No. (Nº de muestra): indica la muestra específica que refleja la información de la tabla.

Drop Events (Eventos descartados): el número de paquetes descartados debido a la falta de recursos de red durante el intervalo de muestreo. Es posible que no represente la cantidad exacta de paquetes descartados, en cambio se ha detectado el número de veces que se han descartado paquetes.

Received Bytes (Octets) (Bytes recibidos [octetos]): el número de octetos de datos, incluidos los paquetes erróneos, recibidos en la red.

Received Packets (Paquetes recibidos): el número de paquetes recibidos durante el intervalo de muestreo.

Broadcast Packets (Paquetes de difusión): el número de paquetes de difusión correctos recibidos durante el intervalo de muestreo.

Multicast Packets (Paquetes de multidifusión): el número de paquetes de multidifusión correctos recibidos durante el intervalo de muestreo.

CRC Align Errors (Errores de alineación de CRC): el número de paquetes recibidos durante la sesión de muestreo con una longitud de 64 a 1.518 octetos. Sin embargo, los paquetes tienen una secuencia de comprobación de tramas (FCS) errónea con un número integral de octetos o una FCS errónea con un número no integral.

Undersize Packets (Paquetes demasiado pequeños): el número de paquetes recibidos de menos de 64 octetos de longitud durante la sesión de muestreo.

Oversize Packets (Paquetes demasiado grandes): el número de paquetes recibidos de más de 1.518 octetos de longitud durante la sesión de muestreo.

Fragments (Fragmentos): el número de paquetes recibidos de menos de 64 octetos de longitud y que han tenido una FCS durante la sesión de muestreo.

Jabbers: el número de paquetes recibidos de más de 1.518 octetos de longitud y que han tenido una FCS durante la sesión de muestreo.

Collisions (Colisiones): realiza una estimación del número total de colisiones de paquetes producidas durante la sesión de muestreo. Las colisiones se detectan cuando los puertos repetidores detectan dos o más estaciones que transmiten simultáneamente.

Utilization (Utilización): realiza una estimación de la utilización de la red del nivel físico principal en una interfaz durante la sesión de muestreo. El valor se refleja en porcentajes con dos decimales.

Visualización de las estadísticas para una entrada específica del historial

1. Abra la página **RMON History Table** (Tabla del historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).

Las estadísticas de entrada se muestran en la página RMON History Table (Tabla del historial de RMON).

Visualización del control del historial de RMON mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver el historial de RMON.

Tabla 9-6. Comandos de la CLI para ver el control del historial de RMON

Comando de la CLI	Descripción
`show rmon history index {throughput | errors | other} [period seconds]`	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# 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

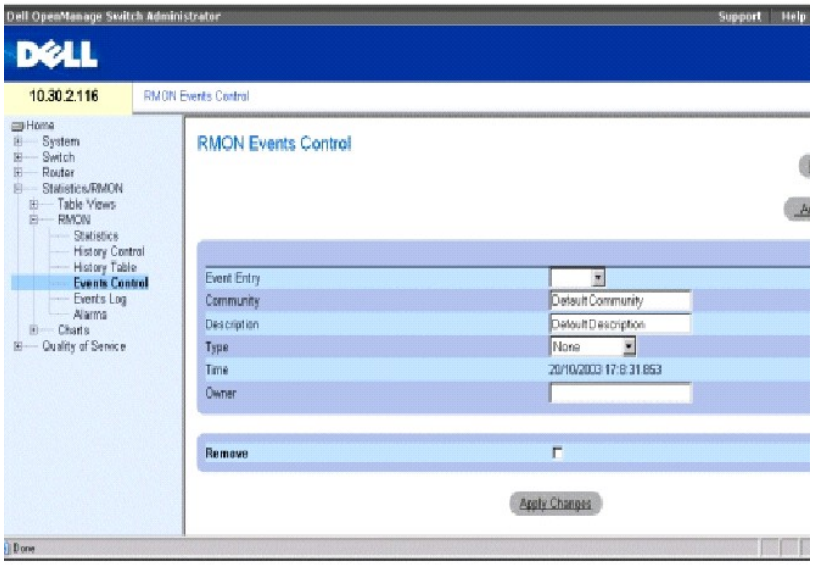
09-Mar-2003 18:30:12 0 0 0 0 0

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, haga clic en **Statistics / RMON→ RMON→ Events Control** (Estadísticas/RMON→ RMON→ Control de eventos) en la vista de árbol.

Ilustración 9-10. Página RMON Events Control (Control de eventos de RMON)



Event Entry (Entrada de eventos): indica el evento.

Community (Comunidad): comunidad a la que pertenece el evento.

