

Dell™ PowerConnect™ serie M6220 — Guía del usuario

[Introducción](#)

[Descripción del hardware](#)

[Uso del administrador de conmutadores Dell™ OpenManage™](#)

[Información sobre cables y puertos](#)

[Configuración de Dell™ PowerConnect™](#)

[Configuración de la información del sistema](#)

[Configuración de la información sobre conmutación](#)

[Creación de dependencias de enlaces](#)

[Visualización de las estadísticas/RMON](#)

[Configuración del enrutamiento](#)




[Configuración de IPv6](#)

[Configuración de la calidad de servicio](#)

[Configuración de la multidifusión IP](#)

[Obtención de ayuda](#)

Notas, avisos y precauciones

-  **NOTA:** una NOTA proporciona información importante que le ayudará a utilizar mejor el ordenador.
-  **AVISO:** un AVISO indica la posibilidad de daños en el hardware o la pérdida de datos, e informa de cómo evitar el problema.
-  **PRECAUCIÓN:** un mensaje de PRECAUCIÓN indica el riesgo de daños materiales, lesiones o incluso la muerte.

La información contenida en este documento puede modificarse sin aviso previo.
© 2007 Dell Inc. Reservados todos los derechos.

Queda estrictamente prohibida la reproducción de este documento en cualquier forma sin la autorización por escrito de Dell Inc.

Marcas comerciales utilizadas en este texto: *Dell*, *Dell OpenManage*, el logotipo de *DELL*, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* y *Latitude* son marcas comerciales de Dell Inc.; *Microsoft*, *Windows* y *Windows Vista* son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos o en otros países. *Procomm Plus* es una marca comercial de Symantec Corporation o sus filiales en los Estados Unidos y en otros países.

Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Modelo M6220

Septiembre de 2007 Rev. A00

[Regresar a la página de contenido](#)

Información sobre cables y puertos

Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [Interfaz Ethernet 10/100/1000](#)
- [Interfaces de ranura 10G doble](#)
- [Conexión del cable serie](#)
- [Conexión de alimentación](#)

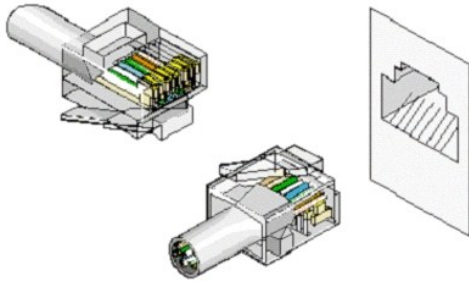
En esta sección se describen las interfaces físicas del conmutador y se proporciona información sobre las conexiones de los cables.

Las estaciones se conectan a los puertos del conmutador a través de los puertos de interfaz física del panel frontal. Para cada estación se establece el modo apropiado (semidúplex, dúplex completo y automático).

Interfaz Ethernet 10/100/1000

El puerto de conmutación se puede conectar a estaciones cableadas en el modo de estación Ethernet RJ-45 estándar mediante cables directos. Los dispositivos de transmisión conectados entre sí utilizan cables cruzados. En la [ilustración 4-1](#) se muestra el conector RJ-45.

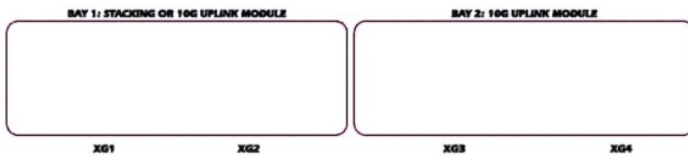
Ilustración 4-1. Conector RJ-45



Interfaces de ranura 10G doble

El M6220 admite interfaces XAUI dobles. Estas interfaces pueden funcionar a 10 Gbps cuando admiten un módulo XFP o a 12 Gbps (sólo la ranura izquierda, vista desde la parte posterior) cuando admiten un módulo de apilamiento. En la [ilustración 4-2](#) se muestran las ranuras XAUI.

Ilustración 4-2. Ranuras XAUI



Conexión del cable serie

Al realizar la configuración inicial, puede utilizar el cable serie USB tipo A a DB9 para conectar el conmutador a un terminal, aunque también puede utilizar un ordenador que ejecute software de emulación de terminal. El cable serie del conmutador es un cable cruzado de USB tipo A a DB-9 hembra (consulte la [ilustración 4-3](#)).

Ilustración 4-3. Conectores serie



Conexión del conmutador a un terminal

1. Conecte el cable serie al conector ASCII RS-232 DTE del terminal (consola).
2. Conecte el cable de la interfaz al puerto serie del conmutador.
3. Si va a configurar una pila, conecte el cable de interfaz al puerto serie del conmutador maestro.

Para más información sobre la conexión al puerto serie de Dell™ PowerConnect™ serie M6220, consulte la *M6220 Series Stackable Switches Getting Started Guide* (Guía de introducción a los conmutadores apilables serie M6220).

Conexión de alimentación

El PowerConnect serie M6220 recibe energía del chasis del servidor del módulo de alta densidad de Dell. Para obtener más información sobre la fuente de alimentación del PowerConnect serie M6220, consulte el *Dell Blade Server Chassis Hardware Owner's Manual* (Manual del propietario del hardware del chasis del servidor del módulo de alta densidad de Dell).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de la información del sistema

Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [Apertura de la página System](#)
- [Definición de la información general del dispositivo](#)
- [Configuración de SNTP](#)
- [Administración de registros](#)
- [Definición del direccionamiento IP](#)
- [Ejecución de los diagnósticos de cables](#)
- [Administración de la seguridad del dispositivo](#)
- [Definición de los parámetros de SNMP](#)
- [Administración de archivos](#)
- [Definición de la configuración avanzada](#)
- [Definición del apilamiento](#)

Apertura de la página System

Utilice los menús que aparecen en la página **System** (Sistema) para definir la relación del conmutador con su entorno. Para visualizar la página **System** (Sistema), haga clic en **System** (Sistema) en la vista de árbol. La página de menú **System** (Sistema) contiene enlaces a las funciones siguientes:

- | [Definición de la información general del dispositivo](#)
- | [Configuración de SNTP](#)
- | [Administración de registros](#)
- | [Definición del direccionamiento IP](#)
- | [Ejecución de los diagnósticos de cables](#)
- | [Administración de la seguridad del dispositivo](#)
- | [Definición de los parámetros de SNMP](#)
- | [Administración de archivos](#)
- | [Definición de la configuración avanzada](#)
- | [Definición del apilamiento](#)

Definición de la información general del dispositivo

La página de menú **General** contiene enlaces a páginas que permiten configurar los parámetros del dispositivo. Utilice esta página para acceder a las funciones siguientes:

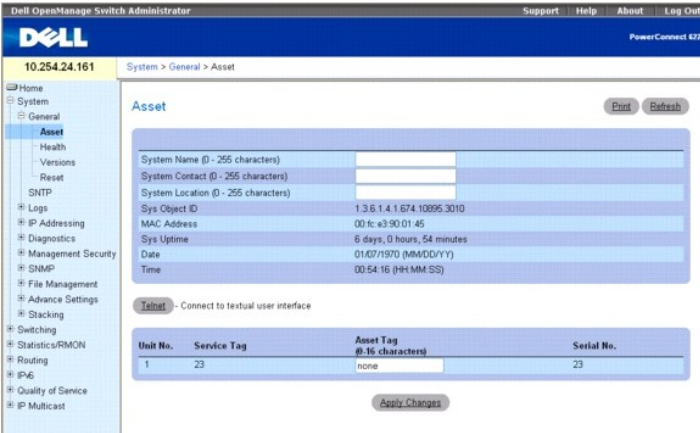
- | [Inventario](#)
- | [Estado del sistema](#)
- | [Versiones](#)
- | [Recursos del sistema](#)
- | [Configuración de la zona horaria](#)
- | [Configuración del horario de verano](#)
- | [Detalles del reloj](#)
- | [Restablecimiento](#)

Inventario

Utilice los campos de la página **Asset** (Inventario) para configurar y ver información general del dispositivo.

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

Ilustración 6-1. Inventario



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

- System Name (0 – 255 characters)** (Nombre del sistema [0–255 caracteres]): sirve para asignar un nombre al sistema del dispositivo.
- System Contact (0 – 255 characters)** (Contacto del sistema [0–255 caracteres]): sirve para asignar el nombre de la persona de contacto.
- System Location (0 – 255 characters)** (Ubicación del sistema [0–255 caracteres]): sirve para especificar una ubicación del sistema.
- Sys Object ID** (ID de objeto del sistema): la ID de objeto del sistema asignada.
- MAC Address** (Dirección MAC): muestra la dirección MAC del conmutador.
- Sys Uptime** (Tiempo de actividad del sistema): muestra el número de días, horas y minutos transcurridos desde el último reinicio.
- Date** (Fecha): muestra la fecha actual del sistema. El formato es mes, día, año (MM/DD/AA). Por ejemplo, 11/01/05 es el 01 de noviembre de 2005.
- Time** (Hora): muestra la hora actual del sistema. El formato es hora, minuto, segundo (HH:MM:SS). Por ejemplo, 20:12:03 es 8:12:03 p.m.
- Unit No.** (Número de unidad): muestra la posición del conmutador en la pila.
- Service Tag** (Etiqueta de servicio): muestra el número de referencia de servicio que se utiliza cuando se efectúan tareas de mantenimiento del dispositivo.
- Asset Tag (0 – 16 characters)** (Etiqueta de inventario [0–16 caracteres]): muestra la referencia del dispositivo definida por el usuario.
- Serial No.** (Número de serie): muestra el número de serie del dispositivo.

Definición de la información del sistema

1. Abra la página **Asset** (Inventario).
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 inventario).
3. Haga clic en **Apply Changes** (Aplicar cambios).

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

Inicio de una sesión Telnet

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

NOTA: los parámetros de Telnet apropiados se establecen antes de iniciar la sesión Telnet. Para obtener información, consulte "[Configuración de una contraseña inicial de Telnet](#)". Si el cliente tiene un entorno Microsoft® Windows®, el programa debe configurarse para Telnet. Si el cliente tiene un entorno Unix, el programa Telnet debe existir en la ruta de acceso.

2. Haga clic en **Telnet**.

Aparece el indicador, lo que indica que el sistema está preparado para recibir información.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la *Guía de referencia de la CLI*:

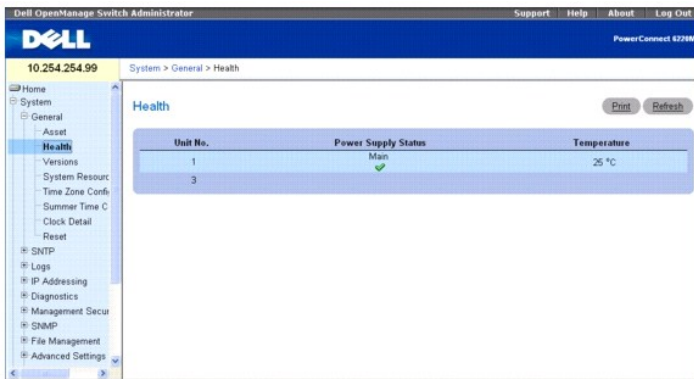
- 1 Comandos de administración del sistema
- 1 Comandos SNMP
- 1 Comandos de reloj

Estado del sistema

Utilice la página **Health** (Estado) para ver información del dispositivo físico, como por ejemplo el estado de las fuentes de energía y de ventilación del conmutador.

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

Ilustración 6-2. Estado



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

Unit No. (Número de unidad): muestra la posición de la unidad en la pila.

Power Supply Status (Estado de la fuente de alimentación): muestra el estado de la fuente de alimentación.

✓ : la fuente de alimentación funciona con normalidad.

✗ : la fuente de alimentación no funciona con normalidad.

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

Temperature (Temperatura): muestra la temperatura a la que está funcionando el dispositivo actualmente.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

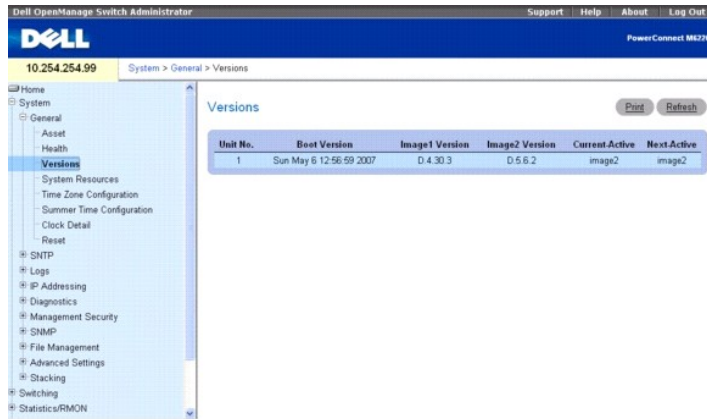
- 1 Comandos de administración del sistema

Versiones

Utilice la página **Versions** (Versiones) para ver la información sobre las versiones de software que se ejecutan actualmente.

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

Ilustración 6-3. Versiones



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

Unit No. (Número de unidad): muestra la posición de la unidad en la pila.

Boot Version (Versión de inicio): muestra la versión de inicio de la imagen activa.

Image1 Version (Versión de la imagen 1): muestra el número de versión de una de las dos imágenes de software disponibles.

Image2 Version (Versión de la imagen 2): muestra el número de versión de la otra imagen de software disponible.

Current-Active (Versión activa actual): muestra la versión de software que se ejecuta actualmente en el dispositivo.

Next-Active (Versión activa posterior): muestra la versión de software que se cargará si la versión actual se bloquea.

Visualización de las versiones del dispositivo mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

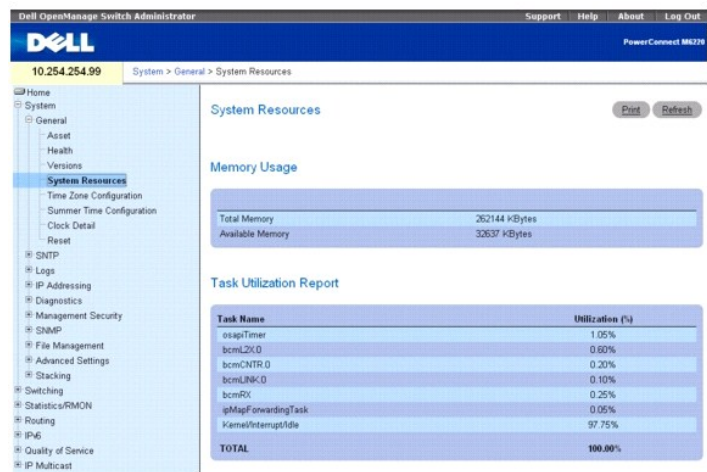
- 1 Comandos de administración del sistema

Recursos del sistema

Utilice la página **System Resources** (Recursos del sistema) para ver información sobre la utilización de la memoria y las tareas.

Para visualizar la página **System Resources** (Recursos del sistema), haga clic en **System** (Sistema) → **General** → **System Resources** (Recursos del sistema) en la vista de árbol.

Ilustración 6-4. Recursos del sistema



La página **System Resources** (Recursos del sistema) contiene los campos siguientes:

Total Memory (Memoria total): muestra la cantidad de memoria total del conmutador.

Available Memory (Memoria disponible): muestra la memoria disponible (que se puede asignar) en el conmutador.

Task Name (Nombre de la tarea): nombre de la tarea activa que se ejecuta en el conmutador.

Utilization (%) (Porcentaje de utilización): porcentaje del tiempo de la CPU que utiliza la tarea correspondiente. Se calcula para una duración de 2 segundos.

Visualización de los recursos del sistema mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

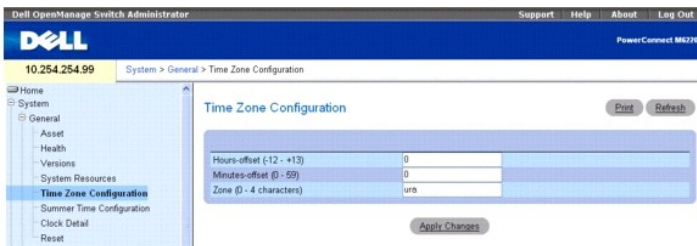
- 1 Comandos de administración del sistema

Configuración de la zona horaria

Utilice la función **Time Zone Configuration** (Configuración de la zona horaria) para configurar la diferencia de zona horaria respecto a la hora universal coordinada (UTC).

Para visualizar la página **Time Zone Configuration** (Configuración de la zona horaria), haga clic en **System** (Sistema) → **General** → **Time Zone Configuration** (Configuración de la zona horaria) en la vista de árbol.

Ilustración 6-5. Configuración de la zona horaria



La página **Time Zone Configuration** (Configuración de la zona horaria) contiene los campos siguientes:

Hours-offset (Diferencia de horas): define la diferencia de horas respecto a la UTC. El intervalo es de -12 a +13.

Minutes-offset (Diferencia de minutos): define la diferencia de minutos respecto a la UTC. El intervalo es de 0-59)

Zone (Zona): define la sigla de la zona horaria. El intervalo es de 0 a 4 caracteres.

Definición de los parámetros de zona horaria

1. Abra la página **Time Zone Configuration** (Configuración de la zona horaria).
2. Defina los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los valores de configuración de la zona horaria y se actualiza el dispositivo.

Configuración de la zona horaria mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

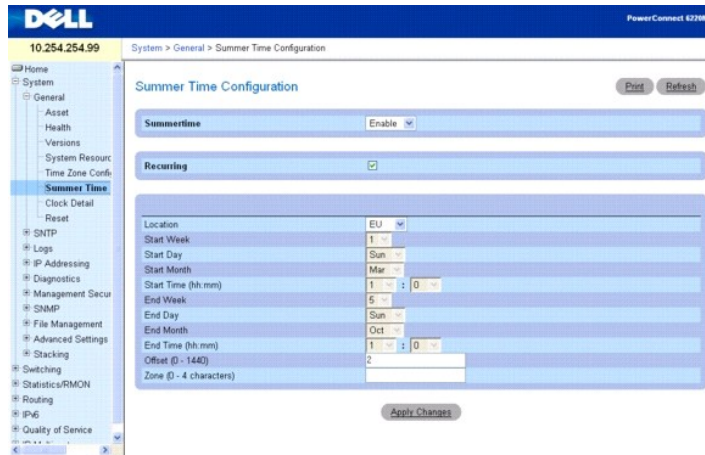
- 1 Comandos de reloj

Configuración del horario de verano

Utilice la página **Summer Time Configuration** (Configuración del horario de verano) para especificar la diferencia y la duración de un horario de verano definido.

Para visualizar la página **Summer Time Configuration** (Configuración del horario de verano), haga clic en **System** (Sistema) → **General** → **Summer Time Configuration** (Configuración del horario de verano) en la vista de árbol.

Ilustración 6-6. Configuración del horario de verano



Los campos de la página **Summer Time Configuration** (Configuración del horario de verano) cambian al marcar o desmarcar la casilla de verificación **Recurring** (Periódico). La página **Summer Time Configuration** (Configuración del horario de verano) contiene los campos siguientes:

Recurring (Periódico): seleccione esta casilla de verificación para indicar que la configuración se repetirá cada año.

Location (Ubicación): este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está seleccionada. La configuración del horario de verano está predefinida para los Estados Unidos y la Unión Europea. Para definir el horario de verano de una ubicación distinta, seleccione **None** (Ninguno).

Start Week (Semana de inicio): seleccione el número de la semana de inicio. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está seleccionada.

Start Day (Día de inicio): seleccione el número del día de inicio. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está seleccionada.

Start Month (Mes de inicio): seleccione el mes de inicio.

Start Time (Hora de inicio): seleccione la hora de inicio en formato hh:mm.

Start Date (Fecha de inicio): seleccione la fecha de inicio. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está desmarcada.

Start Year (Año de inicio): seleccione el año de inicio. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está desmarcada.

End Week (Semana de finalización): seleccione el número de la semana de finalización. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está seleccionada.

End Day (Día de finalización): seleccione el número del día de finalización. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está seleccionada.

End Month (Mes de finalización): seleccione el mes de finalización.

End Time (Hora de finalización): seleccione la hora de finalización en formato hh:mm.

End Date (Fecha de finalización): seleccione la fecha de finalización. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está desmarcada.

End Year (Año de finalización): seleccione el año de finalización. Este campo sólo se muestra si la casilla de verificación **Recurring** (Periódico) está desmarcada.

Offset (Diferencia): defina el número de minutos que deben añadirse durante el horario de verano en el intervalo de 0 a 1 440.

Zone (Zona): defina la sigla de la zona horaria que se mostrará cuando se aplique el horario de verano.

Definición de los parámetros del horario de verano

1. Abra la página **Summer Time Configuration** (Configuración del horario de verano).
2. Defina los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los valores de configuración del horario de verano y se actualiza el dispositivo.

Configuración de los parámetros del horario de verano mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de reloj

Detalles del reloj

Utilice la página **Clock Detail** (Detalles del reloj) para ver información sobre la configuración de la hora actual, la zona horaria y el horario de verano.

Para visualizar la página **Clock Detail** (Detalles del reloj), haga clic en **System** (Sistema)→ **General**→ **Clock Detail** (Detalles del reloj) en la vista de árbol.

Ilustración 6-7. Detalles del reloj

The screenshot shows the Dell OpenManage Switch Administrator interface. The left sidebar contains a tree view with 'System' expanded and 'Clock Detail' selected. The main content area is titled 'Clock Detail' and contains three sections:

- Current Time**:

Time (hh:mm)	11:01:19
Zone	ura (UTC + 0:00)
Date	1 Jan 1970
Time Source	No time source
- Time Zone**:

Zone	ura
Offset	UTC + 0:00
- Summertime**:

Recurring	No
Start Date	1 Jan 2000
Start Time (hh:mm)	00:00
End Date	2 Jan 2000
End Time (hh:mm)	00:00
Offset	0
Zone	Acronym not configured

En la página **Clock Detail** (Detalles del reloj) se proporciona información sobre las funciones del reloj siguientes:

Current Time (Hora actual): en esta sección se muestra la hora actual.

Time Zone (Zona horaria): en esta sección se muestra la configuración de la zona horaria.

Summertime (Horario de verano): en esta sección se muestra la configuración del horario de verano.

Visualización de los detalles del reloj mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de reloj

Restablecimiento

Utilice la página **Reset** (Restablecer) para restablecer el dispositivo.

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

Ilustración 6-8. Restablecimiento

The screenshot shows the Dell OpenManage Switch Administrator interface. The left sidebar contains a tree view with 'System' expanded and 'Reset' selected. The main content area is titled 'Reset' and contains a form with a 'Reset Unit No.' field set to '1 (Master)' and an 'Apply Changes' button.

La página **Reset** (Restablecer) contiene los campos siguientes:

Reset Unit No. (Restablecer número de unidad): sirve para seleccionar el dispositivo de la pila que debe restablecerse.

Restablecimiento del dispositivo

1. Abra la página **Reset** (Restablecer).
2. Haga clic en **Reset Unit No.** (Restablecer número de unidad).
3. Seleccione **Individual Unit** (Unidad individual) o **All** (Todo).
4. Haga clic en el botón **Apply Changes** (Aplicar cambios).
5. Cuando aparezca el mensaje de confirmación, haga clic en **OK** (Aceptar).

Se restablecerá el dispositivo seleccionado. Una vez restablecido el dispositivo, especifique un nombre de usuario y una contraseña.

Configuración de SNTP

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

Las fuentes de la hora se establecen por niveles. Estos niveles definen la precisión del reloj de referencia. Cuanto más alto sea el nivel (siendo cero el valor más alto), más preciso será el reloj. El dispositivo recibe la hora a partir del nivel 1 y subsiguientes, ya que se trata de un dispositivo de nivel 2.

A continuación se muestra un ejemplo de los niveles:

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

La información que se recibe de los servidores SNTP se evalúa a partir del nivel de hora y el tipo de servidor.

Las definiciones de hora de SNTP se evalúan y determinan según los niveles de hora siguientes:

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

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

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 hora de T1 a T4 sirven para determinar la hora del servidor. Éste es el mejor método para sincronizar la hora del dispositivo, ya que es el más seguro. Si se selecciona este método, sólo se aceptará la información de SNTP procedente de los servidores SNTP que se hayan definido en el dispositivo mediante la página **SNTP Servers** (Servidores SNTP).

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

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

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

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

La página de menú **SNTP** contiene enlaces a páginas que permiten configurar los parámetros de SNTP.

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

Utilice esta página para acceder a las funciones siguientes:

- 1 [Configuración global SNTP](#)

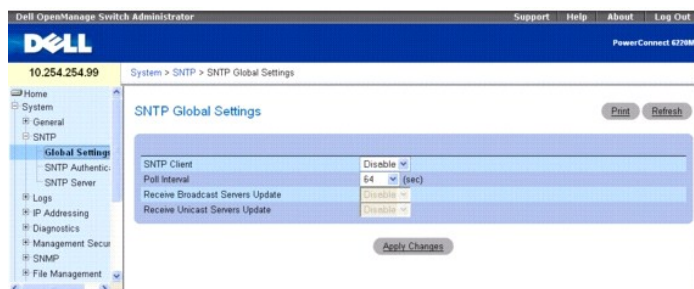
- 1 [Autenticación de SNTP](#)
- 1 [Servidor SNTP](#)

Configuración global de SNTP

Utilice la página SNTP Global Settings (Configuración global de SNTP) para ver y ajustar los parámetros de SNTP.

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

Ilustración 6-9. Configuración global de SNTP



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

SNTP Client (Cliente SNTP): utilice la lista desplegable para activar o desactivar el cliente. Si el cliente está desactivado, algunos de los campos que figuran a continuación también estarán desactivados.

Poll Interval (Intervalo de sondeo): define el intervalo (en segundos) con el que se sondea el servidor SNTP para obtener información de difusión única. El intervalo es de 60 a 1024 segundos.

Receive Broadcast Servers Update (Recibir actualizaciones de servidores de difusión): si está activado, escucha los servidores SNTP para obtener información de hora del servidor de difusión en las interfaces seleccionadas. El dispositivo se sincroniza siempre que se recibe un paquete SNTP, incluso si no se ha solicitado la sincronización.

Receive Unicast Servers Update (Recibir actualizaciones de servidores de difusión única): si está activado, sondea los servidores SNTP que se han definido en el dispositivo para obtener información de hora del servidor de difusión única.

Definición de los parámetros globales de SNTP

1. Abra la página **SNTP Global Settings** (Configuración global de SNTP).
2. Defina los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración global de SNTP y se actualiza el dispositivo.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

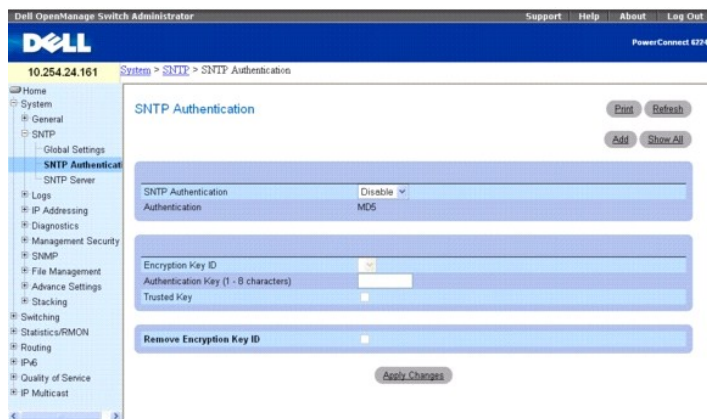
- 1 Comandos de reloj

Autenticación de SNTP

La página **SNTP Authentication** (Autenticación de SNTP) permite activar la autenticación de SNTP entre el dispositivo y un servidor SNTP, así como seleccionar el servidor SNTP deseado. Utilice la página **SNTP Authentication** (Autenticación de SNTP) para activar o desactivar la autenticación de SNTP, modificar la clave de autenticación de una ID de clave de cifrado seleccionada, designar la clave de autenticación seleccionada como clave de confianza y eliminar la ID de clave de cifrado seleccionada.

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

Ilustración 6-10. Autenticación de SNTP



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

SNTP Authentication (Autenticación de SNTP): si se activa, requiere autenticar una sesión SNTP entre el dispositivo y un servidor SNTP.

Authentication (Autenticación): tipo de autenticación. El sistema sólo admite MD5.

Encryption Key ID (ID de clave de cifrado): contiene una lista de las ID de clave definidas por el usuario que sirven para autenticar el servidor SNTP y el dispositivo. Los valores posibles del campo son 1-4294767295.

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

Trusted Key (Clave de confianza): marque esta casilla para especificar la clave de cifrado utilizada (difusión única) o desmárquela para autenticar el servidor SNTP (difusión).

Remove Encryption Key ID (Eliminar ID de clave de cifrado): marque esta casilla para eliminar la clave de autenticación seleccionada.

Adición de una clave de autenticación de SNTP

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

Aparece la página **Add Authentication Key** (Añadir clave de autenticación):

Ilustración 6-11. Adición de una clave de autenticación



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

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

Visualización de la tabla de claves de autenticación

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

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

Ilustración 6-12. Tabla de claves de autenticación

Encryption Key ID	Authentication Key	Trusted Key	Remove
4545	xspgv	Yes	<input type="checkbox"/>

Eliminación de una clave de autenticación

1. Abra la página **SNTP Authentication** (Autenticación de SNTP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **Authentication Key Table** (Tabla de claves de autenticación).
3. Seleccione una entrada de **Authentication Key Table** (Tabla de claves de autenticación) marcando la casilla de verificación **Remove** (Eliminar) correspondiente.
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se elimina la entrada y se actualiza el dispositivo.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

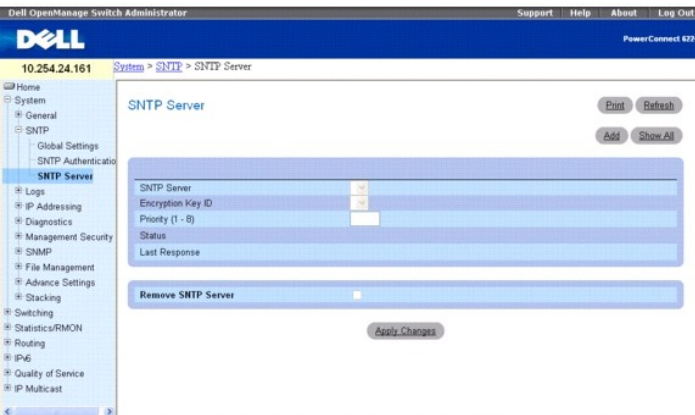
- 1 Comandos de reloj

Servidor SNTP

Utilice la página **SNTP Server** (Servidor SNTP) para ver y modificar información, activar los servidores SNTP y añadir nuevos servidores SNTP.

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

Ilustración 6-13. Servidores SNTP



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

SNTP Server (Servidor SNTP): permite seleccionar la dirección IP del servidor SNTP definida por el usuario en un menú desplegable. Se pueden definir hasta ocho servidores SNTP mediante el botón **Add** (Añadir).

Encryption Key ID (ID de clave de cifrado): permite especificar la ID de clave definida por el usuario utilizada para la comunicación entre el servidor SNTP y el dispositivo. La ID de clave de cifrado se define en la página **SNTP Authentication** (Autenticación de SNTP).

Priority (1-8) (Prioridad [1-8]): permite especificar la prioridad de esta entrada de servidor al determinar la secuencia de servidores a los que se envían las peticiones SNTP. Los valores van del 1 al 8, y el valor predeterminado es 1. Los servidores con los números más bajos tienen prioridad.

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

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

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

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

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

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

Remove SNTP Server (Eliminar servidor SNTP): elimina un servidor SNTP especificado de la lista **SNTTP Servers** (Servidores SNTP).

Adición de un servidor SNTP

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

Aparece la página **Add SNTTP Server** (Añadir servidor SNTP).

Ilustración 6-14. Adición de un servidor SNTP



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

Se añade el servidor SNTP y se actualiza el dispositivo.

Visualización de la tabla de servidores SNTP

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

Aparece la página **SNTTP Servers Table** (Tabla de servidores SNTP).

Ilustración 6-15. Tabla de servidores SNTP



SNTTP Server	Encryption Key ID	Priority	Status	Last Response	Remove
1 10.240.1.10	None	1	Up	Thu 1 Jan 1970 00:00:00	<input type="checkbox"/> Edit

Modificación de un servidor SNTP

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

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

3. Haga clic en **Edit** (Editar) junto a la entrada **SNTTP Server** (Servidor SNTP) que desee modificar.
4. Modifique los campos pertinentes.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se actualiza la información de servidor SNTP.

Eliminación de un servidor SNTP

1. Abra la página **SNTP Servers** (Servidores SNTP).

2. Haga clic en **Show All** (Mostrar todo)

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

3. Seleccione una entrada de **SNTP Server** (Servidor SNTP).

4. Marque la casilla de verificación **Remove** (Eliminar).

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

Se elimina la entrada y se actualiza el dispositivo.

Definición de servidores SNTP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de reloj

Administración de registros

El conmutador puede generar mensajes de respuesta a los eventos, fallos o errores que se producen en la plataforma, así como a los cambios en la configuración u otras incidencias. Estos mensajes se almacenan localmente en la plataforma y se reenvían a uno a más puntos centralizados de recogida con fines de supervisión, así como para su almacenamiento en archivos a largo plazo. La configuración local y remota de la capacidad de registro incluye el filtrado de los mensajes registrados o reenviados según su gravedad y el componente que los ha generado.

El registro *en memoria* almacena los mensajes en la memoria según la configuración de la gravedad y el componente del mensaje. En los sistemas apilables, este registro sólo existe en la parte superior de la plataforma de la pila. Otras plataformas de la pila reenvían sus mensajes a la parte superior del registro de la pila. No se admite el acceso a los registros en memoria que no se encuentren en la parte superior de la plataforma de la pila.

El registro *persistente* se almacena en el almacenamiento persistente. Se pueden configurar dos tipos de registros persistentes.

- 1 El primer tipo de registro es el **registro de inicio del sistema**. El registro de inicio del sistema almacena los primeros mensajes N recibidos después de reiniciarse el sistema. Este registro tiene siempre el atributo de funcionamiento de registro completo establecido en "stop on full" (detenerse cuando esté completo), y puede almacenar hasta 32 mensajes.
- 1 El segundo tipo de registro es el **registro de funcionamiento del sistema**. El registro de funcionamiento del sistema almacena los últimos mensajes N recibidos durante el funcionamiento del sistema. Este registro tiene siempre el atributo de funcionamiento de registro completo establecido en "overwrite" (sobrescribir). Este registro puede almacenar hasta 1 000 mensajes.

El registro de inicio del sistema o el registro de funcionamiento del sistema almacena un mensaje recibido por el subsistema de registro que cumple los criterios de almacenamiento, pero no pueden guardarlo ambos registros. En otras palabras, si el registro de inicio está configurado al iniciarse el sistema, almacenará mensajes hasta llegar al límite. Si el registro de funcionamiento está configurado, empezará a almacenar los mensajes.

El sistema conserva hasta tres versiones de los registros persistentes, con los nombres <ARCHIVO>0.txt, <ARCHIVO>1.txt y <ARCHIVO>2.txt. Cuando se inicie el sistema, se eliminará el registro <ARCHIVO>2.txt, el registro <ARCHIVO>1.txt pasará a llamarse <ARCHIVO>2.txt, el registro <ARCHIVO>0.txt pasará a llamarse <ARCHIVO>1.txt, se creará el registro <ARCHIVO>0.txt y los registros se iniciarán en <ARCHIVO>0.txt. Sustituya <ARCHIVO> en el ejemplo anterior para especificar olog para el registro de funcionamiento y slog para el registro de inicio.

Los registros locales persistentes pueden recuperarse mediante la CLI, xmodem por medio del cable serie local y TFTP.

Para visualizar la página de menú **Logs** (Registros), haga clic en **System** (Sistema) → **Logs** (Registros) en la vista de árbol. Utilice esta página para acceder a las funciones siguientes:

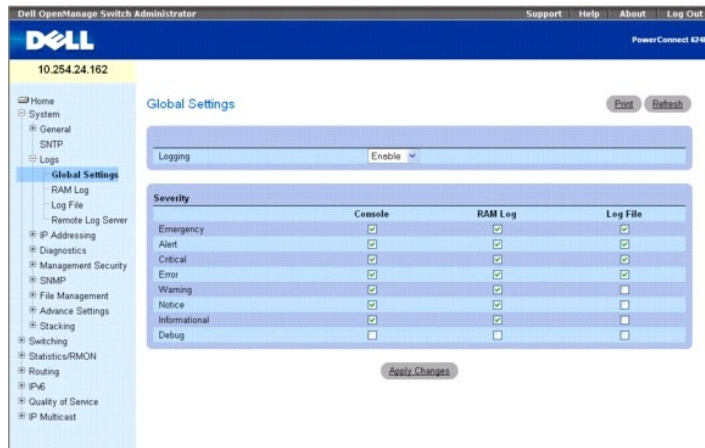
- 1 [Configuración global](#)
- 1 [Tabla de registros de RAM](#)
- 1 [Archivo de registro](#)
- 1 [Configuración de servidores remotos de registros](#)

Configuración global

Utilice la página **Global Settings** (Configuración global) para activar los registros globalmente y definir los parámetros de los registros. Los mensajes de registro de **Severity** (Gravedad) se enumeran de mayor a menor gravedad.

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

Ilustración 6-16. Configuración global



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

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

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

Disable (Desactivar): desactiva la opción de guardar registros. No es posible desactivar el guardado de los registros que se imprimen en la consola.

Gravedad

Utilice las casillas de verificación de esta sección para ajustar la sensibilidad de la consola, la memoria persistente y los archivos de registro.

Si selecciona un nivel específico, todos los niveles superiores se seleccionarán automáticamente. Por ejemplo, si selecciona Error, el sistema seleccionará automáticamente Error, Critical (Grave), Alert (Alerta) y Emergency (Emergencia). Si deselecciona Error, todos los niveles inferiores (por ejemplo, Error, Warning [Advertencia], Notice [Aviso], Informational [Informativo], Debug [Depuración]) se deseleccionarán.

Emergency (Emergencia): indica el nivel más alto de advertencia. Si el dispositivo no funciona o funciona incorrectamente, se guarda un registro de emergencia en el dispositivo.

Alert (Alerta): indica el segundo nivel más alto de advertencia. Un registro de alerta se guarda si se produce un fallo grave en el dispositivo, como por ejemplo que no funcionen las funciones del dispositivo.

Critical (Grave): indica el tercer nivel más alto de advertencia. Un registro grave se guarda cuando ocurre un fallo grave en el dispositivo, por ejemplo, si dos puertos del dispositivo no funcionan mientras los demás puertos del dispositivo sí funcionan.

Error: indica que se ha producido un error en un dispositivo, por ejemplo, cuando un puerto está fuera de línea.

Warning (Advertencia): indica el nivel más bajo de advertencia en un dispositivo.

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

Informational (Informativo): proporciona información sobre el dispositivo.

Debug (Depuración): proporciona información detallada sobre el registro. Sólo el personal de asistencia cualificado puede realizar la depuración de errores.

Las casillas de verificación aparecen bajo las tres columnas siguientes:

Console (Consola): registros enviados a la consola.

RAM Logs (Registros de RAM): registros enviados a la RAM (caché).

Log File (Archivo de registro): registros enviados al archivo (FLASH).

Activación de registros

1. Abra la página **Global Settings** (Configuración global).
2. Seleccione **Enable** (Activar) en el menú desplegable de **Logging** (Registro).
3. Utilice las casillas de verificación para seleccionar el tipo de registro y la gravedad.

NOTA: al seleccionar un nivel de gravedad, todos los niveles de gravedad superiores se seleccionan automáticamente.

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

Se guarda la configuración del registro y se actualiza el dispositivo.

Activación de los registros globales mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

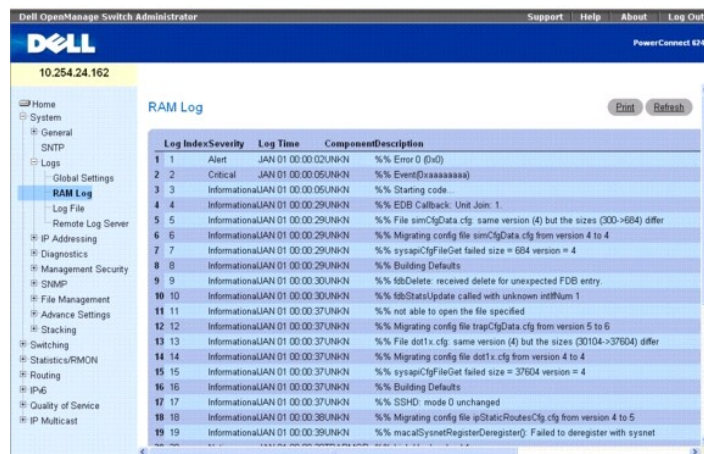
1 Comandos Syslog

Tabla de registros de RAM

Utilice la página **RAM Log Table** (Tabla de registros de RAM) para ver información sobre las entradas de registro de RAM (caché) específicas, como la hora de introducción del registro, la gravedad del registro y una descripción del registro.

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

Ilustración 6-17. Tabla de registros de RAM



Log Index	Severity	Log Time	Component	Description
1	Alert	JAN 01 00:00:00:UN-N	%	Error 0 (0x0)
2	Critical	JAN 01 00:00:05:UN-N	%	Event(D:aaaaaaaa)
3	Informational	JAN 01 00:00:05:UN-N	%	Starting code...
4	Informational	JAN 01 00:00:29:UN-N	%	EDB Callback: Unit Join: 1
5	Informational	JAN 01 00:00:29:UN-N	%	File simCfgData.cfg: same version (4) but the sizes (300->664) differ
6	Informational	JAN 01 00:00:29:UN-N	%	Migrating config file simCfgData.cfg from version 4 to 4
7	Informational	JAN 01 00:00:29:UN-N	%	sysapiCfgFileGet failed size = 664 version = 4
8	Informational	JAN 01 00:00:29:UN-N	%	Building Defaults
9	Informational	JAN 01 00:00:30:UN-N	%	fdbDelete: received delete for unexpected FDB entry.
10	Informational	JAN 01 00:00:30:UN-N	%	fdbStatsUpdate called with unknown intNum 1
11	Informational	JAN 01 00:00:37:UN-N	%	not able to open the file specified
12	Informational	JAN 01 00:00:37:UN-N	%	Migrating config file trapCfgData.cfg from version 5 to 6
13	Informational	JAN 01 00:00:37:UN-N	%	File dot1x.cfg: same version (4) but the sizes (30104->37604) differ
14	Informational	JAN 01 00:00:37:UN-N	%	Migrating config file dot1x.cfg from version 4 to 4
15	Informational	JAN 01 00:00:37:UN-N	%	sysapiCfgFileGet failed size = 37604 version = 4
16	Informational	JAN 01 00:00:37:UN-N	%	Building Defaults
17	Informational	JAN 01 00:00:37:UN-N	%	SSH: mode 0 unchanged
18	Informational	JAN 01 00:00:38:UN-N	%	Migrating config file ipStaticRoutesCfg.cfg from version 4 to 5
19	Informational	JAN 01 00:00:39:UN-N	%	macalSysnetRegisterDeregister(): Failed to deregister with sysnet

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

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

Severity (Gravedad): indica la gravedad del registro.

Log Time (Hora de registro): indica la hora de introducción del registro en la tabla de registros de RAM.

Component (Componente): indica el componente que se registra.

Description (Descripción): proporciona la descripción del registro.

Eliminación de la información de registro

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

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

Eliminación de la información de registro mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

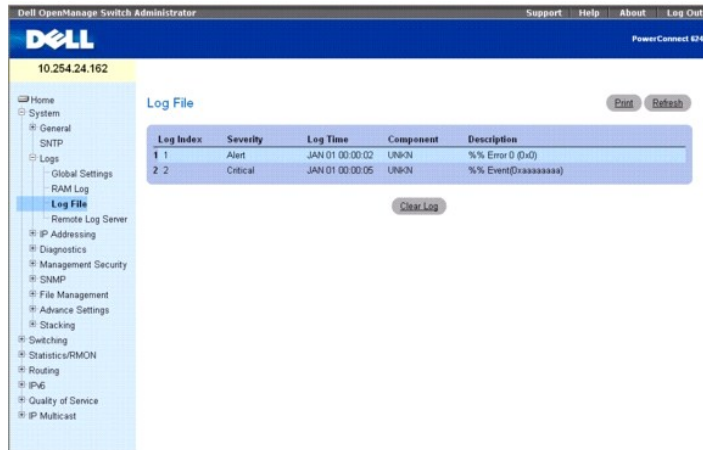
1 Comandos Syslog

Archivo de registro

La página **Log File** (Archivo de registro) contiene información sobre las entradas de registro específicas, como la hora de introducción del registro, la gravedad del registro y una descripción del registro.

Para visualizar la página **Log File** (Archivo de registro), haga clic en **System** (Sistema)→ **Logs** (Registros)→ **Log File** (Archivo de registro) en la vista de árbol.

Ilustración 6-18. Archivo de registro



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

- 1 **Log Index** (Índice de registro): indica el número de registro en la tabla de archivos de registro.
- 1 **Severity** (Gravedad): indica la gravedad del registro.
- 1 **Log Time** (Hora de registro): indica la hora de introducción del registro en la tabla de archivos de registro.
- 1 **Component** (Componente): indica el componente que se registra.
- 1 **Description** (Descripción): proporciona la descripción del registro.

Eliminación de la información de registro

1. Abra la página **Log File Table** (Tabla de archivos de registro).
2. Haga clic en **Clear Log** (Borrar registro).

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

Eliminación de la información de registro mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

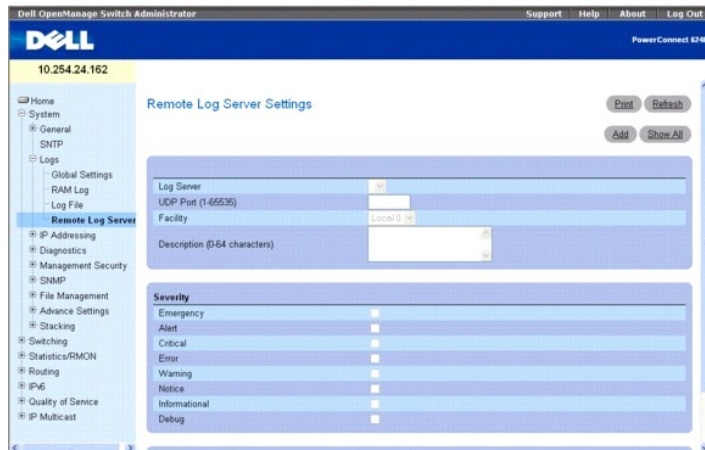
- 1 Comandos Syslog

Configuración de servidores remotos de registros

Utilice la página **Remote Log Server Settings** (Configuración de servidores remotos de registros) para ver los servidores de registros disponibles, para definir nuevos servidores de registros y para establecer la gravedad de los eventos de registro enviados al servidor.

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

Ilustración 6-19. Configuración de servidores remotos de registros



La página **Remote Log Server Settings** (Configuración de servidores remotos de registros) contiene los campos siguientes:

Log Server (Servidor de registros): indica el servidor al que pueden enviarse los registros.

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

Facility (Función): aplicación definida por el usuario desde la cual se envían los registros del sistema al servidor remoto. Sólo se puede asignar una función por servidor. Si se asigna un segundo nivel de función, éste sobrescribirá el primer nivel. Todas las aplicaciones definidas para un dispositivo utilizan la misma función en un servidor. Los valores del campo posibles van de **Local 0** a **Local 7**.

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

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

Remove Log Server (Eliminar servidor de registros): elimina un servidor de la lista de servidores de registros. Si se marca la casilla de verificación, se elimina el servidor de la lista. Si se deja la casilla desmarcada, el servidor se mantiene en la lista.

La página **Remote Log Server Settings** (Configuración de servidores remotos de registros) también contiene una lista de niveles de gravedad. Las definiciones de gravedad son las mismas que las de la página **RAM Log Table** (Tabla de registros de RAM).

Envío de registros a un servidor

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

 **NOTA:** al seleccionar un nivel de gravedad, todos los niveles de gravedad superiores se seleccionan automáticamente.

4. Haga clic en **Apply Changes** (Aplicar cambios).
Se guarda la configuración del registro y se actualiza el dispositivo.

Adición de un servidor nuevo

1. Abra la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).
2. Haga clic en **Add** (Añadir) para visualizar la página **Add Remote Log Server** (Añadir servidor remoto de registros).


 **NOTA:** antes de añadir un nuevo servidor, determine la dirección IP del servidor remoto de registros.

Ilustración 6-20. Adición de un servidor remoto de registros

Add Remote Log Server Print Refresh

Log Server	<input type="text"/>
UDP Port (1-65535)	514
Facility	Local 7
Description (64 characters)	<input type="text"/>

Severity	
Emergency	<input checked="" type="checkbox"/>
Alert	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>
Error	<input checked="" type="checkbox"/>
Warning	<input checked="" type="checkbox"/>
Notice	<input checked="" type="checkbox"/>
Informational	<input checked="" type="checkbox"/>
Debug	<input type="checkbox"/>

Apply Changes Back

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

En la página **Remote Log Server Settings** (Configuración de servidores remotos de registros), sólo se muestra el servidor en la lista de servidores de registros después de volver a la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).

Visualización y eliminación de un servidor de registro

- Abra la página **Remote Log Server Settings** (Configuración de servidores remotos de registros).
- Haga clic en **Show All** (Mostrar todo) para visualizar la página **Remote Log Servers Table** (Tabla de servidores remotos de registros).

Ilustración 6-21. Visualización de todos los servidores de registros

Remote Log Servers Table Print Refresh

Log Server	UDP Port	Facility	Description	Minimum Severity	Remove
1 10.240.10.1	23	Local 7		Informational	<input type="checkbox"/> Edit

Apply Changes Back

- Para eliminar un servidor, marque la casilla de verificación **Remove** (Eliminar) correspondiente.
- Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el servidor y se actualiza el dispositivo.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos Syslog

Definición del direccionamiento IP

Utilice la página **IP Addressing** (Direccionamiento IP) para asignar direcciones IP de puerta de enlace predeterminada y de interfaz de administración, para negociar con el sistema de nombres de dominio, establecer un nombre de dominio predeterminado, realizar la asignación de nombres de host y definir los parámetros ARP y DHCP para las interfaces.

Para visualizar la página **IP Addressing** (Direccionamiento IP), haga clic en **System** (Sistema) → **IP Addressing** (Direccionamiento IP) en la vista de árbol. Utilice esta página para acceder a las funciones siguientes:

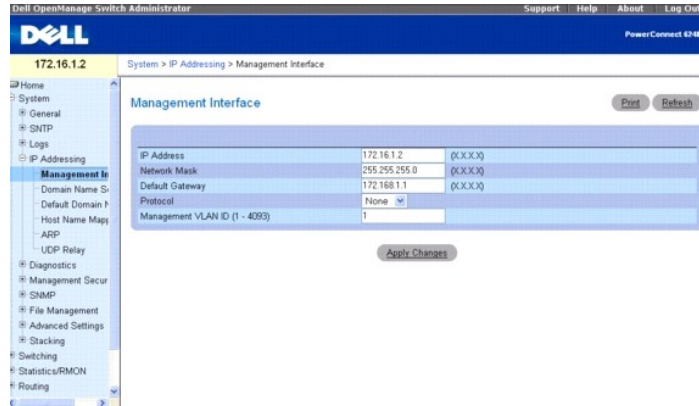
- [Interfaz de administración](#)
- [Servidor de nombres de dominio \(DNS\)](#)
- [Nombre de dominio predeterminado](#)
- [Asignación de nombres de host](#)
- [Tabla de ARP](#)
- [Relé de UDP](#)

Interfaz de administración

Utilice la página de menú **Management Interface** (Interfaz de administración) para asignar la dirección IP de la interfaz de administración, la máscara de subred, la dirección IP de la puerta de enlace predeterminada y para activar o desactivar el protocolo de inicio.

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


Ilustración 6-22. Interfaz de administración



La página **Management Interface** (Interfaz de administración) contiene los campos siguientes:

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


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

 **NOTA:** cada parte de la dirección IP debe empezar por un número que no sea cero. Por ejemplo, las direcciones IP 001.100.192.6 y 192.001.10.3 no son válidas.

Default Gateway (Puerta de enlace predeterminada): permite establecer la dirección IP de la puerta de enlace predeterminada.

Protocol (Protocolo): utilice el menú desplegable para seleccionar Bootp, DHCP o None (Ninguno).

Management VLAN ID (1-4093) (ID de VLAN de administración [1-4093]): permite establecer la ID de VLAN de administración en el intervalo de 1 a 4093.

 **AVISO:** si cambia la VLAN de administración, se desconectará la sesión web.

Modificación de los parámetros de la dirección IP de la interfaz de administración

1. Abra la página **Management Interface** (Interfaz de administración).
2. Modifique la dirección IP en el campo **IP Address** (Dirección IP).
3. Modifique los otros campos necesarios.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros y se actualiza el dispositivo.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos de enrutamiento IP

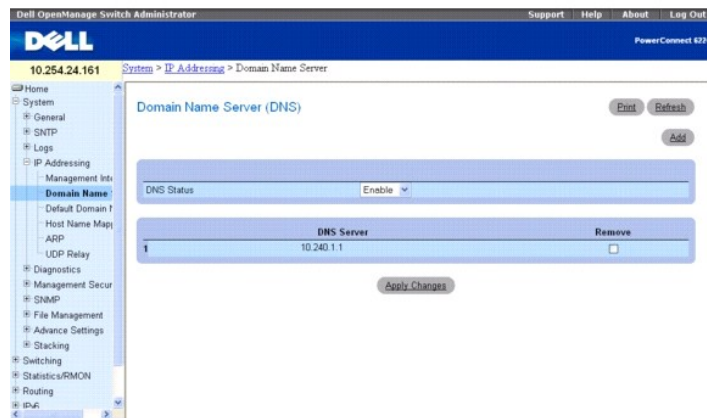
Servidor de nombres de dominio (DNS)

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

Utilice la página **Domain Name Server (DNS)** (Servidor de nombres de dominio [DNS]) para activar servidores DNS específicos.

Para visualizar la página **Domain Name Server** (Servidor de nombres de dominio), haga clic en **System** (Sistema)→ **IP Addressing** (Direccionamiento IP)→ **Domain Name Server** (Servidor de nombres de dominio) en la vista de árbol.

Ilustración 6-23. Servidor de nombres de dominio



La página **Domain Name Server (DNS)** (Servidor de nombres de dominio [DNS]) contiene los campos siguientes:

DNS Status (Estado de DNS): activa o desactiva la conversión de nombres DNS en direcciones IP.

DNS Server (Servidor DNS): contiene una lista de servidores DNS. Los servidores DNS se añaden en la página **Add DNS Server** (Añadir servidor DNS).

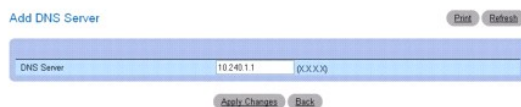
Remove (Eliminar): si se marca esta casilla, elimina el servidor DNS seleccionado.

Adición de un servidor DNS

1. Abra la página **Domain Name Server (DNS)** (Servidor de nombres de dominio [DNS]).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add DNS Server** (Añadir servidor DNS).

Ilustración 6-24. Adición de un servidor DNS



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

Se define el nuevo servidor DNS y se actualiza el dispositivo.

Configuración de los servidores DNS mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

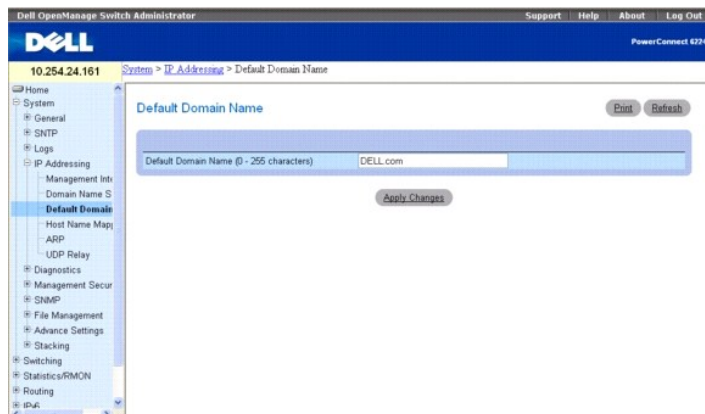
- 1 Comandos de direccionamiento IP

Nombre de dominio predeterminado

Utilice la página **Default Domain Name** (Nombre de dominio predeterminado) para ver y definir los nombres de dominio DNS predeterminados.

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

Ilustración 6-25. Nombre de dominio predeterminado



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

Default Domain Name (0–255 characters) (Nombre de dominio predeterminado [0–255 caracteres]): contiene el nombre de dominio predeterminado definido por el usuario. Una vez configurado, el nombre de dominio predeterminado se aplica a todos los nombres de host incompletos.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

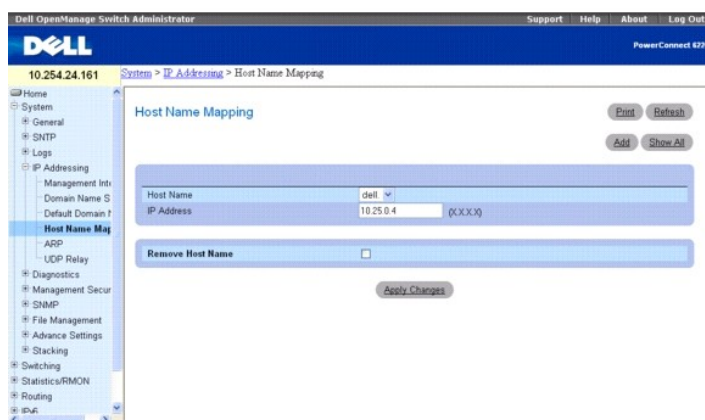
- 1 Comandos de direccionamiento IP

Asignación de nombres de host

Utilice la página **Host Name Mapping** (Asignación de nombres de host) para asignar una dirección IP a un nombre de host estático. La página **Host Name Mapping** (Asignación de nombres de host) proporciona una dirección IP por host.

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

Ilustración 6-26. Asignación de nombres de host



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

Host Name (Nombre de host): contiene una lista de nombres de host. Los nombres de host se definen en la página **Add Static Host Name Mapping** (Añadir asignación de nombres de host estáticos). Cada host proporciona una dirección IP.

IP Address (Dirección IP): proporciona una dirección IP que se asigna al nombre de host especificado.

Remove Host Name (Eliminar nombre de host): si se marca esta casilla, elimina la asignación IP del nombre de host.

Adición de nombres de dominios de host

1. Abra la página **Host Name Mapping** (Asignación de nombres de host).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add Static Host Name Mapping** (Añadir asignación de nombres de host estáticos):

Ilustración 6-27. Adición de asignación de nombres de host estáticos

3. Defina los campos pertinentes.
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Se asigna la dirección IP al nombre de host y se actualiza el dispositivo.

Visualización de la tabla de asignación de nombres de host estáticos

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

Aparece la página **Static Host Name Mapping Table** (Tabla de asignación de nombres de host estáticos):

Ilustración 6-28. Tabla de asignación de nombres de host estáticos

Host Name	IP Address	Remove
DELL	10.25.0.4	<input type="checkbox"/>

Eliminación de un nombre de host de la asignación de direcciones IP

1. Abra la página **Host Name Mapping** (Asignación de nombres de host).
 2. Haga clic en **Show All** (Mostrar todo).
- Se abre la página **Host Name Mapping Table** (Tabla de asignación de nombres de host).
3. Seleccione una entrada de la tabla de asignación de nombres de host.
 4. Marque la casilla de verificación **Remove** (Eliminar).
 5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la tabla de asignación de nombres host y se actualiza el dispositivo.

Asignación de una dirección IP a nombres de host de dominio mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1. Comandos de direccionamiento IP

Tabla de ARP

Utilice la página **ARP Table** (Tabla de ARP) para ver los parámetros de ARP para las interfaces IP. La tabla de ARP muestra la correlación entre cada dirección MAC y la dirección IP correspondiente.

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

Ilustración 6-29. Tabla de ARP



La página ARP Table (Tabla de ARP) contiene los campos siguientes:

IP Address (Dirección IP): dirección IP de la estación, que se asocia con la dirección MAC especificada a continuación.

MAC Address (Dirección MAC): dirección MAC de la estación, que se asocia en la tabla de ARP con la dirección IP.

Visualización de la tabla de ARP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de direccionamiento IP

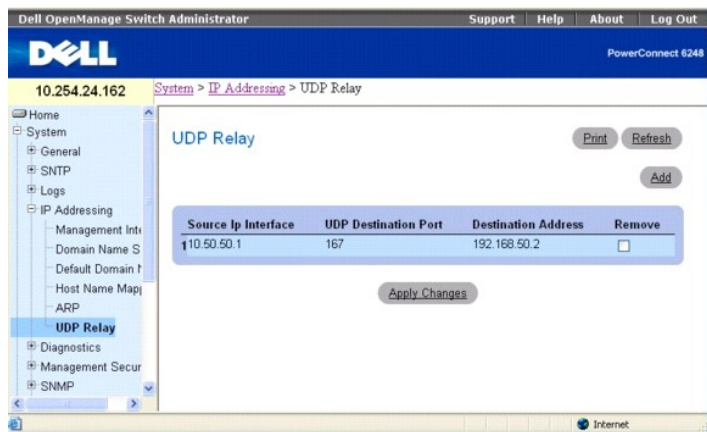
Relé de UDP

El relé de UDP permite que el dispositivo reenvíe difusiones UDP específicas de una interfaz a otra. Los paquetes de difusión IP no suelen enviarse de una interfaz a otra, pero algunas aplicaciones utilizan la difusión UDP para detectar la disponibilidad de un servicio. Otros servicios requieren que los paquetes de difusión UDP se direccionen para poder proporcionar servicios a los clientes de otra subred. EL relé de UDP también permite la navegación desde estaciones de trabajo a servidores en distintas redes.

Utilice la página UDP Relay (Relé de UDP) para añadir, mostrar o eliminar la configuración del relé de UDP.

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

Ilustración 6-30. Relé de UDP



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

Source IP Interface (Interfaz IP de origen): interfaz IP de entrada que transfiere los paquetes UDP. Si este campo es 255.255.255.255, se transfieren los paquetes UDP de todas las interfaces. Los siguientes rangos de direcciones 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]): número de identificación del puerto de destino UDP de los paquetes UDP que se van a transferir. En la tabla siguiente se enumeran las asignaciones de puertos UDP.

Número de puerto UDP	Acrónimo	Aplicación
7	Echo	Echo
11	SysStat	Active User
15	NetStat	NetStat
17	Quote	Quote of the day
19	CHARGEN	Character Generator
20	FTP-data	FTP Data
21	FTP	FTP
37	Time	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who is
53	DOMAIN	Domain Name Server
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
137	NetBiosNameService	NT Server to Station Connections
138	NetBiosDatagramService	NT Server to Station Connections
139	NetBios	SessionServiceNT Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management Traps
513	who	Unix Rwho Daemon
514	syslog	System Log
525	timed	Time Daemon

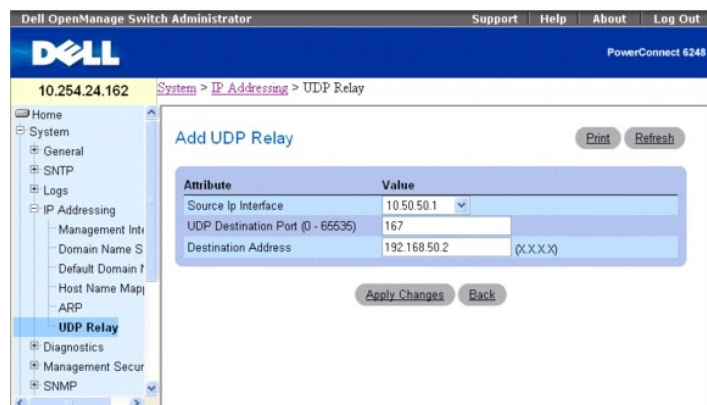
Destination Address (Dirección de destino): interfaz IP que recibe los relés de paquetes UDP. Si este campo tiene el valor 0.0.0.0, se descartan los paquetes UDP. Si el valor es 255.255.255.255, los paquetes UDP se distribuyen a todas las interfaces IP.

Remove (Eliminar): seleccione esta casilla de verificación para eliminar el relé de UDP especificado.

Adición de una entrada de relé de UDP

1. Abra la página **UDP Relay** (Relé de UDP).
2. Haga clic en **Add** (Añadir) para visualizar la página **Add UDP Relay** (Añadir relé de UDP).

Ilustración 6-31. Adición de un relé de UDP



3. Complete los campos **Source IP Interface** (Interfaz IP de origen), **UDP Destination Port** (Puerto de destino UDP) y **Destination Address** (Dirección de destino).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade el relé de UDP y se actualiza el dispositivo.

5. Haga clic en **Back** (Atrás) para volver a la página **UDP Relay** (Relé de UDP).

NOTA: si el relé de 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 servicios siguientes: 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).

Eliminación de una entrada de relé de UDP

1. Abra la página **UDP Relay** (Relé de UDP).
2. Marque la casilla de verificación **Remove** (Eliminar), situada junto al elemento que desea eliminar.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la página **UDP Relay** (Relé de UDP) y se actualiza el dispositivo.

Configuración de la información de relé de UDP mediante la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 [Comandos de direccionamiento IP](#)

Ejecución de los diagnósticos de cables

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

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

Utilice esta página para ir a la siguiente característica:

- 1 [Comprobación integrada de cables para cables de cobre](#)

Comprobación integrada de cables para cables de cobre

Utilice la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre) para realizar comprobaciones en cables de cobre. La comprobación de los cables proporciona información sobre dónde se han producido errores en el cable, la última vez que se ha realizado una prueba del cable y el tipo de error que se ha producido en el cable. Las pruebas utilizan la tecnología de reflectometría en el dominio temporal (TDR) para comprobar la calidad y las características de un cable de cobre conectado a un puerto. Pueden comprobarse cables de hasta 120 metros de longitud. La comprobación de cables se realiza cuando los puertos se encuentran inactivos, salvo la prueba de longitud aproximada del cable.

Para visualizar la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre), haga clic en **System** (Sistema)→ **Diagnostics** (Diagnósticos)→ **Integrated Cable Test** (Comprobación integrada de cables) en la vista de árbol.

Ilustración 6-32. Comprobación integrada de cables para cables de cobre



La página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre) contiene los campos siguientes:

Interface (Interfaz): interfaz a la que está conectada el cable.

Test Result (Resultado de la comprobación): resultados de la comprobación de cables. Los valores posibles son:

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

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

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

OK (Correcto): el cable ha superado la prueba.

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

Cable Fault Distance (Distancia del error del cable): distancia respecto al puerto donde se ha producido el error del cable.

Last Update (Última actualización): última vez que se ha realizado la comprobación del puerto.

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

Realización de una comprobación de cable

1. Asegúrese de que ambos extremos del cable de cobre están conectados a un dispositivo.
2. Abra la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre).
3. Haga clic en **Run Test** (Ejecutar prueba).

Se realiza la comprobación de los cables de cobre, y los resultados se muestran en la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre).

Visualización de la tabla de resultados de la comprobación integrada de cables

1. Abra la página **Integrated Cable Test for Copper Cables** (Comprobación integrada de cables para cables de cobre).
2. Haga clic en **Show All** (Mostrar todo).
3. Seleccione la unidad que desee en el menú desplegable.

En la página web aparece la página **Integrated Cable Test Results Table** (Tabla de resultados de la comprobación integrada de cables), en la que se muestran los resultados de las comprobaciones anteriores realizadas para cada puerto en la unidad seleccionada.

Ilustración 6-33. Tabla de resultados de la comprobación integrada de cables

Interface	Test Result	Cable Fault Distance (m)	Last Update	Cable Length (m)
1/g1	Test has not been performed			
1/g2	Test has not been performed			
1/g3	Test has not been performed			
1/g4	Test has not been performed			
1/g5	Test has not been performed			
1/g6	Test has not been performed			
1/g7	Test has not been performed			
1/g8	Test has not been performed			
1/g9	Test has not been performed			
1/g10	Test has not been performed			
1/g11	Test has not been performed			

Realización de pruebas de los cables de cobre mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de diagnósticos PHY

Administración de la seguridad del dispositivo

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

Para visualizar la página **Management Security** (Seguridad de administración), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) en la vista de árbol. Utilice esta página para acceder a las funciones siguientes:

- 1 [Perfil de acceso](#)
- 1 [Perfiles de autenticación](#)
- 1 [Selección de autenticación](#)
- 1 [Administración de contraseñas](#)
- 1 [Base de datos de usuarios local](#)
- 1 [Contraseñas de línea](#)
- 1 [Contraseña de activación](#)
- 1 [Configuración de TACACS+](#)
- 1 [Configuración de RADIUS](#)
- 1 [Servidor Telnet](#)
- 1 [Deneqación de servicio](#)

Perfil de acceso

Utilice la página **Access Profile** (Perfil de acceso) para definir un perfil y reglas para acceder al dispositivo. Puede limitar el acceso a funciones de administración específicas, interfaces de entrada específicas, direcciones IP de origen o subredes IP de origen.

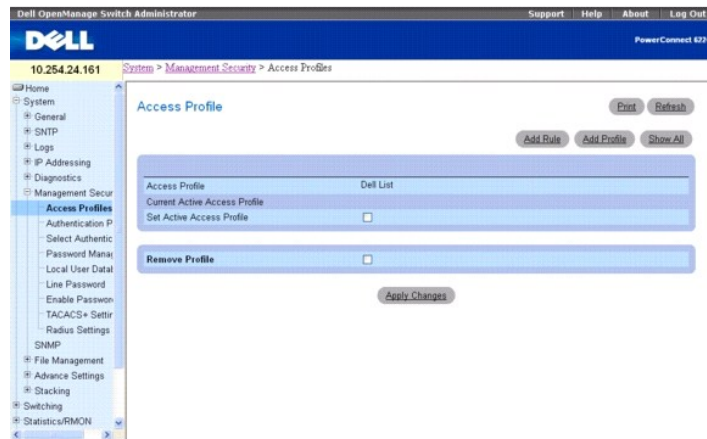
El acceso a la administración puede definirse por separado para cada tipo de método de acceso a la administración, incluidos el acceso web (HTTP), web seguro (HTTPS), Telnet, SSH y SNMP.

Las listas de acceso a la administración contienen las reglas que determinan qué usuarios pueden administrar el dispositivo y qué métodos pueden utilizar para ello. También es posible bloquear el acceso de los usuarios al dispositivo.

Utilice la página **Access Profile** (Perfil de acceso) para configurar las listas de administración y aplicarlas a interfaces específicas.

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

Ilustración 6-34. Perfil de acceso



Access Profile (Perfil de acceso): muestra el perfil de acceso.

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

Set Active Access Profile (Activar perfil de acceso): activa el perfil de acceso.

Remove Profile (Eliminar perfil): si se marca esta casilla, elimina un perfil de acceso de la lista **Access Profile** (Perfil de acceso).

NOTA: la asignación de un perfil de acceso a una interfaz implica que se deniega el acceso a través de otras interfaces. Si un perfil de acceso no está activado, todas las interfaces pueden acceder al dispositivo.

Visualización del perfil de acceso

1. Abra la página **Access Profile** (Perfil de acceso).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Profile Rules Table** (Tabla de reglas del perfil).

Ilustración 6-35. Tabla de reglas de perfil

Profile Rules Table Print Refresh

Interface	Management Method	Source IP Address	Subnet Mask	Action	Priority	Remove
1 1/g1	SNMP	132.25.39.115	255.255.255.255	PERMIT	1	<input type="checkbox"/> Edit
2 1/g12	SSH	192.168.22.15	255.255.255.255	PERMIT	3	<input type="checkbox"/> Edit

Apply Changes Back

Adición de un perfil de acceso

1. Abra la página **Access Profile** (Perfil de acceso).
2. Haga clic en **Add Profile** (Añadir perfil).

Aparece la página **Add an Access Profile** (Añadir un perfil de acceso).

Ilustración 6-36. Adición de un perfil de acceso

Add an Access Profile Print Refresh

Access Profile Name(1-32 characters)

Management Method

Interface Source IP Address Network Mask Prefix Length (0-32)

Action

Rule Priority (1-64)

Apply Changes Back

3. Escriba el nombre del perfil en el cuadro de texto **Access Profile Name** (Nombre de perfil de acceso).
4. Complete los campos:

Management Method (Método de administración): seleccione un método en el cuadro desplegable. La administración elegida restringirá la política.

Interface (Interfaz): marque esta casilla de verificación si la política debe tener una regla basada en la interfaz. La interfaz puede ser una interfaz física, un LAG o una VLAN.

Source IP Address (Dirección IP de origen): seleccione esta casilla de verificación si la política debe tener una regla basada en la dirección IP del cliente que envía el tráfico de administración. Rellene la dirección IP de origen y los detalles de la máscara en los campos proporcionados. Tenga en cuenta que la máscara puede especificarse en dos formatos distintos: en formato ip con puntos (por ejemplo, 255.255.255.0) o longitud de prefijo (por ejemplo, 32).

Action (Acción): elija la acción que debe realizarse cuando las reglas seleccionadas anteriormente coincidan. Utilice el cuadro desplegable y elija Permit (Permitir) o Deny (Denegar) para permitir o denegar el acceso.

Rule Priority (Prioridad de las reglas): permite configurar las prioridades de las reglas. Las reglas se validan al recibir la petición de administración según el orden ascendente de sus prioridades. Si una regla coincide, se realiza una acción y se ignoran las reglas anteriores. Por ejemplo, si configura la dirección IP de origen 10.10.10.10 con prioridad 1 en Permit (Permitir) y la dirección IP de origen 10.10.10.10 con prioridad 2 en Deny (Denegar), se permitirá el acceso si el perfil está activo y se ignorará la segunda regla.

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

Se añade el nuevo perfil de acceso y se actualiza el dispositivo.

Activación de un perfil de acceso

1. Abra la página **Access Profile** (Perfil de acceso).
2. Marque la casilla **Set Access Profile Active** (Activar perfil de acceso).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se activa el perfil de acceso del dispositivo.

Adición de reglas a un perfil de acceso

1. Abra la página **Access Profile** (Perfil de acceso).

El campo **Access Profile** (Perfil de acceso) muestra el perfil al que se añaden reglas cuando aparece la página **Add An Access Profile Rule** (Añadir regla de perfil de acceso).

2. Haga clic en **Add Rule** (Añadir regla).

Aparece la página **Add An Access Profile Rule** (Añadir regla de perfil de acceso).

Ilustración 6-37. Adición de una regla de perfil de acceso

The screenshot shows the 'Add an Access Profile Rule' configuration page. At the top, there are 'Exit' and 'Submit' buttons. Below is a form with the following fields and values:

- Access Profile Name:** No Profile Exists
- Management Method:** NONE
- Interface:** Interface. Sub-fields: Line: Port, LAG: 0/1/2, VLAN: 1
- Source IP Address:** Source IP Address. Sub-fields: Network Mask: (X.X.X), Prefix Length (0-32): (X.X.X)
- Action:** Permit
- Rule Priority (1-64):** 0

At the bottom of the form are 'Apply Changes' and 'Back' buttons.

3. Complete los campos del cuadro de diálogo:

Management Method (Método de administración): seleccione un método en el cuadro desplegable. La administración elegida restringirá la política.

Interface (Interfaz): marque esta casilla de verificación si la política debe tener una regla basada en la interfaz. La interfaz puede ser una interfaz física, un LAG o una VLAN.

Source IP Address (Dirección IP de origen): seleccione esta casilla de verificación si la política debe tener una regla basada en la dirección IP del cliente que origina el tráfico de administración. Rellene la dirección IP de origen y los detalles de la máscara en los cuadros de texto proporcionados. Tenga en cuenta que la máscara puede especificarse en dos formatos distintos: en formato ip con puntos (por ejemplo, 255.255.255.0) o longitud de prefijo (por ejemplo, 32).

Action (Acción): elija la acción que debe realizarse cuando las reglas seleccionadas anteriormente coincidan. Utilice el cuadro desplegable y elija Permit (Permitir) o Deny (Denegar) para permitir o denegar el acceso.

Rule Priority (Prioridad de las reglas): permite configurar las prioridades de las reglas. Las reglas se validan al recibir la petición de administración según el orden ascendente de sus prioridades. Si una regla coincide, se realiza una acción y se ignoran las reglas anteriores. Por ejemplo, si configura la dirección IP de origen 10.10.10.10 con prioridad 1 en Permit (Permitir) y la dirección IP de origen 10.10.10.10 con prioridad 2 en Deny (Denegar), se permitirá el acceso si el perfil está activo y se ignorará la segunda regla.

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

Se añade la regla al perfil de acceso y se actualiza el dispositivo.

Eliminación de una regla

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

Se elimina la regla y se actualiza el dispositivo.

Definición de perfiles de acceso mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

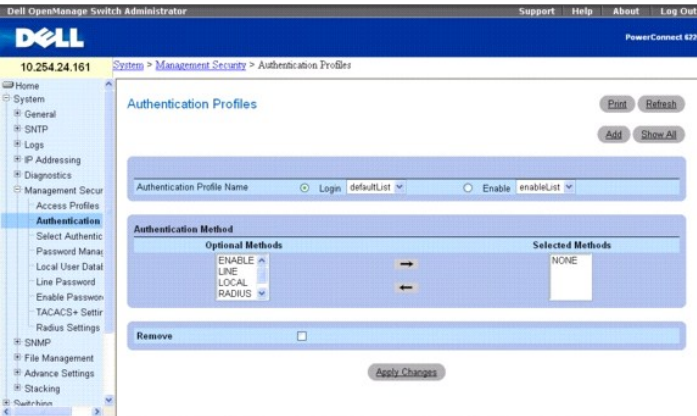
- 1 Comandos de la ACL de administración

Perfiles de autenticación

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

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

Ilustración 6-38. Perfiles de autenticación



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

Nombre de perfil de autenticación

Muestra listas a las que se añaden perfiles de autenticación definidos por el usuario. Utilice los botones de radio para que el perfil de autenticación se aplique a la parte **Login** (Inicio de sesión) o **Enable** (Activar) de las operaciones del conmutador y para seleccionar una de las dos listas disponibles:

Login (Inicio de sesión): permite iniciar una sesión en el conmutador. Las opciones son **defaultList**, **networkList** y cualquier perfil de autenticación de inicio de sesión definido por el usuario.

Enable (Activar): activa el modo de privilegio.

Authentication Method (Método de autenticación)

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

None (Ninguna): no se realiza autenticación del usuario.

Local: la autenticación del usuario se lleva a cabo en el nivel de dispositivo; el dispositivo comprueba el nombre de usuario y la contraseña para la autenticación.

RADIUS: la autenticación del usuario se lleva a cabo en el servidor RADIUS. Para obtener más información sobre los servidores RADIUS, consulte "[Configuración de RADIUS](#)".

TACACS+: la autenticación del usuario se lleva a cabo en el servidor TACACS+. Para obtener más información sobre los servidores TACACS+, consulte "[Configuración de TACACS+](#)".

Line (Línea): indica que se utiliza la contraseña de línea para la autenticación del usuario.

Enable (Activación): indica que se utiliza la contraseña de activación para la autenticación.

NOTA: la autenticación del usuario se lleva a cabo siguiendo el orden de selección de los métodos. Cuando ocurre un error durante la autenticación, se utiliza el siguiente método seleccionado. Por ejemplo, si se selecciona primero la opción **Local** y, después, **RADIUS**, el usuario se autentica primero localmente y después a través de un servidor **RADIUS** externo.

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

Remove (Eliminar): elimina el perfil seleccionado.

Adición de un perfil de autenticación

1. Abra la página **Authentication Profiles** (Perfiles de autenticación).
2. Haga clic en **Add** (Añadir) para visualizar la página **Add Authentication Profile** (Añadir perfil de autenticación).

Ilustración 6-39. Adición del perfil de autenticación

3. Escriba un nombre de perfil de entre 1 y 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 crea un perfil. Puede activar un perfil de autenticación en la página web que se visualiza al hacer clic en **System** (Sistema)→ **Management Security** (Seguridad de administración)→ **Select Authentication** (Seleccionar autenticación).

Modificación de perfiles 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 uno o más métodos en el campo **Optional Methods** (Métodos opcionales) utilizando las flechas.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se actualiza el perfil de autenticación del usuario en el dispositivo.

Eliminación de una entrada de perfiles de autenticación

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

Se abre la página **Authentication Profiles Table** (Tabla de perfiles de autenticación).

Ilustración 6-40. Tabla de perfiles de autenticación

Login Authentication Profiles			
Methods	Remove		
1	defaultList	NONE,LINE	<input type="checkbox"/> Edit

Enable Authentication Profiles			
Methods	Remove		
1	enableList	NONE	<input type="checkbox"/> Edit
2	R&D	LINE,NONE	<input type="checkbox"/> Edit

3. Marque la casilla de verificación **Remove** (Eliminar), situada junto al perfil que desea eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

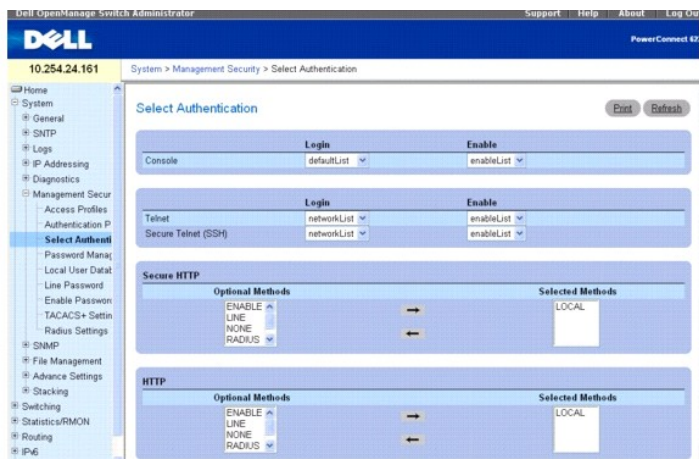
- 1 Comandos AAA

Selección de autenticación

Una vez definidos los perfiles de autenticación, puede aplicarlos a los métodos de acceso de administración. Por ejemplo, los usuarios de la consola se pueden autenticar mediante la lista de perfiles de autenticación 1, mientras que los usuarios de Telnet se autentican mediante la lista de autenticación 2.

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

Ilustración 6-41. Selección de autenticación



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

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

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

Secure Telnet (SSH) (Telnet seguro [SSH]): muestra los perfiles de autenticación utilizados para autenticar a los usuarios de Secure Shell (SSH). SSH permite a los clientes conectarse remotamente a un dispositivo de forma segura y con cifrado.

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

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

Local: la autenticación se lleva a cabo de forma local.

RADIUS: la autenticación se lleva a cabo en el servidor RADIUS.

TACACS+: la autenticación se lleva a cabo en el servidor TACACS+.

Local, None (Local, Ninguno): la autenticación se lleva a cabo primero de forma local.

RADIUS, None (RADIUS, Ninguno): la autenticación se lleva a cabo primero en el servidor RADIUS. Si la autenticación no se puede verificar, no se utilizará ningún método de autenticación. La autenticación no se podrá verificar si no es posible contactar con el servidor remoto para verificar el usuario. Si es posible contactar con el servidor remoto, la respuesta del servidor remoto se respetará siempre.

TACACS+, None (TACACS+, Ninguno): la autenticación se lleva a cabo primero en el servidor TACACS+. Si la autenticación no se puede verificar, no se utilizará ningún método de autenticación. La autenticación no se podrá verificar si no es posible contactar con el servidor remoto para verificar el usuario. Si es posible contactar con el servidor remoto, la respuesta del servidor remoto se respetará siempre.

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

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

RADIUS, Local: la autenticación se lleva a cabo primero en el servidor RADIUS. Si la autenticación no se puede verificar en el servidor RADIUS, la sesión se autentica localmente. Si la sesión no se puede autenticar localmente, se bloquea la sesión.

TACACS+, Local: la autenticación se lleva a cabo primero en el servidor TACACS+. Si la autenticación no se puede verificar en el servidor TACACS+, la sesión se autentica localmente. Si la sesión no se puede autenticar localmente, se bloquea la sesión.

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

RADIUS, Local, None (RADIUS, Local, Ninguno): la autenticación se lleva a cabo primero en el servidor RADIUS. Si la autenticación no se puede verificar en el servidor RADIUS, la sesión se autentica localmente. Si la sesión no se puede autenticar localmente, se permite la sesión.

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

TACACS+, Local, None (TACACS+, Local, Ninguno): la autenticación se lleva a cabo primero en el servidor TACACS+. Si la autenticación no se puede verificar en el servidor TACACS+, la sesión se autentica localmente. Si la sesión no se puede autenticar localmente, se permite la sesión.

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 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 Telnet seguro (SSH)

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

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

Asignación de una secuencia de autenticación a sesiones HTTP

1. Abra la página **Select Authentication** (Seleccionar autenticación).
2. En **HTTP**, seleccione un método de autenticación en el campo **Optional Methods** (Métodos opcionales) y haga clic en el botón de flecha derecha.
El método de autenticación seleccionado se desplaza al campo **Selected Methods** (Métodos seleccionados).
3. Repita este paso hasta que la secuencia de autenticación que desea se visualice en el campo **Selected Methods** (Métodos seleccionados).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La secuencia de autenticación se asigna a las sesiones HTTP.

Asignación de métodos de acceso, perfiles de autenticación o secuencias mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos AAA

Asignación de una secuencia de autenticación a sesiones HTTP seguro

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 flecha derecha.
El método de autenticación seleccionado se desplaza al campo **Selected Methods** (Métodos seleccionados).
3. Repita este paso hasta que la secuencia de autenticación que desea se visualice en el campo **Selected Methods** (Métodos seleccionados).

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

La secuencia de autenticación se asigna a las sesiones HTTP seguro.

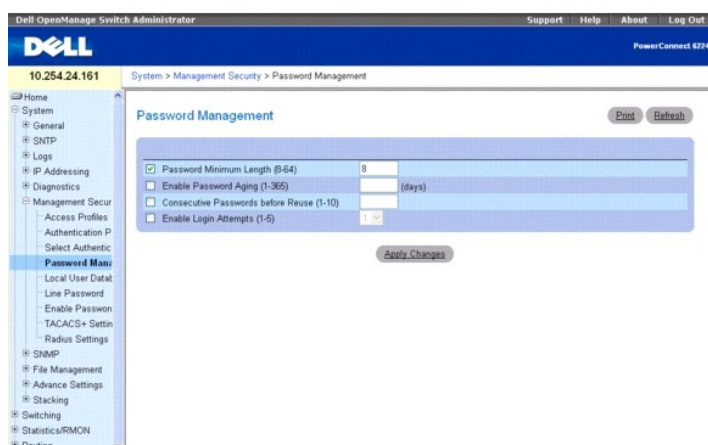
Administración de contraseñas

La administración de contraseñas aumenta la seguridad en la red y mejora el control de las contraseñas. Las contraseñas para el acceso SSH, Telnet, HTTP, HTTPS y SNMP tienen funciones de seguridad asignadas, entre ellas:

- 1 Definición de longitudes mínimas de contraseñas
- 1 Caducidad de contraseñas
- 1 Prevención de reutilización frecuente de contraseñas
- 1 Bloqueo de los usuarios tras intentos de inicio de sesión incorrectos

Para visualizar la página **Password Management** (Administración de contraseñas), haga clic en **System** (Sistema)→ **Management Security** (Seguridad de administración)→ **Password Management** (Administración de contraseñas) en la vista de árbol.

Ilustración 6-42. Administración de contraseñas




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

Password Minimum Length (8-64) (Longitud mínima de contraseña [8-64]): si se marca esta casilla, indica la longitud mínima de la contraseña. Por ejemplo, el administrador puede definir que todas las contraseñas de línea tengan al menos 10 caracteres.

Enable Password Aging (1-365) (Caducidad de contraseña de activación [1-365]): si se marca esta casilla, indica el tiempo que debe transcurrir para que caduque la contraseña. El valor del campo es de 1 a 365 días. La opción de caducidad de contraseña sólo funciona si el reloj del computador está sincronizado con un servidor SNTP. Para obtener información adicional, consulte la sección relativa a los comandos del reloj en la Guía de referencia de la CLI.

Consecutive Passwords before Reuse (1-10) (Contraseñas consecutivas antes de reutilización [1-10]): indica el número de veces que debe cambiarse una contraseña antes de poder volver a utilizarla. Los valores del campo posibles van del 1 al 10.

 **NOTA:** el usuario recibe una notificación para cambiar la contraseña antes de que caduque. Los usuarios web no reciben esta notificación.

Enable Login Attempts (1-5) (Activar intentos de inicio de sesión [1-5]): si se selecciona esta casilla, bloquea el acceso de un usuario al dispositivo cuando se ha utilizado una contraseña incorrecta un número de veces definido. Por ejemplo, si el número de intentos de inicio de sesión se ha definido como cinco y el usuario intenta iniciar sesión cinco veces con una contraseña incorrecta, el dispositivo bloquea el acceso del usuario al realizar el sexto intento. Si esto ocurre, un superusuario debe volver a activar la cuenta del usuario. El intervalo de valores de este campo es de 1 a 5 intentos.

Definición de limitaciones de contraseña

1. Abra la página **Password Management** (Administración de contraseñas).
2. Defina los campos pertinentes.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen las limitaciones de contraseña y se actualiza el dispositivo.

Definición de limitaciones de contraseña mediante los comandos de la CLI

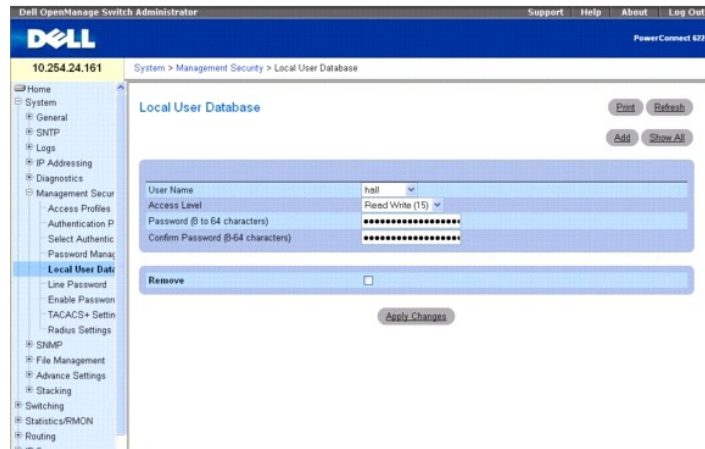
Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

Base de datos de usuarios local

Utilice la página **Local User Database** (Base de datos de usuarios local) para definir contraseñas, derechos de acceso para los usuarios, y para reactivar a los usuarios cuyas cuentas se han suspendido.

Para visualizar la página **Local User Database** (Base de datos de usuarios local), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) → **Local User Database** (Base de datos de usuarios local) en la vista de árbol.

Ilustración 6-43. Base de datos de usuarios local



La página **Local User Database** (Base de datos de usuarios local) contiene los campos siguientes:

User Name (Nombre de usuario): contiene una lista de usuarios.

Access Level (Nivel de acceso): nivel de acceso de los usuarios. El nivel de acceso más bajo es **1** (sólo lectura) y el más alto es **15** (lectura y escritura). Para suspender el acceso de un usuario, establezca el nivel en **0** (sólo un usuario de nivel 15 tiene esta capacidad).

Password (8–64 Characters) (Contraseña [8–64 caracteres]): contraseña definida por el usuario.

Confirm Password (Confirmar contraseña): confirma la contraseña definida por el usuario.

Remove (Eliminar): si se selecciona esta casilla, elimina usuarios de la base de datos de usuarios local.

Asignación de derechos de acceso a un usuario

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Seleccione un usuario en el campo **User Name** (Nombre de usuario).
3. Defina los campos necesarios.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los derechos de acceso y las contraseñas del usuario y se actualiza el dispositivo.

Adición de un usuario a la base de datos de usuarios local

1. Abra la página **Local User Database** (Base de datos de usuarios local).
2. Haga clic en **Add** (Añadir) para visualizar la página **Add User** (Añadir usuario).
Aparece la página **Add a New User** (Añadir nuevo usuario).


Ilustración 6-44. Adición de un nuevo usuario

Add a New User Print Refresh

Attribute	Value
User Name (1 to 20 characters)	<input type="text"/>
Access Level	Read/Write (1) ▾
Password (8 to 64 characters)	*****
Confirm Password (8-64 characters)	*****

Apply Changes Back

- Complete los campos.
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se define el nuevo usuario y se actualiza el dispositivo.

 **NOTA:** puede definir hasta ocho usuarios locales en el dispositivo.

Visualización de usuarios en la base de datos de usuarios local

- Abra la página **Local User Database** (Base de datos de usuarios local).
 - Haga clic en **Show All** (Mostrar todo) para visualizar la página **Local User Table** (Tabla de usuarios locales).
- Se visualizan todos los miembros de la base de datos de usuarios local.

Ilustración 6-45. Tabla de usuarios locales

Local User Table Print Refresh

	User Name	Access Level	Remove
1	amycover	Read Write	<input type="checkbox"/> Edit
2	hopkiser	Read Write	<input type="checkbox"/> Edit
3	hal	Read Write	<input type="checkbox"/> Edit

Apply Changes Back

Eliminación de usuarios de la base de datos de usuarios local

- Abra la página **Local User Database** (Base de datos de usuarios local).
 - Haga clic en **Show All** (Mostrar todo) para visualizar la página **Local User Table** (Tabla de usuarios locales).
 - Seleccione un nombre de usuario.
 - Marque **Remove** (Eliminar).
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se elimina el usuario y se actualiza el dispositivo.

Asignación de usuarios mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

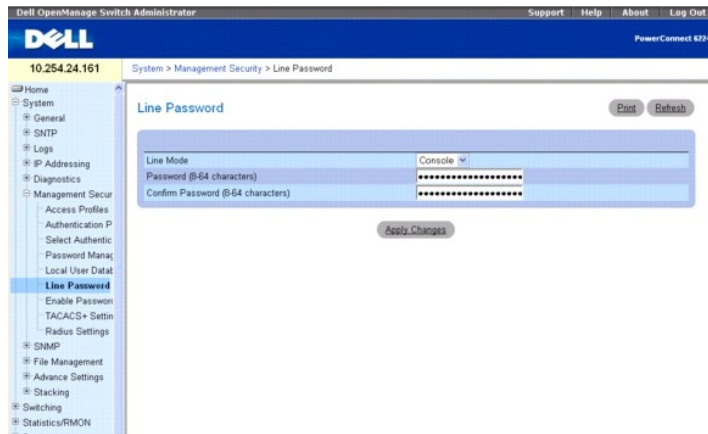
- 1 Comandos AAA

Contraseñas de línea

Utilice la página **Line Password** (Contraseña de línea) para definir contraseñas de línea para los métodos de administración.

Para visualizar la página **Line Password** (Contraseña de línea), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) → **Line Password** (Contraseña de línea) en la vista de árbol.

Ilustración 6-46. Contraseña de línea



La página **Line Password** (Contraseña de línea) contiene los campos siguientes:

Line Mode (Modo de línea): en el menú desplegable se especifica el acceso al dispositivo a través de una sesión de consola, Telnet o Telnet seguro (SSH).

Line Password (8 – 64 characters) (Contraseña de línea [8–64 caracteres]): indica la contraseña de línea para acceder al dispositivo a través de una sesión de consola, Telnet o Telnet seguro. La contraseña se muestra con el formato *****.

Confirm Password (8 – 64 characters) (Confirmar contraseña [8–64 caracteres]): confirma la nueva contraseña de línea. La contraseña se muestra con el formato *****.

Definición de contraseñas de línea

1. Abra la página **Line Password** (Contraseña de línea).
2. Seleccione el acceso al dispositivo a través de una sesión de consola, Telnet o Telnet seguro (SSH).
3. Defina el campo **Line Password** (Contraseña de línea) para el tipo de sesión que utiliza para conectarse al dispositivo.
4. Confirme la contraseña de línea.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la contraseña de línea para el tipo de sesión y se actualiza el dispositivo.

Asignación de contraseñas de línea mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

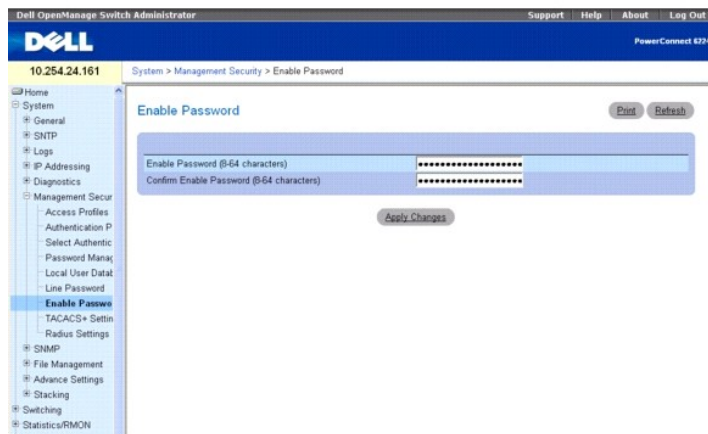
- 1 Comandos AAA

Contraseña de activación

Utilice la página **Enable Password** (Contraseña de activación) para establecer una contraseña local para controlar el acceso a los niveles normal y de privilegio.

Para visualizar la página **Enable Password** (Contraseña de activación), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) → **Enable Password** (Contraseña de activación) en la vista de árbol.

Ilustración 6-47. Contraseña de activación



La página **Enable Password** (Contraseña de activación) contiene los campos siguientes:

Enable Password (8–64 characters) (Contraseña de activación [8–64 caracteres]): contraseña de activación para controlar el acceso a los niveles normal y de privilegio. La contraseña se muestra con el formato *****.

Confirm Enable Password (Confirmar contraseña de activación): confirma la nueva contraseña de activación. La contraseña se muestra con el formato *****.

Definición de contraseñas de activación

1. Abra la página **Enable Password** (Contraseña de activación).
2. Especifique la contraseña de activación.
3. Confirme la contraseña de activación.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se establece la contraseña de activación.

Asignación de contraseñas de activación mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos AAA

Configuración de TACACS+

El dispositivo puede ejercer de cliente del sistema de control de acceso a la controladora de acceso al terminal (TACACS+). TACACS+ proporciona una seguridad centralizada para la validación de los usuarios que acceden a un dispositivo.

TACACS+ es un sistema de administración de usuarios centralizado que, además, es compatible con RADIUS y otros procesos de autenticación. TACACS+ proporciona los servicios siguientes:

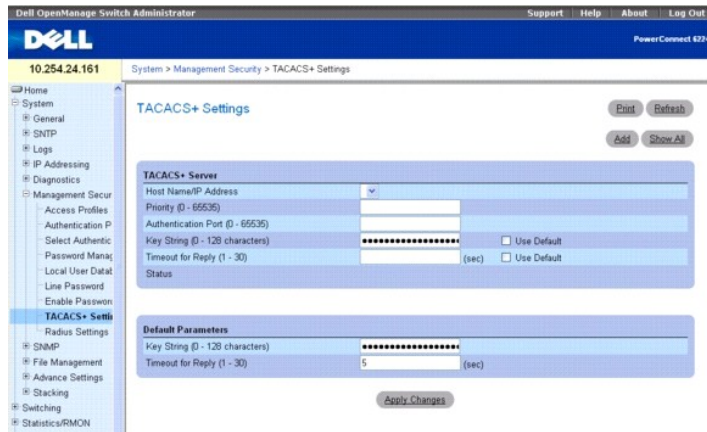
- 1 **Authentication** (Autenticación): proporciona autenticación durante el inicio de sesión y a través de nombres de usuario y contraseñas definidas por el usuario.
- 1 **Authorization** (Autorización): se lleva a cabo cuando se inicia una sesión. Una vez que se ha completado la sesión de autenticación, se inicia una sesión de autorización mediante el nombre de usuario autenticado. El servidor TACACS+ comprueba los privilegios de usuario.

El protocolo TACACS+ asegura la seguridad de la red por medio de intercambios de protocolo cifrados entre el dispositivo y el servidor TACACS+.

La página **TACACS+ Settings** (Configuración de TACACS+) contiene la configuración definida por el usuario y la configuración de TACACS+ predeterminada para el puerto de administración en banda.

Para visualizar la página **TACACS+ Settings** (Configuración de TACACS+), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) → **TACACS+** en la vista de árbol.

Ilustración 6-48. Configuración de TACACS+



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

Host Name / IP Address (Nombre de host/dirección IP): especifica el servidor TACACS+.

Priority (0-65535) (Prioridad [0-65535]): especifica el orden en el que se utilizan los servidores TACACS+. El valor predeterminado es 0.

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

Key String (0-128 Characters) (Cadena de clave [0-128 caracteres]): define la clave de autenticación y de cifrado para las comunicaciones TACACS+ entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con el cifrado utilizado en el servidor TACACS+. Marque la casilla **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 que transcurre antes de que se agote el tiempo de espera de la conexión entre el dispositivo y el servidor TACACS+. El intervalo de valores de este campo es de 1 a 30 segundos. Marque la casilla **Use Default** (Utilizar valor predeterminado) para seleccionar el valor predeterminado de fábrica.

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

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

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

Los campos de la sección **Default Parameters** (Parámetros predeterminados) de la página contienen valores que se aplican automáticamente a nuevos servidores TACACS+.

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

Timeout for Reply (1-30) (Tiempo de espera para respuesta [1-30]): introduzca el tiempo de configuración de usuario global que transcurre antes de que se agote el tiempo de espera de la conexión entre el dispositivo y el servidor TACACS+.

Definición de parámetros de TACACS+

1. Abra la página **TACACS+ Settings** (Configuración de TACACS+).
2. Defina los campos necesarios.
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** (Añadir).

Aparece la página **Add TACACS+ Host** (Añadir host TACACS+).

Ilustración 6-49. Adición de host TACACS+

Add TACACS+ Host Print Refresh

Host Name/IP Address	10.240.13.45	(XXX.X)
Priority (0 - 65536)	258	
Authentication Port (0 - 65536)	43	
Key String (0 - 128 characters)	*****	<input type="checkbox"/> Use Default
Timeout for Reply (1 - 30)	5	<input type="checkbox"/> Use Default

Apply Changes Back

- Defina los campos necesarios.
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se añade el servidor TACACS+ y se actualiza el dispositivo.

Visualización de una lista de servidores TACACS+

- Abra la página TACACS+ Settings (Configuración de TACACS+).
 - Haga clic en **Show All** (Mostrar todo).
- Se abre la página TACACS+ Servers Table (Tabla de servidores TACACS+).

Ilustración 6-50. Tabla de servidores TACACS+

TACACS+ Servers Table Print Refresh

Host IP Address	Priority	Authentication Port	Timeout For Reply (sec)	Status	Remove
10.240.13.45	258	43	5	Not Connected	<input type="checkbox"/> Edit

Apply Changes Back

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

- Abra la página TACACS+ Settings (Configuración de TACACS+).
 - Haga clic en **Show All** (Mostrar todo).
- Se abre la página TACACS+ Servers Table (Tabla de servidores TACACS+).
- Seleccione una entrada de la tabla de servidores TACACS+.
 - Seleccione la casilla de verificación **Remove** (Eliminar).
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se elimina el servidor TACACS+ y se actualiza el dispositivo.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos TACACS+

Configuración de RADIUS

Los servidores RADIUS (servicio de usuario de acceso telefónico de autenticación remota) proporcionan una seguridad adicional para las redes. Un servidor RADIUS mantiene una base de datos de usuarios que contiene información de autenticación para cada usuario. Los servidores RADIUS proporcionan un método de autenticación centralizado para:

- 1 Acceso Telnet
- 1 Acceso web
- 1 Acceso de consola a conmutador
- 1 Puerto de control de acceso (802.1x)

La página **RADIUS Settings** (Configuración de RADIUS) contiene la configuración definida por el usuario y la configuración de RADIUS predeterminada.

Para visualizar la página **RADIUS Settings** (Configuración de RADIUS), haga clic en **System** (Sistema) → **Management Security** (Seguridad de administración) → **RADIUS Settings** (Configuración de RADIUS) en la vista de árbol.

Ilustración 6-51. Configuración de RADIUS

RADIUS Server	
IP Address	10.24.100.18
Priority (0-65535)	256
Authentication Port (0-65535)	1043
Number of Retries (1-10)	4 <input type="checkbox"/> Use Default
Timeout for Reply (1-30)	20 (sec) <input type="checkbox"/> Use Default
Deadtime (0-2000)	500 (min) <input type="checkbox"/> Use Default
Key String (0-128 characters)	drowyeh <input type="checkbox"/> Use Default
Source IP Address	10.240.1.87 (XXXXX) <input type="checkbox"/> Use Default
Usage Type	Login

Default Parameters	
Default Retries (1-10)	3
Default Timeout for Reply (1-30)	20 (sec) <input type="checkbox"/> Use Default
Default Deadtime (0-2000)	1000 (min) <input type="checkbox"/> Use Default
Default Key String (0-128 characters)	key <input type="checkbox"/> Use Default
Source IP Address	202.241.43 (XXXXX)

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

IP Address (Dirección IP): dirección IP del servidor RADIUS.

Priority (0–65535) (Prioridad [0–65535]): indica la prioridad del puerto. Los valores posibles van del 0 al 65535.

Authentication Port (0–65535) (Puerto de autenticación [0–65535]): identifica el puerto de autenticación que se utiliza para verificar la autenticación del servidor RADIUS.

Number of Retries (1–10) (Número de reintentos [1–10]): número de peticiones transmitidas enviadas al servidor RADIUS antes de que se produzca un error. Los posibles valores de este campo están comprendidos entre 1 y 10. El valor predeterminado es 3. Si no se especifica ningún valor específico de host, se aplica el valor global a cada host. Marque la casilla **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado definido por el usuario.


Timeout for Reply (1–30) (Tiempo de espera para respuesta [1–30]): tiempo, en segundos, durante el que el dispositivo espera una respuesta del servidor RADIUS antes de que se agote el tiempo de espera. Los posibles valores de este campo están comprendidos entre 1 y 30. El valor predeterminado es 3. Si no se especifica ningún valor específico de host, se aplica el valor global a cada host. Marque la casilla **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado definido por el usuario.

Deadtime (0–2000) (Tiempo muerto [0–2000]): tiempo, en minutos, durante el que no se envían peticiones de servicio al servidor RADIUS. El intervalo de valores es de 0 a 2000. Si no se especifica ningún valor específico de host, se aplica el valor global a cada host. Marque la casilla **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado definido por el usuario.

Key String (0–128 Characters) (Cadena de clave [0–128 caracteres]): cadena de clave utilizada para la autenticación y el cifrado de todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con el cifrado de RADIUS. Si no se especifica ningún valor específico de host, se aplica el valor global a cada host. Marque la casilla **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado definido por el usuario.

Source IP Address (Dirección IP de origen): dirección IP del dispositivo que accede al servidor RADIUS. Marque la casilla **Use Default** (Utilizar valor predeterminado) para utilizar el valor predeterminado definido por el usuario.

Usage Type (Tipo de uso): cuadro desplegable que se utiliza para seleccionar el tipo de uso del 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 enviadas al servidor RADIUS antes de que se produzca un error.

Default Timeout for Reply (1–30) (Tiempo de espera predeterminado para respuesta [1–30]): tiempo predeterminado, en segundos, durante el que el dispositivo espera una respuesta del servidor RADIUS antes de que se agote el tiempo de espera. Los valores del campo posibles van del 1 al 30.

Default Deadtime (0–2000) (Tiempo muerto predeterminado [0–2000]): especifica el tiempo predeterminado, en minutos, durante el que no se envían peticiones de servicio al servidor RADIUS. El intervalo de valores va de 0 a 2000.

Default Key String (0–128 characters) (Cadena de clave predeterminada [0–128 caracteres]): cadena de clave predeterminada utilizada para la autenticación y el cifrado de todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con el cifrado de 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).

- Haga clic en **Add** (Añadir).

Aparece la página **Add RADIUS Server** (Añadir servidor RADIUS).

Ilustración 6-52. Adición de un servidor RADIUS

Form fields and options:

- IP Address: [] (XXXX)
- Priority (0 - 65535): []
- Authentication Port (0 - 65535): []
- Number of Retries (1 - 10): [] Use Default
- Timeout for Reply (1 - 30): [] (sec) Use Default
- Deadtime (0 - 2000): [] (min) Use Default
- Key String (0 - 128 characters): [] (alphanumeric) Use Default
- Source IP Address: [] Use Default
- Usage Type: ALL

- Defina los campos del diálogo.
- Haga clic en **Apply Changes** (Aplicar cambios).

Se añade el nuevo servidor RADIUS y se actualiza el dispositivo.

Definición de los parámetros de RADIUS

- Abra la página **RADIUS Settings** (Configuración de RADIUS).
- Defina los campos del diálogo.
- Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de RADIUS se actualiza en el dispositivo.

Modificación de la configuración del servidor RADIUS

- Abra la página **RADIUS Settings** (Configuración de RADIUS).
- Haga clic en **Show All** (Mostrar todo).

Aparece la página **RADIUS Servers Table** (Tabla de servidores RADIUS).

Ilustración 6-53. Tabla de servidores RADIUS

	IP Address	Priority	Authentication Port	Number of Retries	Timeout For Reply (sec)	Deadtime (min)	Source IP Address	Usage Type	Remove
1	10.240.10.13	2	23	45	56	3	10.240.13.45	Login	Edit
2	10.240.10.40	4	25	34	53	2	10.240.13.15	Login	Edit
3	10.240.10.14	2	23	43	57	1	10.240.13.45	Login	Edit

- Haga clic en el enlace **Edit** (Editar) de la entrada seleccionada.
- En la página **RADIUS Settings** (Configuración de RADIUS), cambie la configuración del servidor RADIUS.
- Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración del servidor RADIUS y se actualiza el dispositivo.

Eliminación de un servidor RADIUS de la lista de servidores RADIUS

- Abra la página **RADIUS Settings** (Configuración de RADIUS).
- Haga clic en **Show All** (Mostrar todo).

Aparece la página **RADIUS Servers Table** (Tabla de servidores RADIUS).

3. Seleccione un servidor RADIUS y marque **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor RADIUS se elimina de la lista.

Definición de servidores RADIUS mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

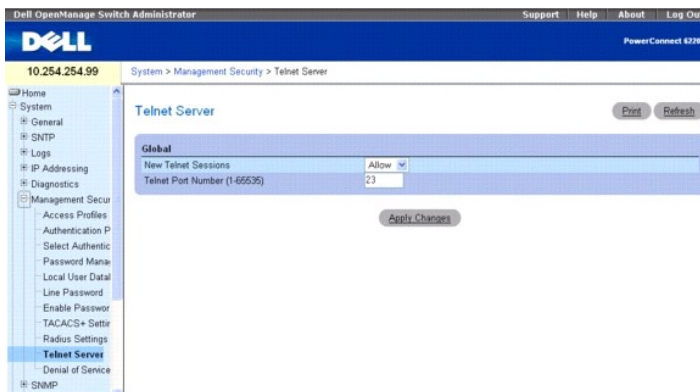
- 1 Comandos Radius

Servidor Telnet

Utilice la página **Telnet Server** (Servidor Telnet) para activar o desactivar el servicio Telnet en el conmutador o para modificar el puerto Telnet.

Para visualizar la página **Telnet Server** (Servidor Telnet), haga clic en **System** (Sistema)→ **Management Security** (Seguridad de administración)→ **Telnet Server** (Servidor Telnet).

Ilustración 6-54. Servidor Telnet



La página **Telnet Server** (Servidor Telnet) contiene los campos siguientes:

New Telnet Sessions (Nuevas sesiones Telnet): controla el modo de administración de las sesiones Telnet de entrada. Si define el modo como **Block** (Bloquear), no se permiten nuevas sesiones Telnet, pero no se interrumpen las sesiones existentes. El valor predeterminado es **Allow** (Permitir).

Telnet Port Number (Número de puerto Telnet): número de puerto en el que puede iniciarse la sesión Telnet. Este puerto se utilizará para las nuevas sesiones Telnet de entrada del conmutador. Tras modificar el puerto del servidor Telnet, las nuevas sesiones Telnet de entrada utilizarán el nuevo puerto y las sesiones Telnet existentes no se verán afectadas.

Modificación de la configuración del servidor Telnet

1. Abra la página **Telnet Server Configuration** (Configuración del servidor Telnet).
2. Configure los campos pertinentes.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración y se actualiza el dispositivo.

Configuración de los servidores Telnet mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

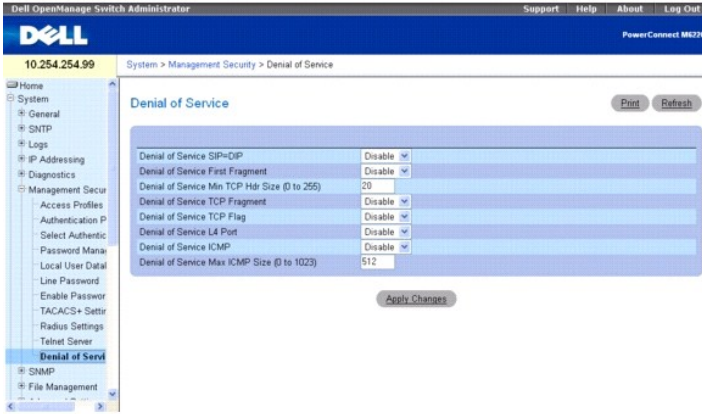
- 1 Comandos del servidor Telnet

Denegación de servicio

La denegación de servicio hace referencia a la explotación de diversas vulnerabilidades que podrían interrumpir el servicio de un host o provocar inestabilidad en la red. Utilice la página **Denial of Service** (Denegación de servicio) para definir la configuración necesaria para evitar ataques de denegación de servicio.

Para visualizar la página Denial of Service (Denegación de servicio), haga clic en **System** (Sistema)→ **Management Security** (Seguridad de administración)→ **Denial of Service** (Denegación de servicio) en la vista de árbol.

Ilustración 6-55. Denegación de servicio



La página Denial of Service (Denegación de servicio) contiene los campos siguientes:

Denial of Service SIP=DIP (Denegación de servicio, SIP=DIP): la activación de la prevención de denegación de servicio (DoS) SIP=DIP provoca que el conmutador descarte paquetes cuya dirección IP de origen coincida con la dirección IP de destino.

Denial of Service First Fragment (Denegación de servicio, First Fragment): la activación de la prevención de DoS First Fragment provoca que el conmutador descarte paquetes cuyo encabezado TCP sea menor que el tamaño del encabezado TCP mínimo configurado (Min TCP Hdr Size).

Denial of Service Min TCP Hdr Size (Denegación de servicio, Min TCP Hdr Size): permite especificar el tamaño del encabezado TCP mínimo permitido. Si se activa la prevención de DoS First Fragment, el conmutador descartará paquetes cuyo encabezado TCP sea menor que este valor configurado.

Denial of Service TCP Fragment (Denegación de servicio, TCP Fragment): la activación de la prevención de DoS TCP Fragment provoca que el conmutador descarte paquetes cuyo desplazamiento de fragmento IP sea igual a uno.

Denial of Service TCP Flag (Denegación de servicio, TCP Flag): la activación de la prevención de DoS TCP Flag provoca que el conmutador descarte paquetes que cumplan alguna de las condiciones siguientes:

- 1 Indicador SYN de TCP activado y puerto de origen TCP establecido en menos de 1024
- 1 Indicadores de control de TCP establecidos en 0 y número de secuencia de TCP establecido en 0
- 1 Indicadores FIN, URG y PSH de TCP activados y número de secuencia de TCP establecido en 0
- 1 Indicadores SYN y FIN de TCP activados

Denial of Service L4 Port (Denegación de servicio, L4 Port): la activación de la prevención de DoS L4 Port provoca que el conmutador descarte paquetes cuyo puerto de origen TCP/UDP coincida con el puerto de destino TCP/UDP.

Denial of Service ICMP (Denegación de servicio, Service ICMP): la activación de la prevención de DoS ICMP provoca que el conmutador descarte paquetes ICMP cuyo tipo se haya establecido en ECHO_REQ (ping) y cuyo tamaño sea mayor que el tamaño del paquete ICMP configurado (ICMP Pkt Size).

Denial of Service Max ICMP Pkt Size (Denegación de servicio, Max ICMP Pkt Size): permite especificar el tamaño máximo del paquete ICMP permitido. Si se activa la prevención de DoS ICMP, el conmutador descartará paquetes ping ICMP cuyo tamaño sea mayor que este valor configurado.

Configuración de los valores de denegación de servicio

1. Abra la página Denial of Service (Denegación de servicio).
2. Especifique la configuración que desea.
3. Haga clic en **Apply Changes** (Aplicar cambios).

El dispositivo se actualiza con la nueva configuración.

Configuración de los valores de denegación de servicio mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de denegación de servicio

Definición de los parámetros de SNMP

El protocolo simple de administración de red (SNMP) proporciona un método para administrar los dispositivos de una red. El dispositivo admite las versiones 1, 2 y 3 de SNMP.

NOTA: de forma predeterminada, SNMPv2 se activa automáticamente en el dispositivo. Para activar SNMPv3, debe definirse una ID de motor local para el dispositivo. La ID de motor local se establece de forma predeterminada en la dirección MAC del conmutador; sin embargo, cuando el conmutador funciona en modo de apilamiento, es importante configurar manualmente la ID de motor local para la pila. Esta ID de motor local debe definirse de forma que sea exclusiva dentro de la red. Es importante hacer esto porque la ID de motor predeterminada de una pila es la dirección MAC de la unidad maestra, que puede cambiar si se produce un error en la unidad maestra y otra unidad toma el control de la pila. Para obtener información sobre cómo configurar la ID de motor local, consulte "[Parámetros globales de SNMP](#)".

SNMPv1 y SNMPv2

El agente SNMP mantiene una lista de variables que se utilizan para administrar el dispositivo. Estas variables se definen en la *base de datos de información de administración* (MIB). La MIB presenta las variables controladas por el agente. El agente SNMP define el formato de especificación de la MIB, así como el formato utilizado para acceder a la información en la red. Los derechos de acceso del agente SNMP se controlan mediante cadenas de acceso.

SNMPv3

SNMPv3 también aplica el control de acceso y un nuevo mecanismo de excepciones para unidades PDU de SNMPv1 y SNMPv2. Además, SNMPv3 tiene definido un modelo de seguridad basado en el usuario (USM) e incluye lo siguiente:

- 1 **Autenticación:** proporciona autenticación de la integridad y el origen de los datos.
- 1 **Privacidad:** impide la divulgación del contenido del mensaje. Para el cifrado se utiliza el encadenamiento de bloques de cifrado (CBC). En un mensaje SNMP, puede activarse la autenticación o bien la autenticación y la privacidad. Sin embargo, no es posible activar la privacidad sin la autenticación.
- 1 **Determinismo temporal:** evita que se produzcan demoras en los mensajes o mensajes redundantes. El agente SNMP compara el mensaje entrante con la información de hora del mensaje.
- 1 **Administración de claves:** define la generación, las actualizaciones y la utilización de las claves.

El dispositivo admite filtros de notificación de SNMP basados en ID de objeto (OID). El sistema utiliza las OID para administrar las funciones del dispositivo. SNMPv3 admite las funciones siguientes:

- 1 Seguridad
- 1 Control de acceso a funciones
- 1 Excepciones

Las claves de autenticación o de privacidad se modifican en el modelo de seguridad basado en el usuario (USM) de SNMPv3.

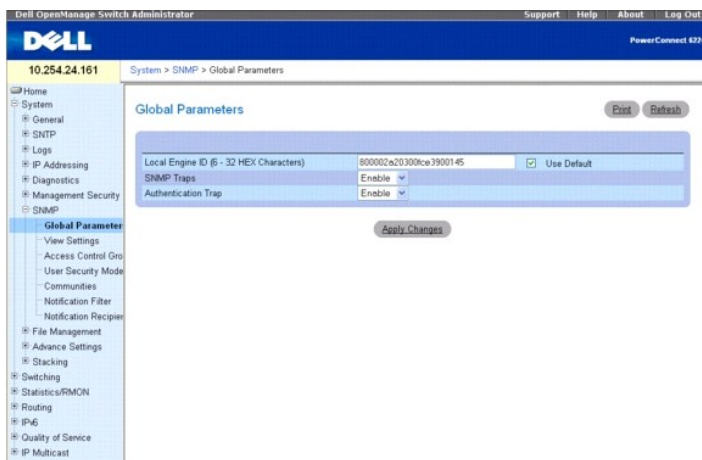
Utilice la página SNMP para definir los parámetros de SNMP. Para visualizar la página SNMP, haga clic en **System** (Sistema) → **SNMP** en la vista de árbol.

Parámetros globales de SNMP

Utilice la página **Global Parameters** (Parámetros globales) para activar las notificaciones de SNMP y de autenticación.

Para visualizar la página **Global Parameters** (Parámetros globales), haga clic en **System** (Sistema) → **SNMP** → **Global Parameters** (Parámetros globales) en la vista de árbol.

Ilustración 6-56. Parámetros globales



La página **Global Parameters** (Parámetros globales) contiene los parámetros siguientes:

Local Engine ID (6 – 32 HEX Characters) (ID de motor local [6–32 caracteres hexadecimales]): define la ID de motor de SNMP local.

Use Default (Utilizar valor predeterminado): configura el dispositivo para que utilice la ID de motor de SNMP predeterminada.

SNMP Traps (Excepciones de SNMP): activa o desactiva el envío de notificaciones de SNMP por parte del dispositivo.

Authentication Trap (Excepción de autenticación): activa o desactiva el envío de excepciones de SNMP por parte del dispositivo cuando se produce un error en la autenticación.

Definición de la ID de motor de SNMP local

1. Abra la página **Global Parameters** (Parámetros globales).
2. Escriba la ID hexadecimal que desee en el campo **Local Engine ID** (ID de motor local).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la nueva ID de motor local y se actualiza el dispositivo.

Utilización de la ID de motor de SNMP predeterminada

1. Abra la página **Global Parameters** (Parámetros globales).
2. Haga clic en la casilla de verificación **Use Default** (Utilizar valor predeterminado).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se crea la ID de motor de SNMP predeterminada, basada en la dirección MAC, y se actualiza el dispositivo.

Activación de excepciones de SNMP

1. Abra la página **Global Parameters** (Parámetros globales).
2. Seleccione **Enable** (Activar) en el campo **SNMP Traps** (Excepciones de SNMP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se activan las notificaciones de SNMP y se actualiza el dispositivo.

Activación de una excepción de autenticación

1. Abra la página **Global Parameters** (Parámetros globales).
2. Seleccione **Enable** (Activar) en el campo **Authentication trap** (Excepción de autenticación).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se activan las notificaciones de autenticación y se actualiza el dispositivo.

Activación de las notificaciones de SNMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos SNMP

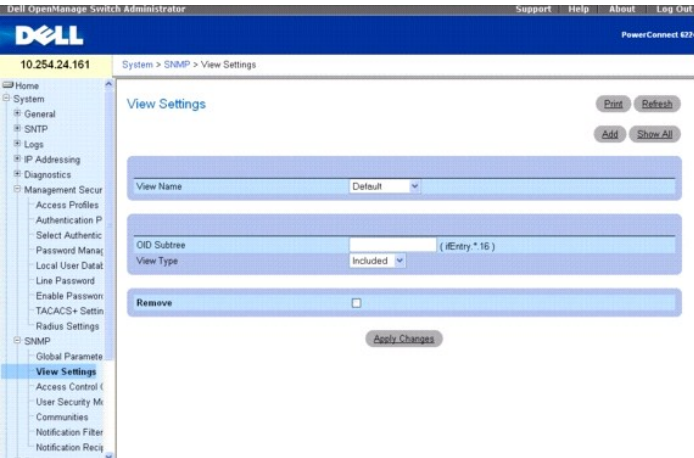
Configuración de vistas de SNMP

Utilice esta página para crear vistas en las que poder definir las funciones del dispositivo que son accesibles y las que están bloqueadas. Puede crear un vista que incluya o excluya las OID correspondientes a las interfaces.

Utilice la página **SNMP View Settings** (Configuración de vistas de SNMP) para definir las vistas de SNMP.

Para visualizar la página **SNMP View Settings** (Configuración de vistas de SNMP), haga clic en **System** (Sistema) → **SNMP** → **View Settings** (Configuración de vistas) en la vista de árbol.

Ilustración 6-57. Configuración de vistas de SNMP



La página SNMP View Settings (Configuración de vistas de SNMP) contiene los campos siguientes:

View Name (Nombre de la vista): contiene una lista de las vistas definidas por el usuario. Un nombre de vista puede contener un máximo de 30 caracteres alfanuméricos.

OID Subtree (Subárbol de OID): especifica una cadena de OID de SNMP válida que puede incluir metacaracteres como *.

View Type (Tipo de vista): especifica si las ID de objeto de la vista se incluyen o se excluyen.

Remove (Eliminar): marque esta casilla para eliminar el tipo de vista que se muestra.

Adición de una vista

1. Abra la página SNMP View Settings (Configuración de vistas de SNMP)..
2. Haga clic en **Add** (Añadir).

Aparece la página **Add View** (Añadir vista):

Ilustración 6-58. Adición de una vista



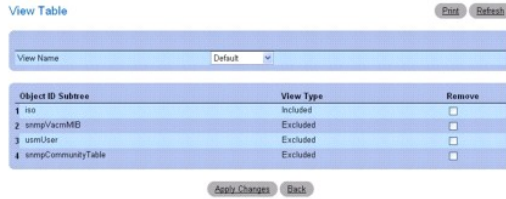
3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se añade la vista de SNMP y se actualiza el dispositivo.

Visualización de la tabla de vistas

1. Abra la página SNMP View Settings (Configuración de vistas de SNMP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **View Table** (Tabla de vistas):

Ilustración 6-59. Tabla de vistas



Eliminación de vistas de SNMP

1. Abra la página **SNMP View Settings** (Configuración de vistas de SNMP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **View Table** (Tabla de vistas).
3. Seleccione una vista de SNMP.
4. Marque la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la vista de SNMP y se actualiza el dispositivo.

Definición de vistas de SNMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

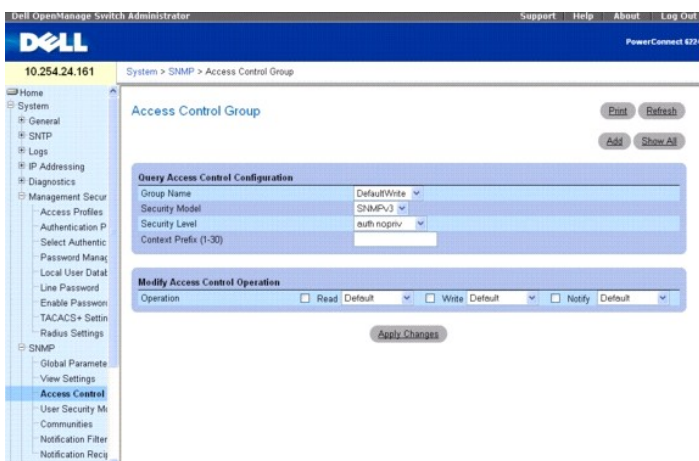
- 1 Comandos SNMP

Grupo de control de acceso

Utilice la página **Access Control Group** (Grupo de control de acceso) para ver información sobre cómo crear grupos SNMP y cómo asignar 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.

Para visualizar la página **Access Control Group** (Grupo de control de acceso), haga clic en **System** (Sistema) → **SNMP** → **Access Control** (Control de acceso) en la vista de árbol.

Ilustración 6-60. Grupo de control de acceso



La página **Access Control Group** (Grupo de control de acceso) contiene los campos siguientes:

Group Name (Nombre de grupo): contiene una lista de 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 asociada al grupo. Los valores del campo posibles son:

- SNMPv1:** el grupo tiene definida la versión SNMPv1.

SNMPv2: el grupo tiene definida la versión SNMPv2.

SNMPv3: el grupo tiene definido el modelo de seguridad basado en el usuario (USM) de SNMPv3.

Security Level (Nivel de seguridad): nivel de seguridad asociado al grupo. Los niveles de seguridad sólo se aplican a los grupos SNMPv3. Los valores del campo posibles son:

noauth nopriv: no se asigna al grupo ni el nivel de seguridad de autenticación ni el nivel de seguridad de privacidad.

auth nopriv: autentica los mensajes de SNMP sin cifrarlos.

auth priv: autentica los mensajes de SNMP y los cifra.

Context Prefix (1-30) (Prefijo de contexto [1-30]): este campo permite al usuario especificar el nombre del contexto introduciendo hasta 30 de los primeros caracteres del nombre del contexto.

Operation (Operación): define los derechos de acceso del grupo. Los valores del campo posibles son:

Read (Lectura): permite seleccionar una vista que restringe el acceso de administración a la visualización del contenido del agente. Si no hay ninguna vista seleccionada, pueden visualizarse todos los objetos excepto la tabla de comunidades y las tablas de acceso y de usuario de SNMPv3.

Write (Escritura): permite seleccionar una vista que permite el acceso de lectura/escritura de la administración al contenido del agente.

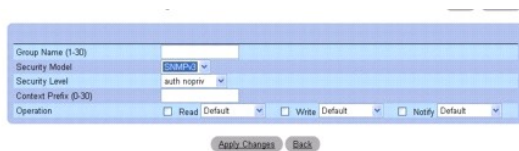
Notify (Notificar): permite seleccionar una vista que permite el envío de excepciones o informes de SNMP.

Adición de grupos SNMP

1. Abra la página **Access Control Configuration** (Configuración de control de acceso).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add an Access Control Configuration** (Añadir una configuración de control de acceso):

Ilustración 6-61. Adición de una configuración de control de acceso



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


Se añade el grupo y se actualiza el dispositivo.

Visualización de la tabla de accesos

1. Abra la página **Access Control Configuration** (Configuración de control de acceso).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Access Table** (Tabla de accesos):

Ilustración 6-62. Tabla de accesos



Group Name	Context Prefix	SNMP Version	Security Level	Read	Write	Notify	Remove
1 DefaultRead		SNMPv1	NoAuth NoPriv	Default		Default	<input type="checkbox"/>
2 DefaultRead		SNMPv2	NoAuth NoPriv	Default		Default	<input type="checkbox"/>
3 DefaultSuper		SNMPv1	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
4 DefaultSuper		SNMPv2	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
5 DefaultWrite		SNMPv1	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>
6 DefaultWrite		SNMPv2	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>

Eliminación de un grupo

1. Abra la página **Access Control Configuration** (Configuración de control de acceso).
2. Haga clic en **Show All** (Mostrar todo).
Se abre la tabla de accesos.
3. Seleccione un grupo.
4. Marque **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).
Se elimina el grupo y se actualiza el dispositivo.

Definición del control de acceso de SNMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

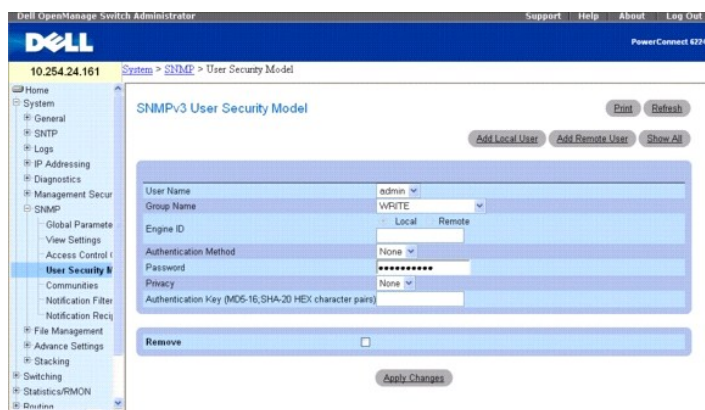
- 1 Comandos SNMP

Modelo de seguridad basado en el usuario (USM) de SNMPv3

Utilice la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3) para asignar usuarios del sistema a grupos SNMP y para definir el método de autenticación de usuarios.

Para visualizar la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3), haga clic en **System** (Sistema) → **SNMP** → **User Security Model** (Modelo de seguridad basado en el usuario) en la vista de árbol.

Ilustración 6-63. Modelo de seguridad basado en el usuario (USM) de SNMPv3



La página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3) contiene los campos siguientes:

User Name (Nombre de usuario): contiene una lista de nombres de usuario definidos por el usuario.

Group Name (Nombre de grupo): contiene una lista de grupos SNMP definidos por el usuario. Los grupos SNMP se definen en la página **Access Control Group** (Grupo de control de acceso).

Engine ID (ID de motor): permite elegir si el usuario seleccionado está asociado a un dispositivo activado SNMPv3 local o remoto especificado.

Remote Engine ID (ID de motor remoto): indica que el usuario está configurado en un dispositivo activado SNMPv3 remoto.

Authentication Method (Método de autenticación): permite especificar el método de autenticación utilizado para autenticar a los usuarios. Los valores del campo posibles son:

None (Ninguna): no se realiza autenticación del usuario.

MD5: los usuarios se autentican mediante el nivel de autenticación HMAC-MD5-96. El usuario debe especificar una contraseña.

SHA: los usuarios se autentican mediante el nivel de autenticación HMAC-SHA-96. El usuario debe introducir una contraseña.

Password (Contraseña): 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 MD5 o Contraseña SHA. La contraseña se define en la página **Add Local User** (Añadir usuario local).

Privacy (Privacidad): permite especificar si va a utilizarse la clave de autenticación. Elija uno de los valores siguientes:

None (Ninguna): no se utiliza una clave de autenticación.

des: se utiliza una contraseña con cifrado simétrico CBC-DES para la clave de autenticación.

des-key: se utiliza una clave de autenticación pregenerada HMAC-MD5-96.

Authentication Key (MD5-16; SHA-20 HEX character pairs) (Clave de autenticación [pares de caracteres hexadecimales: 16 para MD5 y 20 para SHA]): permite especificar la clave de autenticación. Una clave de autenticación sólo se define si el método de autenticación es MD5 o SHA.

Remove (Eliminar): si se marca esta casilla, se elimina el usuario especificado del grupo especificado.

Adición de usuarios locales de SNMPv3 a un grupo

1. Abra la página **SNMPv3 User Security Model** (Modelo de seguridad basado en el usuario de SNMPv3).
2. Haga clic en **Add Local User** (Añadir usuario local).

Aparece la página **Add Local User** (Añadir usuario local):

Ilustración 6-64. Adición de un usuario local

Add Local User

LocalEngineId 800002c03000e3900145

User Name (1-32 characters)

Group Name DefaultRead

Authentication Method None

Password (1-32 characters)

Privacy None

Authentication Key (MD5-16, SHA-20 HEX character pairs)

Apply Changes Back

3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. Se añade el usuario al grupo y se actualiza el dispositivo.

Adición de usuarios remotos de SNMPv3 a un grupo

1. Abra la página **SNMPv3 User Security Model** (Modelo de seguridad basado en el usuario de SNMPv3).
2. Haga clic en **Add Remote User** (Añadir usuario remoto).

Aparece la página **Add Remote User** (Añadir usuario remoto):

Ilustración 6-65. Adición de un usuario remoto

Add Remote User

Remote Engine ID (6-32 HEX Characters)

User Name (1-32 characters)

Group Name DefaultRead

Authentication Method None

Password (1-32 characters)

Privacy None

Authentication Key (MD5-16, SHA-20 HEX character pairs)

Apply Changes Back

3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. Se añade el usuario al grupo y se actualiza el dispositivo.

Visualización de la tabla de modelos de seguridad basados en el usuario

1. Abra la página **SNMPv3 User Security Model (USM)** (Modelo de seguridad basado en el usuario [USM] de SNMPv3).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **User Security Model Table** (Tabla de modelos de seguridad basados en el usuario):

Ilustración 6-66. Tabla de modelos de seguridad basados en el usuario

User Name	Group Name	Remote Engine ID	Authentication	Remove
1 Admin	DefaultRead	800002a030006e3900145	NONE	<input type="checkbox"/>
2 pippin	DefaultRead	800002a030006e3900145	NONE	<input type="checkbox"/>
3 gandalf	DefaultRead	800002a030006e3900145	NONE	<input type="checkbox"/>

Eliminación de una entrada de la tabla de modelos de seguridad basados en el usuario

1. Abra la página **User Security Model** (Modelo de seguridad basado en el usuario).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **User Security Model Table** (Tabla de modelos de seguridad basados en el usuario).

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

Se elimina la entrada y se actualiza el dispositivo.

Definición de usuarios de SNMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos SNMP

Comunidades

Los derechos de acceso se administran mediante la definición de comunidades en la página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2). Cuando se cambian los nombres de comunidad, también cambian los derechos de acceso. Las comunidades SNMP se definen sólo para las versiones SNMPv1 y SNMPv2.

Para visualizar la página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2), haga clic en **System** (Sistema) → **SNMP** → **Communities** (Comunidades) en la vista de árbol.

Ilustración 6-67. Comunidad SNMPv1 y SNMPv2

The screenshot shows the configuration page for an SNMPv1.2 Community. The interface includes a navigation tree on the left with 'Communities' selected. The main content area has the following fields and controls:

- Community String:** A dropdown menu showing 'public'.
- SNMP Management Station:** A text input field.
- Access Mode:** A dropdown menu showing 'Read Only'.
- View Name:** A dropdown menu showing 'Unsecure'.
- Group Name:** A dropdown menu showing 'READ'.
- Remove:** A checkbox that is currently unchecked.
- Buttons:** 'Print', 'Refresh', 'Add', 'Show All', and 'Apply Changes'.

La página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2) contiene los campos siguientes:

Community String (Cadena de comunidad): contiene una lista de cadenas de comunidad definidas por el usuario que actúan como contraseña y se utilizan para autenticar la estación de administración SNMP en el dispositivo. Una cadena de comunidad puede contener un máximo de 20 caracteres.

SNMP Management Station (Estación de administración SNMP): contiene una lista de direcciones IP de las estaciones de administración para las que se han definido cadenas de comunidad.

Basic (Básico): activa el modo básico SNMP para la comunidad seleccionada. Los valores del campo posibles son:

Access Mode (Modo de acceso): define los derechos de acceso de la comunidad. Los valores del campo posibles son:

Read-Only (Sólo lectura): la comunidad tiene acceso de sólo lectura a los objetos MIB configurados en la vista.

Read-Write (Lectura/escritura): la comunidad tiene acceso de lectura/modificación a los objetos MIB configurados en la vista.

Super User (Superusuario): la comunidad tiene acceso de lectura/modificación a todos los objetos MIB.

View Name (Nombre de la vista): contiene una lista de las vistas SNMP definidas por el usuario.

Advanced (Avanzado): contiene una lista de grupos definidos por el usuario. Cuando se selecciona el modo avanzado de SNMP, las reglas de control de acceso de SNMP que forman el grupo se activan para la comunidad seleccionada. El modo avanzado también activa grupos SNMP para comunidades SNMP específicas. El modo avanzado de SNMP sólo se define con SNMPv3.

Remove (Eliminar): elimina una comunidad.

Adición de una nueva comunidad

1. Abra la página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add SNMPv1,2 Community** (Añadir comunidad SNMPv1 y SNMPv2).

Ilustración 6-68. Adición de una comunidad SNMPv1 y SNMPv2

SNMP Management Station [dropdown] [XXX.X] [ALL.0.0.0]
Community String (1-20 characters) [input]
Basic [selected] Access Mode: Read Only View Name: Default
Advanced [] Group Name: DefaultRead
Apply Changes Back

3. Complete los campos pertinentes.

Además de los campos incluidos en la página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2), la página **Add SNMPv1,2 Community** (Añadir comunidad SNMPv1 y SNMPv2) contiene el campo **All (0.0.0.0)** (Todo [0.0.0.0]), que indica que la comunidad puede utilizarse desde cualquier estación de administración.

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

Se guarda la nueva comunidad y se actualiza el dispositivo.

Visualización de comunidades

1. Abra la página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Basic Table** (Tabla básica).

Ilustración 6-69. Tabla básica

Management Station	Community String	Access Mode	View Mode	Remove
1 All	private	Read Only	Default	<input type="checkbox"/>
2 All	public	Read Write	Default	<input type="checkbox"/>

Advanced Table

Community String	Management Station	Group Name
1 private	All	DefaultRead
2 public	All	DefaultWrite

Apply Changes Back

Eliminación de comunidades

1. Abra la página **SNMPv1, 2 Community** (Comunidad SNMPv1 y SNMPv2).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **Basic Table** (Tabla básica).
3. Seleccione una comunidad y marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se elimina la entrada de comunidad y se actualiza el dispositivo.

Configuración de comunidades mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

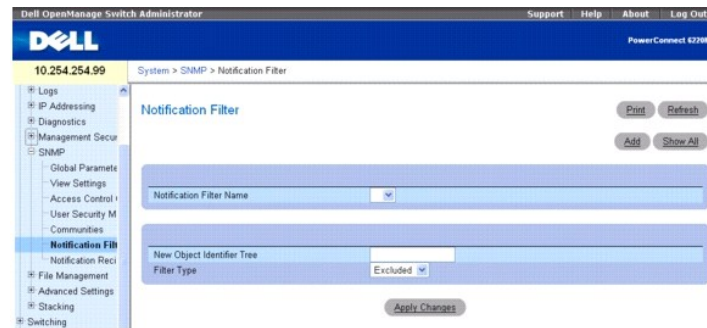
- n Comandos SNMP

Filtro de notificación

Utilice la página **Notification Filter** (Filtro de notificación) para establecer excepciones de filtrado según las OID. Cada OID se enlaza a una función del dispositivo o a un aspecto de la función. La página **Notification Filter** (Filtro de notificación) también permite filtrar notificaciones.

Para visualizar la página **Notification Filter** (Filtro de notificación), haga clic en **System** (Sistema) → **SNMP** → **Notification Filters** (Filtros de notificación) en la vista de árbol.

Ilustración 6-70. Filtro de notificación



La página **Notification Filter** (Filtro de notificación) contiene los campos siguientes:

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 Tree (Nuevo árbol de ID de objeto): muestra la ID de objeto configurada para el filtro seleccionado. Es posible editar este campo.

Filter Type (Tipo de filtro): indica si se envían informes o excepciones relativos a la ID de objeto a los destinatarios de excepciones.

Excluded (Exclusión): se restringe el envío de excepciones o informes de la ID de objeto.

Included (Inclusión): se envían excepciones o informes de la ID de objeto.

Adición de filtros de SNMP

1. Abra la página **Notification Filter** (Filtro de notificación).
 2. Haga clic en **Add** (Añadir).
- Aparece la página **Add Filter** (Añadir filtro):

Ilustración 6-71. Adición de un filtro

3. Defina los campos pertinentes.
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se añade el nuevo filtro y se actualiza el dispositivo.

Visualización de la tabla de filtros

1. Abra la página **Notification Filter** (Filtro de notificación).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Filter Table** (Tabla de filtros), que muestra todos los filtros configurados para el nombre de filtro seleccionado:

Ilustración 6-72. Visualización de una notificación

Eliminación de un filtro

1. Abra la página **Notification Filter** (Filtro de notificación).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **Show Notification** (Mostrar notificación).
3. Seleccione una entrada de la tabla de filtros.
4. Marque **Remove** (Eliminar).
Se elimina la entrada de filtro y se actualiza el dispositivo.

Configuración de filtros de notificación mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos SNMP

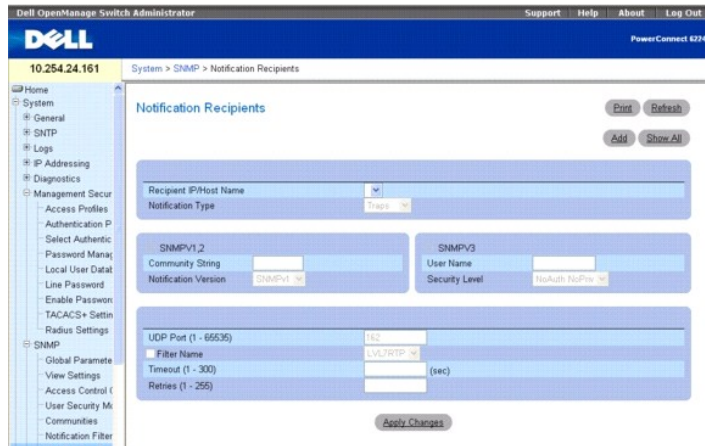
Destinatarios de notificaciones

Utilice la página **Notification Recipients** (Destinatarios de notificaciones) para ver información sobre cómo definir los filtros que determinan si se envían excepciones a usuarios específicos y qué tipo de excepción se envía. Los filtros de notificación de SNMP proporcionan los servicios siguientes:

- 1 Identificación de destinos de excepción de administración
- 1 Filtrado de excepciones
- 1 Selección de parámetros de generación de excepciones
- 1 Comprobaciones de control de acceso

Para visualizar la página **Notification Recipients** (Destinatarios de notificaciones), haga clic en **System** (Sistema) → **SNMP** → **Notification Recipients** (Destinatarios de notificaciones) en la vista de árbol.

Ilustración 6-73. Destinatarios de notificaciones



La página **Notification Recipients** (Destinatarios de notificaciones) contiene los campos siguientes:

Recipient IP (IP del destinatario): contiene una lista de direcciones IP de los destinatarios de notificaciones definida por el usuario.

Notification Type (Tipo de notificación): tipo de notificación enviada. Los valores del campo posibles son:

Trap (Excepción): se envían excepciones.

Inform (Informe): se envían informes.

SNMPv1,2: las versiones 1 o 2 de SNMP están activadas para el destinatario seleccionado. Los valores del campo posibles son:

Community String (Cadena de comunidad): muestra la cadena de comunidad que va a enviarse junto con la notificación.

Notification Version (Versión de notificación): determina la versión de la notificación. Los valores del campo posibles son:

SNMP V1: se envían excepciones de la versión 1 de SNMP. Si se selecciona **Inform** (Informe) como tipo de notificación, no se podrá seleccionar SNMPv1.

SNMP V2: se envían excepciones o informes de la versión 2 de SNMP.

SNMPv3: se activa la versión 3 de SNMP para el destinatario seleccionado. Los valores del campo posibles son:

User Name (Nombre de usuario): permite seleccionar el usuario existente para generar notificaciones.

Security Level (Nivel de seguridad): nivel de seguridad asociado a las notificaciones. Los valores del campo posibles son:

NoAu NoPriv: no se lleva a cabo la autenticación ni el cifrado del paquete.

Auth NoPriv: se lleva a cabo la autenticación del paquete.

Auth Priv: se lleva a cabo la autenticación y el cifrado del paquete.

UDP Port (1-65535) (Puerto UDP [1-65535]): puerto UDP utilizado para enviar notificaciones. El valor predeterminado es 162.

Filter Name (Nombre del filtro): marque esta casilla de verificación para aplicar un filtro de SNMP definido por el usuario (seleccionado en el menú desplegable) a las notificaciones.

Timeout (1-300) (Tiempo de espera [1-300]): tiempo, en segundos, que el dispositivo espera antes de volver a enviar informes. El valor predeterminado es 15 segundos.

Retries (1-255) (Reintentos [1-255]): número máximo de veces que el dispositivo vuelve a enviar una petición de informe. El valor predeterminado es 3.

Adición de un nuevo destinatario de notificaciones

1. Abra la página **Notification Recipients** (Destinatarios de notificaciones).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add Notification Recipients** (Añadir destinatarios de notificaciones):

Ilustración 6-74. Adición de destinatarios de notificaciones

Add Notification Recipients Print Refresh

Recipient IP/Host Name
 Notification Type

SNMPV1.2
 Community String
 Notification Version

SNMPV3
 User Name
 Security Level

UDP Port (1 - 65535)
 Filter Name
 Timeout (1 - 300) (sec)
 Retries (1 - 255)

- Defina los campos pertinentes.
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se añade el destinatario de notificaciones y se actualiza el dispositivo.

Visualización de las tablas de destinatarios de notificaciones

- Abra la página **Notification Recipients** (Destinatarios de notificaciones).
 - Haga clic en **Show All** (Mostrar todo).
- Se abre la página **Notification Recipient Tables** (Tablas de destinatarios de notificaciones).

Ilustración 6-75. Tablas de destinatarios de notificaciones

Notification Recipients Tables Print Refresh

SNMPV1.2 Notification Recipients

Recipients IP/Host Name	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries	Remove

SNMPV3 Notification Recipients

Recipients IP/Host Name	Notification Type	User Name	Security Level	UDP Port	Filter Name	Timeout	Retries	Remove

Apply Changes Back

Eliminación de destinatarios de notificaciones

- Abra la página **Notification Recipients** (Destinatarios de notificaciones).
 - Haga clic en **Show All** (Mostrar todo).
- Se abre la página **Notification Recipient Tables** (Tablas de destinatarios de notificaciones).
- Seleccione la casilla de verificación **Remove** (Eliminar) para uno o varios destinatarios de notificaciones en **SNMPV1,2 Notification Recipient Tables** (Destinatario de notificaciones de SNMPV1,2) o en **SNMPv3 Notification Recipient Tables** (Tablas de destinatarios de notificaciones de SNMPv3).
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se eliminan los destinatarios y se actualiza el dispositivo.

Definición de destinatarios de notificaciones de SNMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos SNMP

Administración de archivos

Utilice la página de menú **File Management** (Administración de archivos) para administrar el software del dispositivo, el archivo de imagen y los archivos de configuración. Los archivos pueden descargarse o cargarse a través de un servidor TFTP. El sistema gestiona dos versiones del software. El sistema que ejecuta una versión anterior del software ignorará (no cargará) un archivo de configuración creado mediante la versión más reciente del software. Cuando el sistema que ejecuta una versión anterior del software detecta un archivo de configuración creado mediante la versión más reciente del software, mostrará una advertencia al usuario.

Información general sobre los archivos de administración

La estructura de los archivos de administración consta de los archivos siguientes:

- 1 **Archivo de configuración de inicio:** conserva la configuración exacta del dispositivo cuando éste se apaga o se reinicia. El archivo de inicio mantiene comandos de configuración, y los comandos de configuración del archivo de configuración en ejecución pueden guardarse en el archivo de inicio.
- 1 **Archivo de configuración en ejecución:** contiene todos los comandos del archivo de inicio, así como todos los comandos introducidos durante la sesión actual. Tras apagar o reiniciar el dispositivo, se pierden todos los comandos almacenados en el archivo de configuración en ejecución. Durante el proceso de inicio, todos los comandos del archivo de inicio se copian en el archivo de configuración en ejecución y se aplican al dispositivo. Durante la sesión, todos los comandos nuevos introducidos se añaden 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 debe copiarse el archivo de configuración en ejecución en el archivo de configuración de inicio. La próxima vez que se reinicie el dispositivo, los comandos se volverán a copiar en el archivo de configuración en ejecución desde el archivo de configuración de inicio.
- 1 **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 se copia el archivo de configuración en ejecución o el archivo de inicio en el archivo de copia de seguridad. Los comandos copiados en el archivo sustituyen a los comandos existentes guardados en el archivo de copia de seguridad. El contenido del archivo de copia de seguridad se puede copiar en el archivo de configuración en ejecución o en el archivo de configuración de inicio. También puede copiarlo en el archivo de copia de seguridad y el archivo de inicio desde un servidor TFTP remoto, o copiar del archivo de copia de seguridad y el archivo de inicio a un servidor remoto.
- 1 **Archivos de imagen:** las imágenes del sistema se guardan en dos sectores de la memoria flash denominados imágenes (Image 1 e Image 2). La imagen activa almacena la copia activa, mientras que la otra imagen almacena una segunda copia. 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. Ésta es una función de seguridad contra fallos que tienen lugar durante el proceso de actualización de inicio.

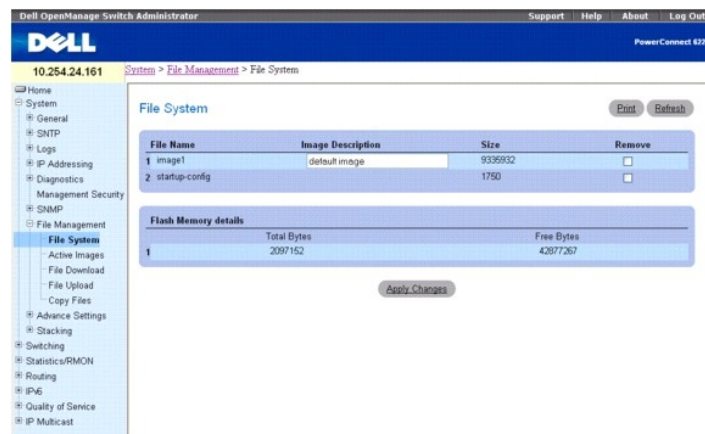
Para visualizar la página **File Management** (Administración de archivos), haga clic en **System** (Sistema) → **File Management** (Administración de archivos) en la vista de árbol.

Sistema de archivos

Utilice la página **File System** (Sistema de archivos) para ver una lista de los archivos del dispositivo.

Para visualizar la página **File System** (Sistema de archivos), haga clic en **System** (Sistema) → **File Management** (Administración de archivos) → **File System** (Sistema de archivos) en la vista de árbol.

Ilustración 6-76. Sistema de archivos



La página **File System** (Sistema de archivos) contiene los campos siguientes:

File Name (Nombre de archivo): campo de texto en el que se muestran los nombres de los archivos del sistema de archivos.

Image Description (0–128) (Descripción de la imagen [0–128]): este campo sirve para configurar y visualizar una descripción de la imagen. Puede introducir hasta 128 caracteres para la descripción.

Size (Tamaño): muestra el tamaño del archivo especificado.

Remove (Eliminar): seleccione esta casilla para eliminar el archivo especificado.

Flash Memory Details (Detalles de la memoria flash): muestra información sobre la memoria flash.

Total Bytes (Total de bytes): muestra la cantidad de memoria flash que se está utilizando.

Free Bytes (Bytes libres): muestra la cantidad de memoria flash disponible.

Eliminación de archivos

1. Abra la página **File System** (Sistema de archivos).
 2. Utilice el campo **File Name** (Nombre de archivo) para seleccionar el archivo que desea eliminar.
 3. Marque la casilla de verificación **Remove** (Eliminar).
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Se elimina el archivo.

Visualización de archivos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

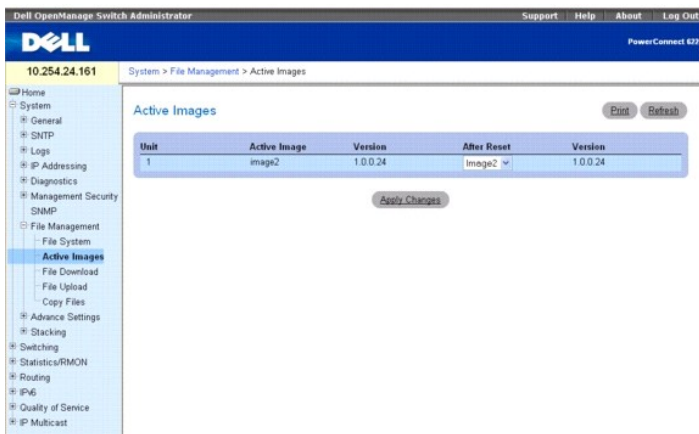
- 1 Comandos de archivos de configuración y de imagen

Imágenes activas

Utilice la página **Active Images** (Imágenes activas) para establecer la imagen de inicio.

Para visualizar la página **Active Images** (Imágenes activas), haga clic en **System** (Sistema)→ **File Management** (Administración de archivos)→ **Active Images** (Imágenes activas) en la vista de árbol.

Ilustración 6-77. Imágenes activas



La página **Active Images** (Imágenes activas) contiene los campos siguientes:

Unit (Unidad): identifica el número de unidad del sistema en la pila.

Active Image (Imagen activa): muestra el nombre de la imagen activa actual.

Version (Versión): muestra el número de versión de la imagen activa actual.

After Reset (Después del restablecimiento): menú desplegable que permite seleccionar la imagen que estará activa después del siguiente restablecimiento.

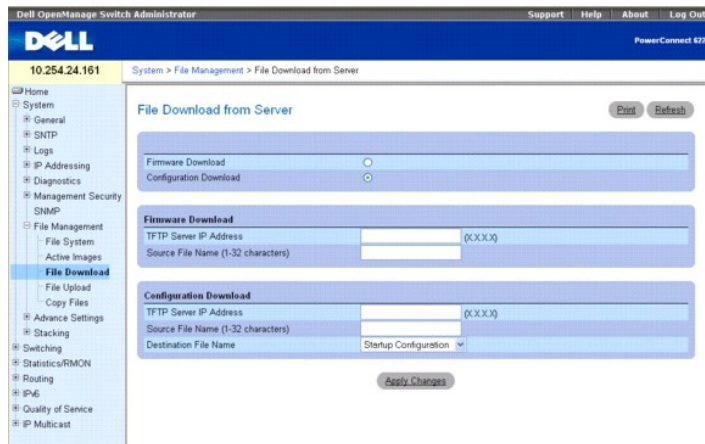
Version (Versión): muestra el número de versión de la imagen que estará activa después del siguiente restablecimiento.

Descarga de archivos del servidor

Utilice la página **File Download From Server** (Descarga de archivos del servidor) para descargar archivos de configuración (ASCII) y de imagen (binarios) del servidor TFTP al dispositivo.

Para visualizar la página **File Download From Server** (Descarga de archivos del servidor), haga clic en **System** (Sistema)→ **File Management** (Administración de archivos)→ **File Download** (Descarga de archivos) en la vista de árbol.

Ilustración 6-78. Descarga de archivos del servidor



La página **File Download From Server** (Descarga de archivos del servidor) contiene los campos siguientes:

Firmware Download (Descarga de firmware): si se selecciona, indica que se va a descargar el archivo de firmware. Si se selecciona esta opción, se atenúan los campos de **Configuration Download** (Descarga de configuración).

Configuration Download (Descarga de configuración): si se selecciona, indica que se va a descargar el archivo de configuración. Si se selecciona **Configuration Download** (Descarga de configuración), se atenúan los campos de **Firmware Download** (Descarga de firmware).

Descarga de firmware

TFTP Server IP Address (Dirección IP del servidor TFTP): indica la dirección IP del servidor TFTP desde el que se descargan los archivos de firmware.

Source File Name (1 – 32 characters) (Nombre de archivo de origen [1–32 caracteres]): nombre del archivo del servidor TFTP, con la ruta de acceso relativa del directorio tftpboot. Por ejemplo, si TFTP está configurado en un servidor remoto, con el directorio tftpboot como *e:\tftp* y el archivo *test.scr* está incluido en *e:\tftp\latest\test.scr*, deberá especificar *\latest\test.scr*.

Descarga de configuración

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP a través del que se descargan los archivos de configuración.

Source File Name (1 – 32 characters) (Nombre de archivo de origen [1–32 caracteres]): nombre del archivo del servidor TFTP.

Destination File Name (Nombre del archivo de destino): archivo de destino en el que se van a descargar los archivos de configuración. Los valores posibles son:

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.

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 va a descargar se encuentra disponible en el servidor TFTP.
3. Complete los campos **TFTP Server IP Address** (Dirección IP del servidor TFTP) y **Source File Name** (Nombre de archivo de origen) (la ruta de acceso completa sin la dirección IP del servidor TFTP).

NOTA: se recomienda no sobrescribir la imagen activa.

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

NOTA: tras iniciar la descarga de un archivo, la página se actualiza y aparece un campo de estado de la transferencia que indica el número de bytes transferidos. La interfaz web se bloquea hasta que finalice la descarga del archivo.

Ilustración 6-79. Progreso de la descarga de archivos

0% 50% 100%	
Percent Complete	Upload Completed
TFTP Server IP Address	172.16.1.1
TFTP Path	/
TFTP Filename	07-06-04 dell_gos.stk
Data Type	Code
Local Filename	image

El software se descarga en el dispositivo.

Descarga de archivos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de archivos de configuración y de imagen

Carga de archivos

Utilice la página **File Upload to Server** (Carga de archivos en el servidor) para cargar archivos de configuración (ASCII) y de imagen (binarios) del dispositivo al servidor TFTP.

Para visualizar la página **File Upload to Server** (Carga de archivos en el servidor), haga clic en **System** (Sistema) → **File Management** (Administración de archivos) → **File Upload** (Carga de archivos) en la vista de árbol.

Ilustración 6-80. Carga de archivos en el servidor

La página **File Upload to Server** (Carga de archivos en el servidor) contiene los campos siguientes:

Firmware Upload (Carga de firmware): indica que va a cargarse el archivo de firmware. Si se selecciona **Firmware Upload** (Carga de firmware), se atenúan los campos de **Configuration Upload** (Carga de configuración).

Configuration Upload (Carga de configuración): indica que el archivo de configuración se ha cargado. Si se selecciona **Configuration Upload** (Carga de configuración), se atenúan los campos de **Firmware Upload** (Carga de firmware).

Carga de imágenes de software

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP en el que se carga la imagen de software.

Destination File Name (1 – 32 characters) (Nombre del archivo de destino [1–32 caracteres]): nombre que tendrá el archivo una vez cargado.

Transfer File Name (Nombre del archivo de transferencia): permite seleccionar el archivo de origen que se va a cargar.

Carga de configuración

TFTP Server IP Address (Dirección IP del servidor TFTP): dirección IP del servidor TFTP en el que se carga el archivo de configuración.

Destination File Name (1 – 32 characters) (Nombre del archivo de destino [1–32 caracteres]): nombre que tendrá el archivo una vez cargado.

Transfer File Name (Nombre del archivo de transferencia): permite seleccionar el archivo de origen que se va a cargar. Los valores de campo válidos 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.

Carga de archivos

1. Abra la página **File Upload to Server** (Carga de archivos en el servidor).
2. Defina los campos aplicables de la página.
3. Haga clic en **Apply Changes** (Aplicar cambios).


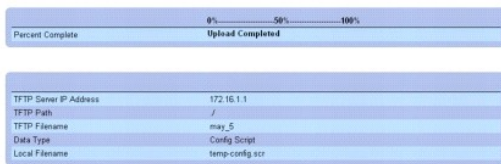
 **NOTA:** tras iniciar la carga de un archivo, la página se actualiza y aparece un campo de estado de la transferencia que indica el número de bytes transferidos. La interfaz web se bloquea hasta que finalice la carga del archivo.

Ilustración 6-81. Progreso de la carga de archivos



Se carga el software en el servidor.

Carga de archivos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de archivos de configuración y de imagen

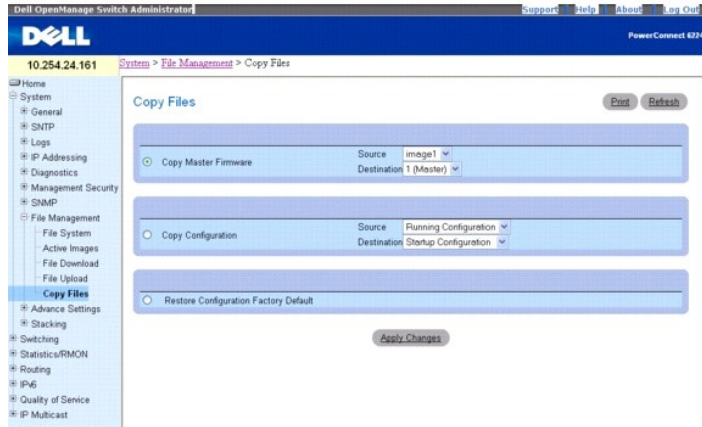
Copia de archivos

La página web Copy Files (Copiar archivos) le ofrece la posibilidad de:

- 1 Copiar imágenes en el sistema de archivos
- 1 Copiar imágenes en y desde servidores remotos
- 1 Realizar copias de seguridad de las imágenes en sistemas locales o remotos
- 1 Restablecer imágenes de sistemas locales o remotos
- 1 Realizar copias de seguridad de los archivos de configuración en el sistema de archivos

Para visualizar la página **Copy Files** (Copiar archivos), haga clic en **System** (Sistema)→ **File Management** (Administración de archivos)→ **Copy Files** (Copiar archivos) en la vista de árbol.

Ilustración 6-82. Copia de archivos



La página **Copy Files** (Copiar archivos) contiene los campos siguientes:

Copy Master Firmware (Copiar firmware maestro): indica que se debe copiar un archivo de imagen de software.

Source (Origen): archivo de origen de la imagen de software desde el que se copia el archivo.

Destination (Destino): unidad de destino en la que se copia el archivo.

Copy Configuration (Copiar configuración): indica que se debe copiar un archivo de configuración.

Source (Origen): archivo de origen de configuración (ejecución, inicio, copia de seguridad) desde el que se copia el archivo.

Destination (Destino): archivo de configuración de destino (ejecución, inicio, copia de seguridad) en el que se copia el archivo.

Restore Configuration Factory Default (Restablecer configuración predeterminada de fábrica): si se marca, especifica que los archivos de configuración predeterminados de fábrica deben restablecerse. Si no se marca esta casilla, se mantiene la configuración actual.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de archivos de configuración y de imagen

Definición de la configuración avanzada

Utilice la configuración avanzada para establecer diversos atributos globales del dispositivo. Los cambios realizados en estos atributos se aplican sólo después de restablecer el dispositivo. Haga clic en **System** (Sistema)→**Advanced Settings** (Configuración avanzada) en la vista de árbol para visualizar la página **Advanced Settings** (Configuración avanzada).

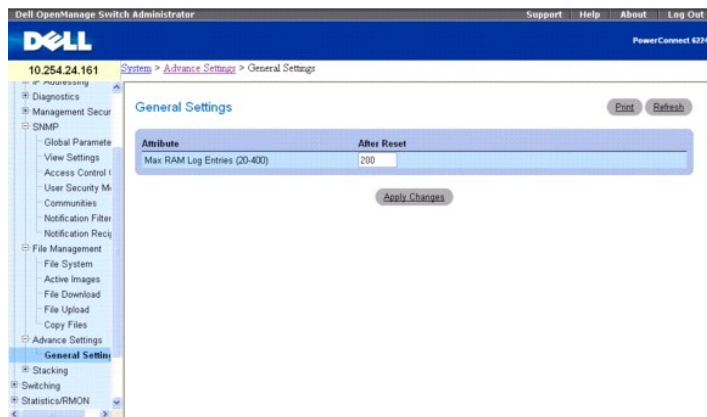
La página **Advanced Settings** (Configuración avanzada) contiene un enlace para configurar los valores generales.

Configuración general

Utilice la página **General Settings** (Configuración general) para definir parámetros generales del dispositivo.

Para visualizar la página **General Settings** (Configuración general), haga clic en **System** (Sistema)→**Advanced Settings** (Configuración avanzada)→**General Settings** (Configuración general) en la vista de árbol.

Ilustración 6-83. Configuración general



La página **General Settings** (Configuración general) contiene los campos siguientes:

Attribute (Atributo): número máximo de entradas en la tabla de registros de RAM. El valor predeterminado es 200 entradas.

After Reset (Después del restablecimiento): número máximo de entradas después de restablecer el dispositivo. Cuando se introduce un valor en esta columna, se asigna memoria a la tabla de campos.

Cambio de tamaño de la asignación de entradas de registros de RAM

1. Abra la página **General Settings** (Configuración general).
2. Introduzca un nuevo valor en el campo **After Reset** (Después del restablecimiento).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El espacio asignado a las entradas de registros de RAM tendrá efecto después del siguiente restablecimiento del dispositivo.

Visualización de la configuración general mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos Syslog

Definición del apilamiento

Utilice los menús de apilamiento para establecer las características de apilamiento del dispositivo. Los cambios realizados en estos atributos se aplican sólo después de restablecer el dispositivo. Haga clic en **System** (Sistema) → **Stacking** (Apilamiento) en la vista de árbol para visualizar la página **Stacking** (Apilamiento). Utilice esta página para acceder a las funciones siguientes:

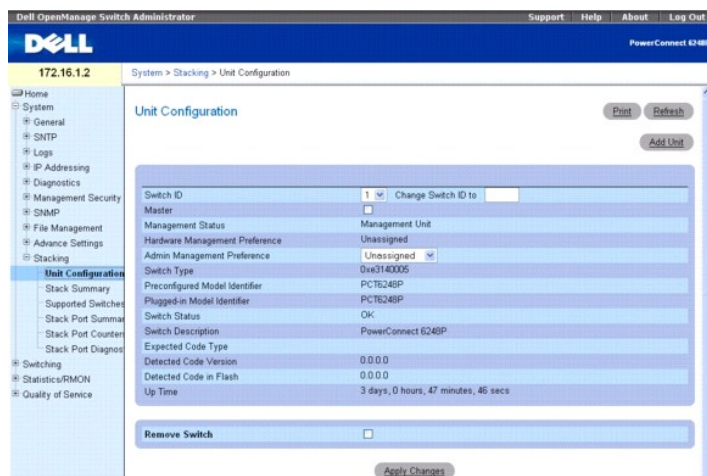
- 1 [Configuración de unidades](#)
- 1 [Resumen de la pila](#)
- 1 [Conmutadores admitidos](#)
- 1 [Resumen de los puertos de la pila](#)
- 1 [Contadores de los puertos de la pila](#)
- 1 [Diagnósticos de los puertos de la pila](#)

Configuración de unidades

Utilice la página **Unit Configuration** (Configuración de unidades) para definir los parámetros generales del dispositivo.

Para visualizar la página **Unit Configuration** (Configuración de unidades), haga clic en **System** (Sistema) → **Stacking** (Apilamiento) → **Unit Configuration** (Configuración de unidades) en la vista de árbol.

Ilustración 6-84. Configuración de unidades



La página **Unit Configuration** (Configuración de unidades) contiene los campos siguientes:

Switch ID (ID de conmutador): permite especificar la unidad que se va a configurar.

Change Switch ID to (Cambiar ID de conmutador a): permite cambiar el número de unidad de la unidad seleccionada.

Master (Maestra): seleccione esta casilla si desea que esta unidad sea una unidad maestra (de administración) en lugar de otra unidad. El valor predeterminado de esta configuración es **Unassigned** (No asignado).

Management Status (Estado de administración): muestra si la unidad seleccionada es una unidad de administración o un miembro de la pila.

Hardware Management Preference (Preferencia de administración de hardware): preferencia de administración para la configuración de hardware que debería seleccionarse como unidad de administración.

Admin Management Preference (Preferencia de administración): determina si esta unidad puede llegar a ser el conmutador maestro. El intervalo de valores va de **Disable** (Desactivar) (la unidad no admite la función de conmutador maestro) a **Preference 15** (Preferencia 15). El valor más alto significa que la unidad es preferible a otra unidad con un valor inferior para ejecutar la función de administración. Hay un valor adicional, **Unassigned** (No asignado), que significa que no se ha configurado ninguna preferencia y se deja la elección del conmutador maestro para las unidades de pila.

Switch Type (Tipo de conmutador): ID de hardware asignada al sistema para determinar el tipo de conmutador.

Preconfigured Model Identifier (Identificador de modelo preconfigurado): cadena de caracteres de 16 bytes que sirve para identificar el modelo preconfigurado de la unidad seleccionada.

Plugged-in Model Identifier (Identificador de modelo conectado): cadena de caracteres de 16 bytes que sirve para identificar el modelo conectado de la unidad seleccionada.

Switch Status (Estado del conmutador): muestra el estado de la unidad seleccionada. Los valores posibles son:

OK (Aceptar): indica que la unidad está bien colocada y en funcionamiento.

Unsupported (No admitido): indica que la unidad está bien colocada pero no puede funcionar como miembro de la pila.

Code Mismatch (Discrepancia de código): indica que el software del conmutador no coincide con el software de la unidad maestra.

Config Mismatch (Discrepancia de configuración): indica que la configuración del conmutador no coincide con la configuración de la unidad maestra.

Not Present (No presente): indica la ausencia de la unidad seleccionada.

Switch Description (Descripción del conmutador): campo de datos de 80 bytes que sirve para identificar el dispositivo.

Expected Code Type (Tipo de código esperado): muestra el identificador de código esperado.

Detected Code Version (Versión de código detectado): número de versión del código en ejecución.

Detected Code in Flash (Código detectado en flash): número de versión del código detectado en flash.

Up Time (Tiempo de actividad): muestra el tiempo durante el que la unidad se ha ejecutado desde su último restablecimiento.

Remove Switch (Eliminar conmutador): seleccione esta casilla para eliminar el conmutador de la pila.

Definición de la configuración de unidades

1. Abra la página **Unit Configuration** (Configuración de unidades).
2. Introduzca nuevos valores en los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los cambios tendrán efecto después del siguiente restablecimiento del dispositivo.

Eliminación de un conmutador

1. Abra la página **Unit Configuration** (Configuración de unidades).
2. Marque **Remove Switch** (Eliminar conmutador).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los cambios tendrán efecto después del siguiente restablecimiento del dispositivo.

Adición de una unidad

Utilice la página **Add Unit** (Añadir unidad) para definir los parámetros generales del dispositivo.

Para visualizar la página **Supported Switches** (Conmutadores admitidos), haga clic en **System** (Sistema) → **Stacking** (Apilamiento) → **Unit Configuration** (Configuración de unidades) en la vista de árbol y, a continuación, haga clic en **Add Unit** (Añadir unidad).

Ilustración 6-85. Adición de una unidad



La página **Add Unit** (Añadir unidad) contiene los campos siguientes:

Switch ID (ID de conmutador): muestra la ID del conmutador seleccionado en la pila. Los usuarios administradores pueden cambiar la numeración de la ID del conmutador seleccionado. Sólo los usuarios con un nivel de acceso 15 pueden cambiar este campo mediante la interfaz web.

Switch Type (Tipo de conmutador): identifica la ID de hardware asignada al conmutador.

Adición de una unidad

1. Abra la página **Unit Configuration** (Configuración de unidades).
2. Haga clic en **Add Unit** (Añadir unidad).
Aparece la página **Add Unit** (Añadir unidad).
3. Introduzca un nuevo valor en el campo **Switch ID** (ID de conmutador).
4. Seleccione el valor que desee en la lista desplegable **Switch Type** (Tipo de conmutador).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los cambios tendrán efecto después del siguiente restablecimiento del dispositivo.

Visualización de la configuración de unidades mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

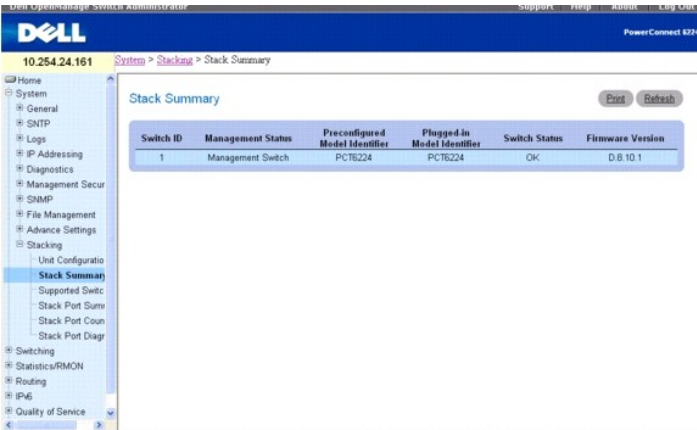
- 1 Comandos de administración del sistema

Resumen de la pila

Utilice la página **Stack Summary** (Resumen de la pila) para ver un resumen de los conmutadores que forman parte de la pila.

Para visualizar la página **Stack Summary** (Resumen de la pila), haga clic en **System** (Sistema) → **Stacking** (Apilamiento) → **Stack Summary** (Resumen de la pila) en la vista de árbol.

Ilustración 6-86. Resumen de la pila



La página **Stack Summary** (Resumen de la pila) contiene los campos siguientes:

Switch ID (ID de conmutador): ID de la unidad. El número máximo de unidades permitidas en la pila es 8.

Management Status (Estado de administración): este campo indica si el conmutador es un conmutador maestro, un miembro de la pila o si no tiene ningún estado asignado.

Pre-configured Model Identifier (Identificador de modelo preconfigurado): campo de 16 caracteres asignado por el fabricante del dispositivo para identificar el dispositivo preconfigurado.

Plugged-in Model Identifier (Identificador de modelo conectado): campo de 16 caracteres asignado por el fabricante del dispositivo para identificar el dispositivo conectado.

Switch Status (Estado del conmutador): indica el estado de la unidad. Existen cinco valores de estado posibles:

OK (Correcto): indica que la unidad está bien colocada y funciona correctamente.

Unsupported (No admitido): indica que no se admite la unidad en la pila.

Code Mismatch (Discrepancia de código): indica que la imagen de software de esta unidad no coincide con la imagen de software que se utiliza en el conmutador maestro de la pila.

Config Mismatch (Discrepancia de configuración): indica que el archivo de configuración de esta unidad no coincide con el archivo de configuración que se utiliza en el conmutador maestro de la pila.

Not Present (No presente): indica la ausencia de la unidad.

Firmware Version (Versión del firmware): indica la versión del código detectada en esta unidad.

Visualización del resumen de la pila mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de administración del sistema

Conmutadores admitidos

Utilice la página **Supported Switches** (Conmutadores admitidos) para ver información sobre los distintos tipos de conmutadores admitidos para el apilamiento y sobre los conmutadores admitidos.

Para visualizar la página **Supported Switches** (Conmutadores admitidos), haga clic en **System** (Sistema) → **Stacking** (Apilamiento) → **Supported Switches** (Conmutadores admitidos) en la vista de árbol.

Ilustración 6-87. Conmutadores admitidos



La página **Supported Switches** (Conmutadores admitidos) contiene los campos siguientes:

Supported Switches (Conmutadores admitidos): lista desplegable que permite seleccionar los conmutadores admitidos.

Switch Index (Índice de conmutadores): especifica el índice de la base de datos que contiene los tipos de conmutadores admitidos.

Switch Type (Tipo de conmutador): ID de hardware asignada al conmutador.

Switch Model ID (ID de modelo de conmutador): muestra una cadena de caracteres de 16 bytes que identifica el modelo del conmutador admitido.

Description (Descripción): campo de datos de 256 bytes que sirve para identificar el dispositivo.

Management Preference (Preferencia de administración): determina si esta unidad puede llegar a ser el conmutador maestro. Si el valor se establece en cero, la unidad no podrá admitir la función de conmutador maestro. El valor más alto significa que la unidad es preferible a otra unidad con un valor inferior para ejecutar la función de administración. El fabricante del dispositivo establece el valor inicial de este campo.

Expected Code Type (Tipo de código esperado): muestra el número de versión del código esperado.

Visualización de características de los conmutadores admitidos

1. Abra la página **Supported Switches** (Conmutadores admitidos).
2. Seleccione el conmutador que desee en la lista desplegable **Supported Switches** (Conmutadores admitidos).

Visualización de los conmutadores admitidos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de administración del sistema

Resumen de los puertos de la pila

Utilice la página **Stack Port Summary** (Resumen de los puertos de la pila) para ver los puertos apilables disponibles. En esta pantalla se visualiza la unidad, la interfaz apilable, el modo configurado de la interfaz y el modo de ejecución, así como el estado y la velocidad del enlace del puerto apilable.

Para visualizar la página **Stack Port Summary** (Resumen de los puertos de la pila), haga clic en **System** (Sistema) → **Stacking** (Apilamiento) → **Stack Port Summary** (Resumen de los puertos de la pila) en la vista de árbol.

Ilustración 6-88. Resumen de los puertos de la pila

Unit	Interface	Configured Stack-mode	Running Stack-mode	Link Status	Link Speed (Gb/s)
1	1/xg1	Ethernet	Ethernet	Link Down	12
1	1/xg2	Ethernet	Ethernet	Link Down	12
1	1/xg3	Ethernet	Ethernet	Link Down	12
1	1/xg4	Ethernet	Ethernet	Link Down	12

La página **Stack Port Summary** (Resumen de los puertos de la pila) contiene los campos siguientes:

Unit (Unidad): número de identificación de la unidad.

Interface (Interfaz): identifica la interfaz de la pila asignada a la unidad.

Configured Stack Mode (Modo de pila configurado): indica si cada unidad puede participar en la pila.

Running Stack Mode (Modo de pila en ejecución): indica si cada unidad participa realmente en la pila.

Link Status (Estado del enlace): indica si la interfaz de la pila de cada unidad funciona.

Link Speed (Gb/s) (Velocidad del enlace [Gb/s]): indica la velocidad nominal del enlace de cada unidad.

Visualización del resumen de los puertos de la pila mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de administración del sistema

Contadores de los puertos de la pila

Utilice la página **Stack Port Counters** (Contadores de los puertos de la pila) para ver las estadísticas transmitidas y recibidas, incluida la velocidad de datos y la tasa de errores.

Para visualizar la página **Stack Port Counters** (Contadores de los puertos de la pila), haga clic en **System** (Sistema)→ **Stacking** (Apilamiento)→ **Stack Point Counters** (Contadores de los puertos de la pila) en la vista de árbol.

Ilustración 6-89. Contadores de los puertos de la pila

Unit	Interface	Data Rate (Mb/s)	Transmit Error Rate (Errors/sec)	Total Errors	Data Rate (Mb/s)	Receive Error Rate (Errors/sec)	Total Errors
1	1/xg1	0	0	0	0	0	0
1	1/xg2	0	0	0	0	0	0
1	1/xg3	0	0	0	0	0	0
1	1/xg4	0	0	0	0	0	0

La página **Stack Port Counters** (Contadores de los puertos de la pila) contiene los campos siguientes:

Unit (Unidad): indica el conmutador subordinado que se visualiza.

Interface (Interfaz): indica el nombre de la interfaz.

Data Rate (Mb/s) (Velocidad de datos [Mb/s]): indica la velocidad a la que se transmiten los datos.

Transmit Error Rate (Errors/sec) (Velocidad de transmisión de errores [errores/s]): indica el número de errores transmitidos por segundo.

Total Errors (Total de errores): número total de errores transmitidos.

Data Rate (Mb/s) (Velocidad de datos [Mb/s]): indica la velocidad a la que se reciben los datos.

Receive Error Rate (Errors/sec) (Velocidad de recepción de errores [errores/s]): indica el número de errores recibidos por segundo.

Total Errors (Total de errores): número total de errores recibidos.

Visualización de los contadores de los puertos de la pila

1. Abra la página **Stack Port Counters** (Contadores de los puertos de la pila).

Visualización de los contadores de los puertos de la pila mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de administración del sistema

Diagnósticos de los puertos de la pila

La página **Stack Port Diagnostics** (Diagnósticos de los puertos de la pila) está dirigida únicamente a ingenieros de aplicaciones de campo (FAE) y desarrolladores.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de la información sobre conmutación

Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [Configuración de la seguridad de la red](#)
- [Configuración de puertos](#)
- [Configuración de la duplicación de tráfico](#)
- [Configuración de tablas de direcciones](#)
- [Configuración de GARP](#)
- [Configuración del protocolo de árbol de extensión](#)
- [Configuración de redes VLAN](#)
- [Agregación de puertos](#)
- [Administración de la compatibilidad con multidifusión](#)
- [Configuración del protocolo de detección de nivel de enlace \(LLDP\)](#)

En esta sección se proporciona información sobre todas las operaciones del sistema e información general sobre la seguridad de la red, puertos, tablas de direcciones, GARP, redes VLAN, árbol de extensión, agregación de puertos y compatibilidad con multidifusión.

La página de menú **Switching** (Conmutación) contiene enlaces a las funciones siguientes:

- 1 [Configuración de la seguridad de la red](#)
- 1 [Configuración de puertos](#)
- 1 [Configuración de la duplicación de tráfico](#)
- 1 [Configuración de tablas de direcciones](#)
- 1 [Configuración de GARP](#)
- 1 [Configuración del protocolo de árbol de extensión](#)
- 1 [Configuración de redes VLAN](#)
- 1 [Agregación de puertos](#)
- 1 [Administración de la compatibilidad con multidifusión](#)
- 1 [Configuración del protocolo de detección de nivel de enlace \(LLDP\)](#)

Configuración de la seguridad de la red

Utilice la página de menú **Network Security** (Seguridad de la red) para definir la seguridad de la red mediante autenticación basada en el puerto, puertos bloqueados, configuración de filtrado de DHCP y listas de control de acceso.

Para visualizar la página **Network Security** (Seguridad de la red), haga clic en **Switching** (Conmutación) → **Network Security** (Seguridad de la red) en la vista de árbol.

La página de menú **Network Security** (Seguridad de la red) contiene enlaces a las funciones siguientes:

- 1 [Autenticación basada en el puerto](#)
- 1 [Varios hosts](#)
- 1 [Usuarios autenticados](#)
- 1 [Seguridad de puertos](#)
- 1 [Filtrado de DHCP](#)
- 1 Listas de control de acceso
- 1 [Configuración de vinculaciones de ACL](#)

Autenticación basada en el puerto

En el modo de autenticación basada en el puerto, cuando 802.1x está activado globalmente y en el puerto, si la autenticación de cualquier suplicador conectado al puerto es satisfactoria, todos los usuarios podrán utilizar el puerto sin ninguna restricción. En este modo, en cualquier momento dado sólo un suplicador puede intentar la autenticación en un puerto. Los puertos en este modo están bajo control bidireccional. Es el modo de autenticación predeterminado.

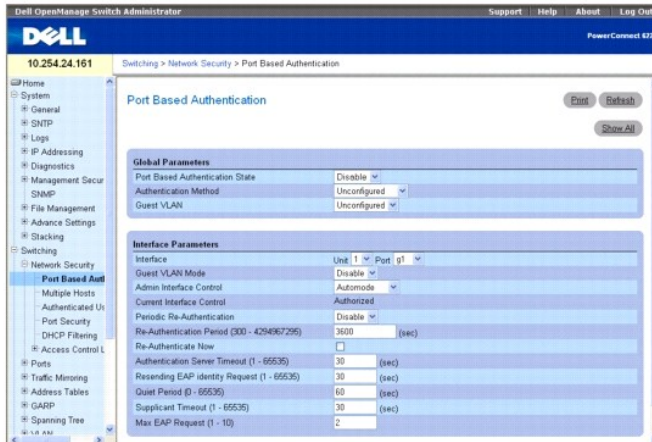
La red 802.1x tiene tres componentes:

- 1 **Authenticators** (Autenticadores): especifica el puerto que se autentica antes de permitir el acceso al sistema.
- 1 **Supplicants** (Suplicadores): especifica el host conectado al puerto autenticado que solicita acceso a los servicios del sistema.
- 1 **Authentication Server** (Servidor de autenticación): especifica el servidor externo, por ejemplo, el servidor RADIUS, que realiza la autenticación en nombre del autenticador, e indica si el usuario puede acceder a los servicios del sistema.

Utilice la página **Port Based Authentication** (Autenticación basada en el puerto) para configurar los parámetros de 802.1x generales para un puerto.

Para visualizar la página **Port Based Authentication** (Autenticación basada en el puerto), haga clic en **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **Port Based Authentication** (Autenticación basada en el puerto) en la vista de árbol.

Ilustración 7-1. Autenticación basada en el puerto



La página **Port Based Authentication** (Autenticación basada en el puerto) contiene los campos siguientes:

Parámetros globales

Port Based Authentication State (Estado de la autenticación basada en el puerto): permite realizar la autenticación basada en el puerto en el conmutador. Los valores del campo posibles son:

Enable (Activar): activa la autenticación basada en el puerto en el conmutador.

Disable (Desactivar): desactiva la autenticación basada en el puerto en el conmutador.

Authentication Method (Método de autenticación): selecciona el método de autenticación utilizado. Los valores del campo posibles son:

Unconfigured (Sin configurar): indica que no se ha seleccionado un método de autenticación.

None (Ninguno): indica que no se utiliza ningún método de autenticación.

RADIUS: indica que la autenticación tiene lugar en el servidor RADIUS.

RADIUS, None (RADIUS, Ninguno): indica que la autenticación tiene lugar en el servidor RADIUS. Si el servidor RADIUS no está disponible, no se utiliza ningún método de autenticación.

None, RADIUS (Ninguno, RADIUS): indica que no se utiliza ningún método de autenticación. Si la autenticación es necesaria, tiene lugar en el servidor RADIUS.

Guest VLAN (VLAN invitada): especifica una VLAN invitada para todos los puertos. Los valores del campo posibles son:

Unconfigured (Sin configurar): la VLAN invitada no está configurada para todos los puertos.

VLAN ID (ID de VLAN): muestra la ID de las VLAN configuradas en el sistema. Seleccione la VLAN que desea usar como VLAN invitada para todos los puertos.

Parámetros de interfaz

Interface (Interfaz): selecciona la unidad y el puerto afectados.

Guest VLAN Mode (Modo de VLAN invitada): activa o desactiva el modo de VLAN invitada en esta interfaz.

Admin Interface Control (Control de la interfaz del administrador): define el estado de autorización del puerto. Los valores del campo posibles son:

Automode (Modo automático): detecta automáticamente el modo de la interfaz.

Authorized (Autorizada): sitúa la interfaz en un estado de autorización sin que se haya autenticado. La interfaz envía y recibe tráfico normal sin la autenticación basada en el puerto del cliente.

Unauthorized (No autorizada): deniega a la interfaz seleccionada el acceso al sistema situándola en el estado de no autorización. El conmutador no puede proporcionar servicios de autenticación al cliente a través de la interfaz.

Current Interface Control (Control de la interfaz actual): muestra el estado de autorización del puerto actual.

Periodic Re-Authentication (Reautenticación periódica): si se activa esta opción, se vuelve a autenticar periódicamente el puerto seleccionado.

Re-Authentication Period (300-4294967295) (Periodo de reautenticación [300-4294967295]): indica el lapso de tiempo en el que se vuelve a autenticar el puerto seleccionado. El valor del campo se expresa en segundos. El valor predeterminado de este campo es 3600 segundos.

Re-Authenticate Now (Volver a autenticar 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 el tiempo que transcurre antes de que el

conmutador vuelve a enviar una petición al servidor de autenticación. El valor del campo se expresa en segundos. El valor predeterminado de este campo es 30 segundos.

Resending EAP Identity Request (1-65535) (Reenvío de la petición de identidad EAP [1-65535]): define el tiempo que transcurre antes de enviar de nuevo las peticiones EAP. El valor del campo se expresa en segundos. El valor predeterminado de este campo es 30 segundos.

Quiet Period (0-65535) (Periodo de silencio [0-65535]): define el periodo durante el que el conmutador permanece en estado de silencio después de producirse un error en el intercambio de autenticación. El intervalo de valores posibles de este campo es 0-65535. El valor del campo se expresa en segundos. El valor predeterminado de este campo es 60 segundos.

Supplicant Timeout (0-65535) (Tiempo de espera del solicitante [0-65535]): indica el tiempo que transcurre antes de volver a enviar las peticiones EAP al usuario. El valor del campo se expresa en segundos. El valor predeterminado de este campo es 30 segundos.

Max EAP Requests (1-10) (Número máximo de peticiones EAP [1-10]): define el número máximo de veces que el conmutador puede enviar una petición EAP antes de que se reinicie el proceso de autenticación en caso de no recibir respuesta. El intervalo de valores posibles de este campo es 1-10 y el valor predeterminado es dos reintentos.

Visualización de la tabla de autenticación basada en el puerto

1. Abra la página **Port Based Authentication** (Autenticación basada en el puerto).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Port Based Authentication Table** (Tabla de autenticación basada en el puerto), donde se muestra la parte izquierda de la tabla:

Ilustración 7-2. Tabla de autenticación basada en el puerto

Ports	Admin Port Control	Current Port Control	Profile	Re-Authentication Period	Re-Authenticate Now	
1 1/fg1	Authorized	Authorized	Default	3600		OK
2 1/fg2	Authorized	Authorized	Default	3600		OK
3 1/fg3	Authorized	Authorized	Default	3600		OK
4 1/fg4	Authorized	Authorized	Default	3600		OK
5 1/fg5	Authorized	Authorized	Default	3600		OK

23 1/fg23	Authorized	Authorized	Default	3600		OK
24 1/fg24	Authorized	Authorized	Default	3600		OK
25 1/fg1	Authorized	Authorized	Default	3600		OK
26 1/fg2	Authorized	Authorized	Default	3600		OK
27 1/fg3	Authorized	Authorized	Default	3600		OK
28 1/fg4	Authorized	Authorized	Default	3600		OK

3. Utilice la barra de desplazamiento horizontal o haga clic en la flecha derecha en la parte inferior de la pantalla para visualizar la parte derecha de la tabla.
4. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de autenticación basada en el puerto correspondiente a otras unidades de la pila, en caso de que existan.

Reautenticación de un puerto

1. Abra la página **Port Based Authentication** (Autenticación basada en el puerto).
2. Marque la opción **Edit** (Editar) para seleccionar la unidad o puerto que desea volver a autenticar.
3. Marque la opción **Reauthenticate Now** (Volver a autenticar ahora).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto especificado se vuelve a autenticar y se actualiza el dispositivo.

Reautenticación de varios puertos en la tabla de autenticación basada en el puerto

1. Abra la página **Port Based Authentication** (Autenticación basada en el puerto).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **Port Based Authentication Table** (Tabla de autenticación basada en el puerto).
3. Marque la opción **Edit** (Editar) para seleccionar las unidades o puertos que desea volver a autenticar.

4. Para volver a autenticar de forma periódica, defina **Periodic Re-Authentication** (Reautenticación periódica) con el valor Enable (Activar) y especifique un valor en **Re-Authentication Period** (Período de reautenticación) para todos los puertos que desee.
5. Para volver a autenticar inmediatamente, marque la opción **Reauthenticate Now** (Reautenticar ahora) para todos los puertos que desee volver a autenticar.
6. Haga clic en **Apply Changes** (Aplicar cambios).

Los puertos especificados se vuelven a autenticar (ya sea de forma inmediata o periódica) y se actualiza el dispositivo.

Cambio de control del puerto administrativo

1. Abra la página **Port Based Authentication** (Autenticación basada en el puerto).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Port Based Authentication Table** (Tabla de autenticación basada en el puerto).

3. Vaya a la parte derecha de la tabla y seleccione la casilla de verificación **Edit** (Editar) para cada puerto que desee configurar. Cambie **Admin Port Control** (Control del puerto administrativo) a **Authorized** (Autorizado), **Unauthorized** (No autorizado) o **Automode** (Modo automático) según corresponda para los puertos seleccionados. Sólo la opción **Automode** (Modo automático) utiliza dot1x para realizar la autenticación. **Authorized** (Autorizado) y **Unauthorized** (No autorizado) se utilizan para prevalecer manualmente.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se actualiza Admin Port Control (Control del puerto administrativo) para los puertos especificados y se actualiza el dispositivo.

Activación de la autenticación basada en el puerto mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos 802.1X

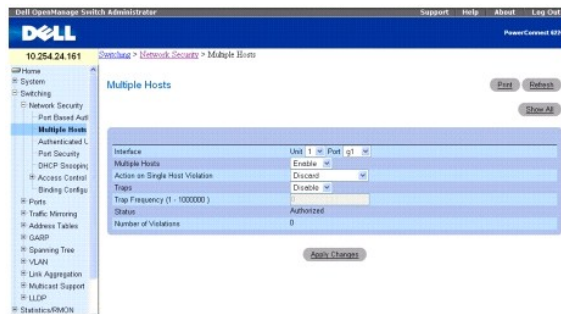
Varios hosts

Cuando un puerto está en modo de varios hosts, sólo es necesario que se autentique un conmutador en dicho puerto. Una vez hecho, cualquier conmutador del puerto podrá acceder a la red. Si el puerto se queda sin autorización por cualquier motivo, todos los conmutadores perderán su acceso a la red y será preciso volver a comenzar el proceso de autenticación.

La página **Multiple Hosts** (Varios hosts) proporciona información para definir valores avanzados de la autenticación basada en el puerto para puertos específicos.

Para visualizar la página **Multiple Hosts** (Varios hosts), haga clic en **Switching** (Conmutación)→**Network Security** (Seguridad de la red)→**Multiple Host** (Varios hosts) en la vista de árbol.

Ilustración 7-3. Varios hosts



La página **Multiple Hosts** (Varios hosts) contiene los campos siguientes:

Interface (Interfaz): especifica los números de unidad y de puerto en los que se deben configurar los valores avanzados de la autenticación basada en el puerto.

Multiple Hosts (Varios hosts): activa o desactiva un único host para autorizar varios hosts para el acceso al sistema. Este valor debe activarse para desactivar el filtrado de entrada o para utilizar la seguridad de bloqueo de puerto en el puerto seleccionado.

Action on Single Host Violation (Acción tras infracción de un único host): define la acción que debe aplicarse en los paquetes que llegan en modo de un único

host desde un host cuya dirección MAC no es la dirección MAC del cliente (suplicador). Los valores del campo posibles son:

Forward (Reenviar): reenvía los paquetes de origen desconocido. Sin embargo, no se obtiene la dirección MAC.

Discard (Descartar): descarta los paquetes de cualquier origen no obtenido. Éste es el valor predeterminado.

Discard Shutdown (Descartar y apagar): descarta los paquetes de cualquier origen no obtenido y apaga el puerto. Los puertos permanecen apagados hasta que se activan o hasta que se restablece el conmutador.

Traps (Excepciones): activa o desactiva el envío de excepciones al host si se produce una infracción.

Trap Frequency (1-1000000) (Frecuencia de excepciones [1-1000000]): define el periodo de tiempo que rige el envío de excepciones al host. El valor predeterminado es 10 segundos. La excepción de seguridad se envía una vez cada 10 segundos con un recuento del número de infracciones.

Status (Estado): muestra el estado del host. Los valores del campo posibles son:

Authorized (Autorizado): indica que el control del puerto está en modo automático y que los clientes tienen acceso completo al puerto.

Unauthorized (No autorizado): indica que el control del puerto es *Force Unauthorized* (Forzar no autorizado), el enlace de puerto está inactivo o el control del puerto es Auto (Automático), pero no se ha autenticado ningún cliente a través del puerto.

Not in auto mode (No en modo automático): indica que el control del puerto es *Forced Authorized* (Forzar autorizado) y que los clientes tienen acceso completo al puerto.

Single-host Lock (Bloqueo de un único host): indica que el control del puerto es *Auto* (Automático) y que se ha autenticado un solo cliente a través del puerto.

No Single Host (No host único): indica que la opción activada es Multiple Host (Varios hosts).

Number of Violations (Número de infracciones): muestra el número de paquetes que han llegado a la interfaz en modo de un único host desde un host cuya dirección MAC no es la dirección MAC del cliente (suplicador).

Visualización de la tabla de varios hosts

1. Abra la página **Multiple Hosts** (Varios hosts).

2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Multiple Host Table** (Tabla de varios hosts).

Ilustración 7-4. Tabla de varios hosts

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations	Edit
1 1/1g1	Enable	Discard	Disable	0	Authorized	0	
2 1/1g2	Enable	Discard	Disable	0	Authorized	0	
3 1/1g3	Enable	Discard	Disable	0	Authorized	0	
4 1/1g4	Enable	Discard	Disable	0	Authorized	0	
...
48 1/1g48	Enable	Discard	Disable	0	Authorized	0	
49 1/1g1	Enable	Discard	Disable	0	Authorized	0	
50 1/1g2	Enable	Discard	Disable	0	Authorized	0	
51 1/1g3	Enable	Discard	Disable	0	Authorized	0	
52 1/1g4	Enable	Discard	Disable	0	Authorized	0	

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de varios hosts correspondiente a otras unidades de la pila, en caso de que existan.

Activación/desactivación de varios hosts para un puerto

1. Abra la página **Multiple Hosts** (Varios hosts).

2. Seleccione la unidad y el puerto afectados en **Interface** (Interfaz).

3. Defina las variables según convenga.

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

Se activa la opción Multiple hosts (Varios hosts) para el puerto especificado y se actualiza el dispositivo.

Activación/desactivación de varios hosts para varios puertos

1. Abra la página **Multiple Hosts** (Varios hosts).
2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Multiple Host Table** (Tabla de varios hosts).
3. Seleccione la casilla de verificación **Edit** (Editar) asociada con los puertos que va a configurar.
4. Cambie las variables de los puertos en cuestión.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Los puertos editados se actualizan, así como el dispositivo.

Configuración de la autenticación de puerto avanzada mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

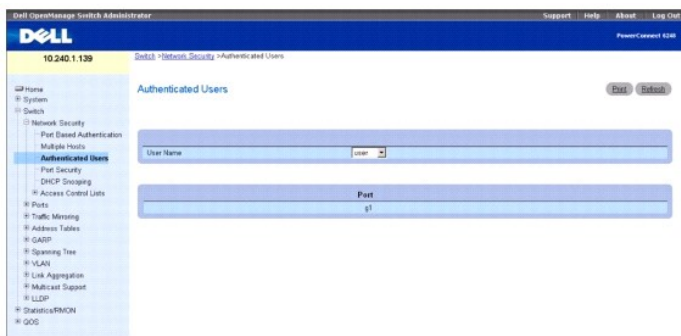
- 1 Comandos 802.1X.

Usuarios autenticados

La página **Authenticated Users** (Usuarios autenticados) muestra las listas de acceso de los usuarios a los puertos.

Para visualizar la página **Authenticated Users** (Usuarios autenticados), haga clic en **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **Authenticated Users** (Usuarios autenticados) en la vista de árbol.

Ilustración 7-5. Usuarios autenticados



La página **Authenticated Users** (Usuarios autenticados) contiene los campos siguientes:

User Name (Nombre de usuario): especifica un usuario de la lista de usuarios autorizados a través del servidor RADIUS.

Port (Puerto): indica el puerto utilizado para la autenticación.

Visualización de usuarios autenticados mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos 802.1X

Seguridad de puertos

La opción **Port Security** (Seguridad de puertos) se puede activar de forma individual para cada puerto. Cuando un puerto está bloqueado, sólo pueden reenviarse paquetes con direcciones MAC de origen permitidas. Todos los demás paquetes se descartan. Una dirección MAC puede definirse como permitida mediante dos métodos: de forma dinámica o estática. Tenga en cuenta que los dos métodos se utilizan simultáneamente cuando un puerto está bloqueado.

El bloqueo dinámico implementa un mecanismo de "primera llegada" para **Port Security** (Seguridad de puertos). Usted especificará cuántas direcciones se pueden obtener en el puerto bloqueado. Si no se ha alcanzado el límite, se obtendrá y se reenviará normalmente un paquete con una dirección MAC de origen desconocida. Una vez alcanzado el límite, no se obtendrán más direcciones en el puerto. Los paquetes con direcciones MAC de origen que no se hayan obtenido quedarán descartados. Tenga en cuenta que puede desactivar el bloqueo dinámico de forma eficaz definiendo el número de entradas dinámicas permitidas en cero.

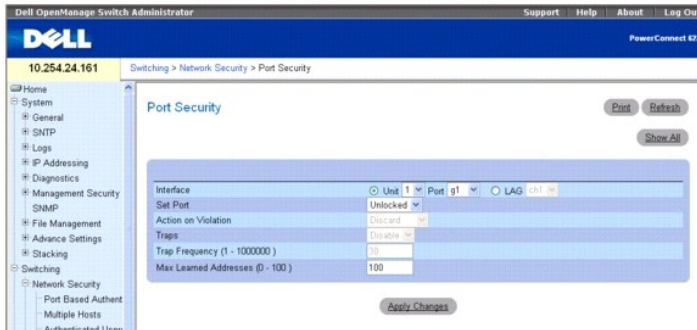
El bloqueo estático permite especificar una lista de direcciones MAC permitidas en un puerto. El comportamiento de los paquetes es el mismo que en el caso del bloqueo dinámico: sólo se pueden reenviar los paquetes con una dirección MAC de origen permitida.

Para ver la dirección MAC obtenida en un puerto específico, añadir una dirección MAC estática a un puerto o suprimir entradas de MAC estáticas, consulte [Configuración de tablas de direcciones](#).

Los puertos desactivados sólo se pueden activar desde la página *Configuring Ports* (Configuración de puertos).

Para visualizar la página *Port Security* (Seguridad de puertos), haga clic en **Switching** (Conmutación)→ **Network Security** (Seguridad de la red)→ **Port Security** (Seguridad de puertos) en la vista de árbol.

Ilustración 7-6. Seguridad de puertos



Interface (Interfaz): seleccione la unidad y el puerto o el LAG en los que desea configurar la seguridad de puertos.

Set Port (Establecer puerto): activa el bloqueo del puerto/LAG. Cuando se bloquea un puerto, todas las direcciones actuales que se habían obtenido dinámicamente mediante el conmutador de dicho puerto se eliminan de la base de datos.

Action on Violation (Acción tras infracción): especifica la acción que se debe aplicar a los paquetes que llegan al puerto/LAG. Si el puerto/LAG está desbloqueado, el campo aparece atenuado. Los valores posibles son:

Discard (Descartar): descarta los paquetes de cualquier origen no obtenido. Éste es el valor predeterminado.

Forward (Reenviar): reenvía los paquetes de origen desconocido. No se obtiene la dirección MAC.

Shutdown (Apagar): descarta los paquetes de cualquier origen no obtenido y envía una excepción. Además, se desactiva el puerto de entrada.

Traps (Excepciones): activa o desactiva el envío de una excepción cuando se recibe un paquete en un puerto/LAG bloqueado.

Trap Frequency (1–1000000) (Frecuencia de excepciones [1–1000000]): indica el período (en segundos) que transcurrirá entre las excepciones.

Max Learned Addresses (0–100) (Número máximo de direcciones obtenidas [0–100]): especifica el número máximo de direcciones MAC seguras que pueden obtenerse en un puerto.

Definición de un puerto bloqueado

1. Abra la página *Port Security* (Seguridad de puertos).
2. Seleccione un número y tipo de interfaz.
3. Seleccione **Locked** (Bloqueado) en el menú desplegable **Set Port** (Establecer puerto).
4. Complete los campos restantes.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto/LAG bloqueado se añade a la tabla de seguridad de puertos y se actualiza el dispositivo.

Visualización de la tabla de seguridad de puertos

1. Abra la página *Port Security* (Seguridad de puertos).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página *Port Security Table* (Tabla de seguridad de puertos).

Ilustración 7-7. Tabla de seguridad de puertos

Port Security Table Print Refresh

Unit

Ports	Current Port Control	Set Port	Set Port Action	Trap	Trap Frequency	Edit
1 1/g1	Link Up	Unblock	Discard	Disable	30	<input type="checkbox"/>
2 1/g2	Link Down	Unblock	Discard	Disable	30	<input type="checkbox"/>
3 1/g3	Link Up	Unblock	Discard	Disable	30	<input type="checkbox"/>

26 1/g2	Link Down	Unblock	Discard	Disable	30	<input type="checkbox"/>
27 1/g3	Link Down	Unblock	Discard	Discard	30	<input type="checkbox"/>
28 1/g4	Link Down	Unblock	Discard	Discard	30	<input type="checkbox"/>

Apply Changes Back

- Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de seguridad de puertos correspondiente a otras unidades de la pila, en caso de que existan.

Definición de varios puertos bloqueados

- Abra la página **Port Security** (Seguridad de puertos).
- Haga clic en **Show All** (Mostrar todo).
Aparece la página **Port Security Table** (Tabla de seguridad de puertos).
- Haga clic en **Edit** (Editar) para cada puerto cuyos parámetros desee cambiar.
- Ahora puede editar los campos necesarios para dichos puertos.
- Haga clic en **Apply Changes** (Aplicar cambios).

Los cambios se aplican a la tabla de seguridad de puertos y se actualiza el dispositivo.

Configuración de la seguridad de puertos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de la tabla de direcciones

Filtrado de DHCP

El filtrado de DHCP es una función muy útil que puede utilizarse como medida de seguridad frente a servidores DHCP no autorizados. Cuando un servidor DHCP no autorizado responde a un cliente que solicita una dirección IP se produce lo que se denomina un ataque conocido. El servidor configura la puerta de enlace para el cliente de modo que sea igual a la dirección IP del servidor. En ese momento, el cliente envía a la máquina no autorizada todo su tráfico IP destinado a otras redes. Esto permite al atacante inspeccionar el tráfico para obtener contraseñas o realizar un ataque de hombre en el medio. Con el filtrado de DHCP, el administrador puede configurar cada puerto como un puerto de confianza o como un puerto no de confianza. El puerto que tiene el servidor DHCP autorizado debe configurarse como puerto de confianza. Todas las respuestas DHCP recibidas en un puerto de confianza se reenvían. Todos los demás puertos deben configurarse como no de confianza. Todas las respuestas DHCP (o BootP) recibidas se descartan.

Para visualizar la página **DHCP Filtering** (Filtrado de DHCP), haga clic en **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **DHCP Filtering** (Filtrado de DHCP) en la vista de árbol.

Ilustración 7-8. Filtrado de DHCP



La página **DHCP Filtering** (Filtrado de DHCP) contiene los campos siguientes:

DHCP Filtering Global Mode (Modo global de filtrado de DHCP): activa y desactiva el filtrado de DHCP. El valor predeterminado es Disabled (Desactivado).

Interface (Interfaz): especifica la unidad y el puerto o LAG afectados. Seleccione la unidad y el puerto o LAG que desee en los menús desplegables.

DHCP Trust Mode (Modo de confianza de DHCP): activa o desactiva el modo de confianza. El valor predeterminado es Disable (Desactivar).

Adición de filtrado de DHCP

1. Abra la página **DHCP Filtering** (Filtrado de DHCP).
2. Especifique la **Interface** (Interfaz) o el **LAG** afectado.
3. Defina los valores que desee para **DHCP Filtering Global Mode** (Modo global de filtrado de DHCP) y **DHCP Filtering Trust Mode** (Modo de confianza de filtrado de DHCP).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se actualizará el dispositivo.

Visualización de la tabla de configuración de la interfaz de filtrado de DHCP

1. Abra la página **DHCP Filtering** (Filtrado de DHCP).
2. Haga clic en **Show All** (Mostrar todo).

La página **DHCP Filtering Table** (Tabla de filtrado de DHCP) muestra todos los puertos, las unidades donde se encuentran y sus modos de confianza de DHCP.

Ilustración 7-9. Tabla de configuración de la interfaz de filtrado de DHCP

Unit	Port	DHCP Trust Mode	Edit
1	1/31	<input type="checkbox"/>	<input type="checkbox"/>
2	1/32	<input type="checkbox"/>	<input type="checkbox"/>
3	1/33	<input type="checkbox"/>	<input type="checkbox"/>

26	1/32	<input type="checkbox"/>	<input type="checkbox"/>
27	1/33	<input type="checkbox"/>	<input type="checkbox"/>
28	1/34	<input type="checkbox"/>	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de filtrado de DHCP correspondiente a otras unidades de la pila, en caso de que existan.

Configuración del filtrado de DHCP en varios puertos

1. Abra la página **DHCP Filtering** (Filtrado de DHCP).
2. Haga clic en **Show All** (Mostrar todo).
Se muestra la página **DHCP Filtering Interface Configuration Table** (Tabla de configuración de la interfaz de filtrado de DHCP).

3. Haga clic en **Edit** (Editar) para cada puerto que desee configurar.
4. Active o desactive el campo **DHCP Trust Mode** (Modo de confianza de DHCP) según convenga para estos puertos.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se aplican los cambios a la tabla de configuración de la interfaz de filtrado de DHCP y se actualiza el dispositivo.

Configuración del filtrado de DHCP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

Configuración de la ACL 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. Su conmutador admite hasta 100 ACL. Sin embargo, los recursos de hardware son limitados y es posible que no admitan 100 ACL completas en su totalidad.

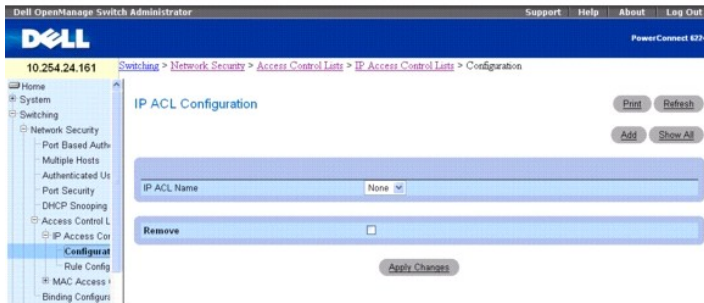
Los paquetes se pueden filtrar en la entrada. Si las reglas de filtrado coinciden, pueden emprenderse algunas acciones, como descartar el paquete o desactivar el puerto. Por ejemplo, un administrador de red define una regla de la ACL según la cual el puerto número 20 puede recibir paquetes TCP. Pero si se recibe un paquete UDP, éste se descarta.

Las ACL están formadas por entradas de control de acceso (ACE), o reglas, compuestas por los filtros que determinan las clasificaciones del tráfico. El número total de reglas que se puede definir para cada ACL es de 10.

Utilice la página **IP ACL Configuration** (Configuración de la ACL IP) para añadir o eliminar ACL basadas en IP.

Para visualizar la página **IP ACL Configuration** (Configuración de la ACL IP), haga clic en **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **Access Control Lists** (Listas de control de acceso) → **IP Access Control Lists** (Listas de control de acceso IP) → **Configuration** (Configuración) en la vista de árbol.

Ilustración 7-10. Configuración de la ACL IP



La página **IP ACL Configuration** (Configuración de la ACL IP) contiene los campos siguientes:

IP ACL Name (Nombre de ACL IP): especifica un nombre definido por el usuario para la ACL.

Remove (Eliminar): elimina la ACL IP seleccionada en el campo IP ACL (ACL IP).

Adición de una ACL basada en IP

1. Abra la página **IP ACL Configuration** (Configuración de la ACL IP).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add IP ACL** (Añadir ACL IP).

Ilustración 7-11. Adición de ACL IP



3. Introduzca el nombre de ACL que desee en el campo de entrada correspondiente.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade la ACL basada en IP y se actualiza el dispositivo.

Eliminación de una ACL basada en IP

1. Abra la página **IP ACL Configuration** (Configuración de la ACL IP) y seleccione la ACL que desea eliminar en el menú desplegable **IP ACL** (ACL IP).
2. Seleccione la casilla de verificación **Remove ACL** (Eliminar ACL).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la ACL basada en IP y se actualiza el dispositivo.

Visualización de ACL IP

1. Abra la página IP ACL Configuration (Configuración de la ACL IP).
2. Haga clic en Show All (Mostrar todo).

Todas las ACL IP y sus datos relacionados se muestran en la página IP ACL Table (Tabla de ACL IP).

Ilustración 7-12. Tabla de ACL IP

IP ACL Name	Rules	Direction	Interface	VLAN
1 ACL1	1	NONE	NONE	NONE
2 ACL2	1	NONE	NONE	NONE

Adición de una ACL basada en IP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos ACL

Configuración de la regla de la ACL IP

Utilice la página IP ACL Rule Configuration (Configuración de la regla de la ACL IP) para definir reglas para ACL basadas en IP. La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple los criterios se reenvía normalmente o se descarta. Además, puede especificar si desea asignar tráfico a una cola concreta, filtrar cierto tráfico, cambiar la etiqueta de VLAN, apagar un puerto o redirigir el tráfico a un puerto concreto.

- ➔ **AVISO:** al final de una lista ACL hay una regla "denegar todo" implícita. Esto significa que si se aplica una ACL a un paquete y ninguna de las reglas explícitas coincide, entonces se aplica la regla final implícita "denegar todo" y el paquete se descarta.

Para visualizar la página IP ACL Rule Configuration (Configuración de la regla de la ACL IP), haga clic en Switching (Conmutación)→ Network Security (Seguridad de la red)→ Access Control Lists (Listas de control de acceso)→ IP Access Control Lists (Listas de control de acceso IP)→ Rule Configuration (Configuración de la regla) en la vista de árbol.

Ilustración 7-13. Configuración de la regla de la ACL IP (estándar)

The screenshot shows the configuration page for an IP ACL rule. The 'IP ACL Name' is set to 'ALCI' and 'Rule ID' is '1'. The 'Action' is set to 'Permit'. Under 'Match Every', the 'Protocol' is set to 'IP'. The 'Source IP Address' is '0.0.0.0' with a 'Wild Card Mask' of '(X.X.X)'. The 'Destination IP Address' is '0.0.0.0' with a 'Wild Card Mask' of '(X.X.X)'. The 'Service Type' is set to 'IP DSCP' with a 'Match to Port' of '(0-63)'. There are also fields for 'IP Precedence' (0-7) and 'IP TOS Bits' (00-FF).

La página IP ACL Rule Configuration (Configuración de la regla de la ACL IP) contiene los campos siguientes:

IP ACL Name (Nombre de ACL IP): especifica una ACL IP existente. Para configurar una nueva ACL IP, utilice la página "[Configuración de la ACL IP](#)".

Rule ID (ID de regla): selecciona o crea ACL definidas por el usuario. Especifique una ID de la regla existente o cree una nueva seleccionando Create (Crear) en el menú desplegable e introduciendo la nueva ID de la regla que desee en el campo contiguo. La nueva ID se crea al hacer clic en Apply Changes (Aplicar cambios). Pueden crearse hasta 10 reglas para cada ACL.

Action (Acción): selecciona la acción de reenvío de la ACL. Seleccione una opción del menú desplegable para aplicar una acción de reenvío. Los valores posibles son:

- Permit** (Permitir): reenvía los paquetes que cumplen los criterios de la ACL.

Deny (Denegar): descarta los paquetes que cumplen los criterios de la ACL.

Assign Queue ID (Asignar ID de cola): haga clic en la casilla de verificación para aplicar este criterio y, a continuación, introduzca un número de identificación del 0 al 6.

Redirect Interface (Interfaz de redirección): seleccione en la lista desplegable una interfaz a la cual puedan redirigirse los paquetes que cumplen esta regla.

Mirror Interface (Interfaz de duplicación): seleccione en la lista desplegable una interfaz en la que puedan duplicarse los paquetes que cumplen esta regla.

Logging (Registro): cuando la casilla de verificación está seleccionada, activa el registro de una ACL concreta. El registro sólo se puede utilizar para la acción de denegar.

Match Every (Coincidir todos): requiere que un paquete cumpla los criterios de esta ACL. Haga clic en la casilla de verificación para aplicar este criterio. La opción Match Every (Coincidir todos) es exclusiva respecto a las demás reglas de filtrado; por lo tanto, si se selecciona, no se podrá acceder a las demás reglas de la pantalla.

Protocol (Protocolo): requiere que el protocolo de un paquete coincida con el protocolo aquí indicado. Haga clic en la casilla de verificación para aplicar este criterio y, a continuación, seleccione una de las opciones siguientes:

Select from List (Seleccionar de la lista): seleccione en la lista desplegable un protocolo en el que pueda basarse la regla.

Match to Value (Coincidir con valor): haga clic aquí para añadir una ID de protocolo definida por el usuario mediante la cual se haga coincidir los paquetes con la regla.

Source IP Address (Dirección IP de origen): requiere que la dirección IP del puerto de origen de un paquete coincida con la dirección aquí indicada. Haga clic en la casilla de verificación y especifique una dirección para aplicar este criterio.

Wild Card Mask (Máscara comodín): especifica la máscara comodín de la dirección IP de origen. Las máscaras comodín determinan qué bits se utilizan y cuáles se ignoran. Una máscara comodín con el valor 255.255.255.255 indica que ningún bit es importante. Un comodín con el valor 0.0.0.0 indica que todos los bits son importantes. Este campo es necesario cuando se ha seleccionado la opción **Source IP Address** (Dirección IP de origen).

Source L4 Port (Puerto L4 de origen): requiere que el puerto de origen TCP/UDP de un paquete coincida con el puerto aquí indicado. Haga clic en la casilla de verificación para aplicar este criterio y seleccione una de las opciones siguientes en el menú desplegable:

Select From List (Seleccionar de la lista): haga clic aquí para seleccionar en la lista un puerto de origen en el que pueda basarse la regla.

Match to Port (Coincidir con puerto): haga clic aquí para añadir una ID de puerto definida por el usuario mediante la cual se haga coincidir los paquetes con la regla.

Destination IP Address (Dirección IP de destino): requiere que la dirección IP del puerto de destino del paquete coincida con la dirección aquí indicada. Haga clic en la casilla de verificación y especifique una dirección para aplicar este criterio.

Wild Card Mask (Máscara comodín): especifica la máscara comodín de la dirección IP de destino. Este campo es necesario cuando se ha seleccionado la opción **Destination IP Address** (Dirección IP de destino).

Destination L4 Port (Puerto L4 de destino): requiere que el puerto de destino TCP/UDP de un paquete coincida con el puerto aquí indicado. Haga clic en la casilla de verificación para aplicar este criterio y, a continuación, seleccione una de las opciones siguientes:

Select From List (Seleccionar de la lista): seleccione en la lista un puerto de destino en el que pueda basarse la regla.

Match to Port (Coincidir con puerto): haga clic aquí para añadir una ID de puerto definida por el usuario mediante la cual se haga coincidir los paquetes con la regla.

Campos de tipo de servicio

Seleccione uno de los tres campos de coincidencia siguientes para usarlo en las coincidencias de paquetes con las ACL:

IP DSCP (DSCP de IP): hace coincidir el valor de DSCP del paquete con la regla. El valor de DSCP o el valor de precedencia IP se usa para establecer coincidencias entre los paquetes y las ACL.

Select From List (Seleccionar de la lista): realice una selección en la lista de valores de palabra clave de DSCP.

Match to Port (Coincidir con puerto): haga clic aquí para añadir una ID de puerto definida por el usuario.

IP Precedence (Precedencia IP): si esta opción está seleccionada, hace coincidir el valor de precedencia IP del paquete con la regla. Especifique el valor de precedencia IP que debe coincidir. El valor de DSCP o el valor de precedencia IP se usa para establecer coincidencias entre los paquetes y las ACL.

IP TOS Bits (Bits de TOS IP): si esta opción está seleccionada, coincide con los bits de tipo de servicio (TOS) de la cabecera IP.

TOS Bits (Bits de TOS): requiere que los bits del campo TOS de un paquete coincidan con el número hexadecimal de dos dígitos aquí especificado.

TOS Mask (Máscara de TOS): especifica las posiciones de bit que se utilizan para la comparación con el campo TOS IP de un paquete.

Remove (Eliminar): elimina una ID de regla cuando se selecciona **Remove** (Eliminar) y se hace clic en **Apply Changes** (Aplicar cambios).

Modificación de una regla basada en IP

 **NOTA:** las reglas sólo se pueden modificar cuando la ACL a la que pertenecen no está vinculada a una interfaz.

1. Abra la página **IP ACL Rule Configuration** (Configuración de la regla de la ACL IP).

2. Seleccione la ACL que desee en el menú desplegable **IP ACL** (ACL IP).
3. Seleccione la regla que desee en el menú desplegable **Rule ID** (ID de regla).
4. Modifique los campos restantes según sea necesario.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la ACL basada en IP y se actualiza el dispositivo.

Adición de una nueva regla a una ACL basada en IP

1. Abra la página **IP ACL Rule Configuration** (Configuración de la regla de la ACL IP).
2. Seleccione la ACL que desee en el menú desplegable **IP ACL** (ACL IP).
3. Seleccione **Create Rule** (Crear regla) en el menú desplegable **Rule ID** (ID de regla) e introduzca un nuevo número de ID.
4. Defina los campos restantes según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva regla se asigna a la ACL basada en IP especificada.

Definición de una regla de la ACL basada en IP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

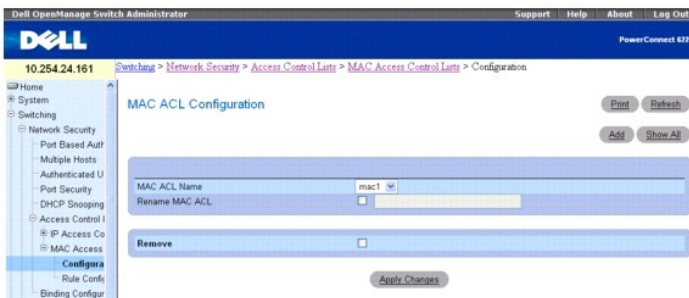
- 1 Comandos ACL

Configuración de la ACL MAC

La página **MAC ACL Configuration** (Configuración de la ACL MAC) permite a los administradores de red definir una ACL basada en MAC. Para obtener una descripción de las listas ACL, consulte "[Configuración de la ACL IP](#)".

Para visualizar la página **MAC ACL Configuration** (Configuración de la ACL MAC), haga clic en **Switching** (Conmutación)→ **Network Security** (Seguridad de la red)→ **Access Control Lists** (Listas de control de acceso)→ **MAC Access Control Lists** (Listas de control de acceso MAC)→ **Configuration** (Configuración) en la vista de árbol.

Ilustración 7-14. Configuración de la ACL MAC



La página **MAC ACL Configuration** (Configuración de la ACL MAC) contiene los campos siguientes:

MAC ACL Name (Nombre de ACL MAC): nombre de la ACL definido por el usuario.

Rename MAC ACL (Cambiar nombre de la ACL MAC): para cambiar el nombre de la ACL MAC, seleccione la casilla de verificación y especifique un nuevo nombre para la ACL MAC en el campo correspondiente.

Remove (Eliminar): haga clic en este campo y, a continuación, haga clic en el botón **Apply Changes** (Aplicar cambios) para eliminar la ACL MAC indicada en el campo **MAC ACL** (ACL MAC).

Adición de una ACL basada en MAC

1. Abra la página **MAC ACL Configuration** (Configuración de la ACL MAC).

- Haga clic en **Add** (Añadir) para visualizar la página **Add MAC ACL** (Añadir ACL MAC).

Ilustración 7-15. Adición de ACL MAC



- Introduzca el nombre de ACL MAC que desee en el campo de entrada.
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se añade la ACL basada en MAC y se actualiza el dispositivo.

Eliminación de una ACL basada en MAC

- Abra la página **MAC ACL Configuration** (Configuración de la ACL MAC) y seleccione la ACL que desea eliminar en el menú desplegable **MACACL** (ACL MAC).
- Seleccione la casilla de verificación **Remove** (Eliminar).
- Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la ACL basada en MAC y se actualiza el dispositivo.

Visualización de ACL MAC

- Abra la página **MAC ACL Configuration** (Configuración de la ACL MAC).
- Haga clic en **Show All** (Mostrar todo).

Aparecerán en pantalla todas las ACL MAC y sus datos relacionados.

Ilustración 7-16. Tabla de ACL MAC



MAC ACL Name	Rules	Direction	Interface	VLAN
big_mac	1	NONE	NONE	

Configuración de ACL basadas en MAC mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

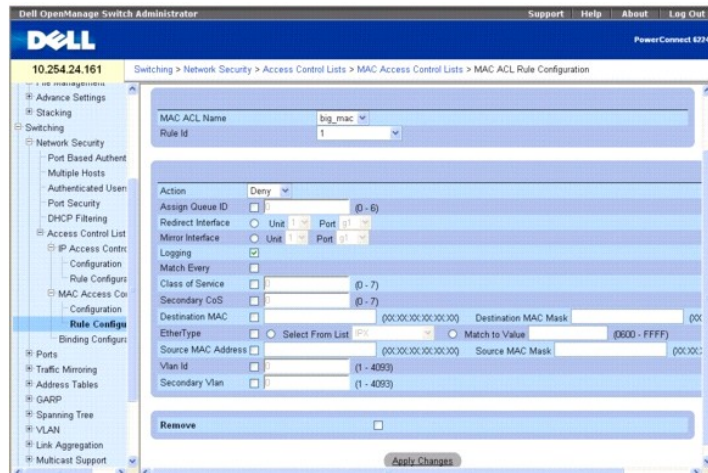
- Comandos ACL

Configuración de la regla de la ACL MAC

Utilice la página **MAC ACL Rule Configuration** (Configuración de la regla de la ACL MAC) para definir reglas para ACL basadas en MAC. La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple los criterios se reenvía normalmente o se descarta. Una regla "denegar todo" predeterminada es la última regla de cada lista.

Para visualizar la página **MAC ACL Rule Configuration** (Configuración de la regla de la ACL MAC), haga clic en **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **Access Control Lists** (Listas de control de acceso) → **MAC Access Control Lists** (Listas de control de acceso MAC) → **Rule Configuration** (Configuración de la regla) en la vista de árbol.

Ilustración 7-17. Configuración de la regla de la ACL MAC



La página **MAC ACL Configuration** (Configuración de la ACL MAC) contiene los campos siguientes:

MAC ACL Name (Nombre de ACL MAC): especifica una ACL MAC existente. Para configurar una nueva ACL MAC, utilice la página [Configuración de la ACL MAC](#).

Rule Id (ID de regla): selecciona o crea ACL definidas por el usuario. Especifique una ID de la regla existente o cree una nueva seleccionando Create (Crear) en el menú desplegable e introduciendo la nueva ID de la regla que desee en el campo contiguo. La nueva ID se crea al hacer clic en Apply Changes (Aplicar cambios).

Action (Acción): selecciona la acción de reenvío de la ACL, que puede tener uno de los valores siguientes:

Permit (Permitir): reenvía los paquetes que cumplen los criterios de la ACL.

Deny (Denegar): descarta los paquetes que cumplen los criterios de la ACL.

Assign Queue ID (Asignar ID de cola): haga clic en la casilla de verificación para aplicar este criterio y, a continuación, introduzca un número de identificación del 0 al 6.

Redirect Interface (Interfaz de redirección): seleccione en la lista desplegable una interfaz a la cual puedan redirigirse los paquetes que cumplen esta regla.

Mirror Interface (Interfaz de duplicación): seleccione en la lista desplegable una interfaz en la que puedan duplicarse los paquetes que cumplen esta regla.

Logging (Registro): haga clic en la casilla de verificación para activar el registro para esta ACL. Esta función sólo se admite para la acción de denegar.

Match Every (Coincidir todos): requiere que un paquete cumpla los criterios de esta ACL. Haga clic en la casilla de verificación para aplicar este criterio.

Class of Service (Clase de servicio): requiere que la clase de servicio (CoS) de un paquete coincida con el valor de CoS aquí indicado. Haga clic en la casilla de verificación y especifique un valor de CoS entre 0 y 7 para aplicar este criterio.

Secondary CoS (CoS secundaria): requiere que la CoS secundaria de un paquete coincida con el valor de CoS aquí indicado. Haga clic en la casilla de verificación y especifique un valor de CoS entre 0 y 7 para aplicar este criterio.

Destination MAC Address (Dirección MAC de destino): requiere que la dirección MAC del puerto de destino de un paquete coincida con la dirección aquí indicada. Haga clic en la casilla de verificación y especifique una dirección para aplicar este criterio.

Destination MAC Mask (Máscara MAC de destino): si lo desea, introduzca la máscara MAC asociada con la dirección MAC de destino con la que debe coincidir.

EtherType: requiere que el valor EtherType de un paquete coincida con el valor EtherType aquí indicado. Haga clic en la casilla de verificación y seleccione una opción de la lista o especifique la ID de EtherType:

Select from List (Seleccionar de la lista): seleccione en el menú desplegable el valor EtherType que desee.

Match to Value (Coincidir con valor): especifique el número de puerto con el que desee hacer coincidir.

Source MAC Address (Dirección MAC de origen): requiere que la dirección MAC del puerto de origen de un paquete coincida con la dirección aquí indicada. Haga clic en la casilla de verificación y especifique una dirección para aplicar este criterio.

Source MAC Mask (Máscara MAC de origen): si lo desea, introduzca la máscara MAC para la dirección MAC de origen con la que debe coincidir.

Vlan Id (ID de VLAN): requiere que la ID de VLAN de un paquete coincida con la ID aquí indicada. Haga clic en la casilla de verificación y especifique la ID de VLAN para aplicar este criterio. Los valores posibles del campo son 1-4093.

Secondary Vlan (VLAN secundaria): requiere que la ID de VLAN secundaria de un paquete coincida con la ID aquí indicada. Haga clic en la casilla de verificación y especifique la ID de VLAN secundaria para aplicar este criterio. Los valores posibles del campo son 1-4093.

Remove (Eliminar): elimina la regla de la ACL MAC cuando se selecciona **Remove** (Eliminar) y se hace clic en **Apply Changes** (Aplicar cambios).

Modificación de una regla basada en MAC

NOTA: las reglas sólo se pueden modificar cuando la ACL a la que pertenecen no está vinculada a una interfaz.

1. Abra la página **MAC ACL Rule Configuration** (Configuración de la regla de la ACL MAC).
2. Seleccione la ACL que desee en el menú desplegable **MAC ACL** (ACL MAC).
3. Seleccione la regla que desee en el menú desplegable **Rule ID** (ID de regla).
4. Modifique los campos restantes según sea necesario.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la ACL basada en MAC y se actualiza el dispositivo.

Adición de una nueva regla a una ACL basada en MAC

1. Abra la página **MAC ACL Rule Configuration** (Configuración de la regla de la ACL MAC).
2. Seleccione la ACL que desee en el menú desplegable **MAC ACL** (ACL MAC).
3. Especifique **Create New Rule** (Crear nueva regla) para **Rule ID** (ID de regla).
4. Especifique un nuevo número de identificación.
5. Defina los campos restantes según convenga.
6. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva regla se asigna a la ACL basada en MAC especificada.

Eliminación de una regla de una ACL basada en MAC

1. Seleccione una ACL.
2. Seleccione una regla en el menú desplegable **Rule ID** (ID de regla).
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la ACL basada en MAC y se actualiza el dispositivo.

Definición de una regla de la ACL basada en MAC mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos ACL

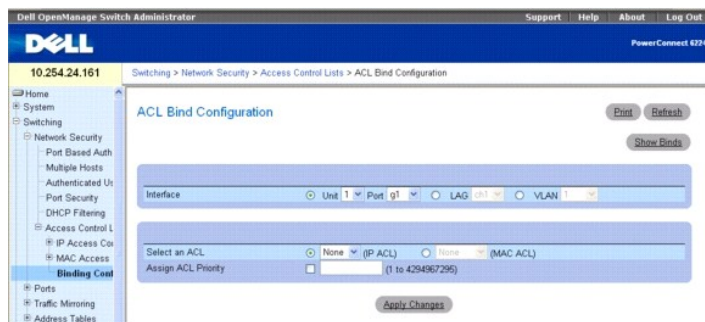
Configuración de vinculaciones de ACL

Cuando una ACL está vinculada a una interfaz, todas las reglas que se han definido se aplican a la interfaz seleccionada. Utilice la página **ACL Bind Configuration** (Configuración de vinculaciones de ACL) para asignar listas ACL a interfaces y prioridades de la ACL.

Desde la interfaz web, puede configurar la regla de la ACL en la dirección de entrada para que dicha regla se aplique a los paquetes que llegan al puerto. Desde la CLI, puede configurar la regla de la ACL en la dirección de entrada o de salida. Las ACL de salida implementan reglas de seguridad en el tráfico que sale del puerto. Puede aplicar ACL a cualquier interfaz física (incluida la 10G), LAG o puerto de enrutamiento.

Para visualizar la página **ACL Bind Configuration** (Configuración de vinculaciones de ACL), haga clic en **Switching** (Conmutación)→ **Network Security** (Seguridad de la red)→ **Access Control Lists** (Listas de control de acceso)→ **Binding Configuration** (Configuración de vinculaciones) en la vista de árbol.

Ilustración 7-18. Configuración de vinculaciones de ACL



La página **ACL Bind Configuration** (Configuración de vinculaciones de ACL) contiene los campos siguientes:


Interface (Interfaz): los botones de radio permiten seleccionar la interfaz por unidad/puerto, LAG o VLAN.

Select an ACL (Seleccionar una ACL): selecciona el tipo de ACL con el que se hacen coincidir los paquetes entrantes. Los paquetes pueden coincidir con ACL basadas en IP o en MAC.

Assign ACL Priority (Asignar prioridad de ACL): asigna la prioridad de esta ACL. Si se aplica más de una ACL a una interfaz, primero se comprueban los criterios de coincidencia para las ACL con mayor prioridad.

Asignación de una ACL a una interfaz

1. Abra la página **ACL Bind Configuration** (Configuración de vinculaciones de ACL).
2. En el campo **Interface** (Interfaz), especifique la unidad y puerto, el LAG o la VLAN que desea configurar.
3. Seleccione la ACL IP o MAC en el campo **Select an ACL** (Seleccionar una ACL).

 **NOTA:** cuando se asigna una ACL en un puerto, LAG o VLAN, los flujos de esa interfaz de entrada que no coinciden con la ACL se hacen coincidir con la regla predeterminada, que es Drop unmatched packets (Descartar paquetes no coincidentes).

4. Especifique la prioridad en **Assign ACL Priority** (Asignar prioridad de ACL).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La ACL se vincula a las interfaces especificadas.

Eliminación de una interfaz de una ACL

1. Abra la página **ACL Bind Configuration** (Configuración de vinculaciones de ACL).
2. Haga clic en **Show All** (Mostrar todo).
3. En el campo **Interface** (Interfaz), especifique la unidad y puerto, el LAG o la VLAN para ver las vinculaciones de ACL para la interfaz en cuestión.
4. Seleccione la casilla de verificación **Remove** (Eliminar) correspondiente a una o varias de las ACL que desee eliminar.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Las ACL especificadas se eliminan de la interfaz.

Asignación de pertenencia a ACL mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos ACL

Configuración de puertos


La página de menú **Ports** (Puertos) proporciona enlaces para funciones de configuración de puertos, que incluyen funciones avanzadas como el control de tormentas y la duplicación de puertos, así como funciones para realizar pruebas de puertos virtuales.

Para visualizar la página, haga clic en **Switching** (Conmutación)→ **Ports** (Puertos) en la vista de árbol. La página de menú **Ports** (Puertos) contiene enlaces a las funciones siguientes:

- 1 [Parámetros globales](#)
- 1 [Configuración de puertos](#)
- 1 [Configuración de puertos protegidos](#)
- 1 [Configuración de LAG](#)
- 1 [Control de tormentas](#)

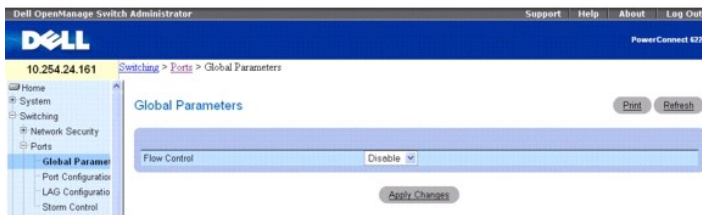
Parámetros globales

Use los parámetros globales para configurar el control de flujo. El control de flujo permite regular el tráfico de un conmutador durante un periodo de tiempo específico, y se define para conmutadores conectados directamente. El control de flujo sólo se puede definir para puertos configurados con modo de funcionamiento dúplex completo. Dado que los puertos en los que se ha definido negociación automática no se pueden añadir como miembros de LAG, el control de flujo de los puertos que pertenecen a LAG no puede estar configurado en modo automático.

 **NOTA:** el control de flujo es incompatible con el modo de prevención de bloqueo de cabecera de línea. El conmutador puede funcionar en cualquiera de los modos, pero no al mismo tiempo.

Para visualizar la página **Global Parameters** (Parámetros globales), haga clic en **Switching** (Conmutación)→ **Ports** (Puertos)→ **Global Parameters** (Parámetros globales) en la vista de árbol.

Figure 7-19. Parámetros globales de puertos



La página **Global Parameters** (Parámetros globales) contiene el campo siguiente:

Flow Control (Control de flujo): seleccione **Enabled** (Activado) o **Disabled** (Desactivado) en el menú desplegable. Este comando afecta a todos los puertos de la pila. El valor predeterminado es **Enabled** (Activado).

Enable (Activar): activa el mecanismo de contrapresión de entrada del conmutador.

Disable (Desactivar): restaura el funcionamiento del conmutador al modo de prevención de bloqueo de cabecera de línea.

Activación de la contrapresión de entrada

1. Abra la página **Ports Global Parameters** (Parámetros globales de puertos).
2. Seleccione **Enable** (Activar) en el menú desplegable del campo **Flow Control** (Control de flujo).
3. Haga clic en **Apply Changes** (Aplicar cambios).
4. La contrapresión de entrada está ahora activada.

Configuración del control de flujo mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

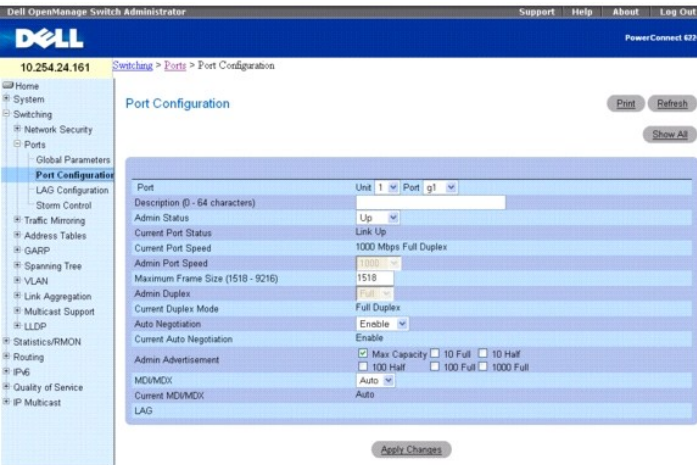
- 1 Comandos de configuración de Ethernet

Configuración de puertos

Utilice la página **Port Configuration** (Configuración de puertos) para definir los parámetros de los puertos.

Para visualizar la página **Port Configuration** (Configuración de puertos), haga clic en **Switching** (Conmutación)→ **Ports** (Puertos)→ **Port Configuration** (Configuración de puertos) en la vista de árbol.

Ilustración 7-20. Configuración de puertos



La página **Port Configuration** (Configuración de puertos) contiene los campos siguientes:

Port (Puerto): especifica la unidad y el puerto para los que se definen los parámetros de puerto.

Description (0–64 Characters) (Descripción [0–64 caracteres]): ofrece una breve descripción de la interfaz, como por ejemplo Ethernet.

Admin Status (Estado de administración): activa (Up) o desactiva (Down) el reenvío de tráfico a través del puerto.

Current Port Status (Estado actual del puerto): especifica si el puerto está operativo o no actualmente.

Current Port Speed (Velocidad actual del puerto): muestra la velocidad del puerto sincronizada real (en bps).

Admin Port Speed (Velocidad del puerto administrativo): fuerza la velocidad del puerto al valor seleccionado: 10 M, 100 M, 1000 M o 10000 M.

Maximum Frame Size (1518–9216) (Tamaño máximo de trama [1518-9216]): los paquetes que superen el tamaño especificado por este umbral se descartarán. El valor predeterminado es 1518.

Admin Duplex (Dúplex de administrador): especifica el modo dúplex del puerto. Las opciones son Full (Dúplex completo) o Half (Semidúplex).

Full (Dúplex completo): indica que la interfaz admite la transmisión entre el conmutador y el cliente en ambas direcciones simultáneamente.

Half (Semidúplex): indica que la interfaz admite la transmisión entre el conmutador y el cliente en una sola dirección cada vez.

Current Duplex Mode (Modo dúplex actual): muestra el modo dúplex sincronizado del puerto.

Auto Negotiation (Negociación automática): activa la negociación automática en el puerto. La negociación automática es un protocolo entre dos enlaces asociados que permite que un puerto anuncie sus capacidades de velocidad de transmisión, modo dúplex y control de flujo a su asociado.

Current Auto Negotiation (Negociación automática actual): muestra la configuración actual de la negociación automática.

Admin Advertisement (Anuncio de administración): especifica las funciones que debe anunciar el puerto. Los valores del campo posibles son:

Max Capability (Capacidad máxima): indica que pueden aceptarse todas las velocidades de puerto y todos los ajustes de modo dúplex.

10 Half (Semidúplex 10): indica que el puerto anuncia una velocidad de 10 Mbps y una configuración en modo semidúplex.

10 Full (Dúplex completo 10): indica que el puerto anuncia una velocidad de 10 Mbps y una configuración en modo dúplex completo.

100 Half (Semidúplex 100): indica que el puerto anuncia una velocidad de 10 Mbps y una configuración en modo semidúplex.

100 Full (Dúplex completo 100): indica que el puerto anuncia una velocidad de 10 Mbps y una configuración en modo dúplex completo.

1000 Full (Dúplex completo 1000): indica que el puerto anuncia una velocidad de 10 Mbps y una configuración en modo dúplex completo.

MDI/MDX: permite que el conmutador descifre entre cables cruzados y no cruzados.

Los concentradores y conmutadores se cablean deliberadamente en el sentido opuesto al cableado de las estaciones finales, de modo que cuando se conecta un concentrador o conmutador a una estación final, se puede usar un cable Ethernet directo y los pares coinciden correctamente. Cuando se conectan dos concentradores/conmutadores entre sí o dos estaciones finales entre sí, se utiliza un cable cruzado para garantizar que se conecten los pares correctos.

Los valores posibles son:

On (Activado): permite al conmutador detectar el tipo de conexión.

Off (Desactivado): requiere el tipo de cable correcto para la conexión al conmutador.

Auto (Automático): el valor se define automáticamente.

Current MDI/MDX (MDI/MDX actual): indica los valores actuales de MDX del conmutador. Los valores del campo posibles son:

MDI: el valor actual de MDI es MDI.

MDX: el valor actual de MDI es MDX.

Auto (Automático): el valor se define automáticamente.

LAG: muestra el número de LAG si este puerto forma parte de un LAG.

Definición de los parámetros de puertos

1. Abra la página **Port Configuration** (Configuración de puertos).
 2. Seleccione una unidad y un puerto en los campos **Unit** (Unidad) y **Port** (Puerto).
 3. Defina los campos disponibles en la pantalla.
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Los parámetros del puerto se guardan en el conmutador.

Visualización de la tabla de puertos

1. Abra la página **Port Configuration** (Configuración de puertos).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **Port Configuration Table** (Tabla de configuración de puertos).

Ilustración 7-21. Tabla de configuración de puertos

Port	Port Status	Port Speed	Max Frame Size	Duplex Mode	Auto Negotiation	Flow Control	MDI/MDX	Copy To	Edit
1 1/1g1	Up	1000	1518	Full	Disable	Disable	Auto		
2 1/1g2	Up	10	1518	Full	Disable	Disable	Auto		
3 1/1g3	Up	100	1518	Full	Disable	Disable	Auto		
2/1ag2	Up	10	1518	Full	Disable	Disable	Auto		
2/1ag3	Up	10	1518	Full	Disable	Disable	Auto		
2/1ag4	Up	10	1518	Full	Disable	Disable	Auto		

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de configuración de puertos correspondiente a otras unidades de la pila, en caso de que existan.

Copia de los valores de configuración de puertos

1. Abra la página **Port Configuration** (Configuración de puertos).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **Port Configuration Table** (Tabla de configuración de puertos).
3. Especifique la unidad y el puerto de los que está copiando en **Copy Parameters From** (Copiar parámetros de).
 4. Haga clic en **Copy To** (Copiar en) para cada puerto que deba recibir estos parámetros.
 5. Haga clic en **Apply Changes** (Aplicar cambios).

Se copian los valores de configuración de los puertos y se actualiza el dispositivo.

Modificación de los valores de configuración de puertos para varios puertos

1. Abra la página **Port Configuration** (Configuración de puertos).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **Port Configuration Table** (Tabla de configuración de puertos).
3. Haga clic en **Edit** (Editar) para cada puerto que desee modificar.
 4. Edite los campos de configuración de puertos según convenga.
 5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los valores de configuración de los puertos y se actualiza el dispositivo.

Configuración de puertos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

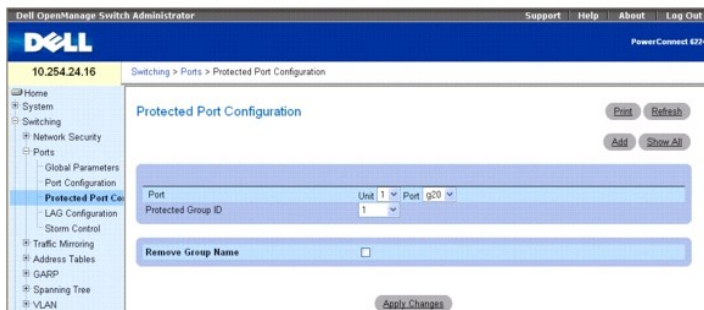
- 1 Comandos de configuración de Ethernet

Configuración de puertos protegidos

Utilice la página **Protected Port Configuration** (Configuración de puertos protegidos) para especificar una función de seguridad de nivel 2, puertos PVE (Private VLAN Edge), que proporcione seguridad basada en puertos entre los puertos que son miembros de la misma VLAN. 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 visualizar la página **Port Configuration** (Configuración de puertos), haga clic en **Switching** (Conmutación) → **Ports** (Puertos) → **Protected Port Configuration** (Configuración de puertos protegidos) en la vista de árbol.

Ilustración 7-22. Configuración de puertos protegidos



La página **Protected Port Configuration** (Configuración de puertos protegidos) contiene los campos siguientes:

Port (Puerto): especifica la unidad y el puerto para los que se definen los parámetros de puerto.

Protected Group ID (ID de grupo protegido): menú desplegable que se utiliza para asignar un puerto al grupo 0, 1 o 2.

Remove Group Name (Eliminar nombre de grupo): marque esta casilla de verificación para desasociar el puerto seleccionado del grupo protegido.

Visualización de la tabla de puertos protegidos

1. Abra la página **Protected Port Configuration** (Configuración de puertos protegidos).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Protected Ports Summary Table** (Tabla de resumen de puertos protegidos).

Ilustración 7-23. Tabla de resumen de puertos protegidos

Protected Ports Summary Done Default

Unit: 1

Port	Group ID	Group Name	Remove
1 1/1			<input type="checkbox"/>
2 1/2			<input type="checkbox"/>
3 1/3			<input type="checkbox"/>
4 1/4	2	Jamestown	<input type="checkbox"/>
5 1/5			<input type="checkbox"/>
6 1/6			<input type="checkbox"/>

24 1/24			<input type="checkbox"/>
25 1/25			<input type="checkbox"/>
26 1/26			<input type="checkbox"/>
27 1/27			<input type="checkbox"/>
28 1/28			<input type="checkbox"/>

Apply Changes Back

3. Seleccione la casilla de verificación **Remove** (Eliminar) y haga clic en **Apply Changes** (Aplicar cambios) para desasociar un puerto de un grupo protegido.
4. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de resumen de puertos protegidos correspondiente a otras unidades de la pila, en caso de que existan.

Adición de grupos de puertos protegidos

1. Abra la página **Protected Port Configuration** (Configuración de puertos protegidos).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add Protected Group** (Añadir grupo protegido).

Ilustración 7-24. Adición de puerto protegido

Add Protected Group Done Default

Protected Group ID (0-2): 2

Protected Group Name (1-32 characters): Jamestown

Apply Changes Back

3. Utilice el menú desplegable para asignar la designación numérica 0, 1 o 2 a la ID de grupo protegido (**Protected Group ID**).
4. Introduzca un valor en **Protected Group Name (1–32 characters)** (Nombre de grupo protegido [1-32 caracteres]).
5. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración del grupo protegido se copia y se actualiza el dispositivo.

Configuración de puertos protegidos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

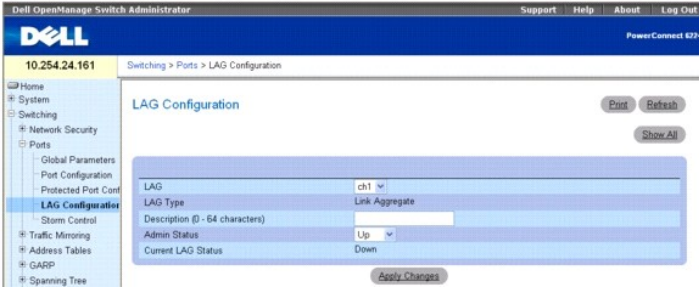
- 1 Comandos switchport protected

Configuración de LAG

La agregación de enlaces permite agregar uno o varios enlaces Ethernet en modo dúplex completo para formar un grupo de agregación de enlaces (LAG). El conmutador puede tratar el LAG como si fuera un único enlace.

Para visualizar la página **LAG Configuration** (Configuración de LAG), haga clic en **Switching** (Conmutación) → **Ports** (Puertos) → **LAG Configuration** (Configuración de LAG) en la vista de árbol.

Ilustración 7-25. Configuración de LAG



La página **LAG Configuration** (Configuración de LAG) contiene los campos siguientes:

LAG: contiene una lista de números de LAG.

LAG Type (Tipo de LAG): tipos de puerto que componen el LAG.

Description (0–64 Characters) (Descripción [0–64 caracteres]): descripción del puerto.

Admin Status (Estado de administración): activa o desactiva el reenvío de tráfico a través del LAG seleccionado.

Current LAG Status (Estado de LAG actual): indica si el LAG seleccionado está activado (Up) o desactivado (Down).

Definición de los parámetros de LAG

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Seleccione un LAG en el campo **LAG**.
3. Defina los campos disponibles en la pantalla.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG se guardan en el conmutador.

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).
3. Aparece la página **LAG Configuration Table** (Tabla de configuración de LAG).

Ilustración 7-26. Tabla de configuración de LAG

LAG Configuration Table Print Refresh

LAG	Description	LAG Type	Admin Status	Current Flow Control	Edit
1 lag1		Link Aggregation	Up	Disable	<input type="checkbox"/>
2 lag2		Link Aggregation	Up	Disable	<input type="checkbox"/>
3 lag3		Link Aggregation	Up	Disable	<input type="checkbox"/>
4 lag4		Link Aggregation	Up	Disable	<input type="checkbox"/>
5 lag5		Link Aggregation	Up	Disable	<input type="checkbox"/>
6 lag6		Link Aggregation	Up	Disable	<input type="checkbox"/>
7 lag7		Link Aggregation	Up	Disable	<input type="checkbox"/>
8 lag8		Link Aggregation	Up	Disable	<input type="checkbox"/>

Apply Changes Back

Edición de los parámetros de LAG

1. Abra la página **LAG Configuration** (Configuración de LAG).
2. Haga clic en **Show All** (Mostrar todo).
3. Aparece la página **LAG Configuration Table** (Tabla de configuración de LAG).
4. Seleccione **Edit** (Editar) para todos los LAG que vaya a modificar.

5. Ahora puede editar **Admin Status** (Estado de administración) y **Description** (Descripción) según convenga.

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

Los parámetros de LAG se guardan en el conmutador.