Description (Descripción): la descripción del evento definido 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): la hora en la que se ha producido el evento.

Owner (Propietario): el dispositivo o usuario que ha definido el evento.

Remove (Eliminar): si se selecciona esta opción, se elimina el evento de la tabla de eventos.

Adición de un evento de RMON

1. Abra la página **RMON Events Control** (Control de eventos de RMON).
2. Haga clic en **Add** (Agregar) para mostrar la página **Add an Event Entry** (Agregar una entrada de evento).
3. Complete la información en el cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

El evento se agrega a la tabla **RMON Event** (Evento de RMON) y el dispositivo se actualiza.

Modificación de un evento de RMON

1. Abra la página **RMON Events Control** (Control de eventos de RMON).
2. Seleccione una entrada en el campo **Event Entry** (Entrada de evento).
3. Modifique los campos de la página y haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la tabla **RMON Events** (Eventos de RMON) se modifica y el dispositivo se actualiza.

Supresión de las 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) para mostrar la tabla **RMON Events** (Eventos de RMON).
3. Haga clic en **Remove** (Eliminar) para eliminar los eventos que desee y, a continuación, haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la tabla se suprime y el dispositivo se actualiza.

NOTA: Sólo se puede eliminar una entrada de evento desde la página **RMON Events Control** (Control de eventos de RMON) haciendo clic en la casilla de verificación **Remove** (Eliminar) de la página.

Definición de los eventos del dispositivo mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir los eventos del dispositivo.

Tabla 9-7. Comandos de la CLI para ver la definición de los eventos del dispositivo

Comando de la CLI	Descripción
`rmon event` *`tipo de índice`* `[community` *`texto`*`] [description` *`texto`*`] [owner` *`nombre`*`]`	Configura los eventos de RMON.
`show rmon events`	Muestra la tabla de eventos de RMON.

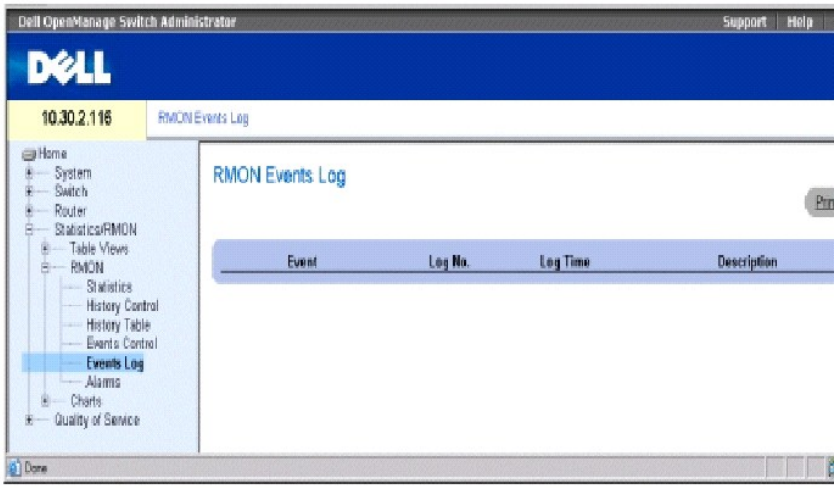
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# rmon event 10 log

Console (config)# exit

Console# disable

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 de la tabla 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, haga clic en **Statistics/RMON→ RMON→ Events Log** (Estadísticas/RMON→ RMON→ Registro de eventos) en la vista de árbol

Ilustración 9-11. Página RMON Events Log (Registro de eventos de RMON)



Event (Evento): el número de entrada de RMON Events Log (Registro de eventos de RMON).

Log No. (Nº de registro): el número de registro.

Log Time (Tiempo de registro): hora en la que se ha especificado la entrada del registro.

Description (Descripción): describe la entrada del registro.

Definición de los eventos del dispositivo mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir los eventos del dispositivo.

Tabla 9-8. Comandos de la CLI para la definición de eventos del 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:

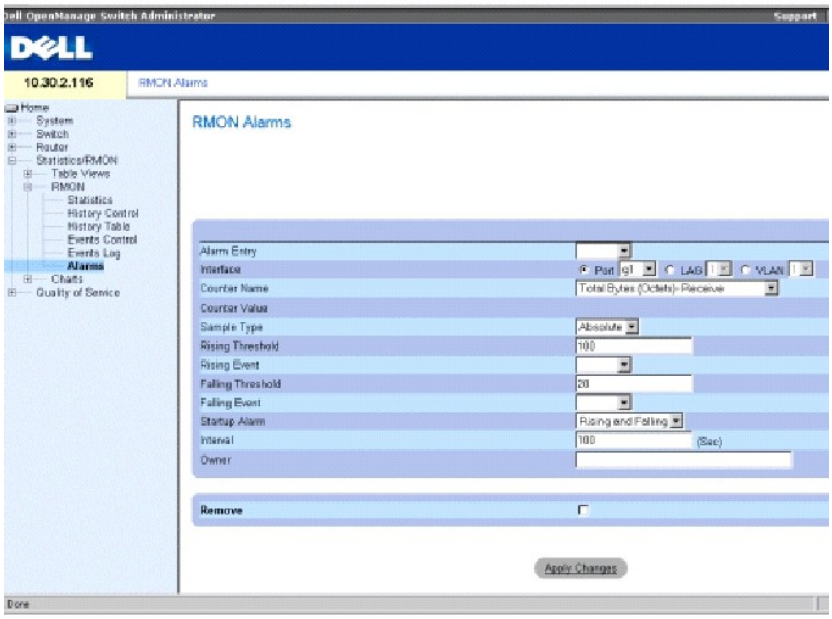
```
Console> show rmon log

Maximum table size: 500

Event   Description                  Time

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

1       Errors                       Jan 18 2002 23:48:19

1       Errors                       Jan 18 2002 23:58:17

2       High Broadcast               Jan 18 2002 23:59:48
```

Definición de alarmas del dispositivo de RMON

Utilice la página **RMON Alarms** (Alarmas de RMON) para establecer las alarmas de la red. Las alarmas de la red se activan cuando se detecta un problema en la red o un evento. Los umbrales superiores e inferiores generan eventos. Para obtener más información sobre los eventos, consulte el apartado Visualización del registro de eventos de RMON .

Para abrir la página, hacer clic en **Statistics/RMON**→ **RMON**→ **Alarms** (Estadísticas/RMON→ RMON→ Alarmas) en la vista de árbol.

Ilustración 9-12. Página RMON Alarms (Alarmas de RMON)



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): el 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 de campo posibles son:

Delta (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 (Umbral superior): 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. Se asigna un color a cada una de las variables supervisadas.

Rising/Falling Event (Evento superior/inferior): el mecanismo que notifica las alarmas, incluido un registro, una captura o ambos. Cuando se selecciona un registro, no hay ningún mecanismo de almacenamiento ni en el dispositivo ni en el sistema de gestión. Sin embargo, si el dispositivo no se restablece, el evento permanece en la tabla de registros del dispositivo. Si se selecciona una captura, se genera una captura de SNMP y se notifica a través del mecanismo de captura. La captura se puede guardar con el mismo mecanismo.

Falling Threshold (Umbral inferior): el umbral inferior aparece gráficamente en la parte inferior de las barras de gráficos. El umbral inferior aparece gráficamente en la parte superior de las barras de gráficos. Se asigna un color a cada una de las variables supervisadas.

Startup Alarm (Alarma de inicio): el activador que hace funcionar la alarma. El umbral superior se define cuando se atraviesa el umbral desde uno con un valor bajo hasta un umbral con un valor más alto.

Interval (sec) (Intervalo [s.]): el intervalo de tiempo entre las alarmas.

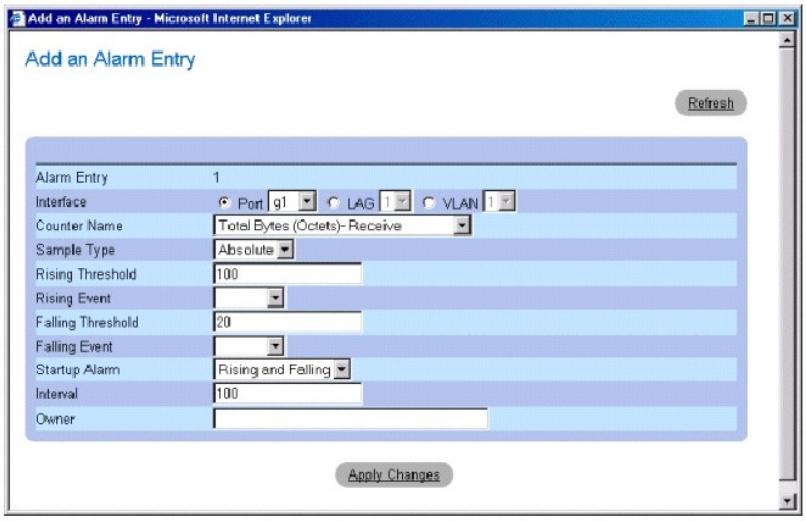
Owner (Propietario): el dispositivo o usuario que ha definido la alarma.