Configuración de LAG mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de canal de puerto

Control de tormentas

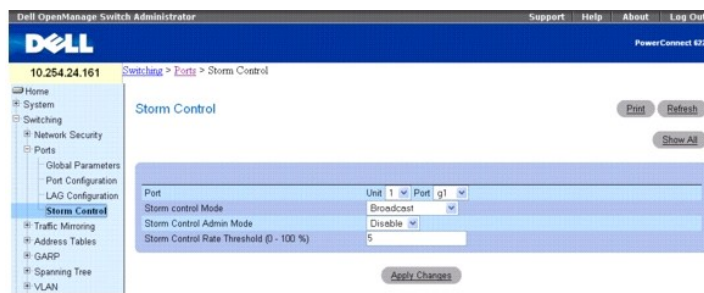
Una tormenta de difusión es el resultado de un número excesivo de mensajes de difusión transmitidos de forma simultánea a través de una red mediante un único puerto. Las respuestas a mensajes reenviados pueden sobrecargar los recursos de red o provocar que se agote el tiempo de espera.

El conmutador mide la velocidad de los paquetes de difusión, multidifusión y difusión única desconocida entrantes para cada puerto y descarta los paquetes cuando la velocidad sobrepasa el valor definido. El control de tormentas se activa en cada interfaz mediante la definición del tipo de paquete y la velocidad de transmisión de los paquetes.

Utilice la página **Storm Control** (Control de tormentas) para activar y configurar el control de tormentas.

Para visualizar la interfaz **Storm Control** (Control de tormentas), haga clic en **Switching** (Conmutación) → **Ports** (Puertos) → **Storm Control** (Control de tormentas) en la vista de árbol.

Ilustración 7-27. Control de tormentas



La página **Storm Control** (Control de tormentas) contiene los campos siguientes:

Port (Puerto): especifica la unidad y el puerto para los que está activado el control de tormentas.

Storm Control Mode (Modo de control de tormentas): especifica el modo de difusión al que se aplica el control de tormentas.

Broadcast (Difusión): si la velocidad del tráfico de difusión de L2 de entrada en una interfaz supera el umbral configurado, el tráfico se descartará.

Multicast (Multidifusión): si la velocidad del tráfico de multidifusión de L2 de entrada en una interfaz supera el umbral configurado, el tráfico se descartará.

Unknown Unicast (Difusión única desconocida): si la velocidad del tráfico de difusión única desconocida de L2 (error en la búsqueda de destino) de entrada en una interfaz supera el umbral configurado, el tráfico se descartará.

Storm Control Admin Mode (Modo de administración de control de tormentas): activa o desactiva el control de tormentas.

Storm Control Rate Threshold (0-100%) (Umbral de velocidad del control de tormentas [0-100%]): especifica la velocidad máxima a la que se reenvían los paquetes desconocidos. El intervalo es un porcentaje del umbral total.

Definición de los parámetros de puerto de control de tormentas

1. Abra la interfaz **Storm Control** (Control de tormentas).

2. Edite los campos en la pantalla.

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

Los parámetros de puerto de control de tormentas se guardan en el conmutador.

Visualización de la tabla de configuración de control de tormentas

1. Abra la interfaz **Storm Control** (Control de tormentas).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Storm Control Settings Table** (Tabla de configuración de control de tormentas).

Ilustración 7-28. Tabla de configuración de control de tormentas

Storm Control Settings Table Print Refresh

Unit 1

Unit		Broadcast Control Mode	Broadcast Rate Threshold	Multicast Control Mode	Multicast Rate Threshold	Unicast Control Mode	Unicast Rate Threshold	Edit
1	1/fg1	Disable	5	Disable	5	Disable	5	<input checked="" type="checkbox"/>
2	1/fg2	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
3	1/fg3	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>

26	1/fg2	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
27	1/fg3	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
28	1/fg4	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>

Apply Changes Back

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de configuración de control de tormentas correspondiente a otras unidades de la pila, en caso de que existan.

Modificación del control de difusión

1. Abra la interfaz **Storm Control** (Control de tormentas).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **Storm Control Settings Table** (Tabla de configuración de control de tormentas).
3. Seleccione **Edit** (Editar) para cada puerto cuyo **Broadcast Control** (Control de difusión) vaya a modificar.
 4. Edite el **Broadcast Control** (Control de difusión) según convenga.
 5. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de puerto de control de tormentas se guardan en el conmutador.

Configuración del control de tormentas mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de configuración de Ethernet

Configuración de la duplicación de tráfico

La duplicación de tráfico permite al usuario configurar el conmutador para que envíe copias de paquetes de un puerto que se está duplicando al puerto de duplicación. La duplicación se puede basar en puerto o bien en flujo.

Utilice la página de menú **Traffic Mirroring** (Duplicación de tráfico) para definir sesiones de duplicación de puertos y configurar la duplicación basada en flujo.

Para visualizar la página, haga clic en **Switching** (Conmutación) → **Traffic Mirroring** (Duplicación de tráfico) en la vista de árbol. La página de menú **Traffic Mirroring** (Duplicación de tráfico) contiene enlaces a las funciones siguientes:

- 1 [Duplicación de puertos](#)
- 1 [Duplicación basada en flujo](#)

Duplicación de puertos

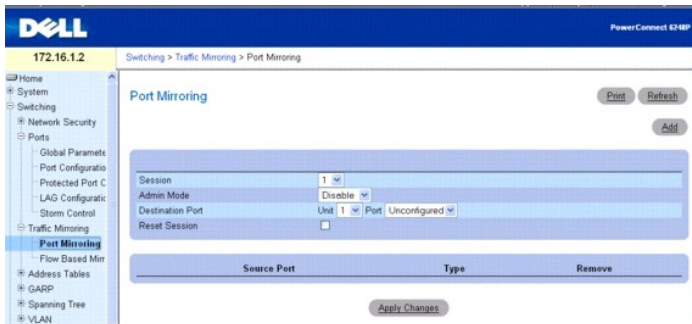
La duplicación de puertos selecciona el tráfico de red para que lo analice un analizador de redes. Este proceso se lleva a cabo para puertos concretos del conmutador. Muchos puertos de conmutación están configurados como puertos de origen y un puerto de conmutación está configurado como puerto de destino. Usted puede configurar el modo de duplicación del tráfico en un puerto de origen. Los paquetes que se reciben en el puerto de origen, que se transmiten a un puerto, o que se reciben y transmiten, pueden duplicarse en el puerto de destino.

El paquete que se copia en el puerto de destino tiene el mismo formato que el paquete original del cable. Esto significa que si el duplicado copia un paquete recibido, el paquete copiado se etiquetará como VLAN o se marcará sin etiqueta como si se recibiera en el puerto de origen. Si el duplicado copia un paquete

transmitido, el paquete copiado se etiquetará como VLAN o se marcará sin etiqueta como si se transmitiera al puerto de origen.

Para visualizar la página **Port Mirroring** (Duplicación de puertos), haga clic en **Switching** (Conmutación)→ **Traffic Mirroring** (Duplicación de tráfico)→ **Port Mirroring** (Duplicación de puertos) en la vista de árbol.

Ilustración 7-29. Duplicación de puertos



La página **Port Mirroring** (Duplicación de puertos) contiene los campos siguientes:

Session (Sesión): especifica la sesión de supervisión.

Admin Mode (Modo de administración): activa o desactiva la duplicación de puertos.

Destination Port (Puerto de destino): seleccione el puerto en el que se puede copiar el tráfico del puerto.

Reset Session (Restablecer sesión): permite restablecer la sesión de supervisión del puerto.

Source Port (Puerto de origen): enumera los puertos de origen que se han añadido de la página **Add Source Port** (Añadir puerto de origen).

Type (Tipo): muestra el tipo de tráfico supervisado en el puerto de origen.

Adición de una sesión de duplicación de puertos

NOTA: un puerto se elimina de una red VLAN o de un LAG cuando se convierte en duplicado de destino.

1. Abra la página **Port Mirroring** (Duplicación de puertos).
2. Haga clic en **Add** (Añadir) para visualizar la página **Add Source Port** (Añadir puerto de origen).

Ilustración 7-30. Adición de puerto de origen



3. Configure los campos siguientes:

Session (Sesión): seleccione la sesión que desea supervisar.

Source Port (Puerto de origen): seleccione la unidad y el puerto desde los que se va a duplicar el tráfico. Pueden duplicarse hasta cuatro puertos de origen en un puerto de destino.

Type (Tipo): especifica el tipo de tráfico supervisado. Los valores del campo posibles son:

TX: sólo supervisa paquetes transmitidos.

RX: sólo supervisa paquetes recibidos.

TX and RX (TX y RX): supervisa tanto paquetes transmitidos como recibidos.

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

Se activa la nueva sesión de duplicación de puertos para la unidad y el puerto en cuestión y se actualiza el dispositivo. El puerto de origen aparece en la tabla **Source Port** (Puerto de origen) de la página **Port Mirroring** (Duplicación de puertos).

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).

Se modifican los campos correspondientes a la sesión de duplicación de puertos y se actualiza el dispositivo.

Eliminación de una sesión de duplicación de puertos

1. Abra la página **Port Mirroring** (Duplicación de puertos).
2. Seleccione la casilla de verificación **Reset Session** (Restablecer sesión).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la sesión de duplicación de puertos y se actualiza el dispositivo.

Configuración de una sesión de duplicación de puertos mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de supervisión de puertos

Duplicación basada en flujo

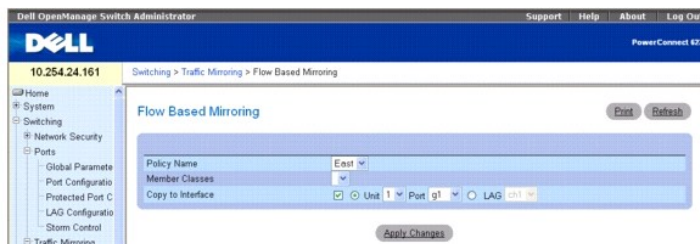
La función de duplicación basada en flujo toma como punto de partida el componente de servicios diferenciados de QoS. En QoS, el usuario crea clases de tráfico para definir criterios de coincidencia y, luego, políticas para definir la acción que debe llevarse a cabo en esa clase de tráfico.

La duplicación basada en flujo permite al usuario copiar algunos tipos de tráfico en un único puerto de destino. Esto ofrece flexibilidad, puesto que en lugar de duplicar todo el tráfico de entrada o de salida en un puerto, el conmutador puede duplicar un subconjunto de ese tráfico. Puede configurar el conmutador para que duplique flujos basados en información de nivel 2, nivel 3 y nivel 4.

Utilice la página **Flow Based Mirroring** (Duplicación basada en flujo) para especificar puertos de duplicación basada en flujo.

Para visualizar la página **Flow Based Mirroring** (Duplicación basada en flujo), haga clic en **Switching** (Conmutación)→ **Traffic Mirroring** (Duplicación de tráfico) → **Flow Based Mirroring** (Duplicación basada en flujo) en la vista de árbol.

Ilustración 7-31. Duplicación basada en flujo



La página **Flow Based Mirroring** (Duplicación basada en flujo) contiene los campos siguientes:

Policy Name (Nombre de política): selecciona una política para asociarla con una clase de tráfico. El nombre de política se define usando la página web "[Configuración de políticas](#)" de servicios diferenciados.

Member Classes (Clases de miembros): selecciona la clase de tráfico asociada con esta política. La clase de miembro se define usando la página web "[Configuración de clases](#)" de servicios diferenciados.

Copy to Interface (Copiar en interfaz): si está seleccionada, esta función permite copiar paquetes en una unidad/puerto o LAG.

Copia de duplicación en un puerto de destino

1. Abra la página **Flow Based Mirroring** (Duplicación basada en flujo).
2. Especifique un valor en **Policy Name** (Nombre de política) y **Member Class** (Clase de miembro) y, a continuación, seleccione la unidad y el puerto de destino que se verán afectados en **Copy to Interface** (Copiar en interfaz).

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

Los detalles de la duplicación basada en flujo se copian en el puerto especificado y el dispositivo se actualiza.

Configuración de duplicación basada en flujo mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de QoS

Configuración de tablas de direcciones

Las direcciones MAC se almacenan en la tabla de direcciones estáticas o dinámicas. Las direcciones estáticas las define el usuario. En cambio, las direcciones dinámicas las obtiene el sistema y se borran tras una expiración de tiempo. Un paquete dirigido a un destino almacenado en una de las tablas se reenvía de inmediato a los puertos. Las tablas de direcciones estáticas y dinámicas pueden ordenarse por interfaz, ID de VLAN o nombre de VLAN. Además, es posible añadir direcciones a las tablas de direcciones estáticas y dinámicas.

Para visualizar la página de menú **Address Tables** (Tablas de direcciones), haga clic en **Switching** (Conmutación) → **Address Tables** (Tablas de direcciones) en la vista de árbol. La página de menú **Address Tables** (Tablas de direcciones) contiene enlaces a las funciones siguientes:

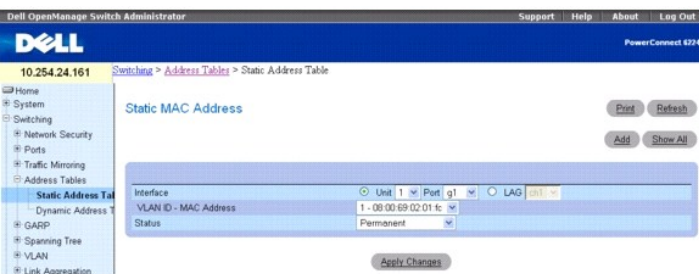
- 1 [Tabla de direcciones estáticas](#)
- 1 [Tabla de direcciones dinámicas](#)

Tabla de direcciones estáticas

La página **Static MAC Address** (Dirección MAC estática) contiene una lista de direcciones MAC estáticas. Una dirección estática se puede añadir y eliminar de la tabla de direcciones MAC estáticas.

Para visualizar la página **Static MAC Address** (Dirección MAC estática), haga clic en **Switching** (Conmutación) → **Address Tables** (Tablas de direcciones) → **Static Address Table** (Tabla de direcciones estáticas) en la vista de árbol.

Ilustración 7-32. Dirección MAC estática



La página **Static MAC Address** (Dirección MAC estática) contiene los campos siguientes:

Interface (Interfaz): especifica la unidad y el puerto o LAG a los que se aplica la dirección MAC estática. Para ver direcciones de una unidad/puerto o LAG diferente, cambie la interfaz que se indica aquí.

VLAN ID - MAC Address (ID de VLAN - Dirección MAC): especifica la ID de VLAN vinculada a la dirección MAC y las direcciones MAC incluidas en la lista actual de direcciones estáticas.

NOTA: sólo se muestran las direcciones MAC asignadas a la VLAN y la interfaz especificadas.

Status (Estado): especifica el estado de la dirección MAC. Los valores posibles son:

Permanent (Permanente): indica que la dirección MAC es permanente.

Secure (Seguro): garantiza que una dirección MAC de puerto bloqueado no se eliminará.

Delete on Reset (Eliminar al restablecer): la dirección MAC se elimina al restablecer el conmutador.

Delete on Timeout (Eliminar al exceder el tiempo de espera): la dirección MAC se elimina cuando se excede el tiempo de espera.

Adición de una dirección MAC estática

1. Abra la página **Static MAC Address** (Dirección MAC estática).

2. Haga clic en **Add** (Añadir).

Aparece la página **Add Static MAC Address** (Añadir dirección MAC estática).

Ilustración 7-33. Adición de dirección MAC estática

The screenshot shows a web interface for adding a static MAC address. The form is titled 'Add Static MAC Address' and has 'Print' and 'Refresh' buttons in the top right. Below the title is a 'New Entry' section with the following fields: 'Interface' (Unit 1, Port g5), 'MAC Address' (08:00:69:02:01:FC), 'VLAN ID' (2), 'VLAN Name' (Default), and 'Status' (Permanent). At the bottom of the form are 'Apply Changes' and 'Back' buttons.

3. Rellene los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección estática nueva se añade a la tabla de direcciones MAC estáticas y se actualiza el dispositivo.

Modificación de una dirección estática en 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).
- Se modifica la dirección MAC estática y se actualiza el dispositivo.

Visualización de la tabla de direcciones MAC estáticas

1. Abra la página **Static MAC Address** (Dirección MAC estática).
2. Haga clic en **Show All** (Mostrar todo).

La página **Static MAC Address Table** (Tabla de direcciones MAC estáticas) muestra todas las direcciones MAC estáticas existentes.

Ilustración 7-34. Tabla de direcciones MAC estáticas

The screenshot shows a table titled 'Static MAC Address Table' with 'Print' and 'Refresh' buttons in the top right. The table has the following columns: MAC, VLAN ID, Interface, Status, and Remove. There are two rows of data:

	MAC	VLAN ID	Interface	Status	Remove
1	08:00:69:02:01:FC	1	1/g5	Permanent	<input type="checkbox"/>
2	08:A6:69:02:01:2B	2	1/g5	Permanent	<input type="checkbox"/>

At the bottom of the table are 'Apply Changes' and 'Back' buttons.

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 la página **Static MAC Address Table** (Tabla de direcciones MAC estáticas).
3. Seleccione la casilla de verificación **Remove** (Eliminar) que corresponda a la dirección que desea eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la dirección estática y se actualiza el dispositivo.

Configuración de los parámetros de direcciones estáticas mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de la tabla de direcciones

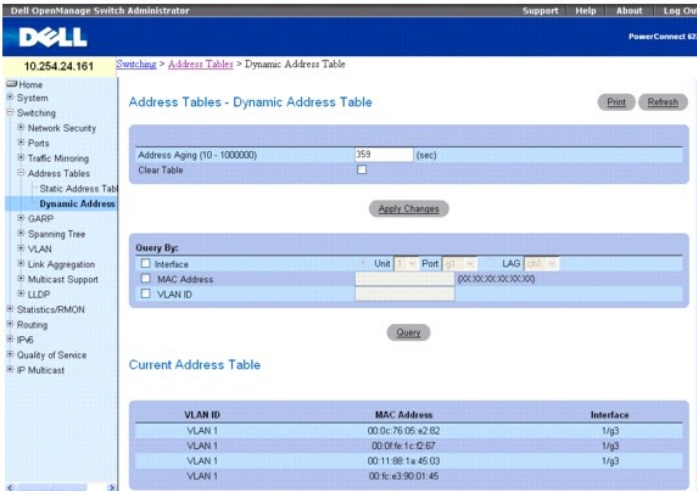
Tabla de direcciones dinámicas

La página **Dynamic Address Table** (Tabla de direcciones dinámicas) contiene campos para realizar consultas sobre datos de la tabla de direcciones dinámicas, como el tipo de interfaz, las direcciones MAC, la VLAN y la clave de ordenación de la tabla. Los paquetes reenviados a una dirección almacenada en la tabla de direcciones se reenvían directamente a esos puertos.

La página **Dynamic Address Table** (Tabla de direcciones dinámicas) también contiene información sobre el tiempo de caducidad que debe transcurrir antes de que una dirección MAC se elimine de la tabla.

Para visualizar la página **Dynamic Address Table** (Tabla de direcciones dinámicas), haga clic en **Switching** (Conmutación) → **Address Tables** (Tablas de direcciones) → **Dynamic Address Table** (Tabla de direcciones dinámicas) en la vista de árbol.

Ilustración 7-35. Tabla de direcciones dinámicas



La página **Dynamic Address Table** (Tabla de direcciones dinámicas) contiene los campos siguientes:

Address Aging (10–1000000) (Duración de direcciones [10–1000000]): especifica el tiempo de caducidad en segundos que debe transcurrir antes de que una dirección MAC dinámica se elimine. El valor predeterminado es 300 segundos.

Clear Table (Borrar tabla): cuando se selecciona esta opción y se hace clic en **Apply Changes** (Aplicar cambios), se borran todos los datos de direcciones MAC dinámicas de la tabla.

La tabla de direcciones dinámicas se puede consultar por:

Interface (Interfaz): especifica la unidad y el puerto a los que se ha consultado una dirección.

LAG: especifica el LAG al que se ha consultado una dirección.

MAC Address (Dirección MAC): especifica la dirección MAC a la que se ha consultado una dirección.

VLAN ID (ID de VLAN): especifica el número de VLAN (a la que está vinculada la dirección MAC) a la que se ha consultado una dirección.

La tabla de dirección actual (**Current Address Table**) contiene parámetros de direcciones dinámicas según los cuales los paquetes se reenvían directamente a los puertos. La tabla de dirección actual contiene los campos siguientes:

VLAN ID (ID de VLAN): muestra el valor de la etiqueta de VLAN.

MAC Address (Dirección MAC): muestra la dirección MAC.

Interface (Interfaz): muestra el número de puerto.

Definición del tiempo de caducidad

1. Abra la página **Dynamic Address Table** (Tabla de direcciones dinámicas).
2. Defina el campo **Address Aging** (Duración de direcciones).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica el tiempo de caducidad y se actualiza el dispositivo.

Consulta de la tabla de direcciones dinámicas

1. Abra la página **Dynamic Address Table** (Tabla de direcciones dinámicas).
2. Defina el parámetro para realizar la consulta en la tabla de direcciones dinámicas..

Las entradas se pueden consultar por **Interface** (Interfaz), **LAG**, **MAC Address** (Dirección MAC) o **VLAN ID** (ID de VLAN).

3. Haga clic en **Query** (Consultar) para consultar la tabla de direcciones dinámicas.

Eliminación de datos de la tabla de direcciones dinámicas

1. Abra la página **Dynamic Address Table** (Tabla de direcciones dinámicas).
2. Seleccione **Clear Table** (Borrar tabla).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se borran todos los datos de la tabla de direcciones dinámicas.

Consulta y ordenación de direcciones dinámicas mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de la tabla de direcciones

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. El protocolo GARP define una serie de conmutadores interesados en un atributo de red dado, como VLAN o dirección multidifusión. Puede acceder a la página **GARP Timers** (Temporizadores de GARP) desde la página de menú **GARP**.

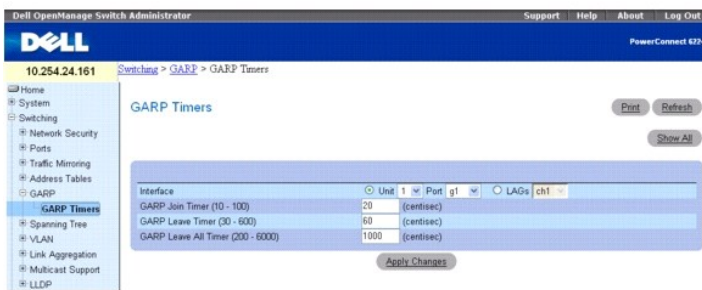
Para visualizar la página de menú **GARP**, haga clic en **Switching** (Conmutación) → **GARP** en la vista de árbol.

Temporizadores de GARP

La página **GARP Timers** (Temporizadores de GARP) contiene campos para activar el protocolo GARP en el conmutador.

Para visualizar la página **GARP Timers** (Temporizadores de GARP), haga clic en **Switching** (Conmutación) → **GARP** → **GARP Timers** (Temporizadores de GARP) en la vista de árbol.

Ilustración 7-36. Temporizadores de GARP



La página **GARP Timers** (Temporizadores de GARP) contiene los campos siguientes:

Interface (Interfaz): especifica la unidad y puerto o el LAG en los que se ha activado el temporizador de GARP.

GARP Join Timer (10–100) (Temporizador de unión de GARP [10–100]): muestra el tiempo, en centisegundos, en el que se transmiten las PDU. El valor posible de este campo es 10-100 y el valor predeterminado es 100 centisegundos.

GARP Leave Timer (30–600) (Temporizador de cese de GARP [30-600]): muestra el tiempo, en centisegundos, durante el cual el conmutador espera antes de abandonar su estado de 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 superior al triple del tiempo de unión. El valor posible de este campo es 30–600 y el valor predeterminado es 60 centisegundos.

GARP Leave All Timer (200–6000) (Temporizador de cese de todos de GARP [200–6000]): muestra el tiempo, en centisegundos, durante el cual todos los conmutadores esperan antes de abandonar su estado GARP. El tiempo de cese de todos debe ser superior al tiempo de cese. El valor posible de este campo es 200–6000 y el valor predeterminado es 1000 centisegundos.

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 se copian en los puertos o LAG seleccionados en la tabla de temporizadores de GARP y se actualiza el dispositivo.

Visualización de parámetros en la tabla de temporizadores de GARP

1. Abra la página **GARP Timers** (Temporizadores de GARP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **GARP Timers Table** (Tabla de temporizadores de GARP).

Ilustración 7-37. Tabla de temporizadores de GARP

Interface	GARP Join Timer	GARP Leave Timer	GARP Leave All Timer	Copy To	Edit
1 1/g1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
2 1/g2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
3 1/g3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
27 1/g3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
28 1/g4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>

LAGs	GARP Join Timer	GARP Leave Timer	GARP Leave All Timer	Copy To	Edit
29 ch1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
30 ch2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
31 ch3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
32 ch4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
33 ch5	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
34 ch6	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
35 ch7	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
36 ch8	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de temporizadores de GARP correspondiente a otras unidades de la pila, en caso de que existan.

Copia de la configuración de temporizadores de GARP

1. Abra la página **GARP Timers** (Temporizadores de GARP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **GARP Timers Table** (Tabla de temporizadores de GARP).

3. Especifique la unidad y el puerto de los que está copiando en **Copy Parameters From** (Copiar parámetros de).
4. Haga clic en **Copy To** (Copiar en) para cada interfaz que deba recibir estos parámetros.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se copian los valores de configuración de los temporizadores de GARP y se actualiza el dispositivo.

Modificación de la configuración de los temporizadores de GARP para varios puertos

1. Abra la página **GARP Timers** (Temporizadores de GARP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **GARP Timers Table** (Tabla de temporizadores de GARP).

3. Haga clic en **Edit** (Editar) para cada interfaz que desee modificar.
4. Edite los campos de temporizadores de GARP según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de los temporizadores de GARP y se actualiza el dispositivo.

Definición de temporizadores de GARP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos GVRP

Configuración del protocolo de árbol de extensión

El protocolo de árbol de extensión (STP) ofrece una topología de árbol de cualquier combinación de puentes. STP proporciona también una ruta entre las estaciones finales de una red para eliminar los bucles. Las versiones de árbol de extensión admitidas son STP clásico, STP múltiple y STP rápida.

El STP clásico proporciona una única ruta entre estaciones finales, con lo que se evitan y eliminan los bucles. Para obtener información sobre cómo configurar el STP clásico, consulte "[Configuración global de STP](#)".

El protocolo de árbol de extensión múltiple (MSTP) admite varias instancias de árbol de extensión para canalizar eficientemente el tráfico de VLAN en diferentes interfaces. Cada instancia de árbol de extensión se comporta según lo especificado en el IEEE 802.1w, árbol de extensión rápida (RSTP), con ligeras modificaciones en el funcionamiento, aunque con el mismo efecto final (el principal efecto es la rápida transición del puerto al estado de "Reenvío"). La diferencia entre el RSTP y el STP tradicional (IEEE 802.1d) es la capacidad de configurar y reconocer conectividad en modo dúplex completo y puertos conectados a estaciones finales, lo que permite una rápida transición del puerto al estado de "Reenvío" y la supresión de la notificación de cambio de topología. Estas características se representan con los parámetros "pointtopoint" (punto a punto) y "edgeport" (puerto perimetral). MSTP es compatible tanto con RSTP como con STP. Su funcionamiento es correcto con puentes STP y RSTP. Un puente MSTP se puede configurar para que su comportamiento sea idéntico al de un puente RSTP o puente STP.

Para visualizar la página de menú **Spanning Tree** (Árbol de extensión), haga clic en **Switching** (Conmutación)→ **Spanning Tree** (Árbol de extensión) en la vista de árbol. Esta página **Spanning Tree** (Árbol de extensión) contiene enlaces a los procedimientos de STP siguientes:

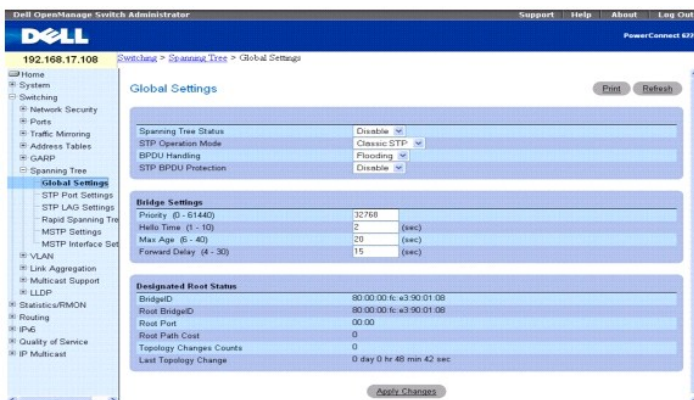
- 1 [Configuración global de STP](#)
- 1 [Configuración de puertos STP](#)
- 1 [Configuración STP del LAG](#)
- 1 [Árbol de extensión rápida](#)
- 1 [Configuración de MSTP](#)
- 1 [Configuración de la interfaz MSTP](#)

Configuración global de STP

La página **STP Global Settings** (Configuración global de STP) contiene campos para activar el protocolo STP en el conmutador.

Para visualizar la página **STP Global Settings** (Configuración global de STP), haga clic en **Switching** (Conmutación)→ **Spanning Tree** (Árbol de extensión)→ **Global Settings** (Configuración global) en la vista de árbol.

Ilustración 7-38. Configuración global del árbol de extensión



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

Spanning Tree Status (Estado del árbol de extensión): activa o desactiva RSTP, STP o MSTP en el conmutador.

STP Operation Mode (Modo de funcionamiento de STP): especifica el modo STP con el que se activa STP en el conmutador. Los valores del campo posibles son: **Classic STP** (STP clásico), **Rapid STP (STP rápida)** y **Multiple STP** (STP múltiple).

BPDU Handling (Manipulación de BPDU): especifica el manejo de paquetes de la unidad de datos del protocolo de puente (BPDU) cuando el árbol de extensión está desactivado en una interfaz. Los valores posibles del campo son **Filtering** (Filtrado) y **Flooding** (Distribución). El valor predeterminado es **Flooding** (Distribución).

STP BPDU Protection (Protección BPDU de STP): desactiva un puerto en caso de que un conmutador nuevo intente acceder a la topología de STP ya existente. Esto evita que los conmutadores que no forman parte original de un STP influyan en la topología STP.

Si está configurada con el valor **Enable** (Activar), cuando se recibe una BPDU en un puerto perimetral, ese puerto se desactiva. Una vez desactivado el puerto, para volverlo a activar es preciso intervenir manualmente.

Configuración del puente

Priority (0–61440) (Prioridad [0–61440]): especifica el valor de prioridad del puente. Cuando los conmutadores o los puentes ejecutan STP, se les asigna una prioridad. Después de intercambiar las BPDU, el conmutador que tiene el valor de prioridad menor se convierte en el puente raíz.

Hello Time (1–10) (Tiempo de saludo [1–10]): especifica el tiempo de saludo del conmutador, que indica el tiempo en segundos durante el que un puente raíz espera entre mensajes de configuración. El valor predeterminado es 2.

Max Age (6–40) (Caducidad máxima [6–40]): especifica el tiempo máximo de caducidad del conmutador, que indica el tiempo en segundos durante el que un puente espera antes de implementar un cambio de topología. El valor predeterminado es 20.

Forward Delay (4–30) (Demora de reenvío [4–30]): especifica el tiempo de demora de reenvío del conmutador, que indica el tiempo en segundos durante el que un puente permanece en estado de escucha y de obtención antes de reenviar paquetes. El valor predeterminado es 15.

Estado de raíz designado

Bridge ID (ID de puente): muestra la ID del puente.

Root Bridge ID (ID de puente raíz): especifica la ID del puente raíz.

Root Port (Puerto raíz): muestra el número de puerto que ofrece la ruta de menor coste desde este puente hasta el puente raíz. Es importante cuando el puente no es el puente raíz. El valor predeterminado es cero.

Root Path Cost (Coste de la ruta raíz): muestra el coste de la ruta desde este puente hasta la raíz.

Topology Changes Counts (Recuentos de cambios de topología): muestra la cantidad total de cambios de estado de STP que se han producido.

Last Topology Change (Último cambio de topología): muestra el tiempo total transcurrido desde el último cambio de topografía. El tiempo se indica en formato día/hora/minuto/segundo, por ejemplo, 5 horas 10 minutos y 4 segundos.

Definición de los parámetros globales de STP

1. Abra la página **STP Global Settings** (Configuración global de STP).
2. Seleccione **Enable** (Activar) en el campo **Spanning Tree Status** (Estado del árbol de extensión).
3. Especifique el tipo de modo **STP** en el campo **STP Operation Mode** (Modo de funcionamiento de STP) y defina los valores restantes.
4. Haga clic en **Apply Changes** (Aplicar cambios).
El protocolo STP se activa en el conmutador.

Modificación de los parámetros globales de STP

1. Abra la página **STP Global Settings** (Configuración global de STP).
2. Modifique los campos de esta página según convenga.
3. Haga clic en **Apply Changes** (Aplicar cambios).
Se modifican los parámetros de STP y se actualiza el dispositivo.

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

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

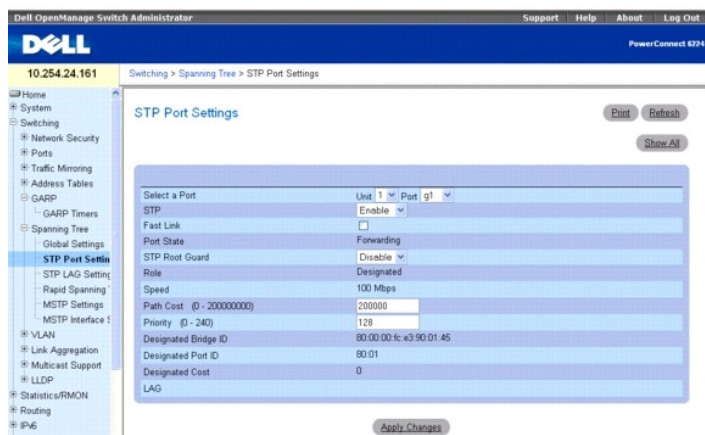
- Comandos del árbol de extensión

Configuración de puertos STP

Utilice la página **STP Port Settings** (Configuración de puertos STP) para asignar propiedades STP a puertos concretos.

Para visualizar la página **STP Port Settings** (Configuración de puertos STP), haga clic en **Switching** (Conmutación) → **Spanning Tree** (Árbol de extensión) → **STP Port Settings** (Configuración de puertos STP) en la vista de árbol.

Ilustración 7-39. Configuración de puertos STP



La página **STP Port Settings** (Configuración de puertos STP) contiene los campos siguientes:

Select a Port (Seleccionar un puerto): especifica la unidad y el puerto en los que se ha activado STP.

STP: activa o desactiva el STP en el puerto.

Fast Link (Enlace rápido): si se selecciona esta opción, se activa el modo de enlace rápido para el puerto. Si se activa el modo de enlace rápido para un puerto, el valor de **Port State** (Estado del puerto) se establece automáticamente en el estado **Forwarding** (Reenvío) si el enlace del puerto está activo. La convergencia de STP puede tardar unos 30–60 segundos en redes de gran tamaño.

Port State (Estado del puerto): indica el estado de STP actual de un puerto. Si está activado, el estado del puerto determina qué acción de reenvío se realiza con el tráfico. El puerto puede tener estos estados:

Disabled (Desactivado): STP está desactivado en el puerto. El puerto reenvía el tráfico a la vez que obtiene direcciones MAC.

Blocking (Bloqueado): el puerto está bloqueado y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC.

Listening (Escucha): el puerto está en modo de escucha. No puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): el puerto está en modo de obtención. No puede reenviar tráfico, pero sí que puede obtener nuevas direcciones MAC.

Forwarding (Reenvío): el puerto está en modo de reenvío. Puede reenviar tráfico y obtener nuevas direcciones MAC.

STP Root Guard (Protección de raíz STP): impide que la raíz de una instancia de árbol de extensión cambie de forma inesperada. Cuando un puente raíz tiene la protección de raíz activada y llega una BPDU superior, el puerto en cuestión pasa a un estado de raíz incoherente, equivalente al estado de escucha. Entonces, se aplica el puente raíz.

Role (Función): muestra la función de este puerto en la topología STP.

Speed (Velocidad): muestra la velocidad a la que funciona el puerto.

Path Cost (0–200000000) (Coste de ruta [0–200000000]): especifica la contribución del puerto al coste de la ruta raíz. El coste de la ruta se ajusta a un valor mayor o menor y se utiliza para reenviar el tráfico cuando se redirige la ruta. El valor cero indica que el coste de la ruta se ha definido según la velocidad del puerto. El valor predeterminado es 0.

Priority (0–240) (Prioridad [0–240]): especifica el valor de prioridad del puerto. El valor de prioridad influye en la selección del puerto cuando un puente tiene dos puertos conectados en un bucle. El valor predeterminado es 128.

Designated Bridge ID (ID del puente designado): muestra la ID del puente designado.

Designated Port ID (ID del puerto designado): muestra la ID del puerto seleccionado.

Designated Cost (Coste designado): muestra el coste del puerto que participa en la topología STP. Los puertos cuyo coste es menor presentan menos probabilidad de ser bloqueados si STP detecta bucles.

LAG: muestra el LAG al que está vinculado el puerto.

Activación de STP en un puerto

1. Abra la página **STP Port Settings** (Configuración de puertos STP).
2. Especifique la unidad y el puerto que desea activar en el campo **Select a Port** (Seleccionar un puerto).
3. Seleccione **Enable** (Activar) en el campo **STP**.
4. Edite los campos **Fast Link** (Enlace rápido), **STP Root Guard** (Protección de raíz STP), **Path Cost** (Coste de ruta) y **Priority** (Prioridad) según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El protocolo STP se activa en el puerto.

Modificación de las propiedades STP del puerto

1. Abra la página **STP Port Settings** (Configuración de puertos STP).
2. Modifique los campos **Fast Link** (Enlace rápido), **STP Root Guard** (Protección de raíz STP), **Path Cost** (Coste de ruta) y **Priority** (Prioridad) según convenga.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros del puerto STP y se actualiza el dispositivo.

Visualización de la tabla de puertos STP

1. Abra la página **STP Port Settings** (Configuración de puertos STP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **STP Port Table** (Tabla de puertos STP).

Ilustración 7-40. Tabla de puertos STP

STP Port Table

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Edit
1/1/1	Enable	On	Disable	Manual Forward Disabled	Disabled	0	128	80:00:00:0:c2:30:01:45	00:00	0	✕
2/1/1	Enable	On	Disable	Disabled	Disabled	0	128	80:00:00:0:c2:30:01:45	00:00	0	✕
3/1/1	Enable	On	Disable	Manual Forward Disabled	Disabled	0	128	80:00:00:0:c2:30:01:45	00:00	0	✕

Apply Changes Back

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de puertos STP correspondiente a otras unidades de la pila, en caso de que existan.

Modificación de la configuración de puertos STP para varios puertos

1. Abra la página **STP Port Settings** (Configuración de puertos STP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **STP Port Table** (Tabla de puertos STP).
3. Haga clic en **Edit** (Editar) para cada puerto que desee modificar.
4. Edite la configuración de puertos STP según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de los puertos STP y se actualiza el dispositivo.

Aplicación de enlace rápido a un puerto

1. Abra la página **STP Port Settings** (Configuración de puertos STP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **STP Port Table** (Tabla de puertos STP).
3. Haga clic en **Edit** (Editar) para cada puerto que desee modificar.
4. Seleccione **Fast Link** (Enlace rápido) para activar el modo de enlace rápido para un puerto. Si se activa el modo de enlace rápido para un puerto, el valor de **Port State** (Estado del puerto) se establece automáticamente en el estado **Forwarding** (Reenvío) si el enlace del puerto está activo.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros del puerto STP para los puertos seleccionados y se actualiza el dispositivo.

Definición de la configuración de los puertos STP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos del árbol de extensión

Configuración STP del LAG

Utilice la página **STP LAG Settings** (Configuración STP del LAG) para asignar parámetros de agregado de puertos STP.

Para visualizar la página **STP LAG Settings** (Configuración STP del LAG), haga clic en **Switching** (Conmutación)→ **Spanning Tree** (Árbol de extensión)→ **STP LAG Settings** (Configuración STP del LAG) en la vista de árbol.

Ilustración 7-41. Configuración STP del LAG



La página **STP LAG Settings** (Configuración STP del LAG) contiene los campos siguientes:

Select a LAG (Seleccionar un LAG): especifica el número de LAG cuyos valores de STP desea modificar.

STP: activa o desactiva el STP en el LAG. El valor predeterminado es Enable (Activar).

Fast Link (Enlace rápido): activa el modo de enlace rápido para el LAG. Si se activa el modo de enlace rápido para un LAG, el valor de **Port State** (Estado del puerto) se establece automáticamente en el estado **Forwarding** (Reenvío) si el LAG está activo. El modo de enlace rápido optimiza el tiempo necesario para la convergencia del protocolo STP. La convergencia de STP puede tardar unos 30-60 segundos en redes de gran tamaño.

Port State (Estado del puerto): muestra el estado de STP actual de un LAG. Si está activado, el estado del LAG determina qué acción de reenvío se realiza con el tráfico. Si el puente descubre un LAG que no funciona correctamente, el LAG se sitúa en el estado **Broken** (Interrumpido). El LAG puede tener estos estados:

Disabled (Desactivado): STP está desactivado en el LAG. El LAG reenvía el tráfico a la vez que obtiene direcciones MAC.

Blocking (Bloqueado): el LAG está bloqueado y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC.

Listening (Escucha): el LAG se encuentra en modo de escucha y no puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): el LAG se encuentra en modo de obtención y no puede reenviar tráfico, pero puede obtener direcciones MAC nuevas.

Forwarding (Reenvío): el LAG se encuentra en el modo de reenvío y puede reenviar tráfico y obtener direcciones MAC.

Broken (Interrumpido): el LAG no funciona correctamente y no puede utilizarse para reenviar tráfico.

Role (Función): muestra la función de este puerto en la topología STP.

Path Cost (0–200000000) (Coste de ruta [0–200000000]): especifica la contribución del LAG al coste de la ruta raíz. El coste de la ruta se ajusta a un valor mayor o menor y se utiliza para reenviar el tráfico cuando se redirecciona la ruta. El valor predeterminado es 0.

Priority (0–240) (Prioridad [0–240]): especifica el valor de prioridad del LAG. El valor de prioridad influye en la elección del LAG cuando un puente tiene dos puertos en bucle. El valor de prioridad oscila entre 0 y 240.

Designated Bridge ID (ID del puente designado): muestra la ID del puente designado.

Designated Port ID (ID del puerto designado): muestra la ID del puerto designado.

Designated Cost (Coste designado): muestra el coste del puerto que participa en la topología STP. Los puertos cuyo coste es menor presentan menos probabilidad de ser bloqueados si STP detecta bucles.

Modificación de los parámetros de STP del LAG para un LAG

1. Abra la página **STP LAG Settings** (Configuración STP del LAG).
2. Seleccione un LAG en el menú desplegable **Select a LAG** (Seleccionar un LAG).
3. Modifique los campos necesarios.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros de STP del LAG y se actualiza el dispositivo.

Visualización de la tabla de STP del LAG

1. Abra la página **STP LAG Settings** (Configuración STP del LAG).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **STP LAG Table** (Tabla de STP del LAG).

Ilustración 7-42. Tabla de STP del LAG

Port	STP Link	Fast Link	STP Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost
261	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
262	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
263	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
264	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
265	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
266	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
267	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0
268	Enable	Disable	Disable	Disabled	0	128	800000	fc:43900145	0000	0

3. Desde esta tabla, puede activar o desactivar el enlace rápido y la protección de raíz STP para un LAG individual haciendo clic en **Fast Link** (Enlace rápido), realizando las selecciones adecuadas y, a continuación, haciendo clic en **Apply Changes** (Aplicar cambios).

Modificación de los parámetros de STP del LAG para varios LAG

1. Abra la página **STP LAG Settings** (Configuración STP del LAG).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **STP LAG Table** (Tabla de STP del LAG).
3. Seleccione **Edit** (Editar) para todos los LAG que vaya a modificar.
4. Modifique los campos necesarios.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros de STP del LAG para los LAG seleccionados y se actualiza el dispositivo.

Definición de la configuración STP del LAG mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

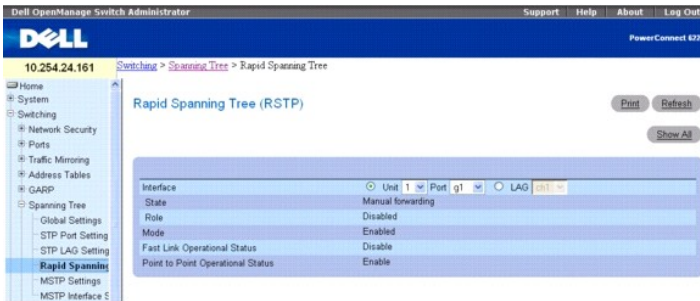
- 1 Comandos del árbol de extensión

Árbol de extensión rápida

El protocolo de árbol de extensión rápida (RSTP) detecta y utiliza topologías de red que permiten una convergencia más rápida del árbol de extensión sin crear bucles de reenvío.

Para visualizar la página **Rapid Spanning Tree** (Árbol de extensión rápida), haga clic en **Switching** (Conmutación)→ **Spanning Tree** (Árbol de extensión)→ **Rapid Spanning Tree** (Árbol de extensión rápida) en la vista de árbol.

Ilustración 7-43. Árbol de extensión rápida



La página **Rapid Spanning Tree** (Árbol de extensión rápida) contiene los campos siguientes:

Interface (Interfaz): determina si RSTP está activado en una unidad/puerto o en un LAG. Haga clic en Unit/Port (Unidad/Puerto) o en LAG para especificar el tipo de interfaz y, a continuación, seleccione en el menú desplegable la unidad, el puerto o el LAG que desea configurar.

State (Estado): muestra el estado de árbol de extensión para el puerto.

Role (Función): muestra la función de árbol de extensión para el puerto en la topología STP.

Mode (Modo): muestra el modo administrativo y si está activado o desactivado.

Fast Link Operational Status (Estado operativo del enlace rápido): indica si el enlace rápido está activado o desactivado para el puerto o el LAG. Si el enlace rápido está activado para un puerto, éste adopta automáticamente el estado de reenvío. Este valor puede cambiarse desde la página "[Configuración de puertos STP](#)" o "[Configuración STP del LAG](#)".

Point-to-Point Operational Status (Estado operativo punto a punto): muestra el estado operativo punto a punto.

Para establecer comunicaciones a través de un enlace punto a punto, el PPP que lo origina envía primero paquetes de protocolo de control de enlace (LCP) para configurar y probar el enlace de datos. Una vez que se ha establecido un enlace y que el LCP ha negociado según proceda los recursos opcionales, el PPP que origina el enlace envía paquetes de protocolo de control de red (NCP) para seleccionar y configurar uno o más protocolos de nivel de red. Cuando se han configurado todos los protocolos de nivel de red seleccionados, los paquetes de cada protocolo de nivel de red pueden enviarse a través del enlace. El enlace permanece configurado para las comunicaciones hasta que paquetes LCP o NCP explícitos cierran el enlace o hasta que se produce algún suceso externo. Éste es el tipo de enlace de puerto de conmutador real.

Visualización de la tabla del árbol de extensión rápida (RSTP)

1. Abra la página **Rapid Spanning Tree (RSTP)** (Árbol de extensión rápida [RSTP]).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Rapid Spanning Tree Table** (Tabla del árbol de extensión rápida).

Ilustración 7-44. Tabla del árbol de extensión rápida

Rapid Spanning Tree Table Print Refresh

Unit

Interface	Role	Fast Link Operational Status	Point to Point Operational Status
1	1/g1	Disabled	Enable
2	1/g2	Disabled	Disable
3	1/g3	Disabled	Enable

26	1/r/g2	Disabled	Disable
27	1/r/g3	Disabled	Disable
28	1/r/g4	Disabled	Disable

LAGs			
29	ch1	Disabled	False
30	ch2	Disabled	False
31	ch3	Disabled	False
32	ch4	Disabled	False
33	ch5	Disabled	False
34	ch6	Disabled	False
35	ch7	Disabled	False
36	ch8	Disabled	False

Back

- Utilice el menú desplegable **Unit** (Unidad) para ver la tabla del árbol de extensión rápida correspondiente a otras unidades de la pila, en caso de que existan.

Definición de los parámetros del RSTP mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

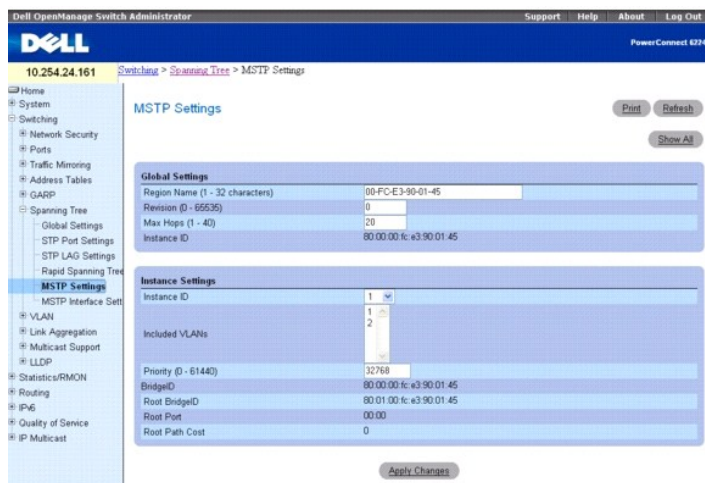
- Comandos del árbol de extensión

Configuración de MSTP

El protocolo de árbol de extensión múltiple (MSTP) admite varias instancias de árbol de extensión para canalizar eficientemente el tráfico de VLAN en diferentes interfaces. El protocolo MSTP es compatible tanto con RSTP como con STP; un puente MSTP se puede configurar para que su comportamiento sea idéntico al de un puente RSTP o puente STP.

Para visualizar la página **MSTP Settings** (Configuración de MSTP), haga clic en **Switching** (Conmutación) → **Spanning Tree** (Árbol de extensión) → **MSTP Settings** (Configuración de MSTP) en la vista de árbol.

Ilustración 7-45. Configuración de MSTP



La página **MSTP Settings** (Configuración de MSTP) contiene los campos siguientes, divididos en dos secciones, **Global Settings** (Configuración global) e **Instance Settings** (Configuración de instancia):

Region Name (1–32 characters) (Nombre de región [1–32 caracteres]): especifica el nombre de región de MST definido por el usuario.

Revision (0–65535) (Revisión [0–65535]): especifica un número sin signo de 16 bits que identifica la revisión de la configuración de MST actual. El número de revisión es necesario como parte de la configuración de MST. El valor predeterminado es 0.

Max Hops (1–40) (Número 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 el paquete BPDU, la información del puerto caduca. El valor predeterminado es 20.

Instance ID (ID de instancia): especifica la ID de la instancia de árbol de extensión. El intervalo de valores de este campo oscila entre 1 y 15, y el valor predeterminado es 1.

Included VLANs (VLAN incluidas): asigna las redes VLAN seleccionadas a la instancia seleccionada. Cada VLAN pertenece a una única instancia.

Priority (0–61440) (Prioridad [0–61440]): especifica la prioridad del conmutador para la instancia de árbol de extensión seleccionada. El valor predeterminado es 32768.

Bridge ID (ID de puente): indica la ID de puente de la instancia seleccionada.

Root Bridge ID (ID de puente raíz): indica la ID del puente raíz, que es el que tiene el menor coste de ruta.

Root Port (Puerto raíz): indica el puerto raíz de la instancia seleccionada.

Root Path Cost (Coste de la ruta raíz): indica el coste de ruta de la instancia seleccionada.

Modificación de la configuración de MSTP

1. Abra la página **MSTP Settings** (Configuración de MSTP).
2. Modifique los campos de las secciones **Global Settings** (Configuración global) e **Instance Settings** (Configuración de instancia) según convenga.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros de MSTP y se actualiza el dispositivo.

Visualización de la tabla de asignación de VLAN de MSTP a instancias

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

Aparece la página **MSTP Settings Table** (Tabla de configuración de MSTP).

Ilustración 7-46. Tabla de configuración de MSTP

VLAN	Instance ID # (I)	Edit
1	0	<input type="checkbox"/>
2	0	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	000	<input type="checkbox"/>
6	2222	<input type="checkbox"/>

3. Para modificar la ID de instancia para una o varias redes VLAN, seleccione **Edit** (Editar) para las redes VLAN que desee.
4. Realice los cambios necesarios en las ID de instancia. Especifique un valor 0 para eliminar la asignación de VLAN a instancia.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican las ID de instancia para las redes VLAN seleccionadas y se actualiza el dispositivo.

Definición de instancias MST mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

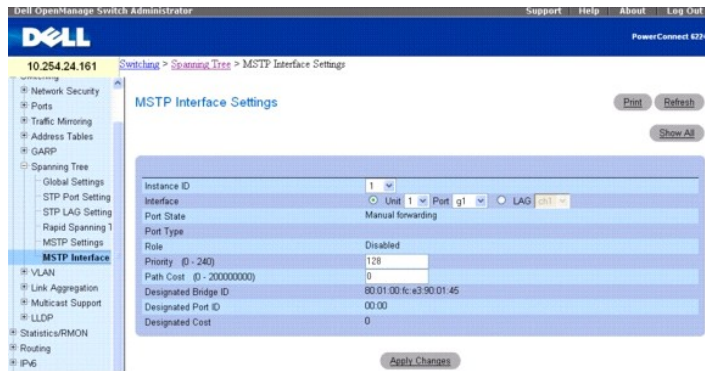
- 1 Comandos del árbol de extensión

Configuración de la interfaz MSTP

Utilice la página **MSTP Interface Settings** (Configuración de la interfaz MSTP) para asignar valores de MSTP a interfaces específicas.

Para visualizar la página **MSTP Interface Settings** (Configuración de la interfaz MSTP), haga clic en **Switching** (Conmutación)→ **Spanning Tree** (Árbol de extensión)→ **MSTP Interface Settings** (Configuración de la interfaz MSTP) en la vista de árbol.

Ilustración 7-47. Configuración de la interfaz MSTP



La página **MSTP Interface Settings** (Configuración de la interfaz MSTP) contiene los campos siguientes:

Instance ID (ID de instancia): selecciona las instancias de MSTP configuradas en el conmutador. El intervalo de valores posibles del campo es 1–15.

Interface (Interfaz): selecciona una unidad/puerto o un LAG para esta instancia de MSTP.

Port State (Estado del puerto): indica si el puerto está activado o desactivado en la instancia específica.

Port Type (Tipo de puerto): indica si MSTP trata el puerto como un puerto de punto a punto o como un puerto conectado a un concentrador, y si el puerto es interno en la región de MST o bien se trata de un puerto de límite. Si se trata de un puerto de límite, también indica si el conmutador del otro lado del enlace funciona en modo RSTP o STP.

Role (Función): indica la función de puerto asignada por el algoritmo STP para proporcionar rutas STP. Los valores del campo posibles son:

Root (Raíz): proporciona la ruta de coste inferior para reenviar paquetes al conmutador raíz.

Designated (Designado): indica el puerto o LAG a través del que el conmutador designado se conecta a la LAN.

Alternate (Alternativa): proporciona una ruta alternativa al conmutador raíz desde la interfaz.

Backup (Reserva): proporciona una ruta de reserva a la LAN designada. Los puertos de reserva sólo existen si hay dos puertos conectados en un bucle mediante un enlace de punto a punto. Los puertos de reserva también existen si una LAN tiene dos o más conexiones conectadas a un segmento compartido.

Disabled (Desactivado): indica que el puerto no participa en el árbol de extensión.

Priority (Prioridad): define la prioridad de la interfaz para la instancia especificada. El intervalo de prioridad es de 0 a 240 en pasos de 16. El valor predeterminado es 128.

Path Cost (0–200000000) (Coste de ruta [0–200000000]): indica la contribución del puerto a la instancia de árbol de extensión. El intervalo siempre debe ser de 0 a 200000000. El valor predeterminado lo fija la velocidad del puerto. El valor predeterminado es:

- 1 Canal de puerto - 20000
- 1 1 000 Mbps (Giga) - 20000
- 1 100 Mbps - 200000
- 1 10 Mbps -2000000

Designated Bridge ID (ID del puente designado): muestra el número de la ID del puente que conecta el enlace o la LAN compartida a la raíz.

Designated Port ID (ID del puerto designado): muestra el número de la ID del puerto en el puente designado que conecta el enlace o la LAN compartida a la raíz.

Designated Cost (Coste designado): muestra el coste de la ruta desde el enlace o la LAN compartida hasta la raíz.

Asignación de la configuración de la interfaz MSTP

1. Abra la página **MSTP Interface Settings** (Configuración de la interfaz MSTP).
2. Seleccione una ID de instancia en el menú desplegable.
3. Especifique un valor para **Port** (Puerto) o **LAG** y, a continuación, seleccione la interfaz en el menú desplegable correspondiente.
4. Especifique un valor para **Interface Priority** (Prioridad de la interfaz) y **Path Cost** (Coste de ruta).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz y se actualiza el dispositivo.

Visualización de la tabla de configuración de la interfaz MSTP

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

Aparece la página **MSTP Interface Table** (Tabla de interfaces MST).

Ilustración 7-48. Tabla de interfaces MSTP

Interface	Role	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Edit
1 1/1g1	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	0001	<input type="checkbox"/>
2 1/1g2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	0002	<input type="checkbox"/>
3 1/1g3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	0003	<input type="checkbox"/>
26 1/1g2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	000A	<input type="checkbox"/>
27 1/1g3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	000B	<input type="checkbox"/>
28 1/1g4	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	000C	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de interfaces MST correspondiente a otras unidades de la pila, en caso de que existan.
4. Para modificar la prioridad del puerto o el coste de la ruta para una o más interfaces, seleccione **Edit** (Editar) para las interfaces deseadas.
5. Realice los cambios necesarios en los valores de las columnas **Port Priority** (Prioridad de puerto) o **Path Cost** (Coste de ruta).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los campos correspondientes a las interfaces seleccionadas y se actualiza el dispositivo.

Definición de interfaces MSTP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos del árbol de extensión

Configuración de redes VLAN

Al añadir compatibilidad con redes LAN virtuales (VLAN) a un conmutador de nivel 2 se obtienen algunas de las ventajas que proporcionan tanto los puentes como el enrutamiento. Como los puentes, un conmutador de VLAN reenvía el tráfico basado en la cabecera de nivel 2, que es rápido; por otro lado, como los enrutadores, particiona la red en segmentos lógicos, lo que permite una mejor administración, seguridad y gestión del tráfico de multidifusión.

Una VLAN es un conjunto de estaciones finales y los puertos de conmutación que las conectan. Pueden existir múltiples razones para la división lógica, como la pertenencia a un departamento o a un proyecto. El único requisito físico es que la estación final y el puerto al que está conectado pertenezcan a la misma VLAN.

Cada VLAN de una red tiene una ID de VLAN asociada, que aparece en la etiqueta IEEE 802.1Q de la cabecera de nivel 2 de los paquetes transmitidos en una VLAN. Una estación final puede omitir la etiqueta, o la parte de la etiqueta correspondiente a la VLAN; en tal caso, el primer puerto de conmutación que reciba el paquete puede rechazarlo o insertar una etiqueta usando la ID de VLAN predeterminada. Un puerto determinado puede manejar tráfico para más de una VLAN, pero sólo puede admitir una ID de VLAN predeterminada.

Para visualizar la página de menú **VLAN**, haga clic en **Switching** (Conmutación)→ **VLAN** en la vista de árbol. La página **VLAN** contiene enlaces a las funciones siguientes:

- 1 [Pertenencia a la VLAN](#)
- 1 [Configuración de puertos de VLAN](#)
- 1 [Configuración de LAG de VLAN](#)
- 1 [Vinculación de MAC a VLAN](#)
- 1 [Vinculación de subred IP a VLAN](#)
- 1 [Grupo de protocolo](#)
- 1 [Parámetros de GVRP](#)

Pertenencia a la VLAN

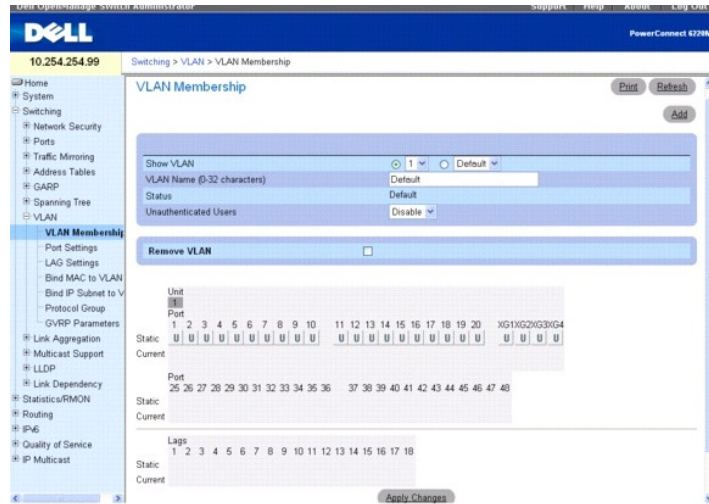
Utilice la página **VLAN Membership** (Pertenencia a la VLAN) para definir grupos de VLAN almacenados en la tabla de pertenencia a la VLAN. El conmutador admite hasta 4094 VLAN. No obstante, en realidad sólo se pueden crear 4 092 VLAN por los siguientes motivos:

- 1 La VLAN 1 es la VLAN predeterminada de la que todos los puertos son miembros.
- 1 La VLAN 4095 está designada como "Discard VLAN" (Descartar VLAN).

Las VLAN válidas que pueden crearse son de la 2 a la 4093. La VLAN 4094 está reservada.

Para visualizar la página **VLAN Membership** (Pertenencia a la VLAN), haga clic en **Switching** (Conmutación) → **VLAN** → **VLAN Membership** (Pertenencia a la VLAN) en la vista de árbol.

Ilustración 7-49. Pertenencia a la VLAN



La página **VLAN Membership** (Pertenencia a la VLAN) está dividida en dos secciones. La sección superior contiene campos que definen la pertenencia a toda la VLAN. La sección inferior contiene tablas que definen la configuración de pertenencias a puertos y LAG específicos de la VLAN. Los campos de **VLAN Membership** (Pertenencia a la VLAN) son los siguientes:

Show VLAN (Mostrar VLAN): selecciona la VLAN que desea visualizar. Utilice el menú desplegable **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN) para seleccionar la VLAN.

VLAN Name (0–32) (Nombre de la VLAN [0–32]): indica el nombre de la VLAN definido por el usuario. Este campo se define usando el botón **Add** (Añadir). Los nombres válidos pueden tener de 0 a 32 caracteres.

Status (Estado): indica el tipo de VLAN. Los valores posibles son:

- Dynamic** (Dinámica): indica que la VLAN se ha creado de forma dinámica a través de GVRP.
- Static** (Estática): indica que la VLAN la ha definido el usuario y puede modificarse.
- Default** (Predeterminada): indica que la VLAN es la predeterminada.

Unauthenticated Users (Usuarios no autenticados): permite el acceso de conmutadores no autorizados a esta VLAN cuando se ha seleccionado la opción **Enable** (Activar).

Remove VLAN (Eliminar VLAN): cuando se selecciona esta opción, se elimina la VLAN mostrada de la tabla de pertenencia a la VLAN.

Las tablas de **VLAN Membership** (Pertenencia a la VLAN) muestran los puertos y LAG que forman parte de la VLAN, así como si tienen etiqueta (T), no tienen etiqueta (U) o están prohibidos (F). Las tablas tienen dos filas: **Static** (Estática) y **Current** (Actual). Desde esta página sólo se puede acceder a la fila **Static** (Estática). La fila **Current** (Actual) se actualiza dinámicamente mediante GVRP o cuando se modifica la línea **Static** (Estática) y se hace clic en **Apply Changes** (Aplicar cambios).

En esta sección de la página hay dos tablas:

Ports (Puertos): muestra y asigna pertenencia a la VLAN a los puertos. Para asignar pertenencia, haga clic en **Static** (Estática) para un puerto concreto. Con cada clic irá alternando entre las opciones U, T y en blanco. Consulte las definiciones en la tabla siguiente.

LAGs (LAG): muestra y asigna pertenencia a la VLAN a los LAG. Para asignar pertenencia, haga clic en **Static** (Estática) para un LAG concreto. Con cada clic irá alternando entre las opciones U, T y en blanco. Consulte las definiciones en la tabla siguiente.

Tabla 7-1. Definiciones de pertenencia de puertos a la VLAN

Control del puerto	Definición
T	Tagged (Con etiqueta): la interfaz es miembro de una VLAN. Todos los paquetes reenviados por la interfaz tienen etiqueta. Los paquetes contienen información de la VLAN.
U	Untagged (Sin etiqueta): la interfaz es miembro de una VLAN. Los paquetes reenviados por la interfaz no tienen etiqueta.

F	Forbidden (Prohibido): indica que la interfaz no puede convertirse en miembro de la VLAN.
Blank	Blank (En blanco): la interfaz no es miembro de una VLAN. Los paquetes asociados con la interfaz no se reenvían.

Adición de nuevas redes VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add VLAN** (Añadir VLAN).

Ilustración 7-50. Adición de VLAN

3. Introduzca una nueva ID de VLAN y un nombre de VLAN.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade la nueva VLAN y se actualiza el dispositivo.

Asignación de pertenencia a VLAN a un puerto o un LAG

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN en el menú desplegable **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN).
3. En la tabla de pertenencia de puertos a la VLAN (**VLAN Port Membership Table**), asigne un valor haciendo clic en la fila **Static** (Estática) para un puerto o LAG específico. Con cada clic irá alternando entre las opciones U, T y en blanco (no es miembro).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna el puerto o LAG a la VLAN con la designación seleccionada, se actualiza la fila **Current** (Actual) con la designación y también se actualiza el dispositivo.

Modificación de grupos de pertenencia a la VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN en el menú desplegable **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN).
3. Modifique los campos necesarios.
4. En la tabla de pertenencia de puertos a la VLAN (**VLAN Port Membership Table**), cambie el valor de un puerto o LAG haciendo clic en la fila **Static** (Estática) correspondiente a ese puerto o LAG. Con cada clic irá alternando entre las opciones U, T y en blanco (no es miembro).
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la información sobre la pertenencia a la VLAN, se actualiza la fila **Current** (Actual) con los cambios en la designación pertinentes y también se actualiza el dispositivo.

Eliminación de una VLAN

1. Abra la página **VLAN Membership** (Pertenencia a la VLAN).
2. Seleccione una VLAN en el menú desplegable **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN).
3. Seleccione la casilla de verificación **Remove VLAN** (Eliminar VLAN).

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

Se elimina la VLAN seleccionada y se actualiza el dispositivo.

Definición de grupos de pertenencia a la VLAN y asignación de puertos/LAG mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de VLAN

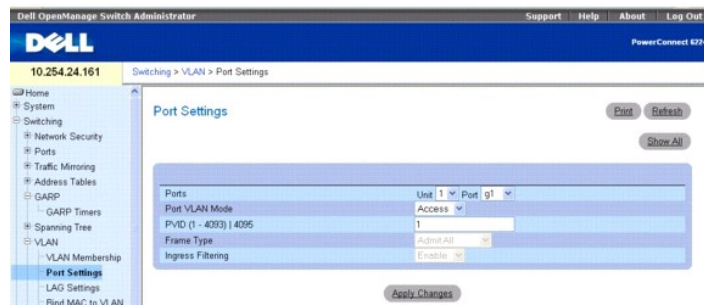
Configuración de puertos de VLAN

En una VLAN basada en puerto, el tráfico sin etiqueta se transmite mediante puentes a través de puertos específicos basados en la PVID de los puertos receptores. Las VLAN basadas en puerto pueden ayudar a optimizar los patrones de tráfico de red porque los paquetes de difusión, de multidifusión y de difusión única desconocida sólo se envían a puertos que pertenecen a la VLAN. Los paquetes que se reciben con una etiqueta de VLAN utilizan esa ID de VLAN para el proceso de conmutación.

Utilice la página **VLAN Port Settings** (Configuración de puertos de VLAN) para identificar un puerto como parte de una VLAN y para definir y modificar los parámetros de puertos de VLAN.

Para visualizar la página **VLAN Port Settings** (Configuración de puertos de VLAN), haga clic en **Switching** (Conmutación) → **VLAN** → **Port Settings** (Configuración de puertos) en la vista de árbol.

Ilustración 7-51. Configuración de puertos de VLAN



La página **VLAN Port Settings** (Configuración de puertos de VLAN) contiene los campos siguientes:

Port (Puerto): especifica la unidad y el puerto incluidos en la VLAN.

Port VLAN Mode (Modo de VLAN de puerto): indica el modo del puerto. Los valores posibles son:

General: el puerto pertenece a redes VLAN, y cada VLAN está definida por el usuario como etiquetada o sin etiquetar (modo 802.1Q completo).

Access (Acceso): el puerto pertenece a una única VLAN sin etiquetar. Cuando un puerto se encuentra en modo de acceso, no es posible designar los tipos de paquete que se aceptan en el puerto (tipo de paquete). Tampoco se puede activar ni desactivar el filtrado de entrada en un puerto de acceso.

Trunk (Combinación de puertos): el puerto pertenece a más de una VLAN y todos los puertos tienen etiqueta (excepto una única VLAN nativa opcional).

PVID (1-4093) | 4095: asigna una ID de VLAN a paquetes sin etiqueta. Los valores posibles son 1-4093 o 4095.

Frame Type (Tipo de trama): especifica el tipo de trama aceptado por el puerto. El valor predeterminado es **Admit All** (Admitir todas). Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): indica que el puerto sólo acepta tramas con etiqueta.

Admit All (Admitir todas): indica que el puerto acepta tramas con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): activa o desactiva el filtrado de entrada en el puerto. El filtrado de entrada descarta las tramas cuya etiqueta de VLAN no coincide con la pertenencia a VLAN del puerto.

Asignación de configuraciones de puertos

- Abra la página **VLAN Port Settings** (Configuración de puertos de VLAN).
- Seleccione el puerto al que desea asignar la configuración desde los menús desplegables **Unit** (Unidad) y **Port** (Puerto).
- Complete los campos restantes de la página.
- Haga clic en **Apply Changes** (Aplicar cambios).

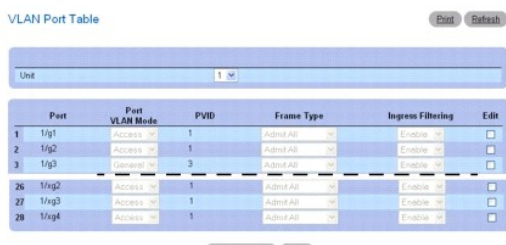
Se define la configuración de los puertos de VLAN y se actualiza el dispositivo.

Visualización de la tabla de puertos de VLAN

1. Abra la página **VLAN Port Settings** (Configuración de puertos de VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **VLAN Port Table** (Tabla de puertos de VLAN).

Ilustración 7-52. Tabla de puertos de VLAN



Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 1/1g1	Access	1	AdmitAll	Enable	<input type="checkbox"/>
2 1/1g2	Access	1	AdmitAll	Enable	<input type="checkbox"/>
3 1/1g3	General	3	AdmitAll	Enable	<input type="checkbox"/>
26 1/1g2	Access	1	AdmitAll	Enable	<input type="checkbox"/>
27 1/1g3	Access	1	AdmitAll	Enable	<input type="checkbox"/>
28 1/1g4	Access	1	AdmitAll	Enable	<input type="checkbox"/>

NOTA: si se ha seleccionado un puerto de tipo **Access** (Acceso), no es posible designar los tipos de paquete que se aceptan en el puerto (tipo de paquete). Tampoco es posible activar ni desactivar el filtrado de entrada en un puerto de acceso.

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de puertos de VLAN correspondiente a otras unidades de la pila, en caso de que existan.

Modificación de la configuración para varios puertos

1. Abra la página **VLAN Port Settings** (Configuración de puertos de VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **VLAN Port Table** (Tabla de puertos de VLAN).

3. Haga clic en **Edit** (Editar) para cada puerto que desee modificar.
4. Edite los campos según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de los puertos de VLAN y se actualiza el dispositivo.

Asignación de puertos a grupos de VLAN mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

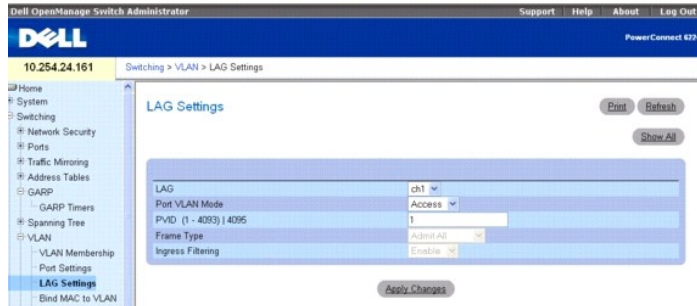
1 Comandos de VLAN

Configuración de LAG de VLAN

Utilice la página **VLAN LAG Settings** (Configuración de LAG de VLAN) para asignar un LAG a una VLAN. Los paquetes sin etiqueta que entran en el conmutador se etiquetan con la ID de los LAG especificada por la PVID.

Para visualizar la página **VLAN LAG Settings** (Configuración de LAG de VLAN), haga clic en **Switching** (Conmutación)→ **VLAN**→ **LAG Settings** (Configuración de LAG) en la vista de árbol.

Ilustración 7-53. Configuración de LAG de VLAN



La página VLAN LAG Settings (Configuración de LAG de VLAN) contiene los campos siguientes:

LAG: especifica el número del LAG incluido en la VLAN.

Port VLAN Mode (Modo de VLAN de puerto): indica el modo de VLAN de puerto para el LAG. Los valores posibles son:

General: el LAG pertenece a redes VLAN, y cada VLAN está definida por el usuario como etiquetada o sin etiquetar (modo 802.1Q completo).

Access (Acceso): el LAG pertenece a una única VLAN sin etiquetar.

Trunk (Combinación de puertos): el LAG pertenece a más de una VLAN y todos los puertos tienen etiqueta (excepto una única VLAN nativa opcional).

PVID (1-4093) | 4095: asigna una ID de VLAN a paquetes sin etiqueta. Los valores del campo posibles son 1-4093 o 4095.

Frame Type (Tipo de trama): especifica el tipo de paquete aceptado por el LAG. El valor predeterminado es Admit Tag Only (Admitir sólo etiqueta). Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): el LAG sólo acepta paquetes con etiqueta.

Admit All (Admitir todos): el LAG acepta paquetes con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): activa o desactiva el filtrado de entrada en el LAG. El filtrado de entrada descarta los paquetes cuya etiqueta de VLAN no coincide con la pertenencia a VLAN del LAG.

Asignación de la configuración de LAG de VLAN

1. Abra la página VLAN LAG Settings (Configuración de LAG de VLAN).
2. Seleccione un LAG en el menú desplegable LAG.
3. Complete los campos restantes de la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros de LAG de VLAN y se actualiza el dispositivo.

Visualización de la tabla de LAG de la VLAN

1. Abra la página VLAN LAG Settings (Configuración de LAG de VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página VLAN LAG Table (Tabla de LAG de la VLAN).

Ilustración 7-54. Tabla de LAG de la VLAN

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 ch1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 ch2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 ch3	Access	1	Admit All	Enable	<input type="checkbox"/>
4 ch4	Access	1	Admit All	Enable	<input type="checkbox"/>
5 ch5	Access	1	Admit All	Enable	<input type="checkbox"/>
6 ch6	Access	1	Admit All	Enable	<input type="checkbox"/>
7 ch7	Access	1	Admit All	Enable	<input type="checkbox"/>
8 ch8	Access	1	Admit All	Enable	<input type="checkbox"/>

Modificación de la configuración para varios LAG

1. Abra la página **VLAN LAG Settings** (Configuración de LAG de VLAN).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **VLAN LAG Table** (Tabla de LAG de la VLAN).
3. Haga clic en **Edit** (Editar) para cada LAG que desee modificar.
4. Edite los campos según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de LAG de VLAN y se actualiza el dispositivo.

Asignación de LAG a grupos de VLAN mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de VLAN

Vinculación de MAC a VLAN

Utilice la página **Bind MAC to VLAN** (Vincular MAC a VLAN) para asignar una entrada MAC a la tabla de VLAN. Una vez especificadas la dirección MAC de origen y la ID de VLAN, todos los puertos del conmutador comparten las configuraciones de MAC a VLAN. La tabla MAC a VLAN admite hasta 128 entradas.

Para visualizar la página **Bind MAC to VLAN** (Vincular MAC a VLAN), haga clic en **Switching** (Conmutación) → **VLAN** → **Bind MAC to VLAN** (Vincular MAC a VLAN) en la vista de árbol.

Ilustración 7-55. Vinculación de MAC a VLAN



La página **Bind MAC to VLAN** (Vincular MAC a VLAN) contiene los campos siguientes:

MAC Address (Dirección MAC): especifica la dirección MAC para una VLAN.

Bind to VLAN (1-4093) (Vincular a VLAN [1-4093]): especifica la VLAN a la que se va a vincular la dirección MAC.

Configuración de la asignación de vinculación de MAC a VLAN

1. Abra la página **Bind MAC to VLAN** (Vincular MAC a VLAN).
2. Especifique la dirección MAC que va a vincular a la VLAN.
3. Especifique la VLAN a la que va a vincular la dirección MAC.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Ahora la dirección MAC y la VLAN indicadas están vinculadas y se ha actualizado el dispositivo.

Visualización de la tabla de LAG de la VLAN

1. Abra la página **Bind MAC to VLAN** (Vincular MAC a VLAN).

- Haga clic en **Show All** (Mostrar todo).

Aparece la página **MAC - VLAN Bind Table** (Tabla de vinculación MAC-VLAN).

Ilustración 7-56. Tabla de vinculación MAC-VLAN

	MAC Address	Bind to VLAN	Remove	Edit
1	0800.6902.0127	2	<input type="checkbox"/>	<input type="checkbox"/>
2	0800.6902.0127	110	<input type="checkbox"/>	<input type="checkbox"/>

Modificación de VLAN para varias direcciones MAC

- Abra la página **Bind MAC to VLAN** (Vincular MAC a VLAN).
- Haga clic en **Show All** (Mostrar todo).
- Aparece la página **MAC - VLAN Bind Table** (Tabla de vinculación MAC-VLAN).
- Haga clic en **Edit** (Editar) para cada dirección MAC con una VLAN que desee modificar.
- Edite los campos **Bind to VLAN** (Vincular a VLAN).
- Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de MAC a VLAN y se actualiza el dispositivo.

Eliminación de una entrada MAC-VLAN

- Abra la página **Bind MAC to VLAN** (Vincular MAC a VLAN).
- Haga clic en **Show All** (Mostrar todo).
- Aparece la página **MAC - VLAN Bind Table** (Tabla de vinculación MAC-VLAN).
- Seleccione **Remove** (Eliminar) para cada entrada que desee eliminar.
- Haga clic en **Apply Changes** (Aplicar cambios).

Se eliminan las entradas y se actualiza el dispositivo.

Vinculación de direcciones MAC a VLAN mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de VLAN

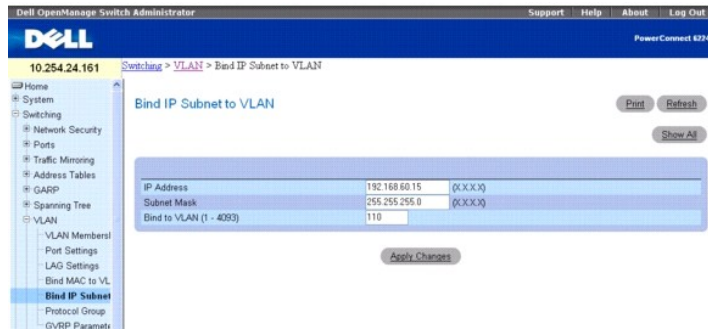
Vinculación de subred IP a VLAN

Una asignación de subred IP a VLAN se define mediante la configuración de una entrada en la tabla de vinculación de subred IP a VLAN, y una entrada se especifica mediante una dirección IP de origen, una máscara de red y la ID de VLAN que se desee. Las configuraciones de vinculación de subred IP a VLAN se comparten en todos los puertos del conmutador. En esta tabla puede haber hasta 64 entradas configuradas.

Utilice la página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN) para asignar una subred IP a una VLAN.

Para visualizar la página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN), haga clic en **Switching** (Conmutación) → **VLAN** → **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN) en la vista de árbol.

Ilustración 7-57. Vinculación de subred IP a VLAN



La página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN) contiene los campos siguientes:

IP Address (Dirección IP): especifica la dirección IP de origen del paquete.

Subnet Mask (Máscara de subred): especifica la máscara de subred IP de origen del paquete.

Bind to VLAN (1–4093) (Vincular a VLAN [1–4093]): especifica la VLAN a la que se asigna la dirección IP.

Vinculación de una subred IP a una VLAN

1. Abra la página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN).
 2. Especifique la dirección IP que va a vincular a la VLAN.
 3. Escriba la subred IP asociada con la dirección IP.
 4. Especifique la ID de VLAN a la que desea asignar la dirección IP y la máscara de subred.
 5. Haga clic en **Apply Changes** (Aplicar cambios).
- Ahora la VLAN y la subred IP indicadas están vinculadas y se ha actualizado el dispositivo.

Visualización de la tabla de vinculación subred IP-VLAN

1. Abra la página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN).
2. Haga clic en **Show All** (Mostrar todo).
3. Aparece la página **IP Subnet - VLAN Bind Table** (Tabla de vinculación subred IP-VLAN).

Ilustración 7-58. Tabla de vinculación subred IP-VLAN

	IP Address	Subnet Mask	Bind to VLAN	Remove	Edit
1	192.168.12.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.13.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.60.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>

Buttons for 'Print', 'Refresh', 'Apply Changes', and 'Back' are visible.

Modificación de la VLAN vinculada a varias direcciones IP

1. Abra la página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN).
2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **IP Subnet - VLAN Bind Table** (Tabla de vinculación subred IP-VLAN).
3. Haga clic en **Edit** (Editar) para cada entrada que desee modificar.
4. Edite los campos según convenga.

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

Se modifica la configuración de vinculación a VLAN y se actualiza el dispositivo.

Eliminación de una entrada MAC-subred IP

1. Abra la página **Bind IP Subnet to VLAN** (Vincular subred IP a VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **IP Subnet - VLAN Bind Table** (Tabla de vinculación subred IP-VLAN).

3. Seleccione **Remove** (Eliminar) para cada entrada que desee eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se eliminan las entradas y se actualiza el dispositivo.

Vinculación de subredes IP a VLAN mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de VLAN

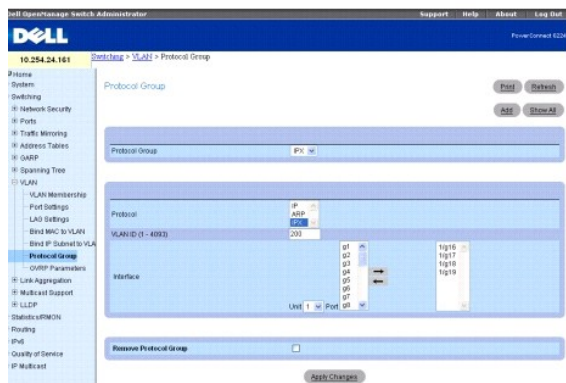
Grupo de protocolo

En una VLAN basada en protocolo, el tráfico se transmite mediante puentes a través de puertos específicos basados en el protocolo de la VLAN. Filtros de paquetes definidos por el usuario determinan si un paquete concreto pertenece a una VLAN concreta. Las VLAN basadas en protocolo suelen usarse en situaciones en las que los segmentos de red contienen hosts que ejecutan múltiples protocolos.

Utilice la página **Protocol Group** (Grupo de protocolo) para configurar qué EtherTypes van con las VLAN correspondientes y, a continuación, habilite algunos puertos para que usen esta configuración.

Para visualizar la página **Protocol Group** (Grupo de protocolo), haga clic en **Switching** (Conmutación)→ **VLAN**→ **Protocol Group** (Grupo de protocolo) en la vista de árbol.

Ilustración 7-59. Grupo de protocolo



La página **Protocol Group** (Grupo de protocolo) contiene los campos siguientes:

Protocol Group (Grupo de protocolo): muestra el nombre asociado con la ID del grupo de protocolo. Para crear un nuevo grupo, haga clic en el botón **Add** (Añadir).

Protocol (Protocolo): especifica el protocolo asociado con este grupo.

VLAN ID (1-4093) (ID de VLAN [1-4093]): especifica la ID de VLAN asociada con este grupo.

Interface (Interfaz): selecciona las interfaces que se van a añadir o eliminar de este grupo. Resalte las interfaces que desee incluir en el grupo de protocolo y haga clic en la flecha derecha. Las interfaces que aparecen en la columna de la derecha forman parte del grupo de protocolo.

Remove Protocol Group (Eliminar grupo de protocolo): elimina el grupo de protocolo mostrado en pantalla cuando se selecciona esta opción y se hace clic en **Apply Changes** (Aplicar cambios). Para eliminar varios grupos al mismo tiempo, haga clic en **Show All** (Mostrar todo) y utilice las casillas de verificación **Remove** (Eliminar) de la tabla de grupo de protocolo (**Protocol Group Table**).

Adición de un grupo de protocolo

1. Abra la página **Protocol Group** (Grupo de protocolo).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add Protocol Group** (Añadir grupo de protocolo).

Ilustración 7-60. Adición de grupo de protocolo



3. Especifique un nuevo nombre de grupo de protocolo y una ID de VLAN para asociarla con este grupo.
4. Vuelva a la página **Protocol Group** (Grupo de protocolo).
5. Seleccione el grupo de protocolo que ha añadido y, a continuación, seleccione el protocolo.
6. En la primera columna **Interface** (Interfaz), haga clic para resaltar las interfaces que desea añadir al grupo de protocolo. Para seleccionar varias interfaces, pulse <Mayús> (en el caso de interfaces contiguas) o <Ctrl> (en el caso de interfaces no contiguas) mientras hace clic con el ratón.
7. Haga clic en la flecha derecha.

Las interfaces seleccionadas pasan a la segunda columna. Todas las interfaces de esta columna forman parte del grupo de protocolo.

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

Se añade el grupo de protocolo y se actualiza el dispositivo.

Modificación de la configuración del grupo de protocolo de VLAN

1. Abra la página **Protocol Group** (Grupo de protocolo).
2. Especifique el protocolo que desea modificar en el menú desplegable **Protocol Group ID** (ID de grupo de protocolo).
3. Cambie el protocolo o la ID de VLAN según convenga.
4. Para añadir una interfaz al grupo, haga clic en la interfaz que desee de la primera columna para resaltarla. Para seleccionar varias interfaces, pulse <Mayús> (en el caso de interfaces contiguas) o <Ctrl> (en el caso de interfaces no contiguas) mientras hace clic con el ratón.
5. Haga clic en la flecha derecha.

La interfaz seleccionada pasa a la segunda columna. Todas las interfaces de esta columna forman parte del grupo de protocolo.

6. Para eliminar una interfaz del grupo, haga clic en la interfaz que desee de la segunda columna para resaltarla.
7. Haga clic en la flecha izquierda.

La interfaz seleccionada se elimina de la segunda columna.

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

Se modifican los parámetros del grupo de protocolo de VLAN y se actualiza el dispositivo.

Eliminación de varios protocolos de la tabla de grupo de protocolo

1. Abra la página **Protocol Group** (Grupo de protocolo).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Protocol Group Table** (Tabla de grupo de protocolo).

Ilustración 7-61. Tabla de grupo de protocolo

Group Name	Protocol	VLAN ID	Interface	Remove
1	IPX	200	1/g1/16 1/g1/17 1/g1/18 1/g1/19	<input type="checkbox"/> Edit
2	IPV2	110	1/g1/21 1/g1/22 1/g1/23 1/g1/24	<input type="checkbox"/> Edit

3. Seleccione **Remove** (Eliminar) para los grupos de protocolo que desee eliminar.

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

Se elimina el protocolo y se actualiza el dispositivo.

Configuración de grupos de protocolo mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos de VLAN

Parámetros de GVRP

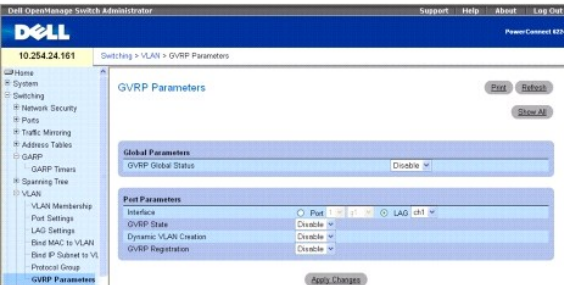
El protocolo de registro de VLAN de GARP ofrece un mecanismo que permite a los conmutadores de red registrar dinámicamente información de pertenencia a la VLAN (y también anular su registro) con los conmutadores de red MAC conectados al mismo segmento, así como distribuir esa información a todos los conmutadores de red LAN con puentes que admitan GVRP.

El funcionamiento del GVRP depende de los servicios proporcionados por el protocolo genérico de registro de atributos (GARP). El GVRP puede crear hasta 1 024 redes VLAN.

Utilice la página **GVRP Global Parameters** (Parámetros globales de GVRP) para activar el GVRP globalmente. También puede activar el GVRP en cada interfaz por separado.

Para visualizar la página **GVRP Global Parameters** (Parámetros globales de GVRP), haga clic en **Switching** (Conmutación)→ **VLAN**→ **GVRP Parameters** (Parámetros de GVRP) en la vista de árbol.

Ilustración 7-62. Parámetros globales de GVRP



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

GVRP Global Status (Estado global de GVRP): activa o desactiva GVRP en el conmutador. El protocolo GVRP está desactivado de forma predeterminada.

Interface (Interfaz): especifica la unidad y puerto o el LAG para los que se ha activado GVRP.

GVRP State (Estado de GVRP): activa o desactiva GVRP en la interfaz especificada.

Dynamic VLAN Creation (Creación de VLAN dinámica): activa o desactiva la creación de VLAN a través de GVRP.

GVRP Registration (Registro de GVRP): activa o desactiva el registro de GVRP.

Activación de GVRP en el conmutador

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 activa en el conmutador.

Activación del registro de VLAN a través de GVRP

1. Abra la página **GVRP Global Parameters** (Parámetros globales de GVRP).
2. Seleccione **Enable** (Activar) en el campo **GVRP Global Status** (Estado global de GVRP) para la interfaz que desee.
3. Seleccione **Enable** (Activar) en el campo **GVRP Registration** (Registro de GVRP).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El registro de VLAN de GVRP se activa en el puerto y se actualiza el dispositivo.

Visualización de la tabla de parámetros de puerto de GVRP

1. Abra la página **GVRP Global Parameters** (Parámetros globales de GVRP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **GVRP Port Parameters Table** (Tabla de parámetros de puerto de GVRP).

Ilustración 7-63. Tabla de parámetros de puerto de GVRP

Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Copy To	Edit	
1	1ig1	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
2	1ig2	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
3	1ig3	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>

26	1hg2	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
27	1hg3	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
28	1hg4	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>

LAGs						
29	lag1	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
30	lag2	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
31	lag3	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
32	lag4	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
33	lag5	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
34	lag6	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
35	lag7	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>
36	lag8	Disable ▼	Enable ▼	Enable ▼	<input type="checkbox"/>	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de parámetros de puerto de GVRP correspondiente a otras unidades de la pila, en caso de que existan.

Copia de los parámetros de GVRP

1. Abra la página **GVRP Global Parameters** (Parámetros globales de GVRP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **GVRP Port Parameters Table** (Tabla de parámetros de puerto de GVRP).
3. Especifique el puerto o LAG del que está copiando en **Copy Parameters From** (Copiar parámetros de).
4. Haga clic en **Copy To** (Copiar en) para cada interfaz o LAG que deba recibir estos parámetros.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se copia la configuración de los parámetros de puerto de GVRP y se actualiza el dispositivo.

Modificación de los parámetros de GVRP para varios puertos

1. Abra la página **GVRP Global Parameters** (Parámetros globales de GVRP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **GVRP Port Parameters Table** (Tabla de parámetros de puerto de GVRP).
3. Haga clic en **Edit** (Editar) para cada interfaz o LAG que desee modificar.
4. Edite los campos de parámetros de puerto de GVRP según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de los parámetros de puerto de GVRP y se actualiza el dispositivo.

Configuración de GVRP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos GVRP

Agregación de puertos

La agregación de enlaces permite agregar uno o varios enlaces Ethernet en modo dúplex completo (FDX) para formar un grupo de agregación de enlaces (LAG). Esto permite al conmutador de red tratar al LAG como si se tratase de un único enlace.

Se admiten LAG estáticos. Cuando se añade un puerto a un LAG como miembro estático, ni transmite ni recibe LACPDU.

Para visualizar la página de menú **Link Aggregation** (Agregación de enlaces), haga clic en **Switching** (Conmutación)→ **Link Aggregation** (Agregación de enlaces) en la vista de árbol. La página **Link Aggregation** (Agregación de enlaces) contiene enlaces a las funciones siguientes:

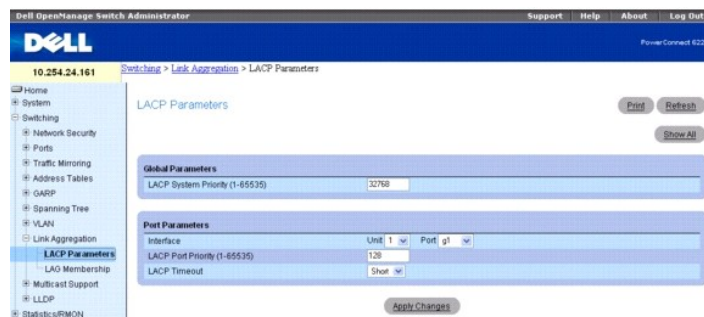
- 1 [Parámetros de LACP](#)
- 1 [Pertencia a LAG](#)
- 1 [Configuración de hash de LAG](#)
- 1 [Resumen de hash de LAG](#)

Parámetros de LACP

La agregación de enlaces se inicia y mantiene por los intercambios periódicos de LACPDU. Utilice la página **LACP Parameters** (Parámetros de LACP) para configurar los grupos LAG de LACP.

Para visualizar la página **LACP Parameters** (Parámetros de LACP), haga clic en **Switching** (Conmutación)→ **Link Aggregation** (Agregación de enlaces)→ **LACP Parameters** (Parámetros de LACP) en la vista de árbol.

Ilustración 7-64. Parámetros de LACP



La página **LACP Parameters** (Parámetros de LACP) está dividida en dos secciones: **Global Parameters** (Parámetros globales) y **Port Parameters** (Parámetros de puerto). A continuación se describen los campos de esta página:

Parámetros globales

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.

Parámetros de puerto

Interface (Interfaz): especifica el número de unidad y de puerto a los que se asignan valores de tiempo de espera y prioridad.

LACP Port Priority (1-65535) (Prioridad de puerto de LACP [1-65535]): especifica el valor de prioridad de LACP para el puerto especificado. El valor predeterminado es 1.

LACP Timeout (Tiempo de espera de LACP): especifica un tiempo de espera de LACP administrativo. Los valores posibles son:

Short (Corto): especifica un valor de tiempo de espera corto.

Long (Largo): especifica un valor de tiempo de espera largo. Éste es el valor predeterminado.

Definición de los parámetros de agregación de enlaces

1. Abra la página **LACP Parameters** (Parámetros de LACP).
2. Rellene los campos según convenga.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se definen los parámetros y se actualiza el dispositivo.

Visualización de la tabla de parámetros de LACP

1. Abra la página **LACP Parameters** (Parámetros de LACP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **LACP Parameters Table** (Tabla de parámetros de LACP).

Ilustración 7-65. Tabla de parámetros de LACP

Port	Port Priority	LACP Timeout	Edit
1 1g1	120	Long	<input checked="" type="checkbox"/>
2 1g2	120	Long	<input type="checkbox"/>
3 1g3	120	Long	<input type="checkbox"/>

26 1g2	120	Long	<input type="checkbox"/>
27 1g3	120	Long	<input type="checkbox"/>
28 1g4	120	Long	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de parámetros de LACP correspondiente a otras unidades de la pila, en caso de que existan.

Modificación de los parámetros de LACP para varios puertos

1. Abra la página **LACP Parameters** (Parámetros de LACP).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **LACP Parameters Table** (Tabla de parámetros de LACP).

3. Haga clic en **Edit** (Editar) para cada puerto que desee modificar.
4. Edite los campos según convenga.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de los parámetros de LACP y se actualiza el dispositivo.

Configuración de los parámetros de LACP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

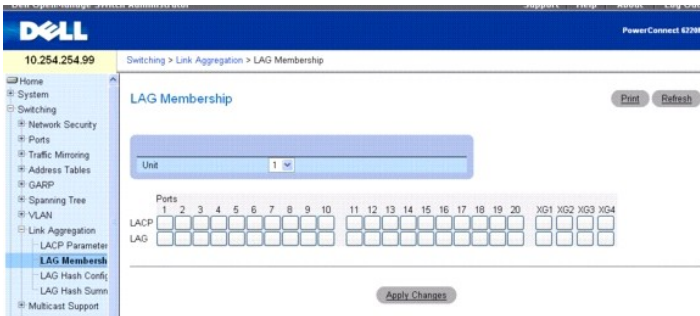
- 1 Comandos LACP

Pertenencia a LAG

El conmutador admite 18 LAG por sistema y 8 puertos por LAG. Utilice la página **LAG Membership** (Pertenencia a LAG) para asignar puertos a los LAG y LACP.

Para visualizar la página **LAG Membership** (Pertenencia a LAG), haga clic en **Switching** (Conmutación)→ **Link Aggregation** (Agregación de enlaces)→ **LACP Membership** (Pertenencia a LAG) en la vista de árbol.

Ilustración 7-66. Pertenencia a LAG



La página **LAG Membership** (Pertenencia a LAG) contiene una tabla con los campos siguientes:

LACP: agrega un puerto LAG a la pertenencia a LACP. En el caso de puertos con un número en la fila **LAG**, puede hacer clic en la fila **LACP** para cambiar el LACP a "on" (activado). Con cada clic se alterna entre las opciones L (LACP) y en blanco (no LACP).

LAG: añade un puerto a un LAG e indica el LAG específico al que pertenece el puerto. Con cada clic se alterna entre los números de LAG, del 1 al 18, y la opción en blanco (ningún LAG asignado).

Adición de un puerto a un LAG

1. Abra la página **LAG Membership** (Pertenencia a LAG).
2. Haga clic en la fila **LAG** para seleccionar el LAG deseado para el puerto.

Se muestra el número de LAG correspondiente a dicho puerto. El número de LAG aumentará cada vez que haga clic con el ratón, hasta llegar a 18, y luego volverá a la opción en blanco (ningún LAG asignado).

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

Se asigna el puerto al LAG seleccionado y se actualiza el dispositivo.

Adición de un puerto LAG a un LACP

1. Abra la página **LAG Membership** (Pertenencia a LAG).
2. Haga clic en la fila **LACP** para que el puerto LAG deseado adopte el valor **L**.

NOTA: para poder agregar el puerto a un LACP, éste debe estar asignado a un LAG.

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

El puerto LAG se agrega al LACP y el dispositivo se actualiza.

Asignación de puertos a LAG y LACP mediante los comandos de la CLI

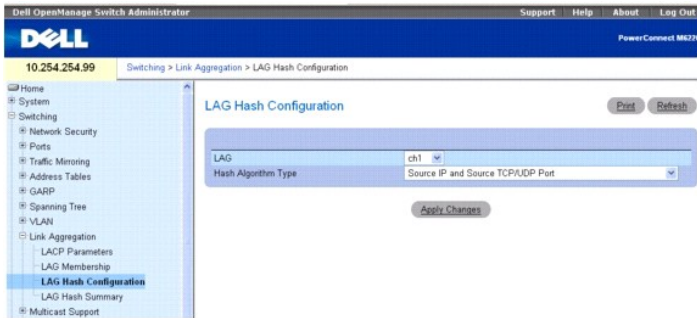
Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

Configuración de hash de LAG

Utilice el algoritmo HASH de LAG para establecer el modo de distribución de tráfico en el enlace del agregador. Para cada combinación de puerto se puede establecer un tipo de HASH.

Para visualizar la página **LAG Hash Configuration** (Configuración de hash de LAG), haga clic en **Switching** (Conmutación)→ **Link Aggregation** (Agregación de enlaces)→ **LAG Hash Configuration** (Configuración de hash de LAG) en la vista de árbol.

Ilustración 7-67. Configuración de hash de LAG



La página **LAG Hash Configuration** (Configuración de hash de LAG) contiene los campos siguientes:

LAG: el menú desplegable proporciona una lista con los números de LAG.

Hash Algorithm Type (Tipo de algoritmo hash): el algoritmo HASH para flujos de tráfico de difusión única puede ser del siguiente tipo:

- 1 Source MAC, VLAN, EtherType, SourceModule and Port Id (MAC de origen, VLAN, EtherType, SourceModule e ID de puerto)
- 1 Destination MAC, VLAN, EtherType, SourceModule and Port Id (MAC de destino, VLAN, EtherType, SourceModule e ID de puerto)
- 1 Source IP and Source TCP/UDP Port (IP de origen y puerto TCP/UDP de origen) (valor predeterminado)
- 1 Destination IP and Destination TCP/UDP Port (IP de destino y puerto TCP/UDP de destino)
- 1 Source/Destination MAC, VLAN, EtherType, source MODID/port (MAC de origen/destino, VLAN, EtherType, MODID/puerto de origen)
- 1 Source/Destination IP and source/destination TCP/UDP port (IP de origen/destino y puerto TCP/UDP de origen/destino)

Configuración de hash de LAG

1. Abra la página **LAG Hash Configuration** (Configuración de hash de LAG).
2. Seleccione el LAG que desea configurar y el algoritmo hash que va a asignar al LAG.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifican los parámetros y se actualiza el dispositivo.

Configuración de hash de LAG mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

Resumen de hash de LAG

La página **LAG Hash Summary** (Resumen de hash de LAG) enumera los canales del sistema y su tipo de algoritmo hash asignado.

Para visualizar la página **LAG Hash Summary** (Resumen de hash de LAG), haga clic en **Switching** (Conmutación)→ **Link Aggregation** (Agregación de enlaces)→ **LAG Hash Summary** (Resumen de hash de LAG) en la vista de árbol.

Ilustración 7-68. Resumen de hash de LAG

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main content area is titled 'LAG Hash Summary' and contains a table with the following data:

LAGs	Hash Algorithm Type	
1	ch1	Source IP and Source TCP/UDP Port
2	ch2	Source IP and Source TCP/UDP Port
3	ch3	Source IP and Source TCP/UDP Port
4	ch4	Source IP and Source TCP/UDP Port
5	ch5	Source IP and Source TCP/UDP Port
6	ch6	Source IP and Source TCP/UDP Port
7	ch7	Source IP and Source TCP/UDP Port
8	ch8	Source IP and Source TCP/UDP Port
9	ch9	Source IP and Source TCP/UDP Port
10	ch10	Source IP and Source TCP/UDP Port
11	ch11	Source IP and Source TCP/UDP Port
12	ch12	Source IP and Source TCP/UDP Port
13	ch13	Source IP and Source TCP/UDP Port
14	ch14	Source IP and Source TCP/UDP Port
15	ch15	Source IP and Source TCP/UDP Port
16	ch16	Source IP and Source TCP/UDP Port
17	ch17	Source IP and Source TCP/UDP Port
18	ch18	Source IP and Source TCP/UDP Port

La página **LAG Hash Summary** (Resumen de hash de LAG) contiene una tabla con los campos siguientes:

LAGs (LAG): muestra una lista con los números de LAG.

Hash Algorithm Type (Tipo de algoritmo hash): muestra el tipo de algoritmo HASH para flujos de tráfico de difusión única que está asociado con el LAG.

Visualización del resumen de algoritmo hash de LAG mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de canal de puerto

Administración de la compatibilidad con multidifusión

El conmutador utiliza la base de datos de reenvío de multidifusión de nivel 2 para tomar decisiones de reenvío para los paquetes que llegan con una dirección MAC de destino de multidifusión. Al limitar la multidifusión a determinados puertos del conmutador, se evita que el tráfico llegue a partes de la red en las que es innecesario.

Cuando un paquete llega al conmutador, la dirección MAC de destino se combina con la ID de VLAN y se lleva a cabo una búsqueda en la base de datos de reenvío de nivel 2. Si no se localiza ninguna coincidencia, el paquete se distribuye a todos los puertos de la VLAN o bien se descarta, según la configuración del conmutador. En cambio, si se localiza una coincidencia, el paquete sólo se reenvía a los puertos que pertenecen al grupo de multidifusión en cuestión.

Para visualizar la página de menú **Multicast Support** (Compatibilidad con multidifusión), haga clic en **Switching** (Conmutación) → **Multicast Support** (Compatibilidad con multidifusión) en la vista de árbol. La página **Multicast Support** (Compatibilidad con multidifusión) contiene enlaces a las funciones siguientes:

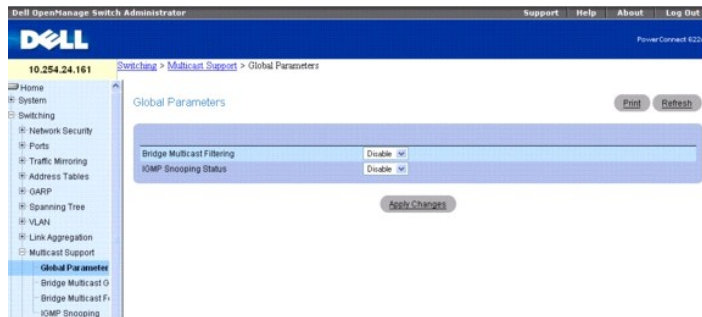
- 1 [Parámetros globales de multidifusión](#)
- 1 [Grupo de multidifusión de puente](#)
- 1 [Reenvío de multidifusión de puente](#)
- 1 [Inspección de IGMP](#)

Parámetros globales de multidifusión

Utilice la página **Multicast Global Parameters** (Parámetros globales de multidifusión) para activar el filtrado de multidifusión de puente o la inspección de IGMP en el conmutador. Los parámetros de estas funciones se pueden modificar desde las páginas web [Reenvío de multidifusión de puente](#) e [Inspección de IGMP](#).

Para visualizar la página **Multicast Global Parameters** (Parámetros globales de multidifusión), haga clic en **Switching** (Conmutación) → **Multicast Support** (Compatibilidad con multidifusión) → **Global Parameters** (Parámetros globales) en la vista de árbol.

Ilustración 7-69. Parámetros globales de multidifusión



La página **Multicast Global Parameters** (Parámetros globales de multidifusión) contiene los campos siguientes:

Bridge Multicast Filtering (Filtrado de multidifusión de puente): activa o desactiva el filtrado de multidifusión de puente. El valor predeterminado es Disabled (Desactivado).

IGMP Snooping Status (Estado de inspección de IGMP): activa o desactiva la inspección de IGMP. El valor predeterminado es Disabled (Desactivado).

Activación del filtrado de multidifusión de puente en el conmutador

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 activa en el conmutador.

Activación del reenvío de multidifusión o la inspección de IGMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

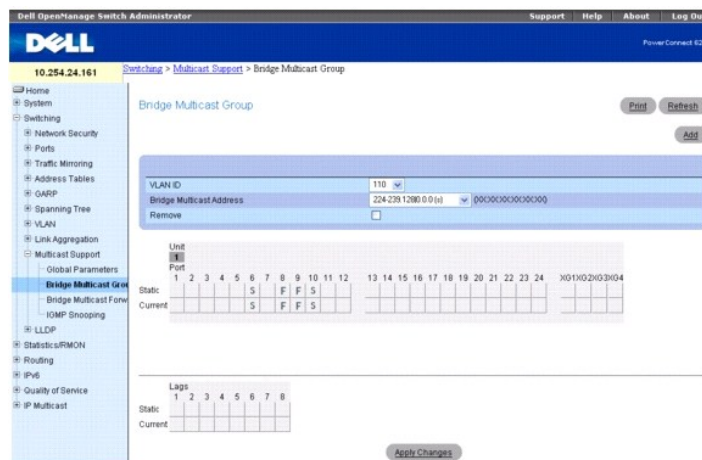
- 1 Comandos de la tabla de direcciones

Grupo de multidifusión de puente

Utilice la página **Bridge Multicast Group** (Grupo de multidifusión de puente) para crear nuevos grupos de servicio de multidifusión o para modificar puertos y LAG asignados a los grupos de servicio de multidifusión existentes. Las interfaces conectadas se muestran en las tablas **Port** (Puerto) y **LAG**, y reflejan el modo en que cada una está unida al grupo de multidifusión.

Para visualizar la página **Bridge Multicast Group** (Grupo de multidifusión de puente), haga clic en **Switching** (Conmutación)→ **Multicast Support** (Compatibilidad con multidifusión)→ **Bridge Multicast Group** (Grupo de multidifusión de puente) en la vista de árbol.

Ilustración 7-70. Grupo de multidifusión de puente



La página **Bridge Multicast Group** (Grupo de multidifusión de puente) contiene los campos siguientes:

VLAN ID (ID de VLAN): selecciona la VLAN a la que se añade un grupo de multidifusión o en la que se modifican puertos de un grupo de multidifusión existente.

Bridge Multicast Address (Dirección de multidifusión de puente): identifica la dirección MAC o dirección IP de un grupo de multidifusión asociada con la ID de VLAN seleccionada. Utilice el botón **Add** (Añadir) para asociar una nueva dirección con una ID de VLAN.

Remove (Eliminar): al seleccionar esta opción, se elimina una dirección de multidifusión de puente.

Tablas de puertos y LAG miembros

Las tablas de **Bridge Multicast Group** (Grupo de multidifusión de puente) muestran los puertos y LAG que son miembros del grupo de multidifusión, además de indicar si son estáticos (S), dinámicos (D) o si están prohibidos (F). Las tablas tienen dos filas: **Static** (Estática) y **Current** (Actual). Desde esta página sólo se puede acceder a la fila **Static** (Estática). La fila **Current** (Actual) se actualiza al modificar la línea **Static** (Estático) y hacer clic en **Apply Changes** (Aplicar cambios).

La página **Bridge Multicast Group** (Grupo de multidifusión de puente) contiene dos tablas que se pueden editar:

Unit and Ports (Unidad y puertos): muestra y asigna pertenencia a grupo de multidifusión a los puertos. Para asignar pertenencia, haga clic en **Static** (Estática) para un puerto concreto. Con cada clic irá alternando entre las opciones S, F y en blanco. Consulte las definiciones en la tabla siguiente.

LAGs (LAG): muestra y asigna pertenencia a grupo de multidifusión a los LAG. Para asignar pertenencia, haga clic en **Static** (Estática) para un LAG concreto. Con cada clic irá alternando entre las opciones S, F y en blanco. Consulte las definiciones en la tabla siguiente.

La tabla siguiente contiene las definiciones de los valores de administración IGMP de puertos/LAG.

Tabla 7-2. Valores de administración IGMP de puertos/LAG

Control del puerto	Definición
D	Dynamic (Dinámico): indica que el puerto o LAG se ha unido al grupo de multidifusión de manera dinámica (se indica en la fila <i>Current</i> [Actual]).
S	Static (Estático): conecta el puerto al grupo de multidifusión como miembro estático en la fila <i>Static</i> (Estático). Se indica en la fila <i>Current</i> (Actual) tras hacer clic en Apply Changes (Aplicar cambios).
Blank	Blank (En blanco): indica que el puerto no está conectado a ningún grupo de multidifusión.

Adición de direcciones de multidifusión de puente

1. Abra la página **Bridge Multicast Group** (Grupo de multidifusión de puente).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add Bridge Multicast Group** (Añadir grupo de multidifusión de puente).

Ilustración 7-71. Adición de grupo de multidifusión de puente

3. Seleccione una ID de VLAN en el menú desplegable.
4. Defina la nueva dirección IP o MAC de multidifusión de puente.
5. En las tablas de **Bridge Multicast Group** (Grupo de multidifusión de puente), asigne un valor haciendo clic en la fila **Static** (Estático) para un puerto o LAG específico. Con cada clic irá alternando entre las opciones S, F y en blanco. (no es miembro).
6. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección de multidifusión de puente se asigna al grupo de multidifusión, se asignan los puertos o LAG al grupo (con las filas **Current** [Actual] actualizadas con los valores **Static** [Estático]) y se actualiza el dispositivo.

Asignación de una interfaz a un grupo de multidifusión existente

1. Abra la página **Bridge Multicast Group** (Grupo de multidifusión de puente).
2. Seleccione la ID de VLAN en el menú desplegable.
Se muestra la dirección de multidifusión de puente asociada.
3. En las tablas de **Bridge Multicast Group** (Grupo de multidifusión de puente), asigne un valor haciendo clic en la fila **Static** (Estático) para un puerto o LAG específico. Con cada clic irá alternando entre las opciones S, F y en blanco (no es miembro).
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se asigna la interfaz al grupo de multidifusión, se actualiza la fila **Current** (Actual) con el valor **Static** (Estático) y también se actualiza el dispositivo.

Eliminación de un grupo de multidifusión de puente

1. Abra la página **Bridge Multicast Group** (Grupo de multidifusión de puente).
2. Seleccione en el menú desplegable la ID de VLAN asociada con el grupo de multidifusión de puente que desea eliminar.
Se muestra la dirección de multidifusión de puente y los puertos/LAG asignados.
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se elimina el grupo de multidifusión de puente seleccionado y se actualiza el dispositivo.

Administración de miembros del servicio de multidifusión mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

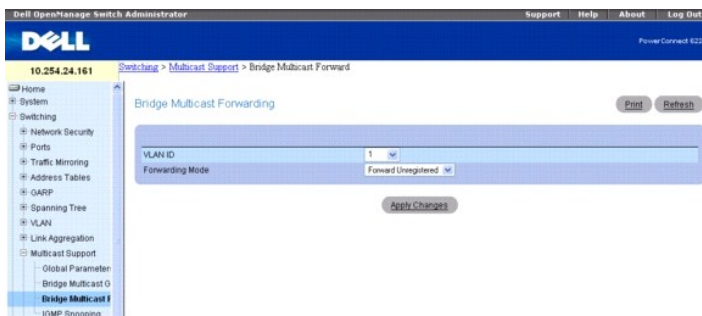
- 1 Comandos de la tabla de direcciones

Reenvío de multidifusión de puente

Utilice la página **Bridge Multicast Forward** (Reenvío de multidifusión de puente) para permitir la conexión de puertos o LAG a un conmutador que está conectado a un conmutador de multidifusión contiguo. Una vez activada la inspección de IGMP, los paquetes de multidifusión se reenvían a la VLAN o puerto adecuado.

Para visualizar la página **Bridge Multicast Forward** (Reenvío de multidifusión de puente), haga clic en **Switching** (Conmutación)→ **Multicast Support** (Compatibilidad con multidifusión)→ **Bridge Multicast Forward** (Reenvío de multidifusión de puente) en la visa de árbol.

Ilustración 7-72. Reenvío de multidifusión de puente



La página **Bridge Multicast Forward** (Reenvío de multidifusión de puente) contiene los campos siguientes y dos tablas que se pueden editar:

VLAN ID (ID de VLAN): selecciona la VLAN afectada.

Forwarding Mode (Modo de reenvío): especifica el modo de reenvío de multidifusión para la VLAN seleccionada. Los valores posibles son:

Forward Unregistered (Reenviar no registrados): permite el reenvío de paquetes de multidifusión IPv4 con una dirección de destino que no coincide con ninguno de los grupos anunciados en informes de pertenencia a IGMP anteriores.

Forward All (Reenviar todo): permite el reenvío de paquetes de multidifusión registrados y no registrados.

Filter Unregistered (Filtrar no registrados): impide el reenvío de los paquetes de multidifusión IPv4 que tengan una dirección de destino que no coincida con ninguno de los grupos anunciados en informes de pertenencia a IGMP anteriores.

Cambio del modo de reenvío de multidifusión de puente

1. Abra la página **Bridge Multicast Forward** (Reenvío de multidifusión de puente).
2. Seleccione una ID de VLAN en el menú desplegable.
3. Seleccione en el menú desplegable el modo de reenvío (**Forwarding Mode**) que desea asignar a la VLAN.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La VLAN se actualiza con el valor de **Forwarding Mode** (Modo de reenvío) y también se actualiza el dispositivo.

Administración de grupos LAG y puertos conectados a enrutadores de multidifusión mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

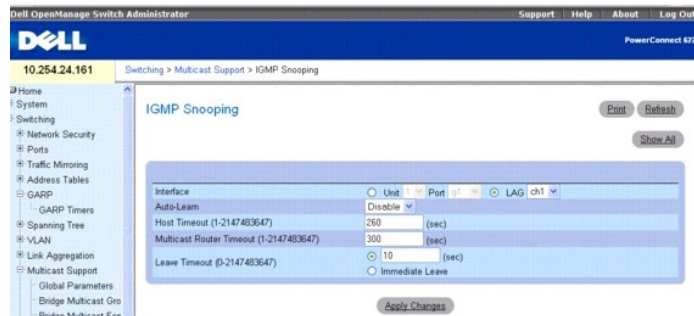
- 1 Comandos de la tabla de direcciones

Inspección de IGMP

Utilice la página **IGMP Snooping** (Inspección de IGMP) para añadir miembros de IGMP.

Para visualizar la página **IGMP Snooping** (Inspección de IGMP), haga clic en **Switching** (Conmutación)→ **Multicast Support** (Compatibilidad con multidifusión)→ **IGMP Snooping** (Inspección de IGMP) en la vista de árbol.

Ilustración 7-73. Inspección de IGMP



La página **IGMP Snooping** (Inspección de IGMP) contiene los campos siguientes:

Interface (Interfaz): selecciona la unidad y el puerto afectados.

Auto-Learn (Obtención automática): activa o desactiva la obtención automática en el conmutador.

Host Timeout (Tiempo de espera de host): especifica el tiempo que transcurre hasta que caduca una entrada de inspección de IGMP. El valor predeterminado es 260 segundos.

Multicast Router Timeout (Tiempo de espera de enrutador de multidifusión): especifica el tiempo que transcurre hasta que caduca una entrada de enrutador de multidifusión. El valor predeterminado es 300 segundos.

Leave Timeout (Tiempo de espera de cese): especifica el tiempo, en segundos, que transcurre desde que se recibe un mensaje de cese del puerto hasta que caduca la entrada. Especifique el tiempo de espera o haga clic en **Immediate Leave** (Cese inmediato) para especificar un tiempo de espera inmediato. El valor predeterminado de tiempo de espera es 10 segundos.

Activación de la inspección de IGMP en el conmutador

1. Abra la página **IGMP Snooping** (Inspección de IGMP).
2. Seleccione la unidad y el puerto que desea configurar desde el campo **Interface** (Interfaz).

3. Rellene los campos de la página según convenga.
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Se activa la inspección de IGMP en el conmutador.

Visualización de la tabla de inspección de IGMP

1. Abra la página **IGMP Snooping** (Inspección de IGMP).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **IGMP Snooping Table** (Tabla de inspección de IGMP).

Ilustración 7-74. Tabla de inspección de IGMP

Port	Auto Leaves Enable	Host Timeout	Multicast Router Timeout	Leave Timeout	Copy To	Edit
1 1/ig1	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
2 1/ig2	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
3 1/ig3	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
LAGs						
29 ch1	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
30 ch2	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
31 ch3	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
32 ch4	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
33 ch5	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
34 ch6	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
35 ch7	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
36 ch8	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de inspección de IGMP correspondiente a otras unidades de la pila, en caso de que existan.

Modificación de la configuración de la inspección de IGMP para varios puertos o LAG

1. Abra la página **IGMP Snooping** (Inspección de IGMP).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **IGMP Snooping Table** (Tabla de inspección de IGMP).
3. Haga clic en **Edit** (Editar) para cada puerto o LAG que desee modificar.
 4. Edite los campos de inspección de IGMP según convenga.
 5. Haga clic en **Apply Changes** (Aplicar cambios).
- Se modifica la configuración de la inspección de IGMP y se actualiza el dispositivo.

Copia de la configuración de la inspección de IGMP en varios puertos o LAG

1. Abra la página **IGMP Snooping** (Inspección de IGMP).
 2. Haga clic en **Show All** (Mostrar todo).
- Aparece la página **IGMP Snooping Table** (Tabla de inspección de IGMP).
3. Haga clic en **Copy Parameters From** (Copiar parámetros de).
 4. Seleccione la unidad/puerto o el LAG que se utilizará como origen de los parámetros deseados.

- Haga clic en **Copy To** (Copiar en) para la unidad/puertos o el LAG en los que se copiarán estos parámetros.
- Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica la configuración de la inspección de IGMP y se actualiza el dispositivo.

Configuración de la inspección de IGMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de inspección de IGMP

Configuración del protocolo de detección de nivel de enlace (LLDP)

El estándar definido IEEE 802.1AB, protocolo de detección de nivel de enlace (LLDP), permite que las estaciones que residen en una LAN 802 puedan ofrecer más funciones y descripciones físicas. Un administrador de red visualiza esta información para identificar la topología del sistema y detectar posibles configuraciones erróneas en la LAN.

LLDP es un protocolo unidireccional; no existen secuencias de petición y respuesta. La información la anuncian estaciones que implementan la función de transmisión, y la reciben y procesan estaciones que implementan la función de recepción. Las funciones de transmisión y recepción se pueden activar y desactivar en cada puerto por separado. De forma predeterminada, tanto la transmisión como la recepción están desactivadas en todos los puertos. La aplicación es responsable de iniciar cada equipo de estado de transmisión y de recepción convenientemente, de acuerdo con el estado configurado y el estado operativo del puerto.

La página de menú **LLDP** contiene enlaces a las funciones siguientes:

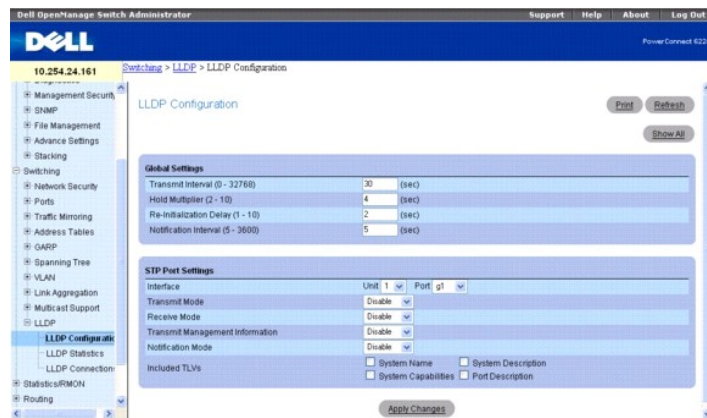
- [Configuración de LLDP](#)
- [Estadísticas de LLDP](#)
- [Conexiones LLDP](#)

Configuración de LLDP

Utilice la página **LLDP Configuration** (Configuración de LLDP) para especificar los parámetros de LLDP. Aquí se pueden especificar tanto los parámetros que afectan a todo el sistema como los relativos a una interfaz concreta.

Para visualizar la página **LLDP Configuration** (Configuración de LLDP), haga clic en **Switching** (Conmutación) → **LLDP** → **LLDP Configuration** (Configuración de LLDP) en la vista de árbol.

Ilustración 7-75. Configuración de LLDP



La página **LLDP Configuration** (Configuración de LLDP) contiene los campos siguientes:

Configuración global

Transmit Interval (1–32768) (Intervalo de transmisión [1–32768]): especifica el intervalo en el que se transmiten las tramas. El valor predeterminado es 30 segundos.

Hold Multiplier (2–10) (Multiplicador de mantenimiento [2–10]): especifica el multiplicador del intervalo de transmisión que se debe asignar al tiempo de vida (TTL). El valor predeterminado es 4.

Re-Initialization Delay (1–10) (Demora de reinicialización [1–10]): especifica la demora que transcurre antes de una reinicialización. El valor predeterminado es 2 segundos.

Notification Interval (5–3600) (Intervalo de notificación [5–3600]): limita la transmisión de notificaciones. El valor predeterminado es 5 segundos.

Configuración de puerto

Interface (Interfaz): especifica el puerto afectado por estos parámetros.

Transmit Mode (Modo de transmisión): activa o desactiva la función de transmisión. El valor predeterminado es Disabled (Desactivado).

Receive Mode (Modo de recepción): activa o desactiva la función de recepción. El valor predeterminado es Disabled (Desactivado).

Transmit Management Information (Transmitir información de administración): activa o desactiva la transmisión de instancias de direcciones de administración. El valor predeterminado es Disabled (Desactivado).

Notification Mode (Modo de notificación): activa o desactiva las notificaciones de cambios remotos. El valor predeterminado es Disabled (Desactivado).

Included TLVs (TLV incluidos): selecciona la información de TLV que se va a transmitir. Las opciones posibles son System Name (Nombre del sistema), System Capabilities (Funciones del sistema), System Description (Descripción del sistema) y Port Description (Descripción del puerto).

Modificación de la configuración de LLDP

1. Abra la página **LLDP Configuration** (Configuración de LLDP).
2. Defina los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LLDP se guardan en el conmutador.

Visualización de la tabla de configuración de la interfaz LLDP

1. Abra la página **LLDP Configuration** (Configuración de LLDP).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **LLDP Interface Settings Table** (Tabla de configuración de la interfaz LLDP).

Ilustración 7-76. Tabla de configuración de la interfaz LLDP

Port	Transmit	Receive	Notify	Management Info	System Name	System Description	System Capabilities	Port Description	Copy To
1-1/1/1	Disable	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2-1/1/2	Disable	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3-1/1/3	Disable	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26-1/1/2	Disable	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27-1/1/2	Disable	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28-1/1/4	Disable	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Utilice el menú desplegable **Unit** (Unidad) para ver la tabla de configuración de la interfaz LLDP correspondiente a otras unidades de la pila, en caso de que existan.

Copia de la configuración de la interfaz LLDP

1. Abra la página **LLDP Configuration** (Configuración de LLDP).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **LLDP Interface Settings Table** (Tabla de configuración de la interfaz LLDP).
3. Especifique la unidad y el puerto de los que está copiando en **Copy Parameters From** (Copiar parámetros de).
4. Haga clic en **Copy To** (Copiar en) para cada unidad/puerto que deba recibir estos parámetros.

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

La configuración de la interfaz LLDP se copia y se actualiza el dispositivo.

Modificación de la configuración de la interfaz LLDP para varios puertos

- Abra la página **LLDP Configuration** (Configuración de LLDP).
- Haga clic en **Show All** (Mostrar todo).

Aparece la página **LLDP Interface Settings Table** (Tabla de configuración de la interfaz LLDP).

- Haga clic en **Edit** (Editar) para cada unidad/puerto que desee modificar.
- Edite los campos de la interfaz LLDP según convenga.
- Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de la interfaz LLDP se modifica y se actualiza el dispositivo.

Configuración de LLDP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de LLDP

Estadísticas de LLDP

Utilice la página **LLDP Statistics** (Estadísticas de LLDP) para ver las estadísticas relacionadas con el protocolo LLDP.

Para visualizar la página **LLDP Statistics** (Estadísticas de LLDP), haga clic en **Switching** (Conmutación)→ **LLDP**→ **LLDP Statistics** (Estadísticas de LLDP) en la vista de árbol.

Ilustración 7-77. Estadísticas de LLDP

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "LLDP Statistics" and includes a "Unit" dropdown menu set to "1". Below this, there are summary statistics: "Last Update" (00:00:00), "Total Inserts" (0), "Total Deletes" (0), and "Total Ageouts" (0). At the bottom, there is a table with the following columns: Interface, Transmit Total, Receive Total, Discards, Errors, Ageouts, TLV Discards, and TLV. The table contains four rows of data for interfaces 1/xg1, 1/xg2, 1/xg3, and 1/xg4, all showing zero values.

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV
1/xg1	0	0	0	0	0	0	0
1/xg2	0	0	0	0	0	0	0
1/xg3	0	0	0	0	0	0	0
1/xg4	0	0	0	0	0	0	0

La página **LLDP Statistics** (Estadísticas de LLDP) muestra las estadísticas siguientes:

Estadísticas relativas a todo el sistema

Last Update (Última actualización): muestra el valor del tiempo de actividad del sistema la última vez que se creó, modificó o eliminó una entrada de datos remota.

Total Inserts (Inserciones totales): muestra el número de veces que un conjunto completo de información anunciada por un conmutador remoto se ha insertado en la tabla.

Total Deletes (Eliminaciones totales): muestra el número de veces que un conjunto completo de información anunciada por un conmutador remoto se ha

eliminado de la tabla.

Total Drops (Descartes totales): muestra el número de veces que un conjunto completo de información anunciada por un conmutador remoto no se ha podido insertar debido a una insuficiencia de recursos.

Total Ageouts (Caducidades totales): muestra el número de veces que cualquier entrada de datos remota se ha eliminado debido a que ha caducado el TTL.

Estadísticas de puerto

Interface (Interfaz): muestra la unidad y el puerto a los que corresponden las estadísticas de esta línea.

Transmit Total (Transmisiones totales): muestra el número total de tramas de LLDP transmitidas en el puerto indicado.

Receive Total (Recepciones totales): muestra el número total de tramas de LLDP válidas recibidas en el puerto indicado.

Discards (Descartes): muestra el número de tramas de LLDP recibidas en el puerto indicado y descartadas por alguna razón.

Errors (Errores): muestra el número de tramas de LLDP no válidas recibidas en el puerto indicado.

Ageouts (Caducidades): muestra el número de veces que una entrada de datos remota en el puerto indicado se ha eliminado debido a que ha caducado el TTL.

TLV Discards (Descartes TLV): muestra el número de TLV (conjuntos de tipo, longitud, valor) de LLDP recibidos en el puerto indicado y que el agente de LLDP ha descartado por alguna razón.

TLV Unknown (TLV desconocidos): muestra el número de TLV de LLDP recibidos en el puerto indicado para un tipo que el agente de LLDP no reconoce.

Utilice el menú desplegable **Unit** (Unidad) para ver las estadísticas de LLDP correspondientes a otras unidades de la pila, en caso de que existan.

Utilice el botón **Clear Statistics** (Borrar estadísticas) para restablecer todas las estadísticas de LLDP a cero.

Visualización de las estadísticas de LLDP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de LLDP

Conexiones LLDP

Utilice la página **LLDP Connections** (Conexiones LLDP) para ver la lista de puertos con el protocolo LLDP activado. Se muestran los detalles básicos de conexión.

Para visualizar la página **LLDP Connections** (Conexiones LLDP), haga clic en **Switching** (Conmutación) → **LLDP** → **LLDP Connections** (Conexiones LLDP) en la vista de árbol

Ilustración 7-78. Tabla de conexiones LLDP



Local Interface	Chassis ID	Port ID	System Name
1/27	00:FC:E3:90:01:54	00:FC:E3:90:01:56	
1/g11	00:FC:E3:90:01:4B	00:FC:E3:90:01:4D	dell_141

La página **LLDP Connections** (Conexiones LLDP) muestra los detalles de puerto siguientes:

Local Interface (Interfaz local): designa una unidad y un puerto de la pila.

Chassis ID (ID de chasis): identifica el chasis del dispositivo de LAN 802.

Port ID (ID de puerto): identifica el número de puerto desde el que se transmite la LLDPDU.

System Name (Nombre del sistema): identifica el nombre del sistema asociado con el dispositivo remoto.

Utilice el menú desplegable **Unit** (Unidad) para ver las conexiones LLDP correspondientes a otras unidades de la pila, en caso de que existan.

Utilice el botón **Clear Table** (Borrar tabla) para borrar toda la información de la tabla **LLDP Connections** (Conexiones LLDP).

Visualización de detalles sobre las conexiones LLDP

1. Abra la página **LLDP Connections** (Conexiones LLDP).
2. Haga clic en la interfaz en el campo **Local Interface** (Interfaz local) para ver detalles de dicho dispositivo.
Aparece la página **LLDP Connections - Detailed** (Detalles de conexiones LLDP) correspondiente al dispositivo.

Ilustración 7-79. Detalles de conexiones LLDP



The screenshot shows the 'LLDP Connections - Detailed' page. At the top, there are 'Print' and 'Refresh' buttons. Below is a table for the local interface:

Local Interface	1/41
TTL	60 (sec)

Below this is a 'Remote' section with the following details:

Chassis ID Subtype	MAC Address
Chassis ID	00:FC:E3:90:01:4B
Port ID Subtype	MAC Address
Port ID	00:FC:E3:90:01:4D
Port Description	14p_g4_sh_141
System Name	dell_141
System Description	L3U7 FASTPATH Routing
System Capabilities Supported	bridge, router
System Capabilities Enabled	bridge
Management Address	IPv4 - 10.254.24.141

At the bottom of the remote section, there is a 'Back' button.

3. Utilice el botón **Back** (Atrás) para volver a la página **LLDP Connections** (Conexiones LLDP).

Visualización de las conexiones LLDP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de LLDP

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración del enrutamiento

Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [ARP](#)
- [IP](#)
- [OSPF](#)
- [Agente de retransmisión BOOTP/DHCP](#)
- [RIP](#)
- [Detección de enrutador](#)
- [Enrutador](#)
- [Enrutamiento de VLAN](#)
- [VRRP](#)
- [Túneles](#)
- [Bucles de retorno](#)

La serie 6200 admite la función de enrutamiento IP. Utilice la página de menú **Routing** (Enrutamiento) para configurar el enrutamiento en las VLAN.

Cuando un paquete accede al conmutador, se comprueba si la dirección MAC de destino coincide con alguna de las interfaces de enrutamiento configuradas. En caso afirmativo, el dispositivo busca en la tabla de hosts una dirección IP de destino que coincida. Si se encuentra una entrada, se direcciona el paquete al host. Si no existe ninguna entrada coincidente, el conmutador busca la dirección IP de destino con el prefijo coincidente más largo. Si se encuentra una entrada, se direcciona el paquete al siguiente salto. Si no existe ninguna coincidencia, se direcciona el paquete al siguiente salto especificado en la ruta predeterminada. Si no hay ninguna ruta predeterminada configurada, se pasa el paquete al software de la serie 6200 para que se administre de la manera apropiada.

Es posible añadir entradas a la tabla de enrutamiento de forma estática por parte del administrador o de forma dinámica por medio de RIP u OSPF. Es posible añadir entradas a la tabla de hosts de forma estática por parte del administrador o de forma dinámica por medio de ARP.

La página de menú **Routing** (Enrutamiento) contiene enlaces a las funciones siguientes:

- 1 [ARP](#)
- 1 [IP](#)
- 1 [OSPF](#)
- 1 [Agente de retransmisión BOOTP/DHCP](#)
- 1 [RIP](#)
- 1 [Detección de enrutador](#)
- 1 [Enrutador](#)
- 1 [Enrutamiento de VLAN](#)
- 1 [VRRP](#)
- 1 [Túneles](#)
- 1 [Bucles de retorno](#)

 **NOTA:** los comandos de la CLI no están disponibles para todas las páginas de enrutamiento.

ARP

La serie 6200 utiliza el protocolo ARP para asociar una dirección MAC de nivel 2 a una dirección IPv4 de nivel 3. Adicionalmente, el administrador puede añadir entradas de forma estática a la tabla de ARP.

ARP es una parte necesaria del protocolo Internet (IP) y se utiliza para traducir una dirección IP a una dirección (MAC) de medios, definida por una red de área local (LAN) como Ethernet. Una estación que necesita enviar un paquete IP debe obtener la dirección MAC del IP de destino, o del enrutador del siguiente salto, si el destino no se encuentra en la misma subred. Esto se consigue mediante la difusión de un paquete de petición de ARP, al que el destinatario correspondiente responde mediante la difusión única de una respuesta de ARP que contenga su dirección MAC. Una vez obtenida, la dirección MAC se utiliza en el campo de la dirección de destino de la cabecera de nivel 2 antepuesto al paquete IP.

La caché de ARP es una tabla que se mantiene localmente en cada estación de una red. No existen requisitos específicos para la creación o el mantenimiento de esta caché, pero como mínimo debe contener la información obtenida del procesamiento de los paquetes del protocolo ARP, que para Ethernet se indican mediante un campo EtherType 0x0806. Las entradas de la caché de ARP se obtienen examinando la información de origen de los campos de carga de paquetes ARP, independientemente de si se trata de una petición o de una respuesta de ARP. Por tanto, cuando una petición de ARP se difunde a todas las estaciones de un segmento de LAN o a una LAN virtual (VLAN), cada destinatario tiene la oportunidad de almacenar la dirección IP y MAC del remitente en su caché de ARP correspondiente. La respuesta de ARP, al ser una difusión única, sólo es visible normalmente para el solicitante, quien almacena la información del remitente en su caché de ARP. La información más reciente siempre sustituye el contenido existente en la caché de ARP.

La caché de ARP puede admitir hasta 896 entradas, si bien el usuario puede configurar este tamaño con cualquier valor comprendido entre 256 y 896. Cuando un dispositivo admite varias interfaces de red, como es el caso de un enrutador, se utiliza una única caché de ARP para todas las interfaces, o bien se mantiene una caché distinta por interfaz. Si bien el segundo enfoque resulta útil cuando el direccionamiento de red no es único para cada interfaz, no sucede lo mismo con la asignación de direcciones MAC de Ethernet, por lo que se utiliza una única caché de ARP.

Es posible mover dispositivos dentro de una red, lo que significa que la dirección IP que estaba asociada a una determinada dirección MAC se encuentra ahora con una MAC diferente o puede haber desaparecido de la red (por ejemplo, si se ha reconfigurado, desconectado o apagado). Esto provoca que la información contenida en la caché de ARP pase a ser obsoleta a menos que se actualicen las entradas como respuesta a la detección de nueva información en la red, que se actualicen periódicamente para determinar si una dirección sigue existiendo o que se eliminen de la caché si la entrada no se ha identificado como un remitente de un paquete ARP durante un intervalo de caducidad, especificado normalmente por medio de la configuración.

La página de menú **ARP** contiene enlaces a páginas web que permiten configurar y visualizar detalles sobre ARP. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **ARP** en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

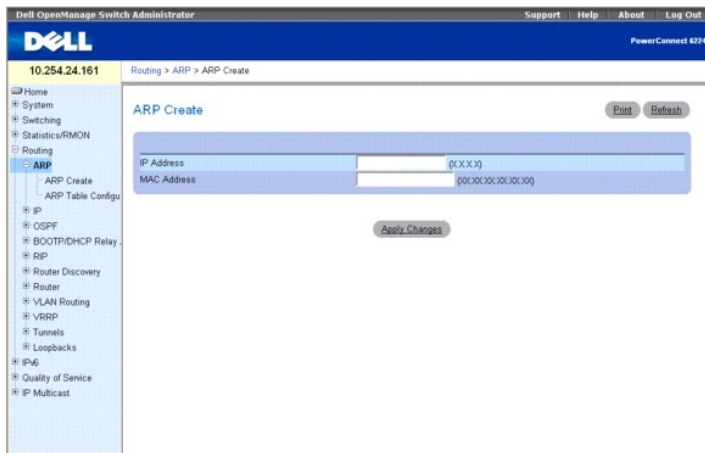
- 1 [Creación de ARP](#)
- 1 [Configuración de la tabla de ARP](#)

Creación de ARP

Utilice la página ARP Create (Crear ARP) para añadir una entrada a la tabla de ARP (protocolo de resolución de direcciones).

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **ARP**→ **ARP Create** (Crear ARP) en la vista de árbol.

Ilustración 10-1. Creación de ARP



La página **ARP Create** (Crear ARP) contiene los campos siguientes:

IP Address (Dirección IP): introduzca la dirección IP que desea añadir. Debe tratarse de la dirección IP de un dispositivo ubicado en una subred y conectado a una de las interfaces de enrutamiento del conmutador existentes.

MAC Address (Dirección MAC): dirección MAC de difusión única del dispositivo. Introduzca la dirección con un formato de seis números hexadecimales de dos dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40.

Adición de una entrada a la tabla de ARP

1. Abra la página **ARP Create** (Crear ARP).
2. Especifique las direcciones que deben asociarse.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Las direcciones ya se encuentran en la caché de ARP.

Adición de entradas a la tabla de ARP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de ARP

Configuración de la tabla de ARP

Utilice esta página para cambiar los parámetros de configuración de la tabla de ARP. También puede utilizar esta pantalla para ver el contenido de la tabla.

Para visualizar la página, haga clic en **Routing** (Ενρυταμηντο)→ **ARP**→ **ARP Table Configuration** (Configuración de la tabla de ARP) en la vista de árbol.

Ilustración 10-2. Configuración de la tabla de ARP



La página **ARP Table Configuration** (Configuración de la tabla de ARP) contiene los campos siguientes:

Age Time (secs) (Caducidad [seg.]): introduzca el valor que desea que el conmutador utilice para la caducidad de la entrada de ARP. Debe introducir un número entero válido, que representa el número de segundos que una entrada de ARP tarda en caducar. El intervalo para este campo es de 15 a 21600 segundos. El valor predeterminado para la caducidad es 1200 segundos.

Response Time (secs) (Tiempo de respuesta [seg.]): introduzca el valor que desea que el conmutador utilice para la expiración del tiempo de respuesta de ARP. Debe introducir un número entero válido, que representa el número de segundos durante los que el conmutador espera una respuesta a una petición de ARP. El intervalo para este campo es de 1 a 10 segundos. El valor predeterminado para el tiempo de respuesta es 1 segundo.

Retries (Reintentos): introduzca un número entero que especifique el número máximo de veces que se reintentará una petición de ARP. El intervalo para este campo es de 0 a 10. El valor predeterminado es 4.

Cache Size (Tamaño de caché): introduzca un número entero que especifique el número máximo de entradas de la caché de ARP. El intervalo para este campo es de 256 a 896. El valor predeterminado es 896.

Dynamic Renew (Renovar dinámicas): este campo controla si el componente de ARP intenta automáticamente renovar las entradas de ARP de tipo dinámico cuando éstas caducan. El valor predeterminado es **Enable** (Activar).

Total Entry Count (Recuento total de entradas): número total de entradas de la tabla de ARP.

Peak Total Entries (Máximo de entradas totales): valor más alto alcanzado por el recuento total de entradas. Este valor se reinicia cada vez que se cambia el valor de **Cache Size** (Tamaño de caché) de la tabla de ARP.

Active Static Entries (Entradas estáticas activas): número total de entradas estáticas activas en la tabla de ARP.

Configured Static Entries (Entradas estáticas configuradas): número total de entradas estáticas configuradas en la tabla de ARP.

Maximum Static Entries (Máximo de entradas estáticas): número máximo de entradas estáticas que pueden definirse.

Remove from Table (Eliminar de la tabla): permite eliminar determinadas entradas de la tabla de ARP. Las opciones enumeradas especifican el tipo de entrada de ARP que se va a eliminar:

- 1 All Dynamic Entries (Todas las entradas dinámicas)
- 1 All Dynamic and Gateway Entries (Todas las entradas dinámicas y de puerta de enlace)
- 1 Specific Dynamic Gateway Entry (Entrada de puerta de enlace dinámica específica)
- 1 Specific Static Entry (Entrada estática específica)

La tabla de ARP se visualiza en la parte inferior de la página y contiene los campos siguientes:

IP Address (Dirección IP): dirección IP de un dispositivo ubicado en una subred y conectado a una de las interfaces de enrutamiento del conmutador.

MAC Address (Dirección MAC): dirección MAC de difusión única del dispositivo. El formato es seis números hexadecimales de dos dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40.

VLAN ID (ID de VLAN): interfaz de enrutamiento asociada a la entrada de ARP.

Type (Tipo): tipo de la entrada de ARP.

Age (Edad): tiempo desde que la entrada se actualizó por última vez en la tabla de ARP. El formato es hh:mm:ss.

Configuración de la tabla de ARP

1. Abra la página **ARP Table Configuration** (Configuración de la tabla de ARP).
2. Cambie los parámetros según sea necesario.

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

Los cambios se guardan y la tabla de ARP se actualiza.

Configuración de la tabla de ARP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de ARP

IP

La página de menú **IP** contiene enlaces a páginas web que permiten configurar y visualizar los datos de enrutamiento IP. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **IP** en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

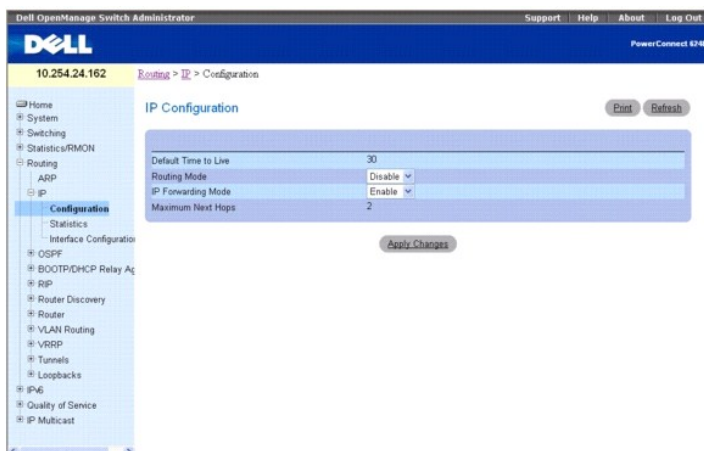
- 1 [Configuración de IP](#)
- 1 [Estadísticas de IP](#)
- 1 [Configuración de interfaz IP](#)

Configuración de IP

Utilice la página **IP Configuration** (Configuración de IP) para configurar los parámetros de enrutamiento del conmutador en contraposición a una interfaz.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **IP** → **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-3. Configuración de IP



La página **IP Configuration** (Configuración de IP) contiene los campos siguientes:

Default Time to Live (Tiempo de vida predeterminado): valor predeterminado que se inserta en el campo Time-To-Live (Tiempo de vida) del encabezado IP de los datagramas originados por el conmutador si no se suministra ningún valor mediante el protocolo de nivel de transferencia.

Routing Mode (Modo de enrutamiento): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Para poder direccionar en una interfaz, es preciso activar el enrutamiento para el conmutador. El enrutamiento también puede activarse y desactivarse para cada interfaz de VLAN. El valor predeterminado es Disable (Desactivar).

IP Forwarding Mode (Modo de reenvío de IP): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Con esto, activará o desactivará el reenvío de tramas IP. El valor predeterminado es Enable (Activar).

Maximum Next Hops (Máximo de siguientes saltos): número máximo de saltos admitidos por el conmutador. Se trata de una constante de tiempo de compilación.

Configuración de los parámetros de enrutamiento IP

1. Abra la página **IP Configuration** (Configuración de IP).
2. Cambie los parámetros según sea necesario.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los cambios se guardan y los parámetros de enrutamiento se actualizan.

Configuración de los parámetros de enrutamiento IP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la *Guía de referencia de la CLI*:

- 1 Comandos de enrutamiento IP
- 1 Comandos de VLAN

Estadísticas de IP

Las estadísticas presentadas en la página **IP Statistics** (Estadísticas de IP) son las especificadas en RFC 1213.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **IP** → **Statistics** (Estadísticas) en la vista de árbol.

Ilustración 10-4. Estadísticas de IP

Field	Value
IpInReceives	520
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	479
IpOutRequests	699
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmChks	0
IpReasmFails	0
IpFragChks	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpMigs	0
IcmpErrors	0

La página **IP Statistics** (Estadísticas de IP) contiene los campos siguientes:

IpInReceives: número total de datagramas de entrada recibidos de las interfaces, incluidos aquéllos recibidos con error.

IpInHdrErrors: número de datagramas de entrada que se han descartado debido a errores en sus encabezados IP, como por ejemplo sumas de comprobación erróneas, discrepancia de número de versión, otros errores de formato, expiración del tiempo de vida, detección de errores al procesar sus opciones de IP, etc.

IpInAddrErrors: número de datagramas de entrada que se han descartado porque la dirección IP que figuraba en el campo de destino de su encabezado IP no era válida para recibirse en esta entidad. Este recuento incluye las direcciones no válidas (por ejemplo, 0.0.0.0) y las direcciones de clases no admitidas (por ejemplo, clase E). Para las entidades que no son puertos de enlace IP y, por tanto, no reenvían datagramas, este recuento incluye los datagramas descartados porque la dirección de destino no era una dirección local.

IpForwDatagrams: número de datagramas de entrada para los que esta entidad no era su destino IP final, por lo que se ha intentado encontrar una ruta para reenviarlos a dicho destino final. En entidades que no actúan como puertos de enlace IP, este recuento incluye sólo los paquetes dirigidos originariamente a través de esta entidad y para los que el procesamiento de la opción de ruta de origen ha sido correcto.

IpInUnknownProtos: número de datagramas con dirección local recibidos correctamente pero descartados debido a un protocolo desconocido o no admitido.

IpInDiscards: número de datagramas IP de entrada para los que no se ha detectado ningún problema que impidiera que continuaran procesándose, pero que se han descartado (por ejemplo, por falta de espacio en el búfer). Tenga en cuenta que este recuento no incluye ninguno de los datagramas descartados mientras estaban a la espera de ser reensamblados.

IpInDelivers: número total de datagramas de entrada entregados con éxito a los protocolos de usuario IP (incluido el protocolo de mensajes de control de Internet, ICMP).

IpOutRequests: número total de datagramas IP que los protocolos de usuario IP locales (incluido ICMP) han proporcionado a IP en peticiones de transmisión. Tenga en cuenta que este recuento no incluye los datagramas contabilizados en ipForwDatagrams.

IpOutDiscards: número de datagramas IP de salida para los que no se ha detectado ningún problema que impidiera su transmisión al destino, pero que se han descartado (por ejemplo, por falta de espacio en el búfer). Tenga en cuenta que este recuento incluiría los datagramas contabilizados en ipForwDatagrams si alguno de dichos paquetes cumpliera este criterio (discrecional) de descarte.

IpOutNoRoutes: número de datagramas IP descartados debido a que no se ha encontrado ninguna ruta para transmitirlos a su destino. Tenga en cuenta que este recuento incluye todos los paquetes contabilizados en ipForwDatagrams que cumplan este criterio de "sin ruta", así como todos los datagramas que un host no puede direccionar debido a que todas sus puertas de enlace predeterminadas están desconectadas.

IpReasmTimeout: número máximo de segundos durante los que los fragmentos recibidos se conservan mientras están a la espera de ser reensamblados en esta entidad.

IpReasmReqds: número de fragmentos IP recibidos que han debido reensamblarse en esta entidad.

IpReasmOKs: número de datagramas IP reensamblados correctamente.

IpReasmFails: número de errores detectados por el algoritmo de reensamblaje de IP, se cual sea el motivo: tiempo de espera agotado, errores, etc. Tenga en cuenta que este recuento no incluye necesariamente los fragmentos IP descartados, ya que algunos algoritmos pueden perder la cuenta del número de fragmentos al combinarlos a medida que se reciben.

IpFragOKs: número de datagramas IP que se han fragmentado correctamente en esta entidad.

IpFragFails: número de datagramas IP que se han descartado porque debían fragmentarse en esta entidad pero no ha sido posible, por ejemplo, debido a que se había establecido el indicador de no fragmentación.

IpFragCreates: número de fragmentos de datagramas IP que se han generado como resultado de la fragmentación realizada en esta entidad.

IpRoutingDiscards: número de entradas de enrutamiento que se ha decidido descartar aunque eran válidas. Un motivo para ello podría ser el de liberar espacio en el búfer para otras entradas de enrutamiento.

IcmpInMsgs: número total de mensajes ICMP que ha recibido la entidad. Tenga en cuenta que este recuento incluye todos los mensajes contabilizados en icmpInErrors.

IcmpInErrors: número de mensajes ICMP que ha recibido la entidad, pero que se ha determinado que contenían errores específicos de ICMP, como por ejemplo sumas de comprobación ICMP erróneas, longitud inadecuada, etc.

IcmpInDestUnreachs: número de mensajes ICMP de tipo "destino inaccesible" que se han recibido.

IcmpInTimeExcds: número de mensajes ICMP de tipo "tiempo excedido" que se han recibido.

IcmpInParmProbs: número de mensajes ICMP de tipo "problema de parámetros" que se han recibido.

IcmpInSrcQuenchs: número de mensajes ICMP de tipo "desconexión de origen" (source quench) que se han recibido.

IcmpInRedirects: número de mensajes ICMP de tipo "redirección" que se han recibido.

IcmpInEchos: número de mensajes ICMP de tipo "petición de eco" que se han recibido.

IcmpInEchoReps: número de mensajes ICMP de tipo "respuesta a eco" que se han recibido.

IcmpInTimestamps: número de mensajes ICMP de tipo "petición de marca de hora" que se han recibido.

IcmpInTimestampReps: número de mensajes ICMP de tipo "respuesta a marca de hora" que se han recibido.

IcmpInAddrMasks: número de mensajes ICMP de tipo "petición de máscara de direcciones" que se han recibido.

IcmpInAddrMaskReps: número de mensajes ICMP de tipo "respuesta a máscara de direcciones" que se han recibido.

IcmpOutMsgs: número total de mensajes ICMP que esta entidad ha intentado enviar. Tenga en cuenta que este recuento incluye todos los mensajes contabilizados en icmpOutErrors.

IcmpOutErrors: número de mensajes ICMP que esta entidad no ha enviado debido a problemas detectados en ICMP, como por ejemplo falta de búferes. Este valor no debe incluir los errores detectados fuera del nivel de ICMP, como por ejemplo la imposibilidad del IP de direccionar el datagrama resultante. En algunas implementaciones puede que no haya ningún tipo de error que contribuya a incrementar este valor.

IcmpOutDestUnreachs: número de mensajes ICMP de tipo "destino inaccesible" que se han enviado.

IcmpOutTimeExcds: número de mensajes ICMP de tipo "tiempo excedido" que se han enviado.

IcmpOutParmProbs: número de mensajes ICMP de tipo "problema de parámetros" que se han enviado.

IcmpOutSrcQuenchs: número de mensajes ICMP de tipo "desconexión de origen" (source quench) que se han enviado.

IcmpOutRedirects: número de mensajes ICMP de tipo "redirección" que se han enviado. Para un host, este objeto siempre es cero, ya que los hosts no envían redirecciones.

IcmpOutEchos: número de mensajes ICMP de tipo "petición de eco" que se han enviado.

IcmpOutEchoReps: número de mensajes ICMP de tipo "respuesta a eco" que se han enviado.

IcmpOutTimestamps: número de mensajes ICMP de tipo "petición de marca de hora" que se han enviado.

IcmpOutTimestampReps: número de mensajes ICMP de tipo "respuesta a marca de hora" que se han enviado.

IcmpOutAddrMasks: número de mensajes ICMP de tipo "petición de máscara de direcciones" que se han enviado.

IcmpOutAddrMaskReps: número de mensajes ICMP de tipo "respuesta a máscara de direcciones" que se han enviado.

Actualización de las estadísticas de IP

1. Abra la página **IP Statistics** (Estadísticas de IP).
2. Haga clic en **Refresh** (Actualizar).

La pantalla muestra el estado actual de los datos del conmutador.

Visualización de las estadísticas de IP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

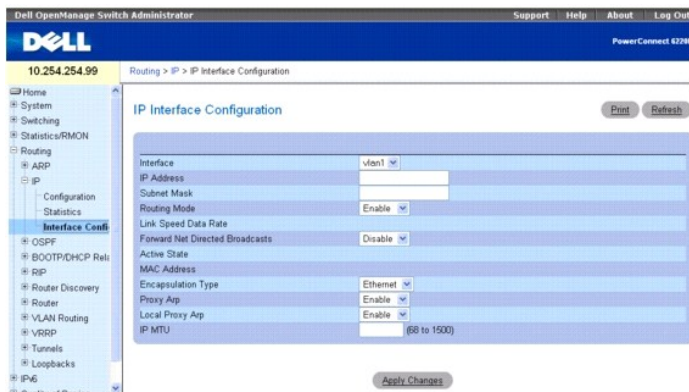
1. Comandos de enrutamiento IP

Configuración de interfaz IP

Utilice la página **IP Interface Configuration** (Configuración de interfaz IP) para actualizar los datos de la interfaz IP de este conmutador.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **IP** → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 10-5. Configuración de interfaz IP



La página **IP Interface Configuration** (Configuración de interfaz IP) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz que desea configurar. El menú desplegable contiene interfaces de bucle de retorno y VLAN creadas desde la página **Switching** (Commutación) → **VLAN** → **VLAN Membership** (Pertenencia a la VLAN) → **Add** (Añadir).

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

Subnet Mask (Máscara de subred): introduzca la máscara de subred de la interfaz. La máscara de subred, también conocida como máscara de subred/red, define la parte de la dirección IP de la interfaz que se utiliza para identificar la red conectada.

Routing Mode (Modo de enrutamiento): permite activar o desactivar el enrutamiento para una interfaz. El valor predeterminado es **Enable** (Activar).

Link Speed Data Rate (Velocidad de datos de enlace): número entero que representa la velocidad de datos del enlace físico de la interfaz especificada. Estos datos sólo son válidos para las interfaces físicas y se miden en megabits por segundo (Mbps).

Forward Net Directed Broadcasts (Reenviar difusiones dirigidas a la red): seleccione cómo deben gestionarse los paquetes de difusión dirigidos a la red. Si se selecciona **Enable** (Activar) en el menú desplegable, se reenvían las difusiones dirigidas a la red. Si se selecciona **Disable** (Desactivar), se descartan. El valor predeterminado es **Disable** (Desactivar).

Active State (Estado activo): el estado de la interfaz especificada puede ser **Active** (Activo) o **Inactive** (Inactivo). Una interfaz se considera activa si el enlace está activo y en estado de reenvío.

MAC Address (Dirección MAC): dirección física fija de la interfaz especificada. El formato es seis números hexadecimales de dos dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40. Este valor es válido para las interfaces físicas. Para las interfaces lógicas, como las interfaces de enrutamiento de VLAN, el campo muestra la dirección MAC del sistema.

Encapsulation Type (Tipo de encapsulación): seleccione en el menú desplegable el tipo de encapsulación del nivel de enlace para los paquetes transmitidos desde la interfaz especificada. Los valores posibles son **Ethernet** y **SNAP**. El valor predeterminado es **Ethernet**.

Proxy ARP (ARP proxy): seleccione **Disable** (Desactivar) o **Enable** (Activar) en el menú desplegable para activar o desactivar el ARP proxy para la interfaz especificada.

Local Proxy ARP (ARP proxy local): seleccione **Disable** (Desactivar) o **Enable** (Activar) en el menú desplegable para activar o desactivar el ARP proxy local para la interfaz especificada.

IP MTU: especifica el tamaño de la unidad de transmisión máxima (MTU) de los paquetes IP enviados en una interfaz. El intervalo válido es de 68 a 1500. El valor predeterminado es 1500.

Modificación de una interfaz IP

1. Abra la página **IP Interface Configuration** (Configuración de interfaz IP).
2. Cambie los valores según sea necesario.

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

Los cambios se guardan y la interfaz IP se actualiza.

Configuración de una interfaz IP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la *Guía de referencia de la CLI*:

- 1 Comandos de direccionamiento IP
 - 1 Comandos de enrutamiento IP
 - 1 Comandos de ARP
-

OSPF

El protocolo de enrutamiento Abria primero la ruta de acceso más corta (OSPF) es un protocolo de puerta de enlace interior (IGP). Cada enrutador OSPF crea un árbol de ruta de acceso más corta para todos los enrutadores y redes del dominio. La información de enrutamiento se propaga en paquetes de actualización de estado de enlace periódicamente y cada vez que cambia la topología de la red. Esta información se recibe, se asimila y se almacena en las bases de datos OSPF de los enrutadores individuales. Son pieza integral del intercambio de bases de datos el número y las direcciones IP de las interfaces que están asociadas al enrutador. OSPF trata las direcciones IP secundarias como redes aisladas conectadas al enrutador. Por tanto, aunque dichas redes se anuncian en el dominio de enrutamiento OSPF, nunca se establecen adyacencias de vecino en direcciones secundarias. También debe tenerse en cuenta que todas las direcciones IP secundarias deben encontrarse en la misma área que la dirección IP principal para que puedan anunciarse mediante OSPF. Esto se aplica siempre en el caso de la implementación de la serie 6200, ya que la configuración del área se realiza por interfaz en lugar de por red.

La página de menú **OSPF** contiene enlaces a páginas web que permiten configurar y visualizar los parámetros y datos de OSPF. Para visualizar esta página, haga clic en **Routing** (Enrutamiento)→ **OSPF** en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

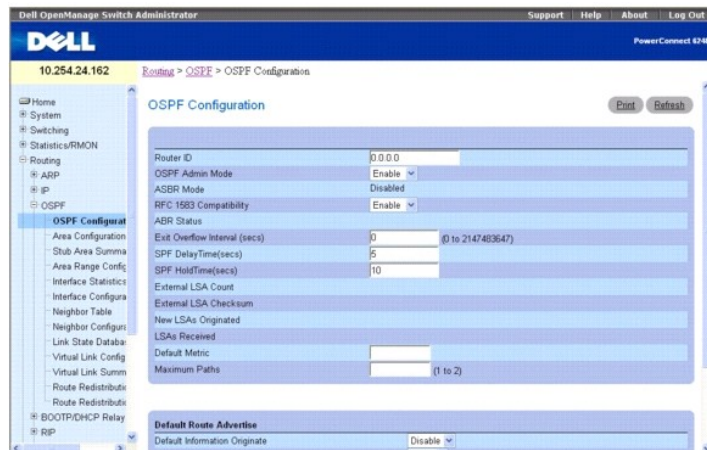
- 1 [Configuración de OSPF](#)
- 1 [Configuración de área](#)
- 1 [Resumen del área de rutas internas](#)
- 1 [Configuración del intervalo de área](#)
- 1 [Estadísticas de la interfaz](#)
- 1 [Configuración de interfaz](#)
- 1 [Tabla de vecinos](#)
- 1 [Configuración de vecino](#)
- 1 [Base de datos de estados de enlace](#)
- 1 [Configuración de enlace virtual](#)
- 1 [Resumen de enlaces virtuales](#)
- 1 [Configuración de redistribución de rutas](#)
- 1 [Resumen de redistribución de rutas](#)

Configuración de OSPF

Utilice la página **OSPF Configuration** (Configuración de OSPF) para activar OSPF en un enrutador y para configurar la configuración de OSPF relacionada.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **OSPF**→ **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-6. Configuración de OSPF



La página OSPF Configuration (Configuración de OSPF) contiene los campos siguientes:

Router ID (ID de enrutador): número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el enrutador dentro del sistema autónomo (AS). Si desea cambiar la ID de enrutador, primero debe desactivar OSPF. Una vez que haya configurado la nueva ID de enrutador, debe volver a activar OSPF para que el cambio tenga efecto. El valor predeterminado es 0.0.0.0, si bien este valor no es una ID de enrutador válida.

OSPF Admin Mode (Modo de administración de OSPF): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si se selecciona Enable (Activar), se activa OSPF para el conmutador. El valor predeterminado es Disable (Desactivar). Para que OSPF esté operativo, antes debe configurar una ID de enrutador.

NOTA: una vez que OSPF se inicializa en el enrutador, permanece inicializado hasta que se restablece el enrutador.

ASBR Mode (Modo ASBR): indica si el modo ASBR está activado o desactivado. Seleccionar Enable (Activar) implica que el enrutador es un enrutador de límite de sistema autónomo (ASBR). El enrutador se convierte automáticamente en un ASBR cuando se configura para redistribuir rutas obtenidas de otro protocolo.

RFC 1583 Compatibility (Compatibilidad con RFC 1583): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable para especificar las normas de preferencia que se utilizan a la hora de elegir entre varios AS-external-LSA (LSA externos al AS) que anuncian el mismo destino. Si se selecciona Enable (Activar), las normas de preferencia son las definidas por RFC 1583. Si se selecciona Disable (Desactivar), las normas de preferencia son las definidas en la sección 16.4.1 de la norma OSPF-2 (RFC 2328), que impiden la formación de bucles de enrutamiento cuando se han originado AS-external-LSA (LSA externos al AS) para el mismo destino desde diferentes áreas. El valor predeterminado es Enable (Activar). Para evitar los bucles de enrutamiento debe seleccionar Disable (Desactivar), pero únicamente si todos los enrutadores OSPF del dominio de enrutamiento son capaces de funcionar de acuerdo con RFC 2328.

ABR Status (Estado de ABR): los valores de este campo pueden ser Enabled (Activado) o Disabled (Desactivado). Enabled (Activado) implica que el enrutador es un enrutador de límite de área (ABR). Disabled (Desactivado) implica que no lo es.

Exit Overflow Interval (sec) (Intervalo de salida de desbordamiento [seg.]): introduzca el número de segundos que el enrutador debe esperar, una vez que ha alcanzado el estado de desbordamiento, hasta intentar salir de dicho estado. Esto permite al enrutador volver a originar AS-external-LSA (LSA externos al AS) no predeterminados. Si introduce 0, el enrutador no abandonará el estado de desbordamiento hasta que se reinicie. El intervalo es de 0 a 2147483647 segundos.

SPF DelayTime (secs) (Tiempo de demora de SPF [seg.]): introduzca el número de segundos que deben transcurrir entre que OSPF recibe un cambio de topología e inicia un cálculo de SPF. El valor es un número entero comprendido entre 0 y 65 535. El tiempo predeterminado es 5 segundos. El valor 0 significa que no hay ninguna demora, es decir, el cálculo de SPF se inicia inmediatamente.

SPF HoldTime(secs) (Tiempo de espera de SPF [seg.]): introduzca el número de segundos que deben transcurrir como mínimo entre dos cálculos de SPF consecutivos. El valor es un número entero comprendido entre 0 y 65 535. El tiempo predeterminado es 10 segundos. El valor 0 significa que no hay ninguna demora, es decir, pueden realizarse dos cálculos de SPF, uno inmediatamente después del otro.

External LSA Count (Número de LSA externos): número de LSA externos (LS tipo 5) en la base de datos de estados de enlace.

External LSA Checksum (Suma de comprobación de LSA externos): total de las sumas de comprobación de LS (estado de enlace) de los LSA externos contenidos en la base de datos de estados de enlace. Este total puede utilizarse para determinar si se ha producido algún cambio en la base de datos de estados de enlace de un enrutador y para comparar las bases de datos de estados de enlace de dos enrutadores. El valor tiene un formato hexadecimal.

New LSAs Originated (Nuevos LSA originados): en cualquier área OSPF, un enrutador origina varios LSA. Cada enrutador origina un router-LSA (LSA de enrutador). Si el enrutador es también el enrutador designado para cualquiera de las redes del área, éste origina network-LSA (LSA de red) para dichas redes. Este valor representa el número de LSA originados por dicho enrutador.

LSAs Received (LSA recibidos): número de LSA recibidos que se han determinado que son nuevas instancias. Este número no incluye las instancias más recientes de los LSA originados por sí mismos.

Default Metric (Métrica predeterminada): establece un valor predeterminado para la métrica de las rutas redistribuidas. Este campo muestra la métrica predeterminada si ya se ha definido una o aparece en blanco si no se ha configurado ninguna. Los valores válidos son de 1 a 16777214.

Maximum Paths (Máximo de rutas de acceso): configure el número máximo de rutas de acceso que OSPF puede notificar a un destino determinado. Los valores válidos son de 1 a 2.

Default Route Advertise (Anunciar ruta predeterminada)

Default Information Originate (Originar información predeterminada): permite activar (Enable) o desactivar (Disable) el anuncio de ruta predeterminada.

Always (Siempre): configura el anuncio de enrutador 0.0.0.0/0.0.0.0 cuando se establece en True (Verdadero).

Metric (Métrica): especifica la métrica de la ruta predeterminada. Los valores válidos son de 1 a 16777214.

Metric Type (Tipo de métrica): especifica el tipo de métrica de la ruta predeterminada. Las opciones son External Type 1 (Tipo externo 1) y External Type 2 (Tipo externo 2). Este último es el valor predeterminado.

Modificación de una configuración de OSPF

1. Abra la página OSPF Configuration (Configuración de OSPF).
2. Cambie los valores según sea necesario.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los cambios se guardan y la interfaz OSPF se actualiza.

Configuración de OSPF mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Configuración de área

La página **OSPF Area Configuration** (Configuración de área OSPF) permite crear una configuración de área de rutas internas y de área no exclusiva de rutas internas (NSSA) una vez que se ha activado OSPF en una interfaz a través de **Routing** (Enrutamiento) → **OSPF** → **Interface Configuration** (Configuración de interfaz). Al menos un enrutador debe tener OSPF activado para que esta página web se visualice.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Area Configuration** (Configuración de área) en la vista de árbol.

Ilustración 10-7. Configuración de área OSPF



La página **OSPF Area Configuration** (Configuración de área OSPF) incluye los campos siguientes:

Área (Área): seleccione en el menú desplegable el área que desea visualizar. Cuando se selecciona un área, se visualizan los campos de Stub Area Information (Información del área de rutas internas).

Area ID (ID de área): identificación del área OSPF. Una ID de área es un número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta una interfaz de enrutador.

External Routing (Enrutamiento externo): definición de las capacidades del enrutador para el área, como por ejemplo si se distribuyen o no AS-external-LSA (LSA externos al AS) al área o a través de ésta. Si se trata de un área de rutas internas, éstas son las opciones posibles con las que puede configurar la capacidad de enrutamiento externo; de lo contrario, la única opción posible es Import External LSAs (Importar LSA externos).

SPF Runs (Ejecuciones de SPF): número de veces que la tabla de rutas intraárea se ha calculado mediante la base de datos de estados de enlace de esta área. Este cálculo suele realizarse mediante el algoritmo de Dijkstra.

Area Border Router Count (Recuento de enrutadores de límite de área): número total de enrutadores de límite de área a los que se puede acceder dentro de esta área. Este valor es inicialmente cero y se calcula en cada paso de SPF.

Area LSA Count (Recuento de LSA del área): número total de anuncios de estado de enlace contenidos en la base de datos de estados de enlace de esta área, incluidos los LSA externos al AS.

Area LSA Checksum (Suma de comprobación de LSA del área): el total sin signo de 32 bits de las sumas de comprobación de LS de los anuncios de estado de enlace contenidas en la base de datos de estados de enlace de esta área. Este total no incluye los anuncios de estado de enlace externos (LS tipo 5). Este total puede utilizarse para determinar si se ha producido algún cambio en la base de datos de estados de enlace de un enrutador y para comparar las bases de datos de estados de enlace de dos enrutadores. El valor tiene un formato hexadecimal.

Stub Area Information (Información del área de rutas internas)

Import Summary LSAs (Importar LSA de resumen): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si se selecciona Enable (Activar), se importan LSA de resumen en áreas de rutas internas.

Metric Value (Valor de métrica): introduzca el valor de métrica que desee aplicar a la ruta predeterminada anunciada en el área de rutas internas. Los valores válidos son de 1 a 16777215.

Metric Type (Tipo de métrica): seleccione el tipo de métrica especificado en el campo Metric Value (Valor de métrica).

Translator Role (Función de traductor): configure la función de traductor de NSSA como Always (Siempre) o Candidate (Candidato).

Translator Stability Interval (Intervalo de estabilidad del traductor): configure el intervalo de estabilidad del traductor de la NSSA seleccionada.

No-Redistribute Mode (Modo de no redistribución): configure la redistribución de rutas de la NSSA seleccionada.

Translator State (Estado del traductor): muestra el estado actual del traductor.

Configuración de un área OSPF

1. Abra la página **OSPF Area Configuration** (Configuración de área OSPF).
2. Especifique el área que desea configurar.
3. Especifique valores en los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El área OSPF está definida y configurada.

Visualización de una configuración de área OSPF

1. Abra la página **OSPF Area Configuration** (Configuración de área OSPF).
2. Seleccione en el menú desplegable el área OSPF que desea visualizar.

Se visualiza la configuración de área OSPF de esta área.

Eliminación de una configuración de área OSPF

Utilice estos pasos para eliminar una configuración de área de rutas internas o de área no exclusiva de rutas internas (NSSA).

1. Abra la página **OSPF Area Configuration** (Configuración de área OSPF).
2. Seleccione en el menú desplegable la configuración de área OSPF que desea eliminar.

Se visualiza la configuración.

3. Haga clic en **Delete** (Eliminar).

Se elimina la configuración de área OSPF.

Configuración del área OSPF mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

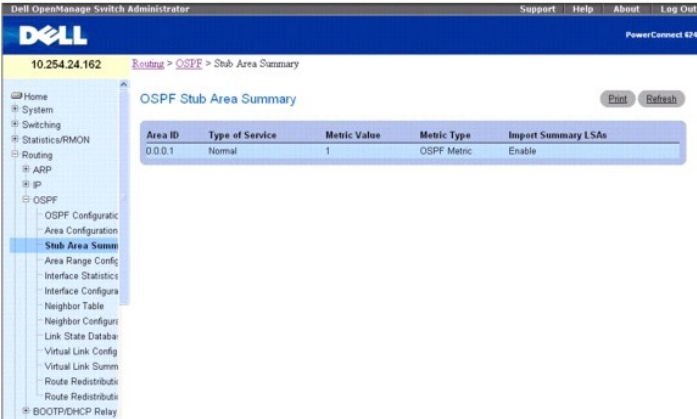
- 1 Comandos de OSPF

Resumen del área de rutas internas

Utilice la página **OSPF Stub Area Summary** (Resumen del área de rutas internas OSPF) para visualizar información sobre el área de rutas internas OSPF.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Stub Area Summary** (Resumen del área de rutas internas) en la vista de árbol.

Ilustración 10-8. Resumen del área de rutas internas OSPF



La página OSPF Stub Area Summary (Resumen del área de rutas internas OSPF) incluye los campos siguientes:

Area ID (ID de área): identificación del área de rutas internas.

Type of Service (Tipo de servicio): tipo de servicio asociado a la métrica de rutas internas. El conmutador sólo admite Normal.

Metric Value (Valor de métrica): muestra el valor de métrica configurado.

Metric Type (Tipo de métrica): tipo de métrica del área de rutas internas. Los tipos válidos son:

- 1 **OSPF Metric** (Métrica OSPF): métrica OSPF normal.
- 1 **Comparable Cost** (Coste comparable): métrica External Type 1 (Tipo externo 1), que es comparable a la métrica OSPF.
- 1 **Non-comparable Cost** (Coste no comparable): métrica External Type 2 (Tipo externo 2), que se supone que es mayor que el coste de la métrica OSPF.

Import Summary LSAs (Importar LSA de resumen): determina si la importación de LSA de resumen está activada o desactivada.

Visualización del área de rutas internas OSPF mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Configuración del intervalo de área

Utilice la página OSPF Area Range Configuration (Configuración del intervalo de área OSPF) para configurar y visualizar un intervalo de área de una NSSA especificada.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Area Range Configuration** (Configuración del intervalo de área) en la vista de árbol.

Ilustración 10-9. Configuración del intervalo de área OSPF



La página OSPF Area Range Configuration (Configuración del intervalo de área OSPF) contiene los campos siguientes:

Area ID (ID de área): seleccione en el menú desplegable el área cuyos datos desea configurar.

IP Address (Dirección IP): introduzca la dirección IP del intervalo de direcciones del área seleccionada.

Subnet Mask (Máscara de subred): introduzca la máscara de subred del intervalo de direcciones del área seleccionada.

LSDB Type (Tipo de LSDB): seleccione el tipo de anuncio de enlace asociado al área y al intervalo de direcciones especificados. El tipo predeterminado es "Network Summary" (Resumen de red).

Advertisement (Anuncio): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si se selecciona Enable (Activar), el intervalo de direcciones se anuncia fuera del área por medio de un LSA de resumen de red. El valor predeterminado es Enable (Activar).

Add (Añadir): marque la casilla de verificación Add (Añadir) para añadir un intervalo de área.

Tabla de intervalo de área OSPF

Area ID (ID de área): muestra el área OSPF.

IP Address (Dirección IP): muestra la dirección IP de un intervalo de direcciones del área.

Subnet Mask (Máscara de subred): muestra la máscara de subred de un intervalo de direcciones del área.

LSDB Type (Tipo de LSDB): muestra el tipo de anuncio de enlace del intervalo de direcciones y del área.

Advertisement (Anuncio): muestra el modo de anuncio del intervalo de direcciones y del área.

Remove (Eliminar): elimina la entrada de área especificada.

Definición de un intervalo de área OSPF

1. Abra la página **OSPF Area Range Configuration** (Configuración del intervalo de área OSPF).
2. Introduzca la ID de área, la dirección IP, la máscara de subred, el tipo de LSDB y el anuncio.
3. Haga clic en la casilla de verificación **Add** (Añadir).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El intervalo de área OSPF está definido y configurado. En la tabla de la página **OSPF Area Range Configuration** (Configuración del intervalo de área OSPF) se muestran todos los intervalos de área OSPF configurados.

Eliminación de una configuración de intervalo de área OSPF

1. Abra la página **OSPF Area Range Configuration** (Configuración del intervalo de área OSPF).
2. Seleccione la casilla de verificación **Remove** (Eliminar) en la fila de **Area ID** (ID de área) que desea eliminar.
3. Haga clic en **Apply Changes** (Aplicar cambios).

El intervalo de direcciones se elimina de la configuración de área.

Configuración del intervalo de área OSPF mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

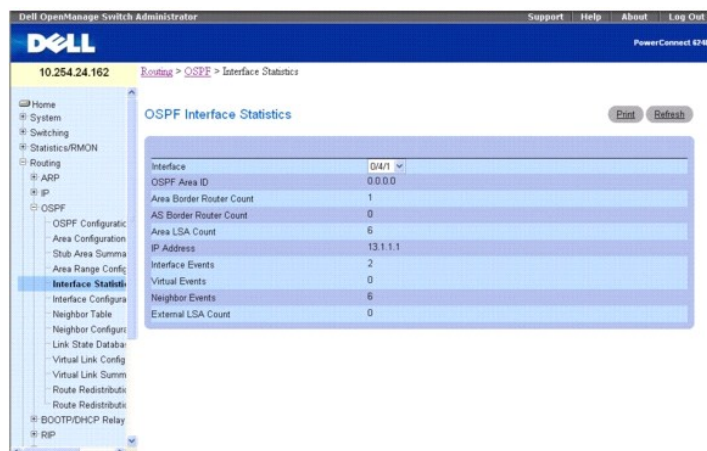
- 1 Comandos de OSPF

Estadísticas de la interfaz

Utilice la página **OSPF Interface Statistics** (Estadísticas de la interfaz OSPF) para ver estadísticas de la interfaz seleccionada. La información se visualiza únicamente si OSPF está activado.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Interface Statistics** (Estadísticas de la interfaz) en la vista de árbol.

Ilustración 10-10. Estadísticas de la interfaz OSPF



La página OSPF Interface Statistics (Estadísticas de la interfaz OSPF) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz cuyos datos desea visualizar.

OSPF Area ID (ID de área OSPF): área OSPF a la que pertenece la interfaz de enrutador seleccionada. Una ID de área OSPF es un número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta la interfaz.

Area Border Router Count (Recuento de enrutadores de límite de área): número total de enrutadores de límite de área a los que se puede acceder dentro de esta área. Este valor es inicialmente cero y se calcula en cada paso de SPF.

AS Border Router Count (Recuento de enrutadores de límite de sistema autónomo): número total de enrutadores de límite de sistema autónomo a los que se puede acceder dentro de esta área. Este valor es inicialmente cero y se calcula en cada paso de SPF.

Area LSA Count (Recuento de LSA del área): número total de anuncios de estado de enlace contenidos en la base de datos de estados de enlace de esta área, incluidos los LSA externos al AS.

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

Interface Events (Eventos de interfaz): número de veces que ha cambiado el estado de la interfaz OSPF especificada o que se ha producido un error.

Virtual Events (Eventos virtuales): número de cambios de estado o errores que se han producido en este enlace virtual.

Neighbor Events (Eventos de vecino): número de veces que ha cambiado el estado de esta relación de vecino o que se ha producido un error.

External LSA Count (Recuento de LSA externos): número de anuncios de estado de enlace externos (LS tipo 5) en la base de datos de estados de enlace.

Visualización de estadísticas de la interfaz OSPF

1. Abra la página OSPF Interface Statistics (Estadísticas de la interfaz OSPF).
2. Seleccione en el menú desplegable la interfaz cuyos datos desea visualizar.

Se muestran las estadísticas de esta interfaz.

Visualización de las estadísticas de la interfaz OSPF mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

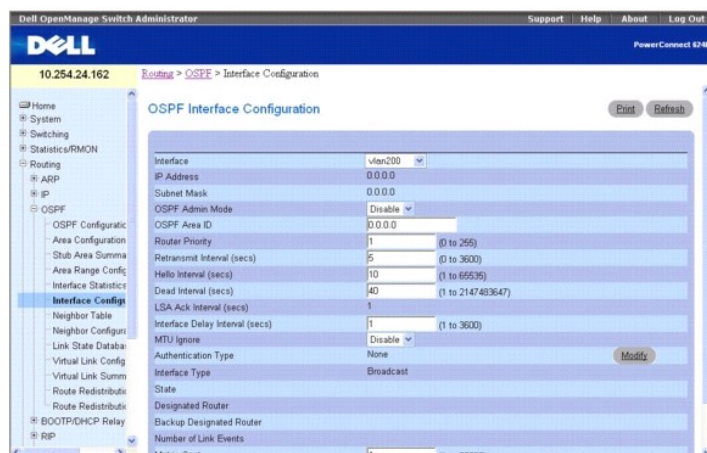
- 1 Comandos de OSPF

Configuración de interfaz

Utilice la página OSPF Interface Configuration (Configuración de interfaz OSPF) para configurar una interfaz OSPF.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 10-11. Configuración de interfaz OSPF



La página OSPF Interface Configuration (Configuración de interfaz OSPF) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz cuyos datos desea visualizar o configurar.

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

Subnet Mask (Máscara de subred): muestra la máscara de subred de la interfaz de VLAN.

OSPF Admin Mode (Modo de administración de OSPF): puede seleccionar Enable (Activar) o Disable (Desactivar) en el menú desplegable. El valor predeterminado es Disable (Desactivar). Puede configurar los parámetros de OSPF sin activar el modo de administración de OSPF, pero la configuración no tendrá efecto hasta que se active dicho modo. La información siguiente sólo se visualiza si el modo de administración está activado: State (Estado), Designated Router (Enrutador designado), Backup Designated Router (Enrutador designado de reserva), Number of Link Events (Número de eventos de enlace), LSA Ack Interval (Intervalo de confirmación de LSA) y Metric Cost (Coste de métrica). Para que OSPF sea completamente funcional, debe introducir una dirección IP y una máscara de subred válidas mediante la página IP Interface Configuration (Configuración de interfaz IP).

NOTA: una vez que OSPF se inicializa en el enrutador, permanece inicializado hasta que se restablece el enrutador.

OSPF Area ID (ID de área OSPF): introduzca el número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área OSPF a la que se conecta la interfaz de enrutador seleccionada. Si asigna una ID de área que no existe, el área se crea con los valores predeterminados.

Router Priority (Prioridad de enrutador): introduzca la prioridad de OSPF de la interfaz seleccionada. La prioridad de una interfaz se especifica mediante un número entero comprendido entre 0 y 255. El valor predeterminado es 1, que es la prioridad de enrutador más alta. El valor 0 indica que el enrutador no puede convertirse en el designado para esta red.

Retransmit Interval (secs) (Intervalo de retransmisión [seg.]): introduzca el intervalo de retransmisión de OSPF para la interfaz especificada. Se trata del número de segundos transcurridos entre los anuncios de estado de enlace correspondientes a las adyacencias de esta interfaz de enrutador. Este valor también se utiliza al retransmitir descripciones de bases de datos y paquetes de petición de estado de enlace. Los valores válidos están comprendidos entre 0 y 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

Hello Interval (secs) (Intervalo de saludo [seg.]): introduzca el intervalo de saludo de OSPF en segundos para la interfaz especificada. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Los valores válidos están comprendidos entre 1 y 65535. El valor predeterminado es 10 segundos.

Dead Interval (secs) (Intervalo de finalización [seg.]): introduzca el intervalo de finalización de OSPF en segundos para la interfaz especificada. Este intervalo corresponde al tiempo que el enrutador debe esperar a ver los paquetes de saludo de un enrutador de vecino antes de declarar que el enrutador está fuera de servicio. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Este valor debe ser un múltiplo del intervalo de saludo (por ejemplo, 4). Los valores válidos están comprendidos entre 1 y 2147483647. El valor predeterminado es 40.

LSA Ack Interval (Intervalo de confirmación de LSA): número de segundos transcurridos entre las transmisiones de paquetes de confirmación de LSA, que debe ser inferior al intervalo de retransmisión.

Interface Delay Interval (secs) (Intervalo de demora de la interfaz [seg.]): introduzca la demora de transmisión de OSPF para la interfaz especificada. Este intervalo corresponde al número estimado de segundos que se tarda en transmitir un paquete de actualización de estado de enlace en la interfaz seleccionada. Los valores válidos están comprendidos entre 1 y 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

MTU Ignore (Ignorar MTU): desactiva la detección de discrepancia de MTU de OSPF al recibir paquetes. El valor predeterminado es Disable (Desactivar).

Authentication Type (Tipo de autenticación): puede seleccionar un tipo de autenticación distinto de None (Ninguno) haciendo clic en el botón **Modify** (Modificar). Aparece una nueva página web, donde puede seleccionar el tipo de autenticación en el menú desplegable. Los valores posibles son:

- None** (Ninguno): estado inicial de la interfaz. Si selecciona esta opción en el menú desplegable de la segunda pantalla y hace clic en **Apply Changes** (Aplicar cambios), volverá a la primera pantalla y no se ejecutará ningún protocolo de autenticación.
- Simple**: si selecciona este valor, se le solicitará que introduzca una clave de autenticación. Esta clave se muestra explícitamente en la cabecera de OSPF de todos los paquetes enviados en la red. Todos los enrutadores de la red deben configurarse con la misma clave.
- Encrypt** (Cifrar): si selecciona este valor, se le solicitará que introduzca una clave de autenticación y una ID de autenticación. Para el cifrado se utiliza el algoritmo MD5 Message-Digest. Todos los enrutadores de la red deben configurarse con la misma clave y la misma ID.

Interface Type (Tipo de interfaz): tipo de interfaz OSPF, que siempre se difunde.

State (Estado): estado actual de la interfaz de enrutador seleccionada. Los valores posibles son:

- Down** (Desconectada): estado inicial de la interfaz. En este estado, los protocolos de nivel bajo han indicado que la interfaz no puede utilizarse. En este estado, los parámetros de la interfaz están configurados con sus valores iniciales. Todos los temporizadores de la interfaz están desactivados, y

no hay ninguna adyacencia asociada a la interfaz.

- 1 **Loopback** (Bucle de retorno): en este estado, existe en la interfaz del enrutador un bucle de retorno a la red por hardware o por software. La interfaz no está disponible para el tráfico regular de datos. Sin embargo, puede seguir siendo interesante obtener información sobre la calidad de esta interfaz, ya sea enviando pings de ICMP o mediante algo parecido a una prueba de errores de bits. Por ello, sigue siendo posible dirigir paquetes IP a una interfaz en estado Loopback (Bucle de retorno). Para facilitar esta operación, dichas interfaces se anuncian en LSA de enrutador como rutas de host único, cuyo destino es la dirección de la interfaz IP.
- 1 **Waiting** (En espera): el enrutador está intentando determinar la identidad del enrutador designado (de reserva) para la red mediante la supervisión de los paquetes de saludo recibidos. El enrutador no tiene permitido elegir un enrutador designado de reserva ni un enrutador designado hasta que no salga del estado Waiting (En espera). Esto evita cambios innecesarios del enrutador designado (de reserva).
- 1 **Designated Router** (Enrutador designado): se trata del enrutador designado en la red asociada. Se establecen adyacencias con todos los demás enrutadores asociados a la red. El enrutador debe asimismo originar un network-LSA (LSA de red) para el nodo de red. El network-LSA (LSA de red) contiene enlaces a todos los enrutadores (incluido el enrutador designado) conectados a la red.
- 1 **Backup Designated Router** (Enrutador designado de reserva): se trata del enrutador designado de reserva en la red asociada. Pasa a ser el enrutador designado si el enrutador designado actual falla. El enrutador establece adyacencias con todos los demás enrutadores asociados a la red. El enrutador designado de reserva lleva a cabo funciones ligeramente diferentes durante el procedimiento de distribución en comparación con el enrutador designado.
- 1 **Other Designated Router** (Otro enrutador designado): la interfaz se conecta a una red NBMA o de difusión en la que se han seleccionado otros enrutadores para ser el enrutador designado y el enrutador designado de reserva. El enrutador intenta formar adyacencias tanto con el enrutador designado como con el enrutador designado de reserva.

El estado sólo se visualiza si está activado el modo de administración de OSPF.

Designated Router (Enrutador designado): identificación del enrutador designado para esta red desde el punto de vista del enrutador de divulgación. El enrutador designado se identifica aquí mediante su ID de enrutador. El valor 0.0.0.0 significa que no hay ningún enrutador designado. Este campo sólo se visualiza si está activado el modo de administración de OSPF.

Backup Designated Router (Enrutador designado de reserva): identificación del enrutador designado de reserva para esta red desde el punto de vista del enrutador de divulgación. El enrutador designado de reserva se identifica aquí mediante su ID de enrutador. El valor 0.0.0.0 significa que no hay ningún enrutador designado de reserva. Este campo sólo se visualiza si está activado el modo de administración de OSPF.

Number of Link Events (Número de eventos de enlace): número de veces que la interfaz OSPF especificada ha cambiado de estado. Este campo sólo se visualiza si está activado el modo de administración de OSPF.

Metric Cost (Coste de métrica): introduzca el valor de esta interfaz para el tipo de servicio (TOS) de coste. El intervalo para el coste de métrica va de 1 a 65535. Este campo sólo puede configurarse o visualizarse si se ha inicializado OSPF en la interfaz.

Configuración de una configuración de interfaz OSPF

1. Abra la página **OSPF Interface Configuration** (Configuración de interfaz OSPF).
2. Especifique la interfaz que desea configurar.
3. Especifique valores en los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La interfaz OSPF está configurada.

Visualización de una configuración de interfaz OSPF

1. Abra la página **OSPF Interface Configuration** (Configuración de interfaz OSPF).
2. Seleccione en el menú desplegable la interfaz de VLAN cuyos datos desea visualizar.

Se visualizan los datos de configuración de esta interfaz.

Configuración de una interfaz OSPF mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

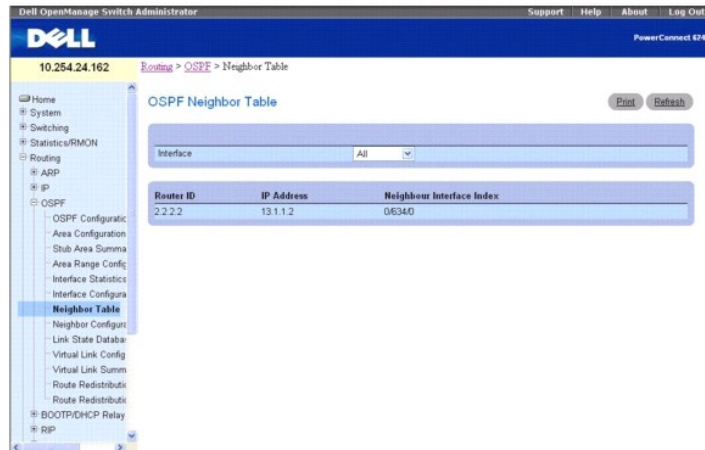
- 1 Comandos de OSPF

Tabla de vecinos

Utilice la página **OSPF Neighbor Table** (Tabla de vecinos OSPF) para visualizar la lista de tablas de vecinos OSPF. Cuando se especifica una ID de vecino en particular, se proporciona información detallada sobre un vecino. La información siguiente sólo se visualiza si se ha activado OSPF.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Neighbor Table** (Tabla de vecinos) en la vista de árbol.

Ilustración 10-12. Tabla de vecinos OSPF



La página OSPF Neighbor Table (Tabla de vecinos OSPF) incluye los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz cuyos datos desea visualizar.

Router ID (ID de enrutador): número entero de 32 bits en formato con punto decimal que representa la interfaz de vecino.

IP Address (Dirección IP): dirección IP de la interfaz del enrutador de vecino para la red conectada. Se utiliza como dirección IP destino cuando se envían paquetes de protocolo como difusiones únicas junto con esta adyacencia. También se utiliza en los router-LSA (LSA de enrutador) como ID de enlace de la red conectada si se ha seleccionado el enrutador de vecino como enrutador designado. La dirección IP de vecino se obtiene cuando se reciben los paquetes de saludo del vecino. En el caso de los enlaces virtuales, la dirección IP de vecino se obtiene durante el proceso de creación de tablas de enrutamiento.

Neighbor Interface Index (Índice de interfaz de vecino): interfaz que identifica el índice de interfaz de vecino.

Visualización de la tabla de vecinos OSPF mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Configuración de vecino

Utilice la página OSPF Neighbor Configuration (Configuración de vecino OSPF) para visualizar la configuración de vecino OSPF correspondiente a una ID de vecino seleccionada. Cuando se especifica una ID de vecino en particular, se proporciona información detallada sobre el vecino. La información siguiente sólo se visualiza cuando se ha activado OSPF y la interfaz tiene un vecino. La dirección IP es la dirección IP del vecino.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Neighbor Configuration** (Configuración de vecino) en la vista de árbol.

Ilustración 10-13. Configuración de vecino OSPF



La página OSPF Neighbor Configuration (Configuración de vecino OSPF) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz de VLAN en la que el enrutamiento está activado.

Neighbor IP Address (Dirección IP de vecino): seleccione la dirección IP del vecino cuyos datos desea visualizar.

Router ID (ID de enrutador): número entero de 32 bits en formato con punto decimal que identifica el enrutador de vecino.

Options (Opciones): capacidades opcionales de OSPF admitidas por el vecino. El campo de opciones de OSPF está presente en los paquetes de saludo OSPF, en los paquetes de descripción de base de datos y en los anuncios de estado de enlace. Este campo permite a los enrutadores OSPF admitir (o no admitir) capacidades opcionales y comunicar su nivel de capacidad a otros enrutadores OSPF. A través de este mecanismo, es posible combinar enrutadores con capacidades distintas en un mismo dominio de enrutamiento OSPF. El valor de este campo es un mapa de bits que indica la capacidad del vecino.

Router Priority (Prioridad de enrutador): muestra la prioridad de OSPF del vecino especificado. La prioridad de un vecino es un número entero comprendido entre 0 y 255. El valor 0 indica que el enrutador no puede convertirse en enrutador designado para esta red.

State (Estado): el estado de un vecino puede ser el siguiente:

- 1 **Down** (Desconectado): estado inicial de una conversación de vecino. Indica que no se ha recibido información reciente procedente del vecino. En las redes NBMA, es posible seguir enviando paquetes de saludo con el estado Down (Desconectado), si bien con una frecuencia reducida.
- 1 **Attempt** (Intentar): este estado sólo es válido para los vecinos conectados a redes NBMA. Indica que no se ha recibido información reciente procedente del vecino, pero que debería hacerse un mayor esfuerzo común para contactar con él. Esto se realiza enviando al vecino paquetes de saludo a intervalos de Hello Interval (Intervalo de saludo).
- 1 **Init** (Iniciar): este estado indica que se ha visto recientemente un paquete de saludo procedente del vecino. Sin embargo, no se ha establecido todavía una comunicación bidireccional con el vecino (es decir, el enrutador no aparecía en el paquete de saludo del vecino). Todos los vecinos que se encuentran en este estado (o en uno superior) se enumeran en los paquetes de saludo enviados desde la interfaz asociada.
- 1 **2-Way** (Bidireccional): este estado indica que la comunicación entre los dos enrutadores es bidireccional. Esto se garantiza a través del funcionamiento del protocolo de saludo. Éste es el estado más avanzado antes de comenzar el establecimiento de adyacencias. El enrutador designado (de reserva) se selecciona de entre el grupo de vecinos que se encuentran en el estado 2-way (Bidireccional) o en uno superior.
- 1 **Exchange Start** (Inicio de intercambio): se trata del primer paso en la creación de una adyacencia entre dos enrutadores de vecino. El objetivo de este paso es decidir qué enrutador es el enrutador maestro y cuál es el número de secuencia de descripción de base de datos (DD) inicial. Las conversaciones de vecino en este estado o en estados superiores se denominan adyacencias.
- 1 **Exchange** (Intercambio): en este estado, el enrutador describe toda su base de datos de estados de enlace enviando paquetes de descripción de base de datos al vecino. En este estado, también pueden enviarse paquetes de petición de estado de enlace que pregunten por los LSA más recientes del vecino. Para el procedimiento de distribución se utilizan todas las adyacencias con el estado Exchange (Intercambio) o un estado superior. Estas adyacencias son totalmente capaces de transmitir y recibir todos los tipos de paquetes de protocolo de enrutamiento OSPF.
- 1 **Loading** (Cargando): en este estado, se envían paquetes de petición de estado de enlace al vecino que preguntan por los LSA más recientes que se han detectado (pero todavía no se han recibido) con el estado Exchange (Intercambio).
- 1 **Full** (Completo): en este estado, los enrutadores de vecino son completamente adyacentes. Estas adyacencias aparecen en los router-LSA (LSA de enrutador) y network-LSA (LSA de red).

Events (Eventos): número de veces que ha cambiado el estado de esta relación de vecino o que se ha producido un error.

Permanence (Permanencia): variable que muestra el estado de la entrada. Dynamic (Dinámico) y Permanent (Permanente) se refieren a cómo se ha dado a conocer el vecino.

Hellos Suppressed (Saludos suprimidos): indica si se están suprimiendo los saludos dirigidos al vecino.

Retransmission Queue Length (Longitud de cola de retransmisión): longitud actual de la cola de retransmisión.

Visualización de la configuración de vecino OSPF

1. Abra la página **OSPF Neighbor Configuration** (Configuración de vecino OSPF).
2. Seleccione la interfaz y la dirección IP que desea visualizar.

Se visualiza la configuración de vecino.

Visualización de la configuración de vecino OSPF mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Base de datos de estados de enlace

Utilice la página **OSPF Link State Database** (Base de datos de estados de enlace OSPF) para visualizar información sobre el estado de los enlaces OSPF.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Link State Database** (Base de datos de estados de enlace) en la vista de árbol.

Ilustración 10-14. Base de datos de estados de enlace OSPF

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays the 'OSPF Link State Database' with a table of OSPF link state information. The table has columns for Router ID, Area ID, LSA Type, LS ID, Age, Sequence, Checksum, and Options. The table contains 14 rows of data representing various OSPF link state advertisements.

Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options
1.1.1.1	0.0.0.0	Router Links	1.1.1.1	336	-2147483641	0x8958	E --
2.2.2.2	0.0.0.0	Router Links	2.2.2.2	340	-2147483640	0xac41	E --
2.2.2.2	0.0.0.0	Network Links	13.1.1.2	460	-2147483647	0xa64e	E --
1.1.1.1	0.0.0.0	Network Summary	17.1.1.0	355	-2147483646	0xba90	E --
2.2.2.2	0.0.0.0	Network Summary	17.1.1.0	351	-2147483646	0x4269	E --
2.2.2.2	0.0.0.0	Summary ASBR	1.1.1.1	351	-2147483647	0xc652	E --
1.1.1.1	0.0.0.1	Router Links	1.1.1.1	340	-2147483644	0xb25c	E --
2.2.2.2	0.0.0.1	Router Links	2.2.2.2	341	-2147483643	0x9486	E --
2.2.2.2	0.0.0.1	Network Links	17.1.1.2	356	-2147483647	0xb37e	E --
1.1.1.1	0.0.0.1	Network Summary	13.1.1.0	365	-2147483646	0xae60	E --
2.2.2.2	0.0.0.1	Network Summary	13.1.1.0	445	-2147483645	0x74ce	E --

La página OSPF Link State Database (Base de datos de estados de enlace OSPF) incluye los campos siguientes:

Router ID (ID de enrutador): número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el enrutador dentro del sistema autónomo (AS). La ID de enrutador se configura en la página IP Configuration (Configuración de IP). Si desea cambiar la ID de enrutador, primero debe desactivar OSPF. Una vez que haya configurado la nueva ID de enrutador, debe volver a activar OSPF para que el cambio tenga efecto. El valor predeterminado es 0.0.0.0, si bien este valor no es una ID de enrutador válida.

Area ID (ID de área): ID de un área OSPF a la que se conecta una de las interfaces de enrutador. Una ID de área es un número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta una interfaz.

LSA Type (Tipo de LSA): formato y función del anuncio de estado de enlace. Los valores posibles son:

- 1 Router Links (Enlaces de enrutador)
- 1 Network Links (Enlaces de red)
- 1 Network Summary (Resumen de red)
- 1 ASBR Summary (Resumen de ASBR)
- 1 AS-external (Externo al AS)

LS ID (ID de LS): ID de estado de enlace (LS) que identifica la parte del dominio de enrutamiento que está describiendo el anuncio. El valor de la ID de LS depende del tipo de estado de enlace del anuncio.

Age (Edad): tiempo en segundos transcurrido desde que se ha originado el anuncio de estado de enlace por primera vez.

Sequence (Secuencia): número entero de 32 bits con signo. Permite detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.

Checksum (Suma de comprobación): sirve para detectar daños en los datos de un anuncio. Estos daños pueden producirse mientras se distribuye un anuncio o mientras éste se encuentra almacenado en la memoria de un enrutador. Este campo es la suma de comprobación de todo el contenido del anuncio, excepto el campo de edad del LS.

Options (Opciones): el campo Options (Opciones) que figura en el encabezado del anuncio de estado de enlace indica qué capacidades opcionales están asociadas al anuncio. Los valores posibles son:

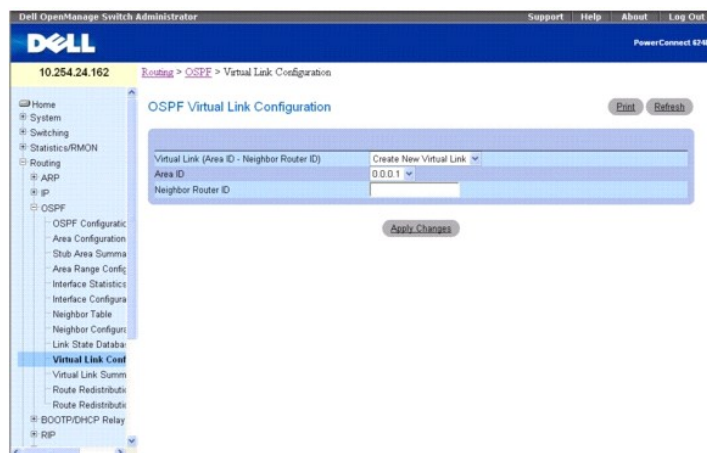
- 1 **Q**: activa la compatibilidad con la ingeniería de tráfico QoS.
- 1 **E**: describe cómo se distribuyen los AS-external-LSA (LSA externos al AS).
- 1 **MC**: describe cómo se reenvían los datagramas de multidifusión IP de acuerdo con las especificaciones estándar.
- 1 **O**: describe si se admiten los Opaque-LSA (LSA opacos).
- 1 **V**: describe si se admiten las extensiones OSPF++ para VPN/COS.

Configuración de enlace virtual

Utilice la página Virtual Link Configuration (Configuración de enlace virtual) para crear o configurar información sobre la interfaz virtual de un área y un vecino específicos. Para poder visualizar esta página, antes debe configurarse un área OSPF válida.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Virtual Link Configuration** (Configuración de enlace virtual) en la vista de árbol.

Ilustración 10-15. Configuración de enlace virtual OSPF – Crear



La página OSPF Virtual Link Configuration (Configuración de enlace virtual OSPF) contiene los campos siguientes:

Virtual Link (Area ID – Neighbor Router ID) (Enlace virtual [ID de área – ID de enrutador de vecino]): seleccione el enlace virtual cuyos datos desea visualizar o configurar. Este parámetro consta de la ID de área y la ID de enrutador de vecino. Para crear un enlace virtual nuevo, seleccione **Create New Virtual Link** (Crear nuevo enlace virtual) en el menú desplegable para definir un nuevo enlace virtual. Cuando se selecciona **Create New Virtual Link** (Crear nuevo enlace virtual), se muestran los campos siguientes:

Area ID (ID de área): número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta una interfaz de enrutador.

Neighbor Router ID (ID de enrutador de vecino): número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el enrutador de vecino que forma parte del enlace virtual.

Hello Interval (Intervalo de saludo): introduzca el intervalo de saludo de OSPF en segundos para la interfaz especificada. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Los valores válidos están comprendidos entre 1 y 65535. El valor predeterminado es 10 segundos.

Dead Interval (Intervalo de finalización): introduzca el intervalo de finalización de OSPF en segundos para la interfaz especificada. Este intervalo corresponde al tiempo que el enrutador debe esperar a ver los paquetes de saludo de un enrutador de vecino antes de declarar que el enrutador está fuera de servicio. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Este valor debe ser un múltiplo del intervalo de saludo (por ejemplo, 4). Los valores válidos están comprendidos entre 1 y 65535. El valor predeterminado es 40 segundos.

Interface Delay Interval (secs.) (Intervalo de demora de la interfaz [seg.]): demora de transmisión de OSPF del enlace virtual en unidades de segundos. Este intervalo corresponde al número estimado de segundos que se tarda en transmitir un paquete de actualización de estado de enlace en esta interfaz.

State (Estado): estado actual del enlace virtual seleccionado. Puede ser uno de los siguientes:

- 1 **Down** (Desconectada): estado inicial de la interfaz. En este estado, los protocolos de nivel bajo han indicado que la interfaz no puede utilizarse. En este estado, los parámetros de la interfaz están configurados con sus valores iniciales. Todos los temporizadores de la interfaz están desactivados, y no hay ninguna adyacencia asociada a la interfaz.
- 1 **Waiting** (En espera): el enrutador está intentando determinar la identidad del enrutador designado (de reserva) mediante la supervisión de los paquetes de saludo recibidos. El enrutador no tiene permitido elegir un enrutador designado de reserva ni un enrutador designado hasta que no salga del estado Waiting (En espera). Esto evita cambios innecesarios del enrutador designado (de reserva).
- 1 **Point-to-Point** (Punto a punto): la interfaz se encuentra operativa y está conectada al enlace virtual. Al entrar en este estado, el enrutador intenta formar una adyacencia con el enrutador de vecino. Se envían paquetes de saludo al vecino a cada intervalo de segundos definido en Hello Interval (Intervalo de saludo).
- 1 **Designated Router** (Enrutador designado): se trata del enrutador designado en la red asociada. Se establecen adyacencias con todos los demás enrutadores asociados a la red. El enrutador debe asimismo originar un network-LSA (LSA de red) para el nodo de red. El network-LSA (LSA de red) contiene enlaces a todos los enrutadores (incluido el enrutador designado) conectados a la red.
- 1 **Backup Designated Router** (Enrutador designado de reserva): se trata del enrutador designado de reserva en la red asociada. Pasa a ser el enrutador designado si el enrutador designado actual falla. El enrutador establece adyacencias con todos los demás enrutadores asociados a la red. El enrutador designado de reserva lleva a cabo funciones ligeramente diferentes durante el procedimiento de distribución en comparación con el enrutador designado.
- 1 **Other Designated Router** (Otro enrutador designado): la interfaz se conecta a una red NBMA o de difusión en la que se han seleccionado otros enrutadores para ser el enrutador designado y el enrutador designado de reserva. El enrutador intenta formar adyacencias tanto con el enrutador designado como con el enrutador designado de reserva.

Neighbor State (Estado de vecino): estado de la relación de vecino virtual.

Retransmit Interval (Intervalo de retransmisión): introduzca el intervalo de retransmisión de OSPF para la interfaz especificada. Se trata del número de segundos transcurridos entre los anuncios de estado de enlace correspondientes a las adyacencias de esta interfaz de enrutador. Este valor también se utiliza al retransmitir descripciones de bases de datos y paquetes de petición de estado de enlace. Los valores válidos están comprendidos entre 0 y 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

Authentication Type (Tipo de autenticación): puede seleccionar un tipo de autenticación distinto de None (Ninguno) haciendo clic en el botón **Configure Authentication** (Configurar autenticación). Aparece una nueva pantalla, donde puede seleccionar el tipo de autenticación en el menú desplegable. Las opciones posibles son:

- 1 **None** (Ninguno): estado inicial de la interfaz. Si selecciona esta opción en el menú desplegable de la segunda pantalla y hace clic en **Apply Changes** (Aplicar cambios), volverá a la primera pantalla.
- 1 **Simple**: si selecciona este valor, se le solicitará que introduzca una clave de autenticación. Esta clave se muestra explícitamente en la cabecera de OSPF de todos los paquetes enviados en la red. Todos los enrutadores de la red deben configurarse con la misma clave.

- 1 **Encrypt (Cifrar)**: si selecciona este valor, se le solicitará que introduzca una clave de autenticación y una ID de autenticación. Para el cifrado se utiliza el algoritmo MD5 Message-Digest. Todos los enrutadores de la red deben configurarse con la misma clave y la misma ID.

Authentication Key (Clave de autenticación): introduzca la clave de autenticación de OSPF para la interfaz especificada. Si opta por no utilizar la autenticación, no se le solicitará que introduzca una clave. Si opta por la autenticación Simple, no puede utilizar una clave de más de 8 caracteres. Si elige Encrypt (Codificar), la clave puede ser de hasta 16 caracteres. El valor de la clave únicamente se visualiza si ha iniciado la sesión con privilegios de lectura y escritura; de lo contrario, se visualiza en forma de asteriscos.

Authentication ID (ID de autenticación): introduzca la ID que se utilizará para la autenticación. Sólo se le solicitará que introduzca una ID si ha seleccionado Encrypt (Cifrar) como tipo de autenticación. La ID es un número comprendido entre 0 y 255, ambos incluidos.

Definición de un nuevo enlace virtual

1. Abra la página **OSPF Virtual Link Configuration** (Configuración de enlace virtual OSPF).
2. Seleccione **Create New Virtual Link** (Crear nuevo enlace virtual) en el menú desplegable **Virtual Link (Area ID - Neighbor Router ID)** (Enlace virtual [ID de área - ID de enrutador de vecino]).
3. Especifique la ID de enrutador de vecino del nuevo enlace virtual.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los campos restantes se visualizan una vez creado el enlace virtual.

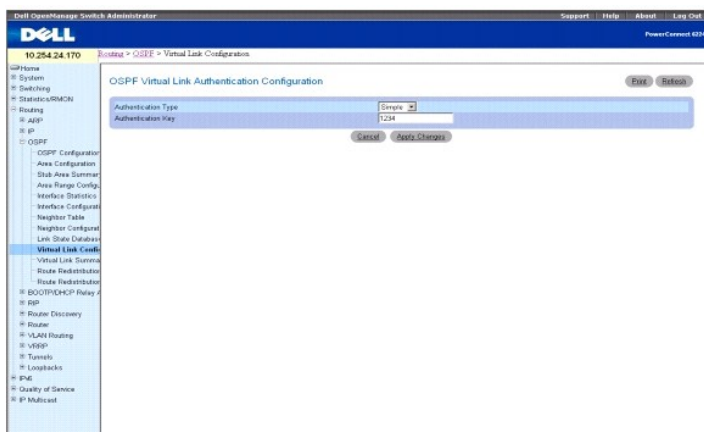
Ilustración 10-16. Configuración de enlace virtual OSPF



5. Haga clic en **Configure Authentication** (Configurar autenticación) para modificar la autenticación.

Aparece la página siguiente:

Ilustración 10-17. Configuración de la autenticación de enlace virtual OSPF



6. Seleccione valores para **Authentication Type** (Tipo de autenticación) y **Authentication Key** (Clave de autenticación).

7. Haga clic en **Apply Changes** (Aplicar cambios) cuando haya terminado.

Configuración de datos de enlace virtual

1. Abra la página **OSPF Virtual Link Configuration** (Configuración de enlace virtual OSPF).
2. Especifique la ID de área y la ID de enrutador de vecino que desea configurar.
3. Introduzca datos en los campos según sea necesario.
4. Haga clic en **Configure Authentication** (Configurar autenticación) para modificar la autenticación.
5. Haga clic en **Apply Changes** (Aplicar cambios) cuando haya terminado.

Se configuran los datos de enlace virtual correspondientes a las ID especificadas y se actualiza el dispositivo.

Visualización de datos de enlace virtual

1. Abra la página **OSPF Virtual Link Configuration** (Configuración de enlace virtual OSPF).
2. Especifique la ID de área y la ID de enrutador de vecino que desea visualizar.

Se visualizan los datos de enlace virtual correspondientes a estas ID.

Eliminación de un enlace virtual

1. Abra la página **OSPF Virtual Link Configuration** (Configuración de enlace virtual OSPF).
2. Especifique la ID de área y la ID de enrutador de vecino asociadas al enlace virtual que desea eliminar.

Se visualizan los datos de enlace virtual relacionados.
3. Haga clic en **Delete** (Eliminar).

Se elimina el enlace virtual y se actualiza el dispositivo.

Configuración de datos de enlace virtual mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Resumen de enlaces virtuales

Utilice la página **OSPF Virtual Link Summary** (Resumen de enlaces virtuales OSPF) para visualizar todos los enlaces virtuales configurados.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Virtual Link Summary** (Resumen de enlaces virtuales) en la vista de árbol.

Ilustración 10-18. Resumen de enlaces virtuales OSPF

Area ID	Neighbor Router ID	Hello Interval (secs)	Dead Interval (secs)	Retransmit Interval (secs)	Itransit Delay Interval (secs)
0.0.0.1	2.2.2.2	10	40	5	1

La página OSPF Virtual Link Summary (Resumen de enlaces virtuales OSPF) contiene los campos siguientes:

Area ID (ID de área): parte correspondiente a la ID de área dentro de la identificación del enlace virtual cuyos datos desea visualizar. La ID de área define, junto con la ID de enrutador de vecino, un enlace virtual.

Neighbor Router ID (ID de enrutador de vecino): parte correspondiente al vecino dentro de la identificación del enlace virtual. Es posible configurar enlaces virtuales entre cualquier par de enrutadores de límite de área que tengan interfaces a un área (no de red troncal) común.

Hello Interval (secs) (Intervalo de saludo [seg.]): intervalo de saludo de OSPF del enlace virtual en unidades de segundos. El valor del intervalo de saludo debe ser el mismo para todos los enrutadores asociados a una red.

Dead Interval (secs) (Intervalo de finalización [seg.]): intervalo de finalización de OSPF del enlace virtual en unidades de segundos. Este intervalo corresponde al tiempo que el enrutador debe esperar a ver los paquetes de saludo de un enrutador de vecino antes de declarar que el enrutador está fuera de servicio. Este parámetro debe ser igual para todos los enrutadores conectados a una red común y debe ser un múltiplo del intervalo de saludo (por ejemplo, 4).

Retransmit Interval (secs) (Intervalo de retransmisión [seg.]): intervalo de retransmisión de OSPF del enlace virtual en unidades de segundos. Se trata del tiempo transcurrido entre los anuncios de estado de enlace correspondientes a las adyacencias de esta interfaz de enrutador. Este valor también se utiliza al retransmitir descripciones de bases de datos y paquetes de petición de estado de enlace.

Itransit Delay Interval (secs) (Intervalo de demora de transmisión de la interfaz [seg.]): demora de transmisión de OSPF del enlace virtual en unidades de segundos. Este intervalo corresponde al número estimado de segundos que se tarda en transmitir un paquete de actualización de estado de enlace en esta interfaz.

Visualización del resumen de enlaces virtuales mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Configuración de redistribución de rutas

Utilice la página **OSPF Route Redistribution Configuration** (Configuración de redistribución de rutas OSPF) para configurar la redistribución en OSPF de las rutas obtenidas de los orígenes Static (Estático), Connected (Conectado) y RIP. Puede redistribuir las rutas obtenidas de todos estos orígenes o de algunos de ellos.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Route Redistribution Configuration** (Configuración de redistribución de rutas) en la vista de árbol.

Ilustración 10-19. Configuración de redistribución de rutas OSPF



La página **OSPF Route Redistribution Configuration** (Configuración de redistribución de rutas OSPF) contiene los campos siguientes:

Configured Source (Origen configurado): protocolo configurado para OSPF para la redistribución de las rutas obtenidas a través de este protocolo. Sólo están disponibles las rutas de origen que se han configurado para su redistribución mediante OSPF. Create (Crear) permite configurar una nueva ruta de origen.

Available Source (Origen disponible): protocolo que puede configurarse para OSPF para la redistribución de las rutas. Esta casilla sólo aparece si se selecciona Create (Crear) para Configured Source (Origen configurado). Los valores posibles son Static (Estático), Connected (Conectado) y RIP.

Metric (Métrica): establece el valor de métrica para las rutas redistribuidas. Este campo muestra un valor de métrica si se ha configurado previamente el origen. Los valores válidos son de 0 a 16777214.

Metric Type (Tipo de métrica): seleccione en el menú desplegable el tipo de métrica OSPF para las rutas redistribuidas.

Tag (Etiqueta): establece el campo de etiqueta en las rutas redistribuidas. Este campo muestra un valor de etiqueta si se ha configurado previamente el origen; de lo contrario, se muestra el valor 0. Los valores válidos son de 0 a 4294967295.

Subnets (Subredes): seleccione en el menú desplegable si las rutas con subredes deben redistribuirse o no.

Distribute List (Lista de distribución): permite seleccionar la lista de acceso que filtra las rutas que van a redistribuirse mediante el protocolo de destino. Sólo se redistribuyen las rutas permitidas. Si este comando se refiere a una lista de acceso no existente, están permitidas todas las rutas. En el menú desplegable se enumeran las listas de control de acceso (ACL) configuradas desde las páginas **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **Access Control Lists** (Listas de control de acceso) → **IP Access Control Lists** (Listas de control de acceso IP). Cuando se utilizan para el filtrado de rutas, los únicos campos de una lista de acceso que se emplean son:

- 1 Dirección IP y máscara de red de origen
- 1 Dirección IP y máscara de red de destino
- 1 Acción (permitir o denegar)

Los demás campos (puerto de origen y de destino, precedencia, TOS, etc.) se omiten.

La dirección IP de origen se compara con la dirección IP de destino de la ruta. La máscara de red IP de origen de la regla de la lista de acceso se trata como máscara comodín, que indica qué bits de la dirección IP de origen deben coincidir con la dirección de destino de la ruta. Tenga en cuenta que un 1 en la máscara indica "Don't Care" (No importa) en el bit correspondiente de la dirección.

Cuando una regla de lista de acceso incluye una dirección IP y una máscara de red de destino (lista de acceso ampliada), la dirección IP de destino se compara con la máscara de red del destino de la ruta. La máscara de red de destino de la lista de acceso sirve de máscara comodín, que indica qué bits de la máscara de destino de la ruta son significativos para la operación de filtrado.

Creación de un origen de redistribución de rutas OSPF

Cuando no se ha configurado ninguna redistribución, el sistema sólo muestra Create (Crear) en el campo Configured Source (Origen configurado) y los orígenes posibles en los campos de Available Source (Origen disponible). Cuando se selecciona un origen disponible, se introducen datos de configuración y se hace clic en **Apply Changes** (Aplicar cambios), el elemento se visualiza en la lista desplegable Configured Source (Origen configurado) y se elimina de la lista desplegable Available Source (Origen disponible).

1. Abra la página **OSPF Route Redistribution Configuration** (Configuración de redistribución de rutas OSPF).
2. Especifique **Create** (Crear) en el campo Configured Source (Origen configurado).
3. Seleccione Static (Estático), Connected (Conectado) o RIP en el campo Available Source (Origen disponible).
4. Haga clic en **Apply Changes** (Aplicar cambios) cuando haya terminado.

Se configuran los datos de redistribución de rutas y se actualiza el dispositivo.

Modificación de los datos de redistribución de rutas OSPF

1. Abra la página OSPF Route Redistribution Configuration (Configuración de redistribución de rutas OSPF).
2. Seleccione un origen en la lista desplegable Configured Source (Origen configurado).
3. Introduzca datos en los campos según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios) cuando haya terminado.

Se configuran los datos de redistribución de rutas y se actualiza el dispositivo.

Configuración de datos de redistribución de rutas OSPF mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

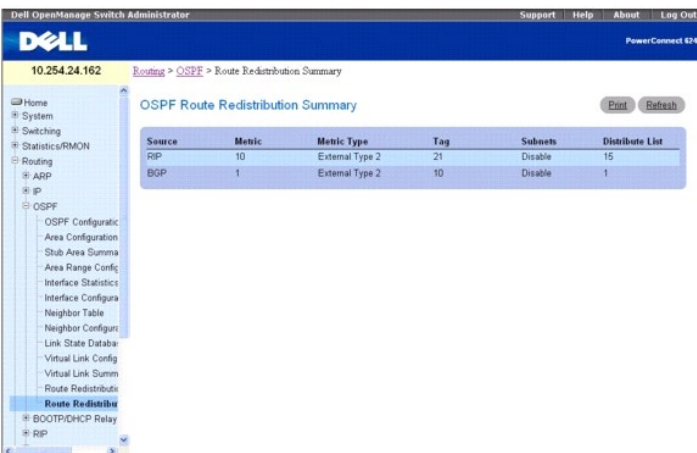
- 1 Comandos de OSPF

Resumen de redistribución de rutas

Utilice la página OSPF Route Redistribution Summary (Resumen de redistribución de rutas OSPF) para visualizar las configuraciones de redistribución de rutas OSPF.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **OSPF** → **Route Redistribution Summary** (Resumen de redistribución de rutas) en la vista de árbol.

Ilustración 10-20. Resumen de redistribución de rutas OSPF



Source	Metric	Metric Type	Tag	Subnets	Distribute List
RIP	10	External Type 2	21	Disable	15
BGP	1	External Type 2	10	Disable	1

La página OSPF Route Redistribution Summary (Resumen de redistribución de rutas OSPF) contiene los campos siguientes:

Source (Origen): ruta de origen que se redistribuirá mediante OSPF.

Metric (Métrica): métrica de rutas redistribuidas para la ruta de origen especificada. Cuando no está configurada, se muestra Unconfigured (Sin configurar).

Metric Type (Tipo de métrica): tipo de métrica OSPF de las rutas redistribuidas.

Tag (Etiqueta): campo de etiqueta de las rutas redistribuidas. Este campo muestra el valor de etiqueta si se ha configurado previamente el origen; de lo contrario, se muestra el valor 0.

Subnets (Subredes): especifica si las rutas con subredes deben redistribuirse o no.

Distribute List (Lista de distribución): lista de acceso que filtra las rutas que van a redistribuirse mediante el protocolo de destino.

Visualización del resumen de redistribución de rutas mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Agente de retransmisión BOOTP/DHCP

El agente de retransmisión BootP/DHCP permite a los clientes y servidores BootP/DHCP intercambiar mensajes BootP/DHCP entre diferentes subredes. El agente de retransmisión recibe las peticiones de los clientes y comprueba la validez de los saltos y los campos giaddr. Si el número de saltos es mayor que el configurado, el agente asume que el paquete se envía en bucle a través de los agentes y lo descarta. Si el campo giaddr es cero, el agente debe rellenarlo con la dirección IP de la interfaz en la que se ha recibido la petición. El agente realiza una difusión única de los paquetes válidos al siguiente destino configurado. El servidor responde con un mensaje BOOTREPLY de difusión única dirigido al agente de retransmisión más cercano al cliente, como se indica en el campo giaddr. Una vez recibido el mensaje BOOTREPLY del servidor, el agente reenvía esta respuesta como difusión o difusión única en la interfaz desde la que ha llegado el mensaje BOOTREQUEST. Esta interfaz puede identificarse mediante el campo giaddr.

El componente DHCP de la serie 6200 también admite opciones de agente de retransmisión DHCP para identificar el circuito de origen cuando los clientes se conectan a Internet mediante un módem de alta velocidad. El agente de retransmisión añade estas opciones cuando se reenvía la petición al servidor y las elimina cuando se envía la respuesta a los clientes.

Si una interfaz tiene más de una dirección IP, el agente de retransmisión debe utilizar la dirección IP principal configurada como su dirección IP de agente de transmisión.

La página de menú **BOOTP/DHCP Relay Agent** (Agente de transmisión BOOTP/DHCP) contiene enlaces a páginas web que permiten configurar y visualizar el agente de retransmisión BOOTP/DHCP. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **BOOTP/DHCP Relay Agent** (Agente de transmisión BOOTP/DHCP) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

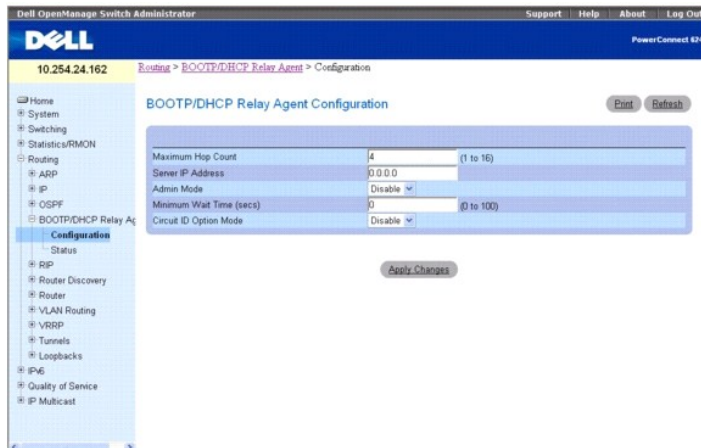
- 1 [Configuración del agente de retransmisión BOOTP/DHCP](#)
- 1 [Estado del agente de retransmisión BOOTP/DHCP](#)

Configuración del agente de retransmisión BOOTP/DHCP

Utilice la página **BOOTP/DHCP Relay Agent Configuration** (Configuración del agente de retransmisión BOOTP/DHCP) para configurar y visualizar un agente de retransmisión BOOTP/DHCP.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **BOOTP/DHCP Relay Agent** (Agente de retransmisión BOOTP/DHCP) → **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-21. Configuración del agente de retransmisión BOOTP/DHCP



La página **BOOTP/DHCP Relay Agent Configuration** (Configuración del agente de retransmisión BOOTP/DHCP) contiene los campos siguientes:

Maximum Hop Count (Recuento máximo de saltos): introduzca el número máximo de saltos que puede tardar una petición de cliente en ser descartada.

Server IP Address (Dirección IP del servidor): introduzca la dirección IP del servidor BOOTP/DHCP o la dirección IP del siguiente agente de retransmisión BOOTP/DHCP.

Admin Mode (Modo de administración): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si se selecciona Enable (Activar), las peticiones BOOTP/DHCP se reenvían a la dirección IP que se ha introducido en el campo Server IP Address (Dirección IP del servidor).

Minimum Wait Time (secs) (Tiempo mínimo de espera [seg.]): introduzca un tiempo en segundos. Este valor se compara con la marca de tiempo de los paquetes de petición del cliente, que debe representar el tiempo transcurrido desde que se ha encendido el cliente. Los paquetes sólo se reenvían cuando la marca de tiempo supera el tiempo mínimo de espera.

Circuit ID Option Mode (Modo de opción de ID de circuito): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si se selecciona Enable (Activar), el agente de retransmisión añade paquetes de cabecera Option 82 (Opción 82) a los paquetes de petición DHCP antes de reenviarlos al servidor, y los quita al reenviar las respuestas al cliente.

Configuración de BOOTP/DHCP

1. Abra la página **BOOTP/DHCP Configuration** (Configuración de BOOTP/DHCP).
2. Introduzca datos en los campos según sea necesario.

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

Se configuran los datos de BOOTP/DHCP y se actualiza el dispositivo.

Configuración de BOOTP/DHCP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

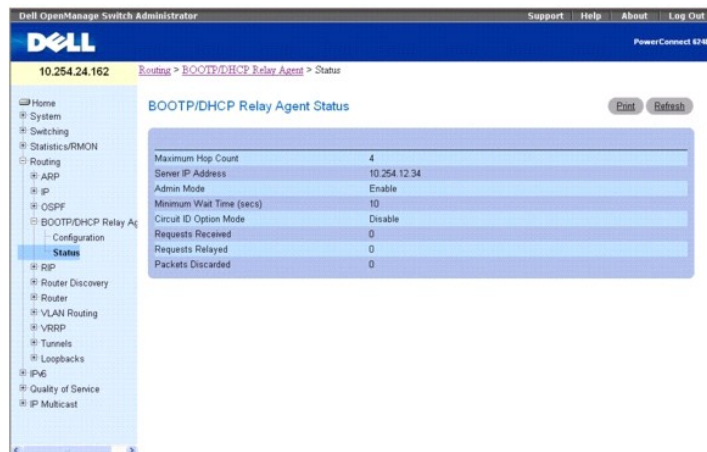
- 1 Comandos para la retransmisión DHCP y BOOTP

Estado del agente de retransmisión BOOTP/DHCP

Utilice la página **BOOTP/DHCP Relay Agent Status** (Estado del agente de retransmisión BOOTP/DHCP) para visualizar información sobre el estado y la configuración del agente de retransmisión BOOTP/DHCP.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **BOOTP/DHCP Relay Agent** (Agente de retransmisión BOOTP/DHCP)→ **Status** (Estado) en la vista de árbol.

Ilustración 10-22. Estado del agente de retransmisión BOOTP/DHCP



La página **BOOTP/DHCP Status** (Estado de BOOTP/DHCP) incluye los campos siguientes:

Maximum Hop Count (Recuento máximo de saltos): número máximo de saltos que una petición de cliente puede realizar antes de ser descartada.

Server IP Address (Dirección IP del servidor): dirección IP del servidor BOOTP/DHCP o dirección IP del siguiente agente de retransmisión BOOTP/DHCP.

Admin Mode (Modo de administración): modo administrativo de la retransmisión. Si se selecciona **Enable** (Activar) en la página de configuración, las peticiones BOOTP/DHCP se reenvían a la dirección IP que se ha introducido en el campo **Server IP Address** (Dirección IP del servidor).

Minimum Wait Time (secs) (Tiempo mínimo de espera [seg.]): tiempo mínimo en segundos. Este valor se compara con la marca de tiempo de los paquetes de petición del cliente, que debe representar el tiempo transcurrido desde que se ha encendido el cliente. Los paquetes sólo se reenvían cuando la marca de tiempo supera el tiempo mínimo de espera.

Circuit ID Option Mode (Modo de opción de ID de circuito): ésta es la opción del agente de retransmisión, que puede activarse (**Enable**) o desactivarse (**Disable**). Si se selecciona **Enable** (Activar), el agente de retransmisión añade paquetes de cabecera **Option 82** (Opción 82) a los paquetes de petición DHCP antes de reenviarlos al servidor, y los quita al reenviar las respuestas al cliente.

Requests Received (Peticiones recibidas): número total de peticiones BOOTP/DHCP recibidas de todos los clientes desde la última vez que se ha restablecido el conmutador.

Requests Relayed (Peticiones transmitidas): número total de peticiones BOOTP/DHCP reenviadas al servidor desde la última vez que se ha restablecido el conmutador.

Packets Discarded (Paquetes descartados): número total de paquetes BOOTP/DHCP descartados por este agente de retransmisión desde la última vez que se ha restablecido el conmutador.

Visualización de BOOTP/DHCP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para la retransmisión DHCP y BOOTP

RIP

El protocolo de información de enrutamiento (RIP) es un protocolo de puerta de enlace interior (IGP) basado en el algoritmo Bellman-Ford que está destinado a redes más pequeñas (diámetro de red no superior a 15 saltos). La información de enrutamiento se propaga en paquetes de actualización RIP que se envían periódicamente y cada vez que cambia la topología de la red. Al recibir una actualización RIP, según si la ruta especificada existe o no en la tabla de rutas, el enrutador puede modificar, eliminar o añadir la ruta en su tabla de rutas. Las preferencias de ruta se expresan por medio de una métrica configurable que indica la distancia de cada destino.

La página de menú **RIP** contiene enlaces a páginas web que permiten configurar y visualizar los parámetros y datos de RIP. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **RIP** en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

- 1 [Configuración de RIP](#)
- 1 [Resumen de interfaces RIP](#)
- 1 [Configuración de interfaz RIP](#)
- 1 [Configuración de redistribución de rutas RIP](#)
- 1 [Resumen de redistribución de rutas RIP](#)

Configuración de RIP

Utilice la página **RIP Configuration** (Configuración de RIP) para activar y configurar RIP, o para desactivarlo, en el modo Global. Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **RIP** → **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-23. Configuración de RIP



La página **RIP Configuration** (Configuración de RIP) contiene los campos siguientes:

RIP Admin Mode (Modo de administración de RIP): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable. Si selecciona **Enable** (Activar), se activa RIP para el conmutador. El valor predeterminado es **Disable** (Desactivar).

Split Horizon Mode (Modo de horizonte dividido): seleccione **None** (Ninguno), **Simple** o **Poison Reverse** (Ruta inalcanzable) en el menú desplegable. El valor predeterminado es **Simple**. El horizonte dividido es una técnica utilizada para evitar problemas causados al incluir rutas en actualizaciones enviadas al enrutador del que se ha obtenido la ruta originalmente. Las opciones son:

- 1 **None** (Ninguno): no se realiza ningún procesamiento especial.
- 1 **Simple**: una ruta no está incluida en las actualizaciones enviadas al enrutador del que se ha obtenido.
- 1 **Poison Reverse** (Ruta inalcanzable): una ruta está incluida en las actualizaciones enviadas al enrutador del que se ha obtenido, pero la métrica está establecida en infinito.

Auto Summary Mode (Modo de resumen automático): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable. Si se selecciona **Enable** (Activar), los grupos de rutas adyacentes se resumen en entradas únicas a fin de reducir el número total de entradas. El valor predeterminado es **Enable** (Activar).

Host Routes Accept Mode (Modo de aceptación de rutas host): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable. Si se selecciona **Enable** (Activar), el enrutador acepta las rutas host. El valor predeterminado es **Enable** (Activar).

Global Route Changes (Cambios de ruta globales): muestra el número de cambios de ruta realizados en la base de datos de rutas IP mediante RIP. En este número no se incluye la actualización de la edad de una ruta.

Global Queries (Consultas globales): muestra el número de respuestas enviadas a consultas RIP desde otros sistemas.

Default Information Originate (Originar información predeterminada): permite activar (**Enable**) o desactivar (**Disable**) el anuncio de ruta predeterminada.

Default Metric (Métrica predeterminada): establece un valor predeterminado para la métrica de las rutas redistribuidas. Este campo muestra la métrica predeterminada si ya se ha definido una o aparece en blanco si no se ha configurado ninguna. Los valores válidos están comprendidos entre 1 y 15.

Configuración de RIP

1. Abra la página **RIP Configuration** (Configuración de RIP).
2. Introduzca datos en los campos según sea necesario.
3. Haga clic en **Apply Changes** (Aplicar cambios) cuando haya terminado.

Se configura RIP y se actualiza el dispositivo.

Configuración de RIP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

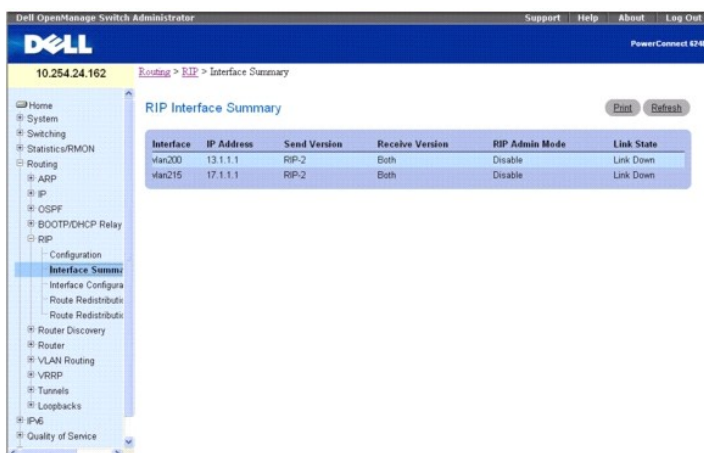
- 1 Comandos para el protocolo de información de enrutamiento (RIP)

Resumen de interfaces RIP

Utilice la página **RIP Interface Summary** (Resumen de interfaces RIP) para visualizar el estado de la configuración de RIP en una interfaz.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **RIP**→ **Interface Summary** (Resumen de interfaces) en la vista de árbol.

Ilustración 10-24. Resumen de interfaces RIP



Interface	IP Address	Send Version	Receive Version	RIP Admin Mode	Link State
Vlan200	13.1.1.1	RIP-2	Both	Disable	Link Down
Vlan215	17.1.1.1	RIP-2	Both	Disable	Link Down

La página **RIP Interface Summary** (Resumen de interfaces RIP) incluye los campos siguientes:

Interface (Interfaz): interfaz, como por ejemplo una VLAN habilitada para el enrutamiento, en la que se ha activado RIP.

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

Send Version (Versión de envío): especifica la versión de RIP a la que se ajustan los paquetes de control RIP enviados desde la interfaz. El valor predeterminado es RIP-2. Los valores posibles son:

- 1 **RIP-1**: se envían paquetes RIP versión 1 mediante difusión.
- 1 **RIP-1c**: modo de compatibilidad con RIP versión 1. Los paquetes con formato RIP versión 2 se transmiten mediante difusión.
- 1 **RIP-2**: se envían paquetes RIP versión 2 mediante multidifusión.
- 1 **None** (Ninguno): no se transmiten paquetes de control RIP.

Receive Version (Versión de recepción): especifica qué paquetes de control de versión de RIP se aceptan en la interfaz. El valor predeterminado es Both (Ambos). Los valores posibles son:

- 1 **RIP-1**: sólo se reciben los paquetes con formato RIP versión 1.
- 1 **RIP-2**: sólo se reciben los paquetes con formato RIP versión 2.
- 1 **Both** (Ambos): se reciben los paquetes con ambos formatos.
- 1 **None** (Ninguno): no se recibe ningún paquete de control RIP.

RIP Admin Mode (Modo de administración de RIP): especifica si RIP está activado o desactivado en la interfaz.

Link State (Estado de enlace): especifica si la interfaz RIP está conectada o desconectada.

Visualización del resumen de interfaces RIP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para el protocolo de información de enrutamiento (RIP)

Configuración de interfaz RIP

Utilice la página **RIP Interface Configuration** (Configuración de interfaz RIP) para activar y configurar RIP, o para desactivarlo, en una interfaz específica.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **RIP** → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 10-25. Configuración de interfaz RIP



La página **RIP Interface Configuration** (Configuración de interfaz RIP) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz cuyos datos desea configurar.

Send Version (Versión de envío): versión de RIP que el enrutador envía con sus actualizaciones de enrutamiento. El valor predeterminado es RIP-2. Los valores posibles son:

- 1 **RIP-1**: se envían paquetes con formato RIP versión 1 mediante difusión.
- 1 **RIP-1c**: modo de compatibilidad con RIP versión 1. Se envían paquetes con formato RIP versión 2 mediante difusión.
- 1 **RIP-2**: se envían paquetes RIP versión 2 mediante multidifusión.
- 1 **None** (Ninguno): no se envía ningún paquete de control RIP.

Receive Version (Versión de recepción): versión de RIP de las actualizaciones de enrutamiento que el enrutador debe aceptar. El valor predeterminado es Both (Ambos). Los valores posibles son:

- 1 **RIP-1**: sólo se aceptan los paquetes con formato RIP versión 1.
- 1 **RIP-2**: sólo se aceptan los paquetes con formato RIP versión 2.
- 1 **Both** (Ambos): se aceptan los paquetes con ambos formatos.
- 1 **None** (Ninguno): no se acepta ningún paquete de control RIP.

RIP Admin Mode (Modo de administración de RIP): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Antes de activar RIP versión 1 o versión 1c en una interfaz, primero debe activar el modo de difusión dirigida a la red en la interfaz correspondiente. El valor predeterminado es Disable (Desactivar).

Authentication Type (Tipo de autenticación): puede seleccionar un tipo de autenticación distinto de None (Ninguno) haciendo clic en el botón **Modify** (Modificar). Aparece una nueva pantalla, donde puede seleccionar el tipo de autenticación en el menú desplegable. Los valores posibles son:

- 1 **None** (Ninguno): estado inicial de la interfaz. Si selecciona esta opción en el menú desplegable de la segunda pantalla y hace clic en **Apply Changes** (Aplicar cambios), volverá a la primera pantalla y no se ejecutará ningún protocolo de autenticación.
- 1 **Simple**: si selecciona este valor, se le solicitará que introduzca una clave de autenticación. Esta clave se muestra explícitamente en la cabecera de RIP de todos los paquetes enviados en la red. Todos los enrutadores de la red deben configurarse con la misma clave.
- 1 **Encrypt** (Cifrar): si selecciona este valor, se le solicitará que introduzca una clave de autenticación y una ID de autenticación. Para el cifrado se utiliza el algoritmo MD5 Message-Digest. Todos los enrutadores de la red deben configurarse con la misma clave y la misma ID.

IP Address (Dirección IP): muestra la dirección IP de la interfaz del enrutador.

Link State (Estado de enlace): especifica si la interfaz RIP está conectada o desconectada.

Bad Packets Received (Paquetes erróneos recibidos): muestra el número de paquetes RIP no válidos o dañados. Este número no incluye las actualizaciones completas enviadas con nueva información.

Bad Routes Received (Rutas erróneas recibidas): muestra el número de rutas, en paquetes RIP válidos, que se han omitido por algún motivo, por ejemplo, el número de actualizaciones de RIP desencadenadas que se han enviado realmente en esta interfaz. Este número no incluye las actualizaciones completas enviadas con nueva información.

Updates Sent (Actualizaciones enviadas): muestra el número de actualizaciones de ruta enviadas.

Configuración de la interfaz RIP

1. Abra la página **RIP Interface Configuration** (Configuración de interfaz RIP).

2. Especifique la interfaz cuyos datos desea configurar.

3. Introduzca datos en los campos según sea necesario:

Send Version (Versión de envío): en el cuadro desplegable, seleccione **None** (Ninguno), **RIP-1**, **RIP-1c** o **RIP-2**.

Receive Version (Versión de recepción): en el cuadro desplegable, seleccione **None** (Ninguno), **RIP-1**, **RIP-2** o **Both** (Ambos).

RIP Admin Mode (Modo de administración de RIP): seleccione **Enable** (Activar) o **Disable** (Desactivar).

Authentication Type (Tipo de autenticación): haga clic en el botón **Modify** (Modificar) para configurar diferentes tipos de autenticación.

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

Se configura la interfaz RIP y se actualiza el dispositivo.

Selección de un método de autenticación

1. Abra la página **RIP Interface Configuration** (Configuración de interfaz RIP).

2. Especifique la interfaz para la que desea configurar el método de autenticación.

3. Haga clic en **Modify** (Modificar).

Se visualiza la página **Authentication Method** (Método de autenticación).

4. Especifique el tipo de autenticación (**None** [Ninguno], **Simple** o **Encrypt** [Cifrar]) en el menú desplegable.

5. Si especifica **Simple** o **Encrypt** (Cifrar) como tipo de autenticación, aparecen campos adicionales. Introduzca la clave de autenticación (si ha seleccionado **Simple** o **Encrypt** [Cifrar]) y la ID de clave de autenticación (si ha seleccionado **Encrypt** [Cifrar]).

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

7. Se actualizan el método de autenticación y el dispositivo.

Configuración de una interfaz RIP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

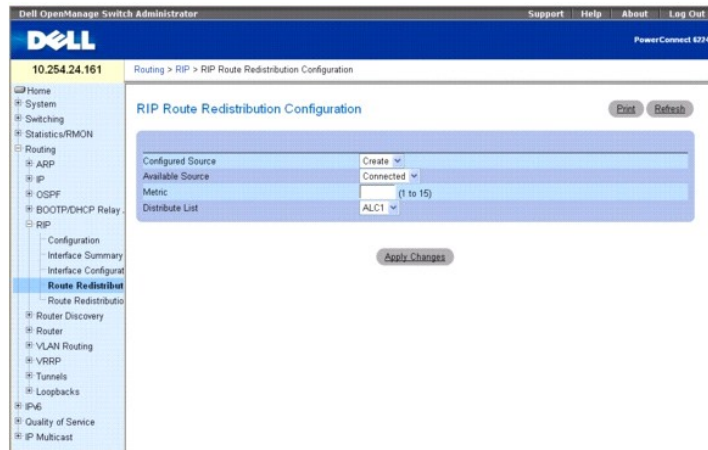
- 1 Comandos para el protocolo de información de enrutamiento (RIP)

Configuración de redistribución de rutas RIP

Utilice la página **RIP Route Redistribution Configuration** (Configuración de redistribución de rutas RIP) para configurar los parámetros de redistribución de rutas RIP. Los valores permitidos para cada campo se visualizan junto al campo. Si se introduce algún valor no válido, se visualiza un mensaje de alerta con la lista de todos los valores válidos.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **RIP** → **Route Redistribution Configuration** (Configuración de redistribución de rutas) en la vista de árbol.

Ilustración 10-26. Configuración de redistribución de rutas RIP



La página **RIP Route Redistribution Configuration** (Configuración de redistribución de rutas RIP) contiene los campos siguientes:

Configured Source (Origen configurado): esta casilla de selección es un selector dinámico que debería rellenarse únicamente con las rutas de origen que ya se han configurado para su redistribución mediante RIP. Create (Crear) permite configurar una ruta de origen disponible.

Available Source (Origen disponible): esta casilla de selección es un selector dinámico que debería rellenarse únicamente con las rutas de origen que no se han configurado previamente para su redistribución mediante RIP. Esta casilla de selección sólo aparece si se selecciona la opción Create (Crear) para Configured Source (Origen configurado). Los valores posibles son:

- 1 **Static** (Estático)
- 1 **Connected** (Conectado)
- 1 **OSPF**

Metric (Métrica): establece el valor de métrica que se utilizará como métrica de las rutas redistribuidas. Este campo muestra la métrica si se ha configurado previamente el origen, y puede modificarse. Los valores válidos son de 1 a 15.

Distribute List (Lista de distribución): esta casilla de selección establece la lista de acceso que filtra las rutas que van a redistribuirse mediante el protocolo de destino. Sólo se redistribuyen las rutas permitidas.

En el menú desplegable se enumeran las listas de control de acceso (ACL) configuradas desde las páginas **Switching** (Conmutación) → **Network Security** (Seguridad de la red) → **Access Control Lists** (Listas de control de acceso) → **IP Access Control Lists** (Listas de control de acceso IP). Cuando se utilizan para el filtrado de rutas, los únicos campos de una lista de acceso que se emplean son:

- 1 Dirección IP y máscara de red de origen
- 1 Dirección IP y máscara de red de destino
- 1 Acción (permitir o denegar)

Los demás campos (puerto de origen y de destino, precedencia, TOS, etc.) se omiten.

La dirección IP de origen se compara con la dirección IP de destino de la ruta. La máscara de red IP de origen de la regla de la lista de acceso se trata como máscara comodín, que indica qué bits de la dirección IP de origen deben coincidir con la dirección de destino de la ruta. Tenga en cuenta que un 1 en la máscara indica "Don't Care" (No importa) en el bit correspondiente de la dirección.

Cuando una regla de lista de acceso incluye una dirección IP y una máscara de red de destino (lista de acceso ampliada), la dirección IP de destino se compara con la máscara de red del destino de la ruta. La máscara de red de destino de la lista de acceso sirve de máscara comodín, que indica qué bits de la máscara de destino de la ruta son significativos para la operación de filtrado.

Creación de un origen configurado

1. Abra la página **RIP Route Redistribution Configuration** (Configuración de redistribución de rutas RIP).
2. Seleccione un origen disponible para configurar.
3. Especifique valores en los demás campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se configura el origen especificado y se actualiza el dispositivo.

Modificación de un origen configurado

1. Abra la página **RIP Route Redistribution Configuration** (Configuración de redistribución de rutas RIP).

2. Seleccione el origen configurado que desea modificar.
 3. Cambie los valores de esta pantalla según sea necesario.
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Se guardan los cambios especificados y se actualiza el dispositivo.

Configuración de redistribución de rutas RIP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para el protocolo de información de enrutamiento (RIP)

Resumen de redistribución de rutas RIP

Utilice la página **RIP Route Redistribution Summary** (Resumen de redistribución de rutas RIP) para visualizar las configuraciones de redistribución de rutas.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **RIP** → **Route Redistribution Summary** (Resumen de redistribución de rutas) en la vista de árbol.

Ilustración 10-27. Resumen de redistribución de rutas RIP

Source	Metric	Match	Distribute List
Connected	1	N.A.	5
Static	2	N.A.	16

La página **RIP Route Redistribution Summary** (Resumen de redistribución de rutas RIP) contiene los campos siguientes:

Source (Origen): ruta de origen que se redistribuirá mediante RIP.

Metric (Métrica): métrica de rutas redistribuidas para la ruta de origen especificada. Cuando no está configurada, se muestra Unconfigured (Sin configurar).

Match (Coincidencia): lista de rutas redistribuidas cuando se ha seleccionado OSPF como origen. Esta lista puede incluir uno o más de los elementos siguientes:

- 1 Internos
- 1 External 1 (Externa 1)
- 1 External 2 (Externa 1)
- 1 NSSA-External 1 (NSSA-Externa 1)
- 1 NSSA-External 2 (NSSA-Externa 1)
- 1 N.A. (No aplicable) (si no es OSPF)

Distribute List (Lista de distribución): lista de acceso que filtra las rutas que van a redistribuirse mediante el protocolo de destino. Si no se configura la lista de distribución, el campo aparece en blanco.

Visualización del resumen de redistribución de rutas RIP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para el protocolo de información de enrutamiento (RIP)

DetECCIÓN DE ENRUTADOR

El protocolo de detección de enrutador sirve a los hosts para identificar los enrutadores operativos en la subred. Los mensajes de detección de enrutador pueden ser de dos tipos: "anuncios de enrutador" y "solicitudes de enrutador". El protocolo exige que cada enrutador anuncie periódicamente las direcciones IP que tiene asociadas. Los hosts escuchan estos anuncios y detectan las direcciones IP de los enrutadores de vecino.

La página de menú **Router Discovery** (Detección de enrutador) contiene enlaces a páginas web que permiten configurar y visualizar los datos de detección de enrutador. Para visualizar este menú, haga clic en **Routing** (Enrutamiento)→ **Router Discovery** (Detección de enrutador) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

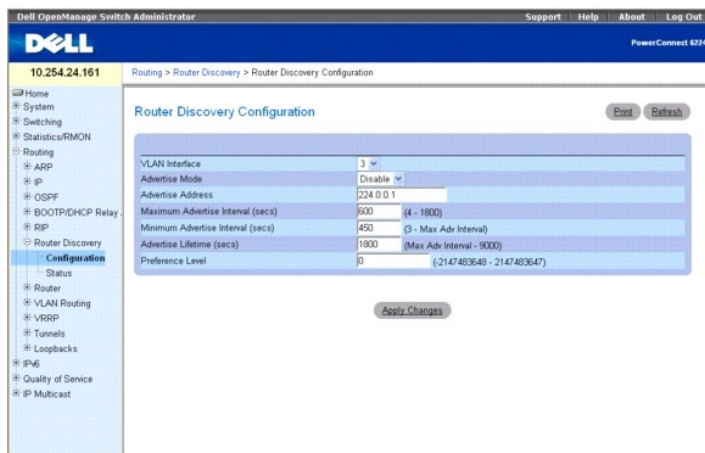
- 1 [Configuración de la detección de enrutador](#)
- 1 [Estado de la detección de enrutador](#)

Configuración de la detección de enrutador

Utilice la página **Router Discovery Configuration** (Configuración de la detección de enrutador) para introducir o cambiar parámetros de la detección de enrutador.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **Router Discovery** (Detección de enrutador)→ **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-28. Configuración de la detección de enrutador



La página **Router Discovery Configuration** (Configuración de la detección de enrutador) contiene los campos siguientes:

VLAN Interface (Interfaz de VLAN): seleccione la interfaz de enrutador cuyos datos desea configurar.

Advertise Mode (Modo de anuncio): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable. Si se selecciona **Enable** (Activar), los anuncios de enrutador se transmiten desde la interfaz seleccionada.

Advertise Address (Dirección de anuncio): introduzca la dirección IP que se utilizará para anunciar el enrutador.

Maximum Advertise Interval (secs) (Intervalo de anuncio máximo [seg.]): introduzca el tiempo máximo (en segundos) que puede transcurrir entre los anuncios de enrutador enviados desde la interfaz.

Minimum Advertise Interval (secs) (Intervalo de anuncio mínimo [seg.]): introduzca el tiempo mínimo (en segundos) que puede transcurrir entre los anuncios de enrutador enviados desde la interfaz.

Advertise Lifetime (secs) (Tiempo de vida de anuncio [seg.]): introduzca el valor (en segundos) que debe utilizarse como campo de tiempo de vida en los anuncios de enrutador enviados desde la interfaz. Se trata del tiempo máximo durante el que los hosts deben considerar las direcciones anunciadas como direcciones de enrutador válidas.

Preference Level (Nivel de preferencia): especifique el nivel de preferencia del enrutador como enrutador predeterminado en relación con otros enrutadores de la misma subred. Son preferibles las direcciones con números altos. Debe introducirse un número entero.

Configuración de la detección de enrutador

1. Abra la página **Router Discovery Configuration** (Configuración de la detección de enrutador).
2. Seleccione la interfaz de enrutador que desea configurar.
3. Configure los datos de los demás campos según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guardan los cambios de configuración especificados y se actualiza el dispositivo.

Configuración de la detección de enrutador mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

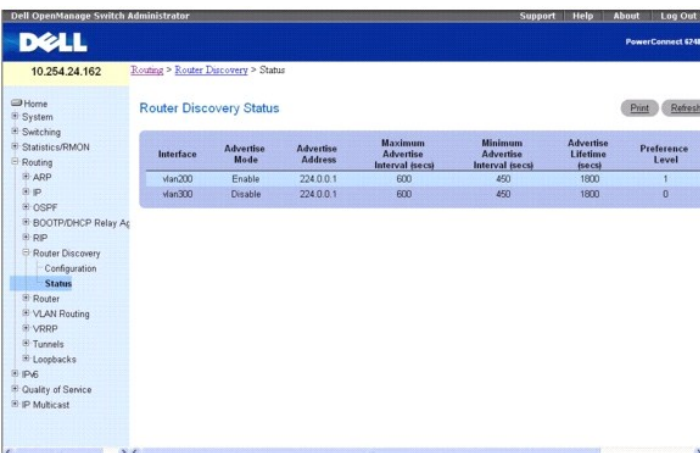
- 1 Comandos para el protocolo de detección de enrutador

Estado de la detección de enrutador

Utilice la página Router Discovery Status (Estado de la detección de enrutador) para visualizar datos de detección de enrutador de cada puerto.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **Router Discovery** (Detección de enrutador) → **Status** (Estado) en la vista de árbol.