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** (Agregar) para mostrar la página **Add an Alarm Entry** (Agregar una entrada de alarma).

Ilustración 9-13. Página Add an Alarm Entry (Agregar una entrada de alarma)



3. Seleccione una interfaz.
4. Complete los campos del cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

La alarma de RMON se agrega y el dispositivo se actualiza.

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 descendente **Alarm Entry** (Entrada de alarma).
3. Modifique los campos en el cuadro de diálogo como desee y haga clic en **Apply Changes** (Aplicar cambios).

La entrada se modifica y el dispositivo se actualiza.

Visualización de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
2. Haga clic en **Show All** (Mostrar todo) para mostrar la tabla **RMON Alarms** (Alarmas de RMON).

Supresión de una entrada de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).

2. Seleccione una entrada en el menú descendente **Alarm Entry** (Entrada de alarma).
3. Marque la casilla de verificación **Remove** (Eliminar) y haga clic en **Apply Changes** (Aplicar cambios).

La entrada se suprime y el dispositivo se actualiza.

Definición de las alarmas del dispositivo mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para definir las alarmas del dispositivo.

Tabla 9-9. Comandos de la CLI para ver las alarmas del dispositivo

Comando de la CLI	Descripción
rmon alarm *índice ID_Objeto_MIB intervalo umbralr umbralf eventor eventof* [type *tipo*] [startup *dirección*] [owner *nombre*]	Configura las condiciones de alarma de RMON.
show rmon alarm-table	Muestra el resumen de la tabla de alarmas.
show rmon alarm	Muestra la configuración de las alarmas 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 gráficos

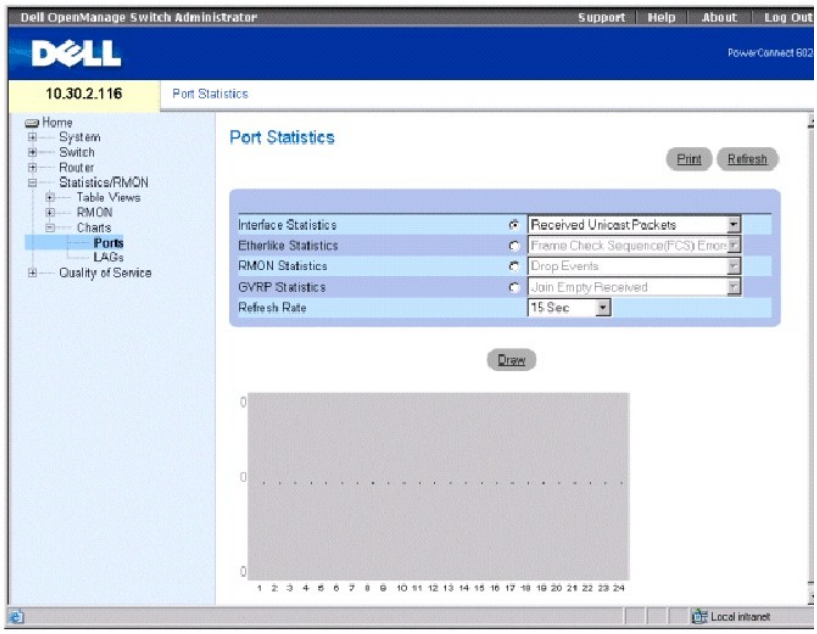
La página **Charts** (Gráficos) contiene enlaces para mostrar estadísticas en formato de gráfico. Para abrir la página, haga clic en **Statistics / RMON→ Charts** (Estadísticas/RMON→ Gráficas) en la vista de árbol.

Visualización de las estadísticas del puerto

Utilice la página **Port Statistics** (Estadísticas de puerto) para mostrar estadísticas en formato de gráfico para los elementos de un puerto.

Para abrir la página, haga clic en **Statistics/RMON**→ **Charts**→ **Ports** (Estadísticas/RMON→ Gráficas→ Puertos) en la vista de árbol.

Ilustración 9-14. Página Port Statistics (Estadísticas de puerto)



Interface Statistics (Estadísticas de la interfaz): selecciona el tipo de estadísticas de interfaz que va a mostrar.

Etherlike Statistics (Estadísticas Etherlike): selecciona el tipo de estadísticas que se debe mostrar.

RMON Statistics (Estadísticas de RMON): selecciona el tipo de estadísticas de RMON que se debe mostrar.

GVRP Statistics (Estadísticas de GVRP): selecciona el tipo de estadísticas de GVRP que se debe mostrar.