Ilustración 10-29. Estado de la detección de enrutador



Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
vlan200	Enable	224.0.0.1	600	450	1800	1
vlan300	Disable	224.0.0.1	600	450	1800	0

La página Router Discovery Status (Estado de la detección de enrutador) incluye los campos siguientes:

Interface (Interfaz): interfaz de enrutador cuyos datos desea visualizar.

Advertise Mode (Modo de anuncio): los valores posibles son Enable (Activar) y Disable (Desactivar). Enable (Activar) indica que la detección de enrutador está activada en la interfaz.

Advertise Address (Dirección de anuncio): dirección IP utilizada para anunciar el enrutador.

Maximum Advertise Interval (secs) (Intervalo de anuncio máximo [seg.]): tiempo máximo (en segundos) que puede transcurrir entre los anuncios de enrutador enviados desde la interfaz.

Minimum Advertise Interval (secs) (Intervalo de anuncio mínimo [seg.]): tiempo mínimo (en segundos) que puede transcurrir entre los anuncios de enrutador enviados desde la interfaz.

Advertise Lifetime (secs) (Tiempo de vida de anuncio [seg.]): valor (en segundos) que debe utilizarse como campo de tiempo de vida en los anuncios de enrutador enviados desde la interfaz. Se trata del tiempo máximo durante el que los hosts deben considerar las direcciones anunciadas como direcciones de enrutador válidas.

Preference Level (Nivel de preferencia): nivel de preferencia del enrutador como enrutador predeterminado en relación con otros enrutadores de la misma subred. Son preferibles las direcciones con números altos.

Visualización del estado de la detección de enrutador mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para el protocolo de detección de enrutador

Enrutador

La página de menú **Router** (Enrutador) contiene enlaces a páginas web que permiten configurar y visualizar las tablas de rutas. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **Router** (Enrutador) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

- 1 [Tabla de rutas](#)

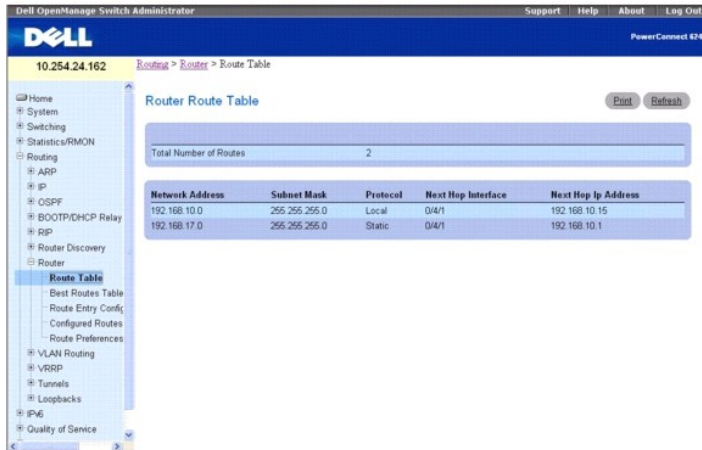
- 1 [Tabla de mejores rutas](#)
- 1 [Configuración de entradas de ruta](#)
- 1 [Rutas configuradas](#)
- 1 [Configuración de las preferencias de ruta](#)

Tabla de rutas

Utilice la página **Router Route Table** (Tabla de rutas de enrutador) para visualizar la configuración de la tabla de rutas.

Para visualizar la página, haga clic en **Routing** (Ενρυσμμεντο)→ **Router** (Ενρυσμτορ)→ **Route Table** (Ταβλα δε ρυσμς) en la vista de árbol.

Ilustración 10-30. Tabla de rutas de enrutador



La página **Router Route Table** (Tabla de rutas de enrutador) incluye los campos siguientes:

Total Number of Routes (Número total de rutas): número total de rutas contenidas en la tabla de rutas.

Network Address (Dirección de red): prefijo de ruta IP para el destino.

Subnet Mask (Máscara de subred): la máscara de subred, también conocida como máscara de subred/red, indica la parte de la dirección IP de la interfaz que identifica la red conectada.

Protocol (Protocolo): este campo indica qué protocolo ha creado la ruta especificada. Las posibilidades son una de las siguientes:

- 1 Local
- 1 **Static (Estático)**
- 1 Default (Predeterminado)
- 1 OSPF Intra (Intra-OSPF)
- 1 OSPF Inter (Inter-OSPF)
- 1 OSPF Type-1 (Tipo 1 OSPF)
- 1 OSPF Type-2 (Tipo 1 OSPF)
- 1 RIP

Next Hop Interface (Interfaz del siguiente salto): interfaz del enrutador de salida que se utilizará para reenviar tráfico al destino.

Next Hop IP Address (Dirección IP del siguiente salto): dirección IP del enrutador de salida que se utilizará para reenviar tráfico al siguiente enrutador (si lo hay) en la ruta de acceso al destino. El siguiente enrutador es siempre uno de los vecinos adyacentes o la dirección IP de la interfaz local de una red conectada directamente.

Visualización de la tabla de rutas de enrutador mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de enrutamiento IP

Tabla de mejores rutas

Utilice la página **Router Best Routes Table** (Tabla de mejores rutas de enrutador) para visualizar las mejores rutas de la tabla de enrutamiento.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **Router** (Enrutador)→ **Best Routes Table** (Tabla de mejores rutas) en la vista de árbol.

Ilustración 10-31. Tabla de mejores rutas de enrutador

Network Address	Subnet Mask	Protocol	Next Hop Interface	Next Hop Ip Address
13.1.1.0	255.255.255.0	Local	loopback1	13.1.1.1
17.1.1.0	255.255.255.0	Local	loopback2	17.1.1.1

La página **Router Best Routes Table** (Tabla de mejores rutas de enrutador) incluye los campos siguientes:

Total Number of Routes (Número total de rutas): número total de rutas contenidas en la tabla de rutas.

Network Address (Dirección de red): prefijo de ruta IP para el destino.

Subnet Mask (Máscara de subred): la máscara de subred, también conocida como máscara de subred/red, indica la parte de la dirección IP de la interfaz que identifica la red conectada.

Protocol (Protocolo): este campo indica qué protocolo ha creado la ruta especificada. Las posibilidades son una de las siguientes:

- 1 Local
- 1 Static (Estático)
- 1 Default (Predeterminado)
- 1 OSPF Intra (Intra-OSPF)
- 1 OSPF Inter (Inter-OSPF)
- 1 OSPF Type-1 (Tipo 1 OSPF)
- 1 OSPF Type-2 (Tipo 1 OSPF)
- 1 RIP

Next Hop Interface (Interfaz del siguiente salto): interfaz del enrutador de salida que se utilizará para reenviar tráfico al destino.

Next Hop IP Address (Dirección IP del siguiente salto): dirección IP del enrutador de salida que se utilizará para reenviar tráfico al siguiente enrutador (si lo hay) en la ruta de acceso al destino. El siguiente enrutador es siempre uno de los vecinos adyacentes o la dirección IP de la interfaz local de una red conectada directamente.

Visualización de la tabla de mejores rutas mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

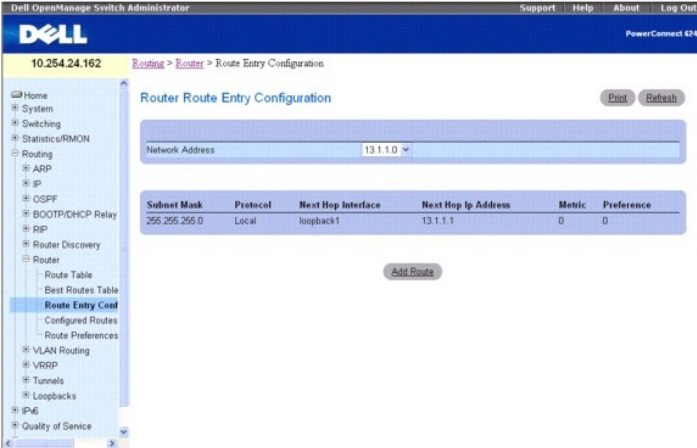
- 1 Comandos de enrutamiento IP

Configuración de entradas de ruta

Utilice la página **Router Route Entry Configuration** (Configuración de entradas de ruta de enrutador) para añadir rutas de enrutador o configurar rutas ya existentes.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **Router** (Enrutador)→ **Route Entry Configuration** (Configuración de entradas de ruta) en la vista de árbol.

Ilustración 10-32. Configuración de entradas de ruta de enrutador



La página **Router Route Entry Configuration** (Configuración de entradas de ruta de enrutador) contiene los campos siguientes:

Network Address (Dirección de red): seleccione en el menú desplegable el prefijo de ruta IP para el destino. Para crear una ruta, debe existir una interfaz de enrutamiento válida y la dirección IP del siguiente salto debe encontrarse en la misma red que la interfaz de enrutamiento. Las interfaces de enrutamiento se crean en la página **IP Interface Configuration** (Configuración de interfaz IP). Las direcciones IP del siguiente salto válidas pueden verse en la página **Route Table** (Tabla de rutas).

Subnet Mask (Máscara de subred): la máscara de subred, también conocida como máscara de subred/red, indica la parte de la dirección IP de la interfaz que identifica la red conectada.

Protocol (Protocolo): este campo indica qué protocolo ha creado la ruta especificada. Los valores posibles son:

- 1 Local
- 1 Static (Estático)
- 1 Default (Predeterminado)
- 1 OSPF Intra (Intra-OSPF)
- 1 OSPF Inter (Inter-OSPF)
- 1 OSPF Type-1 (Tipo 1 OSPF)
- 1 OSPF Type-2 (Tipo 1 OSPF)
- 1 RIP

Next Hop Interface (Interfaz del siguiente salto): interfaz del enrutador de salida que se utilizará para reenviar tráfico al destino.

Next Hop IP Address (Dirección IP del siguiente salto): dirección IP del enrutador de salida que se utilizará para reenviar tráfico al siguiente enrutador (si lo hay) en la ruta de acceso al destino. El siguiente enrutador es siempre uno de los vecinos adyacentes o la dirección IP de la interfaz local de una red conectada directamente. Al crear una ruta, la dirección IP del siguiente salto debe encontrarse en la misma red que la interfaz de enrutamiento. Las direcciones IP del siguiente salto válidas pueden verse en la página "Route Table" (Tabla de rutas).

Metric (Métrica): coste administrativo de la ruta de acceso al destino. Si no se introduce ningún valor, el valor predeterminado es 1. El intervalo es de 0 a 255. Este campo sólo aparece cuando se crea una ruta estática.

Preference (Preferencia): especifica un valor de preferencia para el siguiente salto configurado.

Adición de una ruta de enrutador

1. Abra la página **Router Route Entry Configuration** (Configuración de entradas de ruta de enrutador).
2. Haga clic en **Add Route** (Añadir ruta).

La pantalla se actualiza y la página **Router Route Entry Configuration** (Configuración de entradas de ruta de enrutador) contiene nuevos campos, como se muestra en la [ilustración 10-33](#).

Ilustración 10-33. Añadir ruta – Tipo de ruta predeterminada



3. Utilice el cuadro desplegable situado junto a **Route Type** (Tipo de ruta) para añadir una ruta **Default** (Predeterminada) o **Static** (Estática).

Si se selecciona Static (Estática), la página se actualiza y aparecen nuevos campos, como se muestra en la [ilustración 10-34](#).

Default (Predeterminada): introduzca la dirección de puerta de enlace predeterminada en el campo **Next Hop IP Address** (Dirección IP del siguiente salto).

Static (Estática): introduzca los valores para **Network Address** (Dirección de red), **Subnet Mask** (Máscara de subred), **Next Hop IP Address** (Dirección IP del siguiente salto) y **Preference** (Preferencia).

Ilustración 10-34. Configuración de entradas de ruta – Añadir tipo de ruta estática

Router Route Entry Configuration

Route Type	Static
Network Address	
Subnet Mask	
Next Hop IP Address	
Preference	1 (1 to 255)

Cancel Apply Changes

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

Se añade la nueva ruta y se le redirige a la página Configured Routes (Rutas configuradas).

Adición de una ruta de enrutador mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de enrutamiento IP

Rutas configuradas

Utilice la página **Configured Routes** (Rutas configuradas) para visualizar las rutas que se han configurado.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **Router** (Enrutador) → **Configured Routes** (Rutas configuradas) en la vista de árbol.

Ilustración 10-35. Rutas configuradas

Configured Routes

Network Address	Subnet Mask	Next Hop IP	Preference	Remove
10.1.1.0	255.255.255.0	3.1.1.2	1	<input type="checkbox"/>
10.1.2.0	255.255.255.0	3.1.1.2	1	<input type="checkbox"/>
10.1.3.0	255.255.255.0	3.1.1.2	1	<input type="checkbox"/>

Apply Changes

La página **Configured Routes** (Rutas configuradas) incluye los campos siguientes:

Network Address (Dirección de red): prefijo de ruta IP para el destino.

Subnet Mask (Máscara de subred): la máscara de subred, también conocida como máscara de subred/red, indica la parte de la dirección IP de la interfaz que identifica la red conectada.

Next Hop IP (IP del siguiente salto): interfaz del enrutador de salida que se utilizará para reenviar tráfico al destino.

Preference (Preferencia): muestra las preferencias configuradas para las rutas añadidas.

Remove (Eliminar): utilice esta casilla de verificación para eliminar una ruta configurada.

Adición de una ruta de enrutador

1. Abra la página **Configured Routes** (Rutas configuradas).
2. Haga clic en **Add** (Añadir).

Se visualiza la página **Router Route Entry Configuration** (Configuración de entradas de ruta de enrutador), como se muestra en la [ilustración 10-33](#).

3. Utilice el cuadro desplegable situado junto a **Route Type** (Tipo de ruta) para añadir una ruta **Default** (Predeterminada) o **Static** (Estática).

Default (Predeterminada): introduzca la dirección de puerta de enlace predeterminada en el campo **Next Hop IP Address** (Dirección IP del siguiente salto). En la [ilustración 10-33](#) se muestran los campos que aparecen cuando el valor de **Route Type** (Tipo de ruta) es **Default** (Predeterminada).

Static (Estática): introduzca los valores para **Network Address** (Dirección de red), **Subnet Mask** (Máscara de subred), **Next Hop IP Address** (Dirección IP del siguiente salto) y **Preference** (Preferencia). En la [ilustración 10-34](#) se muestran los campos que aparecen cuando el valor de **Route Type** (Tipo de ruta) es **Static** (Estática).

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

Se añade la nueva ruta y se le devuelve a la página **Configured Routes** (Rutas configuradas).

Visualización de las rutas configuradas mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de enrutamiento IP

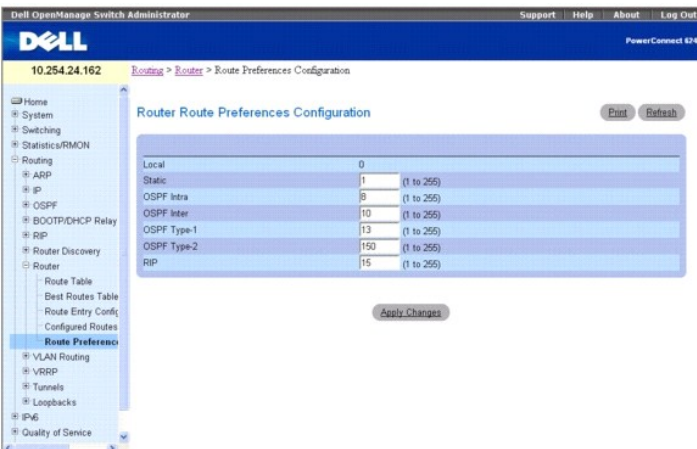
Configuración de las preferencias de ruta

Utilice la página **Router Route Preferences Configuration** (Configuración de las preferencias de ruta de enrutador) para configurar la preferencia predeterminada para cada protocolo (por ejemplo, 60 para las rutas estáticas). Se trata de valores arbitrarios comprendidos entre 1 y 255 que son independientes de la métrica de ruta. La mayoría de los protocolos de enrutamiento utilizan una métrica de ruta para determinar la ruta de acceso más corta, independiente de cualquier otro protocolo.

La mejor ruta a un destino se elige seleccionando la ruta con el valor de preferencia inferior. Cuando existen varias rutas a un destino, los valores de preferencia sirven para determinar la ruta preferida. Si aún así no se sabe cuál es la mejor, se elige la ruta con la mejor métrica. Para evitar problemas con métricas no coincidentes (por ejemplo, las métricas de RIP y OSPF no son directamente comparables), debe configurar valores de preferencia diferentes para cada protocolo.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **Router** (Enrutador) → **Route Preferences Configuration** (Configuración de las preferencias de ruta) en la vista de árbol.

Ilustración 10-36. Configuración de las preferencias de ruta de enrutador



La página **Router Route Preferences Configuration** (Configuración de las preferencias de ruta de enrutador) contiene los campos siguientes:

Local: este campo muestra el valor de preferencia de ruta local.

Static (Estática): valor de preferencia de la ruta estática del enrutador. El valor predeterminado es 1. El intervalo es de 1 a 255.

OSPF Intra (Intra-OSPF): valor de preferencia de la ruta intra-OSPF del enrutador. El valor predeterminado es 8. El intervalo es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que se asignen preferencias a las rutas obtenidas mediante OSPF en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPF Inter (Inter-OSPF): valor de preferencia de la ruta inter-OSPF del enrutador. El valor predeterminado es 10. El intervalo es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que se asignen preferencias a las rutas obtenidas mediante OSPF en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPF Type-1 (Tipo 1 OSPF): valor de preferencia de la ruta tipo 1 OSPF del enrutador. El valor predeterminado es 13. El intervalo es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que se asignen preferencias a las rutas obtenidas mediante OSPF en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPF Type-2 (Tipo 2 OSPF): valor de preferencia de la ruta tipo 2 OSPF del enrutador. El valor predeterminado es 150. El intervalo es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que se asignen preferencias a las rutas obtenidas mediante OSPF en el orden siguiente: intra < inter < tipo 1 < tipo 2.

RIP: valor de preferencia de la ruta RIP del enrutador. El valor predeterminado es 15. El intervalo es de 1 a 255.

Configuración de las preferencias de ruta

1. Abra la página **Route Preferences Configuration** (Configuración de las preferencias de ruta).
2. Defina los campos aplicables de esta página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se configuran las preferencias de ruta y se actualiza el dispositivo.

Configuración de las preferencias de ruta mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de OSPF

Enrutamiento de VLAN

Puede configurar el software de la serie 6200 con algunas VLAN que admitan el enrutamiento. También puede configurar el software para que permita tratar el tráfico de una VLAN como si la VLAN fuera un puerto de enrutador.

Cuando un puerto está activado para la formación de puentes (opción predeterminada) en lugar de para el enrutamiento, todo el procesamiento normal de puentes se lleva a cabo para un paquete de entrada, que luego se asocia a una VLAN. Su dirección MAC de destino (MAC DA) e ID de VLAN se utilizan para realizar una búsqueda en la tabla de direcciones MAC. Si el enrutamiento está activado para la VLAN y la dirección MAC de destino de un paquete de difusión única de entrada corresponde a la de la interfaz de enrutador de puente interno, se direcciona el paquete. Se reenvía un paquete de multidifusión de entrada a todos los puertos de la VLAN, además de a la interfaz de enrutador de puente interno, si se ha recibido en una VLAN direccionada.

Dado que es posible configurar un puerto para que pertenezca a más de una VLAN, puede activarse el enrutamiento de VLAN para todas las VLAN del puerto o para algunas de las VLAN de dicho puerto. El enrutamiento de VLAN puede utilizarse para permitir que más de un puerto físico resida en la misma subred. También puede utilizarse cuando una VLAN abarca varias redes físicas, o cuando se requiere seguridad o segmentación adicionales. En esta sección se muestra cómo configurar el software de la serie 6200 para que admita el enrutamiento de VLAN. Un puerto puede ser un puerto de VLAN o un puerto de enrutador, pero no ambas cosas. Sin embargo, un puerto de VLAN puede formar parte de una VLAN que es a su vez un puerto de enrutador.

La página de menú **VLAN Routing** (Enrutamiento de VLAN) contiene un enlace a una página web que permite visualizar los parámetros y datos del enrutamiento de VLAN. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **VLAN Routing** (Enrutamiento de VLAN) en la vista de árbol. A continuación figura la página web a la que se puede acceder desde esta página de menú:

- 1 [Resumen de enrutamiento de VLAN](#)

Resumen de enrutamiento de VLAN

Utilice la página **VLAN Routing Summary** (Resumen de enrutamiento de VLAN) para visualizar información sobre las interfaces de enrutamiento de VLAN configuradas en el sistema.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **VLAN Routing** (Enrutamiento de VLAN) → **Summary** (Resumen) en la vista de árbol.

Ilustración 10-37. Resumen de enrutamiento de VLAN

Dell OpenManage Switch Administrator

10.254.24.161 Routing > VLAN Routing > Summary

VLAN Routing Summary

VLANID	MAC Address	IP Address	Subnet Mask
200	00 FC E3 90 01 47	192.168.30.25	255.255.255.0
201	00 FC E3 90 01 47	10.10.10.50	255.255.255.0
300	00 FC E3 90 01 47	10.10.30.10	255.255.255.0

La página **VLAN Routing Summary** (Resumen de enrutamiento de VLAN) incluye los campos siguientes:

VLAN ID (ID de VLAN): ID de la VLAN cuyos datos se visualizan en la fila de la tabla actual.

MAC Address (Dirección MAC): dirección MAC asignada a la interfaz de enrutamiento de VLAN.

IP Address (Dirección IP): dirección IP configurada de la interfaz de enrutamiento de VLAN. Tenga en cuenta que si se crea una VLAN y no se configura la dirección IP, la página muestra de forma predeterminada la dirección IP 0.0.0.0. Para configurar la dirección IP, vaya a **IP→ Interface Configuration** (Configuración de interfaz).

Subnet Mask (Máscara de subred): máscara de subred configurada de la interfaz de enrutamiento de VLAN. Su valor es 0.0.0.0 cuando la interfaz de enrutamiento de VLAN se configura por primera vez y debe introducirse en la página IP Interface Configuration (Configuración de interfaz IP).

Visualización del resumen de enrutamiento de VLAN mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la *Guía de referencia de la CLI*:

- 1 Comandos de direccionamiento IP
- 1 Comandos de enrutamiento de LAN virtuales

VRRP

El protocolo de redundancia de enrutador virtual (VRRP) está diseñado para gestionar los errores del enrutador predeterminado gracias al esquema que proporciona para elegir de forma dinámica un enrutador de reserva. En un principio se creó sobre todo para minimizar los periodos de "agujero negro" debidos a un error en el enrutador de puerta de enlace predeterminado, en que se perdía todo el tráfico dirigido a éste hasta que se detectaba el error. Aunque el uso de una configuración estática de las rutas predeterminadas está muy extendido, un enfoque como éste es susceptible de experimentar un único punto de error cuando el enrutador predeterminado falla. VRRP aboga por el concepto de un "enrutador virtual" asociado a una o más direcciones IP que sirven de puertas de enlace predeterminadas. Si falla el enrutador VRRP que controla estas direcciones IP (conocido formalmente como "maestro"), un enrutador VRRP de reserva asume el grupo de direcciones IP y la función de reenvío predeterminada.

La página de menú **VRRP** contiene enlaces a páginas web que permiten configurar y visualizar parámetros y datos. Para visualizar esta página, haga clic en **Routing** (Enrutamiento)→ **VRRP** en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

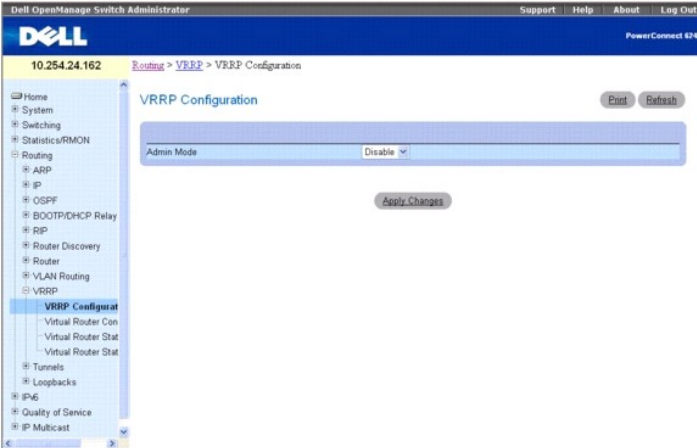
- 1 [Configuración de VRRP](#)
- 1 [Configuración de enrutador virtual](#)
- 1 [Estado del enrutador virtual](#)
- 1 [Estadísticas del enrutador virtual](#)

Configuración de VRRP

Utilice la página **VRRP Configuration** (Configuración de VRRP) para activar o desactivar el estado administrativo de un enrutador virtual.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **VRRP**→ **VRRP Configuration** (Configuración de VRRP) en la vista de árbol.

Ilustración 10-38. Configuración de VRRP



La página VRRP Configuration (Configuración de VRRP) contiene los campos siguientes:

Admin Mode (Modo de administración): establece el estado administrativo de VRRP en el enrutador como activo o inactivo. Seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. El valor predeterminado es Disable (Desactivar).

Cambio del estado de VRRP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

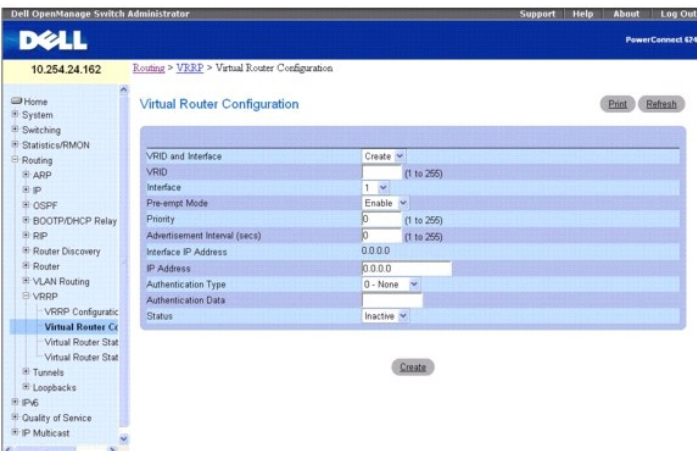
- 1 Comandos para el protocolo de redundancia de enrutador virtual

Configuración de enrutador virtual

Utilice la página Virtual Router Configuration (Configuración de enrutador virtual) para crear un nuevo enrutador virtual o para configurar uno existente.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **VRRP** → **Virtual Router Configuration** (Configuración de enrutador virtual) en la vista de árbol.

Ilustración 10-39. Configuración de enrutador virtual



La página Virtual Router Configuration (Configuración de enrutador virtual) contiene los campos siguientes:

VRID and Interface (VRID e interfaz): seleccione Create (Crear) en el menú desplegable para configurar un nuevo enrutador virtual, o seleccione uno de los enrutadores virtuales enumerados por número de interfaz e ID de enrutador virtual (VRID).

VRID: este campo sólo puede configurarse cuando se está creando un nuevo enrutador virtual, en cuyo caso se debe introducir una ID de enrutador virtual (VRID) comprendida entre 1 y 255.

Interface (Interfaz): este campo sólo puede configurarse cuando se está creando un nuevo enrutador virtual, en cuyo caso se debe seleccionar la interfaz del nuevo enrutador virtual en el menú desplegable.

Pre-empt Mode (Modo de anticipación): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si se selecciona Enable (Activar), un enrutador de reserva se adelanta al enrutador maestro si tiene una prioridad mayor que el enrutador virtual maestro, siempre que el maestro no sea el propietario de la dirección IP del enrutador virtual. El valor predeterminado es Enable (Activar).

Priority (Prioridad): introduzca el valor de prioridad que el enrutador VRRP utilizará para elegir el enrutador virtual maestro. Si la dirección IP virtual es la misma que la dirección IP de la interfaz, la prioridad se establecerá en 255 independientemente del valor que se introduzca. Si se introduce una prioridad de 255 cuando las direcciones IP virtual y de la interfaz no son iguales, la prioridad se establecerá en el valor predeterminado 100.

Advertisement Interval (secs) (Intervalo de anuncio [seg.]): introduzca el tiempo en segundos que debe transcurrir entre la transmisión de paquetes de anuncio mediante este enrutador virtual. Introduzca un número comprendido entre 1 y 255. El valor predeterminado es 1 segundo.

Interface IP Address (Dirección IP de interfaz): indica la dirección IP asociada a la interfaz seleccionada.

IP Address (Dirección IP): introduzca la dirección IP asociada al enrutador virtual. El valor predeterminado es 0.0.0.0, que debe cambiarse antes de seleccionar **Create** (Crear).

Authentication Type (Tipo de autenticación): seleccione en el menú desplegable el tipo de autenticación para el enrutador virtual. El valor predeterminado es None (Ninguno). Las opciones posibles son:

- 1 **0-None** (0-Ninguno): no se lleva a cabo ninguna autenticación.
- 1 **1-Simple**: se lleva a cabo una autenticación mediante una contraseña de texto.

Authentication Data (Datos de autenticación): si ha seleccionado la autenticación simple, introduzca la contraseña.

Status (Estado): seleccione Active (Activo) o Inactive (Inactivo) en el menú desplegable para iniciar o detener el funcionamiento del enrutador virtual. El valor predeterminado es Inactive (Inactivo).

Si desea configurar una dirección VRRP secundaria, configure primero una dirección IP (la dirección principal) para el enrutador virtual. A continuación, podrá añadir varias direcciones secundarias a la interfaz.

Creación de un nuevo enrutador virtual

1. Abra la página **Virtual Router Configuration** (Configuración de enrutador virtual).
2. Seleccione **Create** (Crear) en el menú desplegable VRID and Interface (VRID e interfaz).
3. Especifique la ID y la interfaz del nuevo enrutador virtual.
4. Defina los campos restantes según convenga.
5. Haga clic en **Create** (Crear).

Se guarda el nuevo enrutador virtual y se actualiza el dispositivo.

Configuración de un enrutador virtual

1. Abra la página **Virtual Router Configuration** (Configuración de enrutador virtual).
2. Seleccione la ID y la interfaz del enrutador virtual que desea configurar.
3. Modifique los campos según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración y se actualiza el dispositivo.

Configuración de un enrutador virtual mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para el protocolo de redundancia de enrutador virtual

Estado del enrutador virtual

Utilice la página **Virtual Router Status** (Estado del enrutador virtual) para visualizar el estado del enrutador virtual.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **VRRP** → **Virtual Router Status** (Estado del enrutador virtual) en la vista de árbol.

Ilustración 10-40. Estado del enrutador virtual

VRID	VLANID	Priority	Preempt Mode	Advertisement Interval (secs)	Virtual IP Address	Interface IP Address	Owner	VMAC Address
20	vlan200	4	Enable	1	10.50.50.50	192.168.30.15	False	00:00:5E:00:01:20
110	vlan300	80	Disable	30	10.50.50.52	0.0.0.0	False	00:00:5E:00:01:110

La página **Virtual Router Status** (Estado del enrutador virtual) incluye los campos siguientes:

VRID: identificador del enrutador virtual.

VLANID: indica la interfaz asociada a la ID de enrutador virtual (VRID).

Priority (Prioridad): valor de prioridad utilizado por el enrutador VRRP para elegir el enrutador virtual maestro.

Pre-empt Mode (Modo de anticipo)

- 1 **Enable (Activar):** cuando el enrutador virtual es un enrutador de reserva, éste se adelanta al enrutador maestro si tiene una prioridad mayor que el enrutador virtual maestro, siempre que el maestro no sea el propietario de la dirección IP del enrutador virtual.
- 1 **Disable (Desactivar):** si el enrutador virtual es un enrutador de reserva, no se adelanta al enrutador maestro aunque su prioridad sea mayor.

Advertisement Interval (secs) (Intervalo de anuncio [seg.]): tiempo en segundos que debe transcurrir entre la transmisión de paquetes de anuncio mediante este enrutador virtual.

Virtual IP Address (Dirección IP virtual): dirección IP asociada al enrutador virtual.

Interface IP Address (Dirección IP de interfaz): dirección IP asociada a la interfaz utilizada por el enrutador virtual.

Owner (Propietario): establezca este parámetro como True (Verdadero) si la dirección IP virtual y la dirección IP de la interfaz son la misma; de lo contrario, establézcalo como False (Falso). Si se establece el valor True (Verdadero), el enrutador virtual es el propietario de la dirección IP virtual y siempre se elige como enrutador maestro cuando está activo.

VMAC Address (Dirección MAC virtual): dirección MAC virtual asociada al enrutador virtual, compuesta por un identificador de 24 bits exclusivo desde el punto de vista organizativo, una constante de 16 bits que identifica el bloque de direcciones VRRP y una ID de enrutador virtual de 8 bits. La dirección MAC virtual es 00:00:5e:00:01:XX, donde XX es la VRID.

Auth Type (Tipo de autenticación): tipo de autenticación utilizado por el enrutador virtual.

- 1 **None (Ninguno):** especifica que no hay ningún tipo de autenticación.
- 1 **Simple:** especifica que el tipo de autenticación es una contraseña de texto simple.

State (Estado): estado actual del enrutador virtual:

- 1 **Initialize (Inicializado)**
- 1 **Master (Maestro)**
- 1 **Backup (Reserva)**

Status (Situación): situación actual del enrutador virtual:

- 1 **Inactive (Inactivo)**
- 1 **Active (Activo)**

Secondary IP Address (Dirección IP secundaria): dirección VRRP secundaria configurada para el VRRP principal.

Visualización del estado del enrutador virtual mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

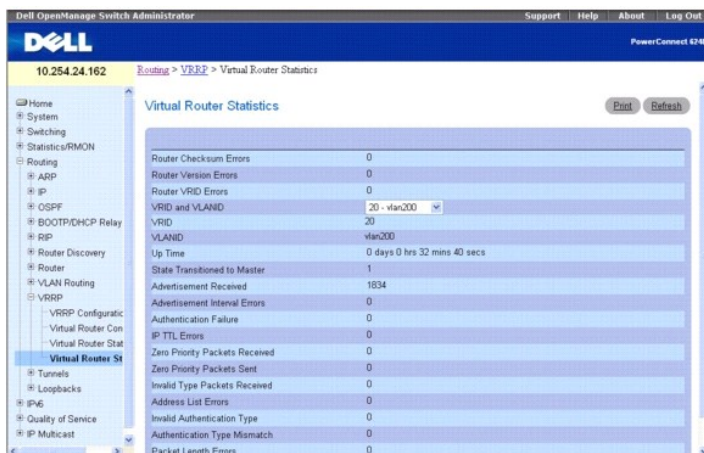
- 1 Comandos para el protocolo de redundancia de enrutador virtual

Estadísticas del enrutador virtual

Utilice la página **Virtual Router Statistics** (Estadísticas del enrutador virtual) para visualizar las estadísticas de un enrutador virtual especificado.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **VRRP**→ **Virtual Router Statistics** (Estadísticas del enrutador virtual) en la vista de árbol..

Ilustración 10-41. Estadísticas del enrutador virtual



Field	Value
Router Checksum Errors	0
Router Version Errors	0
Router VRID Errors	0
VRID and VLANID	20 - vlan200
VRID	20
VLANID	vlan200
Up Time	0 days 0 hrs 32 mins 40 secs
State Transitioned to Master	1
Advertisement Received	1834
Advertisement Interval Errors	0
Authentication Failure	0
IP TTL Errors	0
Zero Priority Packets Received	0
Zero Priority Packets Sent	0
Invalid Type Packets Received	0
Address List Errors	0
Invalid Authentication Type	0
Authentication Type Mismatch	0
Packet Length Errors	0

La página **Virtual Router Statistics** (Estadísticas del enrutador virtual) contiene los campos enumerados a continuación. Muchos de estos campos sólo se visualizan cuando hay una configuración de VRRP válida.

Router Checksum Errors (Errores de suma de comprobación del enrutador): número total de paquetes VRRP recibidos con un valor de suma de comprobación de VRRP no válido.

Router Version Errors (Errores de versión del enrutador): número total de paquetes VRRP recibidos con un número de versión desconocido o no admitido.

Router VRID Errors (Errores de VRID de enrutador): número total de paquetes VRRP recibidos con una VRID no válida para este enrutador virtual.

VRID and VLANID (VRID y VLANID): seleccione el enrutador virtual existente, enumerado por número de interfaz e ID de enrutador virtual, cuya información estadística desea visualizar.

VRID: ID del enrutador virtual seleccionado.

VLANID: interfaz del enrutador virtual seleccionado.

Up Time (Tiempo de actividad): tiempo (en días, horas, minutos y segundos) transcurrido desde que el enrutador virtual ha pasado al estado Initialize (Inicializado).

State Transitioned to Master (Estado pasado a maestro): número total de veces que este enrutador virtual ha pasado al estado Master (Maestro).

Advertisement Received (Anuncio recibido): número total de anuncios VRRP recibidos por este enrutador virtual.

Advertisement Interval Errors (Errores de intervalo de anuncio): número total de paquetes de anuncio VRRP recibidos cuyo intervalo de anuncio era diferente del configurado para el enrutador virtual local.

Authentication Failure (Error de autenticación): número total de paquetes VRRP recibidos que no han superado la comprobación de autenticación.

IP TTL Errors (Errores de TTL IP): número total de paquetes VRRP recibidos por el enrutador virtual con un tiempo de vida (TTL) IP diferente de 255.

Zero Priority Packets Received (Paquetes con prioridad cero recibidos): número total de paquetes VRRP recibidos por el enrutador virtual con una prioridad 0.

Zero Priority Packets Sent (Paquetes con prioridad cero enviados): número total de paquetes VRRP enviados por el enrutador virtual con una prioridad 0.

Invalid Type Packets Received (Paquetes con tipo no válido recibidos): número total de paquetes VRRP recibidos por el enrutador virtual con un valor no válido en el campo Type (Tipo).

Address List Errors (Errores de lista direcciones): número total de paquetes recibidos cuya lista de direcciones no coincide con la lista configurada localmente para el enrutador virtual.

Invalid Authentication Type (Tipo de autenticación no válido): número total de paquetes recibidos con un tipo de autenticación desconocido.

Authentication Type Mismatch (Discrepancia de tipo de autenticación): número total de paquetes recibidos con un tipo de autenticación diferente del método de autenticación configurado localmente.

Packet Length Errors (Errores de longitud de paquete): número total de paquetes recibidos con una longitud de paquete inferior a la del encabezado VRRP.

Visualización de las estadísticas del enrutador virtual

1. Abra la página **Virtual Router Statistics** (Estadísticas del enrutador virtual).

2. Seleccione el enrutador virtual cuya información estadística desea visualizar en el campo **VRID and VLANID** (VRID y VLANID). Esta información sólo se visualiza si existe una configuración de VRRP válida.

Visualización de las estadísticas del enrutador virtual mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para el protocolo de redundancia de enrutador virtual

Túneles

La serie 6200 admite la creación, la eliminación y la administración de interfaces de túnel. Se trata de interfaces dinámicas que se crean y eliminan mediante la configuración de usuario.

Existen dos clases de túneles que facilitan la transición de redes IPv4 a redes IPv6: túneles configurados y túneles automáticos. La distinción radica en que los túneles configurados se configuran explícitamente con un destino o punto final del túnel. Los túneles automáticos, en cambio, extraen el punto final del túnel a partir de la dirección de destino de los paquetes direccionados al túnel.

La serie 6200 admite túneles punto a punto. Las interfaces punto a punto admiten el enrutamiento basado únicamente en la interfaz (no es necesario especificar una dirección de salto siguiente explícita) y permiten la definición de interfaces no numeradas.

La página de menú **Tunnels** (Túneles) contiene enlaces a páginas web que permiten configurar y visualizar los parámetros y datos de túneles. Para visualizar esta página, haga clic en **Routing** (Enrutamiento)→ **Tunnels** (Túneles) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

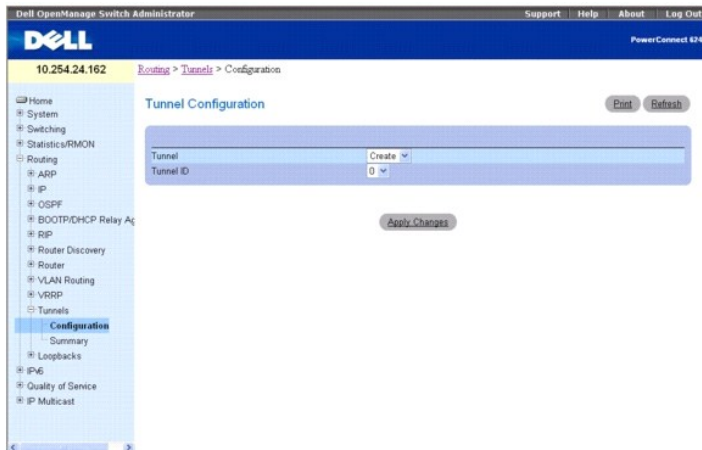
- 1 [Configuración de túneles](#)
- 1 [Resumen de túneles](#)

Configuración de túneles

Utilice la página **Tunnels Configuration** (Configuración de túneles) para crear, configurar o eliminar un túnel.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **Tunnels** (Túneles)→ **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-42. Configuración de túneles



La página **Tunnels Configuration** (Configuración de túneles) contiene los campos siguientes:

Tunnel (Túnel): utilice el menú desplegable para seleccionar una de las ID de túnel configuradas actualmente. Create (Crear) es también una opción válida si no se ha creado el número máximo de interfaces de túnel.

Tunnel ID (ID de túnel): cuando se selecciona Create (Crear) en el selector de túnel, se hace visible la lista de ID de túnel disponibles. Para que se visualicen los demás campos de la página, antes debe seleccionar una ID de túnel para asociarla al nuevo túnel y hacer clic en **Apply Changes** (Aplicar cambios).

Mode (Modo): selector del modo de túnel. IPv6-in-IPv4 (IPv6 en IPv4) es el único modo admitido.

Link Local Only Mode (Modo de sólo dirección local de enlace): active IPv6 en esta interfaz mediante la dirección local de enlace. Esta opción sólo puede configurarse antes de haber especificado una dirección IPv6 explícita.

IPv6 Address (Dirección IPv6): seleccione una dirección IPv6 para la interfaz de túnel seleccionada. Add (Añadir) es también una opción válida si no se ha configurado el número máximo de direcciones.

IPv6 Address (Dirección IPv6): cuando se selecciona Add (Añadir) en el selector de dirección IPv6, se hace visible este campo de entrada de dirección IPv6. La dirección debe introducirse con el formato prefijo/longitud.

También tiene la opción de especificar el identificador exclusivo ampliado de 64 bits (EUI-64).

Source (Origen): seleccione el origen, la dirección IPv4 o la interfaz que desee. Si selecciona Address (Dirección), debe introducir la dirección de origen para este túnel en notación decimal con punto. Si selecciona Interface (Interfaz), debe especificar la interfaz de origen para este túnel. La dirección asociada a la interfaz seleccionada se utiliza como dirección de origen.

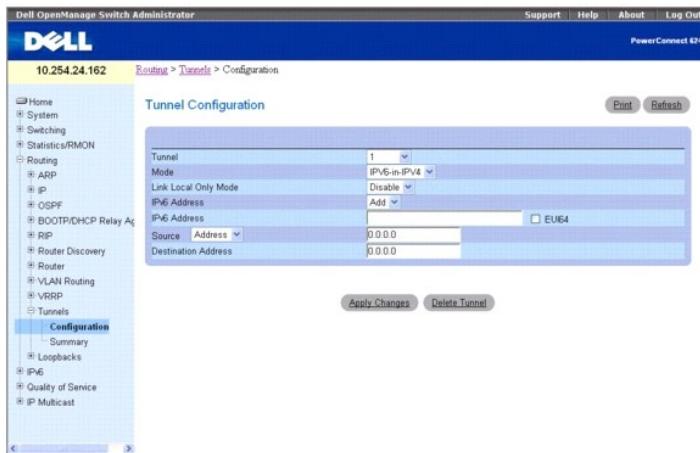
Destination Address (Dirección de destino): dirección de destino IPv4 para este túnel en notación decimal con punto.

Creación de un nuevo túnel

1. Abra la página **Tunnels Configuration** (Configuración de túneles).
2. Seleccione **Create** (Crear) en el menú desplegable **Tunnel** (Túnel).
3. Especifique una ID para utilizar en el campo **Tunnel ID** (ID de túnel).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El campo Tunnel ID (ID de túnel) desaparece y se visualizan los demás campos de túnel.

Ilustración 10-43. Configuración de túneles – Entrada



5. Configure los campos según convenga.
6. Introduzca los valores que desee en los demás campos.
7. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda el nuevo túnel y se actualiza el dispositivo.

Modificación de un túnel existente

1. Abra la página **Tunnels Configuration** (Configuración de túneles).
2. Especifique el túnel que desea modificar en el menú desplegable **Tunnel** (Túnel).
3. Cambie los valores de los demás campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la nueva configuración y se actualiza el dispositivo.

Eliminación de un túnel

1. Abra la página **Tunnels Configuration** (Configuración de túneles).

2. Especifique el túnel que desea eliminar en el menú desplegable **Tunnel** (Túnel).
3. Haga clic en **Delete Tunnel** (Eliminar túnel).

Se elimina el túnel y se actualiza el dispositivo.

Configuración de un túnel mediante los comandos de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

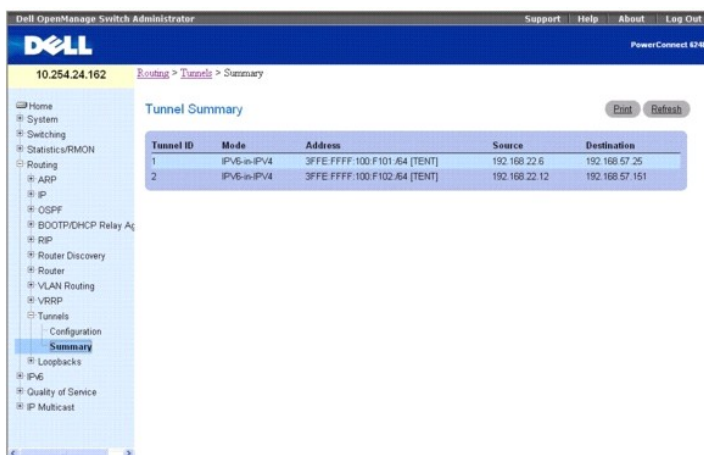
- 1 Comandos para la interfaz de túnel

Resumen de túneles

Utilice la página **Tunnels Summary** (Resumen de túneles) para visualizar un resumen de los túneles configurados.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **Tunnels** (Túneles) → **Summary** (Resumen) en la vista de árbol.

Ilustración 10-44. Resumen de túneles



Tunnel ID	Mode	Address	Source	Destination
1	IPv6-to-IPv4	3FFE.FFFF:100:F101:64 [TENT]	192.168.22.6	192.168.57.25
2	IPv6-to-IPv4	3FFE.FFFF:100:F102:64 [TENT]	192.168.22.12	192.168.57.151

La página **Tunnels Summary** (Resumen de túneles) contiene los campos siguientes:

Tunnel ID (ID de túnel): ID del túnel.

Mode (Modo): modo del túnel.

Address (Dirección): direcciones IPv6 del túnel.

Source (Origen): dirección de origen del túnel. En caso de que se haya configurado una interfaz, se visualizan tanto la interfaz como la dirección. Si la interfaz de origen no tiene ninguna dirección configurada, se visualiza el texto "unconfigured" (sin configurar) en lugar de la dirección.

Destination (Destino): dirección de destino del túnel.

Visualización del resumen de túneles mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para la interfaz de túnel

Bucles de retorno

La serie 6200 admite la creación, la eliminación y la administración de interfaces de bucle de retorno. Se trata de interfaces dinámicas que se crean y eliminan mediante la configuración de usuario. La serie 6200 admite varias interfaces de bucle de retorno.

Un interfaz de bucle de retorno debe estar siempre en funcionamiento. De este modo, ofrece un medio para configurar una dirección IP estable en el dispositivo a la que pueden hacer referencia otros conmutadores. Esta interfaz proporciona la dirección de origen de los paquetes enviados y puede recibir paquetes tanto locales como remotos. Se utiliza generalmente en los protocolos de enrutamiento.

El bucle de retorno no se comporta igual que el puerto de red en sistemas de conmutación. En particular, en una interfaz de bucle de retorno no hay vecinos. Se trata de un pseudodispositivo para asignar direcciones locales de manera que pueda establecerse comunicación con el enrutador a través de esta dirección, que siempre está en funcionamiento y puede recibir tráfico de cualquiera de las interfaces activas existentes. Por tanto, siempre que se pueda acceder desde un cliente remoto, la dirección del bucle de retorno puede utilizarse para comunicarse con el enrutador a través de distintos servicios, como

Telnet y SSH. Así, la dirección de un bucle de retorno se comporta de forma idéntica a cualquiera de las direcciones locales del enrutador en cuanto al procesamiento de paquetes entrantes.

La página de menú **Loopbacks** (Bucles de retorno) contiene enlaces a páginas web que permiten configurar y visualizar los parámetros y datos de los bucles de retorno. Para visualizar esta página, haga clic en **Routing** (Enrutamiento) → **Loopbacks** (Bucles de retorno) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

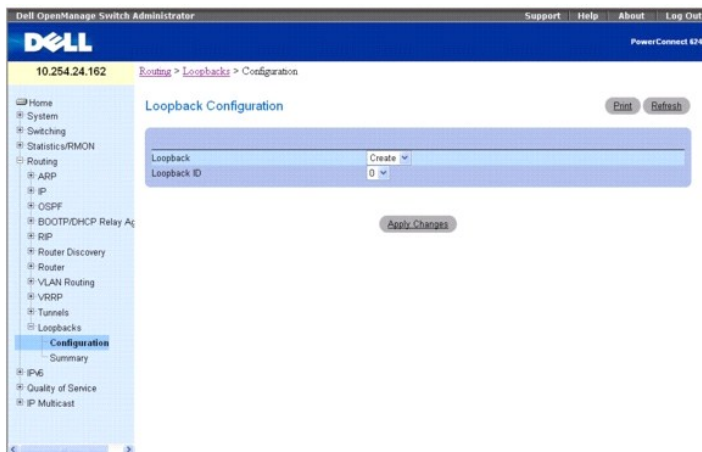
- 1 Configuración de bucles de retorno
- 1 Resumen de bucles de retorno

Configuración de bucles de retorno

Utilice la página **Loopbacks Configuration** (Configuración de bucles de retorno) para crear, configurar o eliminar interfaces de bucle de retorno. También puede configurar o eliminar una dirección secundaria para un bucle de retorno.

Para visualizar la página, haga clic en **Routing** (Enrutamiento) → **Loopbacks** (Bucles de retorno) → **Configuration** (Configuración) en la vista de árbol.

Ilustración 10-45. Configuración de bucles de retorno



Las páginas **Loopbacks Configuration** (Configuración de bucles de retorno) contienen los campos siguientes:

Loopback (Bucle de retorno): utilice el menú desplegable para seleccionar una de las interfaces de bucle de retorno configuradas actualmente. **Create** (Crear) es también una opción válida si no se ha creado el número máximo de interfaces de bucle de retorno.

Loopback ID (ID de bucle de retorno): cuando se selecciona **Create** (Crear) en el campo **Loopback** (Bucle de retorno), se visualiza la lista de ID de bucle de retorno.

Protocol (Protocolo): seleccione IPv4 o IPv6 para configurar los atributos correspondientes de la interfaz de bucle de retorno. El protocolo seleccionado afecta a los campos que se visualizan en esta página.

Link Local Only Mode (Modo de sólo dirección local de enlace): active IPv6 en esta interfaz mediante la dirección local de enlace. Esta opción sólo se visualiza cuando el protocolo especificado es IPv6 y sólo puede configurarse antes de haber especificado una dirección IPv6 explícita.

IPv6 Address (Dirección IPv6): realice una selección en la lista de direcciones IPv6 configuradas para la interfaz de bucle de retorno seleccionada. **Add** (Añadir) es también una opción válida si no se ha configurado el número máximo de direcciones. Esta opción sólo se visualiza cuando el protocolo especificado es IPv6.

IPv6 Address (Dirección IPv6): cuando se selecciona **Add** (Añadir) en el selector de dirección IPv6, se hace visible este campo de entrada de dirección IPv6. Introduzca la dirección con el formato prefijo/longitud. Esta opción sólo se visualiza cuando el protocolo especificado es IPv6.

EU164: también tiene la opción de especificar el identificador exclusivo ampliado de 64 bits (EUI-64). Esta opción sólo se visualiza cuando el protocolo especificado es IPv6.

IPv4 Address (Dirección IPv4): dirección IPv4 principal de esta interfaz en notación decimal con punto. Esta opción sólo se visualiza cuando el protocolo especificado es IPv4.

IPv4 Subnet Mask (Máscara de subred IPv4): máscara de subred IPv4 principal de esta interfaz en notación decimal con punto. Esta opción sólo se visualiza cuando el protocolo especificado es IPv4.

Los campos siguientes se visualizan cuando se ha configurado una dirección principal. Puede configurar varias direcciones secundarias.

Secondary Address (Dirección secundaria): seleccione en el menú desplegable una dirección IPv4 secundaria configurada para la interfaz de bucle de retorno seleccionada. Es posible introducir una nueva dirección en el campo **Secondary IP Address** (Dirección IP secundaria) seleccionando **Add Secondary IP Address** (Añadir dirección IP secundaria), si no se ha configurado el número máximo de direcciones secundarias. Para poder añadir una dirección secundaria, antes es preciso configurar una dirección principal.

Secondary IP Address (Dirección IP secundaria): dirección IP secundaria de esta interfaz en notación decimal con punto. Este campo de entrada sólo es visible cuando se selecciona **Add Secondary** (Añadir secundaria).

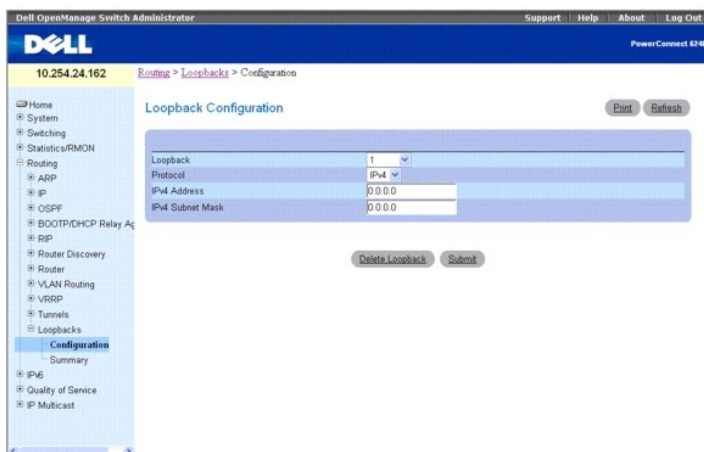
Secondary Subnet Mask (Máscara de subred secundaria): máscara de subred secundaria de esta interfaz en notación decimal con punto. Este campo de entrada sólo es visible cuando se selecciona **Add Secondary** (Añadir secundaria).

Creación de un nuevo bucle de retorno (IPv4)

1. Abra la página **Loopbacks Configuration** (Configuración de bucles de retorno).
2. Seleccione **Create** (Crear) en el menú desplegable **Loopback** (Bucle de retorno).
3. Especifique una ID para utilizar en el campo **Loopback ID** (ID de bucle de retorno).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El campo Loopack ID (ID de bucle de retorno) desaparece y se visualizan los demás campos de bucle de retorno.

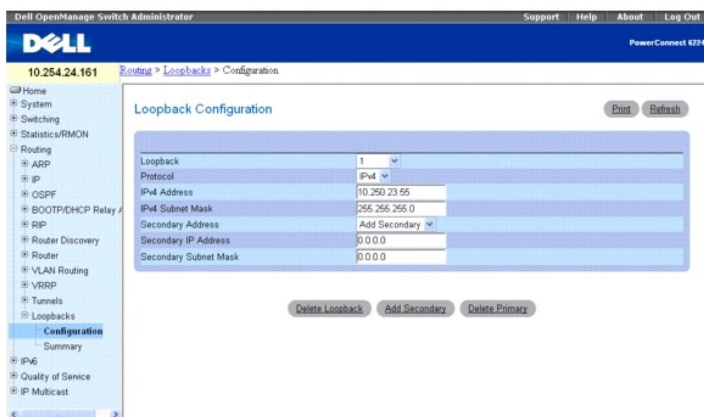
Ilustración 10-46. Configuración de bucles de retorno – Entrada de IPv4



5. Introduzca **IPv4** en el campo **Protocol** (Protocolo).
6. Introduzca los valores que desee en los demás campos.
7. Haga clic en **Submit** (Enviar).

Se guarda el nuevo bucle de retorno y reaparece la página web con los campos de configuración de direcciones secundarias.

Ilustración 10-47. Configuración de bucles de retorno – Añadir dirección secundaria



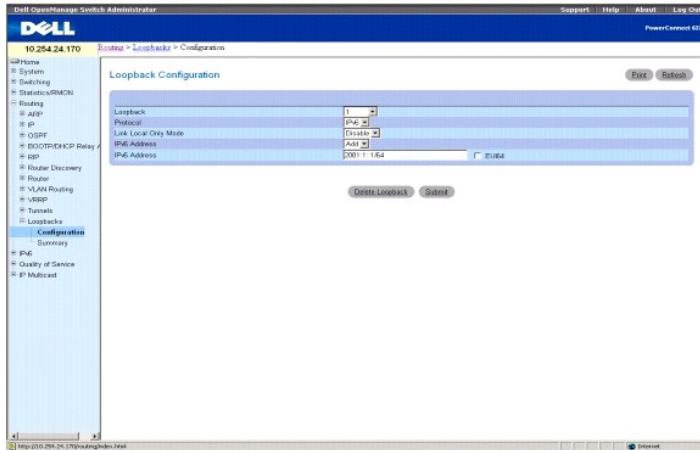
8. Rellene los campos **Secondary Address** (Dirección secundaria), **Secondary IP Address** (Dirección IP secundaria) y **Secondary Subnet Mask** (Máscara de subred secundaria).
9. Haga clic en el botón **Add Secondary** (Añadir secundaria). Se guarda la dirección secundaria y reaparece la página web con las direcciones de bucle de retorno principal y secundaria.

Creación de un nuevo bucle de retorno (IPv6)

1. Abra la página **Loopbacks Configuration** (Configuración de bucles de retorno).
2. Seleccione **Create** (Crear) en el menú desplegable **Loopback** (Bucle de retorno).
3. Especifique una ID para utilizar en el campo **Loopback ID** (ID de bucle de retorno).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El campo Loopack ID (ID de bucle de retorno) desaparece y se visualizan los demás campos de bucle de retorno.

Ilustración 10-48. Configuración de bucles de retorno – Entrada de IPv6



5. Seleccione **IPv6** en el cuadro desplegable del campo **Protocol** (Protocolo).
6. Añada la **dirección IPv6**.
7. Introduzca los valores que desee en los demás campos.
8. Haga clic en **Submit** (Enviar).

Se guarda el nuevo bucle de retorno y se actualiza el dispositivo.

Configuración de un bucle de retorno existente

1. Abra la página **Loopback Configuration** (Configuración de bucles de retorno).
2. Especifique el bucle de retorno que desea configurar en el menú desplegable **Loopback** (Bucle de retorno).
3. Cambie los valores de los demás campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la nueva configuración y se actualiza el dispositivo.

Eliminación de un bucle de retorno

1. Abra la página **Loopback Configuration** (Configuración de bucles de retorno).
2. Especifique el bucle de retorno que desea eliminar en el menú desplegable **Loopback** (Bucle de retorno).
3. Haga clic en **Delete Loopback** (Eliminar bucle de retorno).

Se elimina el bucle de retorno y se actualiza el dispositivo.

Eliminación de una dirección secundaria

1. Abra la página **Loopback Configuration** (Configuración de bucles de retorno).
2. Especifique el bucle de retorno que va a verse afectado.
3. Especifique la dirección secundaria que va a eliminarse.
4. Haga clic en **Delete Selected Secondary** (Eliminar secundaria seleccionada).

Se elimina la dirección secundaria y se actualiza el dispositivo.

Configuración de un bucle de retorno mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la *Guía de referencia de la CLI*:

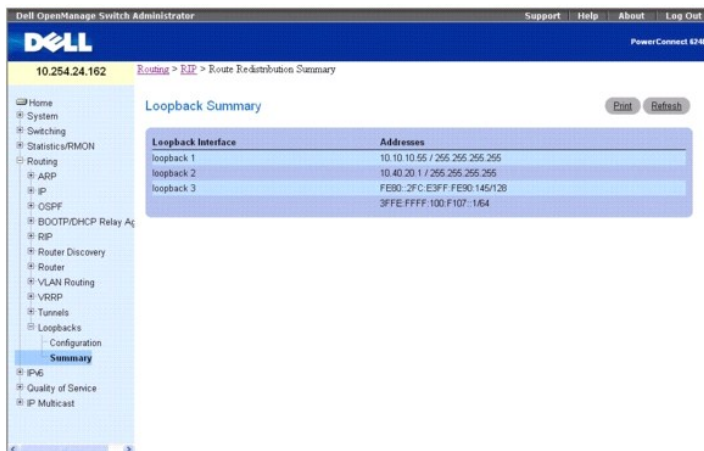
- 1 Comandos para la interfaz de bucle de retorno
- 1 Comandos de direccionamiento IP
- 1 Comandos de enrutamiento IPv6

Resumen de bucles de retorno

Utilice la página **Loopbacks Summary** (Resumen de bucles de retorno) para visualizar un resumen de los bucles de retorno configurados.

Para visualizar la página, haga clic en **Routing** (Enrutamiento)→ **Loopbacks** (Bucles de retorno)→ **Summary** (Resumen) en la vista de árbol.

Ilustración 10-49. Resumen de bucles de retorno



Loopback Interface	Addresses
loopback 1	10.10.10.55 / 255.255.255.255
loopback 2	10.40.20.1 / 255.255.255.255
loopback 3	FE80::2FC:E3FF:FE90:145/120 3FFE:FFFF:100:F107::164

La página **Loopbacks Summary** (Resumen de bucles de retorno) incluye los campos siguientes:

Loopback Interface (Interfaz de bucle de retorno): ID de la interfaz de bucle de retorno configurada.

Addresses (Direcciones): lista de las direcciones configuradas en la interfaz de bucle de retorno.

Visualización del resumen de bucles de retorno mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos para la interfaz de bucle de retorno

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de IPv6

Dell™ PowerConnect™ serie M6220 – Guía del usuario


- [Configuración global](#)
- [Configuración de interfaz](#)
- [Resumen de interfaces](#)
- [Estadísticas de IPv6](#)
- [Tabla de vecinos IPv6](#)
- [DHCPv6](#)
- [OSPFv3](#)
- [Rutas IPv6](#)

IPv6 es la última generación del Protocolo Internet. Con direcciones de 128 bits, frente a las direcciones de 32 bits de IPv4, IPv6 resuelve los problemas de disminución de direcciones observados con IPv4 y acaba con el requisito de traducción de direcciones de red (NAT), utilizado en redes IPv4 para reducir el número de direcciones IP únicas necesarias globalmente en una determinada red. Sus direcciones agregadas pueden disminuir considerablemente el tamaño de la tabla de enrutamiento global mediante combinaciones de direcciones muy conocidas. La seguridad está más integrada y la configuración de la red es más sencilla pero más flexible.

En la serie 6200, IPv6 e IPv4 coexisten. Al igual que ocurre con IPv4, el enrutamiento IPv6 se puede activar en interfaces de bucle de retorno y VLAN. Cada una de las interfaces de enrutamiento L3 se puede utilizar para IPv4, IPv6 o para ambos. Los protocolos IP que estén funcionando en L3 (por ejemplo, UDP y TCP) no experimentarán ningún cambio con IPv6. Por ese motivo, se emplea una única pila CPU para el transporte tanto de IPv4 como de IPv6, y una única interfaz de zócalos proporciona acceso a ambos. Los protocolos de enrutamiento pueden computar rutas correspondientes a una o a ambas versiones IP.

La página de menú IPv6 contiene enlaces a las funciones siguientes:

- 1 [Configuración global](#)
- 1 [Configuración de interfaz](#)
- 1 [Resumen de interfaces](#)
- 1 [Estadísticas de IPv6](#)
- 1 [Tabla de vecinos IPv6](#)
- 1 [DHCPv6](#)
- 1 [OSPFv3](#)
- 1 [Rutas IPv6](#)

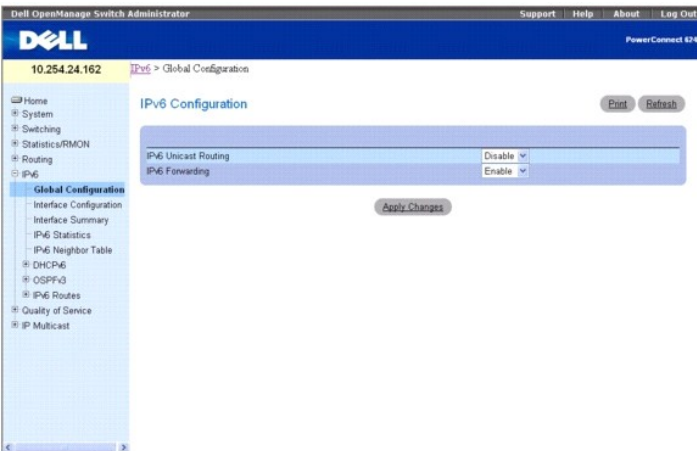
 **NOTA:** los comandos de la CLI no se encuentran disponibles para todas las páginas de IPv6.

Configuración global

Utilice la página Global Configuration (Configuración global) para activar el reenvío IPv6 en el enrutador y activar el reenvío de datagramas de difusión única IPv6.

Para visualizar la página, haga clic en IPv6 → Global Configuration (Configuración global) en la vista de árbol.

Ilustración 11-1. Configuración global de IPv6



La página IPv6 Global Configuration (Configuración global de IPv6) contiene los campos siguientes:

IPv6 Unicast Routing (Enrutamiento de difusión única IPv6): activa o desactiva de forma global el enrutamiento de difusión única IPv6 en el enrutador. El valor predeterminado es Disable (Desactivar).

IPv6 Forwarding (Reenvío IPv6): activa o desactiva el reenvío de tramas IPv6 en el enrutador. El valor predeterminado es Enable (Activar).

Configuración de los parámetros de IPv6

1. Abra la página IPv6 Global Configuration (Configuración global de IPv6).
2. Active o desactive el enrutamiento de difusión única en el menú desplegable.
3. Active o desactive el reenvío de tramas IPv6 en el menú desplegable.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración y se actualiza el dispositivo.

Configuración de IPv6 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de enrutamiento IPv6

Configuración de interfaz

Utilice la página **Interface Configuration** (Configuración de interfaz) para configurar los parámetros de la interfaz IPv6.

Para visualizar la página, haga clic en IPv6 → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 11-2. Configuración de interfaz IPv6

The screenshot shows the 'IPv6 Interface Configuration' page in the Dell OpenManage Switch Administrator. The interface includes a navigation tree on the left with options like Home, System, Switching, Statistics/RMON, Routing, and IPv6. The main area contains the following configuration fields:

Interface	vlan1
IPv6 Mode	Disable
IPv6 Prefix	Add <input type="checkbox"/> Delete <input type="checkbox"/>
IPv6 Prefix	<input type="text"/> <input type="checkbox"/> EUI64
Valid Lifetime by Prefix	0 (0 to 4294967296)
Preferred Lifetime by Prefix	0 (0 to 4294967296)
Onlink Flag by Prefix	Enable
Autonomous Flag by Prefix	Enable
Current State by Prefix	
Routing Mode	Disable
IPv6 Routing Operational Mode	
Interface Maximum Transmit Unit	0 (1280 to 1500) Enter 0 to unconfigure
Router Duplicate Address Detection Transmits	1 (0 to 600)
Router Advertisement NS Interval	0 (1000 to 4294967296) Enter 0 to unconfigure
Router Lifetime Interval	1800 (0 to 9000)
Router Advertisement Reachable Time	0 (0 to 3600000)
Router Advertisement Interval	600 (4 to 1800)
Router Advertisement Managed Config Flag	Disable
Router Advertisement Other Config Flag	Disable
Router Advertisement Suppress Flag	Disable

La página **IPv6 Interface Configuration** (Configuración de interfaz IPv6) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz que se va a configurar. Cuando se modifica la selección, se produce una actualización de la pantalla que hace que todos los campos se actualicen para el puerto que se acaba de seleccionar. Sólo se visualizan los túneles e interfaces activados para enrutamiento.

IPv6 Mode (Modo IPv6): cuando se activa el modo IPv6, la interfaz puede funcionar con este protocolo sin una dirección global. En este caso, se emplea una dirección local de enlace basada en EUI-64. Este selector enumera las dos opciones del modo IPv6: Enable (Activar) y Disable (Desactivar). El valor predeterminado es Disable (Desactivar).

IPv6 Prefix (Prefijo IPv6): puede seleccionar Add (Añadir) o Delete (Eliminar) un prefijo IPv6 en esta interfaz. Si se añade un prefijo, deberá especificarlo en el siguiente campo de prefijo IPv6. Al hacer clic en **Delete** (Eliminar), se elimina un prefijo IPv6 mostrado.

IPv6 Prefix (Prefijo IPv6): especifica el prefijo IPv6 con la longitud de prefijo correspondiente a una interfaz. Cuando se modifica la selección, se actualiza la pantalla y se actualiza el tiempo de vida válido, el tiempo de vida preferido, el indicador de enlace conectado y el indicador autónomo de la dirección IPv6 seleccionada.

EUI-64: si se marca, especifica un prefijo de difusión única de 64 bits.

Valid Lifetime by Prefix (Tiempo de vida válido por prefijo): valor, en segundos, que se debe colocar en el campo **Valid Lifetime** (Tiempo de vida válido) de la opción **Prefix Information** (Información de prefijo) en un anuncio de enrutador. El prefijo es válido para la determinación de enlace conectado de este periodo de tiempo. Los hosts que generan una dirección a partir de este prefijo mediante la configuración automática de direcciones sin estado pueden utilizar dichas direcciones para este periodo de tiempo. Una dirección configurada automáticamente con más antigüedad que el tiempo de vida preferido pero más reciente que el tiempo de vida válido se considera una "dirección no aprobada". Según la definición de RFC 2462, una dirección no aprobada es una "Dirección asignada a una interfaz cuyo uso se desaconseja, pero no se prohíbe. No se debe seguir utilizando una dirección no aprobada como dirección de origen en las nuevas comunicaciones, pero los paquetes que se envían desde o hacia direcciones no aprobadas se entregan según lo previsto. Una dirección no aprobada se puede seguir utilizando como dirección de origen en comunicaciones en las que cambiar a una dirección preferida dificulta una actividad determinada de nivel superior (por ejemplo, una conexión TCP existente)." El intervalo válido es de 0 a 4294967295 segundos.

Preferred Lifetime by Prefix (Tiempo de vida preferido por prefijo): valor, en segundos, que se debe colocar en el campo **Preferred Lifetime** (Tiempo de vida preferido) de la opción **Prefix Information** (Información de prefijo) en un anuncio de enrutador. Las direcciones generadas a partir de un prefijo mediante la configuración automática de direcciones sin estado siguen siendo "preferidas" para este periodo de tiempo. Según la definición de RFC 2462, una dirección preferida es una "Dirección asignada a una interfaz cuyo uso por protocolos de nivel superior es ilimitado. Las direcciones preferidas se pueden utilizar como la dirección de origen (o de destino) de los paquetes enviados desde (o hacia) la interfaz." El intervalo es de 0 a 4294967295 segundos.

Onlink Flag by Prefix (Indicador de enlace conectado por prefijo): especifica el prefijo seleccionado que puede utilizarse para la determinación de enlace conectado. El valor predeterminado es Enable (Activar). Este selector enumera las dos opciones del indicador de enlace conectado: Enable (Activar) y Disable (Desactivar).

Autonomous Flag by Prefix (Indicador autónomo por prefijo): especifica el prefijo seleccionado que puede utilizarse para la configuración de direcciones autónomas. El valor predeterminado es Disable (Desactivar). Este selector enumera las dos opciones del indicador autónomo: Enable (Activar) y Disable (Desactivar).

Current State by Prefix (Estado actual por prefijo): estado operativo de la interfaz correspondiente al prefijo IPv6 seleccionado.

Routing Mode (Modo de enrutamiento): especifica el modo de enrutamiento de una interfaz. Este selector enumera las dos opciones del modo de enrutamiento: Enable (Activar) y Disable (Desactivar). El valor predeterminado es Disable (Desactivar).

IPv6 Routing Operational Mode (Modo operativo de enrutamiento IPv6): especifica el estado operativo de una interfaz. El valor predeterminado es Disable (Desactivar).

Interface Maximum Transmit Unit (Unidad de transmisión máxima de interfaz): especifica la unidad de transmisión máxima de una interfaz. Si el valor es 0, esta interfaz no estará activada para el enrutamiento. Si el enrutamiento está activado, no se puede definir este valor como 0. El rango válido de MTU es de 1280 a 1500.

Router Duplicate Address Detection Transmits (Transmisiones de detección de direcciones duplicadas del enrutador): especifica el número de transmisiones de detección de direcciones duplicadas en una interfaz. Los valores de transmisiones DAD deben estar comprendidos entre 0 y 600.

Router Advertisement NS Interval (Intervalo NS de anuncio del enrutador): especifica el campo del tiempo de retransmisión del anuncio del enrutador enviado desde la interfaz. El valor 0 significa que no se ha especificado el intervalo de este enrutador. El rango del intervalo de solicitudes de vecino debe ser entre 1000 y 4294967295.

Router Lifetime Interval (Intervalo de tiempo de vida del enrutador): especifica el campo de tiempo de vida del anuncio del enrutador enviado desde la interfaz. Este valor debe ser superior o igual al intervalo de anuncio máximo. 0 significa que no se utilizará el enrutador como enrutador predeterminado. El rango del tiempo de vida del enrutador debe ser entre 0 y 9000.

Router Advertisement Reachable Time (Tiempo de anuncio de accesibilidad del enrutador): especifica el tiempo de anuncio del enrutador que debe transcurrir para considerar a un vecino accesible tras la confirmación de detección de vecinos (ND). El rango del tiempo de accesibilidad debe ser entre 0 y 3600000.

Router Advertisement Interval (Intervalo entre anuncios del enrutador): especifica el tiempo máximo permitido entre los envíos de anuncios del enrutador desde la interfaz. El valor predeterminado es 600. El rango del intervalo máximo entre anuncios es de 4 a 1800.

Router Advertisement Managed Config Flag (Indicador de configuración gestionada de anuncios del enrutador): especifica el indicador de configuración de direcciones gestionadas de anuncio del enrutador. Cuando tiene el valor verdadero, los nodos finales usan DHCPv6. Cuando tiene el valor falso, los nodos finales configuran automáticamente las direcciones. El valor predeterminado del indicador es Disable (Desactivar).

Router Advertisement Other Config Flag (Otro indicador de configuración de anuncio del enrutador): especifica otro indicador de configuración con estado de anuncio del enrutador. El valor predeterminado del otro indicador de configuración es Disable (Desactivar).

Router Advertisement Suppress Flag (Indicador de supresión de anuncio del enrutador): especifica la supresión de anuncios del enrutador en una interfaz. El valor predeterminado del indicador de supresión es Disable (Desactivar).

Configuración de interfaz IPv6

1. Abra la página **IPv6 Interface Configuration** (Configuración de interfaz IPv6).
2. Modifique los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guardan las modificaciones de la interfaz IPv6 y se actualiza el dispositivo.

Configuración de una interfaz IPv6 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de enrutamiento IPv6

Resumen de interfaces

Utilice la página **Interface Summary** (Resumen de interfaces) para visualizar la configuración de todas las interfaces IPv6.

Para visualizar la página, haga clic en **IPv6** → **Interface Summary** (Resumen de interfaces) en la vista de árbol.

Ilustración 11-3. Resumen de interfaces IPv6

Interface	Routing Mode	Admin Mode	Operational Mode	IPv6 Prefix/Prefix Length	State	IPv6 Address	State
1/g1	Disabled	Enabled	Disabled				
1/g2	Disabled	Enabled	Disabled				
1/g3	Disabled	Enabled	Disabled				
1/g4	Disabled	Enabled	Disabled				
1/g5	Disabled	Enabled	Disabled				
1/g6	Disabled	Enabled	Disabled				
1/g7	Disabled	Enabled	Disabled				
1/g8	Disabled	Enabled	Disabled				
1/g9	Disabled	Enabled	Disabled				
1/g10	Disabled	Enabled	Disabled				
1/g11	Disabled	Enabled	Disabled				
1/g12	Disabled	Enabled	Disabled				
1/g13	Disabled	Enabled	Disabled				
1/g14	Disabled	Enabled	Disabled				
1/g15	Disabled	Enabled	Disabled				
1/g16	Disabled	Enabled	Disabled				
1/g17	Disabled	Enabled	Disabled				
1/g18	Disabled	Enabled	Disabled				
1/g19	Disabled	Enabled	Disabled				
1/g20	Disabled	Enabled	Disabled				

La página **IPv6 Interface Summary** (Resumen de interfaces IPv6) contiene los campos siguientes:

Interface (Interfaz): especifica la interfaz cuya configuración se muestra en la fila actual de la tabla.

Routing Mode (Modo de enrutamiento): especifica el modo de enrutamiento de la interfaz.

Admin Mode (Modo de administración): especifica el modo de administración de la interfaz.

Operational Mode (Modo operativo): especifica el modo operativo de la interfaz.

IPv6 Prefix/PrefixLength (Prefijo/Longitud de prefijo IPv6): especifica las direcciones IPv6 configuradas en la interfaz.

State (Estado): especifica si la interfaz está activa o no.

Visualización del resumen de interfaces IPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de enrutamiento IPv6

Estadísticas de IPv6

Utilice la página **IPv6 Statistics** (Estadísticas de IPv6) para visualizar las estadísticas de tráfico de IPv6 de una interfaz o de todas ellas.

Para visualizar la página, haga clic en **IPv6** → **IPv6 Statistics** (Estadísticas de IPv6) en la vista de árbol.

Ilustración 11-4. Estadísticas de IPv6

Interface	Total Datagrams Received	Received Datagrams Locally Delivered	Received Datagrams Discarded Due To Header Errors	Received Datagrams Discarded Due To MTU	Received Datagrams Discarded Due To No Route	Received Datagrams With Unknown Protocol	Received Datagrams Discarded Due To Invalid Address	Received Datagrams Discarded Due To Truncated Data	Received Datagrams Discarded Other	Received Datagrams Reassembly Required	Datagrams Successfully Reassembled	Datagrams Failed To Reassemble	Datagrams Forwarded	Datagrams Locally Transmitted	Datagrams Transmit Failed
All	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

La página **IPv6 Statistics** (Estadísticas de IPv6) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz para la que se muestran las estadísticas. Cuando se modifica la selección, se produce una actualización de la pantalla que hace que todos los campos se actualicen para la interfaz que se acaba de seleccionar.

Estadísticas de IPv6

Total Datagrams Received (Total de datagramas recibidos): número total de datagramas de entrada recibidos por la interfaz, incluidos los recibidos con error.

Received Datagrams Locally Delivered (Datagramas recibidos entregados de forma local): número total de datagramas entregados correctamente a los protocolos de usuario IPv6, incluido el protocolo de mensajes de control de Internet (ICMP). Este recuento se incrementa en la interfaz a la que se dirigen dichos datagramas, que podría no ser necesariamente la interfaz de entrada de algunos de los datagramas.

Received Datagrams Discarded Due To Header Errors (Datagramas recibidos descartados por errores de cabecera): número de datagramas de entrada que se han descartado debido a errores en las cabeceras IPv6, como incoherencias en el número de versión, errores diversos de formato, superación del recuento de saltos, detección de errores en el momento de procesar sus opciones de IPv6, etc.

Received Datagrams Discarded Due To MTU (Datagramas recibidos descartados debido a MTU): número de datagramas de entrada que no pudieron reenviarse porque su tamaño superaba la unidad de transmisión máxima (MTU) de enlace de la interfaz de salida.

Received Datagrams Discarded Due To No Route (Datagramas recibidos descartados debido a falta de ruta): número de datagramas de entrada que fueron descartados porque no ha podido encontrarse una ruta para transmitirlos a su destino.

Received Datagrams With Unknown Protocol (Datagramas recibidos con protocolo desconocido): número de datagramas con dirección local recibidos correctamente pero descartados por corresponder a un protocolo desconocido o no compatible. Este recuento se incrementa en la interfaz a la que se dirigen dichos datagramas, que podría no ser necesariamente la interfaz de entrada de algunos de los datagramas.

Received Datagrams Discarded Due To Invalid Address (Datagramas recibidos descartados por tener una dirección no válida): número de datagramas de entrada que fueron descartados porque la dirección IPv6 que figuraba en el campo de destino de su cabecera IPv6 no era una dirección de recepción válida en esta entidad. Este recuento incluye direcciones no válidas (por ejemplo, ::0) y direcciones no compatibles (por ejemplo, direcciones con prefijos no asignados). En el caso de entidades que no sean enrutadores IPv6 y, por lo tanto, que no reenvían datagramas, este recuento incluye los datagramas que fueron descartados porque la dirección de destino no era una dirección local.

Received Datagrams Discarded Due To Truncated Data (Datagramas recibidos descartados por incluir datos truncados): número de datagramas de entrada que fueron descartados porque la trama del datagrama no incluía datos suficientes.

Received Datagrams Discarded Other (Otros datagramas recibidos descartados): número de datagramas IPv6 de entrada para los cuales no se ha detectado ningún problema que impidiera seguir procesándolos pero que se descartaron (por ejemplo, por falta de espacio en el búfer). Tenga en cuenta que este recuento no incluye ninguno de los datagramas descartados mientras estaban a la espera de ser reensamblados.

Received Datagrams Reassembly Required (Datagramas recibidos que requerían reensamblaje): número de fragmentos IPv6 recibidos que debían reensamblarse en esta interfaz. Observe que este recuento se incrementa en la interfaz a la que se dirigen dichos fragmentos, que podría no ser necesariamente la interfaz de entrada de algunos de los fragmentos.

Datagrams Successfully Reassembled (Datagramas reensamblados correctamente): número de datagramas IPv6 reensamblados correctamente. Observe que este recuento se incrementa en la interfaz a la que se dirigen dichos datagramas, que podría no ser necesariamente la interfaz de entrada de algunos de los fragmentos.

Datagrams Failed To Reassemble (Datagramas con errores de reensamblaje): número de errores detectados por el algoritmo de reensamblaje IPv6 (con independencia del motivo: tiempo de espera, errores, etc.). Tenga en cuenta que este recuento no refleja necesariamente los fragmentos IPv6 descartados, ya que algunos algoritmos (sobre todo el algoritmo de RFC 815) pueden perder la cuenta del número de fragmentos al combinarlos a medida que se reciben. Este recuento se incrementa en la interfaz a la que se dirigen estos fragmentos, que podría no ser necesariamente la interfaz de entrada de algunos de los fragmentos.

Datagrams Forwarded (Datagramas reenviados): número de datagramas de salida que esta entidad ha recibido y reenviado a sus destinos finales. En entidades que no actúan como enrutadores IPv6, este número incluye sólo los paquetes dirigidos originariamente a través de esta entidad y para los que el procesamiento de ruta de origen ha sido correcto. Tenga en cuenta que en el caso de un datagrama reenviado correctamente, se incrementa el recuento de la interfaz de salida.

Datagrams Locally Transmitted (Datagramas transmitidos de forma local): número de datagramas que ha transmitido correctamente esta entidad desde esta interfaz de salida.

Datagrams Transmit Failed (Datagramas transmitidos con fallos): número de datagramas que esta entidad no ha podido transmitir correctamente.

Datagrams Successfully Fragmented (Datagramas fragmentados correctamente): número de datagramas IPv6 que se han fragmentado correctamente en esta interfaz de salida.

Datagrams Failed To Fragment (Datagramas con fallos de fragmentación): número de datagramas de salida que no se han podido fragmentar en esta interfaz.

Datagrams Fragments Created (Fragmentos de datagramas creados): número de fragmentos de datagramas de salida que se han generado como resultado de la fragmentación realizada en esta interfaz de salida.

Multicast Datagrams Received (Datagramas de multidifusión recibidos): número de paquetes de multidifusión recibidos por la interfaz.

Multicast Datagrams Transmitted (Datagramas de multidifusión transmitidos): número de paquetes de multidifusión transmitidos por la interfaz.

Estadísticas de ICMPv6

Total ICMPv6 Messages Received (Total de mensajes ICMPv6 recibidos): número total de mensajes ICMP recibidos por la interfaz, incluidos todos los contados por ipv6IcmpInErrors. Tenga en cuenta que esta interfaz es la interfaz a la que se han dirigido los mensajes ICMP y que podría no ser necesariamente la interfaz de entrada de los mensajes.

ICMPv6 Messages With Errors Received (Mensajes ICMPv6 recibidos con error): número de mensajes ICMP que ha recibido la interfaz, que se determinó que tenían errores específicos de ICMP, como errores en la suma de comprobación ICMP, longitud inadecuada, etc.

ICMPv6 Destination Unreachable Messages Received (Mensajes ICMPv6 recibidos de destino inaccesible): número de mensajes ICMP de destino inaccesible recibidos por la interfaz.

ICMPv6 Messages Prohibited Administratively Received (Mensajes ICMPv6 recibidos prohibidos administrativamente): número de mensajes ICMP prohibidos administrativamente, de comunicación/destino inaccesible, recibidos por la interfaz.

ICMPv6 Time Exceeded Messages Received (Mensajes ICMPv6 recibidos de tiempo excedido): número de mensajes ICMP de tiempo excedido recibidos por la interfaz.

ICMPv6 Parameter Problem Messages Received (Mensajes ICMPv6 recibidos de problemas de parámetros): número de mensajes ICMP de problemas de

parámetros recibidos por la interfaz.

ICMPv6 Packet Too Big Messages Received (Mensajes ICMPv6 recibidos de paquetes demasiado grandes): número de mensajes ICMP de paquetes demasiado grandes recibidos por la interfaz.

ICMPv6 Echo Request Messages Received (Mensajes ICMPv6 recibidos de petición de eco): número de mensajes ICMP de petición de eco recibidos por la interfaz.

ICMPv6 Echo Reply Messages Received (Mensajes ICMPv6 recibidos de respuestas de eco): número de mensajes ICMP de respuestas de eco recibidos por la interfaz.

ICMPv6 Router Solicit Messages Received (Mensajes ICMPv6 recibidos de solicitudes del enrutador): número de mensajes ICMP de solicitudes del enrutador recibidos por la interfaz.

ICMPv6 Router Advertisement Messages Received (Mensajes ICMPv6 recibidos de anuncios del enrutador): número de mensajes ICMP de anuncios del enrutador recibidos por la interfaz.

ICMPv6 Neighbor Solicit Messages Received (Mensajes ICMPv6 recibidos de solicitudes de vecino): número de mensajes ICMP de solicitudes de vecino recibidos por la interfaz.

ICMPv6 Neighbor Advertisement Messages Received (Mensajes ICMPv6 recibidos de anuncios de vecino): número de mensajes ICMP de anuncios de vecino recibidos por la interfaz.

ICMPv6 Redirect Messages Received (Mensajes ICMPv6 recibidos de redirección): número de mensajes ICMPv6 de redirección recibidos por la interfaz.

ICMPv6 Group Membership Query Messages Received (Mensajes ICMPv6 recibidos de consultas de pertenencia a grupos): número de mensajes ICMPv6 de consultas de pertenencia a grupos recibidos por la interfaz.

ICMPv6 Group Membership Response Messages Received (Mensajes ICMPv6 recibidos de respuestas de pertenencia a grupos): número de mensajes ICMPv6 de respuestas de pertenencia a grupos recibidos por la interfaz.

ICMPv6 Group Membership Reduction Messages Received (Mensajes ICMPv6 recibidos de reducción de pertenencia a grupos): número de mensajes ICMPv6 de reducción de pertenencia a grupos recibidos por la interfaz.

Total ICMPv6 Messages Transmitted (Total de mensajes ICMPv6 transmitidos): número total de mensajes ICMP que ha intentado enviar esta interfaz. Tenga en cuenta que este recuento incluye todos los mensajes contabilizados en icmpOutErrors.

ICMPv6 Messages Not Transmitted Due To Error (Mensajes ICMPv6 no transmitidos debido a errores): número de mensajes ICMP que esta interfaz no ha enviado debido a problemas detectados en ICMP, como por ejemplo falta de búferes. Este valor no debe incluir los errores detectados fuera del nivel de ICMP, como por ejemplo la imposibilidad del IPv6 de direccionar el datagrama resultante. En algunas implementaciones puede que no haya ningún tipo de error que contribuya a incrementar este valor.

ICMPv6 Destination Unreachable Messages Transmitted (Mensajes ICMPv6 transmitidos de destino inaccesible): número de mensajes ICMP de destino inaccesible enviados por la interfaz.

ICMPv6 Messages Prohibited Administratively Transmitted (Mensajes ICMPv6 transmitidos prohibidos administrativamente): número de mensajes ICMP enviados prohibidos administrativamente, de comunicación/destino inaccesible.

ICMPv6 Time Exceeded Messages Transmitted (Mensajes ICMPv6 transmitidos de tiempo excedido): número de mensajes ICMP de tiempo excedido enviados por la interfaz.

ICMPv6 Parameter Problem Messages Transmitted (Mensajes ICMPv6 transmitidos de problemas de parámetros): número de mensajes ICMP de problemas de parámetros enviados por la interfaz.

ICMPv6 Packet Too Big Messages Transmitted (Mensajes ICMPv6 transmitidos de paquetes demasiado grandes): número de mensajes ICMP de paquetes demasiado grandes enviados por la interfaz.

ICMPv6 Echo Request Messages Transmitted (Mensajes ICMPv6 transmitidos de petición de eco): número de mensajes ICMP de petición de eco enviados por la interfaz.

ICMPv6 Echo Reply Messages Transmitted (Mensajes ICMPv6 transmitidos de respuestas de eco): número de mensajes ICMP de respuestas de eco enviados por la interfaz.

ICMPv6 Router Solicit Messages Transmitted (Mensajes ICMPv6 transmitidos de solicitudes del enrutador): número de mensajes ICMP de solicitudes de enrutador enviados por la interfaz.

ICMPv6 Router Advertisement Messages Transmitted (Mensajes ICMPv6 transmitidos de anuncios del enrutador): número de mensajes ICMP de anuncios del enrutador enviados por la interfaz.

ICMPv6 Neighbor Solicit Messages Transmitted (Mensajes ICMPv6 transmitidos de solicitudes de vecino): número de mensajes ICMP de solicitudes de vecino enviados por la interfaz.

ICMPv6 Neighbor Advertisement Messages Transmitted (Mensajes ICMPv6 transmitidos de anuncios de vecino): número de mensajes ICMP de anuncios de vecino enviados por la interfaz.

ICMPv6 Redirect Messages Transmitted (Mensajes ICMPv6 transmitidos de redirección): número de mensajes de redirección enviados.

ICMPv6 Group Membership Query Messages Transmitted (Mensajes ICMPv6 transmitidos de consultas de pertenencia a grupos): número de mensajes ICMPv6 enviados de consultas de pertenencia a grupos.

ICMPv6 Group Membership Response Messages Transmitted (Mensajes ICMPv6 transmitidos de respuestas de pertenencia a grupos): número de mensajes ICMPv6 enviados de respuestas de pertenencia a grupos.

ICMPv6 Group Membership Reduction Messages Transmitted (Mensajes ICMPv6 transmitidos de reducción de pertenencia a grupos): número de mensajes ICMPv6 enviados de reducción de pertenencia a grupos.

ICMPv6 Duplicate Address Detects (Detecciones de dirección duplicada ICMPv6): número de direcciones duplicadas detectado por la interfaz.

Visualización de las estadísticas de IPv6

1. Abra la página IPv6 Statistics (Estadísticas de IPv6).
2. Seleccione la interfaz que se va a visualizar en el menú desplegable **Interface** (Interfaz).

Aparecen las estadísticas de la interfaz seleccionada.

Visualización de las estadísticas de IPv6 e ICMPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

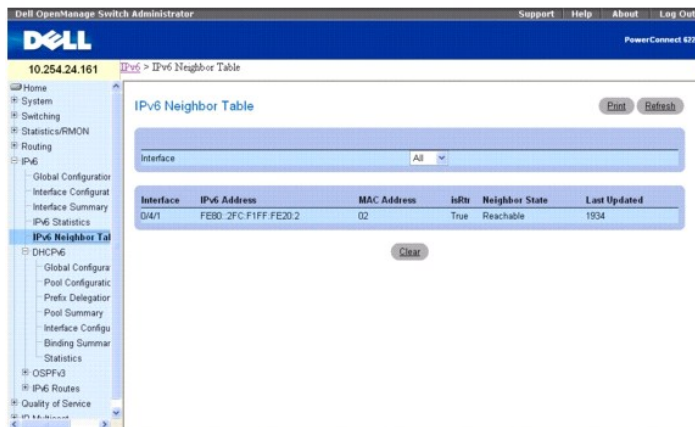
- 1 Comandos de enrutamiento IPv6

Tabla de vecinos IPv6

Utilice la página **IPv6 Neighbor Table** (Tabla de vecinos IPv6) para visualizar los datos de vecinos IPv6 correspondientes a una interfaz especificada.

Para visualizar la página, haga clic en **IPv6** → **IPv6 Neighbor Table** (Tabla de vecinos IPv6) en la vista de árbol.

Ilustración 11-5. Tabla de vecinos IPv6



La página **IPv6 Neighbor Table** (Tabla de vecinos IPv6) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz cuya información de estado de los vecinos se muestra.

Interface (Interfaz): especifica la interfaz cuya configuración se muestra en la fila actual de la tabla.

IPv6 Address (Dirección IPv6): especifica la dirección IPv6 de un vecino o una interfaz.

MAC Address (Dirección MAC): especifica la dirección MAC asociada a una interfaz.

IsRtr: indica si el vecino es un enrutador. Si el vecino es un enrutador, el valor será TRUE (verdadero). Si el vecino no es un enrutador, el valor será FALSE (falso).

Neighbor State (Estado de vecino): especifica el estado de la entrada de caché del vecino. A continuación, se muestran los estados de las entradas dinámicas en la caché de detección de vecinos IPv6:

- 1 **Incmp**: se está realizando una resolución de direcciones en la entrada. Se ha enviado un mensaje de solicitud de vecino a la dirección de multidifusión del nodo solicitado del destino, pero el mensaje de anuncio de vecino correspondiente aún no se ha recibido.
- 1 **Reachable** (Accesible): en los últimos milisegundos del tiempo de accesibilidad, se ha recibido una confirmación afirmativa de que la ruta de reenvío al vecino funcionaba correctamente. En el estado REACH (accesible), el dispositivo no realiza ninguna acción especial cuando se envían paquetes.
- 1 **Stale** (Obsoleto): se han superado los milisegundos del tiempo de accesibilidad desde la recepción de la última confirmación afirmativa que indicaba que la ruta de reenvío funcionaba correctamente. En el estado STALE (obsoleto), el dispositivo no realiza ninguna acción hasta que se envía un paquete.
- 1 **Delay** (Demora): se han superado los milisegundos del tiempo de accesibilidad desde la recepción de la última confirmación afirmativa que indicaba que la ruta de reenvío funcionaba correctamente. Se ha enviado un paquete en los últimos segundos de DELAY_FIRST_PROBE_TIME. Si no se recibe confirmación de accesibilidad durante los segundos especificados en DELAY_FIRST_PROBE_TIME tras entrar en el estado DELAY, envíe un mensaje de solicitud de vecino y cambie el estado por PROBE.
- 1 **Probe** (Sondear): se busca activamente una confirmación de accesibilidad reenviando mensajes de solicitud de vecino cada número de milisegundos especificados en el temporizador de retransmisión hasta que se recibe una confirmación de accesibilidad.

Last Updated (Última actualización): tiempo transcurrido desde que se confirmó que la dirección era accesible.

Visualización de la tabla de vecinos IPv6

1. Abra la página **IPv6 Neighbor Table** (Tabla de vecinos IPv6).
2. Seleccione la interfaz que se va a visualizar en el menú desplegable **Interface** (Interfaz).

Se muestran los datos de vecinos de la interfaz seleccionada.

Visualización de la tabla de vecinos IPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de enrutamiento IPv6

DHCPv6

DHCP se emplea generalmente entre clientes (por ejemplo, hosts) y servidores (por ejemplo, enrutadores) para asignar direcciones IP, puertas de enlace y otras definiciones de conexión en red, como por ejemplo parámetros de DNS, NTP o SIP (Protocolo de inicio de sesión). Sin embargo, IPv6 ofrece originalmente una configuración automática de las direcciones IP a través del protocolo de detección de vecinos (NDP) IPv6 y el uso de mensajes de anuncio del enrutador. Por lo tanto, la función de DHCPv6 dentro de la red es diferente de la del DHCPv4, ya que resulta menos fiable para la asignación de direcciones IP.

Hay una serie de opciones DHCP normalmente admitidas por DHCPv4 que también debe admitir DHCPv6, pero que deben configurarse.

NOTA: la más importante es la opción del servidor DNS configurada en la página web **IPv6→DHCPv6→Pool Configuration** (Configuración de conjunto).

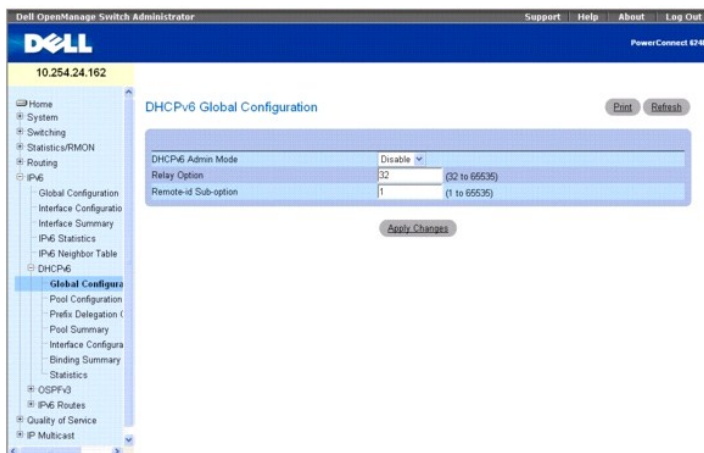
La página de menú **DHCPv6** contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de DHCPv6. Para visualizar esta página, haga clic en **IPv6→DHCPv6** en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

- 1 [Configuración global de DHCPv6](#)
- 1 [Configuración de conjunto DHCPv6](#)
- 1 [Configuración de delegación de prefijo](#)
- 1 [Resumen de conjuntos DHCPv6](#)
- 1 [Configuración de interfaz DHCPv6](#)
- 1 [Resumen de vinculaciones de servidor DHCPv6](#)
- 1 [Estadísticas de DHCPv6](#)

Configuración global de DHCPv6

Utilice la página **DHCPv6 Global Configuration** (Configuración global de DHCPv6) para configurar los parámetros globales de DHCPv6. Para visualizar la página, haga clic en **IPv6→DHCPv6→Global Configuration** (Configuración global) en la vista de árbol.

Ilustración 11-6. Configuración global de DHCPv6



La página **DHCPv6 Global Configuration** (Configuración global de DHCPv6) contiene los campos siguientes:

DHCPv6 Admin Mode (Modo de administración de DHCPv6): especifica el funcionamiento de DHCPv6 en el conmutador. Los valores posibles son Enable (Activar) y Disable (Desactivar). El valor predeterminado es Disable (Desactivar).

Relay Option (Opción de relé): especifica el valor de la opción de información del agente de relé. Se permiten los valores comprendidos entre 32 y 65535 y representan el valor intercambiado entre el agente de relé y el servidor. Cada valor posee un significado diferente (del 1 al 39 están estandarizados). El valor predeterminado, 32, significa OPTION_INFORMATION_REFRESH_TIME (tiempo de actualización de información de la opción).

Remote-id Sub-option (Subopción de ID remota): le permite especificar un número para representar el tipo de la subopción de ID remota de la opción de información del agente de relé. Se permiten los valores comprendidos entre 1 y 65535. El valor predeterminado es 1.

Configuración de los parámetros globales de DHCPv6

1. Abra la página **DHCPv6 Global Configuration** (Configuración global de DHCPv6).
2. Modifique los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guardan las modificaciones de los parámetros DHCPv6 y se actualiza el dispositivo.

Configuración de los parámetros globales de DHCPv6 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos DHCPv6

Configuración de conjunto DHCPv6

Los clientes DHCP para IPv6 se conectan a un servidor que está configurado para utilizar parámetros de un conjunto definido por el usuario. El conjunto se identifica con un nombre de conjunto y contiene direcciones IPv6 y nombres de dominio de servidores DNS.

Utilice la página **Pool Configuration** (Configuración de conjunto) para crear un conjunto o configurar los parámetros de un conjunto.

Para visualizar la página, haga clic en **IPv6**→**DHCPv6**→**Pool Configuration** (Configuración de conjunto) en la vista de árbol.

Ilustración 11-7. Configuración de conjunto - Crear



Ilustración 11-8. Configuración de conjunto - Visualizar



La página **Pool Configuration** (Configuración de conjunto) contiene los campos siguientes:

Pool Name (Nombre de conjunto): menú desplegable que enumera todos los nombres de conjunto configurados. Cuando se selecciona **Create** (Crear), se borran los datos de los campos de la página, para poder introducir la información del nuevo conjunto.

Pool Name (Nombre de conjunto): muestra el conjunto seleccionado en el campo anterior u ofrece la posibilidad de introducir un nombre exclusivo para un conjunto DHCPv6 cuando se selecciona la opción de crear. Se pueden introducir 31 caracteres alfanuméricos como máximo.

DNS Server Address (Dirección de servidor DNS): menú desplegable que especifica la dirección IPv6 de un servidor DNS de un conjunto DHCPv6 concreto. Cuando se selecciona **Add** (Añadir) en el menú, se borran los datos del siguiente campo para poder introducir la nueva dirección.

DNS Server Address (Dirección de servidor DNS): muestra la dirección del servidor DNS seleccionada en el campo anterior. Si ha seleccionado **Add** (añadir) en el campo anterior, debe introducir aquí una nueva dirección de servidor DNS. Haga clic en **Delete** (Eliminar) para borrar una dirección de este conjunto. La dirección se borra al hacer clic en **Apply Changes** (Aplicar cambios).

Domain Name (Nombre de dominio): menú desplegable que especifica la lista de nombres de dominio configurados en un conjunto DHCPv6 concreto. Cuando se selecciona **Add** (Añadir) en el menú, se borran los datos del siguiente campo para poder introducir el nuevo nombre.

Domain Name (Nombre de dominio): muestra el nombre de dominio DNS seleccionado del campo anterior. Si ha seleccionado **Add** (añadir) en el campo anterior, debe introducir aquí un nuevo nombre de dominio DNS. Se pueden introducir 255 caracteres alfanuméricos como máximo. Haga clic en **Delete** (Eliminar) para borrar un nombre de dominio de este conjunto. El nombre se borra al hacer clic en **Apply Changes** (Aplicar cambios).

Delete Pool (Eliminar conjunto): marque esta casilla para eliminar el conjunto mostrado. El conjunto se borra al hacer clic en **Apply Changes** (Aplicar cambios).

Creación de un conjunto DHCPv6

1. Abra la página **Pool Configuration** (Configuración de conjunto).
2. Seleccione **Create** (Crear) en el menú desplegable de nombres de conjunto.
3. Introduzca un nuevo nombre en el campo **Pool Name** (Nombre de conjunto).
4. Especifique una dirección de servidor DNS existente para asociarla a este conjunto o cree una nueva.
5. Especifique un nombre de dominio existente para asociarlo a este conjunto o cree uno nuevo.
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda el nuevo conjunto y se actualiza el dispositivo. Si se ha especificado un nuevo nombre de dominio o dirección de servidor DNS, también se guarda.

Modificación de los parámetros de un conjunto DHCPv6

1. Abra la página **Pool Configuration** (Configuración de conjunto).
2. En el menú desplegable **Pool Name** (Nombre de conjunto), seleccione el conjunto cuyos parámetros van a modificarse.
3. Cambie o configure una nueva dirección de servidor DNS para el conjunto especificado.
4. Cambie o configure un nuevo nombre de dominio para el conjunto especificado.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se guardan las modificaciones de los parámetros del conjunto DHCPv6 y se actualiza el dispositivo.

Eliminación de un parámetro o conjunto DHCPv6

1. Abra la página **Pool Configuration** (Configuración de conjunto).
2. En el menú desplegable **Pool Name** (Nombre de conjunto), seleccione el conjunto pertinente.
3. Haga clic en la casilla **Delete** (Eliminar) si va a eliminar la dirección de servidor DNS de este conjunto.
4. Haga clic en la casilla **Delete** (Eliminar) si va a eliminar el nombre de dominio de este conjunto.
5. Haga clic en la casilla **Delete Pool** (Eliminar conjunto) si va a eliminar el conjunto completo.
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el conjunto o la configuración de sus parámetros y se actualiza el dispositivo.

Configuración de los parámetros del conjunto DHCPv6 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

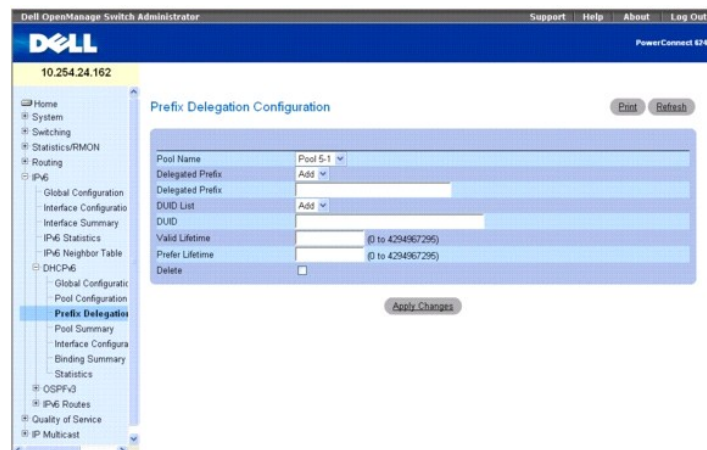
- 1 Comandos DHCPv6

Configuración de delegación de prefijo

Utilice la página **Prefix Delegation Configuration** (Configuración de delegación de prefijo) para configurar un prefijo delegado de un conjunto. Debe haberse creado al menos un conjunto utilizando [DHCPv6 Pool Configuration](#) (Configuración de conjunto DHCPv6) para poder configurar un prefijo delegado.

Para visualizar la página, haga clic en **IPv6** → **DHCPv6** → **Prefix Delegation Configuration** (Configuración de delegación de prefijo) en la vista de árbol.

Ilustración 11-9. Configuración de delegación de prefijo



La página **Prefix Delegation Configuration** (Configuración de delegación de prefijo) contiene los campos siguientes:

Pool Name (Nombre de conjunto): especifica todos los nombres de conjuntos configurados. Seleccione el conjunto que va a configurar.

Delegated Prefix (Prefijo delegado): menú desplegable que especifica el prefijo IPv6 delegado que se asociará al conjunto especificado. Seleccione **Add** (Añadir) para definir un nuevo prefijo delegado para este conjunto.

Delegated Prefix (Prefijo delegado): muestra el prefijo delegado seleccionado o permite introducir uno nuevo.

DUID List (Lista DUID): menú desplegable que selecciona el valor DUID exclusivo del cliente. Seleccione **Add** (Añadir) para definir un nuevo valor DUID para este conjunto.

DUID: muestra el valor DUID seleccionado o permite introducir uno nuevo.

Valid Lifetime (Tiempo de vida válido): especifica el tiempo de vida válido en segundos del prefijo delegado.

Prefer Lifetime (Tiempo de vida preferido): especifica el tiempo de vida preferido en segundos del prefijo delegado.

Delete (Eliminar): elimina la configuración de delegación de prefijo del conjunto mostrado si está marcado y se hace clic en **Apply Changes** (Aplicar cambios).

Configuración de un prefijo delegado para un conjunto

1. Abra la página **Prefix Delegation Configuration** (Configuración de delegación de prefijo).
2. Seleccione el conjunto que va a configurar.
3. Especifique el prefijo delegado.
4. Modifique los campos restantes según sea necesario.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se guardan los parámetros y el prefijo delegado y se actualiza el dispositivo.

Configuración de un prefijo delegado mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

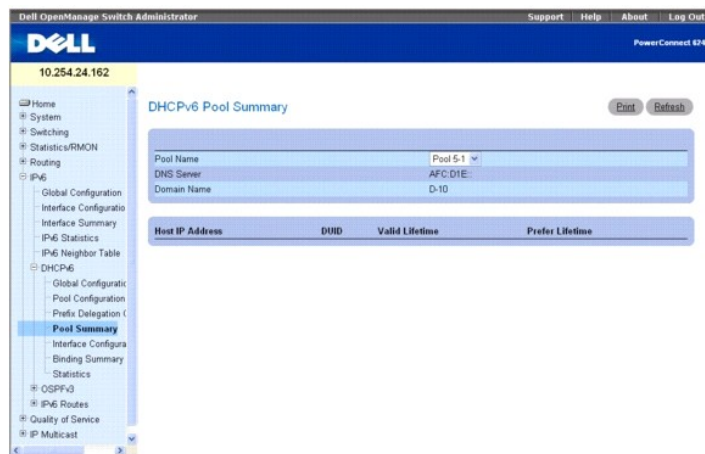
- 1 Comandos DHCPv6

Resumen de conjuntos DHCPv6

Utilice la página **Pool Summary** (Resumen de conjuntos) para visualizar la configuración de todos los conjuntos DHCPv6. Debe crearse al menos un conjunto utilizando [DHCPv6 Pool Configuration](#) (Configuración de conjunto DHCPv6) para que aparezca el resumen de conjuntos.

Para visualizar la página, haga clic en **IPv6** → **DHCPv6** → **Pool Summary** (Resumen de conjuntos) en la vista de árbol.

Ilustración 11-10. Resumen de conjuntos



La página **Pool Summary** (Resumen de conjuntos) contiene los campos siguientes:

Pool Name (Nombre del conjunto): selecciona el conjunto que se mostrará.

DNS Server (Servidor DNS): muestra la dirección IPv6 del servidor DNS asociado.

Domain Name (Nombre de dominio): muestra el nombre de dominio DNS.

Host IP Address (Dirección IP del host): muestra la dirección IPv6 y la longitud de la máscara del prefijo delegado.

DUID: identificador utilizado para identificar el valor DUID exclusivo del cliente.

Valid Lifetime (Tiempo de vida válido): muestra el tiempo de vida válido en segundos del prefijo delegado.

Prefer Lifetime (Tiempo de vida preferido): muestra el tiempo de vida preferido en segundos del prefijo delegado.

Visualización del resumen de conjuntos mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

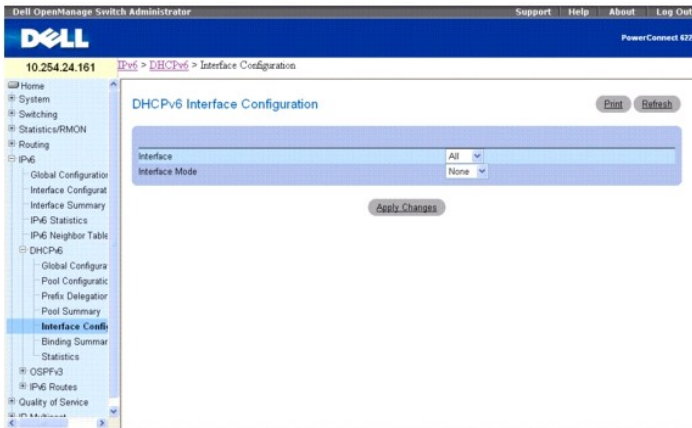
1 Comandos DHCPv6

Configuración de interfaz DHCPv6

Utilice la página DHCPv6 Interface Configuration (Configuración de interfaz DHCPv6) para configurar una interfaz DHCPv6.

Para visualizar la página, haga clic en IPv6 → DHCPv6 → Interface Configuration (Configuración de interfaz) en la vista de árbol.

Ilustración 11-11. Configuración de interfaz DHCPv6



La página DHCPv6 Interface Configuration (Configuración de interfaz DHCPv6) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz para la que esté configurando la función del servidor DHCPv6.

Interface Mode (Modo de interfaz): configure el modo DHCPv6 como servidor o relé. Las funciones de servidor DHCPv6 y de relé DHCPv6 son incompatibles.

Pool Name (Nombre del conjunto): selecciona el conjunto DHCPv6 que contiene los parámetros de delegación de prefijo o sin estado. Este campo aparece cuando la interfaz está en modo de servidor.

Rapid Commit (Confirmar rápido): parámetro opcional. Se especifica para permitir un intercambio abreviado entre el cliente y el servidor. Este campo aparece cuando la interfaz está en modo de servidor.

Preference (Preferencia): selecciona el valor de preferencia utilizado por los clientes para determinar la preferencia entre varios servidores DHCPv6. Se permiten los valores comprendidos entre el 0 y el 4294967295. Este campo aparece cuando la interfaz está en modo de servidor.

Delete (Eliminar): marque esta casilla y haga clic en **Apply Changes** (Aplicar cambios) para eliminar esta configuración. Este campo aparece cuando la interfaz está en modo de servidor o relé.

Relay Interface (Interfaz de relé): selecciona la interfaz para acceder a un servidor de relé. Este campo aparece cuando la interfaz está en modo de relé.

Destination IP Address (Dirección IP de destino): selecciona la dirección IPv6 del servidor de relé DHCPv6. Este campo aparece cuando la interfaz está en modo de relé.

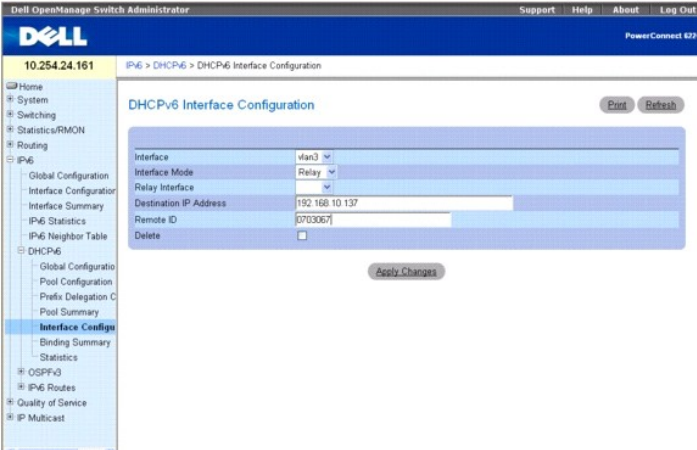
Remote ID (ID remota): selecciona la opción de información de agente de relé. La ID remota debe obtenerse del DUID de servidor DHCPv6 y del número de interfaz de relé o se puede especificar como una cadena definida por el usuario. Este campo aparece cuando la interfaz está en modo de relé.

Configuración de una interfaz DHCPv6 para el modo de interfaz de relé.

1. Abra la página DHCPv6 Interface Configuration (Configuración de interfaz DHCPv6).
2. Especifique la interfaz deseada y seleccione **Relay** (Relé) en el menú desplegable **Interface Mode** (Modo de interfaz).

Aparece la pantalla siguiente:

Ilustración 11-12. Configuración de interfaz DHCPv6 - Relé



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

Se guarda la configuración de la interfaz DHCPv6 y se actualiza el dispositivo.

Configuración de una interfaz DHCPv6 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

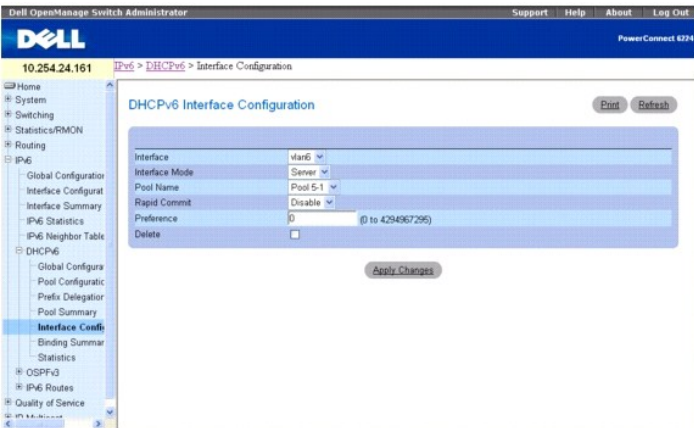
- 1 Comandos DHCPv6

Configuración de una interfaz DHCPv6 para el modo de interfaz de servidor

1. Abra la página **DHCPv6 Interface Configuration** (Configuración de interfaz DHCPv6).
2. Especifique la interfaz deseada y seleccione **Server** (Servidor) en el menú desplegable **Interface Mode** (Modo de interfaz).

Aparece la pantalla siguiente:

Ilustración 11-13. Configuración de interfaz DHCPv6 - Servidor



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

Se guarda la configuración de la interfaz DHCPv6 y se actualiza el dispositivo.

Configuración de una interfaz DHCPv6 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

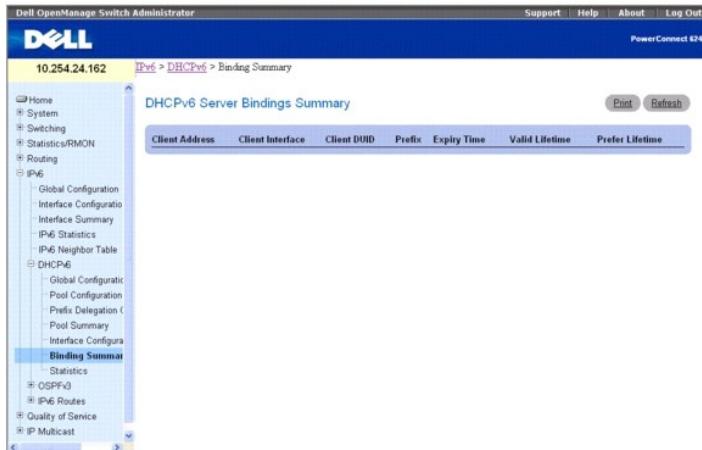
1 Comandos DHCPv6

Resumen de vinculaciones de servidor DHCPv6

Utilice la página **Server Bindings Summary** (Resumen de vinculaciones de servidor) para ver todas las vinculaciones del servidor DHCPv6.

Para visualizar la página, haga clic en IPv6 → DHCPv6 → Bindings Summary (Resumen de vinculaciones) en la vista de árbol.

Ilustración 11-14. Resumen de vinculaciones de servidor



La página **Server Bindings Summary** (Resumen de vinculaciones de servidor) contiene los campos siguientes:

Client Address (Dirección del cliente): especifica la dirección IPv6 del cliente asociada a la vinculación.

Client Interface (Interfaz del cliente): especifica el número de la interfaz donde se ha producido la vinculación del cliente.

Client DUID (DUID de cliente): especifica el identificador DHCPv6 exclusivo del cliente.

Prefix (Prefijo): especifica el tipo de prefijo asociado a esta vinculación.

Expiry Time (Tiempo de caducidad): especifica el número de segundos que debe transcurrir para que el prefijo asociado a una vinculación caduque.

Valid Lifetime (Tiempo de vida válido): especifica el tiempo de vida válido en segundos del prefijo asociado a una vinculación.

Prefer Lifetime (Tiempo de vida preferido): especifica el tiempo de vida preferido en segundos del prefijo asociado a una vinculación.

Visualización de las vinculaciones de servidor mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

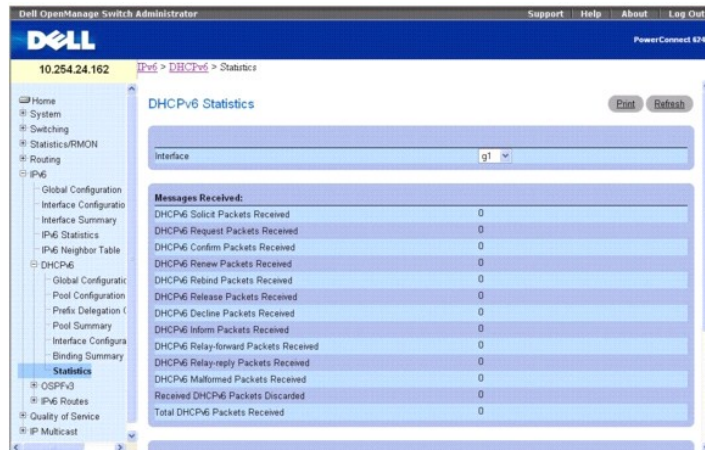
1 Comandos DHCPv6

Estadísticas de DHCPv6

Utilice la página **DHCPv6 Statistics** (Estadísticas de DHCPv6) para visualizar las estadísticas DHCPv6 de una o de todas las interfaces.

Para visualizar la página, haga clic en IPv6 → DHCPv6 → Statistics (Estadísticas) en la vista de árbol.

Ilustración 11-15. Estadísticas de DHCPv6



La página DHCPv6 Statistics (Estadísticas de DHCPv6) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar o configurar. Si selecciona **All (Todo)**, aparecerán los datos de todas las interfaces.

Mensajes recibidos

Esta sección especifica el conjunto de todas las estadísticas de nivel de interfaz en relación con los mensajes recibidos.

DHCPv6 Solicit Packets Received (Paquetes DHCPv6 recibidos de solicitud): especifica el número de solicitudes.

DHCPv6 Request Packets Received (Paquetes DHCPv6 recibidos de petición): especifica el número de peticiones.

DHCPv6 Confirm Packets Received (Paquetes DHCPv6 recibidos de confirmación): especifica el número de confirmaciones.

DHCPv6 Renew Packets Received (Paquetes DHCPv6 recibidos de renovación): especifica el número de renovaciones.

DHCPv6 Rebind Packets Received (Paquetes DHCPv6 recibidos de reenlace): especifica el número de reenlaces.

DHCPv6 Release Packets Received (Paquetes DHCPv6 recibidos de liberación): especifica el número de liberaciones.

DHCPv6 Decline Packets Received (Paquetes DHCPv6 recibidos de rechazo): especifica el número de rechazos.

DHCPv6 Inform Packets Received (Paquetes DHCPv6 recibidos de informes): especifica el número de informes.

DHCPv6 Relay-forward Packets Received (Paquetes DHCPv6 recibidos de reenvío de relé): especifica el número de reenvíos de relé.

DHCPv6 Relay-reply Packets Received (Paquetes DHCPv6 recibidos de respuesta de relé): especifica el número de respuestas de relé.

DHCPv6 Malformed Packets Received (Paquetes mal formados DHCPv6 recibidos): especifica el número de paquetes mal formados.

Received DHCPv6 Packets Discarded (Paquetes descartados DHCPv6 recibidos): especifica el número de paquetes descartados.

Total DHCPv6 Packets Received (Total de paquetes DHCPv6 recibidos): especifica el número total de paquetes recibidos.

Mensajes enviados

Esta sección especifica el conjunto de todas las estadísticas de nivel de interfaz en relación con los mensajes enviados.

DHCPv6 Advertisement Packets Transmitted (Paquetes de anuncio DHCPv6 transmitidos): especifica el número de anuncios.

DHCPv6 Reply Packets Transmitted (Paquetes de respuesta DHCPv6 transmitidos): especifica el número de respuestas.

DHCPv6 Reconfig Packets Transmitted (Paquetes de reconfiguración DHCPv6 transmitidos): especifica el número de reconfiguraciones.

DHCPv6 Relay-forward Packets Transmitted (Paquetes DHCPv6 transmitidos de reenvío de relé): especifica el número de reenvíos de relé.

DHCPv6 Relay-reply Packets Transmitted (Paquetes DHCPv6 transmitidos de respuesta de relé): especifica el número de respuestas de relé.

Total DHCPv6 Packets Sent (Total de paquetes DHCPv6 enviados): especifica el número total de paquetes transmitidos.

Clear (Borrar): reinicia los recuentos de paquetes de interfaz.

Visualización de las estadísticas de DHCPv6

1. Abra la página DHCPv6 Statistics (Estadísticas de DHCPv6).
2. Seleccione la interfaz que se va a visualizar en el menú desplegable Interface (Interfaz).

Aparecen las estadísticas de DHCPv6 de la interfaz seleccionada.

Visualización de las estadísticas de DHCPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos DHCPv6

OSPFv3

OSPFv3 es el protocolo de enrutamiento para abrir la ruta más corta primero de IPv6. Es similar a OSPFv2 en cuanto al concepto de base de datos de estados de enlace, intra/interárea y enlaces virtuales y rutas externas AS. Se distingue de su contrapunto IPv4 en una serie de aspectos, como por ejemplo los siguientes: la comunicación con homólogos se realiza mediante direcciones locales de enlace; el protocolo se centra en un enlace, no en la red; y la semántica de las direcciones se ha transformado en LSA de hoja, que en última instancia permite su uso tanto para IPv4 como para IPv6. También se admiten los enlaces punto a punto para permitir el funcionamiento por túneles.

Es posible activar OSPF y OSPFv3 al mismo tiempo. OSPF funciona con IPv4 y OSPFv3 funciona con IPv6.

La página de menú **OSPFv3** contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de OSPFv3. Para visualizar esta página, haga clic en **IPv6** → **OSPFv3** en la vista de árbol.

A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

- 1 [Configuración de OSPFv3](#)
- 1 [Configuración del área OSPFv3](#)
- 1 [Resumen del área de rutas internas OSPFv3](#)
- 1 [Configuración del intervalo de área OSPFv3](#)
- 1 [Configuración de interfaz OSPFv3](#)
- 1 [Estadísticas de interfaz OSPFv3](#)
- 1 [Vecinos OSPFv3](#)
- 1 [Tabla de vecinos OSPFv3](#)
- 1 [Base de datos de estados de enlace OSPFv3](#)
- 1 [Configuración de enlace virtual OSPFv3](#)
- 1 [Resumen de enlaces virtuales OSPFv3](#)
- 1 [Configuración de redistribución de rutas OSPFv3](#)
- 1 [Resumen de redistribución de rutas OSPFv3](#)

Configuración de OSPFv3

Utilice la página OSPFv3 Configuration (Configuración de OSPFv3) para activar y configurar OSPFv3 para un conmutador.

Para visualizar la página, haga clic en **IPv6** → **OSPFv3** → **Configuration** (Configuración) en la vista de árbol.


Ilustración 11-16. Configuración de OSPFv3



La página OSPFv3 Configuration (Configuración de OSPFv3) contiene los campos siguientes:

Router ID (ID de enrutador): número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el enrutador dentro del sistema autónomo (AS). Si desea cambiar la ID de enrutador, primero debe desactivar OSPFv3. Una vez que haya configurado la nueva ID de enrutador, debe volver a activar OSPFv3 para que el cambio tenga efecto. El valor predeterminado es 0.0.0.0, pero esta no es una ID de enrutador válida y debe modificarse antes de hacer clic en el botón **Apply Changes** (Aplicar cambios).

OSPFv3 Admin Mode (Modo de administración de OSPFv3): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable. Si selecciona **Enable** (Activar), se activa OSPFv3 para el conmutador. El valor predeterminado es **Enable** (Activar). Para que OSPFv3 esté operativo, antes debe configurar una ID de enrutador. Esta acción también puede realizarse emitiendo el comando de CLI, `router-id`, en el modo OSPF del enrutador IPv6.

 **NOTA:** una vez que OSPFv3 se inicialice en el enrutador, permanecerá inicializado hasta que este se restablezca.

ASBR Mode (Modo ASBR): indica si el modo ASBR está activado o desactivado. Seleccionar **Enable** (Activar) implica que el enrutador es un enrutador de límite de sistema autónomo (ASBR). El enrutador se convierte automáticamente en un ASBR cuando se configura para redistribuir rutas obtenidas de otro protocolo.

ABR Status (Estado de ABR): los valores de este campo pueden ser **Enable** (Activar) o **Disable** (Desactivar). El campo aparece sólo si existe una configuración válida. **Enabled** (Activado) implica que el enrutador es un enrutador de límite de área (ABR). **Disabled** (Desactivado) implica que no lo es.

Exit Overflow Interval (secs) (Intervalo de salida de desbordamiento [seg.]): introduzca el número de segundos que el enrutador debe esperar, una vez que ha alcanzado el estado de desbordamiento, hasta intentar salir de dicho estado. Esto permite al enrutador volver a originar AS-external-LSA (LSA externos al AS) no predeterminados. Si introduce 0, el enrutador no abandonará el estado de desbordamiento hasta que se reinicie. El intervalo es de 0 a 2147483647 segundos.

External LSA Count (Número de LSA externos): número de LSA externos (LS tipo 5) en la base de datos de estados de enlace.

External LSA Checksum (Suma de comprobación de LSA externos): total de las sumas de comprobación de LS (estado de enlace) de los LSA externos contenidos en la base de datos de estados de enlace. Este total puede utilizarse para determinar si se ha producido algún cambio en la base de datos de estados de enlace de un enrutador y para comparar las bases de datos de estados de enlace de dos enrutadores.

New LSAs Originated (Nuevos LSA originados): en cualquier área OSPFv3, un enrutador origina varios LSA. Cada enrutador origina un router-LSA (LSA de enrutador). Si el enrutador es también el enrutador designado para cualquiera de las redes del área, éste origina network-LSA (LSA de red) para dichas redes. Este valor representa el número de LSA originados por dicho enrutador.

LSAs Received (LSA recibidos): número de LSA recibidos que se han determinado que son nuevas instancias. Este número no incluye las instancias más recientes de los LSA originados por sí mismos.

External LSDB Limit (Límite LSDB externo): número máximo de AS-external-LSA (LSA externos al AS) que se puede guardar en la base de datos. -1 implica que se pueden guardar los LSA que se desee. El rango válido de valores es de -1 a 2147483647.

Default Metric (Métrica predeterminada): configura un valor predeterminado de métrica de las rutas redistribuidas. Este campo muestra la métrica predeterminada si ya se ha definido una o estará en blanco si no se ha configurado previamente. Los valores válidos están comprendidos entre 1 y 16777214.

Maximum Paths (Máximo de rutas de acceso): configure el número máximo de rutas de acceso que OSPFv3 puede notificar a un destino determinado. Los valores válidos están comprendidos entre 1 y 2.

Default Information Originate (Originar información predeterminada): permite activar (**Enable**) o desactivar (**Disable**) el anuncio de ruta predeterminada. Tenga en cuenta que los valores **Always** (Siempre), **Metric** (Métrica) y **Metric Type** (Tipo de métrica) sólo se pueden configurar después de haber definido **Default Information Originate** (Originar información predeterminada) con el valor **Enable** (Activar). Si **Default Information Originate** se configura con el valor **Enable** y los valores **Always**, **Metric** y **Metric Type** ya están configurados, al volver a configurar **Default Information Originate** como **Disable**, los valores **Always**, **Metric** y **Metric Type** volverán a tener el valor predeterminado.

Always (Siempre): configura el anuncio de enrutador como `::/0` cuando se establece en **True** (Verdadero).

Metric (Métrica): especifica la métrica de la ruta predeterminada. Los valores válidos están comprendidos entre 0 y 16777214.

Metric Type (Tipo de métrica): especifica el tipo de métrica de la ruta predeterminada. Los valores válidos son **External Type 1** (Tipo externo 1) y **External Type 2** (Tipo externo 2).

Configuración de OSPFv3

1. Abra la página **OSPFv3 Configuration** (Configuración de OSPFv3).
2. Modifique los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de OSPFv3 y se actualiza el dispositivo.

Configuración de OSPFv3 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

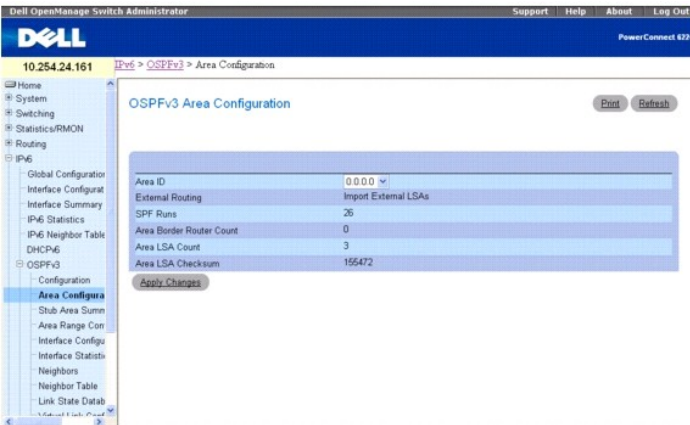
1 Comandos OSPFv3

Configuración del área OSPFv3

Utilice la página **OSPFv3 Area Configuration** (Configuración del área OSPFv3) para crear y configurar un área OSPFv3.

Para visualizar la página, haga clic en **IPv6** → **OSPFv3** → **Area Configuration** (Configuración de área) en la vista de árbol.

Ilustración 11-17. Configuración de área OSPFv3



La página OSPFv3 Area Configuration (Configuración de área OSPFv3) contiene los campos siguientes:

Area ID (ID de área): el área OSPFv3. Una ID de área es un número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta una interfaz de enrutador.

External Routing (Enrutamiento externo): definición de las capacidades del enrutador para el área, como por ejemplo si se distribuyen o no AS-external-LSA (LSA externos al AS) al área o a través de ésta. Si se trata de un área de rutas internas, éstas son las opciones posibles con las que puede configurar la capacidad de enrutamiento externo; de lo contrario, la única opción posible es Import External LSAs (Importar LSA externos).

SPF Runs (Ejecuciones de SPF): número de veces que la tabla de rutas intraárea se ha calculado mediante la base de datos de estados de enlace de esta área. Este cálculo suele realizarse mediante el algoritmo de Dijkstra.

Area Border Router Count (Recuento de enrutadores de límite de área): número total de enrutadores de límite de área a los que se puede acceder dentro de esta área. Este valor es inicialmente cero y se calcula en cada paso de SPF.

Area LSA Count (Recuento de LSA del área): número total de anuncios de estado de enlace contenidos en la base de datos de estados de enlace de esta área, incluidos los LSA externos al AS.

Area LSA Checksum (Suma de comprobación de LSA del área): el total sin signo de 32 bits de las sumas de comprobación de LS de los anuncios de estado de enlace contenidas en la base de datos de estados de enlace de esta área. Este total no incluye los anuncios de estado de enlace externos (LS tipo 5). Este total puede utilizarse para determinar si se ha producido algún cambio en la base de datos de estados de enlace de un enrutador y para comparar las bases de datos de estados de enlace de dos enrutadores. El valor tiene un formato hexadecimal.

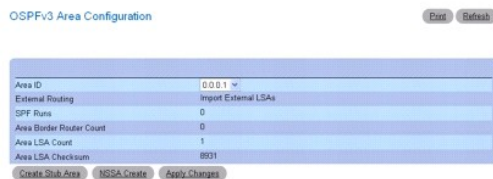
Configuración de un área OSPFv3

1. Abra la página OSPFv3 Area Configuration (Configuración de área OSPFv3).
2. Modifique los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración y se actualiza el dispositivo.

La página web vuelve a aparecer con los botones **Create Stub Area** (Crear área de rutas internas) y **NSSA Create** (Crear NSSA).

Ilustración 11-18. Configuración de área OSPFv3 - Crear área de rutas internas y Crear NSSA



Configuración de un área de rutas internas OSPFv3

1. Abra la página OSPFv3 Area Configuration (Configuración de área OSPFv3).
2. Modifique los campos necesarios.

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

La página web vuelve a aparecer con los botones **Create Stub Area** (Crear área de rutas internas) y **NSSA Create** (Crear NSSA). Vea la [ilustración 11-18](#).

4. Haga clic en **Create Stub Area** (Crear área de rutas internas).

Aparecen los campos de **Stub Area Information** (Información de área de rutas internas).

Ilustración 11-19. Configuración de área de rutas internas OSPFv3

OSPFv3 Area Configuration Print Refresh

Area ID	0.0.0.1
External Routing	Import No LSAs
SPF Runs	8
Area Border Router Count	0
Area LSA Count	4
Area LSA Checksum	10506

Stub Area Information

Import Summary LSAs	Enable
Metric Value	1 (1 to 16777215)

Delete Stub Area Apply Changes

5. Complete los campos restantes.

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

Se guarda la información de área de rutas internas y se actualiza el dispositivo.

Configuración de un área NSSA OSPFv3

1. Abra la página **OSPFv3 Area Configuration** (Configuración de área OSPFv3).

2. Modifique los campos necesarios.

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

La página web vuelve a aparecer con los botones **Create Stub Area** (Crear área de rutas internas) y **NSSA Create** (Crear NSSA). Vea la [ilustración 11-18](#).

4. Haga clic en **NSSA Create** (Crear NSSA) en la página web **OSPFv3 Area Configuration** (Configuración de área OSPFv3).

La página web vuelve a aparecer mostrando las opciones de configuración de NSSA.

Ilustración 11-20. Configuración de área OSPFv3 - NSSA

OSPFv3 Area Configuration Print Refresh

Area ID	0.0.0.1
External Routing	Import NSSAs
SPF Runs	10
Area Border Router Count	0
Area LSA Count	3
Area LSA Checksum	96443

NSSA Specific Information

Import Summary LSAs	Enable
Default Information Originate	False
Default Metric	10 (1 to 16777214)
Default Metric Type	Non-comparable Cost
Translator Role	Candidate
Translator Stability Interval	40 (1 to 3600)
No-Redistribute Mode	Enable
Translator State	Elected

NSSA Delete Apply Changes

5. Complete los campos restantes.

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

Se guarda la información de NSSA y se actualiza el dispositivo.

Eliminación de información de área de rutas internas OSPFv3

1. Abra la página OSPFv3 Area Configuration (Configuración de área OSPFv3) con la información de área de rutas internas configurada.
2. Haga clic en **Delete Stub Area** (Eliminar área de rutas internas).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Eliminación de información de NSSA OSPFv3

1. Abra la página OSPFv3 Area Configuration (Configuración de área OSPFv3) con la información de NSSA configurada.
2. Haga clic en **NSSA Delete** (Eliminar NSSA).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Configuración de un área OSPFv3 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

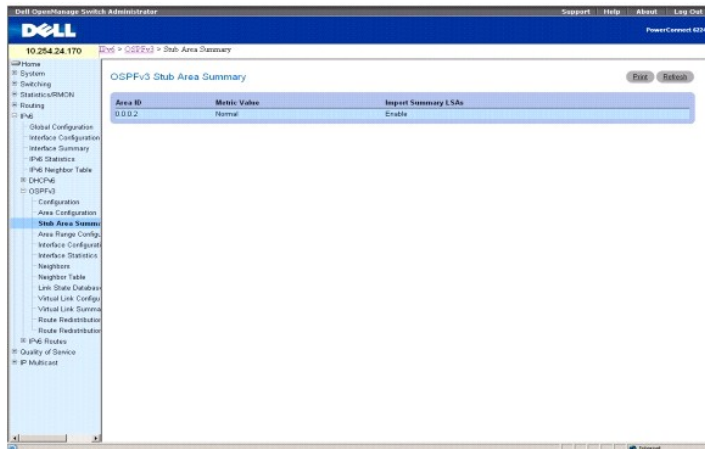
- 1 Comandos OSPFv3

Resumen del área de rutas internas OSPFv3

Utilice la página OSPFv3 Stub Area Summary (Resumen del área de rutas internas OSPFv3) para visualizar información sobre el área de rutas internas OSPFv3.

Para visualizar la página, haga clic en IPv6 → OSPFv3 → Stub Area Summary (Resumen del área de rutas internas) en la vista de árbol.

Ilustración 11-21. Resumen del área de rutas internas OSPFv3



La página OSPFv3 Stub Area Configuration (Configuración de área de rutas internas OSPFv3) contiene los campos siguientes:

Area ID (ID de área): identificación del área de rutas internas.

Metric Value (Valor de métrica): valor de métrica aplicado a la ruta predeterminada anunciada en el área.

Import Summary LSAs (Importar LSA de resumen): determina si la importación de LSA de resumen está activada o desactivada.

Visualización del resumen del área de rutas internas OSPFv3 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

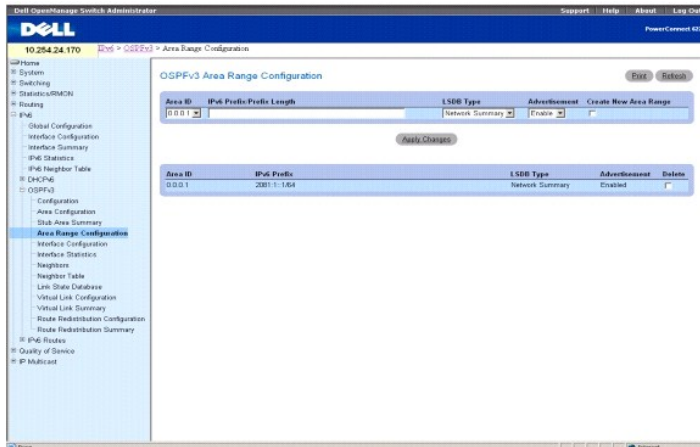
- 1 Comandos OSPFv3

Configuración del intervalo de área OSPFv3

Utilice la página OSPFv3 Area Range Configuration (Configuración del intervalo de área OSPFv3) para configurar los intervalos de área OSPFv3.

Para visualizar la página, haga clic en IPv6→ OSPFv3→ Area Range Configuration (Configuración del intervalo de área) en la vista de árbol.

Ilustración 11-22. Configuración del intervalo de área OSPFv3



La página OSPFv3 Area Range Configuration (Configuración del intervalo de área OSPFv3) contiene los campos siguientes:

Area ID (ID de área): selecciona el área cuyos datos van a configurarse.

IPv6 Prefix/Prefix Length (Prefijo/Longitud de prefijo IPv6): introduzca el prefijo/longitud de prefijo IPv6 correspondientes al intervalo de direcciones del área seleccionada.

LSDB Type (Tipo de LSDB): seleccione el tipo de anuncio de enlace asociado al área y al intervalo de direcciones especificados. El tipo predeterminado es Network Summary (Resumen de red).

Advertisement (Anuncio): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable. Si selecciona Enable (Activar), el intervalo de direcciones se anuncia fuera del área por medio de un LSA de resumen de red. El valor predeterminado es Enable (Activar).

Create New Area Range (Crear nuevo intervalo de área): marque esta casilla de verificación para crear un nuevo intervalo de área OSPFv3 con los valores especificados.

Area ID (ID de área): el área OSPFv3.

IPv6 Prefix (Prefijo IPv6): prefijo IPv6 de un intervalo de direcciones del área.

LSDB Type (Tipo de LSDB): tipo de anuncio de enlace del intervalo de direcciones y del área.

Advertisement (Anuncio): modo de anuncio del intervalo de direcciones y del área.

Delete (Eliminar): marque esta casilla de verificación para eliminar el intervalo de área OSPFv3 especificado.

Configuración de un intervalo de área OSPFv3

1. Abra la página OSPFv3 Area Range Configuration (Configuración de un intervalo de área OSPFv3).
2. Modifique los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda el intervalo de área OSPFv3 y se actualiza el dispositivo.

Configuración de un intervalo de área OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

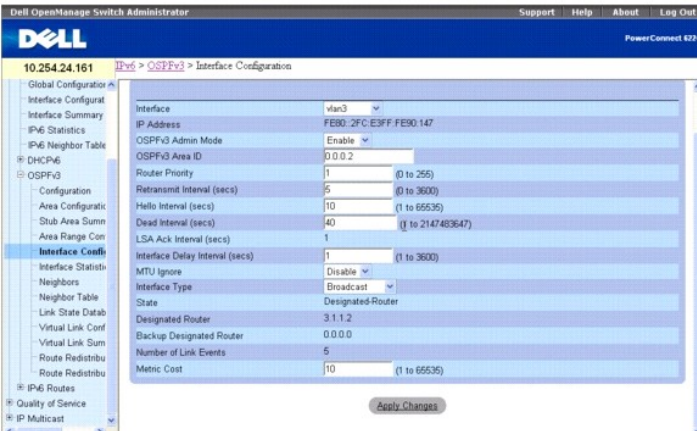
1 Comandos OSPFv3

Configuración de interfaz OSPFv3

Utilice la página OSPFv3 Interface Configuration (Configuración de interfaz OSPFv3) para crear y configurar interfaces OSPFv3.

Para visualizar la página, haga clic en IPv6→ OSPFv3→ Interface Configuration (Configuración de interfaz) en la vista de árbol.

Ilustración 11-23. Configuración de interfaz OSPFv3



La página OSPFv3 Interface Configuration (Configuración de interfaz OSPFv3) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar o configurar.

IP Address (Dirección IP): dirección IPv6 de la interfaz.

OSPFv3 Admin Mode (Modo de administración de OSPFv3): puede seleccionar Enable (Activar) o Disable (Desactivar) en el menú desplegable. El valor predeterminado es Disable (Desactivar). Puede configurar los parámetros de OSPFv3 sin activar el modo de administración de OSPFv3, pero la configuración no tendrá efecto hasta que se active dicho modo. La información siguiente sólo se visualiza si el modo de administración está activado: State (Estado), Designated Router (Enrutador designado), Backup Designated Router (Enrutador designado de reserva), Number of Link Events (Número de eventos de enlace), LSA Ack Interval (Intervalo de confirmación de LSA) y Metric Cost (Coste de métrica). Para que OSPFv3 funcione correctamente, debe haberse especificado valores válidos para Prefijo/Longitud de prefijo IPv6 en la interfaz. Estos valores pueden especificarse mediante la CLI con el comando `ipv6 address` en el modo de configuración de la interfaz.

Una vez que OSPFv3 se inicialice en el enrutador, permanecerá inicializado hasta que se restablezca el enrutador.

OSPFv3 Area ID (ID de área OSPFv3): introduzca el número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área OSPFv3 a la que se conecta la interfaz de enrutador seleccionada. Si asigna una ID de área que no existe, el área se crea con los valores predeterminados.

Router Priority (Prioridad de enrutador): introduzca la prioridad de OSPFv3 de la interfaz seleccionada. La prioridad de una interfaz se especifica mediante un número entero comprendido entre 0 y 255. El valor predeterminado es 1, que es la prioridad de enrutador más alta. El valor 0 indica que el enrutador no puede convertirse en el designado para esta red.

Retransmit Interval (secs) (Intervalo de retransmisión [seg.]): introduzca el intervalo de retransmisión de OSPFv3 para la interfaz especificada. Se trata del número de segundos transcurridos entre los anuncios de estado de enlace correspondientes a las adyacencias de esta interfaz de enrutador. Este valor también se utiliza al retransmitir descripciones de bases de datos y paquetes de petición de estado de enlace. Los valores válidos están comprendidos entre 0 y 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

Hello Interval (secs) (Intervalo de saludo [seg.]): introduzca el intervalo de saludo de OSPFv3 en segundos para la interfaz especificada. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Los valores válidos están comprendidos entre 1 y 65535. El valor predeterminado es 10 segundos.

Dead Interval (secs) (Intervalo de finalización [seg.]): introduzca el intervalo de finalización de OSPFv3 en segundos para la interfaz especificada. Este intervalo corresponde al tiempo que el enrutador debe esperar a ver los paquetes de saludo de un enrutador de vecino antes de declarar que el enrutador está fuera de servicio. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Este valor debe ser un múltiplo del intervalo de saludo (por ejemplo, 4). Los valores válidos están comprendidos entre 1 y 2147483647. El valor predeterminado es 40.

LSA Ack Interval (sec) (Intervalo de confirmación de LSA [seg.]): muestra el número de segundos transcurridos entre las transmisiones de paquetes de confirmación de LSA, que debe ser inferior al intervalo de retransmisión.

Interface Delay Interval (secs) (Intervalo de demora de la interfaz [seg.]): introduzca la demora de transmisión de OSPFv3 para la interfaz especificada. Este intervalo corresponde al número estimado de segundos que se tarda en transmitir un paquete de actualización de estado de enlace en la interfaz seleccionada. Los valores válidos están comprendidos entre 1 y 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

MTU Ignore (Ignorar MTU): desactiva la detección de discrepancia de MTU de OSPFv3 al recibir paquetes. El valor predeterminado es Disable (Desactivar).

Interface Type (Tipo de interfaz): introduzca el tipo de interfaz, que puede configurarse en los modos de difusión o punto a punto. El tipo de interfaz predeterminado es de difusión.

State (Estado): estado actual de la interfaz de enrutador seleccionada. Puede ser uno de los siguientes:

- 1 **Down** (Desconectada): estado inicial de la interfaz. En este estado, los protocolos de nivel bajo han indicado que la interfaz no puede utilizarse. En este estado, los parámetros de la interfaz están configurados con sus valores iniciales. Todos los temporizadores de la interfaz están desactivados, y no hay ninguna adyacencia asociada a la interfaz.
- 1 **Loopback** (Bucle de retorno): en este estado, existe en la interfaz del enrutador un bucle de retorno a la red por hardware o por software. La interfaz no está disponible para el tráfico regular de datos. Sin embargo, puede seguir siendo interesante obtener información sobre la calidad de esta interfaz, ya sea enviando pings de ICMP o mediante algo parecido a una prueba de errores de bits. Por ello, sigue siendo posible dirigir paquetes IP a una interfaz en estado Loopback (Bucle de retorno). Para facilitar esta operación, dichas interfaces se anuncian en LSA de enrutador como rutas de host único, cuyo destino es la dirección de la interfaz IP.
- 1 **Waiting** (En espera): el enrutador está intentando determinar la identidad del enrutador designado (de reserva) para la red mediante la supervisión de los paquetes de saludo recibidos. El enrutador no tiene permitido elegir un enrutador designado de reserva ni un enrutador designado hasta que no salga del estado Waiting (En espera). Esto evita cambios innecesarios del enrutador designado (de reserva).

- 1 **Designated Router** (Enrutador designado): se trata del enrutador designado en la red asociada. Se establecen adyacencias con todos los demás enrutadores asociados a la red. El enrutador debe asimismo originar un network-LSA (LSA de red) para el nodo de red. El network-LSA (LSA de red) contiene enlaces a todos los enrutadores (incluido el enrutador designado) conectados a la red.
- 1 **Backup Designated Router** (Enrutador designado de reserva): se trata del enrutador designado de reserva en la red asociada. Pasa a ser el enrutador designado si el enrutador actual falla. El enrutador establece adyacencias con todos los demás enrutadores asociados a la red. El enrutador designado de reserva lleva a cabo funciones ligeramente diferentes durante el procedimiento de distribución en comparación con el enrutador designado.
- 1 **Other Designated Router** (Otro enrutador designado): la interfaz se conecta a una red NBMA o de difusión en la que se han seleccionado otros enrutadores para ser el enrutador designado y el enrutador designado de reserva. El enrutador intenta formar adyacencias tanto con el enrutador designado como con el enrutador designado de reserva.

El estado sólo se visualiza si está activado el modo de administración de OSPFv3.

Designated Router (Enrutador designado): identificación del enrutador designado para esta red desde el punto de vista del enrutador de divulgación. El enrutador designado se identifica aquí mediante su ID de enrutador. El valor 0.0.0.0 significa que no hay ningún enrutador designado. Este campo sólo se visualiza si está activado el modo de administración de OSPFv3.

Backup Designated Router (Enrutador designado de reserva): identificación del enrutador designado de reserva para esta red desde el punto de vista del enrutador de divulgación. El enrutador designado de reserva se identifica aquí mediante su ID de enrutador. El valor 0.0.0.0 significa que no hay ningún enrutador designado de reserva. Este campo sólo se visualiza si está activado el modo de administración de OSPFv3.

Number of Link Events (Número de eventos de enlace): número de veces que la interfaz OSPFv3 especificada ha cambiado de estado. Este campo sólo se visualiza si está activado el modo de administración de OSPFv3.

Metric Cost (Coste de métrica): introduzca el valor de esta interfaz para el tipo de servicio (TOS) de coste. El intervalo para el coste de métrica va de 1 a 65535. Este campo sólo puede configurarse si se ha inicializado OSPFv3 en la interfaz.

Configuración de una interfaz OSPFv3

1. Abra la página **OSPFv3 Interface Configuration** (Configuración de interfaz OSPFv3).
2. Seleccione la interfaz en la que desea configurar OSPFv3.
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La interfaz OSPFv3 queda configurada y se actualiza el dispositivo.

Configuración de una interfaz OSPFv3 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos OSPFv3

Estadísticas de interfaz OSPFv3

Utilice la página **OSPFv3 Interface Statistics** (Estadísticas de interfaz OSPFv3) para visualizar las estadísticas de interfaz OSPFv3. La información se visualiza únicamente si OSPF está activado.

Para visualizar la página, haga clic en **IPv6** → **OSPFv3** → **Interface Statistics** (Estadísticas de la interfaz) en la vista de árbol.

Ilustración 11-24. Estadísticas de interfaz OSPFv3

OSPFv3 Interface Statistics	
Interface	10.204.24.170
OSPFv3 Area ID	0.0.0.1
Area Border Router Count	1
AS Border Router Count	0
Area LSA Count	14
IPv6 Address	FE80::2FC:EFF:FE80::10D
Interface Events	3
Virtual Events	2
Neighbor Events	6
External LSA Count	0

La página **OSPFv3 Interface Statistics** (Estadísticas de interfaz OSPFv3) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar.

OSPF Area ID (ID de área OSPF): área OSPF a la que pertenece la interfaz de enrutador seleccionada. Una ID de área OSPF es un número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta la interfaz.

Area Border Router Count (Recuento de enrutadores de límite de área): número total de enrutadores de límite de área a los que se puede acceder dentro de esta área. Este valor es inicialmente cero y se calcula en cada paso de SPF.

AS Border Router Count (Recuento de enrutadores de límite de sistema autónomo): número total de enrutadores de límite de sistema autónomo a los que se puede acceder dentro de esta área. Este valor es inicialmente cero y se calcula en cada paso de SPF.

Area LSA Count (Recuento de LSA del área): número total de anuncios de estado de enlace contenidos en la base de datos de estados de enlace de esta área, incluidos los LSA externos al AS.

IPv6 Address (Dirección IPv6): dirección IPv6 de la interfaz.

Interface Events (Eventos de interfaz): número de veces que ha cambiado el estado de la interfaz OSPF especificada o que se ha producido un error.

Virtual Events (Eventos virtuales): número de cambios de estado o errores que se han producido en este enlace virtual.

Neighbor Events (Eventos de vecino): número de veces que ha cambiado el estado de esta relación de vecino o que se ha producido un error.

External LSA Count (Recuento de LSA externos): número de anuncios de estado de enlace externos (LS tipo 5) en la base de datos de estados de enlace.

Visualización de las estadísticas de interfaz OSPFv3

1. Abra la página **OSPFv3 Interface Statistics** (Estadísticas de interfaz OSPFv3).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).

Se muestran las estadísticas de la interfaz.

Visualización de las estadísticas de interfaz OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

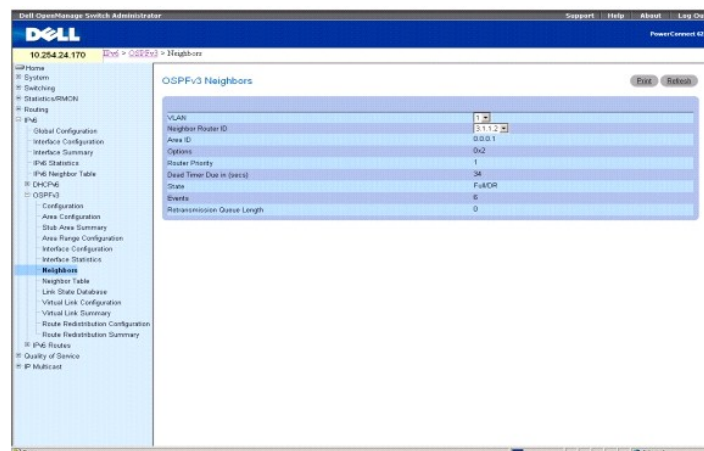
- 1 Comandos OSPFv3

Vecinos OSPFv3

Utilice la página **OSPFv3 Neighbors** (Vecinos OSPFv3) para visualizar la configuración de vecino OSPF correspondiente a una ID de vecino determinada. Cuando se especifica una ID de vecino en particular, se proporciona información detallada sobre dicho vecino. La información de vecino sólo se visualiza cuando se ha activado OSPF y la interfaz tiene un vecino. La dirección IP es la dirección IP del vecino.

Para visualizar la página, haga clic en **IPv6** → **OSPFv3** → **Neighbors** (Vecinos) en la vista de árbol.

Ilustración 11-25. Vecinos OSPFv3



La página **OSPFv3 Neighbors** (Vecinos OSPFv3) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz cuyos datos se van a mostrar o configurar.

Neighbor Router ID (ID de enrutador de vecino): selecciona la dirección IP del vecino cuyos datos desea visualizar.

Area ID (ID de área): número entero de 32 bits en formato con punto decimal que identifica el enrutador de vecino.

Options (Opciones): capacidades opcionales de OSPF admitidas por el vecino. En los paquetes de saludo se incluyen también las funciones de OSPF opcionales del vecino. De este modo, los paquetes de saludos recibidos pueden descartarse (es decir, las relaciones de vecino ni siquiera comienzan a formarse) si existe una discrepancia en determinadas funciones OSPF cruciales.

Router Priority (Prioridad de enrutador): muestra la prioridad de OSPF del vecino especificado. La prioridad de un vecino es un número entero comprendido entre 0 y 255. El valor 0 indica que el enrutador no puede convertirse en enrutador designado para esta red.

Dead Timer Due in (secs) (Temporizador de finalización vencido en [seg.]): si los paquetes de saludo no llegan, especifica el período que debe transcurrir antes de declarar que el vecino está inoperativo.

State (Estado): el estado de un vecino puede ser el siguiente:

- 1 **Down** (Desconectado): estado inicial de una conversación de vecino. Indica que no se ha recibido información reciente procedente del vecino. En las redes NBMA, es posible seguir enviando paquetes de saludo con el estado Down (Desconectado), si bien con una frecuencia reducida.
- 1 **Attempt** (Intentar): este estado sólo es válido para los vecinos conectados a redes NBMA. Indica que no se ha recibido información reciente procedente del vecino, pero que debería hacerse un mayor esfuerzo común para contactar con él. Esto se realiza enviando al vecino paquetes de saludo a intervalos de Hello Interval (Intervalo de saludo).
- 1 **Init** (Iniciar): este estado indica que se ha visto recientemente un paquete de saludo procedente del vecino. Sin embargo, no se ha establecido todavía una comunicación bidireccional con el vecino (es decir, el enrutador no aparecía en el paquete de saludo del vecino). Todos los vecinos que se encuentran en este estado (o en uno superior) se enumeran en los paquetes de saludo enviados desde la interfaz asociada.
- 1 **2-Way** (Bidireccional): este estado indica que la comunicación entre los dos enrutadores es bidireccional. Esto se garantiza a través del funcionamiento del protocolo de saludo. Este es el estado más avanzado antes de comenzar el establecimiento de adyacencias. El enrutador designado (de reserva) se selecciona de entre el grupo de vecinos que se encuentran en el estado 2-way (Bidireccional) o en uno superior.
- 1 **Exchange Start** (Inicio de intercambio): se trata del primer paso en la creación de una adyacencia entre dos enrutadores de vecino. El objetivo de este paso es decidir qué enrutador es el enrutador maestro y cuál es el número de secuencia de descripción de base de datos (DD) inicial. Las conversaciones de vecino en este estado o en estados superiores se denominan adyacencias.
- 1 **Exchange** (Intercambio): en este estado, el enrutador describe toda su base de datos de estados de enlace enviando paquetes de descripción de base de datos al vecino. En este estado, también pueden enviarse paquetes de petición de estado de enlace que pregunten por los LSA más recientes del vecino. Para el procedimiento de distribución se utilizan todas las adyacencias con el estado Exchange (Intercambio) o un estado superior. Estas adyacencias son totalmente capaces de transmitir y recibir todos los tipos de paquetes de protocolo de enrutamiento OSPF.
- 1 **Loading** (Cargando): en este estado, se envían paquetes de petición de estado de enlace al vecino que preguntan por los LSA más recientes que se han detectado (pero todavía no se han recibido) con el estado Exchange (Intercambio).
- 1 **Full** (Completo): en este estado, los enrutadores de vecino son completamente adyacentes. Estas adyacencias aparecen ahora en los router-LSA (LSA de enrutador) y network-LSA (LSA de red).

Events (Eventos): número de veces que ha cambiado el estado de esta relación de vecino o que se ha producido un error.

Retransmission Queue Length (Longitud de cola de retransmisión): longitud actual de la cola de retransmisión.

Visualización de vecinos OSPFv3

1. Abra la página **OSPFv3 Neighbors** (Vecinos OSPFv3).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).
3. Seleccione la ID de enrutador de vecino que se va a visualizar.

Aparecen las estadísticas correspondientes a la ID de vecino de interfaz seleccionada.

Visualización de los vecinos OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

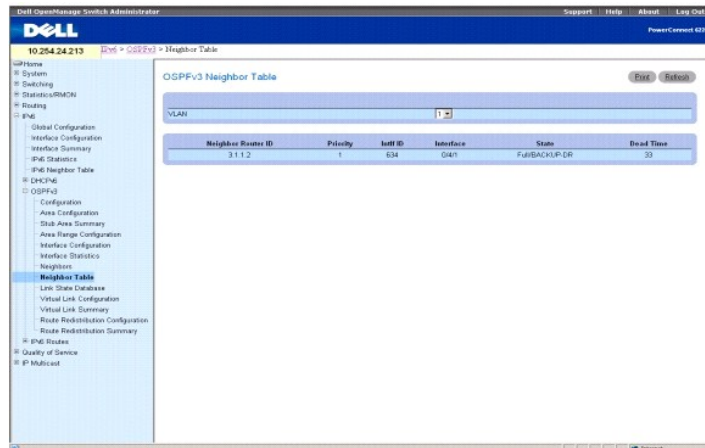
- 1 Comandos OSPFv3

Tabla de vecinos OSPFv3

Utilice la página **OSPFv3 Neighbor Table** (Tabla de vecinos OSPFv3) para visualizar la lista de tablas de vecinos OSPF. Cuando se especifica una ID de vecino en particular, se proporciona información detallada sobre un vecino. La tabla de vecinos sólo se visualiza si se ha activado OSPF.

Para visualizar la página, haga clic en **IPv6→ OSPFv3→ Neighbor Table** (Tabla de vecinos) en la vista de árbol.

Ilustración 11-26. Tabla de vecinos OSPFv3



La página **OSPFv3 Neighbor Table** (Tabla de vecinos OSPFv3) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz cuyos datos se van a mostrar o configurar.

Neighbor Router ID (ID de enrutador de vecino): número entero de 32 bits en formato con punto decimal que representa la interfaz de vecino.

Priority (Prioridad): prioridad de este vecino en el algoritmo de elección de enrutador designado. El valor 0 indica que el vecino no puede convertirse en el enrutador designado para esta red.

IntfID: ID de interfaz que anuncia el vecino en sus paquetes de saludo en este enlace.

Interface (Interfaz): ranura/puerto que identifica el índice de interfaz del vecino.

State (Estado): estado de la relación con este vecino.

Dead Time (Tiempo muerto): número de segundos transcurridos desde la recepción del último saludo de los vecinos adyacentes. Establezca 0 para los vecinos cuyo estado sea inferior o igual a Init.

Visualización de la tabla de vecinos OSPFv3

1. Abra la página **OSPFv3 Neighbors Table** (Tabla de vecinos OSPFv3).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).

Aparece la tabla de vecinos OSPF de la interfaz seleccionada.

Visualización de la tabla de vecinos OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos OSPFv3

Base de datos de estados de enlace OSPFv3

Utilice la página **OSPFv3 Link State Database** (Base de datos de estados de enlace OSPFv3) para visualizar la base de datos de estados de enlace.

Para visualizar la página, haga clic en **IPv6** → **OSPFv3** → **Link State Database** (Base de datos de estados de enlace) en la vista de árbol.

Ilustración 11-27. Base de datos de estados de enlace OSPFv3

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays the 'OSPFv3 Link State Database' with a table containing one entry. The table has columns for Adv. Router, Area ID, LSA Type, Link ID, Age, Sequence, Checksum, Options, and Rtr Opt. The entry shows Adv. Router: 10.250.14.14, Area ID: 0.0.0.0, LSA Type: Intra Prefix, Link ID: 0, Age: 147, Sequence: 80000001, Checksum: c90b, and Rtr Opt. is empty.

Adv. Router	Area ID	LSA Type	Link ID	Age	Sequence	Checksum	Options	Rtr Opt.
10.250.14.14	0.0.0.0	Intra Prefix	0	147	80000001	c90b		

La página OSPFv3 Link State Database (Base de datos de estados de enlace OSPFv3) contiene los campos siguientes:

Adv. Router (Enrutador): número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el enrutador dentro del sistema autónomo (AS). La ID de enrutador se configura en la página de configuración de OSPFv3.

Area ID (ID de área): ID de un área OSPF a la que se conecta una de las interfaces de enrutador. Una ID de área es un número entero de 32 bits en formato con punto decimal que identifica de forma exclusiva el área a la que se conecta una interfaz.

LSA Type (Tipo de LSA): formato y función del anuncio de estado de enlace. Los tipos, definidos en el apartado A.4 de RFC 2740, pueden ser los siguientes:

- 1 Router-LSA (LSA de enrutador)
- 1 Network-LSA (LSA de red)
- 1 Inter-Area-Prefix-LSA (LSA de prefijo interárea)
- 1 Inter-Area-Router-LSA (LSA de enrutador interárea)
- 1 AS-External-LSA (LSA externo al AS)
- 1 Type-7-LSA (LSA de tipo 7)
- 1 Link-LSA (LSA de enlace)
- 1 Intra-Area-Prefix-LSA (LSA de prefijo intraárea)

Link ID (ID de enlace): ID de estado de enlace que identifica la parte del dominio de enrutamiento que está describiendo el anuncio. El valor de la ID de LS depende del tipo de estado de enlace del anuncio.

Age (Edad): tiempo en segundos transcurrido desde que se ha originado el anuncio de estado de enlace por primera vez.

Sequence (Secuencia): número entero de 32 bits con signo. Permite detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.

Checksum (Suma de comprobación): sirve para detectar daños en los datos de un anuncio. Estos daños pueden producirse mientras se distribuye un anuncio o mientras éste se encuentra almacenado en la memoria de un enrutador. Este campo es la suma de comprobación de todo el contenido del anuncio, excepto el campo de edad del LS.

Options (Opciones): el campo Options (Opciones) que figura en el encabezado del anuncio de estado de enlace indica qué capacidades opcionales están asociadas al anuncio. Las opciones son:

- 1 V6: si no está seleccionado, el enlace se excluye de los cálculos de enrutamiento IPv6.
- 1 E: describe cómo se distribuyen los AS-external-LSA (LSA externos al AS).
- 1 MC: describe si los datagramas de multidifusión IP se reenvían de acuerdo con las especificaciones.
- 1 N: describe cómo se gestionan los LSA de tipo 7.
- 1 R: muestra si el iniciador es un enrutador activo. La opción R es el bit del enrutador y, cuando no está seleccionada, las rutas que pasan a través del nodo de divulgación no se pueden calcular.
- 1 DC: describe cómo gestiona el sistema los circuitos de petición.

Rtr Opt.: muestra las opciones específicas del enrutador.

Visualización de la base de datos de estados de enlace OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

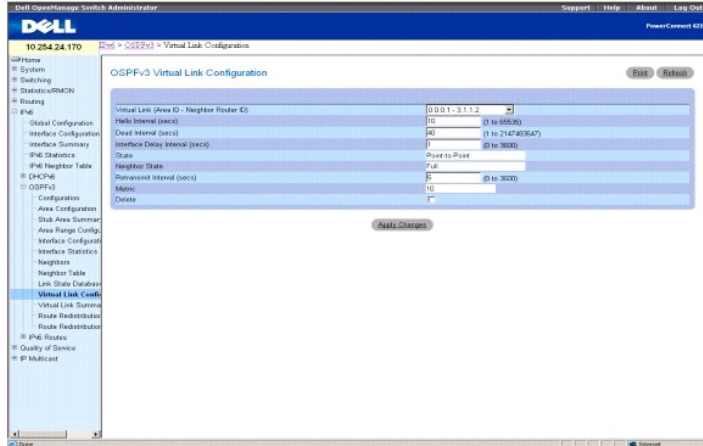
- 1 Comandos OSPFv3

Configuración de enlace virtual OSPFv3

Utilice la página OSPFv3 Virtual Link Configuration (Configuración de enlace virtual OSPFv3) para definir un nuevo enlace virtual o configurar uno ya existente. Para visualizar esta página, debe definirse un área OSPFv3 válida mediante la página OSPFv3 Area Configuration (Configuración de área OSPFv3).

Para visualizar la página, haga clic en IPv6 → OSPFv3 → Virtual Link Configuration (Configuración de enlace virtual) en la vista de árbol.

Ilustración 11-28. Configuración de enlace virtual OSPFv3



La página OSPFv3 Virtual Link Configuration (Configuración de enlace virtual OSPFv3) contiene los campos siguientes:

Create New Virtual Link (Crear nuevo enlace virtual): seleccione esta opción en el menú desplegable para definir un nuevo enlace virtual. La parte correspondiente al área dentro de la identificación del enlace virtual es fija: se le solicita que introduzca la ID de enrutador de vecino en una nueva pantalla.

Virtual Link (Area ID - Neighbor Router ID) (Enlace virtual [ID de área - ID de enrutador de vecino]): seleccione el enlace virtual cuyos datos desea visualizar o configurar. Este parámetro consta de la ID de área y la ID de enrutador de vecino.

Hello Interval (secs) (Intervalo de saludo [seg.]): introduzca el intervalo de saludo de OSPF en segundos para la interfaz especificada. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Los valores válidos están comprendidos entre 1 y 65535. El valor predeterminado es 10 segundos.

Dead Interval (secs) (Intervalo de finalización [seg.]): introduzca el intervalo de finalización de OSPF en segundos para la interfaz especificada. Este intervalo corresponde al tiempo que el enrutador debe esperar a ver los paquetes de saludo de un enrutador de vecino antes de declarar que el enrutador está fuera de servicio. Este parámetro debe ser el mismo para todos los enrutadores conectados a una red. Este valor debe ser un múltiplo del intervalo de saludo (por ejemplo, 4). Los valores válidos están comprendidos entre 1 y 2147483647. El valor predeterminado es 40.

Interface Delay Interval (secs) (Intervalo de demora de la interfaz [seg.]): introduzca la demora de transmisión de OSPF para la interfaz especificada. Este intervalo corresponde al número estimado de segundos que se tarda en transmitir un paquete de actualización de estado de enlace en la interfaz seleccionada. Los valores válidos están comprendidos entre 1 y 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

State (Estado): estado actual del enlace virtual seleccionado. Puede ser uno de los siguientes:

- 1 **Down** (Desconectada): estado inicial de la interfaz. En este estado, los protocolos de nivel bajo han indicado que la interfaz no puede utilizarse. En este estado, los parámetros de la interfaz están configurados con sus valores iniciales. Todos los temporizadores de la interfaz están desactivados, y no hay ninguna adyacencia asociada a la interfaz.
- 1 **Waiting** (En espera): el enrutador está intentando determinar la identidad del enrutador designado (de reserva) mediante la supervisión de los paquetes de saludo recibidos. El enrutador no tiene permitido elegir un enrutador designado de reserva ni un enrutador designado hasta que no salga del estado Waiting (En espera). Esto evita cambios innecesarios del enrutador designado (de reserva).
- 1 **Point-to-Point** (Punto a punto): la interfaz se encuentra operativa y está conectada al enlace virtual. Al entrar en este estado, el enrutador intenta formar una adyacencia con el enrutador de vecino. Se envían paquetes de saludo al vecino a cada intervalo de segundos definido en Hello Interval (Intervalo de saludo).
- 1 **Designated Router** (Enrutador designado): se trata del enrutador designado en la red asociada. Se establecen adyacencias con todos los demás enrutadores asociados a la red. El enrutador debe asimismo originar un network-LSA (LSA de red) para el nodo de red. El network-LSA (LSA de red) contiene enlaces a todos los enrutadores (incluido el enrutador designado) conectados a la red.
- 1 **Backup Designated Router** (Enrutador designado de reserva): se trata del enrutador designado de reserva en la red asociada. Pasa a ser el enrutador designado si el enrutador designado actual falla. El enrutador establece adyacencias con todos los demás enrutadores asociados a la red. El enrutador designado de reserva lleva a cabo funciones ligeramente diferentes durante el procedimiento de distribución en comparación con el enrutador designado.
- 1 **Other Designated Router** (Otro enrutador designado): la interfaz se conecta a una red NBMA o de difusión en la que se han seleccionado otros enrutadores para ser el enrutador designado y el enrutador designado de reserva. El enrutador intenta formar adyacencias tanto con el enrutador designado como con el enrutador designado de reserva.

Neighbor State (Estado de vecino): estado de la relación de vecino virtual.

Retransmit Interval (Intervalo de retransmisión): introduzca el intervalo de retransmisión de OSPF para la interfaz especificada. Se trata del número de segundos transcurridos entre los anuncios de estado de enlace correspondientes a las adyacencias de esta interfaz de enrutador. Este valor también se utiliza al retransmitir descripciones de bases de datos y paquetes de petición de estado de enlace. Los valores válidos están comprendidos entre 1 y 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

Metric (Métrica): valor de métrica que utiliza el enlace virtual.

Delete (Eliminar): elimina el enlace virtual especificado de la configuración del enrutador.

Creación de un nuevo enlace virtual

1. Abra la página OSPFv3 Virtual Link Configuration (Configuración de enlace virtual OSPFv3).
2. Seleccione **Create New Virtual Link** (Crear nuevo enlace virtual) en el menú desplegable para definir un nuevo enlace virtual.
3. Introduzca la ID de enrutador de vecino.
4. Haga clic en **Create** (Crear).

Se crea el enlace y se abre de nuevo la página de configuración de enlace virtual.

Configuración de un enlace virtual

1. Abra la página OSPFv3 Virtual Link Configuration (Configuración de enlace virtual OSPFv3).
2. Seleccione el enlace virtual que desea configurar.
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).
5. Se configura el enlace virtual de OSPFv3 y se actualiza el dispositivo.

Configuración de un enlace virtual OSPFv3 mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

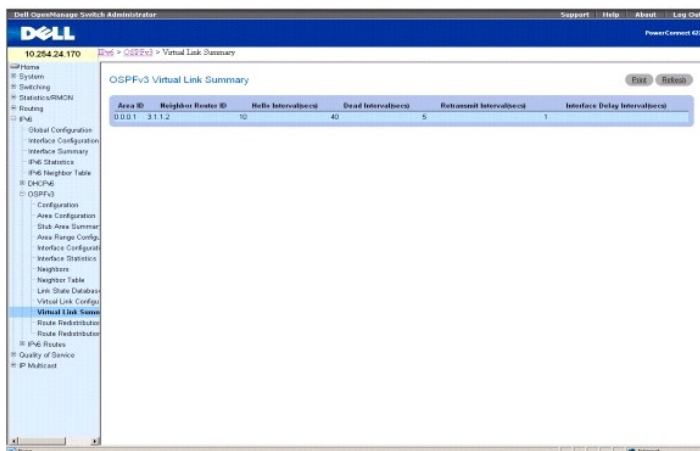
- 1 Comandos OSPFv3

Resumen de enlaces virtuales OSPFv3

Utilice la página OSPFv3 Virtual Link Summary (Resumen de enlaces virtuales OSPFv3) para visualizar los datos de enlaces virtuales por ID de área e ID de enrutador de vecino.

Para visualizar la página, haga clic en IPv6 → OSPFv3 → Virtual Link Summary (Resumen de enlaces virtuales) en la vista de árbol.

Ilustración 11-29. Resumen de enlaces virtuales OSPFv3



Area ID	Neighbor Router ID	Hello Interval (secs)	Dead Interval (secs)	Retransmit Interval (secs)	Interface Delay Interval (secs)
0001	3112	10	40	5	1

La página OSPFv3 Virtual Link Summary (Resumen de enlaces virtuales OSPFv3) contiene los campos siguientes:

Area ID (ID de área): parte correspondiente a la ID de área dentro de la identificación del enlace virtual cuyos datos desea visualizar. La ID de área define, junto con la ID de enrutador de vecino, un enlace virtual.

Neighbor Router ID (ID de enrutador de vecino): parte correspondiente al vecino dentro de la identificación del enlace virtual. Es posible configurar enlaces virtuales entre cualquier par de enrutadores de límite de área que tengan interfaces a un área (no de red troncal) común.

Hello Interval (secs) (Intervalo de saludo [seg.]): intervalo de saludo de OSPF del enlace virtual en unidades de segundos. El valor del intervalo de saludo debe ser el mismo para todos los enrutadores asociados a una red.

Dead Interval (secs) (Intervalo de finalización [seg.]): intervalo de finalización de OSPF del enlace virtual en unidades de segundos. Este intervalo corresponde al tiempo que el enrutador debe esperar a ver los paquetes de saludo de un enrutador de vecino antes de declarar que el enrutador está fuera de servicio. Este parámetro debe ser igual para todos los enrutadores conectados a una red común y debe ser un múltiplo del intervalo de saludo (por ejemplo, 4).

Retransmit Interval (secs) (Intervalo de retransmisión [seg.]): intervalo de retransmisión de OSPF del enlace virtual en unidades de segundos. Se trata del tiempo transcurrido entre los anuncios de estado de enlace correspondientes a las adyacencias de esta interfaz de enrutador. Este valor también se utiliza al retransmitir descripciones de bases de datos y paquetes de petición de estado de enlace.

Interface Delay Interval (secs) (Intervalo de demora de la interfaz [seg.]): demora de transmisión de OSPF del enlace virtual en unidades de segundos. Este intervalo corresponde al número estimado de segundos que se tarda en transmitir un paquete de actualización de estado de enlace en esta interfaz.

Visualización del resumen de enlaces virtuales OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

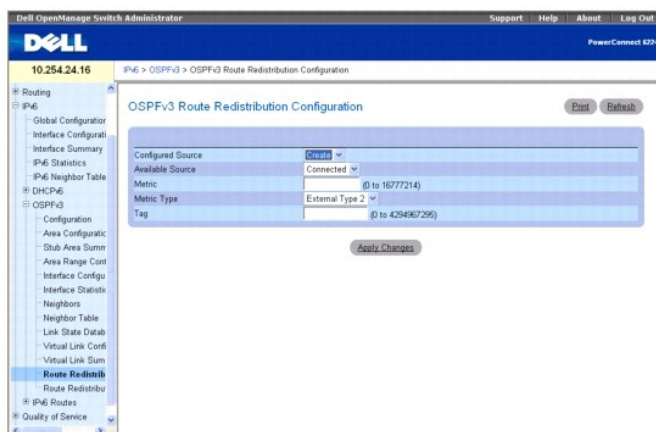
- 1 Comandos OSPFv3

Configuración de redistribución de rutas OSPFv3

Utilice la página OSPFv3 Route Redistribution Configuration (Configuración de redistribución de rutas OSPFv3) para configurar la redistribución de rutas.

Para visualizar la página, haga clic en IPv6 → OSPFv3 → Route Redistribution Configuration (Configuración de redistribución de rutas) en la vista de árbol.

Ilustración 11-30. Configuración de redistribución de rutas OSPFv3



La página OSPFv3 Route Redistribution Configuration (Configuración de redistribución de rutas OSPFv3) contiene los campos siguientes:

Configured Source (Origen configurado): este menú desplegable es un selector dinámico que sólo muestra las rutas de origen configuradas para redistribuirse mediante OSPF. La primera opción de la casilla de selección es Create (Crear) que sirve para configurar otra ruta de origen entre las rutas de origen disponibles. Los valores posibles son Static (Estático), Connected (Conectado) y Create (Crear).

Available Source (Origen disponible): este menú desplegable es un selector dinámico que sólo muestra las rutas de origen que no se han configurado previamente para redistribuirse mediante OSPF. Este menú sólo aparece si selecciona la opción Create (Crear) para Configured Source (Origen configurado). Los valores posibles son Static (Estático) y Connected (Conectado).

Metric (Métrica): establece el valor de métrica que se utilizará como métrica de las rutas redistribuidas. Este campo muestra la métrica si se ha configurado previamente el origen, y puede modificarse. Los valores válidos están comprendidos entre 0 y 16777214.

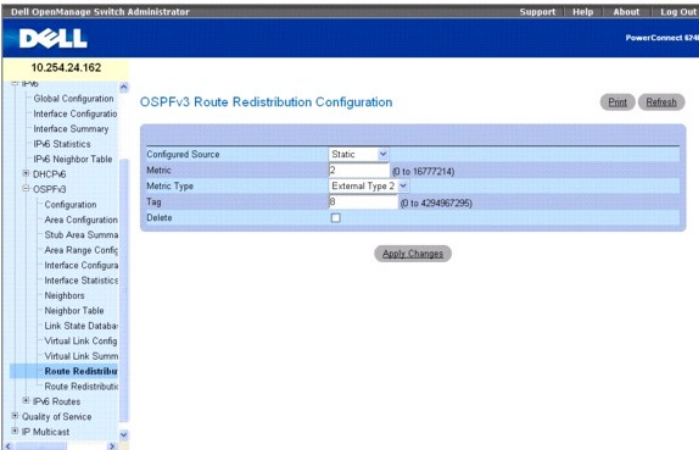
Metric Type (Tipo de métrica): establece el tipo de métrica de OSPF de las rutas redistribuidas.

Tag (Etiqueta): establece el campo de etiqueta en las rutas redistribuidas. Este campo muestra la etiqueta si se ha configurado previamente el origen; de lo contrario, se muestra el valor 0. Los valores válidos están comprendidos entre 0 y 4294967295.

Configuración de la redistribución de rutas OSPFv3

1. Abra la página OSPFv3 Route Redistribution Configuration (Configuración de redistribución de rutas OSPFv3).
2. Especifique **Create** (Crear) para instalar un nuevo origen configurado o bien seleccione **Connected** (Conectado) o **Static** (Estático) para modificar un origen configurado existente.

Ilustración 11-31. Configuración de redistribución de rutas OSPFv3 - Origen configurado



3. Configure o modifique los campos restantes según sea necesario.

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

Se configura la redistribución de rutas seleccionadas de OSPFv3 y se actualiza el dispositivo.

Configuración de redistribución de rutas OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

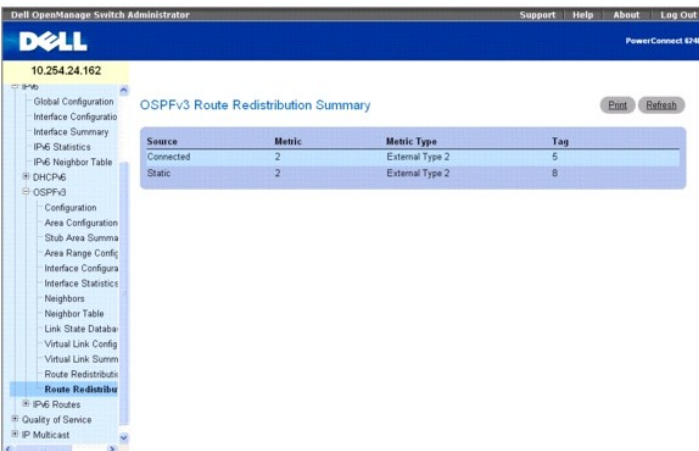
1 Comandos OSPFv3

Resumen de redistribución de rutas OSPFv3

Utilice la página OSPFv3 Route Redistribution Summary (Resumen de redistribución de rutas OSPFv3) para ver la configuración de la redistribución de rutas por origen.

Para visualizar la página, haga clic en IPv6 → OSPFv3 → Route Redistribution Summary (Resumen de redistribución de rutas) en la vista de árbol.

Ilustración 11-32. Resumen de redistribución de rutas OSPFv3



La página OSPFv3 Route Redistribution Summary (Resumen de redistribución de rutas OSPFv3) contiene los campos siguientes:

Source (Origen): ruta de origen que se redistribuirá mediante OSPF.

Metric (Métrica): métrica de rutas redistribuidas para la ruta de origen especificada. Cuando no está configurada, se muestra Unconfigured (Sin configurar).

Metric Type (Tipo de métrica): tipo de métrica OSPF de las rutas redistribuidas.

Tag (Etiqueta): campo de etiqueta de las rutas redistribuidas. Este campo muestra la etiqueta si se ha configurado previamente el origen; de lo contrario, se muestra el valor 0.

Visualización del resumen de redistribución de rutas OSPFv3 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos OSPFv3

Rutas IPv6

La página de menú **IPv6 Routes** (Rutas IPv6) contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de las rutas IPv6. Para visualizar la página, haga clic en **IPv6** → **IPv6 Routes** (Rutas IPv6) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

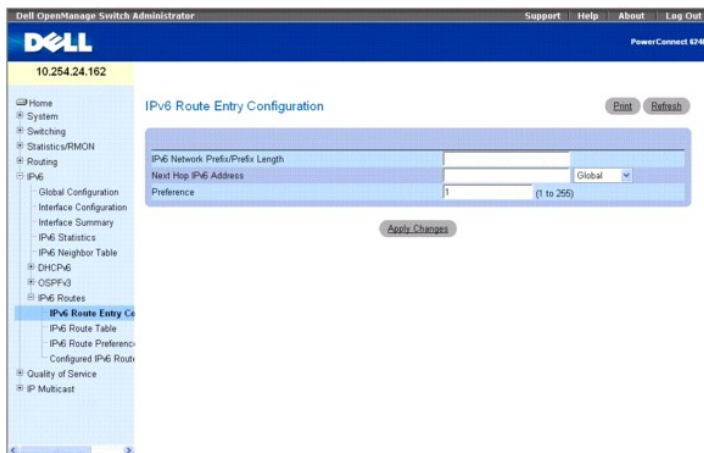
- 1 [Configuración de entradas de ruta IPv6](#)
- 1 [Tabla de rutas IPv6](#)
- 1 [Preferencias de ruta IPv6](#)
- 1 [Rutas IPv6 configuradas](#)

Configuración de entradas de ruta IPv6

Utilice la página **IPv6 Route Entry Configuration** (Configuración de entradas de ruta IPv6) para configurar la información de las rutas IPv6.

Para visualizar la página, haga clic en **IPv6** → **IPv6 Routes** (Rutas IPv6) → **IPv6 Route Entry Configuration** (Configuración de entradas de ruta IPv6) en la vista de árbol.

Ilustración 11-33. Configuración de entradas de ruta IPv6



La página **IPv6 Route Entry Configuration** (Configuración de entradas de ruta IPv6) contiene los campos siguientes:

IPv6 Network Prefix/PrefixLength (Prefijo de red/Longitud de prefijo IPv6): introduzca un prefijo y una dirección de red IPv6 válidos.

Next Hop IPv6 Address (Dirección IPv6 del siguiente salto): introduzca una dirección del siguiente salto de IPv6. Si la dirección IPv6 del siguiente salto especificada es una dirección IPv6 local de enlace, especifique la interfaz de la dirección del siguiente salto IPv6 local de enlace. En el menú desplegable, seleccione el valor **Global** o **Link-local** (Local de enlace) que se aplicará a esta dirección.

Preference (Preferencia): introduzca un valor de preferencia para la ruta designada. Los valores válidos están comprendidos entre 1 y 255. El valor predeterminado es 1.

Configuración de entradas de ruta IPv6

1. Abra la página **IPv6 Route Entry Configuration** (Configuración de entradas de ruta IPv6).
2. Modifique los campos necesarios.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se configura las entradas de ruta de IPv6 y se actualiza el dispositivo.

Configuración de entradas de ruta mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

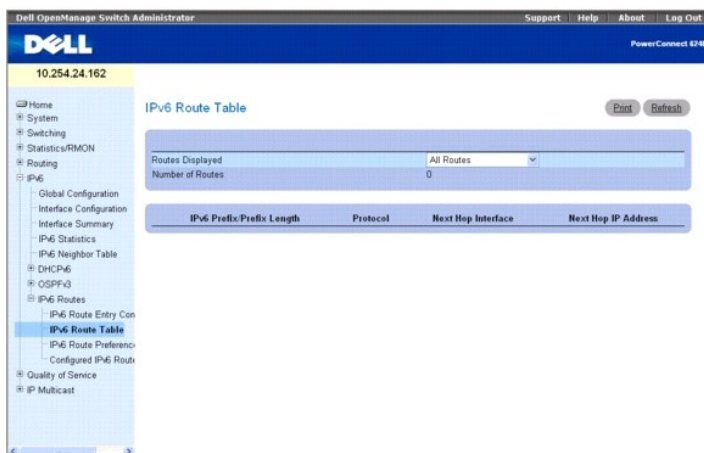
- 1 Comandos de enrutamiento IPv6

Tabla de rutas IPv6

Utilice la página **IPv6 Route Table** (Tabla de rutas IPv6) para visualizar todas las rutas IPv6 activas y sus configuraciones.

Para visualizar la página, haga clic en **IPv6** → **IPv6 Routes (Rutas IPv6)** → **IPv6 Route Table** (Tabla de rutas IPv6) en la vista de árbol.

Ilustración 11-34. Tabla de rutas IPv6



La página **IPv6 Route Table** (Tabla de rutas IPv6) contiene los campos siguientes:

Routes Displayed (Rutas mostradas): en el menú desplegable, seleccione si desea ver las rutas configuradas, las mejores rutas o todas las rutas.

Number of Routes (Número de rutas): muestra el número total de rutas activas y las mejores rutas del tipo seleccionado que se encuentran en la tabla de rutas.

IPv6 Prefix/Prefix Length (Prefijo/Longitud de prefijo IPv6): muestra la longitud de prefijo y el prefijo de red correspondiente a la ruta activa.

Protocol (Protocolo): muestra el tipo de protocolo de la ruta activa.

Next Hop Interface (Interfaz del siguiente salto): muestra la interfaz en la que está activa la ruta.

Next Hop IPv6 Address (Dirección IPv6 del siguiente salto): muestra la dirección IPv6 del siguiente salto correspondiente a la ruta activa.

Visualización de la tabla de rutas IPv6

1. Abra la página **IPv6 RouteTable** (Tabla de rutas IPv6).
2. Seleccione el tipo de rutas que se visualizarán en el campo **Routes Displayed** (Rutas mostradas).

Aparecen las rutas seleccionadas.

Visualización de la tabla de rutas IPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de enrutamiento IPv6

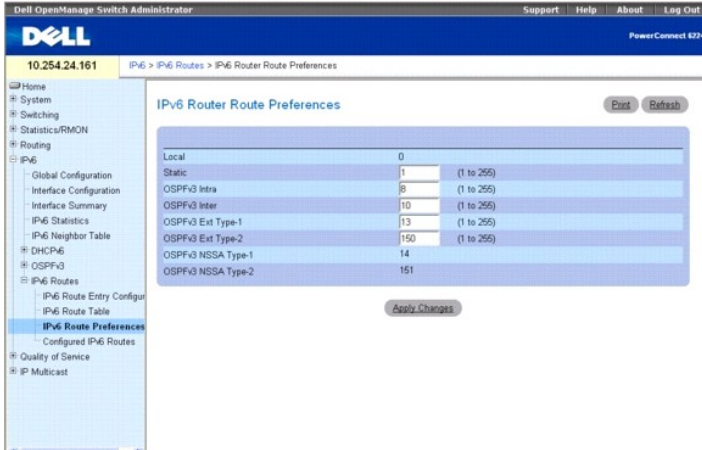
Preferencias de ruta IPv6

Utilice la página **IPv6 Route Preferences** (Preferencias de ruta IPv6) para configurar la preferencia predeterminada de cada protocolo. Se trata de valores

arbitrarios comprendidos entre 1 y 255 independientes de la métrica de ruta. La mayoría de los protocolos de enrutamiento utilizan una métrica de ruta para determinar la ruta de acceso más corta, independiente de cualquier otro protocolo. La mejor ruta a un destino se elige seleccionando la ruta con el valor de preferencia inferior. Cuando existen varias rutas a un destino, los valores de preferencia sirven para determinar la ruta preferida. Si aún así no se sabe cuál es la mejor, se elige la ruta con la mejor métrica. Para evitar problemas con métricas no coincidentes, debe configurar diferentes valores de preferencia para cada uno de los protocolos.

Para visualizar la página, haga clic en **IPv6** → **IPv6 Routes (Rutas IPv6)** → **IPv6 Route Preferences (Preferencias de ruta IPv6)** en la vista de árbol.

Ilustración 11-35. Preferencias de ruta IPv6



La página **IPv6 Route Preferences (Preferencias de ruta IPv6)** contiene los campos que se muestran a continuación. En cada caso, el valor inferior indica la preferencia superior.

Local: muestra la preferencia local y no se puede configurar. El valor es 0, la máxima preferencia.

Static (Estática): valor de preferencia de ruta estática del enrutador. El valor predeterminado es 1. El intervalo es de 1 a 255.

OSPFv3 Intra (Intra-OSPFv3): valor de preferencia de la ruta intra-OSPFv3 del enrutador. El valor predeterminado es 8. El intervalo es de 1 a 255. La especificación de OSPFv3 requiere que se asignen preferencias a las rutas obtenidas mediante OSPFv3 en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPFv3 Inter (Inter-OSPFv3): valor de preferencia de la ruta inter-OSPFv3 del enrutador. El valor predeterminado es 10. El intervalo es de 1 a 255. La especificación de OSPFv3 requiere que se asignen preferencias a las rutas obtenidas mediante OSPFv3 en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPFv3 Type-1 (Tipo 1 OSPFv3): valor de preferencia de la ruta tipo 1 OSPFv3 del enrutador. El valor predeterminado es 13. El intervalo es de 1 a 255. La especificación de OSPFv3 requiere que se asignen preferencias a las rutas obtenidas mediante OSPFv3 en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPFv3 Type-2 (Tipo 2 OSPFv3): valor de preferencia de la ruta tipo 2 OSPFv3 del enrutador. El valor predeterminado es 150. El intervalo es de 1 a 255. La especificación de OSPFv3 requiere que se asignen preferencias a las rutas obtenidas mediante OSPFv3 en el orden siguiente: intra < inter < tipo 1 < tipo 2.

OSPFv3 NSSA Type-1 (Tipo 1 de NSSA OSPFv3): muestra el valor de preferencia de la ruta tipo 1 de NSSA OSPFv3 del enrutador.

OSPFv3 NSSA Type-2 (Tipo 2 de NSSA OSPFv3): muestra el valor de preferencia de la ruta tipo 2 de NSSA OSPFv3 del enrutador.

Configuración de preferencias de ruta IPv6

1. Abra la página **IPv6 Route Preferences (Preferencias de ruta IPv6)**.
2. Configure la preferencia predeterminada para cada protocolo.
3. Haga clic en **Apply Changes (Aplicar cambios)**.

Se configuran las preferencias de ruta para IPv6 y se actualiza el dispositivo.

Configuración de las preferencias de ruta IPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

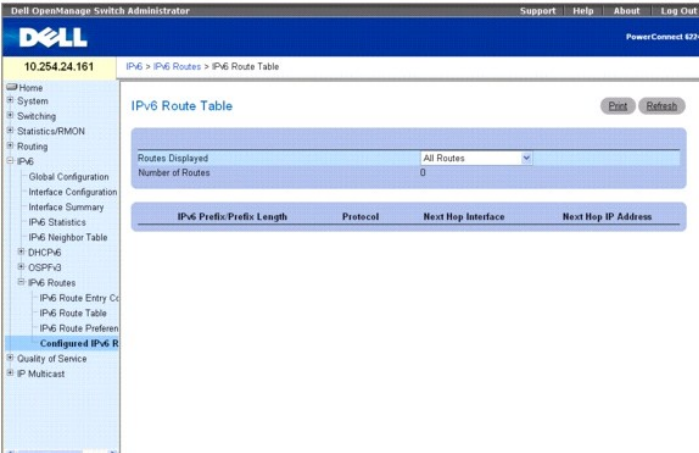
- 1 Comandos de enrutamiento IPv6

Rutas IPv6 configuradas

Utilice la página **Configured IPv6 Routes (Rutas IPv6 configuradas)** para mostrar las rutas IPv6 seleccionadas.

Para visualizar la página, haga clic en **IPv6** → **IPv6 Routes (Rutas IPv6)** → **Configured IPv6 Routes (Rutas IPv6 configuradas)** en la vista de árbol.

Ilustración 11-36. Rutas IPv6 configuradas



La página **Configured IPv6 Routes** (Rutas IPv6 configuradas) contiene los campos siguientes:

Routes Displayed (Rutas mostradas): seleccione si desea ver las rutas configuradas, las mejores rutas o todas las rutas.

Cuando se selecciona la opción **Configured Routes** (Rutas configuradas), se muestran los campos siguientes:

IPv6 Prefix/Prefix Length (Prefijo/Longitud de prefijo IPv6): muestra la longitud de prefijo y el prefijo de red correspondiente a la ruta configurada.

Next Hop IP (IP del siguiente salto): muestra la dirección IPv6 del siguiente salto correspondiente a la ruta configurada.

Next Hop Interface (Interfaz del siguiente salto): muestra la interfaz del siguiente salto correspondiente a la ruta configurada.

Preference (Preferencia): muestra la preferencia de la ruta configurada.

Delete (Eliminar): marque esta casilla y haga clic en el botón **Refresh** (Actualizar) para eliminar la ruta mostrada.

Cuando se seleccionan las opciones **Best Routes** (Mejores rutas) o **All Routes** (Todas las rutas), se muestran los campos siguientes:

Number of Routes (Número de rutas): muestra el número de mejores rutas o de todas las rutas.

IPv6 Prefix/Prefix Length (Prefijo/Longitud de prefijo IPv6): muestra la longitud de prefijo y el prefijo de red correspondiente a la ruta configurada.

Protocol (Protocolo): muestra el protocolo utilizado para las rutas configuradas.

Next Hop Interface (Interfaz del siguiente salto): muestra la interfaz del siguiente salto correspondiente a la ruta configurada.

Next Hop IP Address (Dirección IP del siguiente salto): muestra la dirección IPv6 del siguiente salto correspondiente a la ruta configurada.

Visualización de rutas IPv6

1. Abra la página **Configured IPv6 Routes** (Rutas IPv6 configuradas).
2. En el menú desplegable **Routes Displayed** (Rutas mostradas), seleccione las rutas que desea ver.
Aparecen las rutas seleccionadas y sus configuraciones.

Visualización de las rutas IPv6 mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de enrutamiento IPv6

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de la calidad de servicio

Dell™ PowerConnect™ serie M6220 — Guía del usuario

- [Información general sobre la calidad de servicio](#)
- [Configuración de servicios diferenciados](#)
- [Clase de servicio](#)

En la presente sección se proporciona información general sobre la calidad de servicio (QoS), así como explicaciones sobre las diversas funciones de dicha calidad disponibles en la página de menú Quality of Service (Calidad de servicio): Differentiated Services (Servicios diferenciados) y Class of Service (Clase de servicio).

Información general sobre la calidad de servicio

En un conmutador típico, cada uno de los puertos físicos está formado por una o más colas que se encargan de la transmisión de paquetes en la red conectada. A menudo se proporcionan diversas colas por puerto con la finalidad de otorgar preferencia a determinados paquetes respecto a otros partiendo de criterios definidos por el usuario. Cuando un paquete se coloca en la cola para su transmisión en un puerto, la velocidad a la que se entrega depende del método de configuración de dicha cola y, posiblemente, de la cantidad de tráfico presente en otras colas del puerto. Si se requiere una demora, los paquetes se retienen en la cola hasta que el programador conceda a la cola la autorización necesaria para llevar a cabo la transmisión. A medida que las colas se llenan, no se dispone del espacio necesario para retener la transmisión de los paquetes, y el conmutador los descarta.

Por QoS se entiende el método que permite una entrega de datos previsible y coherente mediante la distinción entre paquetes que presentan unos requisitos de temporización estrictos y los que son más tolerantes frente a demoras. En una red capaz de proporcionar QoS, los paquetes con requisitos de temporización estrictos reciben un "tratamiento especial". Teniendo en cuenta este concepto, todos los elementos de la red deben ser capaces de proporcionar QoS. La presencia de, como mínimo, un nodo que no pueda proporcionar QoS crea una deficiencia en la ruta de acceso a la red y, en consecuencia, el rendimiento del conjunto del flujo de paquetes se ve comprometido.

Para visualizar la página de menú Quality of Service (Calidad de servicio), haga clic en **Quality of Service** (Calidad de servicio) en la vista de árbol. Los dos tipos disponibles de QoS cuentan con enlaces que se encuentran en esta página de menú. Dichos enlaces son:

- 1 [Configuración de servicios diferenciados](#)
- 1 [Clase de servicio](#)

Configuración de servicios diferenciados

Información general sobre los servicios diferenciados

La función de calidad de servicio (QoS) es compatible con los servicios diferenciados (DiffServ) y, por lo tanto, permite clasificar el tráfico en flujos y proporcionarle determinados tratamientos de calidad de servicio según los comportamientos por salto definidos.

Las redes estándar basadas en IP están diseñadas para proporcionar un servicio de entrega de datos de "mejor esfuerzo". La utilización de un servicio de "mejor esfuerzo" implica que la red entregará los datos de forma puntual, aunque no se garantiza que siempre sea así. Durante periodos de congestión, los paquetes pueden estar sujetos a demoras, envíos esporádicos o incluso se pueden llegar a descartar. En las aplicaciones habituales de Internet, como el correo electrónico y la transferencia de archivos, una ligera degradación del servicio es aceptable y, en muchos casos, ni siquiera se llega a percibir. En cambio, toda degradación de servicio que afecte a aplicaciones con requisitos de temporización estrictos, como las de voz o multimedia, conlleva efectos no deseados.

Definición de servicios diferenciados

Para utilizar los servicios diferenciados para QoS, en primer lugar se deben utilizar las páginas web accesibles desde la página de menú **Differentiated Services** (Servicios diferenciados) para definir las categorías siguientes, así como sus criterios:

1. Class (Clase): crea clases y define sus criterios
2. Policy (Política): crea políticas, asocia clases con políticas y define enunciados de políticas
3. Service (Servicio): añade una política a una interfaz entrante

Los paquetes se clasifican y procesan a partir de los criterios definidos. Una clase define los criterios de clasificación. Los atributos de una política son los que definen el procesamiento. Los atributos de políticas se pueden definir para instancias de clases concretas, y son estos atributos los que se aplican cuando se produce una coincidencia. Una política puede contener diversas clases. Cuando una política está activa, las acciones adoptadas dependen de la clase que coincida con el paquete.

El procesamiento de paquetes empieza con una prueba de los criterios de coincidencia de la clase para un paquete. Una política se aplica a un paquete cuando en dicha política se encuentra una coincidencia de clase.

La página de menú **Differentiated Services** (Servicios diferenciados) contiene enlaces a las diversas funciones de visualización y configuración de servicios diferenciados.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) en la vista de árbol. La página de menú **Differentiated Services** (Servicios diferenciados) contiene enlaces a las funciones siguientes:

- 1 [Configuración de servicios diferenciados](#)
- 1 [Configuración de clases](#)
- 1 [Criterios de clases](#)
- 1 [Configuración de políticas](#)
- 1 [Definición de clases de políticas](#)
- 1 [Configuración de servicios](#)
- 1 [Estadísticas detalladas de servicios](#)

Configuración de servicios diferenciados

Utilice la página **Diffserv Configuration** (Configuración de servicios diferenciados) para visualizar la información de grupo de estado general de servicios diferenciados, que incluye la configuración actual del modo administrativo, así como el número actual y máximo de filas de cada una de las tablas MIB privadas de servicios diferenciados principales.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Diffserv Configuration** (Configuración de servicios diferenciados) en el árbol de vista.

Ilustración 12-1. Configuración de servicios diferenciados



La página **Diffserv Configuration** (Configuración de servicios diferenciados) contiene los campos siguientes:

Diffserv Admin Mode (Modo de administración de servicios diferenciados): activa y desactiva el modo de administración. Mientras está desactivado, la configuración de servicios diferenciados se conserva y se puede modificar, pero no está activa. En cambio, mientras está activado, los servicios diferenciados están activos.

Tabla MIB

Class Table (Tabla de clases): muestra el número actual y máximo de filas de la tabla de clases.

Class Rule Table (Tabla de reglas de clases): muestra el número actual y máximo de filas de la tabla de reglas de clases.

Policy Table (Tabla de políticas): muestra el número actual y máximo de filas de la tabla de políticas.

Policy Instance Table (Tabla de instancias de políticas): muestra el número actual y máximo de filas de la tabla de instancias de políticas.

Policy Attributes Table (Tabla de atributos de políticas): muestra el número actual y máximo de filas de la tabla de atributos de políticas.

Service Table (Tabla de servicios): muestra el número actual y máximo de filas de la tabla de servicios.

Cambio del modo de administración de servicios diferenciados

1. Abra la página **Diffserv Configuration** (Configuración de servicios diferenciados).
2. Active o desactive **Diffserv Admin Mode** (Modo de administración de servicios diferenciados) al seleccionar **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se modifica el modo de administración de servicios diferenciados y se actualiza el dispositivo.

Visualización de las tablas MIB mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

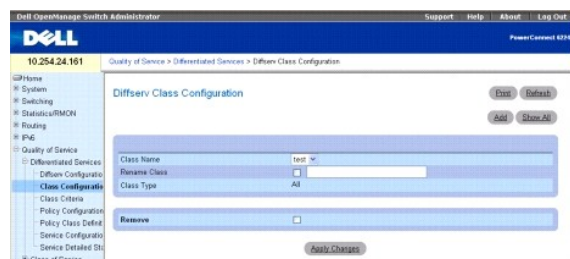
- 1 Comandos de QoS

Configuración de clases

Utilice la página **Diffserv Class Configuration** (Configuración de clases de servicios diferenciados) para añadir un nuevo nombre de clase de servicios diferenciados o para cambiar o eliminar el nombre de una clase existente.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Class Configuration** (Configuración de clases) en el árbol de vista.

Ilustración 12-2. Configuración de clases de servicios diferenciados



La página **Diffserv Class Configuration** (Configuración de clases de servicios diferenciados) contiene los campos siguientes:

Class Name (Nombre de clase): selecciona un nombre de clase para cambiarlo o eliminarlo. Haga clic en **Add** (Añadir) para configurar un nuevo nombre de clase.

Rename Class (Cambiar nombre de clase): al marcar esta casilla e introducir un nuevo nombre, se cambia el nombre de la clase mostrada.

Class Type (Tipo de clase): enumera todos los tipos de clases. Actualmente, el único valor de **Class Type** (Tipo de clase) que admite el hardware es **All** (Todos).

All (Todos): todos los diversos criterios de coincidencia definidos para la clase se deben cumplir para una coincidencia de paquete. **All** (Todos) significa el **Y** lógico de todos los criterios de coincidencia.

Remove (Eliminar): elimina el nombre de clase mostrado al seleccionarlo y hacer clic en **Apply Changes** (Aplicar cambios).

Cambio de nombre de una configuración de clases

1. Abra la página **Class Configuration** (Configuración de clases).
2. Seleccione el nombre de la clase que desea cambiar en el menú desplegable **Class Name** (Nombre de clase).
3. Haga clic en la casilla **Rename Class** (Cambiar nombre de clase) y, a continuación, escriba el nuevo nombre en el campo adyacente.
4. Haga clic en **Apply Changes** (Aplicar cambios).

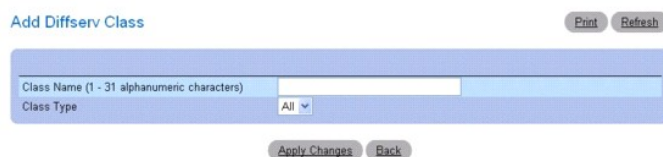
Se modifica el nombre de la configuración de clases y se actualiza el dispositivo.

Adición de una configuración de clases de servicios diferenciados

1. Abra la página **Class Configuration** (Configuración de clases).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add Diffserv Class** (Añadir clase de servicios diferenciados).

Ilustración 12-3. Adición de clase de servicios diferenciados



3. Escriba el nuevo nombre en el campo **Class Name** (Nombre de clase).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añade el nombre de clase y se actualiza el dispositivo.

Eliminación de una configuración de clases

1. Abra la página **Class Configuration** (Configuración de clases).
2. Seleccione el nombre de la clase que desea eliminar en el menú desplegable **Class Name** (Nombre de clase).
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la configuración de clases asociada y se actualiza el dispositivo.

Visualización de configuraciones de clases

1. Abra la página **Class Configuration** (Configuración de clases).
2. Haga clic en **Show All** (Mostrar todo).

Todas las configuraciones de clases se muestran en la página **Diffserv Class Summary** (Resumen de clases de servicios diferenciados).

Ilustración 12-4. Resumen de clases de servicios diferenciados

	Class Name	Class Type	Reference Class
1	Class B	All	Class A
2	Class A	All	Class A
3	Class C	All	Class B

Adición de una configuración de clases mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de QoS

Criterios de clases

Utilice la página **Diffserv Class Criteria** (Criterios de clases de servicios diferenciados) para definir los criterios que se asociarán a una clase de servicios diferenciados. Estas clases de servicios diferenciados se utilizarán para priorizar los paquetes a medida que se vayan recibiendo.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Class Criteria** (Criterios de clases) en el árbol de vista.

Ilustración 12-5. Criterios de clases de servicios diferenciados

La página **Diffserv Class Criteria** (Criterios de clases de servicios diferenciados) contiene los campos siguientes:

Class Name (Nombre de clase): selecciona el nombre de la clase para la que se especifican criterios.

Class Type (Tipo de clase): muestra el tipo de clase. El único tipo de clase admitido que se puede configurar es **All** (Todos).

Coincidencia con atributos

Utilice los campos siguientes para establecer coincidencias entre paquetes y una clase. Haga clic en la casilla de verificación para cada campo que se deba utilizar como criterio para una clase e introduzca los datos en el campo correspondiente. Puede disponer de múltiples criterios de coincidencia para una misma clase. La lógica es una "Y lógica" booleana para estos criterios.

Source IP Address (Dirección IP de origen): requiere que la dirección IP del puerto de origen de un paquete coincida con la dirección aquí indicada.

Subnet Mask (Máscara de subred): máscara de subred de la dirección IP de origen. Este campo es necesario cuando se ha seleccionado la opción **Source IP Address** (Dirección IP de origen).

Destination IP Address (Dirección IP de destino): requiere que la dirección IP del puerto de destino del paquete coincida con la dirección aquí indicada.

Subnet Mask (Máscara de subred): máscara de subred de la dirección IP de destino. Este campo es necesario cuando se ha seleccionado la opción **Destination IP Address** (Dirección IP de destino).

Source L4 Port (Puerto L4 de origen): requiere que el puerto de origen TCP/UDP de un paquete coincida con el puerto aquí indicado. Seleccione una de las opciones siguientes:

Select From List (Seleccionar de la lista): haga clic para realizar una selección de una lista de puertos de origen muy conocidos con los que deben coincidir los paquetes.

Match to Port (Coincidir con puerto): haga clic aquí para añadir una ID de puerto definida por el usuario con la que deben coincidir los paquetes.

Destination L4 Port (Puerto L4 de destino): requiere que el puerto de destino TCP/UDP de un paquete coincida con el puerto aquí indicado. Seleccione una de las opciones siguientes:

Select From List (Seleccionar de la lista): realice una selección de una lista de puertos de destino muy conocidos con los que deben coincidir los paquetes.

Match to Port (Coincidir con puerto): haga clic aquí para añadir una ID de puerto definida por el usuario con la que deben coincidir los paquetes.

Protocol (Protocolo): requiere que el protocolo de un paquete coincida con el protocolo aquí indicado. Seleccione una de las opciones siguientes:

Select from List (Seleccionar de la lista): realice una selección en la lista desplegable de protocolos.

Match to Protocol ID (Coincidir con ID de protocolo): introduzca una ID de protocolo con la que deberán coincidir los paquetes.

EtherType: requiere que el valor EtherType de la trama coincida con el valor EtherType aquí indicado. Seleccione una de las opciones siguientes:

Select from List (Seleccionar de la lista): realice una selección en la lista desplegable de valores Ethertype.

Match to Port (Coincidir con puerto): introduzca una ID de EtherType con la que deberán coincidir los paquetes.

Class of Service (CoS) (Clase de servicio): requiere que la CoS del paquete para paquetes entrantes coincida con la CoS aquí indicada.

Source MAC Address (Dirección MAC de origen): requiere que la dirección MAC de origen del paquete para paquetes entrantes coincida con la dirección aquí

indicada.

Source MAC Mask (Máscara MAC de origen): especifica la máscara comodín de la dirección MAC de origen. Las máscaras comodín determinan qué bits se utilizan y cuáles se ignoran. Una máscara comodín con el valor 255.255.255.255 indica que ningún bit es importante. En cambio, un comodín con el valor 0.0.0.0 indica que todos los bits son importantes. Este campo es necesario cuando se ha seleccionado la opción **Source MAC Address** (Dirección MAC de origen).

Destination MAC Address (Dirección MAC de destino): requiere que la dirección MAC de destino del paquete para paquetes entrantes coincida con la dirección aquí indicada.

Destination MAC Mask (Máscara MAC de destino): especifica la máscara comodín de la dirección MAC de destino. Las máscaras comodín determinan qué bits se utilizan y cuáles se ignoran. Una máscara comodín con el valor 255.255.255.255 indica que ningún bit es importante. En cambio, un comodín con el valor 0.0.0.0 indica que todos los bits son importantes. Este campo es necesario cuando se ha seleccionado la opción **Destination MAC Address** (Dirección MAC de destino).

VLAN ID (ID de VLAN): requiere que la ID de VLAN del paquete para paquetes entrantes coincida con la ID de VLAN aquí indicada.

Secondary VLAN ID (ID de VLAN secundaria): requiere que la ID de VLAN secundaria del paquete para paquetes entrantes coincida con la ID de VLAN aquí indicada.

Reference Class (Clase de referencia): selecciona una clase para iniciar la creación de referencias para criterios. Seleccione la casilla de verificación **Add Diffserv Class** (Añadir clase de servicios diferenciados) y, a continuación, seleccione una clase de servicios diferenciados configurada previamente del menú desplegable relacionado:

Crterios de tipo de servicio

Haga clic para seleccionar uno de los tres campos de coincidencia siguientes para utilizarlo en las coincidencias de paquetes con los criterios de clase:

IP DSCP (DSCP de IP): cuando se selecciona esta opción, se establece una coincidencia entre el punto de código de servicios diferenciados (DSCP) del paquete y los criterios de la clase. Puede seleccionar el tipo de DSCP del menú desplegable o bien puede introducir un valor de DSCP para establecer la coincidencia.

IP Precedence (Precedencia IP): al seleccionar esta opción e introducir un valor, se establece una coincidencia entre el valor de precedencia IP del paquete y los criterios de la clase.

IP TOS Bits (Bits TOS de IP): al seleccionar esta opción e introducir un valor, se establece una coincidencia entre los bits de tipo de servicio del paquete del encabezado IP y los criterios de la clase.

Match Every (Coincidir con todos): al seleccionar esta opción, el paquete debe coincidir con todos los criterios.

Definición de criterios de clases

1. Abra la página **Diffserv Class Criteria** (Criterios de clases de servicios diferenciados).
2. En el menú desplegable, seleccione el **Class Name** (Nombre de clase) para la que está introduciendo los atributos de coincidencia.
3. Seleccione los atributos con los que se deben establecer las coincidencias para esta clase y especifique sus criterios.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se añaden los criterios a esta clase y se actualiza el dispositivo.

Configuración de criterios de clases mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

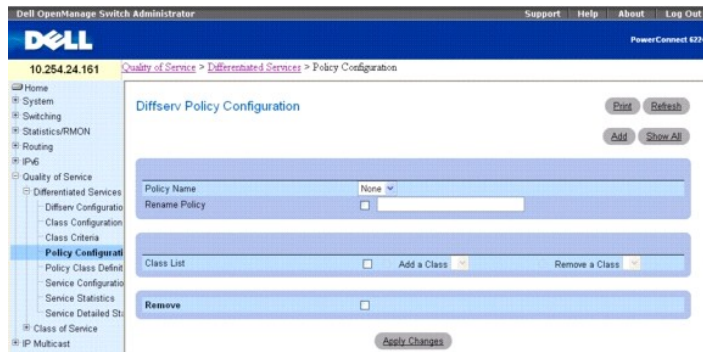
- 1 Comandos de QoS

Configuración de políticas

Utilice la página **Diffserv Policy Configuration** (Configuración de políticas de servicios diferenciados) para asociar un conjunto de clases con uno o varios enunciados de políticas.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Policy Configuration** (Configuración de políticas) en el árbol de vista.

Ilustración 12-6. Configuración de políticas de servicios diferenciados



La página **Diffserv Policy Configuration** (Configuración de políticas de servicios diferenciados) contiene los campos siguientes:

Policy Name (Nombre de política): selecciona el nombre de la política que se asociará con la clase o clases.

Rename Policy (Cambiar nombre de política): al seleccionar esta casilla, introducir un nuevo nombre y hacer clic en **Apply Changes** (Aplicar cambios), se cambia el nombre de la política en cuestión.

Class List (Lista de clases): configura la asociación de clases para la política.

Add a Class (Añadir una clase): asocia la clase seleccionada en el menú desplegable con una política.

Remove a Class (Eliminar una clase): elimina la clase seleccionada de la política.

Remove (Eliminar): elimina el nombre de la política seleccionado del dispositivo.

Asociación de una clase con una política o eliminación de la asociación

1. Abra la página **Diffserv Policy Configuration** (Configuración de políticas de servicios diferenciados).
2. Seleccione el nombre de política que se asociará con la clase.
3. En el campo **Class List** (Lista de clases), seleccione la casilla de verificación y, a continuación, haga clic en el botón de radio **Add a Class** (Añadir una clase) o **Remove a Class** (Eliminar una clase) y seleccione la clase en el menú desplegable relacionado.
Utilice **Add a Class** (Añadir una clase) para asociar dicha clase con esta política. Utilice **Remove a Class** (Eliminar una clase) para eliminar dicha clase de esta política.
4. En el menú desplegable, seleccione la clase en la que se efectuarán los cambios.
5. Haga clic en **Apply Changes** (Aplicar cambios).
Se guarda la política modificada y se actualiza el dispositivo.

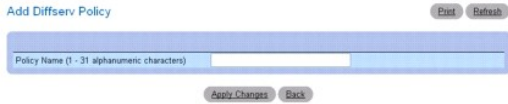
Cambio de nombre de una política

1. Abra la página **Diffserv Policy Configuration** (Configuración de políticas de servicios diferenciados).
2. Seleccione el nombre de la política que desee cambiar.
3. Para realizar el cambio, seleccione **Rename Policy** (Cambiar nombre de política) e introduzca el nuevo nombre en el campo adyacente.
Se guarda el nombre modificado de la política y se actualiza el dispositivo.

Adición de un nuevo nombre de política

1. Abra la página **Diffserv Policy Configuration** (Configuración de políticas de servicios diferenciados).
2. Haga clic en **Add** (Añadir).
Aparece la página **Add Diffserv Policy** (Añadir política de servicios diferenciados).

Ilustración 12-7. Adición de política de servicios diferenciados



3. Introduzca el nuevo nombre de política.
4. Haga clic en **Apply Changes** (Aplicar cambios).
Se guarda la nueva política y se actualiza el dispositivo.

Visualización del resumen de políticas

1. Abra la página **Policy Configuration** (Configuración de políticas).
2. Haga clic en **Show All** (Mostrar todo).

La página **Diffserv Policy Summary** (Resumen de políticas de servicios diferenciados) muestra todos los nombres de políticas, sus tipos de política, así como las clases de miembros.

Ilustración 12-8. Resumen de políticas de servicios diferenciados



Eliminación de una configuración de política

1. Abra la página **Diffserv Policy Configuration** (Configuración de políticas de servicios diferenciados).
2. Seleccione el nombre de la política que desea eliminar del menú desplegable **Policy Name** (Nombre de política).
3. Marque la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la configuración de la política asociada y se actualiza el dispositivo.

Definición de configuraciones de políticas mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

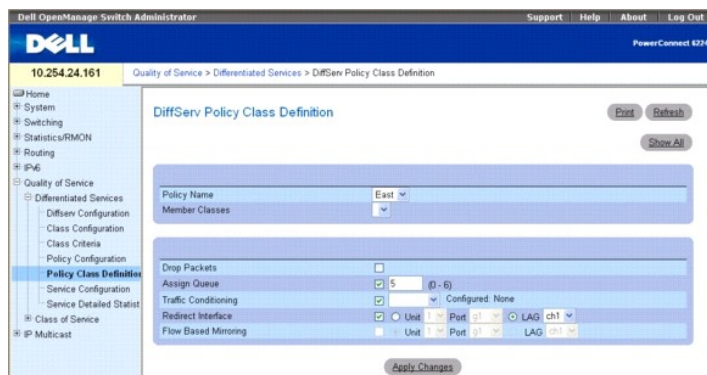
- 1 Comandos de QoS

Definición de clases de políticas

Utilice la página **Diffserv Policy Class Definition** (Definición de clases de políticas de servicios diferenciados) para asociar una clase a una política, así como para definir los atributos para la instancia de clase de política en cuestión.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Policy Class Definition** (Definición de clases de políticas) en el árbol de vista.

Ilustración 12-9. Definición de clases de políticas de servicios diferenciados



La página **Diffserv Policy Class Definition** (Definición de clases de políticas de servicios diferenciados) contiene los campos siguientes:

Policy Name (Nombre de política): selecciona la política que se asociará con una clase de miembro de un menú desplegable.

Member Classes (Clases de miembros): selecciona la clase de miembro que se asociará con este nombre de política de un menú desplegable.

Drop Packets (Descartar paquetes): seleccione este campo para descartar paquetes para esta clase de política.

Assign Queue (Asignar cola): asigna los paquetes de esta clase de política a una cola. El intervalo válido es de 0 a 6.

Traffic Conditioning (Condicionamiento de tráfico): al marcar esta opción y seleccionar una condición del menú desplegable, se asigna un tipo de condicionamiento de tráfico. Este campo afecta al tratamiento que recibe el tráfico que coincide con esta clase de política. Elija entre **None** (Ninguno), **Marking** (Marcado) y **Policing** (Aplicación de políticas). Cuando se selecciona **Marking** (Marcado) o **Policing** (Aplicación de políticas), la pantalla cambia para mostrar los campos correspondientes.

1. **None** (Ninguno): no especifica ningún condicionamiento de tráfico durante el procesamiento de paquetes. Ésta es la opción predeterminada.
1. **Marking** (Marcado): permite marcar uno de los campos siguientes en el paquete: IP DSCP (DSCP de IP), IP Precedence (Precedencia IP) o Class of Service (Clase de servicio). Para obtener más información sobre los campos que se muestran al seleccionar **Marking** (Marcado), consulte "[Condición del tráfico de marcado de paquetes](#)".
1. **Policing** (Aplicación de políticas): permite configurar el método de aplicación de políticas, así como el tratamiento que se brinda a los paquetes que se considera que cumplen y no cumplen las especificaciones. Para obtener más información sobre los campos que se muestran al seleccionar **Policing** (Aplicación de políticas), consulte "[Aplicación de políticas a la condición del tráfico](#)".

Redirect Interface (Redirigir interfaz): muestra si esta opción es aplicable a la clase de política en cuestión y especifica la interfaz o el LAG utilizados.

Flow Based Mirroring (Duplicación basada en flujo): muestra si esta opción es aplicable a la clase de política en cuestión y especifica la interfaz o el LAG utilizados.

Definición de una instancia de clase de política

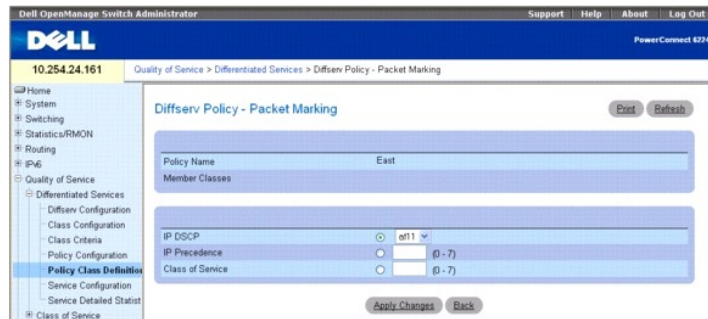
1. Abra la página **Diffserv Policy Class Definition** (Definición de clases de políticas de servicios diferenciados).
2. Seleccione la política y la clase de miembro que se asociarán.
3. Especifique los atributos que se aplicarán a esta instancia de clase de política mediante la utilización del resto de campos de la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la clase de política y se actualiza el dispositivo.

Condición del tráfico de marcado de paquetes

Al seleccionar **Marking** (Marcado) como **Traffic Condition** (Condición de tráfico), se muestra la página **Packet Marking** (Marcado de paquetes) siguiente.

Ilustración 12-10. Definición de clases de políticas - Marcado de paquetes



La página **Diffserv Policy - Packet Marking** (Política de servicios diferenciados - Marcado de paquetes) contiene los campos siguientes:

Policy Name (Nombre de política): muestra la política asociada con una clase de miembro.

Member Classes (Clases de miembros): muestra la clase de miembro asociada con este nombre de política.

Asimismo, tiene la posibilidad de marcar uno de los campos siguientes en el paquete:

IP DSCP (DSCP de IP): selecciona el DSCP de IP que se marcará. Puede seleccionarlo del menú desplegable o bien puede introducirlo directamente en el campo User Value (Valor de usuario).

IP Precedence (Precedencia IP): selecciona el número de cola de precedencia IP especificado que se marcará.

Class of Service (Clase de servicio): selecciona el número de cola de clase de servicio especificado que se marcará.

Configuración de marcado de paquetes para una instancia de clase de política

1. Seleccione **Marking** (Marcado) en el menú desplegable **Traffic Conditioning** (Condicionamiento de tráfico) en la página **Diffserv Policy Class Definition** (Definición de clases de políticas de servicios diferenciados).

La página **Packet Marking** (Marcado de paquetes) se muestra tal como aparece en la [ilustración 12-10](#).

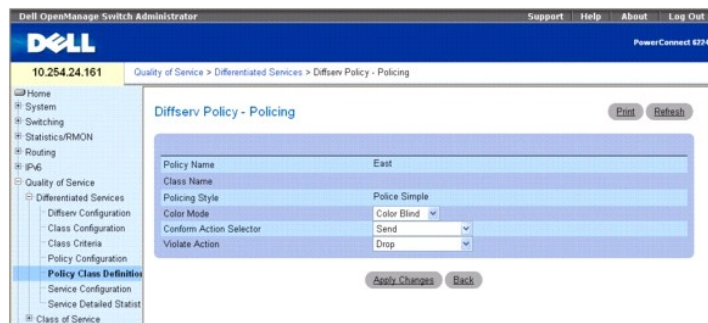
2. Seleccione **IP DSCP** (DSCP de IP), **IP Precedence** (Precedencia IP) o **Class of Service** (Clase de servicio) para realizar el marcado de esta clase de política.
3. Seleccione un valor o introdúzcalo directamente para este campo.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se define la clase de política y se actualiza el dispositivo.

Aplicación de políticas a la condición del tráfico

Al seleccionar **Policing** (Aplicación de políticas) como **Traffic Condition** (Condición de tráfico), se muestra la página **Diffserv Policy - Policing** (Política de servicios diferenciados - Aplicación de políticas) siguiente.

Ilustración 12-11. Definición de clases de políticas - Aplicación de políticas



La página **Diffserv Policy - Policing** (Política de servicios diferenciados - Aplicación de políticas) contiene los campos siguientes:

Policy Name (Nombre de política): muestra la política para la que se configura la aplicación de políticas.

Class Name (Nombre de clase): muestra la clase de miembro asociada con este nombre de política.

Policing Style (Estilo de aplicación de políticas): selecciona el estilo de aplicación de políticas que se utiliza.

Color Mode (Modo de color): selecciona el tipo de aplicación de políticas de color que se utiliza. En el menú desplegable, seleccione **Color Blind** (Insensible al color) o **Color Aware** (Sensible al color).

Conform Action Selector (Selector de acciones de cumplimiento): selecciona el tratamiento que se aplica a los paquetes que se considera que cumplen las especificaciones (por debajo de la tasa que marca la directiva). Las opciones disponibles son **Send** (Enviar), **Drop** (Descartar), **Mark CoS** (Marcar Cos), **Mark IP DSCP** (Marcar DSCP de IP) y **Mark IP Precedence** (Marcar precedencia IP).

Violate Action (Acción en caso de infracción): selecciona el tratamiento que se aplica a los paquetes que se considera que no cumplen las especificaciones (por encima de la tasa que marca la directiva). Las opciones disponibles son **Send** (Enviar), **Drop** (Descartar), **Mark CoS** (Marcar Cos), **Mark IP DSCP** (Marcar DSCP de IP) y **Mark IP Precedence** (Marcar precedencia IP).

Configuración de la aplicación de políticas para una instancia de clase de política

1. Seleccione **Policing** (Aplicación de políticas) en el menú desplegable **Traffic Conditioning** (Condicionamiento de tráfico) de la página **Diffserv Policy Class Definition** (Definición de clases de políticas de servicios diferenciados).

La página **Diffserv Policy - Policing** (Política de servicios diferenciados - Aplicación de políticas) se muestra tal como aparece en la [ilustración 12-11](#).

2. Márquela para seleccionar uno o varios criterios de aplicación de políticas que se utilizarán para esta clase de política.
3. Seleccione un valor o introdúzcalo directamente para cada campo seleccionado.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Aparece la página **Policy Rate Configuration** (Configuración de tasas de políticas) siguiente.

Ilustración 12-12. Configuración de tasas de políticas

Policy Name	Esst
Class Name	test
Color Mode	Color Blind
Committed Rate (kbps)	(1 to 4294967295) kbps
Committed Burst Size (kB)	(1 to 128) kBytes
Conform Action	Send
Violate Action	Drop

5. Introduzca los valores de criterios correspondientes para **Committed Rate** (Velocidad asegurada) o **Committed Burst Size** (Tamaño asegurado de ráfaga).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se configura la aplicación de políticas para la instancia de clase de política específica y se actualiza el dispositivo.

Definición de clases de políticas mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

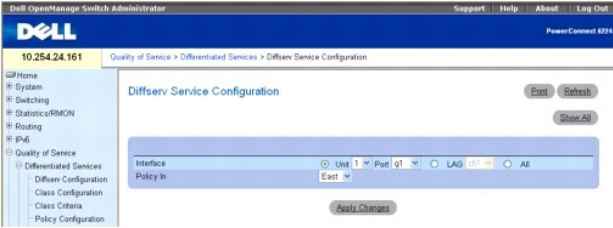
1. Comandos de QoS

Configuración de servicios

Utilice la página **Diffserv Service Configuration** (Configuración de servicios de servicios diferenciados) para activar una política en un puerto.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Service Configuration** (Configuración de servicios) en el árbol de vista.

Ilustración 12-13. Configuración de servicios de servicios diferenciados



La página **Diffserv Service Configuration** (Configuración de servicios de servicios diferenciados) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz (unidad/puerto, LAG o todos) a los que se aplicarán los cambios de los menús desplegables.

Policy In (Política en vigor): selecciona la política que se asociará con el puerto de un menú desplegable.

Activación de una política en un puerto

1. Abra la página **Diffserv Service Configuration** (Configuración de servicios de servicios diferenciados).
2. Seleccione la interfaz de los menús desplegables.
3. Seleccione la política del menú desplegable.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se activa la política en la interfaz y se actualiza el dispositivo.

Visualización del resumen del servicio de servicios diferenciados

1. Abra la página **Diffserv Service Configuration** (Configuración de servicios de servicios diferenciados).
2. Haga clic en **Show All** (Mostrar todo).

Aparece la página **Diffserv Service Summary** (Resumen del servicio de servicios diferenciados).

Ilustración 12-14. Resumen del servicio de servicios diferenciados

Interface	Direction	Operation Status	Policy Name
1/g1	In	Down	East

Asignación de una política a un puerto mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

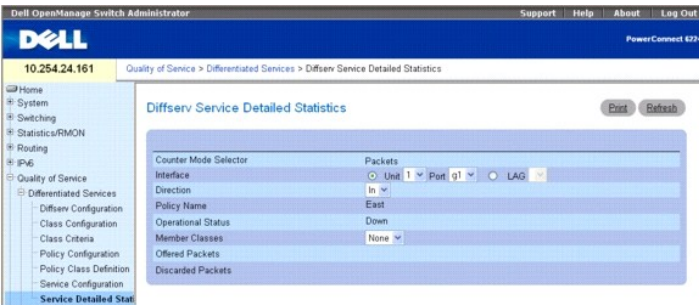
- 1 Comandos de QoS

Estadísticas detalladas de servicios

Utilice la página **Diffserv Service Detailed Statistics** (Estadísticas detalladas de servicios de servicios diferenciados) para mostrar los detalles de paquetes de un puerto y clase particulares.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Differentiated Services** (Servicios diferenciados) → **Service Detailed Statistics** (Estadísticas detalladas de servicios) en el árbol de vista.

Ilustración 12-15. Estadísticas detalladas de servicios de servicios diferenciados



La página **Diffserv Service Detailed Statistics** (Estadísticas detalladas de servicios de servicios diferenciados) contiene los campos siguientes:

Counter Mode Selector (Selector del modo de contador): tipo de estadísticas que se van a mostrar. El único tipo disponible es Packets (Paquetes).

Interface (Interfaz): selecciona la unidad y el puerto o el LAG cuyas estadísticas de servicios se mostrarán.

Direction (Dirección): selecciona la dirección de los paquetes cuyas estadísticas de servicios se mostrarán.

Policy Name (Nombre de política): muestra la política asociada con la interfaz seleccionada.

Operational Status (Estado operativo): muestra si la política está activa en la interfaz en cuestión.

Member Classes (Clases de miembros): selecciona la clase de miembro cuyas estadísticas de octetos se mostrarán.

Offered Packets (Paquetes ofrecidos): muestra la cantidad de paquetes que coinciden con la política.

Discarded Packets (Paquetes descartados): muestra la cantidad de paquetes que la política ha descartado.

Visualización de estadísticas de servicios

1. Abra la página **Diffserv Service Detailed Statistics** (Estadísticas detalladas de servicios de servicios diferenciados).
2. Rellene los campos según convenga.

Se muestran las estadísticas de paquetes de la interfaz, la dirección y la clase especificadas.

Configuración de las estadísticas de servicios mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de QoS

Clase de servicio

La función de envío a la cola de clase de servicio (CoS) permite configurar directamente determinados aspectos del envío a cola de conmutador. Dicha función proporciona el comportamiento de QoS deseado para distintos tipos de tráfico de red cuando no se requieren las complejidades de servicios diferenciados. La prioridad de un paquete que llega a una interfaz se puede utilizar para dirigir el paquete en cuestión a la cola de CoS saliente adecuada a través de una tabla de asignación. Las características de la cola de CoS que afectan a la asignación de cola, como la amplitud de banda mínima garantizada, el modelado de velocidades de transmisión, etcétera, son parámetros que el propio usuario puede configurar en el nivel de la cola o del puerto.

Se admiten hasta siete colas por puerto. Aunque el hardware admite ocho colas, el subsistema de apilamiento siempre reserva una para uso interno.

Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Class of Service** (Clase de servicio) en la vista de árbol. La página de menú **Class of Service** (Clase de servicio) contiene enlaces a las funciones siguientes:

- 1 [Configuración de la tabla de asignación](#)
- 1 [Configuración de interfaz](#)
- 1 [Configuración de la cola de interfaz](#)

Configuración de la tabla de asignación

Todos los puertos del conmutador se pueden configurar para que confíen en uno de los campos de paquete (802.1p, IP Precedence [Precedencia IP] o IP DSCP [DSCP de IP]) o bien para que no confíen en ninguna designación de prioridad del paquete (modo no de confianza). Si el puerto se configura en un modo de confianza, utiliza una tabla de asignación adecuada para el campo de confianza que se esté utilizando. Esta tabla indica la cola de CoS a la que se debe reenviar el paquete en el puerto o puertos de salida adecuados. Por supuesto, el campo de confianza debe existir en el paquete para que la tabla de asignación resulte de utilidad, así que existen acciones predeterminadas que se llevan a cabo cuando dicho campo no existe. Estas acciones implican el

direccionamiento del paquete a un nivel de CoS específico configurado para el puerto de entrada como conjunto, tomando como base la prioridad predeterminada del puerto existente tal y como la tabla de asignación 802.1p actual la asigna a una clase de tráfico.

Como alternativa, cuando un puerto está configurado como no de confianza, éste no confía en ninguna designación de prioridad de paquete entrante y, en su lugar, utiliza el valor de prioridad predeterminado del puerto. Todos los paquetes que llegan a la entrada de un puerto no de confianza se dirigen a una cola de CoS específica del puerto o puertos de salida adecuados, según la prioridad predeterminada configurada del puerto de entrada. Este proceso también se utiliza en casos en los que una asignación de puerto de confianza no se puede respetar, como cuando un paquete no IP llega a un puerto configurado para confiar en el valor de DSCP de IP.

Utilice la página **Mapping Table Configuration** (Configuración de la tabla de asignación) para definir el método de asignación de la clase de servicio a un paquete.

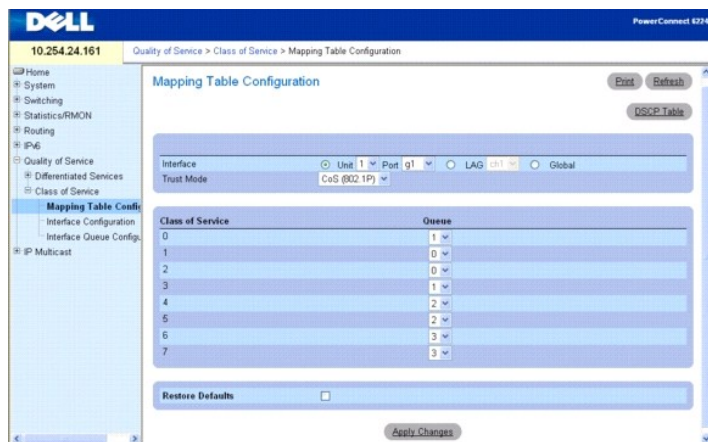
Para visualizar la página, haga clic en **Quality of Service** (Calidad de servicio) → **Class of Service** (Clase de servicio) → **Mapping Table Configuration** (Configuración de la tabla de asignación) en el árbol de vista.

El modo de confianza seleccionado en la página **Mapping Table Configuration** (Configuración de la tabla de asignación) afecta al modo de visualización de la página, así como a los campos a los que se puede acceder desde la misma. En dicha página hay tres modos de confianza disponibles:

- 1 Untrusted (None) (No de confianza [Ninguno])
- 1 CoS (802.1P)
- 1 IP DSCP (DSCP de IP)

CoS (802.1P) es el modo predeterminado, así que ésta es la página que se muestra al seleccionar **Mapping Table Configuration** (Configuración de la tabla de asignación) en la página de menú **Class of Service** (Clase de servicio).

Ilustración 12-16. Configuración de la tabla de asignación - CoS (802.1P)



Modo de confianza CoS (802.1P)

La página **Mapping Table Configuration** (Configuración de la tabla de asignación) de CoS (802.1P) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz a la que se aplicará la configuración de clase de servicio. Seleccione una unidad y un puerto o un LAG, o bien seleccione la opción Global para aplicar la clase de configuración a todas las interfaces.

Trust Mode (Modo de confianza): selecciona el modo de confianza que se aplicará. **CoS (802.1P)** es el modo predeterminado.

Class of Service (Clase de servicio): enumera cada una de las clases de servicio en una línea independiente para así poder asignar una cola independiente a cada clase de servicio.

Queue (Cola): selecciona una cola para cada **clase de servicio** del menú desplegable. Las colas predeterminadas se muestran inicialmente.

Restore Defaults (Restablecer valores predeterminados): al seleccionar esta opción y hacer clic en **Apply Changes** (Aplicar cambios), se restablecen los valores predeterminados de la cola.

Configuración del modo de confianza CoS (802.1P)

1. Abra la página **Mapping Table Configuration** (Configuración de la tabla de asignación).
2. Seleccione la unidad y el puerto o el LAG a los que se aplicarán los cambios, o bien seleccione la opción Global para aplicar la configuración a todas las interfaces.
3. Seleccione un **modo de confianza**.
4. Seleccione una cola para asociar con cada **clase de servicio**.

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

Se aplican los cambios efectuados a las interfaces seleccionadas y se actualiza el dispositivo.

Restablecimiento de los valores predeterminados de la cola

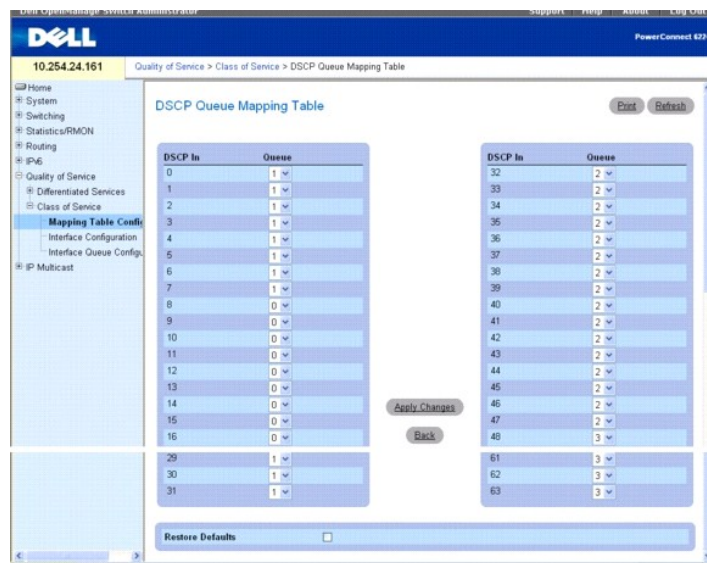
1. Abra la página **Mapping Table Configuration** (Configuración de la tabla de asignación).
2. Haga clic en la casilla de verificación **Restore Defaults** (Restablecer valores predeterminados).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Las colas recuperan los valores predeterminados para cada clase de servicio y se actualiza el dispositivo.

Configuración de la tabla de DSCP de IP

Para acceder a **DSCP Queue Mapping Table** (Tabla de asignación de colas de DSCP), haga clic en **Quality of Service** (Calidad de servicio) → **Class of Service** (Clase de servicio) → **Mapping Table Configuration** (Configuración de la tabla de asignación) en la vista de árbol y, a continuación, haga clic en el enlace de la tabla de DSCP.

Ilustración 12-17. Tabla de asignación de colas de DSCP



La página **DSCP Queue Mapping Table** (Tabla de asignación de colas de DSCP) contiene los campos siguientes:

DSCP In (Entrada DSCP): marque esta opción para seleccionarla como criterio e introduzca el punto de código de servicios diferenciados del paquete que se debe utilizar. Este campo determina la cola a la que se envía el paquete.

Queue ID (ID de cola): selecciona la cola a la que se envía el paquete.

Restablecimiento de los valores predeterminados de la cola

1. Abra la página **DSCP Queue Mapping Table** (Tabla de asignación de colas de DSCP).
2. Haga clic en la casilla de verificación **Restore Defaults** (Restablecer valores predeterminados).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los valores de la cola recuperan sus valores predeterminados y se actualiza el dispositivo.

Configuración de la tabla de asignación mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

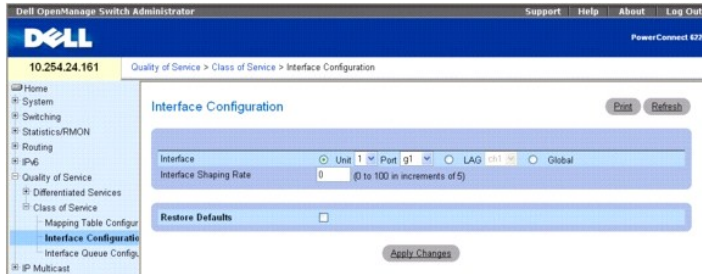
- 1 Comandos de QoS

Configuración de interfaz

Utilice la página **Interface Configuration** (Configuración de interfaz) para especificar de forma individual puertos para la configuración de la CoS, así como para aplicar una velocidad de modelado de interfaces a los puertos seleccionados.

Para visualizar la página **Interface Configuration** (Configuración de interfaz), haga clic en **Quality of Service** (Calidad de servicio) → **Class of Service** (Clase de servicio) → **Interface Configuration** (Configuración de interfaz) en el árbol de vista.

Ilustración 12-18. Configuración de interfaz



La página **Interface Configuration** (Configuración de interfaz) contiene los campos siguientes:

Interface (Interfaz): selecciona la interfaz a la que se aplicará la velocidad de modelado de interfaces.

Interface Shaping Rate (Velocidad de modelado de interfaces): determina el límite máximo de tráfico que puede abandonar un puerto. El valor especificado representa un porcentaje del máximo de amplitud de banda negociada. Los valores válidos oscilan entre 0 y 100, en incrementos de 5.

Restore Defaults (Restablecer valores predeterminados): al seleccionar esta opción, se restablece la velocidad de modelado de interfaces predeterminada en las interfaces seleccionadas.

Definición de la configuración de interfaz

1. Abra la página **Interface Configuration** (Configuración de interfaz).
2. Seleccione la unidad y el puerto o el LAG a los que se aplicarán los cambios, o bien seleccione la opción **Global** para aplicar la configuración a todas las interfaces.
3. Introduzca la velocidad de modelado de interfaces que se aplicará a los puertos en cuestión.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se aplica la nueva velocidad de modelado de interfaces a las interfaces seleccionadas y se actualiza el dispositivo.

Restablecimiento de la velocidad de modelado predeterminada

1. Abra la página **Interface Configuration** (Configuración de interfaz).
2. Haga clic en la casilla de verificación **Restore Defaults** (Restablecer valores predeterminados).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Todos los puertos recuperan la velocidad de modelado predeterminada y se actualiza el dispositivo.

Definición de la configuración de interfaz mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de QoS

Configuración de la cola de interfaz

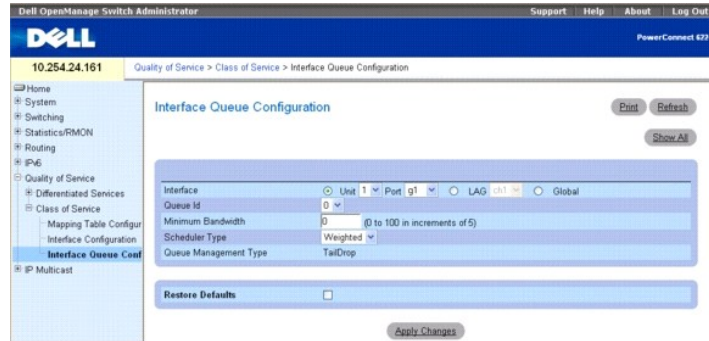
Utilice la página **Interface Queue Configuration** (Configuración de la cola de interfaz) para definir el comportamiento de una determinada cola al configurar colas de salida del conmutador. Los parámetros configurables por el usuario controlan la cantidad de amplitud de banda que utiliza la cola, la profundidad de

la cola durante momentos de congestión, así como la planificación de la transmisión de paquetes desde el conjunto de todas las colas de un puerto. Cada puerto dispone de su propia configuración relativa a la cola de CoS.

El proceso de configuración se simplifica al permitir que cada parámetro de cola de CoS se configure de forma global o bien para cada uno de los puertos. Se aplica un cambio de configuración global automáticamente a todos los puertos del sistema.

Para visualizar la página **Interface Queue Configuration** (Configuración de la cola de interfaz), haga clic en **Quality of Service** (Calidad de servicio)→ **Class of Service** (Clase de servicio)→ **Interface Queue Configuration** (Configuración de la cola de interfaz) en el árbol de vista.

Ilustración 12-19. Configuración de la cola de interfaz



La página **Interface Queue Configuration** (Configuración de la cola de interfaz) contiene los campos siguientes:

Interface (Interfaz): especifica la interfaz (unidad/puerto, LAG o global) que se está configurando.

Queue ID (ID de cola): selecciona la cola que se configurará del menú desplegable.

Minimum Bandwidth (Amplitud de banda mínima): selecciona un porcentaje del máximo de amplitud de banda negociada para el puerto. Especifique un porcentaje que oscile entre 0 y 100, en incrementos de 5.

Scheduler Type (Tipo de programador): selecciona el tipo de procesamiento de cola del menú desplegable. Las opciones son **Weighted** (Ponderado) y **Strict** (Estricto). Si se define cada cola de forma individual, el usuario podrá crear las características de servicio que desee para distintos tipos de tráfico.

Weighted (Ponderado): el turno rotativo ponderado asocia una ponderación a cada cola. Éste es el valor predeterminado.

Strict (Estricto): la prioridad estricta entrega en primer lugar el tráfico con la mayor prioridad de la cola.

Queue Management Type (Tipo de administración de colas): muestra el tipo de administración de paquetes que se utiliza para todos los paquetes, es decir, Taildrop (Descarte del final de la cola). Todos los paquetes de una cola no corren riesgos si no se produce la congestión. Sin embargo, llegado el caso, se descartan todos los paquetes adicionales de la cola.

Configuración de una cola de interfaz

1. Abra la página **Interface Queue Configuration** (Configuración de la cola de interfaz).
2. Seleccione el puerto al que se aplicará la configuración de los menús desplegables **Interface Unit** (Unidad de interfaz) y **Port** (Puerto).
3. Utilice los campos restantes para configurar la cola y sus valores para el puerto en cuestión.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se configura la cola y se actualiza el dispositivo.

Visualización de la configuración de la cola de interfaz

1. Abra la página **Interface Queue Configuration** (Configuración de la cola de interfaz).
2. Haga clic en **Show All** (Mostrar todo).
Aparece la página **Interface Queue Status** (Estado de las colas de interfaz).
3. Seleccione **Unit / Port** (Unidad/puerto), **LAG** o **Global**.

Ilustración 12-20. Estado de las colas de interfaz

Dell OpenManage Switch Administrator Support Help About Log Out
DELL PowerConnect 6224

10.254.24.161 Quality of Service > Class of Service > Interface Queue Status

Home System Switching Statistics/RMON Routing QoS Quality of Service Differentiated Services Class of Service Mapping Table Conf Interface Configurat Interface Queue Con IP Multicast

Interface Queue Status Print Refresh

Interface Unit Port LAG Global

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	weighted	taildrop
1	0	weighted	taildrop
2	0	weighted	taildrop
3	0	weighted	taildrop
4	0	weighted	taildrop
5	0	weighted	taildrop
6	0	weighted	taildrop

Back

Configuración de una cola de interfaz mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de QoS

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de la multidifusión IP

Dell™ PowerConnect™ serie M6220 — Guía del usuario

- [DVMRP](#)
- [IGMP](#)
- [Multidifusión](#)
- [PIM-DM](#)
- [PIM-SM](#)

Los protocolos de multidifusión se utilizan para entregar paquetes de multidifusión de un origen a varios receptores. Facilitan un mejor uso de la amplitud de banda y un menor procesamiento del host y del enrutador, con lo que su uso es idóneo en aplicaciones de conferencia de vídeo y audio, herramientas de pizarra o tableros de cotizaciones, entre otras.

Las aplicaciones de multidifusión envían una copia de un paquete y la dirigen a un grupo de receptores (dirección del grupo de multidifusión) que desea recibirla, en lugar de a un único receptor (dirección de difusión única). La multidifusión depende de la red para reenviar los paquetes únicamente a las redes y hosts que deben recibirlos.

Los enrutadores que admiten la multidifusión o que la tienen activada reenvían paquetes de multidifusión según las rutas especificadas en la base de datos de información de enrutamiento de multidifusión (MRIB). Los protocolos de multidifusión que se ejecutan en el enrutador crean estas rutas en la MRIB durante el proceso de creación de árboles de distribución de multidifusión. Los distintos protocolos de enrutamiento de multidifusión IP utilizan técnicas diferentes para crear dichos árboles.

Si el tráfico de multidifusión va a direccionarse a través de parte de una red que no admite la multidifusión (enrutadores que no la admiten), los paquetes de multidifusión se encapsulan en un datagrama IP y se envían como paquetes de difusión única. Cuando el enrutador de multidifusión del extremo remoto del túnel recibe el paquete, extrae la encapsulación IP y reenvía el paquete como paquete de multidifusión IP. Este proceso de encapsulación de paquetes de multidifusión IP se denomina tunelado.

Para ver la página de menú **IP Multicast** (Multidifusión IP), haga clic en **IP Multicast** (Multidifusión IP) en la vista de árbol. La página de menú **IP Multicast** (Multidifusión IP) contiene enlaces a los procedimientos siguientes:

- 1 [DVMRP](#)
- 1 [IGMP](#)
- 1 [Multidifusión](#)
- 1 [PIM-DM](#)
- 1 [PIM-SM](#)

DVMRP

DVMRP intercambia paquetes sonda con todos los enrutadores que lo tienen activado, establece relaciones bidireccionales entre vecinos y genera una tabla de vecinos. Intercambia paquetes de informe y crea una tabla de topología de difusión única, con la que genera la tabla de enrutamiento de multidifusión. Esta tabla se utiliza para direccionar los paquetes de multidifusión. Dado que todos los enrutadores DVMRP utilizan el mismo protocolo de enrutamiento de difusión única, se evitan los bucles de enrutamiento.

La página de menú **DVMRP** contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de DVMRP. Para visualizar esta página, haga clic en **IP Multicast** (Multidifusión IP) → **DVMRP** en la vista de árbol.