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Visualización de las estadísticas de puerto

1. Abra la página **Port Statistics** (Estadísticas de puerto).
2. Seleccione el tipo de estadísticas que se debe mostrar.
3. Seleccione la frecuencia de actualización deseada en el menú descendente **Refresh Rate** (Frecuencia de actualización).
4. Haga clic en **Draw** (Dibujar).

Se muestra el gráfico de la estadística seleccionada.

Visualización de las estadísticas de puerto mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver las estadísticas de puerto.

Tabla 9-10. Comandos de la CLI para ver las estadísticas de puerto

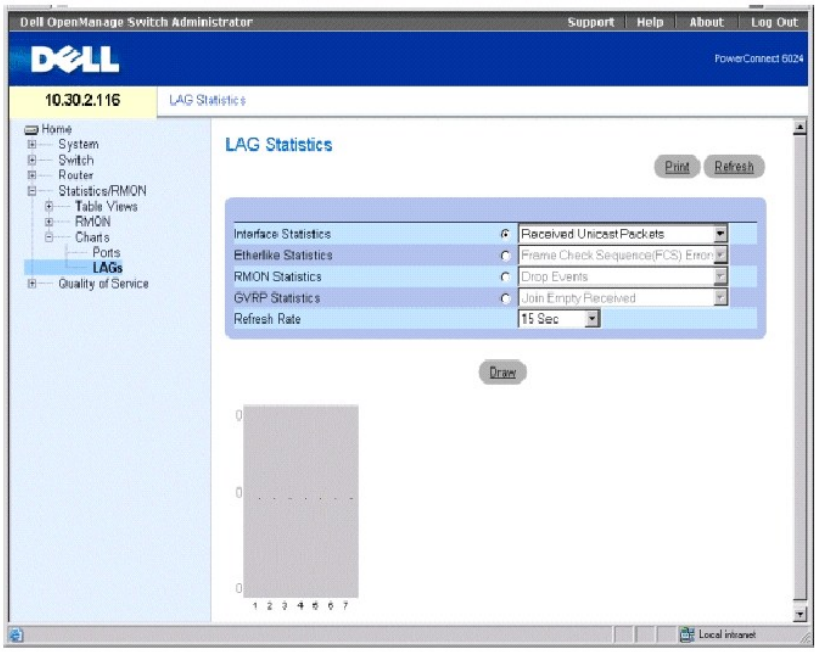
Comando de la CLI	Descripción
`show interfaces counters [ethernet` *`interfaz`* `| port- channel` *`número_canal_puerto`*`]`	Muestra la pantalla de tráfico desde el punto de vista de una interfaz física.
`show rmon statistics {ethernet` *`interfaz`* `| port-channel` *`número_canal_puerto`*`}`	Muestra 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 mostrar las estadísticas de en formato de gráfico para grupos agregados de conexiones.

Para abrir la página, haga clic en **Statistics/RMON**→ **Charts**→ **LAGs** (Estadísticas/RMON→ Gráficas→ LAG) en la vista de árbol.

Ilustración 9-15. Página LAG Statistics (Estadísticas de LAG)



Interface Statistics (Estadísticas de la interfaz): selecciona el tipo de estadísticas de interfaz que va a mostrar.

Etherlike Statistics (Estadísticas Etherlike): selecciona el tipo de estadísticas que se debe mostrar.

RMON Statistics (Estadísticas de RMON): selecciona el tipo de estadísticas de RMON que se debe mostrar.

GVRP Statistics (Estadísticas de GVRP): selecciona el tipo de estadísticas de GVRP que se debe mostrar.

Refresh Rate (Frecuencia de actualización): el tiempo que transcurre antes de que las estadísticas se actualicen. Los posibles valores de campo son No Refresh (No actualizar), 15, 30 y 60 segundos.

Visualización de las estadísticas de LAG

1. Abra la página **LAG Statistics** (Estadísticas de LAG).
2. Seleccione el tipo de estadísticas que se debe mostrar.
3. Seleccione la frecuencia de actualización deseada en el menú descendente **Refresh Rate** (Frecuencia de actualización).
4. Haga clic en **Draw** (Dibujar).

Se muestra el gráfico de la estadística seleccionada.

Visualización de las estadísticas de LAG mediante los comandos de la CLI

La siguiente tabla contiene los comandos de la CLI para ver las estadísticas de LAG.

Tabla 9-11. Comandos de la CLI para ver las estadísticas de LAG

Comando de la CLI	Descripción
`show interfaces counters [ethernet` *`interfaz`* `| port- channel` *`número_canal_puerto`*`]`	Muestra la pantalla de tráfico desde el punto de vista de una 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.

Regresar a la página de contenido