A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

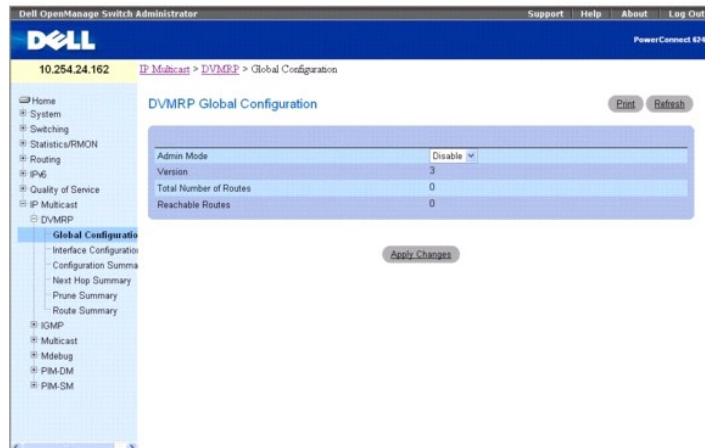
- 1 [Configuración global de DVMRP](#)
- 1 [Configuración de la interfaz DVMRP](#)
- 1 [Resumen de la configuración de DVMRP](#)
- 1 [Resumen del siguiente salto](#)
- 1 [Resumen de poda](#)
- 1 [Resumen de rutas](#)

Configuración global de DVMRP

Utilice la página **DVMRP Global Configuration** (Configuración global de DVMRP) para definir los valores globales de DVMRP.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **DVMRP** → **Global Configuration** (Configuración global) en la vista de árbol.

Ilustración 13-1. Configuración global de DVMRP



La página **DVMRP Global Configuration** (Configuración global de DVMRP) contiene los campos siguientes:

Admin Mode (Modo de administración): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable. De este modo, se define el estado de administración de DVMRP como activo o inactivo. El valor predeterminado es **Disable** (Desactivar).

Version (Versión): valor actual de la cadena de caracteres de la versión de DVMRP.

Total Number of Routes (Número total de rutas): número de rutas especificadas en la tabla de enrutamiento de DVMRP.

Reachable Routes (Rutas accesibles): número de rutas especificadas en la tabla de enrutamiento de DVMRP que tienen una métrica no infinita.

Definición del modo de administración de DVMRP

1. Abra la página **DVMRP Global Configuration** (Configuración global de DVMRP).
2. Defina **Admin Mode** (Modo de administración) como **Enable** (Activar) o **Disable** (Desactivar) para activar o desactivar DVMRP.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de DVMRP y se actualiza el dispositivo.

Configuración de DVMRP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

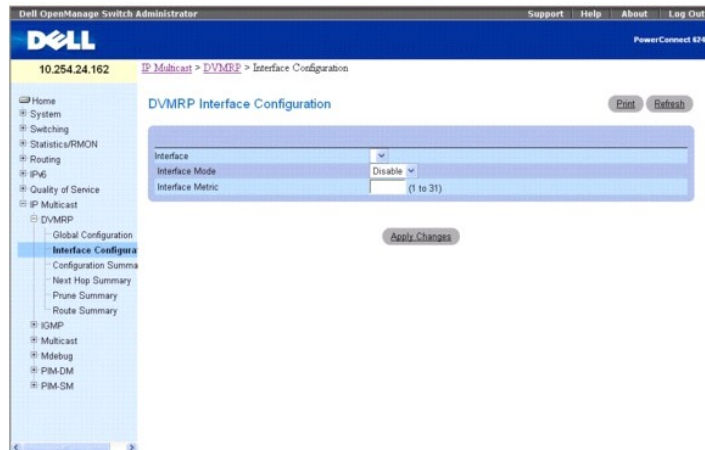
- 1 Comandos de DVMRP

Configuración de la interfaz DVMRP

Utilice la página **DVMRP Interface Configuration** (Configuración de la interfaz DVMRP) para configurar una interfaz DVMRP. Debe configurar al menos una interfaz de enrutador antes de configurar una interfaz DVMRP. De lo contrario, aparece un mensaje que indica que no hay interfaces de enrutador disponibles y no se muestra la pantalla de configuración.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **DVMRP** → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 13-2. Configuración de la interfaz DVMRP



La página **DVMRP Interface Configuration** (Configuración de la interfaz DVMRP) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a configurar. Debe configurar al menos una interfaz de enrutador antes de configurar una interfaz DVMRP.

Interface Mode (Modo de interfaz): seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable para definir el modo de administración de la interfaz de enrutamiento de DVMRP seleccionada.

Interface Metric (Métrica de la interfaz): introduzca la métrica de DVMRP para la interfaz seleccionada. Este valor se envía en mensajes de DVMRP como coste de acceder a esta red. Los valores válidos están comprendidos entre 1 y 31.

Configuración de una interfaz DVMRP

1. Abra la página **DVMRP Interface Configuration** (Configuración de la interfaz DVMRP).
2. Seleccione la interfaz que va a configurar en el campo **Interface** (Interfaz).
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz y se actualiza el dispositivo.

Configuración de una interfaz DVMRP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de DVMRP

Resumen de la configuración de DVMRP

Utilice la página **DVMRP Configuration Summary** (Resumen de la configuración de DVMRP) para ver o imprimir los datos y la configuración de DVMRP correspondientes a una interfaz seleccionada. Debe configurar al menos una interfaz de enrutador para poder ver los datos de una interfaz DVMRP. De lo contrario, aparece un mensaje que indica que no hay interfaces de enrutador disponibles y no se muestra la pantalla de resumen de la configuración.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **DVMRP** → **Configuration Summary** (Resumen de la configuración) en la vista de árbol.

Ilustración 13-3. Resumen de la configuración de DVMRP



La página **DVMRP Configuration Summary** (Resumen de la configuración de DVMRP) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar. Debe configurar al menos una interfaz de enrutador para poder ver los datos de una interfaz DVMRP.

Parámetros de interfaz

Interface Mode (Modo de interfaz): muestra el modo de administración de la interfaz de enrutamiento de DVMRP seleccionada, con los valores Enable (Activar) o Disable (Desactivar).

Protocol State (Estado del protocolo): muestra el estado operativo del protocolo DVMRP en la interfaz seleccionada, con los valores Operational (Operativo) o Non-operational (No operativo).

Local Address (Dirección local): muestra la dirección IP que se utiliza como dirección de origen de los paquetes enviados desde la interfaz seleccionada.

Interface Metric (Métrica de la interfaz): muestra la métrica que se utiliza para calcular los vectores de distancia correspondientes a la interfaz seleccionada.

Estadísticas de la interfaz

Generation ID (ID de generación): muestra la ID de generación de DVMRP que el enrutador utiliza para la interfaz seleccionada. Este valor se restablece cada vez que se inicia o se reinicia una interfaz y se coloca en mensajes de poda. Si se produce un cambio en una ID de generación, se informa a los enrutadores vecinos de que debe descartarse cualquier información previa sobre ese enrutador.

Received Bad Packets (Paquetes erróneos recibidos): número de paquetes no válidos recibidos en la interfaz seleccionada.

Received Bad Routes (Rutas erróneas recibidas): número de rutas no válidas recibidas en la interfaz seleccionada.

Sent Routes (Rutas enviadas): número de rutas enviadas en la interfaz seleccionada.

Parámetros de vecinos

Neighbor IP (IP de vecino): dirección IP del vecino del que se muestra información.

State (Estado): estado del enrutador vecino especificado en la interfaz seleccionada, que puede ser activo o inactivo.

Neighbor Uptime (Tiempo de actividad del vecino): tiempo de actividad de DVMRP del vecino especificado en la interfaz seleccionada. Se trata del tiempo transcurrido desde que se obtuvo la entrada del vecino.

Neighbor Expiry Time (Tiempo de caducidad del vecino): tiempo de caducidad de DVMRP del vecino especificado en la interfaz seleccionada. Se trata del tiempo restante antes de que caduque la entrada del vecino, y no es aplicable si el estado del enrutador vecino es inactivo.

Generation ID (ID de generación): ID de generación de DVMRP del vecino especificado en la interfaz seleccionada.

Major Version (Versión principal): versión principal de DVMRP del vecino especificado en la interfaz seleccionada.

Minor Version (Versión secundaria): versión secundaria de DVMRP del vecino especificado en la interfaz seleccionada.

Capabilities (Funciones): funciones de DVMRP del vecino especificado en la interfaz seleccionada.

Received Routes (Rutas recibidas): número de rutas recibidas para el vecino especificado en la interfaz seleccionada.

Received Bad Packets (Paquetes erróneos recibidos): número de paquetes no válidos recibidos para el vecino especificado en la interfaz seleccionada.

Received Bad Routes (Rutas erróneas recibidas): número de rutas no válidas recibidas para el vecino especificado en la interfaz seleccionada.

Visualización del resumen de la configuración de DVMRP mediante el comando de la CLI

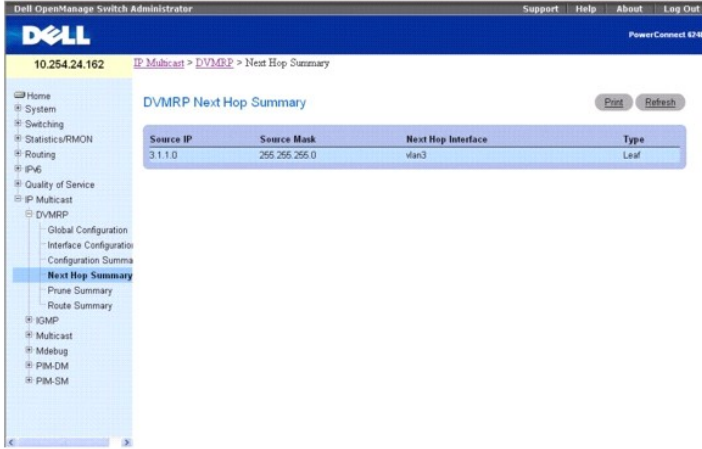
Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

Resumen del siguiente salto

Utilice la página **Next Hop Summary** (Resumen del siguiente salto) para ver o imprimir el resumen del siguiente salto por la IP de origen.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP)→ **DVMRP**→ **Next Hop Summary** (Resumen del siguiente salto) en la vista de árbol.

Ilustración 13-4. Resumen del siguiente salto



La página **Next Hop Summary** (Resumen del siguiente salto) contiene los campos siguientes:

Source IP (IP de origen): muestra la dirección IP que se utiliza con la máscara de origen para identificar la red de origen correspondiente a esta entrada de la tabla.

Source Mask (Máscara de origen): muestra la máscara de red que se utiliza con la dirección IP de origen.

Next Hop Interface (Interfaz del siguiente salto): muestra la interfaz de salida correspondiente al siguiente salto.

Type (Tipo): muestra el tipo del siguiente salto. Leaf (Hoja) significa que no existen vecinos dependientes descendentes en la interfaz de salida. De lo contrario, el tipo es Branch (Rama).

Visualización del resumen del siguiente salto mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

Resumen de poda

Utilice la página **Prune Summary** (Resumen de poda) para ver o imprimir el resumen de poda por la IP de grupo.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP)→ **DVMRP**→ **Prune Summary** (Resumen de poda) en la vista de árbol.

Ilustración 13-5. Resumen de poda

Group IP	Source IP	Source Mask	Expiry Time (secs)
224.2.2.24	3.1.1.0	255.255.255.0	532

La página **Prune Summary** (Resumen de poda) contiene los campos siguientes:

Group IP (IP de grupo): dirección del grupo que se ha podado.

Source IP (IP de origen): dirección del origen o de la red de origen que se ha podado.

Source Mask (Máscara de origen): máscara de subred que se combinará con la dirección IP de origen para identificar el origen o la red de origen que se ha podado.

Expiry Time (secs) (Tiempo de caducidad [seg.]): tiempo restante antes de que caduque esta poda en el vecino ascendente. Si no se han recibido mensajes de poda de los vecinos descendentes, se establece en el valor del temporizador de duración de poda predeterminado; de lo contrario, se establece en el valor más pequeño recibido o en valor del temporizador predeterminado, el que sea inferior de los dos.

Visualización del resumen de poda mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de DVMRP

Resumen de rutas

Utilice la página **Route Summary** (Resumen de rutas) para ver o imprimir el resumen de rutas de DVMRP.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **DVMRP** → **Route Summary** (Resumen de rutas) en la vista de árbol.

Ilustración 13-6. Resumen de rutas

Source Address	Source Mask	Upstream Neighbor	Interface	Metric	Expiry Time (secs)	UP Time (secs)
9.0.0.0	255.0.0.0	0.0.0.0	vlan0	0	0	224
16.0.0.0	255.0.0.0	0.0.0.0	vlan10	0	0	224
20.20.15.0	255.255.255.0	9.1.1.3	vlan0	4	0	205
20.20.20.0	255.255.255.0	9.1.1.3	vlan0	4	0	205

La página **Route Summary** (Resumen de rutas) contiene los campos siguientes:

Source Address (Dirección de origen): dirección de red que se combina con la máscara de origen para identificar los orígenes de esta entrada.

Source Mask (Máscara de origen): máscara de subred que se combinará con la dirección de origen para identificar los orígenes de esta entrada.

Upstream Neighbor (Vecino ascendente): dirección del vecino ascendente (por ejemplo, un vecino RPF) desde la que se reciben datagramas IP de estos orígenes.

Interface (Interfaz): interfaz en la que se reciben los datagramas IP que estos orígenes han enviado. Un valor de 0 suele indicar que la ruta es un conjunto para el que no existe una interfaz del siguiente salto.

Metric (Métrica): distancia expresada en saltos a la subred de origen.

Expiry Time (Tiempo de caducidad): tiempo mínimo restante antes de que caduque esta entrada.

Up Time (Tiempo de actividad): tiempo transcurrido desde que el enrutador obtuvo la ruta representada por esta entrada.

Visualización del resumen de rutas de DVMRP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de DVMRP

IGMP

Los sistemas IPv4 (hosts y enrutadores) utilizan el protocolo de administración de grupos de Internet (IGMP) para notificar su pertenencia a grupos de multidifusión IP a cualquier enrutador de multidifusión vecino. La serie 6200 realiza la función de enrutador de multidifusión del protocolo IGMP, es decir, recopila la información sobre pertenencia que necesita el enrutamiento de multidifusión activo. Los protocolos de enrutamiento de multidifusión que se admiten actualmente en la serie 6200 son DVMRP, PIM-DM y PIM-SM.

La serie 6200 admite la versión 3 de IGMP. Esta versión es compatible con el filtrado de orígenes, que es la capacidad que tiene un sistema para notificar su interés en recibir paquetes únicamente de direcciones de origen específicas, necesario para admitir la multidifusión específica de origen (SSM), o de todas las direcciones de origen que no sean específicas enviadas a una determinada dirección de multidifusión. Está diseñada para que pueda interoperar con las versiones 1 y 2.

La página de menú **IGMP** contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de IGMP. Para visualizar esta página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** en la vista de árbol.

A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

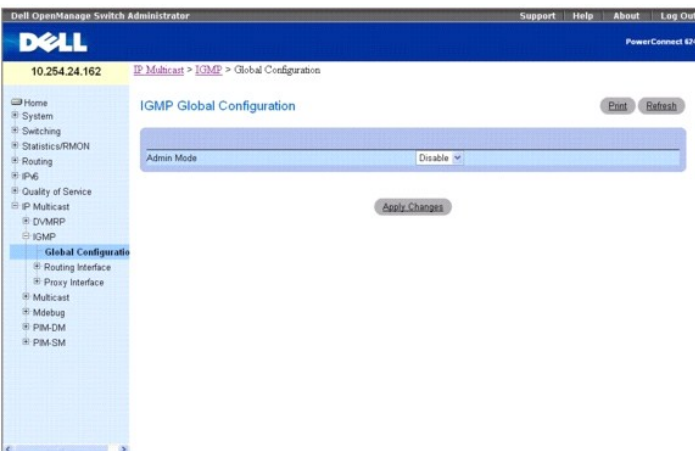
- 1 [Configuración global de IGMP](#)
- 1 [Interfaz de enrutamiento](#)
- 1 [Interfaz de proxy](#)

Configuración global de IGMP

Utilice la página **IGMP Global Configuration** (Configuración global de IGMP) para definir IGMP en el sistema como activo o inactivo.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Global Configuration** (Configuración global) en la vista de árbol.

Ilustración 13-7. Configuración global de IGMP



La página **IGMP Global Configuration** (Configuración global de IGMP) contiene el campo siguiente:

Admin Mode (Modo de administración): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable para definir el estado de administración de IGMP del enrutador como activo o inactivo. El valor predeterminado es **Disable** (Desactivar).

Definición del modo de IGMP

1. Abra la página **IGMP Global Configuration** (Configuración global de IGMP).
2. Defina **Admin Mode** (Modo de administración) como **Enable** (Activar) o **Disable** (Desactivar) para activar o desactivar IGMP.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de IGMP y se actualiza el dispositivo.

Definición del modo de IGMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de IGMP

Interfaz de enrutamiento

La página de menú **Routing Interface** (Interfaz de enrutamiento) contiene enlaces a páginas web que permiten configurar y visualizar los parámetros y datos del enrutamiento IGMP. Para visualizar esta página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Routing Interface** (Interfaz de enrutamiento) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

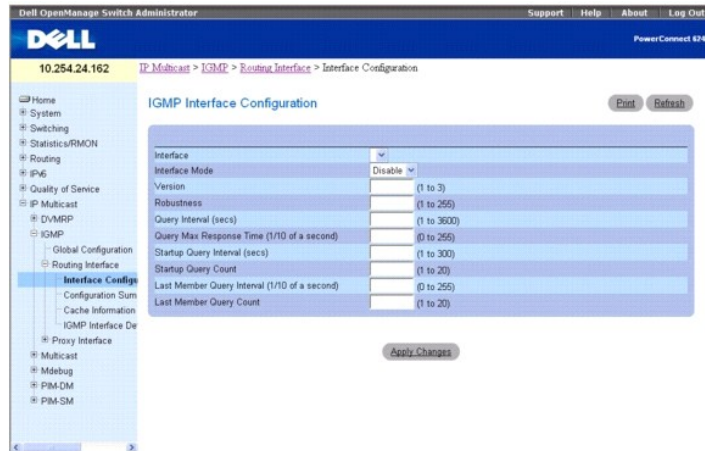
- 1 [Configuración de interfaz IGMP](#)
- 1 [Resumen de la configuración de IGMP](#)
- 1 [Información sobre caché de IGMP](#)
- 1 [Información detallada de pertenencia a la interfaz IGMP](#)

Configuración de interfaz IGMP

Utilice la página **IGMP Interface Configuration** (Configuración de interfaz IGMP) para configurar o mostrar los parámetros de la interfaz del enrutador. Debe configurar como mínimo una interfaz de enrutamiento válida para poder acceder a esta página y configurar el IGMP de multidifusión IP.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Routing Interface** (Interfaz de enrutamiento) → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 13-8. Configuración de interfaz IGMP



La página **IGMP Interface Configuration** (Configuración de interfaz IGMP) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz cuyos datos desea visualizar o configurar.

Interface Mode (Modo de interfaz): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable para definir el estado de administración de IGMP en la interfaz seleccionada. El valor predeterminado es **Disable** (Desactivar).

Version (Versión): introduzca la versión de IGMP que desea configurar en la interfaz seleccionada. Los valores válidos están comprendidos entre 1 y 3, y el valor predeterminado es 3. Este campo sólo puede configurarse si el modo de interfaz IGMP está activado.

Robustness (Robustez): introduzca el valor de robustez. Esta variable permite la adaptación a la pérdida prevista de paquetes en una subred. Si prevé que en la subred se van a producir pérdidas, debe introducir un número más alto para este parámetro. IGMP es robusto (variable de robustez 1) con las pérdidas de paquetes. Los valores válidos están comprendidos entre 1 y 255. El valor predeterminado es 2.

Query Interval (secs) (Intervalo de consulta [seg.]): introduzca la frecuencia, expresada en segundos, a la que se transmitirán los paquetes de consulta al host IGMP en esta interfaz. Los valores válidos están comprendidos entre 1 y 3 600. El valor predeterminado es 125.

Query Max Response Time (1/10 of a second) (Tiempo máximo de respuesta a consulta [1/10 de segundo]): introduzca el tiempo máximo de respuesta a consulta que se anunciará en las consultas IGMPv2 en esta interfaz, expresado en décimas de segundo. El valor predeterminado es 100. Los valores válidos están comprendidos entre 0 y 255.

Startup Query Interval (secs) (Intervalo de consulta de inicio [seg.]): introduzca el número de segundos entre la transmisión de consultas de inicio en la interfaz seleccionada. Los valores válidos están comprendidos entre 1 y 300. El valor predeterminado es 31.

Startup Query Count (Recuento de consultas de inicio): introduzca el número de consultas que se enviarán durante el inicio. Los valores válidos están comprendidos entre 1 y 20. El valor predeterminado es 2.

Last Member Query Interval (1/10 of a second) (Intervalo de consulta de último miembro [1/10 de segundo]): introduzca el intervalo de consulta de último miembro, expresado en décimas de segundo. Se trata del tiempo máximo de respuesta que se insertará en consultas específicas de grupo que se envían como respuesta a mensajes de grupo de cese. Asimismo, es el tiempo que transcurre entre mensajes de consultas específicas de grupo. Los valores válidos están comprendidos entre 0 y 255. El valor predeterminado es 10, que no se utiliza en la versión 1 de IGMP.

Last Member Query Count (Recuento de consultas de último miembro): introduzca el número de consultas que se enviarán al recibir un informe de grupo de cese. Los valores válidos están comprendidos entre 1 y 20. El valor predeterminado es 2.

Configuración de una interfaz de enrutamiento IGMP

1. Abra la página **IGMP Interface Configuration** (Configuración de interfaz IGMP).
2. Seleccione la interfaz que va a configurar en el campo **Interface** (Interfaz).
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz y se actualiza el dispositivo.

Configuración de una interfaz de enrutamiento IGMP mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de IGMP

Resumen de la configuración de IGMP

Utilice la página **IGMP Configuration Summary** (Resumen de la configuración de IGMP) para visualizar los parámetros y datos del enrutamiento IGMP. Debe configurar como mínimo una interfaz de enrutador IGMP para acceder a esta página.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Routing Interface** (Interfaz de enrutamiento) → **Configuration Summary** (Resumen de la configuración) en la vista de árbol.

Ilustración 13-9. Resumen de la configuración de IGMP

Interface Parameters	
Interface Mode	Enable
IP Address	3.1.1.2
Subnet Mask	255.255.255.0
Protocol State	Operational
Version	3
Query Interval (secs)	125
Query Max Response Time (1/10 of a second)	100
Robustness	2
Startup Query Interval (secs)	31
Startup Query Count	2
Last Member Query Interval (1/10 of a second)	10
Last Member Query Count	2

Interface Statistics	
Querier	3.1.1.2
Querier Status	Querier
Querier Up Time (secs)	1832
Querier Expiry Time (secs)	0
Wrong Version Queries	0
Number of Joins	0
Number of Groups	0

La página **IGMP Configuration Summary** (Resumen de la configuración de IGMP) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar.

Parámetros de interfaz

Interface Mode (Modo de interfaz): estado de administración de IGMP en la interfaz seleccionada.

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

Subnet Mask (Máscara de subred): máscara de subred correspondiente a la dirección IP de la interfaz seleccionada.

Protocol State (Estado del protocolo): estado operativo de IGMP en la interfaz seleccionada.

Version (Versión): versión de IGMP configurada en la interfaz seleccionada.

Query Interval (secs) (Intervalo de consulta [seg.]): frecuencia con la que se transmiten los paquetes de consulta al host IGMP en la interfaz seleccionada.

Query Max Response Time (1/10 of a second) (Tiempo máximo de respuesta a consulta [1/10 de segundo]): tiempo máximo de respuesta a consulta que se anuncia en las consultas IGMPv2 enviadas desde la interfaz seleccionada.

Robustness (Robustez): parámetro de robustez de la interfaz seleccionada. Esta variable permite la adaptación a la pérdida prevista de paquetes en una subred. Si se prevé que se van a producir pérdidas en una subred, puede aumentar la variable de robustez. IGMP es robusto (variable de robustez 1) con las pérdidas de paquetes.

Startup Query Interval (secs) (Intervalo de consulta de inicio [seg.]): intervalo en el que se envían consultas de inicio en la interfaz seleccionada.

Startup Query Count (Recuento de consultas de inicio): número de consultas que se enviarán durante el inicio.

Last Member Query Interval (1/10 of a second) (Intervalo de consulta de último miembro [1/10 de segundo]): tiempo máximo de respuesta que se inserta en consultas específicas de grupo enviadas en respuesta a mensajes de grupo de cese. También se trata del tiempo que transcurre entre mensajes de consultas específicas de grupo. Es posible ajustar este valor para modificar la latencia de cese de la red. Si se introduce un valor pequeño, se reduce el tiempo para detectar la pérdida del último miembro de un grupo. Este valor no se utiliza en la versión 1 de IGMP.

Last Member Query Count (Recuento de consultas de último miembro): número de consultas que se enviarán al recibir un informe de grupo de cese.

Estadísticas de la interfaz

Querier (Solicitante): dirección del solicitante IGMP en la subred IP a la que se conecta la interfaz seleccionada.

Querier Status (Estado del solicitante): indica si la interfaz seleccionada tiene o no solicitantes.

Querier Up Time (secs) (Tiempo de actividad del solicitante [seg.]): tiempo, expresado en segundos, que ha transcurrido desde que se modificó por última vez el solicitante de la interfaz IGMP.

Querier Expiry Time (secs) (Tiempo de caducidad del solicitante [seg.]): tiempo restante, expresado en segundos, antes de que caduque el otro temporizador actual del solicitante. Si el sistema local es el solicitante, el valor es cero.

Wrong Version Queries (Consultas de versión errónea): número de consultas que se han recibido en la interfaz seleccionada con una versión de IGMP que no coincide con la configurada para la interfaz durante la duración de la entrada. IGMP requiere que todos los enrutadores de una LAN estén configurados para que ejecuten la misma versión de IGMP. Por lo tanto, se indica un error de configuración si se reciben consultas con un número de versión erróneo.

Number of Joins (Número de uniones): número de veces que se ha añadido una pertenencia a grupo en la interfaz seleccionada, es decir, el número de veces que se ha añadido una entrada de esta interfaz a la tabla de caché. Esto indica la cantidad de actividad de IGMP que hay en la interfaz.

Number of Groups (Número de grupos): número actual de entradas correspondientes a la interfaz seleccionada presentes en la tabla de caché.

Visualización de la configuración de enrutamiento IGMP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

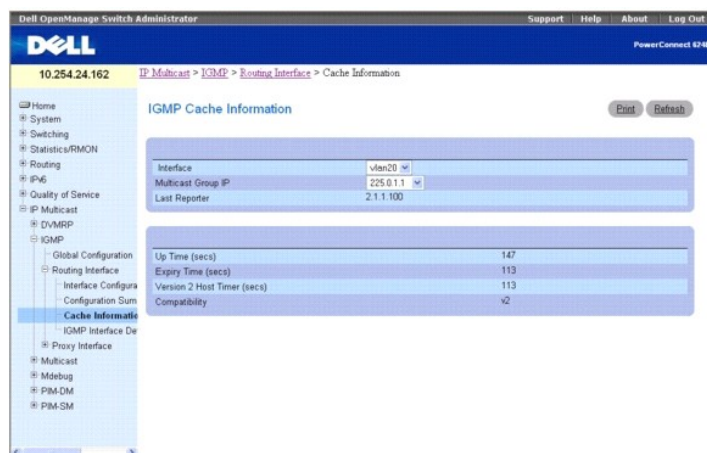
- 1 Comandos de IGMP

Información sobre caché de IGMP

Utilice la página **IGMP Cache Information** (Información sobre caché de IGMP) para ver los datos y parámetros de caché correspondientes a una dirección de grupo de multidifusión IP. Debe configurar como mínimo una interfaz de enrutador IGMP para acceder a esta página. Asimismo, se deben haber recibido los informes de pertenencia a grupo en la interfaz seleccionada para que los datos se muestren en esta página.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Routing Interface** (Interfaz de enrutamiento) → **Cache Information** (Información sobre caché) en la vista de árbol.

Ilustración 13-10. Información sobre caché de IGMP



La página **IGMP Cache Information** (Información sobre caché de IGMP) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar.

Multicast Group IP (IP de grupo de multidifusión): seleccione la dirección del grupo de multidifusión IP cuyos datos desea visualizar. Si no se han recibido informes de pertenencia a grupo en la interfaz seleccionada, no puede realizar esta selección y no se muestra ningún dato en esta página.

Last Reporter (Último informador): dirección IP del origen del último informe de pertenencia recibido para la dirección del grupo de multidifusión IP en la interfaz seleccionada.

Up Time (Tiempo de actividad): tiempo transcurrido desde la creación de esta entrada.

Expiry Time (Tiempo de caducidad): tiempo mínimo restante antes de que caduque esta entrada.

Version 1 Host Timer (Temporizador de host versión 1): tiempo restante hasta que el enrutador local asuma que ya no hay miembros de la versión 1 de IGMP en la subred IP conectada a esta interfaz. Cuando se recibe un informe de pertenencia a IGMPv1, este temporizador se restablece al temporizador de pertenencia a grupo. Mientras este temporizador no esté en cero, el enrutador local ignora los mensajes de cese de IGMPv2 de este grupo que recibe en la interfaz seleccionada. Este campo sólo aparece si la interfaz está configurada para la versión 1 de IGMP.

Version 2 Host Timer (Temporizador de host versión 2): tiempo restante hasta que el enrutador local asuma que ya no hay miembros de la versión 1 de IGMP en la subred IP conectada a esta interfaz. Cuando se recibe un informe de pertenencia a IGMPv2, este temporizador se restablece al temporizador de pertenencia a grupo. Mientras este temporizador no esté en cero, el enrutador local ignora los mensajes de cese de IGMPv1 e IGMPv3 de este grupo que recibe en la interfaz seleccionada. Este campo sólo aparece si la interfaz está configurada para la versión 2 de IGMP.

Compatibility (Compatibilidad): muestra el modo de compatibilidad de grupo (versiones 1, 2 y 3) correspondiente a este grupo en la interfaz especificada.

Filter Mode (Modo de filtrado): modo de filtrado de origen (con los valores Include [Incluir], Exclude [Excluir] y NA [ND]) correspondiente al grupo especificado en esta interfaz. Si el modo NA (ND) está activo, el campo aparece en blanco.

Visualización de información sobre caché mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

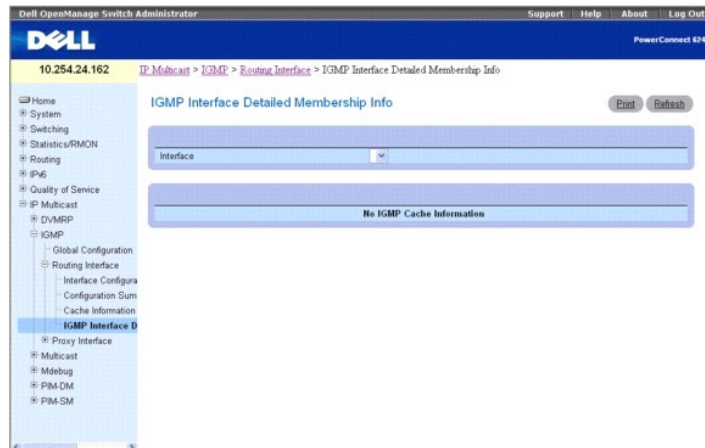
- 1 Comandos de IGMP

Información detallada de pertenencia a la interfaz IGMP

Utilice la página **IGMP Interface Detailed Membership Info** (Información detallada de pertenencia a la interfaz IGMP) para ver información detallada de pertenencia correspondiente a una interfaz. Debe configurar como mínimo una interfaz de enrutador IGMP para acceder a esta página. Asimismo, se deben haber recibido los informes de pertenencia a grupo en la interfaz seleccionada para que los datos se muestren en esta página.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Routing Interface** (Interfaz de enrutamiento) → **IGMP Interface Detailed Membership Info** (Información detallada de pertenencia a la interfaz IGMP) en la vista de árbol.

Ilustración 13-11. Información detallada de pertenencia a la interfaz IGMP



La página **IGMP Interface Detailed Membership Info** (Información detallada de pertenencia a la interfaz IGMP) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar.

Multicast Group IP (IP de grupo de multidifusión): seleccione la dirección del grupo de multidifusión IP cuyos datos desea visualizar. Si no se han recibido informes de pertenencia a grupo en la interfaz seleccionada, no puede realizar esta selección y no se muestra ninguno de los campos restantes.

Interface (Interfaz): interfaz en la que se reenvían los paquetes de multidifusión.

Group Compatibility Mode (Modo de compatibilidad de grupo): modo de compatibilidad de grupo (versiones 1, 2 y 3) correspondiente a este grupo en la interfaz especificada.

Filter Mode (Modo de filtrado): modo de filtrado de origen correspondiente al grupo especificado en esta interfaz. Los valores posibles son Include (Incluir), Exclude (Excluir) y NA (ND).

Source Hosts (Hosts de origen): direcciones de origen que son miembros de esta dirección de multidifusión.

Expiry Time (Tiempo de caducidad): intervalo de tiempo de caducidad para cada dirección de origen que es miembro de este grupo de multidifusión. Se trata del tiempo tras el que caduca la entrada de origen especificada.

Visualización de información detallada de pertenencia a la interfaz IGMP

1. Abra la página **IGMP Interface Detailed Membership Info** (Información detallada de pertenencia a la interfaz IGMP).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).
3. Seleccione la IP que desea en **Multicast Group IP** (IP de grupo de multidifusión).

Se muestra información detallada de pertenencia correspondiente a esta interfaz y la IP del grupo de multidifusión.

Visualización de información detallada de pertenencia a la interfaz IGMP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de IGMP

Interfaz de proxy

El propósito del proxy IGMP es activar un enrutador de multidifusión para obtener información de pertenencia a un grupo de multidifusión y poder reenviar paquetes de multidifusión según la información de pertenencia a grupo. El proxy IGMP sólo puede funcionar en determinadas topologías que no requieren protocolos de enrutamiento de multidifusión (por ejemplo, DVMRP, PIM-DM y PIM-SM) y que tienen topologías de árbol o similares, ya que no admite funciones como árboles de extensión para corregir bucles de rutas de paquetes.

La página de menú **Proxy Interface** (Interfaz de proxy) contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de la interfaz de proxy. Para visualizar esta página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Proxy Interface** (Interfaz de proxy) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

- 1 [Configuración de la interfaz de proxy IGMP](#)
- 1 [Resumen de la configuración de proxy IGMP](#)
- 1 [Información de pertenencia a la interfaz de proxy IGMP](#)
- 1 [Información detallada de pertenencia a la interfaz de proxy IGMP](#)

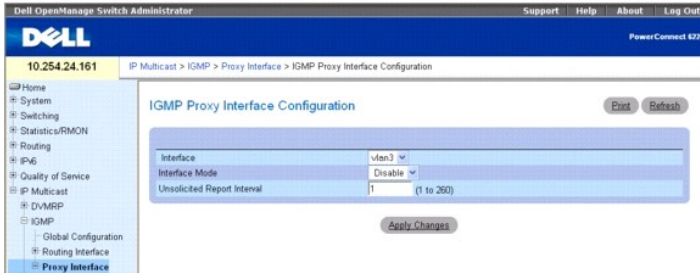
Configuración de la interfaz de proxy IGMP

El enrutador IGMP (sistema IPv4) utiliza el proxy IGMP para activar el sistema para que emita mensajes de host IGMP en nombre de los hosts que el sistema ha detectado mediante interfaces del enrutador IGMP estándar. Por consiguiente, esta función actúa como proxy de todos los hosts que residen en las interfaces del enrutador.

Utilice la página **IGMP Proxy Interface Configuration** (Configuración de la interfaz de proxy IGMP) para configurar el proxy IGMP para una interfaz. Debe haber configurado como mínimo una interfaz de enrutador para poder configurar o visualizar los datos de una interfaz de proxy IGMP y no debe ser una interfaz de enrutamiento IGMP.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Proxy Interface** (Interfaz de proxy) → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 13-12. Configuración de la interfaz de proxy IGMP



La página **IGMP Proxy Interface Configuration** (Configuración de la interfaz de proxy IGMP) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable el puerto cuyos datos desea visualizar o configurar. Debe haber configurado como mínimo una interfaz de enrutador para poder configurar o visualizar los datos de una interfaz de proxy IGMP y no debe ser una interfaz de enrutamiento IGMP. Este campo sólo puede configurarse si el modo de interfaz está desactivado.

Interface Mode (Modo de interfaz): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable para definir el estado de administración del proxy IGMP en la interfaz seleccionada. El valor predeterminado es **Disable** (Desactivar). Para activar el modo de interfaz de proxy IGMP, deben activarse los modos de administración global de enrutamiento, IGMP y multidifusión.

Unsolicited Report Interval (Intervalo de informe no solicitado): introduzca el valor del intervalo de tiempo no solicitado en segundos. El intervalo de informe no solicitado es el tiempo que transcurre entre las repeticiones de un informe inicial del host sobre pertenencia a un grupo. Los valores válidos están comprendidos entre 1 y 260. El valor predeterminado es 1.

Configuración de la interfaz de proxy IGMP

1. Abra la página **IGMP Proxy Interface Configuration** (Configuración de la interfaz de proxy IGMP).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz de proxy y se actualiza el dispositivo.

Configuración de la interfaz de proxy IGMP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

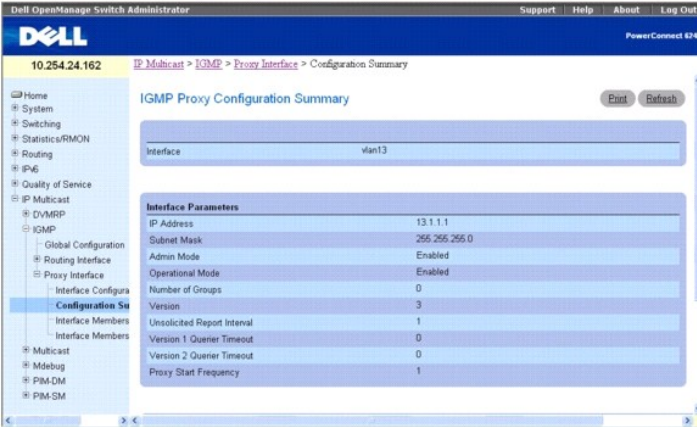
- 1 Comandos del proxy IGMP

Resumen de la configuración de proxy IGMP

Utilice la página **IGMP Proxy Configuration Summary** (Resumen de la configuración de proxy IGMP) para ver las configuraciones de la interfaz de proxy por interfaz. Debe haber configurado como mínimo una interfaz de enrutador para que los datos se muestren en esta página.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Proxy Interface** (Interfaz de proxy) → **Configuration Summary** (Resumen de la configuración) en la vista de árbol.

Ilustración 13-13. Resumen de la configuración de proxy IGMP



La página **IGMP Proxy Configuration Summary** (Resumen de la configuración de proxy IGMP) contiene los campos siguientes:

Interface (Interfaz): muestra la interfaz en la que está activado el proxy IGMP. Sólo puede haber una interfaz de proxy IGMP.

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

Subnet Mask (Máscara de subred): máscara de subred correspondiente a la dirección IP de la interfaz de proxy IGMP.

Admin Mode (Modo de administración): estado de administración del proxy IGMP en la interfaz seleccionada.

Operational Mode (Modo operativo): estado operativo de la interfaz de proxy IGMP.

Number of Groups (Número de grupos): número actual de entradas de grupo de multidifusión correspondientes a la interfaz de proxy IGMP presentes en la tabla de caché.

Version (Versión): versión de IGMP configurada en la interfaz de proxy IGMP.

Unsolicited Report Interval (Intervalo de informe no solicitado): tiempo que transcurre entre las repeticiones de un informe inicial del host sobre pertenencia a un grupo. Valor predeterminado: 1 segundo.

Version 1 Querier Timeout (Tiempo de espera del solicitante versión 1): tiempo de espera del solicitante correspondiente a la versión 1 anterior de IGMP expresado en segundos. El intervalo del solicitante de la versión anterior es el tiempo de espera para que el host vuelva al modo IGMPv3 cuando se recibe una consulta de una versión anterior. Cuando se recibe una consulta de una versión anterior, los hosts establecen el temporizador actual del solicitante de la versión anterior en el intervalo del solicitante de la versión anterior.

Version 2 Querier Timeout (Tiempo de espera del solicitante versión 2): tiempo de espera del solicitante correspondiente a la versión 1 anterior de IGMP expresado en segundos.

Proxy Start Frequency (Frecuencia de inicio de proxy): número de veces que se ha activado el proxy.

Proxy Interface Statistics (Estadísticas de la interfaz de proxy): consultas recibidas, informes recibidos y enviados, y ceses recibidos y enviados.

Visualización de las configuraciones de la interfaz de proxy IGMP mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

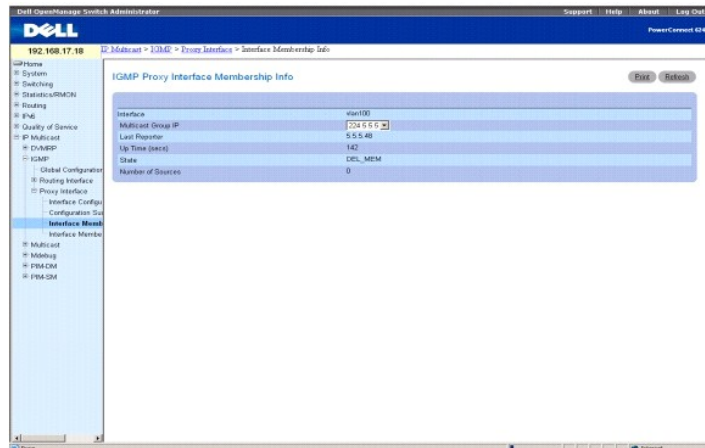
- 1 Comandos del proxy IGMP

Información de pertenencia a la interfaz de proxy IGMP

Utilice la página **IGMP Proxy Interface Membership Info** (Información de pertenencia a la interfaz de proxy IGMP) para ver los datos de pertenencia a una interfaz correspondientes a una dirección de grupo de multidifusión IP específica. Debe haber configurado como mínimo una interfaz de enrutador para poder ver la información de pertenencia a interfaz y no debe ser una interfaz de enrutamiento IGMP. Asimismo, si no se han recibido informes de pertenencia a grupo en la interfaz seleccionada, no se mostrarán datos en esta página.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Proxy Interface** (Interfaz de proxy) → **Interface Membership Info** (Información de pertenencia a interfaz) en la vista de árbol.

Ilustración 13-14. Información de pertenencia a la interfaz de proxy IGMP



La página **IGMP Proxy Interface Membership Info** (Información de pertenencia a la interfaz de proxy IGMP) contiene los campos siguientes:

Interface (Interfaz): muestra la interfaz en la que está activado el proxy IGMP.

Multicast Group IP (IP de grupo de multidifusión): seleccione la dirección del grupo de multidifusión IP cuyos datos desea visualizar. Si no se han recibido informes de pertenencia a grupo en la interfaz seleccionada, no puede realizar esta selección y no se muestra ninguno de los datos siguientes.

Last Reporter (Último informador): dirección IP del origen del último informe de pertenencia recibido para la dirección del grupo de multidifusión IP en la interfaz de proxy IGMP.

Up Time (secs) (Tiempo de actividad [seg.]): tiempo transcurrido desde la creación de esta entrada.

State (Estado): estado de la entrada de host. Un host puede tener uno de los estados que se indican a continuación. **Non-member state** (Estado no miembro): no pertenece al grupo de la interfaz. **Delaying member state** (Estado miembro con demora): el host pertenece al grupo de la interfaz y se ejecuta el temporizador de informes. El temporizador de informes se utiliza para enviar los informes. **Idle member state** (Estado miembro inactivo): el host pertenece al grupo de la interfaz y no se ejecuta el temporizador de informes.

Number of Sources (Número de orígenes): número de hosts de origen presentes en el grupo de multidifusión seleccionado.

Visualización de información de pertenencia a la interfaz de proxy IGMP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

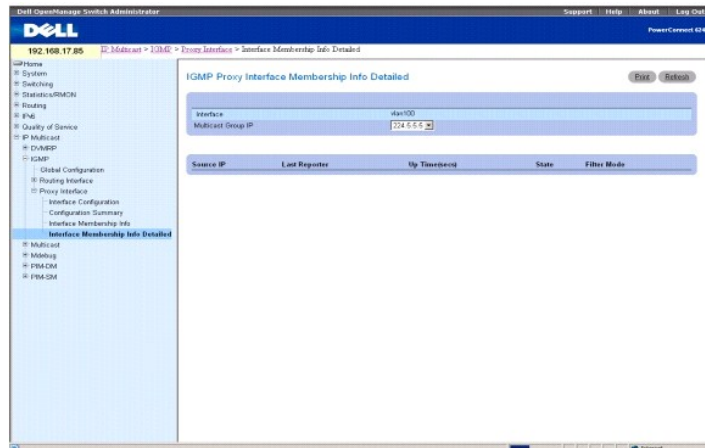
- 1 Comandos del proxy IGMP

Información detallada de pertenencia a la interfaz de proxy IGMP

Utilice la página **IGMP Proxy Interface Membership Info Detailed** (Información detallada de pertenencia a la interfaz de proxy IGMP) para ver información detallada sobre la pertenencia a una interfaz. Debe haber configurado como mínimo una interfaz de enrutador para poder ver la información detallada de pertenencia a interfaz y no debe ser una interfaz de enrutamiento IGMP. Asimismo, si no se han recibido informes de pertenencia a grupo en la interfaz seleccionada, no puede ver los datos.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **IGMP** → **Proxy Interface** (Interfaz de proxy) → **Interface Membership Info Detailed** (Información detallada de pertenencia a interfaz) en la vista de árbol.

Ilustración 13-15. Información detallada de pertenencia a la interfaz de proxy IGMP



La página **IGMP Proxy Interface Membership Info Detailed** (Información detallada de pertenencia a la interfaz de proxy IGMP) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar.

Multicast Group IP (IP de grupo de multidifusión): seleccione la dirección del grupo de multidifusión IP cuyos datos desea visualizar. Si no se han recibido informes de pertenencia a grupo en la interfaz seleccionada, no puede realizar esta selección y no se muestran los datos que no pueden configurarse.

Source IP (IP de origen): muestra las direcciones de origen que son miembros de esta dirección de multidifusión.

Last Reporter (Último informador): dirección IP del origen del último informe de pertenencia recibido para la dirección del grupo de multidifusión IP en la interfaz seleccionada.

Up Time (secs) (Tiempo de actividad [seg.]): muestra el tiempo de actividad desde que se creó la entrada en la tabla de caché.

State (Estado): estado de la entrada de host. Un host puede tener uno de los estados siguientes:

Non-member State (Estado no miembro): el host no pertenece al grupo de la interfaz.

Delaying Member State (Estado miembro con demora): el host pertenece al grupo de la interfaz y se ejecuta el temporizador de informes. El temporizador de informes se utiliza para enviar los informes.

Idle Member State (Estado miembro inactivo): el host pertenece al grupo de la interfaz y no se ejecuta el temporizador de informes.

Filter Mode (Modo de filtrado): modo de filtrado de grupo (con los valores Include [Incluir], Exclude [Excluir] y None [Ninguno]) correspondiente al grupo especificado en la interfaz de proxy IGMP.

Visualización de información detallada de pertenencia a la interfaz de proxy IGMP

1. Abra la página **IGMP Proxy Interface Membership Info Detailed** (Información detallada de pertenencia a la interfaz de proxy IGMP).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).
3. Seleccione la IP que desea en **Multicast Group IP** (IP de grupo de multidifusión).

Se muestran datos detallados de pertenencia correspondientes a esta interfaz y la IP del grupo de multidifusión.

Visualización de información detallada de pertenencia a la interfaz de proxy IGMP mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos del proxy IGMP

Multidifusión

La página de menú **Multicast** (Multidifusión) contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de multidifusión. Para visualizar esta página, haga clic en **IP Multicast** (Multidifusión IP) → **Multicast** (Multidifusión) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

- 1 [Configuración global de multidifusión](#)
- 1 [Configuración de la interfaz de multidifusión](#)
- 1 [Resumen de rutas de multidifusión](#)

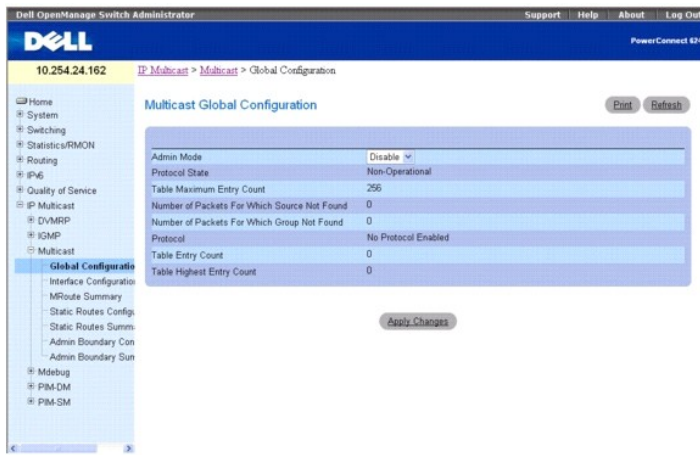
- 1 [Configuración de rutas estáticas de multidifusión](#)
- 1 [Resumen de rutas estáticas de multidifusión](#)
- 1 [Configuración del límite de administración de multidifusión](#)
- 1 [Resumen de los límites de administración de multidifusión](#)

Configuración global de multidifusión

Utilice la página **Multicast Global Configuration** (Configuración global de multidifusión) para configurar el estado de administración del reenvío de multidifusión en el enrutador, así como para ver los parámetros globales de multidifusión.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **Multicast** (Multidifusión) → **Global Configuration** (Configuración global) en la vista de árbol.

Ilustración 13-16. Configuración global de multidifusión



La página **Multicast Global Configuration** (Configuración global de multidifusión) contiene los campos siguientes:

Admin Mode (Modo de administración): seleccione **Enable** (Activar) o **Disable** (Desactivar) para definir el estado de administración del reenvío de multidifusión en el enrutador. El valor predeterminado es **Disable** (Desactivar).

Protocol State (Estado del protocolo): estado operativo del módulo de reenvío de multidifusión.

Table Maximum Entry Count (Recuento máximo de entradas de la tabla): número máximo de entradas que puede haber en la tabla de enrutamiento de multidifusión IP.

Number Of Packets For Which Source Not Found (Número de paquetes cuyo origen no se ha encontrado): número de paquetes de multidifusión que debían direccionarse pero que no han superado la comprobación RPF.

Number Of Packets For Which Group Not Found (Número de paquetes cuyo grupo no se ha encontrado): número de paquetes de multidifusión que debían direccionarse pero cuya ruta de multidifusión no se ha encontrado.

Protocol (Protocolo): protocolo de enrutamiento de multidifusión activado actualmente en el enrutador, si hay alguno.

Table Entry Count (Recuento de entradas de la tabla): número de entradas de rutas de multidifusión presentes actualmente en la tabla de rutas de multidifusión.

Table Highest Entry Count (Recuento más alto de entradas de la tabla): número más alto de entradas de rutas de multidifusión que ha habido en la tabla de rutas de multidifusión.

Configuración del modo de administración del reenvío de multidifusión

1. Abra la página **Multicast Global Configuration** (Configuración global de multidifusión).
2. Seleccione **Enable** (Activar) o **Disable** (Desactivar) en **Admin Mode** (Modo de administración).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración global de multidifusión y se actualiza el dispositivo.

Configuración y visualización de los parámetros de reenvío de multidifusión mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

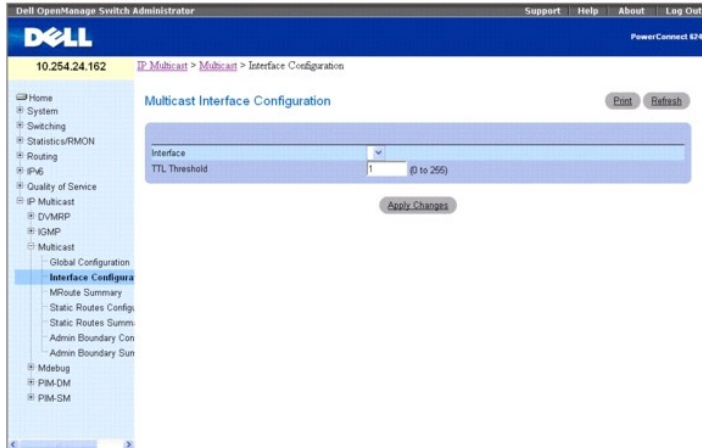
- 1 Comandos de multidifusión

Configuración de la interfaz de multidifusión

Utilice la página **Multicast Interface Configuration** (Configuración de la interfaz de multidifusión) para configurar el umbral TTL de una interfaz de multidifusión. Debe configurar como mínimo una interfaz de enrutador para que los campos aparezcan en esta página.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP)→ **Multicast** (Multidifusión)→ **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 13-17. Configuración de la interfaz de multidifusión



La página **Multicast Interface Configuration** (Configuración de la interfaz de multidifusión) contiene los campos siguientes:

Interface (Interfaz): seleccione en el menú desplegable la interfaz de enrutamiento que desea configurar.

TTL Threshold (Umbral TTL): introduzca el umbral TTL por debajo del cual no se reenviará un paquete de datos de multidifusión desde la interfaz seleccionada. Introduzca un número entre 0 y 255. Si introduce 0, se reenvían todos los paquetes de multidifusión de la interfaz seleccionada. Debe configurar como mínimo una interfaz de enrutador para poder ver este campo.

Configuración de una interfaz de multidifusión

1. Abra la página **Multicast Interface Configuration** (Configuración de la interfaz de multidifusión).
2. Seleccione la interfaz que desea configurar en el menú desplegable **Interface** (Interfaz).
3. Introduzca el umbral TTL que desea en **TTL Threshold** (Umbral TTL).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz de multidifusión y se actualiza el dispositivo.

Configuración de una interfaz de multidifusión mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de multidifusión

Resumen de rutas de multidifusión

Utilice la página **Multicast MRoute Summary** (Resumen de rutas de multidifusión) para ver información sobre las rutas de multidifusión.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP)→ **Multicast** (Multidifusión)→ **MRoute Summary** (Resumen de rutas de multidifusión) en la vista de árbol.

Ilustración 13-18. Resumen de rutas de multidifusión

Source IP	Group IP	Incoming Interface	Outgoing Interfaces	Up Time (secs)	Expiry Time (secs)	RPF Neighbour	Protocol	Flags
3.1.1.100	255.0.2.2	vlan30	vlan10	520	182	0.0.0.0	PIMDM	----

La página **Multicast MRoute Summary** (Resumen de rutas de multidifusión) contiene los campos siguientes:

Source IP (IP de origen): dirección IP del origen del paquete de multidifusión que, junto con la IP de grupo, identifica una entrada de la tabla de rutas de multidifusión.

Group IP (IP de grupo): dirección IP del grupo de destino.

Incoming Interface (Interfaz de entrada): interfaz de entrada en la que llegan los paquetes de multidifusión de este origen o grupo.

Outgoing Interfaces (Interfaces de salida): lista de interfaces de salida en las que se reenvían los paquetes de multidifusión de este origen o grupo.

Up Time (secs) (Tiempo de actividad [seg.]): tiempo, expresado en segundos, que ha transcurrido desde la creación de la entrada.

Expiry Time (secs) (Tiempo de caducidad [seg.]): tiempo, expresado en segundos, que falta para que esta entrada caduque y se elimine de la tabla.

RPF Neighbor (Vecino RPF): dirección IP del vecino de reenvío de ruta inversa.

Protocol (Protocolo): protocolo de enrutamiento de multidifusión que ha creado esta entrada. A continuación se indican los posibles protocolos:

- 1 PIM-DM
- 1 PIM-SM
- 1 DVMRP

Flags (Indicadores): el valor que se muestra en este campo es válido si el protocolo de enrutamiento de multidifusión que se ejecuta es PIM-SM. Los valores posibles son RPT o SPT. Para el resto de protocolos se muestra "-----".

Visualización del resumen de rutas de multidifusión mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

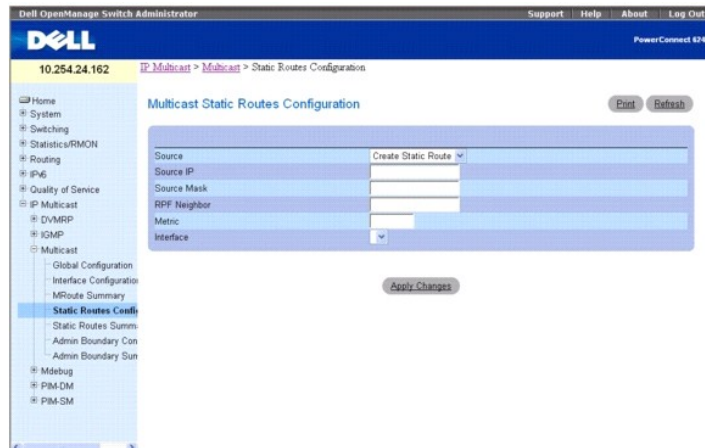
- 1 Comandos de multidifusión

Configuración de rutas estáticas de multidifusión

Utilice la página **Multicast Static Routes Configuration** (Configuración de rutas estáticas de multidifusión) para configurar una entrada estática nueva en la tabla de rutas de multidifusión o para modificar una existente.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **Multicast** (Multidifusión) → **Static Routes Configuration** (Configuración de rutas estáticas) en la vista de árbol.

Ilustración 13-19. Configuración de rutas estáticas de multidifusión



La página **Multicast Static Routes Configuration** (Configuración de rutas estáticas de multidifusión) contiene los campos siguientes:

Source (Origen): seleccione **Create Static Route** (Crear ruta estática) para configurar una entrada estática nueva en la tabla de rutas de multidifusión o bien seleccione una de las entradas existentes en el menú desplegable.

Source IP (IP de origen): introduzca la dirección IP que identifica el origen del paquete de multidifusión para la entrada que está creando.

Source Mask (Máscara de origen): introduzca la máscara de subred que se aplicará a la dirección IP de origen.

RPF Neighbor (Vecino RPF): introduzca la dirección IP del enrutador vecino en la ruta de acceso al origen.

Metric (Métrica): introduzca el coste de estado del enlace correspondiente a la ruta de acceso al origen de multidifusión. El intervalo es 0-255, y el valor predeterminado es 1. Puede cambiar la métrica de una ruta configurada; para ello, seleccione la ruta estática y edite este campo.

Interface (Interfaz): seleccione en el menú desplegable el número de la interfaz. Se trata de la interfaz que se conecta al enrutador vecino para la dirección IP de origen especificada.

Configuración de una ruta estática

1. Abra la página **Static Routes** (Rutas estáticas).
2. Seleccione **Create Static Route** (Crear ruta estática) en el campo **Source** (Origen) para configurar una entrada estática nueva o bien seleccione una de las entradas existentes.
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la ruta estática que se ha creado o modificado y se actualiza el dispositivo.

Configuración de una ruta estática mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de multidifusión

Resumen de rutas estáticas de multidifusión

Utilice la página **Multicast Static Routes Summary** (Resumen de rutas estáticas de multidifusión) para ver las rutas estáticas y sus configuraciones.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **Multicast** (Multidifusión) → **Static Routes Summary** (Resumen de rutas estáticas) en la vista de árbol.

Ilustración 13-20. Resumen de rutas estáticas de multidifusión

Source IP	Source Mask	RPF Address	Metric	VLANID
3.1.1.1	255.255.255.0	6.1.1.1	1	vlan3

La página **Multicast Static Routes Summary** (Resumen de rutas estáticas de multidifusión) contiene los campos siguientes:

Source IP (IP de origen): dirección IP que identifica el origen del paquete de multidifusión para esta ruta.

Source Mask (Máscara de origen): máscara de subred que se aplica a la dirección IP de origen.

RPF Address (Dirección RPF): dirección IP del vecino RPF.

Metric (Métrica): coste de estado del enlace correspondiente a la ruta de acceso al origen de multidifusión. El intervalo es 0-255.

VLANID (ID de VLAN): número de la VLAN de entrada cuya dirección IP se utiliza como RPF para la dirección IP de origen especificada.

Visualización del resumen de rutas estáticas mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de multidifusión

Configuración del límite de administración de multidifusión

Un límite de ámbito de administración puede definirse como un modo de detener la entrada y la salida de tráfico de multidifusión para un determinado intervalo de direcciones de multidifusión en una interfaz de enrutamiento específica. Utilice la página **Multicast Admin Boundary Configuration** (Configuración del límite de administración de multidifusión) para configurar un límite de ámbito de administración nuevo o uno ya existente. Para ver esta página, debe haber configurado la multidifusión y una interfaz de enrutamiento válida.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **Multicast** (Multidifusión) → **Admin Boundary Configuration** (Configuración del límite de administración) en la vista de árbol.

Ilustración 13-21. Configuración del límite de administración de multidifusión

La página **Multicast Admin Boundary Configuration** (Configuración del límite de administración de multidifusión) contiene los campos siguientes:

Group (Grupo): seleccione **Create Boundary** (Crear límite) en el menú desplegable para crear un límite de ámbito de administración nuevo o bien seleccione una de las especificaciones de límite ya existentes para ver o actualizar su configuración.

Interface (Interfaz): seleccione la interfaz de enrutador para la que va a configurarse el límite de ámbito de administración.

Group IP (IP de grupo): introduzca la dirección del grupo de multidifusión para el inicio del intervalo de direcciones que se van a excluir. La dirección debe estar comprendida en el intervalo de 239.0.0.0 a 239.255.255.255.

Group Mask (Máscara de grupo): introduzca la máscara que se aplicará a la dirección del grupo de multidifusión. La combinación de la máscara y la IP de grupo proporciona el intervalo de direcciones de ámbito de administración para la interfaz seleccionada.

Configuración de un límite de administración

1. Abra la página **Multicast Admin Boundary Configuration** (Configuración del límite de administración de multidifusión).
2. Seleccione **Create Boundary** (Crear límite) en el campo **Group IP** (IP de grupo) para configurar un límite de ámbito de administración nuevo o bien seleccione una de las entradas existentes.
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda el límite de ámbito de administración que se ha creado o modificado y se actualiza el dispositivo.

Configuración de un límite de administración mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

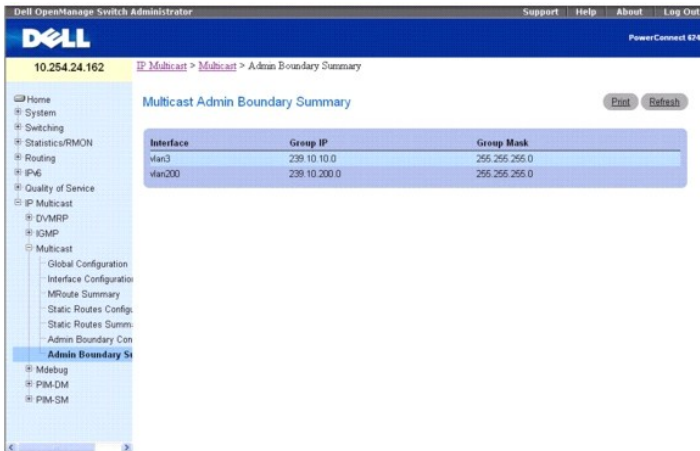
1. Comandos de multidifusión

Resumen de los límites de administración de multidifusión

Utilice la página **Multicast Admin Boundary Summary** (Resumen de los límites de administración de multidifusión) para ver los límites de ámbito de administración existentes.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **Multicast** (Multidifusión) → **Admin Boundary Summary** (Resumen de los límites de administración) en la vista de árbol.

Ilustración 13-22. Resumen de los límites de administración de multidifusión



Interface	Group IP	Group Mask
vlan3	239.10.10.0	255.255.255.0
vlan200	239.10.200.0	255.255.255.0

La página **Multicast Admin Boundary Summary** (Resumen de los límites de administración de multidifusión) contiene los campos siguientes:

Interface (Interfaz): interfaz de enrutador a la que se aplica el intervalo de direcciones de ámbito de administración.

Group IP (IP de grupo): dirección del grupo de multidifusión para el inicio del intervalo de direcciones que se van a excluir.

Group Mask (Máscara de grupo): máscara que se aplica a la dirección del grupo de multidifusión. La combinación de la máscara y la IP de grupo proporciona el intervalo de direcciones de ámbito de administración para la interfaz seleccionada.

Visualización del resumen de los límites de administración de multidifusión mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

PIM-DM

PIM-DM es un sencillo protocolo de enrutamiento de multidifusión independiente. Utiliza una tabla de enrutamiento de difusión única existente y un mecanismo de unión, poda e injerto para crear un árbol. PIM-DM crea árboles de distribución de la ruta de acceso más corta basados en el origen que utilizan RPF. No puede utilizarse para crear un árbol de distribución compartido, como en el caso de PIM-SM. PIM-DM asume que cuando el emisor inicia el envío de datos, todos los hosts y enrutadores descendentes desean recibir un datagrama de multidifusión. Inicialmente, distribuye el tráfico de multidifusión a través de la red. Los enrutadores que no tienen vecinos descendentes vuelven a podar el tráfico no deseado. Además de los mensajes de poda, PIM-DM utiliza mensajes de injerto y aserción. Los mensajes de injerto se utilizan siempre que un nuevo host desee unirse al grupo. Los mensajes de aserción se utilizan para cerrar los flujos duplicados en la misma red de acceso múltiple.

PIM-DM tiene dos versiones. La versión 2 no utiliza el mensaje IGMP, sino un mensaje encapsulado en el paquete IP con el número de protocolo 103. En esta versión, se introduce un mensaje de saludo en lugar del mensaje de consulta.

PIM-DM es adecuado para:

- 1 Receptores densamente distribuidos
- 1 De pocos emisores a muchos receptores (debido a una distribución frecuente)
- 1 Volumen elevado de tráfico de multidifusión
- 1 Flujo constante de tráfico

La página de menú **PIM-DM** contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de **PIM-DM**. Para visualizar esta página, haga clic en **IP Multicast (Multidifusión IP)** → **PIM-DM** en la vista de árbol.

A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

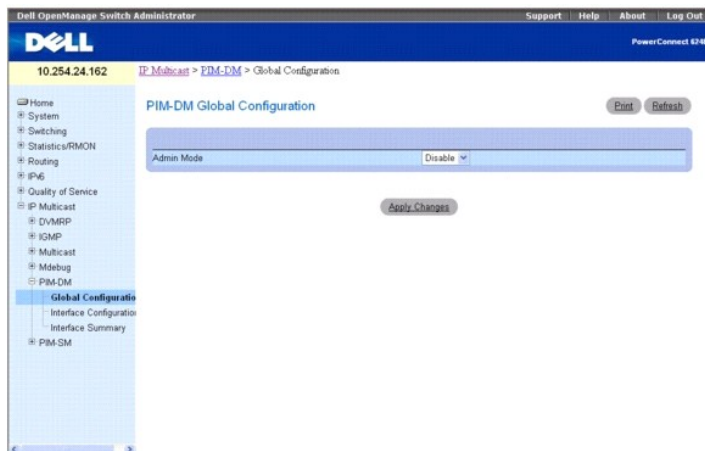
- 1 [Configuración global de PIM-DM](#)
- 1 [Configuración de la interfaz PIM-DM](#)
- 1 [Resumen de interfaces PIM-DM](#)

Configuración global de PIM-DM

Utilice la página **PIM-DM Global Configuration** (Configuración global de PIM-DM) para configurar el estado de administración de PIM-DM en este sistema.

Para visualizar la página, haga clic en **IP Multicast (Multidifusión IP)** → **PIM-DM** → **Global Configuration** (Configuración global) en la vista de árbol.

Ilustración 13-23. Configuración global de PIM-DM



La página **PIM-DM Global Configuration** (Configuración global de PIM-DM) contiene el campo siguiente:

Admin Mode (Modo de administración): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable para definir el estado de administración de PIM-DM en el sistema. El valor predeterminado es **Disable** (Desactivar).

Configuración de PIM-DM

1. Abra la página **PIM-DM Global Configuration** (Configuración global de PIM-DM).
2. Defina **Admin Mode** (Modo de administración) como **Enable** (Activar) o **Disable** (Desactivar) para activar o desactivar PIM-DM.

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

Se guarda la configuración de PIM-DM y se actualiza el dispositivo.

Configuración de PIM-DM mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

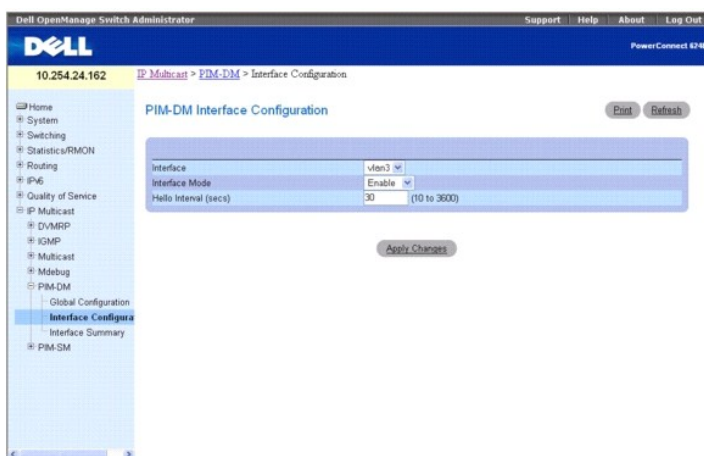
- 1 Comandos de PIM-DM

Configuración de la interfaz PIM-DM

Utilice la página **PIM-DM Interface Configuration** (Configuración de la interfaz PIM-DM) para configurar interfaces específicas con PIM-DM. PIM-DM debe estar activado en la página **PIM-DM Global Configuration** (Configuración global de PIM-DM) para que se muestre esta página de configuración de la interfaz.

Para visualizar la página, haga clic en **IP Multicast** (Multidifusión IP) → **PIM-DM** → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 13-24. Configuración de la interfaz PIM-DM



La página **PIM-DM Interface Configuration** (Configuración de la interfaz PIM-DM) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar o configurar. Debe haber configurado como mínimo una interfaz de enrutador para poder configurar o mostrar datos de una interfaz PIM-DM; de lo contrario, se muestra un mensaje de error.

Interface Mode (Modo de interfaz): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable para definir el estado de administración de PIM-DM para la interfaz seleccionada. El valor predeterminado es **Disable** (Desactivar).

Hello Interval (secs) (Intervalo de saludo [seg.]): introduzca el número de segundos que deben transcurrir entre los mensajes de saludo de PIM transmitidos desde la interfaz seleccionada. El valor predeterminado es 30. Los valores válidos están comprendidos entre 10 y 3600.

Configuración de PIM-DM para una interfaz

1. Abra la página **PIM-DM Interface Configuration** (Configuración de la interfaz PIM-DM).
2. Seleccione la interfaz que va a configurar en el campo **Interface** (Interfaz).
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz y se actualiza el dispositivo.

Configuración de PIM-DM para una interfaz mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de PIM-DM

Resumen de interfaces PIM-DM

Utilice la página **PIM-DM Interface Summary** (Resumen de interfaces PIM-DM) para mostrar una interfaz PIM-DM y su configuración. Como mínimo debe haber una interfaz configurada como PIM-DM en este enrutador para que se muestre la página.

Para visualizar la página, haga clic en **IP Multicast (Multidifusión IP)** → **PIM-DM** → **Interface Summary** (Resumen de interfaces) en la vista de árbol.

Ilustración 13-25. Resumen de interfaces PIM-DM



La página **PIM-DM Interface Summary** (Resumen de interfaces PIM-DM) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar. Debe haber como mínimo una interfaz de enrutador configurada para poder mostrar datos de una interfaz PIM-DM; de lo contrario, se muestra un mensaje de error.

Parámetros de interfaz

Interface Mode (Modo de interfaz): muestra el estado de administración de PIM-DM para la interfaz seleccionada. El valor predeterminado es **Disable** (Desactivar).

Protocol State (Estado del protocolo): estado operativo del protocolo PIM-DM en esta interfaz.

Hello Interval (secs) (Intervalo de saludo [seg.]): frecuencia con la que se transmiten los mensajes de saludo de PIM en la interfaz seleccionada.

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

Estadísticas de la interfaz

Neighbor Count (Recuento de vecinos): número de vecinos PIM en la interfaz seleccionada.

Designated Router (Enrutador designado): enrutador designado en la interfaz PIM seleccionada. En las interfaces punto a punto, es 0.0.0.0.

Vecinos de la interfaz

Neighbor IP (IP de vecino): dirección IP del vecino PIM sobre el que esta entrada contiene información.

Up Time (hh:mm:ss) (Tiempo de actividad [hh:mm:ss]): tiempo transcurrido desde que este vecino PIM fue (por última vez) vecino del enrutador local.

Expiry Time (hh:mm:ss) (Tiempo de caducidad [hh:mm:ss]): tiempo mínimo restante antes de que caduque este vecino PIM.

Visualización del resumen de interfaces PIM-DM mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

1 Comandos de PIM-DM

PIM-SM

PIM-SM se utiliza para direccionar de manera eficaz el tráfico de multidifusión a grupos de multidifusión que pueden abarcar redes de área amplia y en casos en que la amplitud de banda es una limitación. Utiliza árboles compartidos de manera predeterminada e implementa árboles basados en el origen para obtener mayor eficacia. Esta velocidad de umbral de datos se utiliza para alternar entre árboles. PIM-SM asume que no hay hosts que deseen el tráfico de multidifusión, a menos que lo soliciten específicamente. Crea un árbol de distribución compartido centrado en un punto de encuentro (RP) definido desde el que el tráfico de origen se transmite a los receptores. Los emisores envían primero los datos de multidifusión al RP que, a su vez, envía los datos a los receptores en dirección descendente por el árbol compartido. Los árboles compartidos centrados en un RP no proporcionan necesariamente la ruta de acceso más corta u óptima. En estos casos, PIM-SM proporciona un medio para cambiar a árboles específicos del origen más eficaces.

La página de menú **PIM-SM** contiene enlaces a páginas web que permiten definir y visualizar los parámetros y datos de PIM-SM. Para visualizar esta página, haga clic en **IP Multicast (Multidifusión IP)** → **PIM-SM** en la vista de árbol.

A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

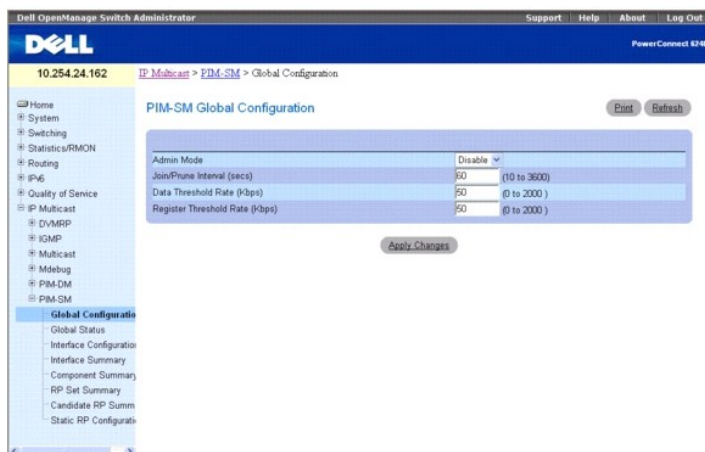
- 1 [Configuración global de PIM-SM](#)
- 1 [Estado global de PIM-SM](#)
- 1 [Configuración de la interfaz PIM-SM](#)
- 1 [Resumen de interfaces PIM-SM](#)
- 1 [Resumen de componentes](#)
- 1 [Resumen de conjuntos de RP](#)
- 1 [Resumen de RP candidatos](#)
- 1 [Configuración de RP estático](#)

Configuración global de PIM-SM

Utilice la página PIM-SM Global Configuration (Configuración global de PIM-SM) para configurar los valores globales de PIM-SM para este sistema.

Para visualizar la página, haga clic en Multicast (Multidifusión)→ PIM-SM→ Global Configuration (Configuración global) en la vista de árbol.

Ilustración 13-26. Configuración global de PIM-SM



La página PIM-SM Global Configuration (Configuración global de PIM-SM) contiene los campos siguientes:

Admin Mode (Modo de administración): (seleccione Enable (Activar) o Disable (Desactivar) en el menú desplegable para definir el estado de administración de PIM-SM en el sistema. Debe activar IGMP antes de activar PIM-SM. El valor predeterminado es Disable (Desactivar).

Join/Prune Interval (secs) (Intervalo de unión/poda [seg.]): introduzca el intervalo entre la transmisión de mensajes de unión y poda de PIM-SM. Los valores válidos están comprendidos entre 10 y 3600 segundos. El valor predeterminado es 60.

Data Threshold Rate (Kbps) (Velocidad de umbral de datos [Kbps]): introduzca la velocidad mínima de datos de origen en kilobits/segundo por encima de la cual el enrutador de último salto cambia a un árbol de ruta de acceso más corta específico del origen. Los valores válidos están comprendidos entre 0 y 2000 kilobits/segundo. El valor predeterminado es 50.

Register Threshold Rate (Kbps) (Velocidad de umbral de registro [Kbps]): introduzca la velocidad mínima de datos de origen en kilobits/segundo por encima de la cual el enrutador de punto de encuentro cambia a un árbol de ruta de acceso más corta específico del origen. Los valores válidos están comprendidos entre 0 y 2000 kilobits/segundo. El valor predeterminado es 50.

Configuración de PIM-SM

1. Abra la página PIM-SM Global Configuration (Configuración global de PIM-SM).
2. Defina **Admin Mode** (Modo de administración) como Enable (Activar) o Disable (Desactivar) para activar o desactivar PIM-SM.
3. Modifique los campos restantes según sea necesario.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz y se actualiza el dispositivo.

Configuración de PIM-SM mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

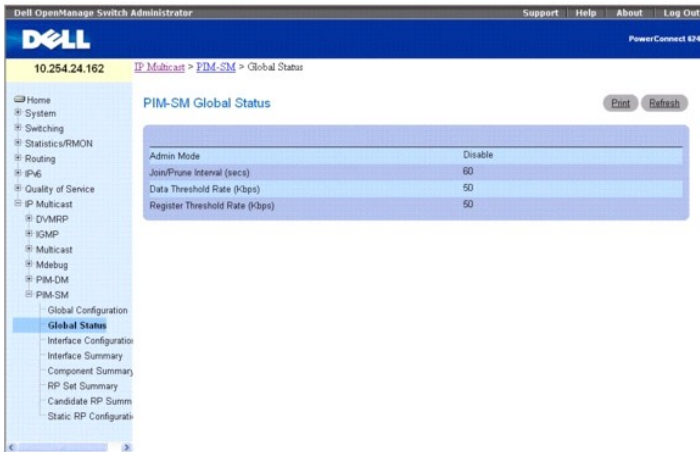
- 1 Comandos de PIM-SM

Estado global de PIM-SM

Utilice la página **PIM-SM Global Status** (Estado global de PIM-SM) para ver los valores globales seleccionados en la página **PIM-SM Global Configuration** (Configuración global de PIM-SM).

Para visualizar la página, haga clic en **Multicast** (Multidifusión) → **PIM-SM** → **Global Status** (Estado global) en la vista de árbol.

Ilustración 13-27. Estado global de PIM-SM



La página **PIM-SM Global Status** (Estado global de PIM-SM) contiene los campos siguientes:

Admin Mode (Modo de administración): estado de administración de PIM-SM en el enrutador con los valores Enable (Activar) o Disable (Desactivar).

Join/Prune Interval (secs) (Intervalo de unión/poda [seg.]): intervalo entre la transmisión de mensajes de unión y poda de PIM-SM.

Data Threshold Rate (Kbps) (Velocidad de umbral de datos [Kbps]): velocidad mínima de datos de origen en kilobits/segundo por encima de la cual el enrutador de último salto cambia a un árbol de ruta de acceso más corta específico del origen.

Register Threshold Rate (Kbps) (Velocidad de umbral de registro [Kbps]): velocidad mínima de datos de origen en kilobits/segundo por encima de la cual el enrutador de punto de encuentro cambia a un árbol de ruta de acceso más corta específico del origen.

Visualización del estado global de PIM-SM mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

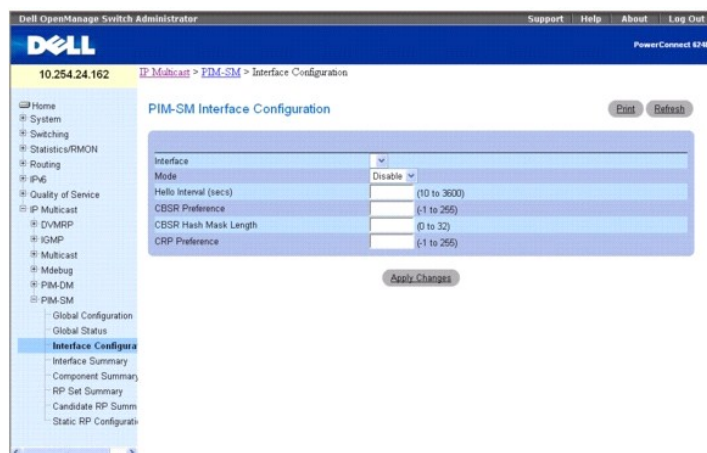
- 1 Comandos de PIM-SM

Configuración de la interfaz PIM-SM

Utilice la página **PIM-SM Interface Configuration** (Configuración de la interfaz PIM-SM) para configurar PIM-SM para una interfaz. PIM-SM debe estar activado en la página **PIM-SM Global Configuration** (Configuración global de PIM-SM) para que se muestre esta página de configuración de la interfaz.

Para visualizar la página, haga clic en **Multicast** (Multidifusión) → **PIM-SM** → **Interface Configuration** (Configuración de interfaz) en la vista de árbol.

Ilustración 13-28. Configuración de la interfaz PIM-SM



La página **PIM-SM Interface Configuration** (Configuración de la interfaz PIM-SM) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar o configurar. Como mínimo, debe haber una interfaz de enrutamiento para mostrar o configurar los datos.

Mode (Modo): seleccione **Enable** (Activar) o **Disable** (Desactivar) en el menú desplegable para definir el estado de administración de PIM-SM en esta interfaz. El valor predeterminado es **Disable** (Desactivar).

Hello Interval (secs) (Intervalo de saludo [seg.]): introduzca el tiempo en segundos entre la transmisión de mensajes de saludo de PIM en esta interfaz. Los valores válidos están comprendidos entre 10 y 3600 segundos. El valor predeterminado es 30.

CBSR Preference (Preferencia CBSR): introduzca el valor de preferencia para la interfaz local como enrutador de inicio automático candidato. El valor -1 se utiliza para indicar que la interfaz local no es una interfaz BSR candidata. Los valores válidos están comprendidos entre -1 y 255. El valor predeterminado es 0.

CBSR Hash Mask Length (Longitud de la máscara hash CBSR): introduzca la longitud de la máscara hash CBSR que se anunciará en los mensajes de inicio automático si esta interfaz se elige como enrutador de inicio automático. Esta longitud de máscara hash se utiliza en el algoritmo hash para seleccionar el RP de un grupo determinado. Los valores válidos están comprendidos entre 0 y 32. El valor predeterminado es 30.

CRP Preference (Preferencia CRP): introduzca el valor de preferencia para la interfaz local como enrutador de inicio automático candidato. El valor -1 se utiliza para indicar que la interfaz local no es una interfaz BSR candidata. Los valores válidos están comprendidos entre -1 y 255. El valor predeterminado es 0.

Configuración de PIM-SM para una interfaz

1. Abra la página **PIM-SM Interface Configuration** (Configuración de la interfaz PIM-SM).
2. Seleccione la interfaz que va a configurar en el campo **Interface** (Interfaz).
3. Seleccione **Enable** (Activar) en el campo **Mode** (Modo).
4. Modifique los campos restantes según sea necesario.
5. Haga clic en **Apply Changes** (Aplicar cambios).

Se guarda la configuración de la interfaz y se actualiza el dispositivo.

Configuración de PIM-SM para una interfaz mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

1. Comandos de PIM-SM

Resumen de interfaces PIM-SM

Utilice la página **PIM-SM Interface Summary** (Resumen de interfaces PIM-SM) para mostrar una interfaz PIM-SM y su configuración. Como mínimo debe haber una interfaz configurada como PIM-SM en este enrutador para que se muestre la página.

Para visualizar la página, haga clic en **Multicast** (Multidifusión) → **PIM-SM** → **Interface Summary** (Resumen de interfaces) en la vista de árbol.

Ilustración 13-29. Resumen de interfaces PIM-SM



La página **PIM-SM Interface Summary** (Resumen de interfaces PIM-SM) contiene los campos siguientes:

Interface (Interfaz): seleccione la interfaz cuyos datos se van a mostrar.

Mode (Modo): estado de administración de PIM-SM en el enrutador con los valores Enable (Activar) o Disable (Desactivar).

Protocol State (Estado del protocolo): estado operativo del protocolo PIM-SM en la interfaz seleccionada, con los valores Operational (Operativo) o Non-operational (No operativo).

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

Net Mask (Máscara de red): máscara de red correspondiente a la dirección IP de la interfaz PIM seleccionada.

Designated Router (Enrutador designado): enrutador designado en la interfaz PIM seleccionada. En las interfaces punto a punto, este objeto tiene el valor 0.0.0.0.

Hello Interval (secs) (Intervalo de saludo [seg.]): frecuencia con la que se transmiten los mensajes de saludo de PIM en la interfaz seleccionada.

CBSR Preference (Preferencia CBSR): valor de preferencia para la interfaz local como enrutador de inicio automático candidato. El valor -1 se utiliza para indicar que la interfaz local no es una interfaz BSR candidata.

CBSR Hash Mask Length (Longitud de la máscara hash CBSR): longitud de la máscara hash CBSR que se anunciará en los mensajes de inicio automático si esta interfaz se elige como enrutador de inicio automático. Esta longitud de máscara hash se utiliza en el algoritmo hash para seleccionar el RP de un grupo determinado.

CRP Preference (Preferencia CRP): valor de preferencia para la interfaz local como enrutador de inicio automático candidato. El valor -1 se utiliza para indicar que la interfaz local no es una interfaz BSR candidata.

Neighbor Count (Recuento de vecinos): número de vecinos PIM en la interfaz seleccionada.

IP Address (Dirección IP): dirección IP del vecino PIM para esta entrada.

Up Time (hh:mm:ss) (Tiempo de actividad [hh:mm:ss]): tiempo transcurrido desde que este vecino PIM fue (por última vez) vecino del enrutador local.

Expiry Time (hh:mm:ss) (Tiempo de caducidad [hh:mm:ss]): tiempo mínimo restante antes de que caduque este vecino PIM.

Visualización del resumen de interfaces PIM-SM

1. Abra la página **PIM-SM Interface Summary** (Resumen de interfaces PIM-SM).
2. Seleccione la interfaz que desea visualizar en el menú desplegable **Interface** (Interfaz).

Se muestran los datos de configuración de PIM-SM para esta interfaz.

Visualización del resumen de interfaces PIM-SM mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de PIM-SM

Resumen de componentes

Utilice la página **Component Summary** (Resumen de componentes) para ver información sobre los componentes PIM-SM.

Para visualizar la página, haga clic en **Multicast (Multidifusión)**→ **PIM-SM**→ **Component Summary** (Resumen de componentes) en la vista de árbol.

Ilustración 13-30. Resumen de componentes



La página **Component Summary** (Resumen de componentes) contiene los campos siguientes:

Component Index (Índice de componentes): número exclusivo que identifica el índice de componentes.

Component BSR Address (Dirección BSR del componente): dirección IP del enrutador de inicio automático (BSR) para la región PIM local.

Component BSR Expiry Time (hh:mm:ss) (Tiempo de caducidad BSR del componente [hh:mm:ss]): tiempo mínimo restante antes de que se declare el enrutador de inicio automático en el dominio local.

Component CRP Hold Time (hh:mm:ss) (Tiempo de espera CRP del componente [hh:mm:ss]): tiempo de espera del componente cuando es un punto de encuentro candidato en el dominio local.

Visualización del resumen de componentes PIM-SM mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

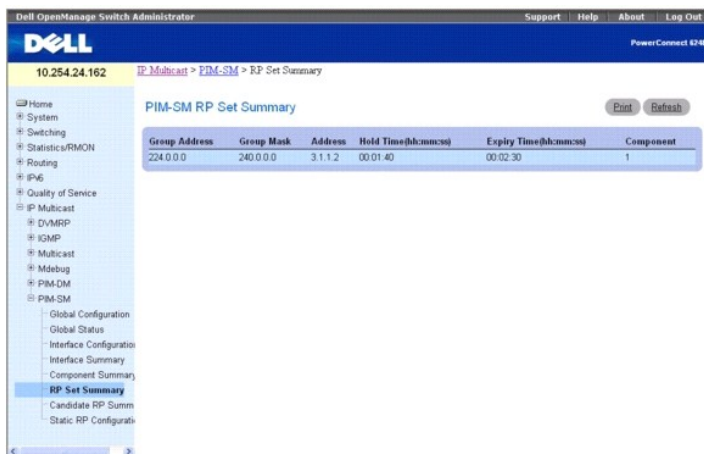
- 1 Comandos de PIM-SM

Resumen de conjuntos de RP

Utilice la página **PIM-SM RP Set Summary** (Resumen de conjuntos de RP de PIM-SM) para ver información sobre el RP estático correspondiente al enrutador PIM-SM.

Para visualizar la página, haga clic en **Multicast (Multidifusión)**→ **PIM-SM**→ **RP Set Summary** (Resumen de conjuntos de RP) en la vista de árbol.

Ilustración 13-31. Resumen de conjuntos de RP de PIM-SM



En la página **PIM-SM RP Set Summary** (Resumen de conjuntos de RP de PIM-SM) se muestran los campos siguientes en una tabla:

Group Address (Dirección de grupo): muestra la dirección del grupo de multidifusión IP.

Group Mask (Máscara de grupo): muestra la máscara de dirección del grupo de multidifusión.

Address (Dirección): muestra la dirección IP del RP candidato.

Hold Time (hh:mm:ss) (Tiempo de espera [hh:mm:ss]): tiempo de espera de un RP candidato. Si el enrutador local no es el BSR, este valor es 0.

Expiry Time (hh:mm:ss) (Tiempo de caducidad [hh:mm:ss]): tiempo mínimo restante antes de que se declare el RP candidato como fuera de servicio.

Component (Componente): número que identifica el componente de manera exclusiva. Cada instancia del protocolo conectada a un dominio distinto debe tener un valor de índice diferente.

Visualización del resumen de conjuntos de RP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

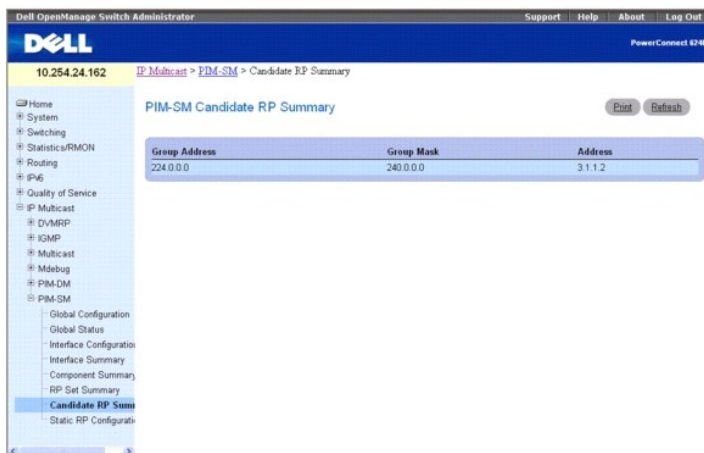
- 1 Comandos de PIM-SM

Resumen de RP candidatos

Utilice la página **PIM-SM Candidate RP Summary** (Resumen de RP candidatos de PIM-SM) para ver información sobre PIM correspondiente a los puntos de encuentro (RP) candidatos para cada grupo de multidifusión IP.

Para visualizar la página, haga clic en **Multicast** (Multidifusión) → **PIM-SM** → **Candidate RP Summary** (Resumen de RP candidatos) en la vista de árbol.

Ilustración 13-32. Resumen de RP candidatos de PIM-SM



Group Address	Group Mask	Address
224.0.0.0	240.0.0.0	3.1.1.2

En la página **PIM-SM Candidate RP Summary** (Resumen de RP candidatos de PIM-SM) se muestran los campos siguientes en una tabla:

Group Address (Dirección de grupo): dirección del grupo transmitida en anuncios de RP candidatos.

Group Mask (Máscara de grupo): máscara de dirección del grupo transmitida en anuncios de RP candidatos para identificar completamente el ámbito del grupo que admite el enrutador si se ha elegido como punto de encuentro.

Address (Dirección): muestra la dirección de difusión única de la interfaz que se anuncia como RP candidato.

Visualización del resumen de RP candidatos de PIM-SM mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

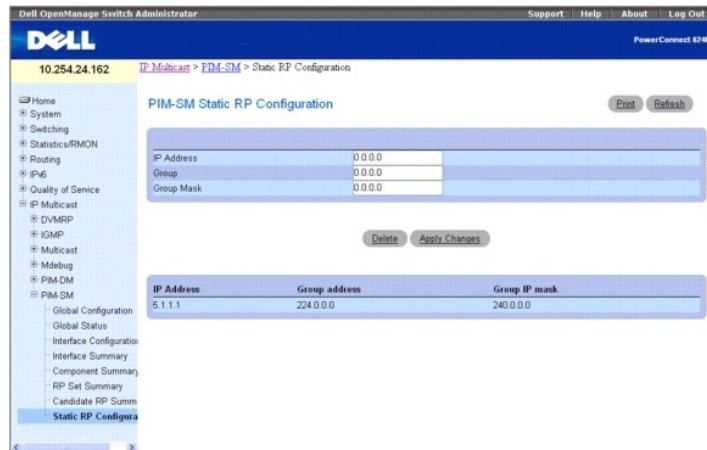
- 1 Comandos de PIM-SM

Configuración de RP estático

Utilice la página **Static RP Configuration** (Configuración de RP estático) para crear la dirección IP del RP estático especificado correspondiente al enrutador PIM-SM.

Para visualizar la página, haga clic en **Multicast** (Multidifusión) → **PIM-SM** → **Static RP Configuration** (Configuración de RP estático) en la vista de árbol.

Ilustración 13-33. Configuración de RP estático



La página **Static RP Configuration** (Configuración de RP estático) contiene los campos siguientes:

IP Address (Dirección IP): dirección IP del RP que va a crearse.

Group (Grupo): dirección de grupo del RP que va a crearse.

Group Mask (Máscara de grupo): máscara IP de grupo del RP que va a crearse.

Las configuraciones existentes se muestran en una tabla en la parte inferior de la página.

Configuración de un RP estático

1. Abra la página **Static RP Configuration** (Configuración de RP estático).
2. Introduzca la dirección IP, la dirección IP del grupo y la máscara de grupo para la configuración del RP estático.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se crea la dirección IP del RP estático especificado para el enrutador PIM-SM y se actualiza el dispositivo.

Configuración de un RP estático mediante el comando de la CLI

Para obtener información sobre el comando de la CLI que realiza esta función, consulte el capítulo siguiente de la *Guía de referencia de la CLI*:

- 1 Comandos de PIM-SM

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de Dell™ PowerConnect™


Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [Inicio de la CLI](#)
- [Información de configuración general](#)
- [Inicio del conmutador](#)
- [Información general sobre configuración](#)
- [Configuración avanzada](#)
- [Descarga de software y reinicio](#)
- [Funciones del menú de inicio](#)
- [Ejemplo de proceso de configuración](#)


En este capítulo se describe la configuración inicial del conmutador. Se tratan los temas siguientes:

- I [Inicio de la CLI](#)
- I [Información de configuración general](#)
- I [Inicio del conmutador](#)
- I [Información general sobre configuración](#)
- I [Configuración avanzada](#)
- I [Descarga de software y reinicio](#)
- I [Funciones del menú de inicio](#)
- I [Ejemplo de proceso de configuración](#)

Cuando se hayan realizado todas las conexiones externas, conecte un terminal al conmutador para supervisar el inicio y otros procedimientos.


 **NOTA:** si instala una *pila* de conmutadores, conecte el terminal al conmutador maestro. La primera vez que se enciende una pila, los conmutadores eligen el conmutador que debe actuar como maestro, que puede ocupar cualquier posición de la pila. Este conmutador tendrá encendido el LED de conmutador maestro. Si conecta el terminal a un conmutador subordinado, no podrá utilizar la CLI.

A continuación, siga el orden de los procedimientos de instalación y configuración que se muestran en la [ilustración 5-1](#). Para la configuración inicial, configure el conmutador de manera estándar. La ejecución de otras funciones se describe más adelante en esta sección.

 **AVISO:** antes de continuar, lea las notas de la versión de este producto. Puede descargar las notas de la versión de la página web de asistencia de Dell (support.dell.com).

Inicio de la CLI

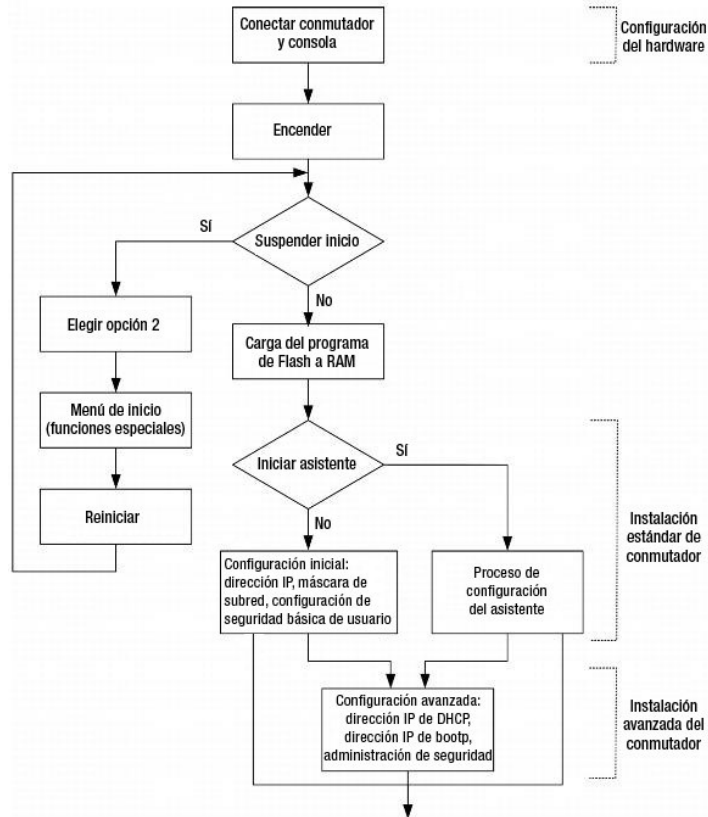
Para empezar a ejecutar la CLI, realice los pasos siguientes:

 **NOTA:** los pasos que se describen a continuación sólo deben utilizarse en la línea de consola.

1. Inicie el conmutador y espere a que finalice el procedimiento de inicio. Una vez finalizado, aparece el mensaje de bienvenida a **Easy Setup Wizard** (Asistente para configuración fácil).
2. Configure el conmutador mediante **Easy Setup Wizard** e introduzca los comandos pertinentes para realizar las tareas necesarias.
3. Cuando haya terminado, salga de la sesión con el comando **quit** o **exit**.

El conmutador (o la pila) puede administrarse a través de una conexión directa con el puerto de consola del conmutador o de una conexión Telnet. Puede acceder al conmutador sin tener una cuenta de usuario si está conectado directamente al conmutador. Sin embargo, para acceder al conmutador a través de Telnet, debe haber una cuenta de usuario definida como mínimo. Asimismo, si se accede a través de una conexión Telnet, el conmutador debe tener una dirección IP definida, el acceso correspondiente a la administración otorgado y una estación de trabajo conectada al conmutador antes de utilizar los comandos de la CLI.

Ilustración 5-1. Diagrama de flujo de instalación y configuración



Información de configuración general

Los conmutadores de la serie 6200 se entregan con archivos binarios que contienen el sistema operativo del conmutador y con archivos de configuración ASCII que definen la relación del conmutador con el entorno de red. El proceso de configuración consiste en ajustar los archivos de configuración ASCII de modo que el conmutador encaje en su topología de red única.

Negociación automática

La negociación automática permite que un conmutador (o una pila que funciona como una sola unidad) anuncie modos de funcionamiento y comparta información con otro conmutador con el que comparte un segmento de enlace punto a punto. De este modo, se configuran automáticamente los dos conmutadores para beneficiarse al máximo de sus capacidades.

La negociación automática se realiza por completo en las capas físicas durante el inicio del enlace, sin sobrecarga adicional del MAC o de las capas de protocolo superiores. La negociación automática permite que los puertos realicen lo siguiente:

- 1 Anunciar sus capacidades
- 1 Confirmar el recibo y comprensión de los modos comunes de funcionamiento que comparten ambos conmutadores
- 1 Rechazar el uso de modos operativos que no comparten ambos conmutadores
- 1 Configurar cada puerto para obtener el modo operativo de máximo nivel que ambos puertos pueden admitir

NOTA: asegúrese de que utiliza la negociación automática en ambos lados del enlace, siempre que sea posible, para evitar posibles problemas.

Si va a conectar un puerto del conmutador a la tarjeta de interfaz de red (NIC) de una estación de trabajo o servidor que no admite la negociación automática, o no está configurada para ésta, se requieren varios pasos adicionales. El puerto de conmutación y la NIC deben configurarse manualmente con la misma velocidad y modo dúplex. Este proceso puede realizarse mediante la interfaz del explorador web o mediante los comandos de la CLI.

AVISO: si la estación del otro lado del enlace intenta realizar una negociación automática con un puerto que está configurado para el modo dúplex completo, el resultado de la negociación automática es que la estación intentará funcionar en modo semidúplex. La discrepancia resultante puede provocar una pérdida de tramas considerable. Se trata de una consecuencia inherente al estándar de negociación automática.

Configuración de conexión a través del terminal

El conmutador requiere la configuración de los parámetros de conexión a través del terminal siguientes:

- | Sin paridad
- | 1 bit de paro
- | 8 bits de datos
- | Sin control de flujo


Velocidad en baudios

La velocidad en baudios puede modificarse manualmente a cualquiera de los valores siguientes:

- | 2400
- | 4800
- | 9600 (velocidad en baudios predeterminada)
- | 19200
- | 38400
- | 57600
- | 115200

A continuación figura un ejemplo de configuración para cambiar la velocidad en baudios predeterminada mediante los comandos de la CLI:

```
console#configure
console(config)#line console
console(config-line)#speed 115200
```

 **NOTA:** no olvide definir la velocidad en baudios en el software emulador de terminal de la estación de trabajo para que coincida con la velocidad del conmutador.

Otros requisitos de configuración

Los requisitos siguientes son necesarios para descargar el software incorporado y configurar el conmutador:

- | Terminal ASCII (o emulación) conectado al puerto serie (cable cruzado) de la parte posterior de la unidad
- | Dirección IP asignada al conmutador para que pueda utilizarse el mando a distancia de éste con Telnet, SSH, etc.

Inicio del conmutador

Cuando la alimentación se enciende con el terminal local ya conectado, el conmutador realiza la autoprueba de encendido (POST). La POST se ejecuta cada vez que se inicializa el conmutador y comprueba los componentes de hardware para determinar si es totalmente funcional antes del inicio completo.

Si se detecta un problema crítico, el flujo de programa se detiene. Si la POST se ejecuta correctamente, se carga una imagen ejecutable válida en la RAM.

Se muestran mensajes de la POST en el terminal que indican si la prueba ha finalizado correctamente o no.

Para iniciar el conmutador, realice los pasos siguientes:

1. Asegúrese de que el cable serie esté conectado al terminal.
2. Conecte la fuente de alimentación al conmutador.
3. Encienda el conmutador.

Cuando se inicia el conmutador, la prueba de inicio solicita primero la disponibilidad de la memoria del conmutador y, a continuación, prosigue con el inicio.

4. Durante el inicio, puede utilizar el menú **Boot** (Inicio) si es necesario para ejecutar procedimientos especiales. Para acceder al menú **Boot** (Inicio), pulse **2** en los 10 segundos posteriores a la aparición del mensaje siguiente:

```
Select an option. If no selection in 10 seconds then
operational code will start.
1 - Start operational code.
2 - Start Boot Menu.

Select (1, 2):2
```

Para obtener información sobre el menú **Boot** (Inicio), consulte "[Funciones del menú de inicio](#)". El texto que figura a continuación es un ejemplo de la POST completa que se muestra:

```
CPU Card ID: 0x508541

volume descriptor ptr (pVolDesc): 0xffefd00

cache block I/O descriptor ptr (cbio): 0xffefde0

auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0

# of different files in use: 0

# of descriptors for deleted files: 0

# of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL; (in boot sector: )

- volume Id: 0x0

- total number of sectors: 60,716

- bytes per sector: 512

- # of sectors per cluster: 4

- # of reserved sectors: 1

- FAT entry size: FAT16

- # of sectors per FAT copy: 60

- # of FAT table copies: 2

- # of hidden sectors: 4

- first cluster is in sector # 136

- Update last access date for open-read-close = FALSE

- directory structure: VFAT

- root dir start sector: 121

- # of sectors per root: 15

- max # of entries in root: 240

FAT handler information:

-----

- allocation group size: 2 clusters

- free space on volume: 15,335,424 bytes

Boot Menu Version: 22 Dec 2006

Select an option. If no selection in 10 seconds then

operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

Boot Menu Version: 22 Dec 2006

Options available (Opciones disponibles)


1 - Start operational code (Iniciar código operativo)

2 - Change baud rate (Cambiar velocidad en baudios)
```

- 3 - Retrieve event log using XMODEM (Recuperar el registro de eventos mediante XMODEM)
 - 4 - Load new operational code using XMODEM (Cargar un código operativo nuevo mediante XMODEM)
 - 5 - Display operational code vital product data (Ver el código operativo de datos de productos vitales)
 - 6 - Run flash diagnostics (Ejecutar diagnósticos de la memoria flash)
 - 7 - Update boot code (Actualizar código de inicio)
 - 8 - Delete backup image (Eliminar imagen de copia de seguridad)
 - 9 - Reset the system (Restablecer el sistema)
 - 10 - Restore configuration to factory defaults (delete config files) (Restablecer la configuración a los valores predeterminados de fábrica [eliminar los archivos de configuración])
 - 11 - Activate Backup Image (Activar imagen de copia de seguridad)
 - 12 - Password Recovery Procedure (Procedimiento de recuperación de contraseña)
- [Boot Menu]

El proceso de inicio dura aproximadamente 60 segundos.

El mensaje de inicio automático que aparece al final de la POST (vea las últimas líneas) indica que no ha habido problemas durante el inicio. Para volver al código operativo desde el indicador [Boot Menu] (Menú de inicio), pulse 1.

 **NOTA:** a continuación se muestra un ejemplo de configuración. Algunos elementos como direcciones, versiones y fechas pueden variar según el conmutador.

Operational Code Date: Fri May 4 07:44:08 2007

Uncompressing....

50% 100%

|||||

Attaching interface lo0...done

Adding 36263 symbols for standalone.

volume descriptor ptr (pVolDesc): 0xffc0650

cache block I/O descriptor ptr (cbio): 0xffc0730

auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0

of different files in use: 0

of descriptors for deleted files: 0

of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL; (in boot sector:)

- volume Id: 0x0

- total number of sectors: 60,716

- bytes per sector: 512

- # of sectors per cluster: 4

- # of reserved sectors: 1

- FAT entry size: FAT16

- # of sectors per FAT copy: 60

- # of FAT table copies: 2

- # of hidden sectors: 4

- first cluster is in sector # 136

```

- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240
FAT handler information:
-----
- allocation group size: 2 clusters
- free space on volume: 15,337,472 bytes
Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz, CPU: 533.33332
8 MHz
SOC unit 0 attached to PCI device BCM56314_A0
SOC unit 1 attached to PCI device BCM56314_A0
Adding BCM transport pointers
Configuring CPUTRANS TX
Configuring CPUTRANS RX
hpc - No stack ports. Starting in stand-alone mode.
(Unit 1 - Waiting to select management unit)>
<188> JAN 01 00:00:08 0.0.0.0-1 POE[254746256]: broad_poe.c(286) 4 % Unable to set POE Power bank 73
Applying configuration, please wait ...
No Potential unit to configure as Standby when unit 1 joined
<187> JAN 01 00:00:13 192.168.2.1-1 UNITMGR[244207968]: unitmgr.c(4490) 15 % No
Potential unit to configure as Standby when unit 1 joined
....
console>

```

Una vez que el conmutador se inicie correctamente, aparece un indicador y puede utilizar el terminal local para empezar a configurar el conmutador. Sin embargo, antes de configurar el conmutador, asegúrese de que la versión del software instalada en el conmutador es la más reciente. Si no es así, descargue e instale la última versión. Consulte "[Descarga de software y reinicio](#)".


Información general sobre configuración

Antes de configurar el conmutador, solicite al administrador de red la información siguiente:

- 1 Máscara de subred IP para la red
- 1 Dirección IP de la puerta de enlace predeterminada (enrutador del siguiente salto) para configurar la ruta predeterminada

Existen dos tipos de configuración:

- 1 La configuración *inicial* consta de funciones de configuración con consideraciones de seguridad básicas.
- 1 La configuración *avanzada* incluye la configuración de IP dinámica y consideraciones de seguridad más avanzadas.

 **AVISO:** tras realizar cualquier cambio en la configuración, la nueva configuración debe guardarse antes de reiniciar. Para guardar la configuración, introduzca:

```
console#copy running-config startup-config
```

Easy Setup Wizard

Easy Setup Wizard (Asistente para configuración fácil) se abre cuando se inicia el sistema sin configuración o únicamente con la configuración predeterminada de fábrica. Este asistente le guiará por los pasos iniciales para definir la configuración y la seguridad básicas del sistema y para administrar el conmutador. **Easy Setup Wizard** requiere que la cuenta del administrador inicial esté configurada al encender el conmutador. Esta configuración de la cuenta de administración mediante el asistente tiene el máximo nivel de privilegios (nivel 15).

Easy Setup Wizard le guía por la configuración inicial básica de un conmutador recién instalado a fin de que sea funcional y pueda implantarse

inmediatamente y administrarse por completo a través de la web, de la CLI y de Dell Network Manager remoto. Tras realizar la configuración inicial, puede acceder al sistema para definir una configuración más avanzada.

De manera predeterminada, el conmutador se entrega con la dirección IP 192.168.2.1 y la máscara de red 255.255.255.0. El sistema está configurado con la ID de VLAN de administración predeterminada = 1. La configuración inicial debe realizarse a través de la interfaz serie, ya que no puede acceder a otras interfaces de administración sin una dirección IP.

El asistente realiza la configuración siguiente en el conmutador:

- 1 Establece la cuenta de usuario con privilegios inicial con una contraseña válida. El asistente configura una cuenta de usuario con privilegios durante la configuración. Se concede el nivel máximo de privilegios (nivel 15) a la cuenta inicial.
- 1 Activa el uso exclusivo de la autenticación local en el inicio de sesión de la CLI y el acceso HTTP/HTTPS. Posteriormente podrá configurar Radius o TACACS+.
- 1 Configura la dirección IP para la VLAN de administración.
- 1 Configura la cadena de comunidad SNMP que va a utilizar el administrador SNMP en una dirección IP determinada. Puede saltarse este paso si no utiliza la administración SNMP en este conmutador. Si se configura, se establece el nivel de acceso predeterminado superior para la interfaz de administración SNMP. Inicialmente sólo se activa SNMPv1/2c. SNMPv3 se desactiva hasta que vuelva a configurar el acceso de seguridad para SNMPv3 (por ejemplo, ID de motor, vista, etc.). La cadena de comunidad SNMP puede incluir espacios. El asistente requiere el uso de comillas si desea introducir espacios en la cadena de comunidad. A pesar de que se pueden introducir espacios en la cadena de comunidad, no se aconseja utilizarlos. La cadena de comunidad predeterminada no contiene espacios.
- 1 Permite especificar la IP del servidor de administración o permite el acceso SNMP desde todas las direcciones IP.
- 1 Configura la dirección IP de la puerta de enlace predeterminada.

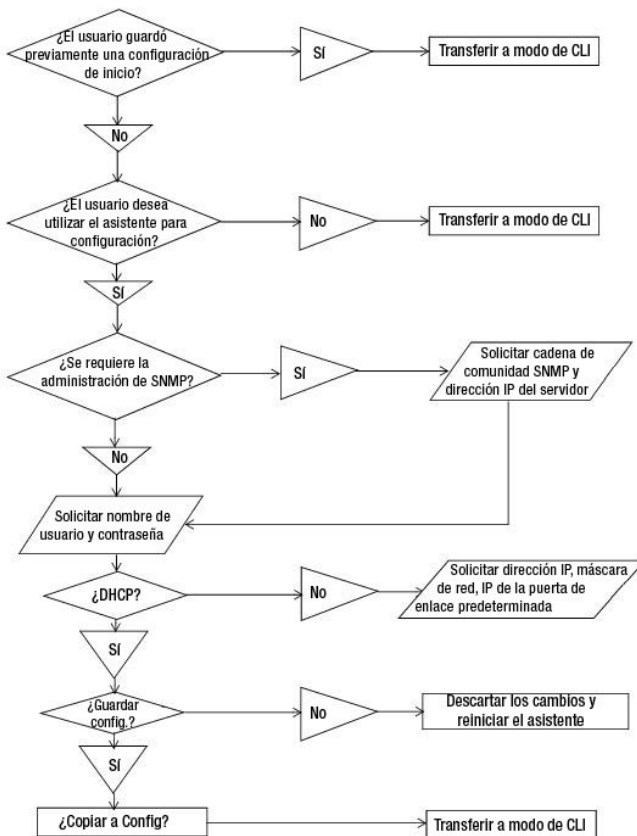
Si no utiliza el asistente inicialmente, la sesión adopta como valor predeterminado el modo de la CLI. El asistente para configuración se mostrará cada vez que inicie la sesión hasta que se guarde una configuración. Cuando se haya guardado, la opción del asistente sólo volverá a aparecer si restablece el conmutador a la configuración predeterminada de fábrica.

Dado que un conmutador puede encenderse en el campo sin una conexión serie, el conmutador espera 60 segundos a que el usuario responda a un indicador de configuración, si todavía no se ha configurado el conmutador. Si no se da una respuesta, el conmutador continúa con el funcionamiento normal utilizando la configuración predeterminada de fábrica. La próxima vez que se reinicie el sistema, tendrá otra oportunidad para ejecutar el asistente para configuración.

Flujo de funcionamiento

En el diagrama de flujo de funcionamiento que figura a continuación se ilustran los procedimientos de Easy Setup Wizard.

Ilustración 5-2. Diagrama de flujo del asistente para configuración




Ejemplo de una sesión con Easy Setup Wizard

En esta sección se describe una sesión con Easy Setup Wizard. Consulte el diagrama de estado de la sección anterior para ver el flujo general. Los valores que se utilizan en la siguiente sesión son sólo ejemplos. Solicite los valores reales al administrador de red:

- 1 La dirección IP para la VLAN de administración es 192.168.1.1:255.255.255.0.
- 1 El nombre de usuario es *admin* y la contraseña es *admin123*.
- 1 La dirección IP del sistema de administración de red es 192.168.1.10.
- 1 La puerta de enlace predeterminada es 192.168.1.100.
- 1 La cadena de comunidad SNMP que se va a utilizar es *Dell_Network_Manager*.

El asistente para configuración define los valores iniciales como se ha indicado anteriormente. Cuando haya completado el asistente, el sistema queda configurado de la siguiente manera:

- 1 Se ha activado SNMPv1/2c y la cadena de comunidad se ha configurado de la forma indicada anteriormente. SNMPv3 está desactivado.
- 1 Se ha configurado la cuenta de usuario *admin* de la forma indicada.
- 1 Se ha configurado un sistema de administración en red. Desde esta estación de administración puede acceder a las interfaces SNMP, HTTP y CLI. También puede permitir que todas las direcciones IP tengan acceso a estas interfaces de administración especificando la dirección IP (0.0.0.0).
- 1 Se ha configurado una dirección IP para la VLAN de administración predeterminada (1).
- 1 Se ha configurado una dirección de puerta de enlace predeterminada.

 **NOTA:** en el ejemplo siguiente las opciones de usuario posibles se incluyen entre corchetes []. Además, cuando procede se incluye el valor predeterminado entre llaves { }. Si pulsa <Intro> sin definir opciones, se aceptará el valor predeterminado. El texto de ayuda se muestra entre paréntesis.

En el ejemplo siguiente se muestra la secuencia de indicadores y respuestas asociados a la ejecución de un ejemplo de sesión de Easy Setup Wizard de Dell con los valores indicados anteriormente.

```
Welcome to Dell Easy Setup Wizard
```

```
The setup wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. Note: You can exit the setup wizard at any point by entering [ctrl+z].
```

```
Would you like to run the set up wizard (you must answer this question within 60 seconds)? [Y/N] y
```

Paso 1:

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

- o Set up the initial SNMP version 2 account now.
- o Return later and set up other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

```
Would you like to set up the SNMP management interface now? [Y/N] y
```

```
To set up the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell Network Manager or other management interfaces to change this setting and to add additional management system later. For more information on adding management systems, see the user documentation.
```

```
To add a management station:
```

```
Please enter the SNMP community string to be used {public}:
```

```
>> Dell_Network_Manager<Intro>
```

```
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station {0.0.0.0}:
```

```
>> 192.168.2.10<Intro>
```

Paso 2:


```
Now we need to set up your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may set up other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.
```

```
To set up a user account:
```

```
Please enter the user name {admin}: admin<Intro>
```

```
Please enter the user password: *****<Intro>
```

```
Please reenter the user password: *****<Intro>
```

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

Paso 3:

Next, an IP address is set up. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network).


To set up an IP address:

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server (192.168.2.1):

```
>> 192.168.2.1<Intro>
```


Please enter the IP subnet mask (A.B.C.D or /nn){255.255.255.0}:

```
>> 255.255.255.0<Intro>
```

 **NOTA:** si ha seleccionado DHCP anteriormente, el sistema no solicitará la máscara de subred IP, ya que el servidor DHCP proporciona esta información.

Paso 4:

Finally, set up the default gateway. Please enter the IP address of the gateway from which this network is reachable (for example 0.0.0.0): >> 192.168.2.100<Intro>

 **NOTA:** si ha seleccionado DHCP anteriormente, el sistema no solicitará una puerta de enlace predeterminada, ya que el servidor DHCP proporciona esta información.

This is the configuration information that has been collected:

SNMP Interface = "Dell_Network_Manager"@192.168.1.10

User Account set up = admin

Password = *****

Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 192.168.2.100

Paso 5:

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

Thank you for using Dell Easy Set up Wizard. You will now enter CLI mode.

Configuración avanzada

Conceptos básicos de la CLI

El comando help de los modos User EXEC y Privileged EXEC muestra los accesos directos del teclado. A continuación se muestra la pantalla de ejemplo del comando help:

```
Console>help

HELP (AYUDA):

Special keys (Teclas especiales):

DEL, BS .... delete previous character (borrar el carácter anterior)

Ctrl-A .... go to beginning of line (ir al principio de la línea)

Ctrl-E .... go to end of line (ir al final de la línea)

Ctrl-F .... go forward one character (avanzar un carácter)

Ctrl-B .... go backward one character (retroceder un carácter)

Ctrl-D .... delete current character (borrar el carácter actual)

Ctrl-U, X .. delete to beginning of line (borrar hasta el principio de la línea)

Ctrl-K .... delete to end of line (borrar hasta el final de la línea)

Ctrl-W .... delete previous word (borrar la palabra anterior)
```

Ctrl-T transpose previous character (transponer el carácter anterior)

Ctrl-P go to previous line in history buffer (ir a la línea anterior del búfer de historial)

Ctrl-R rewrites or pastes the line (volver a escribir o pegar la línea)

Ctrl-N go to next line in history buffer (ir a la línea siguiente del búfer de historial)

Ctrl-Y print last deleted character (imprimir el último carácter borrado)

Ctrl-Z return to root command prompt (volver al indicador de comandos raíz)

Ctrl-Q enables serial flow (activar el flujo serie)

Ctrl-S disables serial flow (desactivar el flujo serie)

Tab, <SPACE> command-line completion (tecla de tabulación, <ESPACIO> finalización de la línea de comandos)

Exit go to next lower command prompt (ir al siguiente indicador de comandos inferior)

? list choices (enumerar opciones)

Ayuda contextual

Utilice el comando `?` para obtener ayuda contextual en la CLI. Puede utilizarse para obtener la lista de posibles comandos secundarios o para enumerar los posibles comandos que empiezan por algunos que se han introducido parcialmente. El comando `?`, si se especifica en una línea vacía, proporciona la lista de comandos posibles para el nivel específico del árbol de comandos. También puede utilizarse en una entrada de comando para volver a la lista de parámetros que se necesitan para completar el comando. Los parámetros que el usuario ya ha proporcionado no aparecen en la lista de comandos, de modo que sólo se enumeran los parámetros que faltan.

Convención para la asignación de nombres de interfaz

En una implementación de la CLI estándar, existe una convención aceptada para asignar nombres a las interfaces de la CLI. La convención para asignar nombres a las interfaces de los dispositivos Dell es la siguiente:

- 1 **N.º de unidad/ID de interfaz:** cada interfaz se identifica mediante el *n.º de unidad* seguido del símbolo */y*, a continuación, la *ID de interfaz* (vea la explicación que figura más adelante). Por ejemplo, **2/g10** identifica el puerto Gigabit 10 de la segunda unidad de una pila.
- 1 **N.º de unidad:** el número de unidad sólo se utiliza en una solución de apilamiento en que ciertos conmutadores están apilados para formar un dispositivo virtual. En este caso, el *número de unidad* es el identificador de dispositivo físico de la pila.
- 1 **ID de interfaz:** está formada por el tipo de interfaz seguido del número de interfaz. Existe una lista predefinida de *tipos de interfaz* (vea la explicación que figura más adelante). Si van a definirse tipos de interfaz adicionales, deben registrarse en Dell. Por ejemplo, **2/g10** identifica el puerto Gigabit 10 de la segunda unidad.
- 1 **Tipos de interfaz:** los siguientes tipos de interfaz se definen en los conmutadores de la serie 6200:
 - o **g:** puerto Ethernet Gigabit (por ejemplo, **1/g2** es el puerto Ethernet Gigabit 2).
 - o **xg:** puerto Ethernet Gigabit 10 (por ejemplo, **1/xg2** es el puerto Ethernet Gigabit 10 2).

Guía de referencia de la CLI de los sistemas PowerConnect 6200

Para obtener información detallada sobre todos los comandos de la CLI disponibles para los conmutadores de la serie 6200, consulte la *Guía de referencia de la CLI*.

En esta sección se proporciona información de resumen sobre las tareas comunes siguientes:

- 1 [Modificación de la configuración predeterminada de los puertos de conmutación](#)
- 1 [Recuperación de una dirección IP de un servidor DHCP](#)
- 1 [Configuración de una contraseña inicial de consola](#)
- 1 [Configuración de una contraseña inicial de Telnet](#)
- 1 [Configuración de una contraseña inicial de HTTP](#)
- 1 [Configuración de una contraseña inicial de HTTPS](#)

Modificación de la configuración predeterminada de los puertos de conmutación

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

Al iniciar sesión por primera vez, la CLI accede a la raíz de la jerarquía de comandos. Para ir a un nivel distinto de la jerarquía de comandos, introduzca comandos como `configure`, que permite que la CLI acceda al subárbol `config`. Para volver al nivel anterior de la jerarquía de comandos, utilice el comando `exit`.

```
SwitchA#configure
SwitchA(config)#exit
```

SwitchA#

En los ejemplos siguientes se muestran las líneas de comandos que utilizan los conmutadores de la serie 6200:

- 1 **SwitchA>**: indica que el nombre del dispositivo es *SwitchA* y que la CLI se encuentra en el nivel superior de la jerarquía de comandos. La CLI también está en *modo User EXEC*.
- 1 **SwitchA#**: este indicador es similar al indicador anterior, excepto que # indica que la CLI está en modo Privileged EXEC (no en modo User EXEC).
- 1 **SwitchA(config)#**: indica que la CLI está en modo *Global Configuration* de la jerarquía de comandos. Acceda a este modo escribiendo **configure** en el nivel superior.
- 1 **SwitchA(config-if)#**: este indicador indica que la CLI está en modo de configuración *Interface*. Acceda a este modo escribiendo **interface range ethernet**, **interface range port-channel** o **interface range vlan** en el modo de configuración. En este caso, no hay ninguna referencia específica a una interfaz, por lo que el sistema funciona en un conjunto genérico de interfaces.
- 1 **SwitchA(config-if-1/g1)#**: indica que la CLI funciona en la interfaz Ethernet Gigabit 1.

Configuración predeterminada de los puertos de conmutación

En la tabla siguiente se describe la configuración predeterminada de los puertos de conmutación.

Tabla 5-1. Configuración predeterminada de los puertos

Función	Configuración predeterminada
Modo y velocidad del puerto	Negociación automática 1000M
Estado de reenvío del puerto	Activado
Prevención de bloqueo de cabecera de línea	Activada
Control de flujo	Desactivado
Contrapresión	Desactivada

A continuación figura un ejemplo para cambiar la velocidad del puerto 1/ g1 mediante los comandos de la CLI:


```
console(config)#interface ethernet 1/g1  
  
console(config-if-1/g1)#speed 100
```

Recuperación de una dirección IP de un servidor DHCP

Cuando se utiliza el protocolo DHCP para recuperar una dirección IP, el conmutador actúa como cliente DHCP.

Para recuperar una dirección IP de un servidor DHCP, realice los pasos siguientes:

Seleccione un puerto y conéctelo a un servidor DHCP o a una subred que contenga un servidor DHCP para recuperar la dirección IP.

 **NOTA:** no es necesario eliminar la configuración del conmutador para recuperar una dirección IP correspondiente al servidor DHCP.

1. Introduzca los comandos siguientes para utilizar el puerto seleccionado para recibir la dirección IP.

- 1 Asignación de direcciones IP dinámicas:

```
console#config  
  
console(config)#ip address dhcp
```

La interfaz recibe la dirección IP automáticamente.

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

```
console#show ip interface  
  
Management Interface:  
  
IP Address..... 10.240.4.125  
  
Subnet Mask..... 255.255.255.0  
  
Default Gateway..... 10.240.4.1  
  
Burned In MAC Address..... 00:10:18:82:04:35  
  
Network Configuration Protocol Current..... DHCP  
  
Management VLAN ID..... 1
```

```

Routing Interfaces:
                                     Netdir Multi
Interface IP Address IP Mask Bcast CastFwd
-----
vlan1      192.168.10.10 255.255.255.0 Disable Disable
vlan2      0.0.0.0 0.0.0.0 Enable Disable
loopback2 0.0.0.0 0.0.0.0 Disable Disable

```

Gestión de la seguridad y configuración de contraseñas


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

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

Configuración de contraseñas de seguridad

Las contraseñas de seguridad pueden configurarse para los servicios siguientes:

- 1 Consola
- 1 Telnet
- 1 SSH
- 1 HTTP
- 1 HTTPS

 **NOTA:** al crear un nombre de usuario, la prioridad predeterminada es "1", que otorga el acceso pero no derechos de configuración. Se debe establecer una prioridad de "15" para permitir el acceso al conmutador y otorgar derechos de configuración.

Configuración de una contraseña inicial de consola

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

```

console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line console
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password secret123

```

- 1 Al iniciar sesión por primera vez en un conmutador a través de una sesión de consola, introduzca **secret123** en el indicador de contraseña.
- 1 Cuando cambie el modo de un conmutador a activado, introduzca **secret123** en el indicador de contraseña.

Configuración de una contraseña inicial de Telnet

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

```

console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line telnet
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password pass1234

```

- 1 Al iniciar sesión por primera vez en un conmutador a través de una sesión Telnet, introduzca **pass1234** en el indicador de contraseña.
- 1 Cuando cambie el modo de un conmutador a activado, introduzca **pass1234**.

Configuración de una contraseña inicial de HTTP


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

```
console(config)#ip http authentication local  
  
console(config)#username admin password user1234 level 15
```


Configuración de una contraseña inicial de HTTPS

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


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

 **NOTA:** debe crear un certificado de cifrado nuevo cada vez que actualice la aplicación del software de control (o instale una nueva versión) en el conmutador.

Escriba una vez los comandos siguientes durante la configuración del uso de una sesión HTTPS a través de una sesión SSH, Telnet o de consola.

 **NOTA:** en el explorador web, active SSL 2.0 o superior para que aparezca el contenido de la página.


```
console(config)#crypto certificate 1 generate  
  
console(config)#ip https server
```

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

Descarga de software y reinicio

Descarga de software a través de XModem

En esta sección se incluyen instrucciones para descargar software del conmutador (imágenes del sistema y de inicio) mediante XModem, que es un protocolo de transferencia de datos para actualizar los archivos de configuración de copia de seguridad.

 **NOTA:** debe estar conectado a la interfaz de consola serie al descargar software, ya que la descarga de xmodem no funciona en ninguna otra aplicación.

Para descargar un archivo de imagen de software mediante XModem:

Especifique la ruta del archivo de origen para iniciar el proceso de transferencia.


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

```
console#copy xmodem image  
  
Mode..... XMODEM  
  
Data Type..... Code  
  
Destination Filename..... image2  
  
Management access will be blocked for the duration of the transfer  
  
Are you sure you want to start? (y/n) y  
  
console#boot system image2
```

Descarga de software a través del servidor TFTP

En esta sección se incluyen instrucciones para descargar software del conmutador (imágenes del sistema y de inicio) a través de un servidor TFTP. Antes de descargar el software, el servidor TFTP debe estar disponible en la red.

El conmutador se inicia y se ejecuta al descomprimir la imagen del sistema desde el área de la memoria flash en la que se almacena una copia de la imagen del sistema.

 **AVISO:** debe ejecutar el comando **boot system** para activar la imagen que se acaba de descargar.

En el próximo inicio, el conmutador descomprime y ejecuta la imagen del sistema 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 del conmutador y que puedan enviarse comandos ping a un servidor TFTP.
2. Asegúrese de que el archivo que se descarga se guarde en el servidor TFTP (archivo .stk).
3. Introduzca el comando **show version** para comprobar qué versión del software se está ejecutando actualmente en el conmutador.

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

```
console>show version

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash
-----unit image1 image2 current-active next-active
-----

1 0.15.0.0 0.15.0.0 image1 image1
```

4. Introduzca el comando **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

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash
-----unit image1 image2 current-active next-active
-----

1 0.15.0.0 0.15.0.0 image1 image1
```

5. Introduzca el comando **copy tftp://{dirección tftp}/{nombre de archivo} image2** para copiar una nueva imagen del sistema en el conmutador.

Cuando se descarga la nueva imagen, se guarda en el área asignada para la otra copia de la imagen del sistema (image2, como se muestra en el ejemplo). A continuación se muestra un ejemplo de la información que aparece:

```
console#copy tftp://10.254.24.64/pc62xxr0v34.stk image2

Mode..... TFTP

Set TFTP Server IP..... 10.254.24.64

TFTP Path..... ./

TFTP Filename..... pc62xxr0v34.stk

Data Type..... Code

Destination Filename..... image2

Management access will be blocked for the duration of the transfer

Are you sure you want to start? (y/n) y
```

Los signos de exclamación indican que el proceso de copia se encuentra en curso. Un punto indica que el proceso de copia ha superado el tiempo de espera. Una fila con varios puntos indica que el proceso de copia ha fallado.

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

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


```
console#boot system image2
```

```
Activating image image2 ..
```

```
console>show bootvar
```

```
Image Descriptions
```

```
image1 : default image
```

```
image2 :
```

```
Images currently available on Flash
```

```
-----unit image1 image2 current-active next-active
```

```
-----
```

```
1 0.15.0.0 0.15.0.0 image1 image2
```

Si la imagen para el próximo inicio no se selecciona mediante el comando **boot system**, el sistema se inicia desde la imagen activa actualmente (image1, como se muestra en el ejemplo).

7. Introduzca el comando **reload**. Aparece el mensaje siguiente:

```
console#reload
```

```
Management switch has unsaved changes.
```

```
Are you sure you want to continue? (y/n)
```

8. Introduzca **y**. Aparece el mensaje siguiente.

```
Configuration Not Saved!
```

```
Are you sure you want to reload the stack? (y/n)
```

9. Introduzca **y** para reiniciar el conmutador.

Update Bootcode

Utilice el comando **update bootcode** para actualizar el código de inicio de todos los conmutadores. Para cada conmutador, el código de inicio se extrae de la imagen activa y se programa para la memoria flash. Para actualizar el código de inicio de un conmutador, especifique la unidad en el comando (como se muestra en el ejemplo siguiente).

Para ver el código de inicio de un conmutador, reinicie ese conmutador. Las fechas de creación se muestran durante el proceso de inicio.

1. Introduzca el comando siguiente, donde 2 es el número de la unidad:

```
console# update bootcode 2
```

```
Updating boot code ...
```

```
Boot code update completed successfully.
```

2. Introduzca el comando **reload**.

```
console#reload
```

```
Are you sure you want to reload the stack? (y/n)
```

3. Introduzca **y** para reiniciar el conmutador.

Funciones del menú de inicio

Puede realizar muchas tareas de configuración a través del menú **Boot** (Inicio), que puede iniciarse tras la finalización de la primera parte de la POST.

Para mostrar el menú **Boot** (Inicio):

1. Durante el proceso de inicio, pulse **2** en los 10 segundos posteriores a la aparición del mensaje siguiente:

```
Boot Menu Version: Oct 20 2004
```

Select an option. If no selection in 10 seconds then
operational code will start.

- 1 - Start operational code.
- 2 - Start Boot Menu.

Select (1, 2):

El menú **Boot** (Inicio) muestra y contiene las funciones de configuración siguientes:

- 1 - Start operational code (Iniciar código operativo)
- 2 - Change baud rate (Cambiar velocidad en baudios)
- 3 - Retrieve event log using XMODEM (Recuperar el registro de eventos mediante XMODEM)
- 4 - Load new operational code using XMODEM (Cargar un código operativo nuevo mediante XMODEM)
- 5 - Display operational code vital product data (Ver el código operativo de datos de productos vitales)
- 6 - Run flash diagnostics (Ejecutar diagnósticos de la memoria flash)
- 7 - Update boot code (Actualizar código de inicio)
- 8 - Delete backup image (Eliminar imagen de copia de seguridad)
- 9 - Reset the system (Restablecer el sistema)
- 10 - Restore configuration to factory defaults (delete config files) (Restablecer la configuración a los valores predeterminados de fábrica [eliminar los archivos de configuración])
- 11 - Activate Backup Image (Activar imagen de copia de seguridad)
- 12 - Password Recovery Procedure (Procedimiento de recuperación de contraseña)

En las secciones siguientes se describen las opciones del menú **Boot** (Inicio).

Inicio del código operativo

Utilice la opción 1 para reanudar la carga del código operativo.

Para volver a iniciar el proceso de inicio desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **1** y pulse <Intro>.

Aparece el mensaje siguiente:

```
Operational Code Date: Thu Jun 8 12:51:44 2006

Uncompressing....

50% 100%

|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

1 File: bootos.c Line: 462 Task: fffff00 EC: 2863311530 (0xaaaaaaaa)

(0 d 0 hrs 0 min 13 sec)

Timebase: 24,750275 MHz, MEM: 99,001100 MHz, PCI: 33,000366 MHz, CPU: 198.002200 MHz

PCI device BCM5675_A0 attached as unit 0.

PCI device BCM5695_B0 attached as unit 1.

PCI device BCM5695_B0 attached as unit 2.

PCI device BCM5673_A1 attached as unit 3.

PCI device BCM5673_A1 attached as unit 4.

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

st_state(0) = 0x0
```

```
st_state(1) = 0x3
```

```
st_state(2) = 0x2
```

Cambio de la velocidad en baudios

Utilice la opción 2 para cambiar la velocidad en baudios de la interfaz serie.

Para cambiar la velocidad en baudios desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **2** y pulse <Intro>.

Aparece el mensaje siguiente:

```
[Boot Menu] 2
```

```
Select baud rate:
```

```
1 - 1200
```

```
2 - 2400
```

```
3 - 4800
```

```
4 - 9600
```


```
5 - 19200
```

```
6 - 38400
```

```
7 - 57600
```

```
8 - 115200
```

```
0 - no change
```

 **NOTA:** la velocidad en baudios seleccionada se aplica inmediatamente.

2. Se reanuda el proceso de inicio.

Recuperación del registro de eventos mediante XMODEM

Utilice la opción 3 para recuperar el registro de eventos y descargarlo en el terminal ASCII.

Para recuperar el registro de eventos desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **3** y pulse <Intro>.

Aparece el mensaje siguiente:

```
[Boot Menu] 3
```

```
Sending event log, start XMODEM receive....
```

```
File ascii.log.bin Ready to SEND in binary mode
```

```
Estimated File Size 169K, 1345 Sectors, 172032 Bytes
```

```
Estimated transmission time 3 minutes 20 seconds
```

```
Send several Control-X characters to cancel before transfer starts.
```

2. Se reanuda el proceso de inicio.

Carga de un código operativo nuevo mediante XMODEM

Utilice la opción 4 cuando sea necesario descargar una nueva versión del software para sustituir archivos dañados o para actualizar el software del sistema.

Para descargar software desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **4** y pulse <Intro>.

Aparece el mensaje siguiente:

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC...
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cancel before transfer starts.
```

2. Cuando utilice HyperTerminal, haga clic en **Transfer** (Transferir) en la barra de menús de **HyperTerminal**.

3. En el menú **Transfer** (Transferir), haga clic en **Send File** (Enviar archivo).

Se abre la ventana **Send File** (Enviar archivo).

4. Introduzca la ruta de acceso para que se descargue el archivo.

5. Asegúrese de que el protocolo está definido como Xmodem.

6. Haga clic en **Send** (Enviar).

Se descarga el software. La descarga de software tarda varios minutos. Es posible que la aplicación de emulación de terminal, como HyperTerminal, muestre el progreso del proceso de descarga.

Visualización del código operativo de datos de productos vitales

Utilice la opción 5 para ver información sobre la imagen de inicio.

Para ver información sobre la imagen de inicio desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **5** y pulse <Intro>.

Aparece el mensaje siguiente:

```
[Boot Menu] 5
The following image is in the Flash File System:
File Name.....image1
CRC.....0xb017 (45079)
Target Device.....0x00508541
Size.....0x8ec50c (9356556)
Number of Components.....2
Operational Code Size.....0x7ec048 (8306760)
Operational Code Offset.....0x74 (116)
Operational Code FLASH flag.....1
Operational Code CRC.....0x9B4D
Boot Code Version.....1
Boot Code Size.....0x10000 (1048576)
Boot Code Offset.....0x7ec0bc (8306876)
Boot Code FLASH flag.....0
Boot Code CRC.....0x1CB8
VPD - rel 0 ver 31 maint_lvl 0
Timestamp - Thu Jun 8 12:51:44 2006
File - pc62xxr0v31.stk
```

2. Se reanuda el proceso de inicio.

Ejecución de diagnósticos de la memoria flash

Utilice la opción **6** para ejecutar diagnósticos de la memoria flash. La acción del usuario se confirma con una pregunta Y/N (Sí/No) antes de ejecutar el comando.

Para realizar una prueba completa de la memoria flash desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **6** y pulse <Intro>.

Aparece el mensaje siguiente:

```
[Boot Menu] 6

Do you wish to run flash diagnostics? (Boot code region will not be tested.) (y/n): y

Input number of diagnostic iterations -> 1

Testing 2 x 28F128J3 base: 0xfe000000

Iterations remaining = 1

Erasing sector 0

Verify sector 0 erased

Writing sector 0

Erasing sector 1

Verify sector 1 erased

Writing sector 1

Erasing sector 2

Verify sector 2 erased

Writing sector 2

Erasing sector 3

Verify sector 3 erased

Writing sector 3

Erasing sector 4

Verify sector 4 erased

Writing sector 4

Erasing sector 5


Verify sector 5 erased

Writing sector 5

Erasing sector 6

Verify sector 6 erased

Writing sector 6
```

 **NOTA:** este proceso se ejecuta hasta que se hayan borrado todos los sectores, se hayan verificado los sectores borrados y se hayan escrito los sectores.

```
Flash Diagnostics passed
```

```
[Boot Menu]
```

2. Se reanuda el proceso de inicio.

Actualización del código de inicio

Utilice la opción **7** para actualizar el código de inicio en la memoria flash. Esta opción sólo es válida tras cargar el nuevo código de inicio mediante la opción **4** del menú **Boot** (Inicio). La acción del usuario se confirma con una pregunta Y/N (Sí/No) antes de ejecutar el comando.

Para descargar software desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **7** y pulse <Intro>.

Aparece el mensaje siguiente:

```
Do you wish to update Boot Code? (y/n) y
```

```
Erasing Boot Flash.....Done.
```

```
Wrote 0x10000 bytes.
```

```
Wrote 0x20000 bytes.
```

```
Wrote 0x30000 bytes.
```

```
Wrote 0x40000 bytes.
```

```
Wrote 0x50000 bytes.
```

```
Wrote 0x60000 bytes.
```

```
Boot code updated
```

2. Se reanuda el proceso de inicio.

Eliminación de la imagen de copia de seguridad

Utilice la opción **8** para eliminar la imagen de copia de seguridad de la memoria flash. La acción del usuario se confirma con una pregunta Y/N (Sí/No) antes de ejecutar el comando.

Para eliminar la imagen de copia de seguridad desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **8** y pulse <Intro>.

Aparece el mensaje siguiente:

```
Are you SURE you want to delete backup image : image2 ? (y/n):y
```

```
Backup image deleted...
```

```
[Boot Menu]
```

2. Se reanuda el proceso de inicio.

Restablecimiento del sistema

Utilice la opción **9** para borrar toda la memoria flash y restablecer el sistema a la configuración predeterminada. La acción del usuario se confirma con una pregunta Y/N (Sí/No) antes de ejecutar el comando.

Para restablecer el sistema desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **9** y pulse <Intro>.

Aparece el mensaje siguiente:

```
[Boot Menu] 9
```

```
Are you SURE you want to reset the system? (y/n):y
```

2. El proceso de inicio comienza de nuevo.

Restablecimiento de la configuración a los valores predeterminados de fábrica (eliminación de los archivos de configuración)

Utilice la opción **10** para cargar utilizando la configuración predeterminada del sistema y para iniciar sin utilizar la configuración de inicio actual. Al seleccionar la opción **10** en el menú **Boot** (Inicio), se restablecen los valores predeterminados del sistema. La secuencia de inicio podrá iniciarse seleccionando **1** en el menú **Boot** (Inicio).

Para descargar software desde el menú **Boot** (Inicio):

1. En el menú **Boot** (Inicio), seleccione **10** y pulse <Intro>.

Aparece el mensaje siguiente:

```
Are you SURE you want to delete the configuration? (y/n):y
```

2. Se reanuda el proceso de inicio.

Activación de la imagen de copia de seguridad

Utilice la opción 11 para activar la imagen de copia de seguridad. Cuando se selecciona esta opción, la imagen activa pasa a ser la copia de seguridad.

Para activar la imagen de copia de seguridad:

1. En el menú **Boot** (Inicio), seleccione **11** y pulse <Intro>.

Aparece el mensaje siguiente:

```
Backup image - image2 activated.
```

2. Se reanuda el proceso de inicio.

Procedimiento de recuperación de contraseña

Utilice la opción 12 si pierde una contraseña. Esta opción permite que el conmutador se inicie una vez sin solicitar la contraseña de consola. Tenga en cuenta que la contraseña *activa* no se solicita en este modo.

Para recuperar una contraseña perdida únicamente para el terminal local:

1. En el menú **Boot** (Inicio), seleccione **12** y pulse <Intro>.

La contraseña se borra.

2. Se reanuda el proceso de inicio.
3. Para garantizar la seguridad del conmutador, vuelva a configurar las contraseñas para los métodos de administración que sean aplicables.

Ejemplo de proceso de configuración

En esta sección se describen los pasos básicos necesarios para establecer una conexión de administración de red remota con el conmutador. No se explican las diversas configuraciones disponibles en el conmutador ni los comandos pertinentes.

En esta sección también se describe el acceso al conmutador por primera vez con las definiciones y la configuración predeterminadas. Si una configuración definida anteriormente causa problemas, se debe borrar el archivo de configuración de inicio (que es la configuración del conmutador cuando se enciende) y reiniciar el conmutador. Consulte "[Configuración predeterminada del dispositivo](#)".

Requisitos de configuración del conmutador

Se requieren los componentes siguientes para este ejemplo:

- 1 Conmutador PowerConnect serie 6200
- 1 Una estación de trabajo con los componentes siguientes instalados:
 - o Tarjeta adaptadora de red
 - o Aplicación de terminal ASCII (por ejemplo, Microsoft® Windows® HyperTerminal o Procomm Plus™ Terminal)
 - o Una aplicación de explorador
- 1 Un cable F2F de módem nulo
- 1 Cables UTP directos o cruzados (categoría 5)

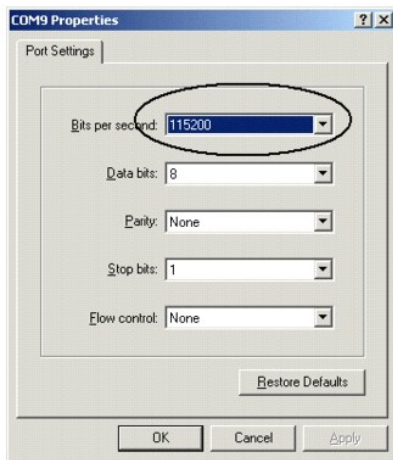
Conexión inicial

1. Mediante el puerto RS-232, conecte el conmutador a la estación de trabajo.

2. Configure el terminal ASCII con los valores siguientes y seleccione el puerto COM adecuado.

En la pantalla de ejemplo se utiliza HyperTerminal.

Ilustración 5-3. Ventana de propiedades de HyperTerminal



NOTA: la velocidad en baudios predeterminada de un conmutador nuevo es 9 600. El conmutador puede tener otra velocidad en baudios. Si se utiliza la velocidad predeterminada y no se ve el terminal del conmutador, pruebe con otra velocidad en baudios.

3. Utilice un cable de módem nulo F2F para conectar la estación de trabajo al conmutador.

NOTA: si configura una *pila*, conecte la estación de trabajo al conmutador maestro.

4. Conecte el cable de alimentación del conmutador y encienda el conmutador. El sistema ejecuta el proceso de inicio. Cuando aparezca la información siguiente, puede acceder al menú **Boot** (Inicio) seleccionando **2**, si es necesario, para ejecutar procedimientos especiales.

```
Select an option. If no selection in 10 seconds then operational code will start.
```

```
1 - Start operational code.
```

```
2 - Start Boot Menu.
```

```
Select (1, 2):2
```

Si no accede al menú **Boot** (Inicio), el sistema continúa con la operación descomprimiendo el código en la RAM. El código empieza a ejecutarse desde la RAM y se muestra la lista de los números de puertos disponibles y los estados correspondientes (activos o inactivos).

NOTA: la pantalla siguiente es un ejemplo de configuración. Algunos elementos como direcciones, versiones y fechas pueden variar según el conmutador.

```
current volume configuration:
- volume label: NO LABEL; (in boot sector: )
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
```



```
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240
FAT handler information:
-----
- allocation group size: 2 clusters
- free space on volume: 21,348,352 bytes
Boot Menu Version: 27 Apr 2006

Select an option. If no selection in 10 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.

Select (1, 2):1

Operational Code Date: Wed May 17 10:54:19 2006

Uncompressing....

50% 100%

|||||
volume descriptor ptr (pVolDesc): 0xfd7e6c0
cache block I/O descriptor ptr (cbio): 0xfd7fe40
auto disk check on mount: NOT ENABLED
max # of simultaneously open files: 22
file descriptors in use: 0
# of different files in use: 0
# of descriptors for deleted files: 0
# of obsolete descriptors: 0
current volume configuration:
- volume label: NO LABEL; (in boot sector: )
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
```

```

- max # of entries in root: 240

FAT handler information:
-----

- allocation group size: 2 clusters

- free space on volume: 21,350,400 bytes

File: unitmgr.c, Line: 3419, Error 0 (0x0)

Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz, CPU: 533,333328 MHz

SOC unit 0 attached to PCI device BCM56304_B0

SOC unit 1 attached to PCI device BCM56304_B0

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

hpc - No stack ports. Starting in stand-alone mode.

(Unit 1 - Waiting to select management unit)>

```

Configuración predeterminada del dispositivo

Para restablecer la configuración predeterminada del dispositivo, utilice el comando `delete startup-config` en el indicador de modo con privilegios (`#`) y reinicie el dispositivo. Cuando se vuelva a cargar el dispositivo, se configurará con los valores predeterminados.

```

console>

console>enable

console#delete startup-config

Startup file was deleted

console#reload

Management switch has unsaved changes.

Are you sure you want to continue? (y/n) y

Configuration Not Saved!

Are you sure you want to reload the stack? (y/n) y

Reloading all switches..

```

Activación de la administración remota

1. Introduzca el comando `enable` en la consola para acceder al modo de pantalla de Privileged EXEC, tal como figura a continuación:

```

console>enable

console#

```

2. Conecte la estación de administración al conmutador a través de uno de los puertos Ethernet o de una red conectada al conmutador con un cable CAT5.

En este ejemplo se utiliza el puerto `1/g1`.

3. Compruebe (en el terminal ASCII) que el estado de la interfaz ha cambiado a activado y que el estado de STP es de reenvío (tras 30 segundos), 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: 1/g1

```

```
01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port 1/g1: STP status Forwarding
```

- Introduzca el comando **config** en la consola para acceder al modo de pantalla de configuración, tal como figura a continuación:

```
console#config
```

- Utilice el comando siguiente para definir la dirección IP como DHCP:

```
console(config)#ip address dhcp
```

- Utilice el comando siguiente para definir la puerta de enlace predeterminada:

```
console(config)#ip default-gateway 10.254.24.162
```

- Si la estación de administración forma parte 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 conmutador. En este ejemplo, la dirección estática es 192.168.20.100.

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1 200
```

- Ejecute el comando ping para la estación de administración en el conmutador para comprobar que se ha alcanzado la conectividad.

Espere 30 segundos a que el puerto esté en modo de reenvío STP antes de ejecutar el comando ping para la estación de administración. En este ejemplo, la dirección IP de la estación de administración es 50.1.1.2.

```
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
```

- Defina un nombre de usuario y una contraseña para permitir el acceso con privilegios de nivel 15 al conmutador para un usuario remoto (HTTP y HTTPS).

En este ejemplo, el nombre de usuario es **Dell**, la contraseña es **Dell1234** y el nivel de privilegio es 15. Los niveles de privilegio están comprendidos entre 1 y 15 (nivel máximo). El acceso de nivel 15 es el único nivel de acceso posible para la interfaz web.

```
console#config
```

```
console(config)#username Dell password Dell1234 level 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
```

- Defina un nombre de usuario y una contraseña para permitir el acceso de un usuario local a un servidor web, Telnet o una consola, por ejemplo.

En este ejemplo, el nombre de usuario y la contraseña es **Dell**, la contraseña es **Dell1234** y el nivel de privilegio es 15.

```
console(config)#username Dell password Dell1234 level 15
```

```
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 tommy123

console(config-line)#exit

console(config)#line telnet

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password bobby123

console(config-line)#exit

console(config)#line ssh

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password jones123

console(config-line)#exit
```

11. Guarde el archivo **running-config** en el archivo **startup-config**.

De este modo, se garantiza que la configuración que acaba de finalizar es la misma si se reinicia el conmutador.

```
console(config)#exit

console#copy running-config startup-config
```

En este momento el conmutador está configurado y puede administrarse a través de distintas opciones como Telnet o la interfaz del explorador web, entre otras.

Configuración del acceso seguro a la administración (HTTPS)

Al administrar el conmutador de forma segura a través del explorador web estándar, se utiliza el protocolo de seguridad SSL (capa de conexión segura).

Para administrar el conmutador de forma segura a través del explorador web estándar, realice lo siguiente:

1. Para configurar el conmutador para que permita el servidor HTTPS y para crear una clave de seguridad, utilice los comandos **ip https server** y **crypto certificate 1 generate**:

```
console#configure

console(config)#crypto certificate 1 generate

Generating RSA private key, 1024 bit long modulus

console(config)#ip https server

console(config)#
```

2. Configure la estación de administración del mismo modo que para una conexión HTTP normal.
3. Conéctese al conmutador a través de HTTPS escribiendo la dirección `https://dirección IP del dispositivo` en la ventana del explorador (debe introducir `https`).

Aparece la ventana **Security Alert** (Alerta de seguridad).

4. Haga clic en **Yes** (Sí) para confirmar la aceptación del certificado de seguridad (si no está autenticado por terceros).

Aparece la pantalla de inicio de sesión.

5. Introduzca el nombre de usuario y la contraseña asignados.

Aparece el administrador de conmutadores Dell OpenManage™.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Obtención de ayuda


Dell™ PowerConnect™ serie M6220 – Guía del usuario


- [Obtención de asistencia](#)
- [Formación y certificación Dell para empresas](#)
- [Problemas con el pedido](#)
- [Información sobre productos](#)
- [Devolución de artículos para reparación bajo garantía o abono](#)
- [Antes de llamar](#)
- [Cómo ponerse en contacto con Dell](#)

Cómo obtener asistencia

En caso de que tenga algún problema en el ordenador, puede llevar a cabo los pasos siguientes para diagnosticar el problema y solucionarlo:


1. Rellene la [lista de verificación de diagnósticos](#).
2. Consulte la amplia gama de servicios en línea de Dell disponibles en su página web de asistencia (support.dell.com) para obtener ayuda sobre la instalación y los procedimientos de solución de problemas. Consulte [Servicios en línea](#) para obtener una lista más amplia de recursos de asistencia en línea de Dell.
3. Si los pasos descritos anteriormente no han resuelto el problema, consulte [Cómo ponerse en contacto con Dell](#).

 **NOTA:** llame al servicio de asistencia de Dell desde un teléfono situado cerca del ordenador para que puedan guiarle en los procedimientos necesarios.

 **NOTA:** es posible que el sistema de código de servicio rápido de Dell no esté disponible en todos los países.

Cuando el sistema telefónico automatizado de Dell se lo solicite, marque el código de servicio rápido para dirigir su llamada directamente al personal de asistencia apropiado. Si no tiene un código de servicio rápido, abra la carpeta **Dell Accesorios** (Accesorios Dell), haga doble clic en el icono **Express Service Code** (Código de servicio rápido) y siga las instrucciones que se indican.

Para obtener instrucciones sobre el uso del servicio de asistencia de Dell, consulte [Servicio de asistencia](#).

 **NOTA:** puede que algunos de los servicios que se describen a continuación no estén disponibles en todas las ubicaciones fuera del área continental de EE. UU. Llame a un representante local de Dell para obtener información sobre disponibilidad.

Servicios en línea

Puede obtener más información sobre los productos y servicios de Dell en las páginas web siguientes:

www.dell.com

www.dell.com/ap (sólo para países asiáticos y del Pacífico)

www.dell.com/jp (sólo para Japón)

www.euro.dell.com (sólo para Europa)

www.dell.com/la (para países de Latinoamérica y del Caribe)

www.dell.ca (sólo para Canadá)

Puede acceder a la asistencia de Dell a través de las páginas web y direcciones de correo electrónico siguientes:

- 1 Páginas web de asistencia de Dell

support.dell.com

support.jp.dell.com (sólo para Japón)

support.euro.dell.com (sólo para Europa)

- 1 Direcciones de correo electrónico de asistencia de Dell

mobile_support@us.dell.com

support@us.dell.com

la-techsupport@dell.com (sólo para países de Latinoamérica y del Caribe)

apsupport@dell.com (sólo para países asiáticos y del Pacífico)

- 1 Direcciones de correo electrónico de marketing y ventas de Dell

apmarketing@dell.com (sólo para países asiáticos y del Pacífico)

sales_canada@dell.com (sólo para Canadá)

- 1 Protocolo de transferencia de archivos (FTP) anónimo

ftp.dell.com

Regístrese como usuario: `anonymous` (anónimo) y utilice su dirección de correo electrónico como contraseña.

Servicio automatizado de estado de pedidos

Para comprobar el estado de un pedido de productos Dell, puede ir a support.dell.com o llamar al servicio automatizado de estado de pedidos. Un contestador automático le solicitará los datos necesarios para localizar el pedido e informarle sobre su estado. Para obtener el número de teléfono necesario, consulte [Cómo ponerse en contacto con Dell](#).

Servicio de asistencia

Dell pone a su disposición un servicio de asistencia, disponible las 24 horas del día los siete días de la semana, para dar respuesta a todas sus preguntas sobre el hardware de Dell. Nuestro personal de asistencia utiliza diagnósticos computerizados para proporcionar respuestas rápidas y precisas.

Para ponerse en contacto con el servicio de asistencia de Dell, consulte [Antes de llamar](#) y lea la información de contacto correspondiente a su región.

Formación y certificación Dell para empresas

Tiene a su disposición el servicio de formación y certificación Dell para empresas. Para obtener más información, visite www.dell.com/training. Es posible que este servicio no se ofrezca en todas las regiones.

Problemas con el pedido

Si tiene algún problema con un pedido (por ejemplo, si falta alguna pieza, hay piezas equivocadas o la factura es incorrecta), póngase en contacto con el departamento de atención al cliente de Dell. Tenga a mano la factura o el albarán cuando haga la llamada. Para obtener el número de teléfono necesario, consulte [Cómo ponerse en contacto con Dell](#).

Información sobre productos

Si necesita información sobre otros productos disponibles de Dell o desea realizar un pedido, visite la página web de Dell (www.dell.com). Para saber el número de teléfono al que debe llamar o para hablar con un especialista en ventas, consulte [Cómo ponerse en contacto con Dell](#).

Devolución de artículos para reparación bajo garantía o abono

Prepare todos los artículos que vaya a devolver, ya sea para su reparación bajo garantía o para su abono, de la manera siguiente:

1. Llame a Dell para obtener un número de autorización para devolución de material y anótelo de manera clara y destacada en el exterior de la caja.


Para obtener el número de teléfono necesario, consulte [Cómo ponerse en contacto con Dell](#).

2. Incluya una copia de la factura y una carta que describa el motivo de la devolución.
3. Incluya una copia de la lista de verificación de diagnósticos (consulte [Lista de verificación de diagnósticos](#)) donde se indiquen las pruebas que ha ejecutado y todos los mensajes de error notificados por Dell Diagnostics.
4. Incluya todos los accesorios correspondientes al artículo que vaya a devolver (cables de alimentación, soportes multimedia tales como CD o disquetes, guías, etc.) si la devolución es para obtener un abono.
5. Embale 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. No se aceptará el envío de paquetes a portes debidos.

Toda devolución que no satisfaga los requisitos indicados será rechazada por el departamento de recepción de Dell y le será devuelta.

Antes de llamar

 **NOTA:** cuando llame, tenga a mano su código de servicio rápido. Este código contribuirá a que el sistema de asistencia telefónica automatizada de Dell gestione de manera más eficiente su llamada.


No olvide rellenar la lista de verificación de diagnósticos (consulte [Lista de verificación de diagnósticos](#)). Si es posible, encienda el ordenador antes de llamar a Dell para solicitar asistencia y haga la llamada desde un teléfono que esté cerca de éste. Es posible que se le pida que escriba algunos comandos con el teclado, que proporcione información detallada durante las operaciones o que pruebe otros procedimientos para solucionar problemas que únicamente pueden realizarse con el ordenador. Asegúrese de tener a mano la documentación del ordenador.

 **PRECAUCIÓN:** antes de manipular el interior del ordenador, lea las instrucciones de seguridad incluidas en la *Guía de información del producto*.

Lista de verificación de diagnósticos
Nombre:
Fecha:
Dirección:
Teléfono:
Etiqueta de servicio (código de barras en la parte inferior o posterior del ordenador):
Código de servicio rápido:
Número de autorización para devolución de material (si se lo ha proporcionado un técnico de asistencia de Dell):
Sistema operativo y versión:
Dispositivos:
Tarjetas de expansión:
¿El ordenador está conectado a una red? Sí/No
Red, versión y adaptador de red:
Programas y versiones:
Consulte la documentación del sistema operativo para determinar el contenido de los archivos de inicio del sistema. Si el ordenador está conectado a una impresora, imprima todos los archivos. Si no puede imprimirlos, tome nota del contenido de cada archivo antes de llamar a Dell.
Mensaje de error, código de sonido o código de diagnóstico:
Descripción del problema y procedimientos de solución de problemas que ha realizado:

Cómo ponerse en contacto con Dell

Los clientes de los Estados Unidos pueden llamar al 800-WWW.DELL (800.999.3355).

 **NOTA:** si no dispone de una conexión a Internet activa, puede encontrar información de contacto en la factura de compra, albarán o catálogo del producto de Dell.

Dell proporciona varias opciones de servicio y asistencia en línea o telefónica. Puesto que la disponibilidad varía en función del país y del producto, es posible que no pueda disponer de algunos servicios en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio al cliente:

1. Vaya a support.dell.com.
2. Verifique su país o región en el menú desplegable **Choose A Country/Region** (Elija un país/región) en la parte inferior de la página.
3. Haga clic en **Contáctenos** en el lado izquierdo de la página.
4. Seleccione el enlace de servicio o asistencia apropiado de acuerdo con sus necesidades.
5. Elija el método para ponerse en contacto con Dell que le resulte más cómodo.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso del administrador de conmutadores Dell™ OpenManage™

Dell™ PowerConnect™ serie M6220 — Guía del usuario

- [Definición de la dirección IP del conmutador](#)
- [Inicio de la aplicación](#)
- [Descripción de la interfaz](#)
- [Uso de los botones del administrador de conmutadores](#)
- [Definición de campos](#)
- [Acceso al conmutador a través de la CLI](#)
- [Uso de la CLI](#)

Definición de la dirección IP del conmutador

Existen dos métodos para establecer la dirección IP, que consisten en utilizar DHCP o en asignar la dirección de forma estática. Consulte la sección "[Acceso al conmutador a través de la CLI](#)" para iniciar la CLI.

Definición de la dirección IP con DHCP

1. Escriba `enable` en el indicador de console> y pulse <Intro>.
2. En el indicador de console#, escriba `config` y pulse <Intro>.
3. Escriba `ip address dhcp` y pulse <Intro>.
4. Escriba `exit`.
5. Escriba `show ip interface management` en el indicador de console#.

Definición de una dirección estática


1. Escriba `enable` en el indicador de console> y pulse <Intro>.
2. En el indicador de console#, escriba `config` y pulse <Intro>.
3. Escriba `ip address none`.
4. Para configurar una dirección IP 10.256.24.64 con una máscara de red 255.255.248.0 y una puerta de enlace 10.256.24.1, escriba lo siguiente:

```
ip address 10.256.24.64 255.255.248.0
ip default-gateway 10.256.24.1
```
5. Escriba `exit`.
6. Escriba `show ip interface management`.

Inicio de la aplicación

1. Abra un explorador web.
2. Introduzca la dirección IP del conmutador (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 "[Información general sobre la configuración](#)".
3. Cuando se abra la ventana **Login** (Inicio de sesión), introduzca su nombre de usuario y contraseña.

 **NOTA:** el conmutador no está configurado con una contraseña predeterminada, así que puede configurarlo sin necesidad de introducir una contraseña al conectarse a la CLI mediante el puerto de consola. En las contraseñas se distingue entre mayúsculas y minúsculas, y son alfanuméricas. Para obtener información sobre cómo recuperar una contraseña olvidada, consulte "[Procedimiento de recuperación de contraseña](#)".

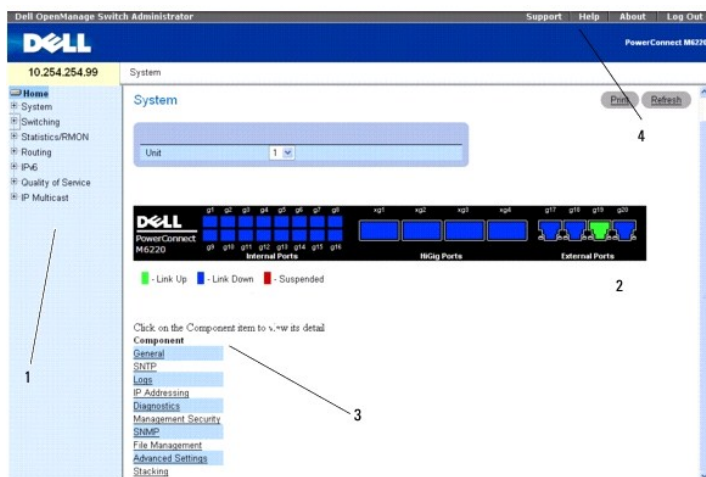
- Haga clic en **OK** (Aceptar).
- Se abre la página de inicio del administrador de conmutadores Dell OpenManage.

Descripción de la interfaz

La página de inicio (vea la [ilustración 3-1](#)) contiene las vistas siguientes:

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

Ilustración 3-1. Componentes del administrador de conmutadores



En la [tabla 3-1](#) se enumeran los componentes de la interfaz con los números correspondientes.

Tabla 3-1. Componentes de la interfaz

Componente	Nombre
1	La vista de árbol incluye una lista de las distintas funciones del dispositivo. Las bifurcaciones de la vista de árbol se pueden expandir para ver todos los componentes de una función específica o se pueden contraer para ocultar los componentes de la función. Si arrastra la barra vertical hacia la derecha, puede ampliar el área del árbol para ver el nombre completo de un componente.
2	La vista de dispositivo proporciona información sobre los puertos del dispositivo, la configuración y el estado actuales, los datos de la tabla y los componentes de la función. El color de los puertos indica si un puerto está actualmente activo. El color verde indica que el puerto está activado, el rojo indica que se ha producido un error en el puerto y el azul indica que el enlace está desactivado. NOTA: el estado de los LED no aparece en la vista de dispositivo. El estado de los LED sólo se puede determinar mirando directamente el conmutador. Para obtener información sobre los LED, consulte " Definiciones de los LED ". Según la opción que seleccione, el área de la parte inferior de la vista de dispositivo mostrará otra información sobre el dispositivo o cuadros de diálogo para configurar parámetros.
3	La lista de componentes contiene una lista de los componentes de las funciones. Los componentes también pueden visualizarse ampliando una función de la vista de árbol.
4	Los botones de información proporcionan acceso a datos sobre el conmutador y al servicio de asistencia de Dell. Para obtener más información, consulte " Botones de información ".

Uso de los botones del administrador de conmutadores

Botones de información

Tabla 3-2. Botones de información

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

Botones de administración de dispositivos

Tabla 3-3. Botones de administración de dispositivos

Botón	Descripción
Apply Changes	Aplica los cambios establecidos en el dispositivo.
Add	Añade información a las tablas o a los cuadros de diálogo.
Telnet	Inicia una sesión Telnet.
Query	Genera consultas sobre las tablas.
Show All	Muestra las tablas de dispositivos.
Flechas izquierda y derecha	Mueve información entre las listas.
Refresh	Actualiza la información de los dispositivos.
Reset All Counters	Restablece los contadores de estadísticas.
Print	Imprime la página del sistema de administración de red o la información de las tablas.
Draw	Crea gráficos de estadísticas directamente.

Casillas de verificación

Tabla 3-4. Casillas de verificación

Tipo de casilla de verificación	Descripción
Add	Hiperenlace que lleva a la página de configuración.
Remove	Elimina el elemento seleccionado.
General selection	Sirve para activar un elemento de configuración, por ejemplo, ajustar la sensibilidad de los archivos de registro, seleccionar criterios de asignación para servicios diferenciados o seleccionar los parámetros de las reglas ACL.

Definición de campos


Los campos definidos por el usuario pueden contener de 1 a 159 caracteres, a menos que se especifique lo contrario en la página web del administrador de conmutadores Dell OpenManage.

Se pueden utilizar todos los caracteres, excepto los siguientes:

- 1 \
- 1 /
- 1 :
- 1 *
- 1 ?
- 1 <
- 1 >
- 1 |

Acceso al conmutador a través de la CLI

El conmutador se puede administrar a través de una conexión directa con el puerto de consola o de una conexión Telnet.


 **NOTA:** si está administrando una pila, asegúrese de que el cable de interfaz serie esté conectado al conmutador maestro de la pila.

El uso de la CLI es similar a la introducción de comandos en un sistema Linux. Si el acceso se realiza a través de una conexión Telnet, asegúrese de que el dispositivo tenga una dirección IP definida y de que la estación de trabajo utilizada para acceder al dispositivo esté conectada a éste antes de utilizar los comandos de la CLI.


Para obtener más información sobre la configuración de una dirección IP inicial, consulte "[Información general sobre la configuración](#)".

Conexión de la consola

1. Encienda el conmutador (o la pila) y espere hasta que se haya iniciado completamente.

 **NOTA:** si instala una pila de conmutadores, conecte el terminal al conmutador maestro. Este conmutador tendrá encendido el LED de conmutador maestro. La primera vez que se enciende una pila, los conmutadores eligen el conmutador que debe actuar como maestro, que puede ocupar cualquier posición de la pila. Si conecta el terminal a un conmutador subordinado, no podrá utilizar la CLI a través de la interfaz serie de dicho conmutador.

2. Si el administrador no ha configurado un método de autenticación de inicio de sesión, aparece el indicador de `console>` al iniciarse el conmutador. De lo contrario, se mostrará el indicador de inicio de sesión `User:`.

 **NOTA:** en los pasos siguientes se presupone que se ha configurado la contraseña y el usuario `admin` en el sistema.

3. Escriba `admin` en el indicador y pulse `<Intro>`.

Se mostrará el indicador `Password:`

4. Introduzca la contraseña, que se visualiza en forma de asteriscos (*).

Se mostrará el indicador de `console#`.

5. Configure el dispositivo e introduzca los comandos necesarios para completar las tareas que se deben realizar.

6. Cuando haya terminado, salga de la sesión con el comando `quit` o `exit`.

Conexión Telnet

Telnet es un protocolo TCP/IP de emulación de terminal. Los terminales ASCII pueden conectarse virtualmente al dispositivo local mediante una red de protocolo TCP/IP. Telnet constituye una alternativa a un terminal de inicio de sesión local, en el que es necesario un inicio de sesión remoto.

El conmutador admite hasta cuatro sesiones Telnet simultáneas. En una sesión Telnet se pueden utilizar todos los comandos de la CLI.

Uso de la CLI

Información general sobre el modo de comandos

La CLI está dividida en modos de comandos. Cada modo de comandos dispone de un conjunto de comandos específicos. Si se escribe un signo de interrogación en el indicador de la consola, aparece una lista de los comandos disponibles para ese modo de comandos en particular.

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

Durante la inicialización de sesión en la CLI, el modo de la CLI es el modo `User EXEC`. En este modo sólo hay disponible un pequeño grupo de comandos. Este nivel está reservado para tareas que no modifican la configuración del conmutador y se usa para acceder a subsistemas de configuración. El modo `Privileged EXEC` puede requerir una contraseña, si la contraseña de activación está configurada. Consulte "[Gestión de la seguridad y configuración de contraseñas](#)" para obtener más información sobre cómo configurar contraseñas de activación.

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


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

El modo `Interface Configuration` configura el dispositivo en el nivel de interfaz física. Los comandos de la interfaz que requieren subcomandos tienen otro nivel, el modo `Subinterface Configuration`.

Modo User EXEC

La petición de nivel User EXEC consta del nombre de host seguido del paréntesis angular (>). Por ejemplo:

```
console>
```

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

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

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

Modo Privileged EXEC

El acceso al modo Privileged se puede proteger para evitar el acceso no autorizado al mismo y garantizar el funcionamiento de los parámetros operativos. En las contraseñas se distingue entre mayúsculas y minúsculas, y cada carácter de una contraseña se muestra en la pantalla como un asterisco.

Para acceder al modo Privileged EXEC y ver sus comandos:

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

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

```
console#
```

3. Para enumerar los comandos Privileged EXEC, escriba un signo de interrogación en el indicador de comandos.
4. Para cambiar del modo Privileged EXEC al modo User EXEC, escriba el comando `exit` o pulse las teclas <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#exit
console>
```

Utilice el comando `exit` para volver al modo anterior. Por ejemplo, puede cambiar del modo Interface Configuration al modo Global Configuration y del modo Global Configuration al modo Privileged EXEC.

Modo Global Configuration

Los comandos del modo Global Configuration se aplican a las funciones del sistema en vez de a un protocolo o una interfaz específicos.

Para acceder al modo Global Configuration:

1. En el indicador del modo Privileged EXEC, escriba `configure` y pulse <Intro>. El modo Global Configuration consta del nombre de host del dispositivo, seguido de (`config`) y el símbolo de almohadilla (#).

```
console(config)#
```

2. Para enumerar los comandos del modo Global Configuration, introduzca un signo de interrogación en el indicador de comandos.
3. Para cambiar 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 del modo Interface Configuration modifican la configuración de interfaz IP específica, incluido el grupo de puente, la descripción, etc. Los modos de Interface Configuration son:

- 1 **VLAN:** contiene comandos para crear y configurar una VLAN completa, por ejemplo, crear una VLAN y aplicarle una dirección IP.
- 1 **Port Channel** (Canal de puerto): contiene comandos para configurar grupos agregados de enlaces (LAG).
- 1 **Ethernet:** contiene comandos para administrar la configuración de puertos Ethernet.
- 1 **Loopback** (Bucle de retorno): contiene comandos para administrar la configuración de la interfaz de bucle de retorno.
- 1 **Tunnel** (Túnel): contiene comandos para administrar la configuración de la interfaz de túnel.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Descripción del hardware

Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [Descripción de los puertos](#)
- [Otras características](#)
- [Definiciones de los LED](#)

Esta sección contiene información sobre las características de los dispositivos y las configuraciones de hardware de los módulos. Se tratan los temas siguientes:

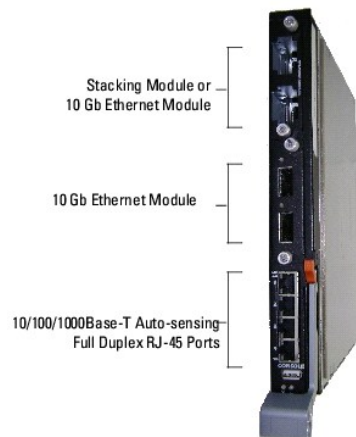
- 1 [Panel frontal de Dell™ PowerConnect™ serie M6220](#)
- 1 [Puerto de consola \(RS-232\)](#)
- 1 [Dimensiones físicas](#)
- 1 [Fuentes de alimentación](#)
- 1 [Sistema de ventilación](#)
- 1 [Apilamiento](#)
- 1 [Definiciones de los LED](#)

Descripción de los puertos

Panel frontal de Dell™ PowerConnect™ serie M6220

El panel frontal de PowerConnect serie M6220 incluye cuatro puertos RJ-45 10/100/1000Base-T con cuatro puertos Ethernet de 10 Gigabit. También cuenta con 16 puertos internos que se conectan a cada uno de los módulos de alta densidad del servidor.

Ilustración 2-1. PowerConnect serie M6220



- 1 El conmutador detecta automáticamente la diferencia entre los cables cruzados y directos en los puertos RJ-45.
- 1 Los puertos RJ-45 admiten modo dúplex completo y semidúplex.

Puerto de consola (RS-232)

El puerto de consola (RS-232) sólo se utiliza para la administración a través de una interfaz serie. Este puerto proporciona una conexión directa al conmutador y sirve para acceder a la CLI desde un terminal de consola conectado a un puerto EIA/TIA-232.


Para conectar desde el puerto de consola del M6220 a un terminal, utilice el cable serie proporcionado, que consta de un conector USB Tipo A en un extremo y un conector DB-9 hembra en el otro. El puerto de consola del M6220 es un puerto USB ubicado en la parte inferior del panel frontal.

El puerto de consola admite datos asíncronos de ocho bits de datos, un bit de paro, ningún bit de paridad y sin control de flujo. La velocidad en baudios predeterminada es de 9 600 bps.

- **NOTA:** si instala una pila de conmutadores, debe ensamblar la pila y cablearla antes de encenderla y configurarla. La primera vez que se enciende una pila, los conmutadores eligen un conmutador maestro, que puede ocupar cualquier posición de la pila. Conecte el terminal al conmutador maestro. Si conecta el terminal a un conmutador subordinado, no podrá utilizar la CLI.

Redirección de consola

El chasis del servidor del módulo de alta densidad de Dell incluye una característica de redirección de consola que permite gestionar cada módulo M6220 desde una única conexión serie al chasis. Para más información sobre la redirección de consola, consulte la *Dell Blade Server CMC User's Guide* (Guía del usuario del servidor del módulo de alta densidad CMC de Dell).

 **NOTA:** Cuando utiliza la redirección de consola para acceder a un módulo, el puerto externo de consola de dicho módulo permanece inactivo y se terminan todas las sesiones de consola en curso.

Otras características

Dimensiones físicas

Para obtener información acerca de las dimensiones físicas de PowerConnect serie M6220, consulte el *Dell Blade Server Chassis Hardware Owner's Manual* (Manual del propietario del hardware del chasis del servidor del módulo de alta densidad de Dell).

Fuentes de alimentación

Para más información acerca de la alimentación del PowerConnect serie M6220, consulte el *Dell Blade Server Chassis Hardware Owner's Manual* (Manual del propietario del hardware del chasis del servidor del módulo de alta densidad de Dell).

Sistema de ventilación

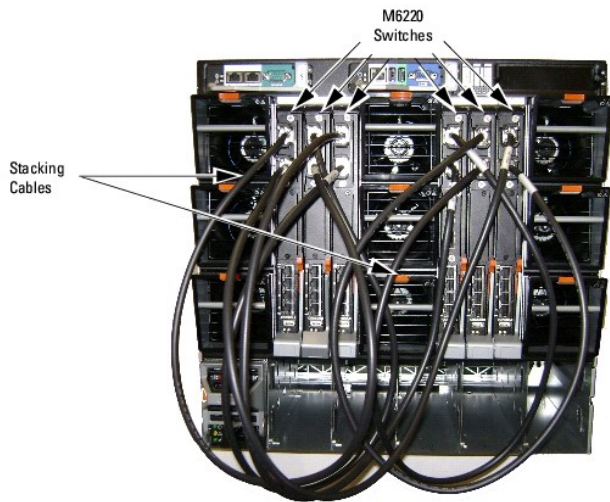
Para obtener información acerca del sistema de ventilación de PowerConnect serie M6220, consulte el *Dell Blade Server Chassis Hardware Owner's Manual* (Manual del propietario del hardware del chasis del servidor del módulo de alta densidad de Dell).

Apilamiento

Puede apilar hasta 12 conmutadores PowerConnect serie M6220, lo que representa hasta 240 puertos de 1 Gb. Para crear una pila, conecte unidades adyacentes mediante los puertos de apilamiento situados en la parte superior del panel de conmutadores. Vea la [ilustración 2-2](#).

1. Instale un módulo de apilamiento adquirido por separado en el compartimiento 1 posterior de cada uno de los conmutadores de la pila.
2. En cada conmutador de la pila, conecte uno de los cables de apilamiento cortos desde el puerto de apilamiento número uno del conmutador hacia el puerto de apilamiento número dos del conmutador siguiente.
3. Si es necesario, utilice un cable de apilamiento largo (3 metros), adquirido por separado, para conectar los conmutadores. Repita este proceso hasta que todos los dispositivos estén conectados.
4. Utilice el resto de cable de apilamiento para conectar los demás puertos libres, desde el puerto número uno del último conmutador, hasta el puerto número dos del primer conmutador.

Ilustración 2-2. Conexión de una pila de conmutadores



In [Ilustración 2-2](#), la pila tiene seis conmutadores PowerConnect serie M6220 conectados a través de los puertos de apilamiento. El primer puerto de apilamiento de cada M6220 se encuentra conectado físicamente al segundo puerto de apilamiento del siguiente M6220 utilizando un cable de apilamiento. El primer puerto de apilamiento del sexto conmutador está conectado al segundo puerto de apilamiento del primer conmutador.

Reserva apilable

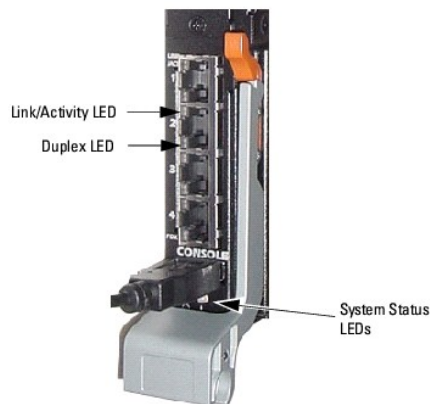
La función de apilamiento admite una unidad de copia de seguridad o "en espera" que adoptará el papel de unidad maestra si se produce un error en la unidad maestra de la pila. En cuanto se detecta en la pila un error en la unidad maestra, la unidad en espera inicializa el plano de control y activa el resto de unidades de pila con la configuración actual. La unidad en espera conserva una copia sincronizada de la configuración en ejecución de la pila. Durante la conmutación, todos los puertos se activan y se desactivan para evitar posibles bucles y conseguir que el estado de las aplicaciones de software del nuevo maestro sea coherente.

La unidad en espera está preconfigurada en la pila. Sin embargo, puede utilizar la CLI para seleccionar un miembro de la pila distinto como unidad en espera. Para obtener más información, consulte la *Guía de referencia de la CLI*.

Definiciones de los LED

El panel frontal incluye diodos emisores de luz (LED) que indican el estado de los enlaces de los puertos de 1 Gb integrados y el estado del sistema.


Ilustración 2-3. LED del panel frontal



En la [tabla 2-1](#) se definen los LED del sistema:

Tabla 2-1. Definiciones del estado de los LED del M6220

LED	Color	Definición

①	Luz verde	El módulo M6220 recibe alimentación
	Luz apagada	El módulo M6220 no recibe alimentación.
	Azul	El conmutador es la unidad maestra actual de la pila.
	Desactivada	El conmutador no es la unidad maestra actual de la pila.
	Luz ámbar	Se ha producido un error

LED del puerto del módulo XFP

Los conectores XFP se encuentran en el módulo XFP al insertarlo en el M6220. En la [tabla 2-2](#) se definen los LED del puerto XFP:

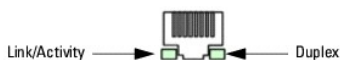
Tabla 2-2. Definiciones de los LED del puerto XFP

LED	Color	Definición
XFP	Luz verde	El puerto está actualmente enlazado.
	Luz verde parpadeante	El puerto está actualmente enviando o recibiendo tráfico de red.
	Luz apagada	El puerto no está enlazado.

LED del puerto 10/100/1000Base-T

Cada puerto 10/100/1000Base-T tiene dos LED. En la ilustración siguiente se muestran los LED del puerto 10/100/1000Base-T.

Ilustración 2-4. LED del puerto 10/100/1000 Base-T



La [tabla 2-3](#) contiene definiciones de los LED del puerto 10/100/1000Base-T.

Table 2-3. Definiciones del puerto 10/100/1000Base-T

LED	Color	Definición
Enlace/actividad (LNK/ACT)	Luz verde	El puerto funciona a 1 000 Mbps.
	Luz ámbar	El puerto funciona a 10/100 Mbps.
	Luz fija	Enlace establecido pero sin actividad.
	Luz parpadeante	Enlace establecido con actividad.
	Luz apagada	No hay ningún enlace.
Dúplex	Luz verde	Modo dúplex completo.
	Luz apagada	Modo semidúplex.


[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Introducción

Dell™ PowerConnect™ serie M6220 — Guía del usuario

- [Funciones](#)
- [Documentación de la CLI](#)

 **AVISO:** antes de continuar, lea las notas de la versión de este producto. Puede descargar las notas de la versión de la página web de asistencia de Dell (support.dell.com).

El Dell™ PowerConnect™ serie M6220 es un módulo de alta densidad de conmutador Ethernet Gigabit de nivel 3, para utilizarse en el chasis de servidor de módulo de alta densidad de Dell. El PowerConnect serie M6220 está basado en la arquitectura de Dell PowerConnect serie 6200.

Funciones

En esta sección se describen las funciones del conmutador configurables por el usuario. Para obtener una lista de todas las funciones, consulte las notas de la versión del software.

Funciones basadas en el puerto

Compatibilidad con tramas gigantes

Las tramas gigantes permiten transportar la misma cantidad de datos en un número menor de tramas para garantizar una menor sobrecarga, un menor tiempo de procesamiento y menos interrupciones.

Compatibilidad con la MDI/MDIX automática

El conmutador admite la detección automática entre cables cruzados y directos.

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

Para obtener información sobre la configuración de MDI/MDIX para puertos o LAG, consulte "[Configuración de puertos](#)" o "[Configuración de LAG](#)".

Negociación automática

La negociación automática permite que un conmutador anuncie modos de funcionamiento. La función de negociación automática permite el intercambio de información entre dos conmutadores que comparten un segmento de enlace punto a punto, así como la configuración automática de ambos conmutadores para aprovechar al máximo sus capacidades de transmisión.

La serie PowerConnect 6200 mejora la negociación automática, ya que incorpora la posibilidad de anunciar puertos. El anuncio de puertos permite al administrador del sistema configurar las velocidades de puerto anunciadas.

Para obtener información sobre la negociación automática, consulte "[Configuración de puertos](#)" o "[Configuración de LAG](#)".

Compatibilidad con el control de flujo (IEEE 802.3x)

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

Para obtener información sobre la configuración del control de flujo para puertos o LAG, consulte "[Configuración de puertos](#)" o "[Configuración de LAG](#)".

Prevención de bloqueo de cabecera de línea

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

Compatibilidad con la contrapresión

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

Reenvío y almacenamiento alternativo (ASF)

La función de reenvío y almacenamiento alternativo (ASF) reduce la latencia de paquetes grandes. Cuando está activada esta función, la unidad de administración de memoria (MMU) puede reenviar un paquete al puerto de salida antes de que se reciba por completo en la memoria del conjunto de búferes de pila (CBP). La función ASF, que también recibe el nombre de modo de conexión directa, se puede configurar a través de la interfaz de línea de comandos. Para obtener información sobre cómo configurar la función ASF, consulte la guía de referencia de la CLI.

Funciones compatibles con las direcciones MAC

Compatibilidad con direcciones MAC

El conmutador admite un máximo de 8 192 direcciones MAC y reserva dos direcciones MAC para uso del sistema.

Obtención automática de direcciones MAC

El conmutador permite obtener automáticamente direcciones MAC a partir de los paquetes entrantes.

Caducidad automática de las direcciones MAC

Las direcciones MAC en las que no ha habido tráfico durante un periodo de tiempo determinado caducan, lo que impide que la tabla de direcciones se desborde.

Para obtener información sobre la configuración del periodo de caducidad de las direcciones MAC, consulte "[Tabla de direcciones dinámicas](#)".

Entradas de MAC estáticas

Las entradas de MAC definidas por el usuario se almacenan en la tabla de direcciones con las direcciones obtenidas automáticamente.

Para obtener información sobre la configuración de direcciones MAC estáticas, consulte "[Tabla 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 añaden a la tabla de hardware. Los paquetes que en el futuro se envíen a esta dirección o desde esta dirección se reenvían de forma más eficaz.

Compatibilidad con la multidifusión de MAC

El servicio de multidifusión es un servicio de difusión limitado que permite las conexiones de uno a varios y de varios a varios. En los servicios de multidifusión de nivel 2, se recibe una única trama dirigida a una dirección de multidifusión específica y se crean copias de dicha trama que se van a transmitir a cada puerto pertinente.

Para obtener información sobre la configuración de la compatibilidad con la multidifusión de MAC, consulte "[Administración de la compatibilidad con multidifusión](#)".

Funciones del nivel 2

Inspección de IGMP

La inspección de IGMP examina el contenido de las tramas de IGMP cuando las reenvía el conmutador desde las estaciones a un enrutador de multidifusión ascendente. La inspección permite que el conmutador identifique las estaciones interesadas en sesiones de multidifusión y los enrutadores de multidifusión que envían tramas de multidifusión.

Duplicación de puertos

La duplicación de puertos supervisa y duplica el tráfico de red mediante el reenvío de copias de los paquetes entrantes y salientes de hasta cuatro puertos de origen a un puerto supervisor.

Control de tormentas de difusión

Cuando se reenvían las tramas de nivel 2, las tramas de difusión, de difusión única desconocida y de multidifusión se distribuyen a todos los puertos de la red de área local virtual (VLAN) pertinente. La distribución ocupa amplitud de banda y carga todos los nodos conectados en todos los puertos. El control de tormentas limita la cantidad de tramas de difusión, de difusión única desconocida y de multidifusión que el conmutador acepta y reenvía.

Características de la dependencia de enlaces

La característica de dependencia de enlaces proporciona la capacidad de habilitar o deshabilitar uno o más puertos, basándose en el estado de los enlaces de uno o más puertos.

Para obtener información acerca de la dependencia de enlaces, consulte "[Creación de dependencias de enlaces](#)".

Funciones compatibles con la red de área local virtual

Compatibilidad con VLAN

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

Para obtener información sobre la configuración de las VLAN, consulte "[Configuración de redes 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 "[Configuración de redes VLAN](#)".

VLAN basadas en el protocolo IEEE 802.1v

Las reglas de clasificación de VLAN se definen según la identificación del protocolo de nivel (nivel 2) de enlace de datos. Las VLAN basadas en protocolos sirven para aislar el tráfico de nivel 2 de forma que se distinga de los protocolos de nivel 3.

Para obtener información sobre la definición de las VLAN basadas en protocolos, consulte "[Grupo de protocolo](#)".

Conformidad completa con el etiquetado de VLAN 802.1Q

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

Compatibilidad con GVRP

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

Para obtener información sobre la configuración de GVRP, consulte "[Parámetros de GVRP](#)".

Puertos protegidos (Private VLAN Edge)

Los puertos PVE (Private VLAN Edge) son una función de seguridad de nivel 2 que proporciona seguridad basada en puertos entre los puertos que son miembros de la misma 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.

VLAN basadas en subredes

Esta función permite asignar paquetes entrantes sin etiqueta a una VLAN y una clase de tráfico según la dirección IP de origen del paquete.

Para obtener información sobre la configuración de VLAN basadas en subredes, consulte "[Vinculación de subred IP a VLAN](#)".

VLAN basadas en MAC

Esta función permite asignar paquetes entrantes sin etiqueta a una VLAN y una clase de tráfico según la dirección MAC de origen del paquete.

Para obtener información sobre la configuración de VLAN basadas en MAC, consulte "[Vinculación de MAC a VLAN](#)".

Funciones del protocolo de árbol de extensión

Protocolo de árbol de extensión (STP) por conmutador

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

Para obtener información sobre cómo configurar el protocolo de árbol de extensión, consulte "[Configuración del protocolo de árbol de extensión](#)".

Protocolo de árbol de extensión rápida IEEE 802.1w

El protocolo de árbol de extensión rápida (RSTP) detecta y utiliza las topologías de red para permitir una convergencia más rápida sin que se creen bucles de reenvío.

Para obtener información sobre cómo configurar el protocolo de árbol de extensión rápida, consulte "[Árbol de extensión rápida](#)".

Árbol de extensión múltiple

El funcionamiento del protocolo de árbol de extensión múltiple (MSTP) asigna las VLAN a las instancias de árbol de extensión. MSTP incorpora un escenario de equilibrio de carga distinto. Los paquetes asignados a varias VLAN se transmiten por distintas rutas dentro de las regiones de MSTP (Regiones de MST). Las regiones son uno o varios puentes MSTP interconectados que tienen una configuración MSTP idéntica. El estándar permite a los administradores asignar tráfico de VLAN a rutas exclusivas.

Para obtener información sobre cómo configurar el árbol de extensión múltiple, consulte "[Configuración de MSTP](#)".

Protección de raíz de árbol de extensión

La protección de raíz de árbol de extensión sirve para evitar que la raíz de una instancia de árbol de extensión cambie de forma inesperada. La prioridad de una ID de puente puede establecerse en cero, pero otra ID de puente con una dirección MAC inferior también puede establecer su prioridad en cero y asumir el control de la raíz.

Protección de la unidad de datos del protocolo de puente

La protección BPDU de árbol de extensión sirve para desactivar el puerto, en caso de que un nuevo dispositivo intente acceder a la topología ya existente de STP. De este modo, los dispositivos que inicialmente no formaban parte de STP no podrán influir en la topología de STP.

Funciones de agregación de enlaces

Agregación de enlaces

Para formar un solo grupo agregado de enlaces (LAG), se pueden combinar hasta ocho puertos. Esto permite la protección de tolerancia a errores contra la interrupción de enlaces físicos, conexiones con una mayor amplitud de banda y una mejor resolución de amplitud de banda.

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

Para obtener información sobre la configuración de LAG, consulte "[Configuración de LAG](#)".

Agregación de enlaces y LACP

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

Para obtener información sobre LACP, consulte "[Parámetros de LACP](#)".

Funciones de enrutamiento IPv4

Protocolo de resolución de direcciones

PowerConnect 6200 utiliza el protocolo ARP para asociar una dirección MAC de nivel 2 con una dirección IPv4 de nivel 3. Adicionalmente, el administrador puede añadir entradas de forma estática a la tabla de ARP.

Abrir primero la ruta de acceso más corta (OSPF)

El protocolo de enrutamiento OSPF define dos tipos de áreas: el área OSPF regular y el área de rutas internas OSPF. La información sobre rutas internas y externas OSPF puede propagarse en toda el área OSPF regular; puede admitir el tráfico de transmisión y los enlaces virtuales. Las áreas de rutas internas OSPF no reciben información sobre rutas externas; el objetivo de configurar áreas de rutas internas es limitar el tamaño de la base de datos de áreas para los enrutadores que tienen recursos limitados.

Agente de retransmisión BOOTP/DHCP

El protocolo BootP permite a un dispositivo solicitar y recibir datos y parámetros de configuración de un servidor adecuado. El protocolo de configuración dinámica de host (DHCP) es una extensión de BootP que permite la recepción de parámetros de configuración adicionales desde un servidor de red al iniciarse el sistema. Cabe destacar que mientras que BootP deja de funcionar una vez obtenida una dirección IP, el servicio DHCP es un proceso continuo. Por ejemplo, la dirección IP asignada al sistema tiene un tiempo de concesión que puede caducar, y puede renovarse directamente.

Protocolo de información de enrutamiento

El protocolo de enrutamiento utilizado en un sistema Internet autónomo se denomina protocolo de puerta de enlace interior (IGP). RIP es un IGP diseñado para funcionar con redes de tamaño moderado.

Protocolo de redundancia de enrutamiento virtual

El protocolo de redundancia de enrutamiento virtual (VRRP) sirve para proporcionar a los hosts enrutadores redundantes en la topología de red sin necesidad de que los hosts vuelvan a configurarse o sepan que hay varios enrutadores.

Funciones de enrutamiento IPv6

DHCPv6

DHCPv6 incorpora el concepto de servidor sin estado, en el que DHCPv6 no se utiliza para asignar direcciones IP a los clientes, sino que únicamente proporciona otro tipo de información de redes, como por ejemplo, información sobre DNS, NTP (Protocolo de hora de red) o SIP (Protocolo de inicio de sesión).

OSPFv3

OSPFv3 proporciona un protocolo de enrutamiento para la conexión a redes IPv6. OSPFv3 es un nuevo componente de enrutamiento basado en el componente OSPF versión 2. En IPv6 de pila doble, puede configurar y utilizar tanto el componente OSPF como el componente OSPFv3.

Rutas IPv6

Dado que IPv4 e IPv6 pueden coexistir en una misma red, el enrutador de dicha red debe reenviar ambos tipos de tráfico. Gracias a esta coexistencia, PowerConnect 6200 mantiene dos tablas de enrutamiento, rto y rto6, ambas aptas para realizar reenvíos a través del mismo conjunto de interfaces. Las interfaces IPv6 se administran de forma similar a las interfaces IPv4.

Funciones de calidad de servicio

Compatibilidad con la calidad de servicio (QoS)

Para resolver el tráfico de red imprevisible y optimizar el rendimiento, puede aplicar la calidad de servicio (QoS) en toda la red para asegurarse de que el tráfico de red se prioriza según un criterio específico. El conmutador admite dos tipos de QoS: servicios diferenciados y clase de servicio.

Servicios diferenciados

La función de calidad de servicio (QoS) es compatible con los servicios diferenciados (DiffServ) y, por lo tanto, permite clasificar el tráfico en flujos y proporcionarle determinados tratamientos de calidad de servicio según los comportamientos por salto definidos.

Clase de servicio

La función de envío a cola de clase de servicio (CoS) permite configurar directamente determinados aspectos del envío a cola del conmutador. Dicha función proporciona el comportamiento de QoS deseado para distintos tipos de tráfico de red cuando no se requieren las complejidades de servicios diferenciados.

Funciones de multidifusión IPv4

Protocolo de enrutamiento de multidifusión de vectores de distancia

DVMRP intercambia paquetes de sonda con todos los enrutadores que lo tienen activado, establece relaciones bidireccionales entre vecinos y genera una tabla de vecinos. Intercambia paquetes de informe y crea una tabla de topología de difusión única, que se utiliza para generar la tabla de enrutamiento de multidifusión. Esta tabla de rutas de multidifusión se utilizará después para direccionar los paquetes de multidifusión.

Protocolo de administración de grupos de Internet

Los sistemas IPv4 (hosts y enrutadores) utilizan el protocolo de administración de grupos de Internet (IGMP) para notificar su pertenencia a grupos de multidifusión IP a cualquier enrutador de multidifusión vecino. PowerConnect 6200 realiza la función de enrutador de multidifusión del protocolo IGMP, es decir, recopila la información sobre pertenencia que necesita el enrutamiento de multidifusión activo.

Multidifusión independiente de protocolo-Modo denso

La multidifusión independiente de protocolo (PIM) es un protocolo de enrutamiento de multidifusión estándar que proporciona un enrutamiento de multidifusión escalable entre dominios en Internet y es independiente de los mecanismos proporcionados por cualquier protocolo de enrutamiento de difusión única concreto. El protocolo PIM-DM utiliza una tabla de enrutamiento de difusión única existente y un mecanismo de unión, poda e injerto para crear un árbol. PIM-DM crea árboles de distribución de la ruta de acceso más corta basados en el origen que utilizan el reenvío de ruta inversa (RPF).

Multidifusión independiente de protocolo-Modo disperso

PIM-SM se utiliza para direccionar de manera eficaz el tráfico de multidifusión a grupos de multidifusión que pueden abarcar redes de área amplia y en casos en que la amplitud de banda es una limitación. Utiliza árboles compartidos de manera predeterminada e implementa árboles basados en el origen para obtener mayor eficacia. Esta velocidad de umbral de datos se utiliza para alternar entre árboles.

Funciones de administración de conmutadores

Registros de excepciones y alarmas de SNMP

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

Para obtener información sobre alarmas y excepciones de SNMP, consulte "[Definición de los parámetros globales de SNTp](#)".

Administración basada en web

El sistema se puede administrar desde cualquier explorador web. El conmutador tiene incorporado un servidor web que sirve páginas HTML que pueden utilizarse para supervisar y configurar el sistema.

Descarga del archivo de configuración

El archivo de configuración del conmutador incluye tanto los datos de configuración del dispositivo de todo el sistema como los datos específicos de cada puerto. Los archivos de configuración se pueden visualizar a través de los comandos de la interfaz de línea de comandos (CLI).

Para obtener información sobre la descarga de archivos de configuración, consulte "[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 de software, consulte "[Descarga de software y reinicio](#)".

Protocolo trivial de transferencia de archivos (TFTP)

La serie PowerConnect 6200 admite la carga y descarga de imágenes de inicio, firmware y configuración a través de TFTP.

Supervisión remota (RMON)

La RMON es una MIB estándar que define las estadísticas actuales e históricas del nivel MAC y los objetos de control, lo que permite capturar información en tiempo real en toda la red.

Protocolo simple de administración de red (SNMP) versiones 1, 2 y 3

El sistema se puede administrar totalmente utilizando una combinación de variables de base de datos de información de administración (MIB), cuyos valores combinados representan todas las facetas del estado del sistema, y el protocolo SNMP para examinar y posiblemente modificar dichos valores. Se admite SNMP v1/v2c/v3 en el protocolo de transporte UDP/IP.

Interfaz de línea de comandos

La sintaxis y la semántica de la interfaz de línea de comandos (CLI) se adaptan a las prácticas habituales en el sector en la medida de lo posible. La CLI se compone de elementos obligatorios y opcionales. La ayuda contextual proporciona intervalos de formato y de valores permitidos para los comandos actuales, y el intérprete de la CLI completa comandos y palabras clave.

Syslog

Syslog es un protocolo que permite enviar notificaciones de eventos a un conjunto de servidores remotos concretos, donde se almacenan, analizan y resuelven.

Para obtener información sobre Syslog, consulte "[Administración de registros](#)".

SNTP

El protocolo simple de hora de red (SNTP) garantiza una sincronización de la hora del conmutador de la red con una precisión de milisegundos. La sincronización de la hora se lleva a cabo mediante un servidor SNTP de la red.

Para obtener más información sobre SNTP, consulte "[Configuración de SNTP](#)".

Funciones de seguridad

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) garantizan que sólo los usuarios autorizados tengan acceso a recursos específicos y bloquean los intentos injustificados para acceder a los recursos de red. Las ACL se utilizan para proporcionar un control del flujo de tráfico, restringir el contenido de las actualizaciones de enrutamiento, decidir qué tipos de tráfico se deben reenviar o bloquear y, especialmente, proporcionar seguridad para la red.

Para obtener información sobre la definición de las ACL, consulte "[Configuración de la ACL IP](#)" y "[Configuración de la ACL MAC](#)".

Autenticación basada en el puerto (802.1x)

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

Compatibilidad con el bloqueo de puertos

La función de bloqueo de puertos limita el acceso a un puerto a los usuarios con direcciones MAC específicas. Estas direcciones se definen manualmente o se obtienen en el puerto pertinente. Cuando se detecta una trama en un puerto bloqueado y la dirección MAC de origen de la trama no está vinculada a dicho puerto, se inicia el mecanismo de protección.

Para obtener información sobre la activación de la seguridad del bloqueo de puertos, consulte "[Seguridad de puertos](#)".

Seguridad de administración de contraseñas

La administración de contraseñas aumenta la seguridad en la red y mejora el control de las contraseñas. Las contraseñas para el acceso SSH, Telnet, HTTP, HTTPS y SNMP tienen funciones de seguridad asignadas.

Para obtener más información sobre la administración de contraseñas, consulte "[Administración de contraseñas](#)".

TACACS+

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

Ciente RADIUS

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

SSH/SSL

Secure Shell (SSH) es un protocolo que permite realizar una conexión remota segura a un dispositivo. Esta conexión proporciona una función parecida a una conexión Telnet de entrada.

El protocolo de capa de conexión segura (SSL) permite abstraer una conexión cifrada entre dos estaciones. Una vez establecida dicha conexión, se utilizará prácticamente del mismo modo que una conexión no segura.

Documentación de la CLI

Otro recurso para Dell PowerConnect serie 6200 es la *Guía de referencia de la CLI*. Esta guía proporciona información sobre los comandos de la CLI utilizados para configurar y administrar el conmutador y la pila. El documento ofrece descripciones completas, sintaxis, valores predeterminados y ejemplos de la CLI.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Creación de dependencias de enlaces

Dell™ PowerConnect™ serie M6220 – Guía del usuario

[Resumen de dependencias de enlaces](#)

La característica de dependencia de enlaces proporciona la capacidad de habilitar o deshabilitar uno o más puertos, basándose en el estado de los enlaces de uno o más puertos. Con la dependencia de enlaces habilitada en un puerto, el estado de enlace de dicho puerto dependerá del estado del enlace de otro puerto. Por ejemplo, si el puerto A depende del puerto B y el conmutador detecta un enlace perdido en el puerto B, el conmutador automáticamente descargará el enlace en el puerto A. Cuando se restablece el enlace al puerto B, el conmutador automáticamente restablece el enlace al puerto A.

Puede crear hasta 16 grupos de dependencia. Los puertos que formen parte de la dependencia de enlaces pueden estar en todas las unidades de pila (unidad administradora/miembro).

La característica de dependencia de enlaces es compatible con las situaciones siguientes:

- 1 Puerto dependiente de un puerto: si un puerto pierde el enlace, el conmutador desactiva el enlace en otro puerto.
- 1 Puerto dependiente de un LAG: si todos los puertos en un grupo de canales pierden el enlace, el conmutador desactiva el enlace en otro puerto.
- 1 LAG dependiente de un puerto: si un puerto pierde el enlace, el conmutador desactiva todos los enlaces en un grupo de canales.
- 1 Comando de puertos múltiples: si un grupo de puertos pierden su enlace, el conmutador desactiva el enlace en otro grupo de puertos.
- 1 Puertos superpuestos: los puertos superpuestos en diferentes grupos se desactivarán sólo si ambos puertos dependientes pierden el enlace.

La página del menú **Link Dependency** (Dependencia de enlace) contiene un enlace a la página [Link Dependency Summary](#) (Resumen de dependencia de enlaces).

Resumen de dependencias de enlaces

Utilice la página **Link Dependency Summary** (Resumen de dependencia de enlace) para ver todas las dependencias de enlaces del sistema y acceder a la página **Link Dependency Configuration** (Configuración de la dependencia de enlaces). Puede crear hasta 16 grupos de dependencia. La página muestra los grupos, se hayan o no configurado.

Para visualizar la página **Link Dependency Summary** (Resumen de dependencia de enlaces), haga clic en **Switching** → (Χοινομαχί (v) **Link Dependency** → (Dependencia de enlaces) **Link Dependency Summary** (Resumen de dependencia de enlaces) en la vista de árbol.

Ilustración 8-1. Resumen de la dependencia de enlaces

Group ID	Member Ports	Ports Depended On	Remove
1	Not configured	Not configured	<input type="checkbox"/> Modify
2	Not configured	Not configured	<input type="checkbox"/> Modify
3	Not configured	Not configured	<input type="checkbox"/> Modify
4	Not configured	Not configured	<input type="checkbox"/> Modify
5	Not configured	Not configured	<input type="checkbox"/> Modify
6	Not configured	Not configured	<input type="checkbox"/> Modify
7	Not configured	Not configured	<input type="checkbox"/> Modify
8	Not configured	Not configured	<input type="checkbox"/> Modify
9	Not configured	Not configured	<input type="checkbox"/> Modify
10	Not configured	Not configured	<input type="checkbox"/> Modify
11	Not configured	Not configured	<input type="checkbox"/> Modify
12	Not configured	Not configured	<input type="checkbox"/> Modify
13	Not configured	Not configured	<input type="checkbox"/> Modify
14	Not configured	Not configured	<input type="checkbox"/> Modify
15	Not configured	Not configured	<input type="checkbox"/> Modify
16	Not configured	Not configured	<input type="checkbox"/> Modify

La página **Link Dependency Summary** (Resumen de la dependencia de enlaces) contiene los siguientes campos:

Group ID (ID del grupo): el número de identificación del grupo.

Member Ports (Puertos miembro): la lista de puertos miembro que pertenecen al grupo.

Ports Depended On (Puertos de los que dependen): la lista de puertos de los cuales dependen los grupos.

Remove (Eliminar): casilla de verificación para eliminar la configuración de un grupo.

Modify (Modificar): enlace para modificar la configuración de un grupo. Haga clic en el enlace **Modify** (modificar) para acceder a la página de configuración del grupo.

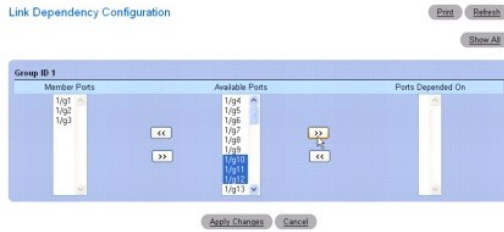
Modificación de un grupo de dependencia de enlaces

1. Abra la página **Link Dependency Summary** (Resumen de dependencia de enlaces).

- En la fila de la ID del grupo del grupo de dependencia que desea configurar, haga clic en el enlace **Modify** (Modificar).

Se muestra la página **Link Dependency Group Configuration** (Configuración de grupo de dependencia de enlace).

Ilustración 8-2. Configuración de grupo de dependencia de enlaces



- Para agregar un puerto a la columna de **Member Ports** (Puertos miembro), haga clic en el puerto de la columna **Available Ports** (Puertos disponibles), y haga clic en el botón **<<** a la izquierda de la columna **Available Ports** (Puertos disponibles). Mantenga presionada la tecla **Ctrl** y haga clic sobre los puertos para seleccionarlos.
 - Para agregar un puerto a la columna **Ports Depended On** (Puertos de los cuales depende), haga clic en el puerto en la columna **Available Ports** (Puertos disponibles), y haga clic en el botón **>>** a la derecha de la columna **Available Ports** (Puertos disponibles).
 - Haga clic en **Apply Changes** (Aplicar cambios).
- Se modifica la configuración de dependencia de enlaces para el grupo, y se actualiza el dispositivo.
- Haga clic en **Show All** (Mostrar todo) para regresar a la página **Link Dependency Summary** (Resumen de dependencia de enlaces).

Quitar todos los puertos de un grupo de dependencia de enlaces

- Abra la página **Link Dependency Summary** (Resumen de dependencia de enlaces).
- En la fila de la ID del grupo del grupo de dependencia de enlaces que desea configurar, seleccione la casilla de verificación **Remove** (Eliminar).
- Haga clic en **Apply Changes** (Aplicar cambios).

Se eliminan todos los puertos del grupo de dependencia de enlaces, y se actualiza el dispositivo.

Configuración de los grupos de dependencia de enlaces con comandos CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- Comandos de dependencia de enlaces

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Dell™ PowerConnect™ serie M6220 — Guía del usuario



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



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



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

La información contenida en este documento puede modificarse sin aviso previo.
© 2007 Dell Inc. Reservados todos los derechos.

Queda estrictamente prohibida la reproducción de este documento en cualquier forma sin la autorización por escrito de Dell Inc.

Marcas comerciales utilizadas en este texto: *Dell*, *Dell OpenManage*, el logotipo de *DELL*, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* y *Latitude* son marcas comerciales de Dell Inc.; *Microsoft*, *Windows* y *Windows Vista* son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos o en otros países. *Procomm Plus* es una marca comercial de Symantec Corporation o sus filiales en los Estados Unidos y en otros países.

Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Modelo M6220

Septiembre de 2007 Rev. A00

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Visualización de las estadísticas/RMON


Dell™ PowerConnect™ serie M6220 – Guía del usuario

- [Vistas de tabla](#)
- [RMON](#)
- [Gráficos](#)

La supervisión remota (RMON) permite que el administrador de red conozca el estado y el rendimiento de la red a través de un acceso remoto. Se admiten cuatro grupos de supervisión que se definen como parte del estándar RMON: estadísticas, historial, alarmas y eventos.

En esta sección se describen las opciones de RMON disponibles en la página de menú **Statistics/RMON** (Estadísticas/RMON). Estas opciones son la visualización de las estadísticas en formato de tabla, la edición y visualización de las estadísticas de RMON y la creación de gráficos sobre las estadísticas de LAG y de puerto. La página de menú **Statistics/RMON** (Estadísticas/RMON) permite acceder a estas opciones a través de las páginas de menú siguientes:

- 1 [Vistas de tabla](#)
- 1 [RMON](#)
- 1 [Gráficos](#)

 **NOTA:** los comandos de la CLI no se encuentran disponibles para todas las páginas de estadísticas/RMON.

Vistas de tabla

La página de menú **Table Views** (Vistas de tabla) contiene enlaces a páginas web que permiten visualizar estadísticas en formato de tabla. Para visualizar esta página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) en la vista de árbol. A continuación figuran las páginas web a las que se puede acceder desde esta página de menú:

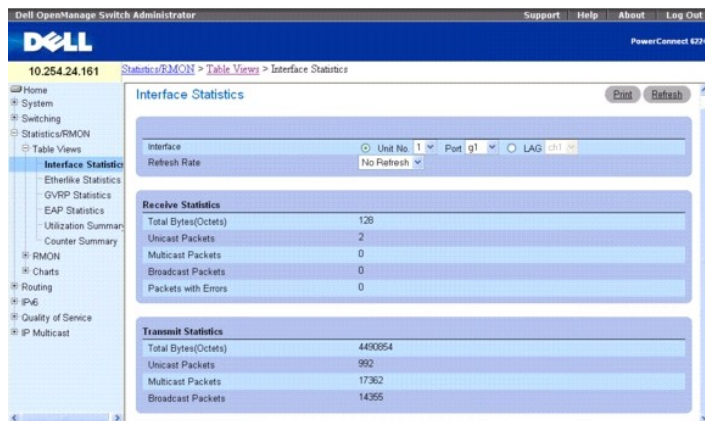
- 1 [Estadísticas de la interfaz](#)
- 1 [Estadísticas de Etherlike](#)
- 1 [Estadísticas de GVRP](#)
- 1 [Estadísticas de EAP](#)
- 1 [Resumen de utilización](#)
- 1 [Resumen de contadores](#)

Estadísticas de la interfaz

Utilice la página **Interface Statistics** (Estadísticas de la interfaz) para ver las estadísticas de los paquetes recibidos y transmitidos. Los campos de los paquetes recibidos y transmitidos son idénticos.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **Interface Statistics** (Estadísticas de la interfaz) en la vista de árbol.

Ilustración 9-1. Estadísticas de la interfaz



La página **Interface Statistics** (Estadísticas de la interfaz) contiene los campos siguientes:

Interface (Interfaz): permite seleccionar la interfaz física (unidad, puerto) o la interfaz LAG cuyas estadísticas van a mostrarse.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Estadísticas recibidas

Total Bytes (Octets) (Total de bytes [octetos]): muestra el número total de octetos recibidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): muestra el número total de paquetes de difusión única recibidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): muestra el número total de paquetes de multidifusión recibidos en la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): muestra el número total de paquetes de difusión recibidos en la interfaz seleccionada.

Packets with Errors (Paquetes con errores): muestra el número total de paquetes con errores recibidos en la interfaz seleccionada.

Transmisión de estadísticas

Total Bytes (Octets) (Total de bytes [octetos]): muestra el número total de octetos transmitidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): muestra el número total de paquetes de difusión única transmitidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): muestra el número total de paquetes de multidifusión transmitidos en la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): muestra el número total de paquetes de difusión transmitidos en la interfaz seleccionada.

Visualización de estadísticas de interfaz

1. Abra la página **Interface Statistics** (Estadísticas de la interfaz).

2. Especifique una interfaz.

Se muestran las estadísticas de la interfaz especificada.

Visualización de las estadísticas de la interfaz mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

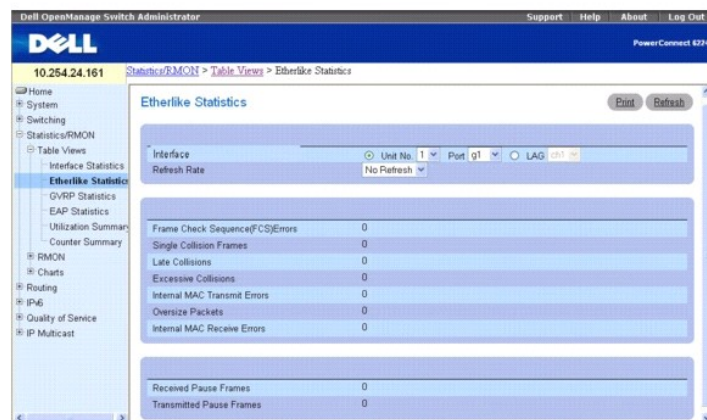
- 1 Comandos de configuración de Ethernet

Estadísticas de Etherlike

Utilice la página **Etherlike Statistics** (Estadísticas de Etherlike) para ver las estadísticas de la interfaz.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **Etherlike Statistics** (Estadísticas de Etherlike) en la vista de árbol.

Ilustración 9-2. Estadísticas de Etherlike



La página **Etherlike Statistics** (Estadísticas de Etherlike) contiene los campos siguientes:

Interface (Interfaz): permite seleccionar la interfaz física (unidad, puerto) o la interfaz LAG cuyas estadísticas van a mostrarse.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Frame Check Sequence (FCS) Errors (Errores de secuencia de verificación de tramas [FCS]): muestra el número de errores FCS recibidos en la interfaz seleccionada.

Signal Collision Frames (Tramas de colisión de señales): muestra el número de errores de tramas de colisión de señales recibidos en la interfaz seleccionada.

Late Collisions (Colisiones tardías): muestra el número de colisiones demoradas recibidas en la interfaz seleccionada.

Excessive Collisions (Colisiones excesivas): muestra el número de colisiones excesivas recibidas en la interfaz seleccionada.

Internal MAC Transmit Errors (Errores de transmisión MAC internos): muestra el número de errores de transmisión MAC internos en la interfaz seleccionada.

Oversize Packets (Paquetes demasiado grandes): muestra el número total de paquetes recibidos de más de 1 518 octetos (sin incluir los bits de trama, pero incluidos los octetos FCS), pero que estaban formados correctamente.

Internal MAC Receive Errors (Errores de recepción MAC internos): muestra el número de errores de recepción MAC internos en la interfaz seleccionada.

Received Pause Frames (Tramas de pausa recibidas): muestra el número de tramas de pausa recibidas en la interfaz seleccionada.

Transmitted Pause Frames (Tramas de pausa transmitidas): muestra el número de tramas de pausa transmitidas en la interfaz seleccionada.

Visualización de estadísticas de Etherlike para una interfaz

1. Abra la página **Etherlike Statistics** (Estadísticas de Etherlike).
2. Especifique una interfaz.

Se muestran las estadísticas de la interfaz especificada.

Estadísticas de GVRP

Utilice la página **GVRP Statistics** (Estadísticas de GVRP) para ver las estadísticas de conmutador de GVRP.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **GVRP Statistics** (Estadísticas de GVRP) en la vista de árbol.

Ilustración 9-3. Estadísticas de GVRP

GVRP Statistics Table		
Attribute(Counted)	Received	Transmitted
Join Empty	0	0
Empty	0	0
Leave Empty	0	0
Join In	0	0
Leave In	0	0
Leave All	0	0

Error Statistics	
Error Type	Received
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0

La página **GVRP Statistics** (Estadísticas de GVRP) contiene los campos siguientes:

Interface (Interfaz): permite seleccionar la interfaz física (unidad, puerto) o la interfaz LAG cuyas estadísticas van a mostrarse.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Atributos de la tabla de estadísticas de GVRP (Contadores) - Recibidos/Transmitidos

Join Empty (Unir vacíos): muestra las estadísticas de Join Empty de GVRP del conmutador.

Empty (Vacíos): muestra las estadísticas de Empty de GVRP del conmutador.

Leave Empty (Dejar vacíos): muestra las estadísticas de Leave Empty de GVRP del conmutador.

Join In (Unir): muestra las estadísticas de Join In de GVRP del conmutador.

Leave In (Dejar): muestra las estadísticas de Leave In de GVRP del conmutador.

Leave All (Dejar todo): muestra las estadísticas de Leave All de GVRP del conmutador.

Error Statistics - Received (Estadísticas de error - Recibidas)

Invalid Protocol ID (ID de protocolo no válido): muestra las estadísticas de Invalid Protocol ID de GVRP del conmutador.

Invalid Attribute Type (Tipo de atributo no válido): muestra las estadísticas de Invalid Attribute Type de GVRP del conmutador.

Invalid Attribute Value (Valor de atributo no válido): muestra las estadísticas de Invalid Attribute Value de GVRP del conmutador.

Invalid Attribute Length (Longitud de atributo no válida): muestra las estadísticas de Invalid Attribute Length de GVRP del conmutador.

Invalid Event (Evento no válido): muestra las estadísticas de Invalid Event de GVRP del conmutador.

Visualización de las estadísticas de GVRP para una interfaz

1. Abra la página GVRP Statistics (Estadísticas de GVRP).
2. Seleccione una interfaz en el campo Interface (Interfaz).

Se muestran las estadísticas de GVRP para la interfaz especificada.

Visualización de las estadísticas de GVRP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos GVRP

Estadísticas de EAP

Utilice la página EAP Statistics (Estadísticas de EAP) para ver información sobre los paquetes EAP recibidos en un puerto específico. Para obtener más información sobre EAP, consulte "[Autenticación basada en el puerto](#)".

Para visualizar la página EAP Statistics (Estadísticas de EAP), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **EAP Statistics** (Estadísticas de EAP) en la vista de árbol.

Ilustración 9-4. Estadísticas de EAP

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is Statistics/RMON > Table Views > EAP Statistics. The interface includes a navigation tree on the left with 'EAP Statistics' selected. The main content area displays 'EAP Statistics' with a 'Print' and 'Refresh' button. Below the buttons are two dropdown menus: 'Interface' (set to '1') and 'Port' (set to 'g1'). A 'Refresh Rate' dropdown is set to 'No Refresh'. A table lists various EAP statistics, all with a value of 0, except for 'Last Frames Source' which is '0000.0000.0000'.

Interface	Unit No.	Port
1	1	g1

Refresh Rate: No Refresh

Frames Received	0
Frames Transmitted	0
Start Frames Received	0
Log off Frames Received	0
Response ID Frames Received	0
Response Frames Received	0
Request Frames Transmitted	0
Request ID Frames Transmitted	0
Invalid Frames Received	0
Length Error Frames Received	0
Last Frames Version	0
Last Frames Source	0000.0000.0000

Interface (Interfaz): especifica la interfaz que se sondea para obtener estadísticas.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Frames Received (Tramas recibidas): muestra el número de tramas EAPOL válidas recibidas en el puerto.

Frames Transmitted (Tramas transmitidas): muestra el número de tramas EAPOL transmitidas a través del puerto.

Start Frames Received (Tramas de inicio recibidas): muestra el número de tramas de inicio EAPOL recibidas en el puerto.

Log off Frames Received (Tramas de cierre de sesión recibidas): muestra el número de tramas de cierre de sesión EAPOL que se han recibido en el puerto.

Respond ID Frames Received (Tramas de ID de respuesta recibidas): muestra el número de tramas de ID de respuesta EAP que se han recibido en el puerto.

Respond Frames Received (Tramas de respuesta recibidas): muestra el número de tramas de respuesta EAP válidas recibidas en el puerto.

Request ID Frames Received (Tramas de ID de petición recibidas): muestra el número de tramas de ID de petición EAP que se han recibido en el puerto.

Request Frames Transmitted (Tramas de petición transmitidas): muestra el número de tramas de petición EAP transmitidas a través del puerto.

Request ID Frames Transmitted (Tramas de ID de petición transmitidas): muestra el número de tramas de ID de petición EAP transmitidas a través del puerto.

Invalid Frames Received (Tramas no válidas recibidas): muestra el número de tramas EAPOL no reconocidas que se han recibido en este puerto.

Length Error Frames Received (Tramas con longitud errónea recibidas): muestra el número de tramas EAPOL con una longitud de cuerpo de paquete no válida recibidas en este puerto.

Last Frames Version (Versión de la última trama): muestra el número de versión del protocolo que va unido a la trama EAPOL que se ha recibido más recientemente.

Last Frames Source (Origen de la última trama): muestra la dirección MAC de origen que va unida a la trama EAPOL que se ha recibido más recientemente.

Visualización de las estadísticas de EAP para una interfaz

1. Abra la página **EAP Statistics** (Estadísticas de EAP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Aparecen las estadísticas de EAP de la interfaz seleccionada.

Visualización de las estadísticas de EAP mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

1 Comandos 802.1X

Resumen de utilización

Utilice la página **Utilization Summary** (Resumen de utilización) para ver las estadísticas de utilización de la interfaz.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Table Views** (Vistas de tabla) → **Utilization Summary** (Resumen de utilización) en la vista de árbol.

Ilustración 9-5. Resumen de utilización

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Utilization Summary" and includes a "Unit" dropdown menu set to "1" and a "Refresh Rate" dropdown menu set to "No Refresh". Below these are two tables. The first table shows interface utilization for three interfaces: 1/g1 (Up), 1/g2 (Down), and 1/g3 (Up). The second table shows Global System LAGs (LAGs) for eight channels (ch1 through ch8), all of which are Down.

Interface	Interface Status	Interface Utilization %	Unicast Received %	Non Unicast Packets Received %	Error Packets Received %
1	1/g1	Up	0	0	0
2	1/g2	Down	0	0	0
3	1/g3	Up	0	0	0

Global System LAGs	LAG Status	LAG Utilization %	LAG Unicast Received %	LAG Non Unicast Packets Received %	LAG Error Packets Received %
1	ch1	Down	0	0	0
2	ch2	Down	0	0	0
3	ch3	Down	0	0	0
4	ch4	Down	0	0	0
5	ch5	Down	0	0	0
6	ch6	Down	0	0	0
7	ch7	Down	0	0	0
8	ch8	Down	0	0	0

La página **Utilization Summary** (Resumen de utilización) contiene los campos siguientes:

Unit (Unidad): especifica la unidad para la que se muestran las estadísticas.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Interface (Interfaz): especifica la interfaz para la que se muestran las estadísticas.

Interface Status (Estado de la interfaz): muestra el estado de la interfaz.

Interface Utilization % (Porcentaje de utilización de la interfaz): muestra el porcentaje de utilización de la interfaz de red basado en el modo dúplex de la interfaz. El intervalo de este porcentaje es del 0 al 200%. El porcentaje máximo de 200% de una conexión dúplex completa indica que el tráfico que tiene lugar a través de la interfaz utiliza el 100% de la amplitud de banda de las conexiones entrantes y salientes. El porcentaje máximo de una conexión semidúplex media es 100%.

Unicast Received % (Porcentaje de difusión única recibida): muestra el porcentaje de paquetes de difusión única recibidos en la interfaz.

Non Unicast Packets Received % (Porcentaje de paquetes que no son de difusión única recibidos): muestra el porcentaje de paquetes que no son de difusión única que se han recibido en la interfaz.

Error Packets Received % (Porcentaje de paquetes con error recibidos): muestra el número de paquetes con errores recibidos en la interfaz.

Visualización de las estadísticas de utilización de la interfaz mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de RMON

Resumen de contadores

Utilice la página **Counter Summary** (Resumen de contadores) para ver las estadísticas de utilización de la interfaz en sumas numéricas en vez de porcentajes.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON)→ **Table Views** (Vistas de tabla)→ **Counter Summary** (Resumen de contadores) en la vista de árbol.

Ilustración 9-6. Resumen de contadores

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Counter Summary" and includes a "Unit" dropdown menu set to "1" and a "Refresh Rate" dropdown menu set to "No Refresh". Below these are two tables. The first table, "Counter Summary", has columns for Interface, Interface Status, Received Unicast Packets, Transmit Unicast Packets, Received Non Unicast Packets, Transmit Non Unicast Packets, Received Errors, and Transmit Errors. The second table, "Global System LAGs", has columns for LAG ID, LAG Name, LAG Status, Received Unicast Packets, Transmit Unicast Packets, Received Non Unicast Packets, and Transmit Errors.

Interface	Interface Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Non Unicast Packets	Received Errors	Transmit Errors
1/g1	Up	6635623	6339	365892	133900	0	0
2/g2	Down	0	0	0	0	0	0
3/g3	Down	0	0	0	0	0	0

LAG ID	LAG Name	LAG Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Errors
1	ch1	Down	0	0	0	0
2	ch2	Down	0	0	0	0
3	ch3	Down	0	0	0	0
4	ch4	Down	0	0	0	0
5	ch5	Down	0	0	0	0
6	ch6	Down	0	0	0	0
7	ch7	Down	0	0	0	0
8	ch8	Down	0	0	0	0

La página **Counter Summary** (Resumen de contadores) contiene los campos siguientes:

Unit (Unidad): especifica la unidad para la que se muestran las estadísticas.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Interface (Interfaz): especifica la interfaz para la que se muestran las estadísticas.

Interface Status (Estado de la interfaz): muestra el estado de la interfaz.

Received Unicast Packets (Paquetes de difusión única recibidos): muestra el número de paquetes de difusión única recibidos en la interfaz.

Transmit Unicast Packets (Paquetes de difusión única transmitidos): muestra el número de paquetes de difusión única transmitidos desde la interfaz.

Received Non Unicast Packets (Paquetes que no son de difusión única recibidos): muestra el número de paquetes que no son de difusión única recibidos en la interfaz.

Transmit Non Unicast Packets (Paquetes que no son de difusión única transmitidos): muestra el número de paquetes que no son de difusión única transmitidos desde la interfaz.

Received Errors (Errores recibidos): muestra el número de errores recibidos en la interfaz.

Transmit Errors (Errores transmitidos): muestra el número de errores transmitidos desde la interfaz.

Definición de la frecuencia de actualización

1. Abra la página **Counter Summary** (Resumen de contadores).
2. Seleccione la frecuencia de actualización en el menú desplegable.

Se actualizan las estadísticas de las interfaces seleccionadas a la frecuencia especificada.

Visualización de las estadísticas de utilización del puerto numérico mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de RMON

RMON

La supervisión remota (RMON) permite que el administrador de red conozca el estado y el rendimiento de la red a través de un acceso remoto.

Para visualizar la página de menú **RMON**, haga clic en **Statistics/RMON** (Estadísticas/RMON)→ **RMON** en la vista de árbol. La página de menú **RMON** contiene enlaces a las funciones siguientes:

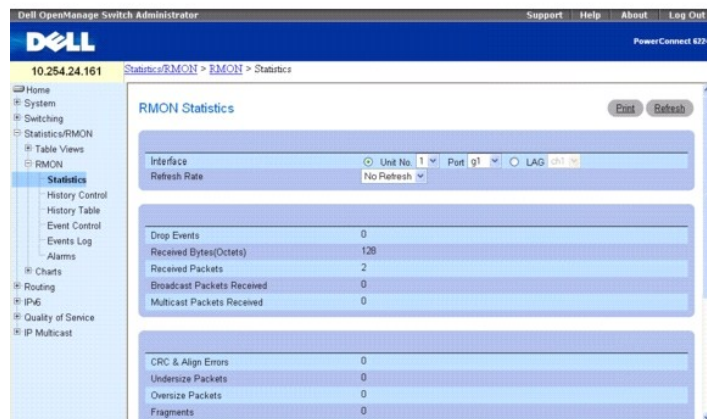
- 1 [Estadísticas de RMON](#)
- 1 [Estadísticas de control de historial de RMON](#)
- 1 [Tabla de historial de RMON](#)
- 1 [Control de eventos de RMON](#)
- 1 [Registro de eventos de RMON](#)
- 1 [Alarmas de RMON](#)

Estadísticas de RMON

Utilice la página **RMON Statistics** (Estadísticas de RMON) para ver información detallada sobre el uso del conmutador, como por ejemplo las estadísticas y los errores de procesamiento de paquetes que se han producido en el conmutador.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON)→ **RMON**→ **Statistics** (Estadísticas) en la vista de árbol.

Ilustración 9-7. Estadísticas de RMON



The screenshot displays the Dell OpenManage Switch Administrator interface. The main content area shows the 'RMON Statistics' page for interface 'g1'. The interface includes a navigation tree on the left with 'Statistics' selected. The main panel shows a table of statistics for interface 'g1' on unit '1'. The statistics are as follows:

Statistic	Value
Drop Events	0
Received Bytes/Octets	128
Received Packets	2
Broadcast Packets Received	0
Multicast Packets Received	0
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0

La página **RMON Statistics** (Estadísticas de RMON) contiene los campos siguientes:

Interface (Interfaz): especifica si se muestran las estadísticas de una unidad o de un LAG, así como la unidad o el LAG que se muestra.

Refresh Rate (Frecuencia de actualización): especifica el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son No Refresh (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es No Refresh (No actualizar).

Drop Events (Eventos descartados): muestra el número de eventos descartados en la interfaz desde la última actualización del conmutador.

Received Bytes (Octets) (Bytes [octetos] recibidos): muestra el número de octetos recibidos en la interfaz desde la última actualización del conmutador. Este número incluye los paquetes erróneos y los octetos FCS, pero no incluye los bits de trama.

Received Packets (Paquetes recibidos): muestra el número de paquetes recibidos en la interfaz, incluidos los paquetes erróneos, los paquetes de multidifusión y los paquetes de difusión, desde la última actualización del conmutador.

Broadcast Packets Received (Paquetes de difusión recibidos): muestra el número de paquetes de difusión correctos recibidos en la interfaz desde la última actualización del conmutador. Este número no incluye los paquetes de multidifusión.

Multicast Packets Received (Paquetes de multidifusión recibidos): muestra el número de paquetes de multidifusión correctos recibidos en la interfaz desde la última actualización del conmutador.

CRC & Align Errors (Errores de CRC y de alineamiento): muestra el número de errores de CRC (verificación de redundancia cíclica) y de alineamiento que se han producido en la interfaz desde la última actualización del conmutador.

Undersize Packets (Paquetes demasiado pequeños): muestra el número de paquetes cuyo tamaño es demasiado pequeño (menos de 64 octetos) recibidos en la interfaz desde la última actualización del conmutador.

Oversize Packets (Paquetes demasiado grandes): muestra el número de paquetes cuyo tamaño es demasiado grande (más de 1 518 octetos) recibidos en la interfaz desde la última actualización del conmutador.

Fragments (Fragmentos): muestra el número de fragmentos (paquetes con menos de 64 octetos, sin incluir los bits de trama, pero incluidos los octetos FCS) recibidos en la interfaz desde la última actualización del conmutador.

Jabbers (Mensajes jabber): muestra el número de paquetes recibidos cuya longitud es superior a 1 518 octetos y que han tenido una FCS durante la sesión de muestreo.

Collisions (Colisiones): muestra el número de colisiones recibidas en la interfaz desde la última actualización del conmutador.

Frames of 64 Bytes (Tramas de 64 bytes): muestra el número de tramas de 64 bytes recibidas en la interfaz desde la última actualización del conmutador.

Frames of 65 to 127 Bytes (Tramas de 65 a 127 bytes): muestra el número de tramas de 65 a 127 bytes recibidas en la interfaz desde la última actualización del conmutador.

Frames of 128 to 255 Bytes (Tramas de 128 a 255 bytes): muestra el número de tramas de 128 a 255 bytes recibidas en la interfaz desde la última actualización del conmutador.

Frames of 256 to 511 Bytes (Tramas de 256 a 511 bytes): muestra el número de tramas de 256 a 511 bytes recibidas en la interfaz desde la última actualización del conmutador.

Frames of 512 to 1023 Bytes (Tramas de 512 a 1023 bytes): muestra el número de tramas de 512 a 1023 bytes recibidas en la interfaz desde la última actualización del conmutador.

Frames of 1024 to 1518 Bytes (Tramas de 1024 a 1518 bytes): muestra el número de tramas de 1024 a 1518 bytes recibidas en la interfaz desde la última actualización del conmutador.

Visualización de las estadísticas de interfaz

1. Abra la página **RMON Statistics Group** (Grupo de estadísticas de RMON).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Aparecen las estadísticas de la interfaz seleccionada.

Visualización de las estadísticas de RMON mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

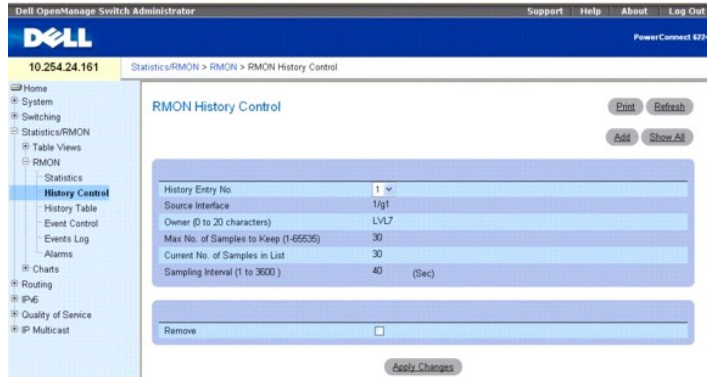
1 Comandos de RMON

Estadísticas de control de historial de RMON

Utilice la página **RMON History Control** (Control de historial de RMON) para mantener un historial de estadísticas en cada puerto. Para cada interfaz (ya sea un puerto físico o un canal de puerto), puede definir la cantidad de depósitos existentes y el intervalo de tiempo entre cada instantánea de depósito.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **History Control** (Control de historial) en la vista de árbol.

Ilustración 9-8. Control de historial de RMON



La página **RMON History Control** (Control de historial de RMON) contiene los campos siguientes:

History Entry (Entrada del historial): selecciona el número de entrada de la tabla de control de historial de RMON.

Source Interface (Interfaz de origen): especifica la interfaz de la que se obtienen las muestras del historial.

Owner (0–20 characters) (Propietario [0–20 caracteres]): indica el usuario o la estación de RMON que ha solicitado información sobre RMON.

Max No. of Samples to Keep (1–65535) (Número máximo de muestras que se deben conservar [1–65535]): define el número de depósitos históricos para esta interfaz.

Current No. of Samples in List (Número actual de muestras en la lista): muestra el número actual de muestras obtenidas.

Sampling Interval (1–3600) (Intervalo de muestreo [1–3600]): define la frecuencia con la que se obtienen los muestreos desde los puertos. Los valores posibles están comprendidos entre 1 y 3600 segundos. El valor predeterminado es 1800 segundos (30 minutos).

Remove (Eliminar): si se selecciona, elimina la entrada de la tabla de control de historial de RMON que se muestra.

Adición de una entrada del control de historial

1. Abra la página **RMON History Control** (Control de historial de RMON).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add History Entry** (Añadir entrada del historial).

Ilustración 9-9. Adición de una entrada del historial



3. Rellene los campos de esta página y haga clic en **Apply Changes** (Aplicar cambios).

La entrada se añade a la tabla de control de historial de RMON.

Visualización de la tabla de control de historial de RMON

1. Abra la página **RMON History Control** (Control de historial de RMON).
2. Haga clic en **Show All** (Mostrar todo).

Se muestra la tabla de control de historial de RMON.

Ilustración 9-10. Tabla de control de historial de RMON

History Control Table Print Refresh

History Entry No.	Source Interface	Sampling Interval	Current Number of Samples	Owner	Remove
1	1g1	1000	10		<input type="checkbox"/>

Apply Changes Back

Eliminación de una entrada de la tabla de control de historial

1. Abra la página **RMON History Control** (Control de historial de RMON).
2. Seleccione la casilla de verificación **Remove** (Eliminar) en la fila de la entrada del historial que desea eliminar.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la tabla y se actualiza el dispositivo.

Visualización del control de historial de RMON mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de RMON

Tabla de historial de RMON

Utilice la página **RMON History Table** (Tabla de historial de RMON) para ver muestreos estadísticos de red específicos de la interfaz. Cada entrada de la tabla representa todos los valores del contador compilados durante una única muestra.

Para visualizar la página **RMON History Table** (Tabla de historial de RMON), haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **History Table** (Tabla de historial) en la vista de árbol.

Ilustración 9-11. Tabla de historial de RMON

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is Statistics/RMON > RMON > RMON History Table. The configuration table for the RMON History Table is as follows:

History Entry No.	Owner	Source Interface	Max No. of Samples to Keep	Sampling Interval
1	RTP	1g1	15	45 (sec)

Below the configuration table is the RMON History Table data table:

Sample No.	Drop Events	Received Bytes (Octets)	Received Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
1	0	49595	210	42	13	0	0	0	0	0	0

La página **RMON History Table** (Tabla de historial de RMON) contiene los campos siguientes:

History Entry No. (Número de entrada del historial): selecciona el número de entrada del historial que va a mostrarse en la tabla de historial de RMON.

Owner (Propietario): muestra el nombre del propietario del grupo de estadísticas de RMON, si está disponible.

Source Interface (Interfaz de origen): indica la interfaz o el LAG en los que se recopilan las estadísticas.

Max No. of Samples to Keep (Número máximo de muestras que se deben conservar): determina la longitud de la lista de la tabla de historial para cada número de entrada del historial.

Sampling Interval (Intervalo de muestreo): define el tiempo, en segundos, que transcurre entre las sucesivas muestras.

Sample No. (Número de muestra): indica la muestra específica que refleja la información de la tabla.

Drop Events (Eventos descartados): muestra el número total de eventos en los que el puerto descartó paquetes por falta de recursos. Tenga en cuenta que este número no coincide necesariamente con el número de paquetes descartados; se trata del número de veces que se ha detectado esta condición.

Received Bytes (Octets) (Bytes [octetos] recibidos): muestra el número total de octetos de datos (incluidos los de los paquetes erróneos) recibidos en la red (sin incluir los bits de trama, pero incluidos los octetos de la secuencia de verificación de tramas [FCS]).

Received Packets (Paquetes recibidos): muestra el número total de paquetes recibidos (incluidos los paquetes erróneos, los paquetes de difusión y los paquetes de multidifusión) durante el intervalo de muestreo.

Broadcast Packets (Paquetes de difusión): muestra el número total de paquetes correctos recibidos que se dirigieron a la dirección de difusión. Tenga en

cuenta no se incluyen los paquetes de multidifusión.

Multicast Packets (Paquetes de multidifusión): muestra el número total de paquetes correctos recibidos que se dirigieron a la dirección de multidifusión. Tenga en cuenta que este número no incluye los paquetes dirigidos a la dirección de difusión.

CRC Align Errors (Errores de alineamiento de CRC): muestra el número total de paquetes recibidos cuya longitud (sin incluir los bits de trama, pero incluidos los octetos FCS) era de 64 a 1.518 octetos, ambos incluidos, pero que tenían una FCS errónea con un número entero de octetos (error de FCS) o una FCS errónea con un número no entero de octetos (error de alineamiento).

Undersize Packets (Paquetes demasiado pequeños): muestra el número total de paquetes recibidos cuya longitud era inferior a 64 octetos (sin incluir los bits de trama, pero incluidos los octetos FCS), pero que estaban formados correctamente.

Oversize Packets (Paquetes demasiado grandes): muestra el número total de paquetes recibidos de más de 1.518 octetos (sin incluir los bits de trama, pero incluidos los octetos FCS), pero que estaban formados correctamente.

Fragments (Fragmentos): muestra el número total de paquetes recibidos cuya longitud era inferior a 64 octetos, sin incluir los bits de trama, pero incluyendo una FCS con un número entero de octetos (error de FCS) o una FCS errónea con un número no entero de octetos (error de alineamiento).

Jabbers (Mensajes jabber): muestra el número total de paquetes recibidos con una longitud superior a 1.518 octetos (sin incluir los bits de trama, pero incluidos los octetos FCS), y con una secuencia de verificación de tramas (FCS) errónea con un número entero de octetos (error de FCS) o con una FCS errónea con un número no entero de octetos (error de alineamiento).

Collisions (Colisiones): muestra el mejor cálculo aproximado del número total de colisiones en este segmento Ethernet.

Utilization (Uso): estima el uso de red de capa física principal en una interfaz durante la sesión de muestreo. El valor se refleja en tanto por ciento hasta dos decimales.

Visualización de las estadísticas para una entrada específica del historial

1. Abra la página **RMON History Table** (Tabla de historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Número de entrada del historial).

Las estadísticas de la entrada se muestran en la pantalla.

Visualización del control de historial de RMON mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de RMON

Control de eventos de RMON

Utilice la página **RMON Events Control** (Control de eventos de RMON) para definir los eventos de RMON. Las alarmas de RMON utilizan los eventos para que ocurra alguna acción cuando se cruza el umbral de un determinado contador de RMON. La información sobre el evento puede almacenarse en un registro o enviarse en forma de excepción a un receptor de excepciones.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **Event Control** (Control de eventos) en la vista de árbol.

Ilustración 9-12. Control de eventos de RMON

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "RMON Event Control" and contains the following configuration fields:

Event Entry	11
Community	public
Description	general access
Event Type	Log and Trap
Time	96079
Owner	

Below the fields, there is a "Remove" checkbox and an "Apply Changes" button.

La página **RMON Event Control** (Control de eventos de RMON) contiene los campos siguientes:

Event Entry (Entrada de evento): selecciona el evento.

Community (Comunidad): especifica la comunidad a la que pertenece el evento.

Description (Descripción): describe el evento definido por el usuario.

Event Type (Tipo de evento): selecciona 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): muestra la hora en la que se ha producido el evento.

Owner (Propietario): muestra el conmutador o el usuario que ha definido el evento.

Remove (Eliminar): si se selecciona, elimina el evento de la tabla de eventos.

Adición de un evento de RMON

1. Abra la página **RMON Event Control** (Control de eventos de RMON).

2. Haga clic en **Add** (Añadir).

Aparece la página **Add an Event Entry** (Añadir una entrada de evento).

Ilustración 9-13. Adición de una entrada de evento

Event Entry	2
Community	<input type="text"/>
Description	<input type="text"/>
Event Type	None
Owner	<input type="text"/>

3. Rellene los campos de esta página.

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

Se añade el evento a la tabla de eventos de RMON y se actualiza el dispositivo.

Modificación de un evento de RMON

1. Abra la página **RMON Event Control** (Control de eventos de RMON).

2. Haga clic en **Show All** (Mostrar todo) para visualizar la página **Event Control Table** (Tabla de control de eventos).

3. Marque la casilla de verificación **Edit** (Editar) para que se modifique la entrada de evento.

4. Modifique los campos de la página según convenga.

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

Se modifica la entrada de la tabla de eventos de RMON y se actualiza el dispositivo.

Visualización de la tabla de control de eventos de RMON

1. Abra la página **RMON Event Control** (Control de eventos de RMON).

2. Haga clic en **Show All** (Mostrar todo).

Se muestra la tabla de control de eventos.

Ilustración 9-14. Tabla de control de eventos

Event Entry	Community	Description	Event Type	Time	Owner	Remove	Edit
-------------	-----------	-------------	------------	------	-------	--------	------

Eliminación de entradas de eventos de RMON

1. Abra la página **RMON Event Control** (Control de eventos de RMON).
2. Seleccione el evento que desea eliminar del menú desplegable en el campo **Event Entry** (Entrada de evento) y marque **Remove** (Eliminar).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina la entrada de la tabla y se actualiza el dispositivo.

Definición de eventos de conmutador mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de RMON

Registro de eventos de RMON

Utilice la página **RMON Event Log** (Registro de eventos de RMON) para ver una lista de eventos de RMON.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **Events Log** (Registro de eventos) en la vista de árbol.

Ilustración 9-15. Registro de eventos de RMON

Event	Log No.	Log Time	Description
-------	---------	----------	-------------

La página **RMON Event Log** (Registro de eventos de RMON) contiene los campos siguientes:

Event (Evento): muestra el número de entrada del registro de eventos de RMON.

Log No. (Número de registro): muestra el número de registro.

Log Time (Hora de registro): muestra la hora en la que se ha introducido la entrada del registro.

Description (Descripción): describe la entrada del registro.

Definición de eventos de conmutador mediante el comando de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

- 1 Comandos de RMON

Alarmas de RMON

Utilice la página **RMON Alarms** (Alarmas de RMON) para establecer las alarmas de red. Las alarmas se activan cuando se cruzan determinados umbrales de los contadores de RMON configurados. La alarma hace que se produzca un evento. Los eventos pueden configurarse como parte del grupo de eventos de RMON. Para obtener más información sobre eventos, consulte "[Registro de eventos de RMON](#)".

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **RMON** → **Alarms** (Alarmas) en la vista de árbol.

Ilustración 9-16. Alarmas de RMON



La página **RMON Alarms** (Alarmas de RMON) contiene los campos siguientes:

Alarm Entry (Entrada de alarma): selecciona una alarma específica en el menú desplegable.

OID: especifica el identificador de objeto.

Counter Value (Valor del contador): muestra el número de eventos seleccionados que se cuentan.

Sample Type (Tipo de muestra): muestra el método de muestreo para la variable seleccionada y compara el valor con los umbrales. Los valores del campo posibles son:

Delta: resta del valor actual el último valor de muestra. La diferencia de los valores se compara con el umbral.

Absolute (Absoluto): compara los valores directamente con los umbrales al final del intervalo de muestreo. Éste es el valor predeterminado.

Rising Threshold (0-2147483647) (Umbral superior [0-2147483647]): muestra el valor del contador superior que activa la alarma del umbral superior. El umbral superior aparece en la parte superior de las barras de gráficos. Cada variable supervisada tiene asignado un color. El valor predeterminado es 100.

Rising Event (Evento superior): muestra el mecanismo en el que se notifican alarmas, por ejemplo, un registro, una excepción o ambos. Cuando se selecciona un registro, no existe ningún mecanismo de almacenamiento en el conmutador ni en el sistema de administración. Sin embargo, si el conmutador no se restablece, el evento permanece en la tabla de registros del conmutador. Si se selecciona una excepción, se genera una excepción de SNMP y se notifica a través del mecanismo de la excepción. La excepción se puede guardar con el mismo mecanismo.

Falling Threshold (0-2147483647) (Umbral inferior [0-2147483647]): muestra el valor del contador inferior que activa la alarma del umbral inferior. El umbral inferior se presenta gráficamente en la parte superior de las barras de gráficos. Cada variable supervisada tiene asignado un color. El valor predeterminado es 20.

Falling Event (Evento inferior): muestra el mecanismo en el que se notifican alarmas, por ejemplo, un registro, una excepción o ambos. Cuando se selecciona un registro, no existe ningún mecanismo de almacenamiento en el conmutador ni en el sistema de administración. Sin embargo, si el conmutador no se restablece, el evento permanece en la tabla de registros del conmutador. Si se selecciona una excepción, se genera una excepción de SNMP y se notifica a través del mecanismo de la excepción. La excepción se puede guardar con el mismo mecanismo.

Startup Alarms (Alarmas de inicio): muestra el tipo de evento. Las opciones son Rising (Superior); Rising-Falling (Superior-inferior) y Falling (Inferior).

Interval (0-2147483647) (Intervalo [0-2147483647]): muestra el intervalo de tiempo entre alarmas. El valor predeterminado es 100.

Owner (Propietario): muestra el conmutador o el usuario que ha definido la alarma.

Remove (Eliminar): si se selecciona, elimina una alarma de RMON.

Adición de una entrada de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
2. Haga clic en **Add** (Añadir).

Aparece la página **Add an Alarm Entry** (Añadir una entrada de alarma).

Ilustración 9-17. Adición de una entrada de alarma

Add an Alarm Entry End Refresh

Alarm Entry	1
OID	
Sample Type	Absolute
Rising Threshold (0 to 2147483647)	
Rising Event	
Falling Threshold (0 to 2147483647)	
Falling Event	
Startup Alarms	Rising
Interval (0 to 2147483647)	(Sec)
Owner	

Apply Changes Back

3. Rellene los campos de esta página según convenga.
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Se añade la alarma de RMON y se actualiza el dispositivo.

Visualización de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
 2. Haga clic en **Show All** (Mostrar todo).
- Se muestra la parte izquierda de la tabla de alarmas de RMON.

Ilustración 9-18. Tabla de alarmas de RMON

RMON Alarms Table End Refresh

Alarm Entry	OID	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event
1		0	Absolute	10	1	20	2

Apply Changes Back

3. Haga clic en la flecha derecha situada en la parte inferior de la pantalla para ver la parte derecha de la tabla.

Eliminación de una entrada de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
 2. Seleccione una entrada en el menú desplegable **Alarm Entry** (Entrada de alarma).
 3. Marque la casilla de verificación **Remove** (Eliminar) y haga clic en **Apply Changes** (Aplicar cambios).
- Se elimina la entrada y se actualiza el dispositivo.

Eliminación de varias entradas de la tabla de alarmas

1. Abra la página **RMON Alarms** (Alarmas de RMON).
 2. Haga clic en **Show All** (Mostrar todo).
- Se muestra la tabla de alarmas de RMON.
3. Marque la casilla de verificación **Remove** (Eliminar) para eliminar cada entrada de alarma.
 4. Haga clic en **Apply Changes** (Aplicar cambios).
- Se eliminan las entradas y se actualiza el dispositivo.

Definición de alarmas del conmutador mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte el capítulo siguiente de la Guía de referencia de la CLI:

Gráficos

La página de menú **Chart** (Gráfico) contiene enlaces a páginas web que permiten generar estadísticas en un gráfico. Para visualizar la página de menú **Charts** (Gráficos), haga clic en **Statistics/RMON** (Estadísticas/RMON)→ **Charts** (Gráficos) en la vista de árbol. La página de menú **Charts** (Gráficos) contiene enlaces a las funciones siguientes:

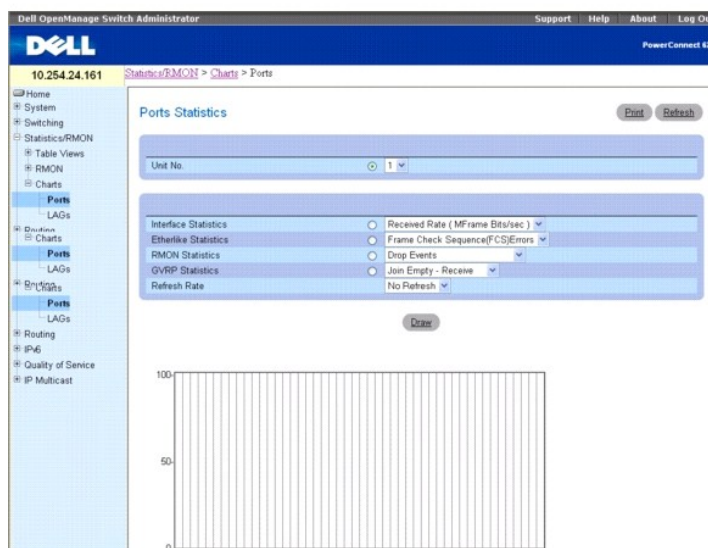
- 1 [Estadísticas de puerto](#)
- 1 [Estadísticas de LAG](#)

Estadísticas de puerto

Utilice la página **Ports Statistics** (Estadísticas de puerto) para generar estadísticas relativas a un puerto en un gráfico.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON)→ **Charts** (Gráficos)→ **Ports** (Puertos) en la vista de árbol.

Ilustración 9-19. Estadísticas de puerto



La página **Ports Statistics** (Estadísticas de puerto) contiene los campos siguientes:

Unit No. (Número de unidad): selecciona el puerto que va a mostrarse.

Interface Statistics (Estadísticas de interfaz): si se activa, selecciona las estadísticas de interfaz y especifica el tipo de estadísticas de interfaz que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Received Rate (MFrame Bits/sec)** (Velocidad de recepción [MFrame bits/s]).

Etherlike Statistics (Estadísticas de Etherlike): si se activa, selecciona las estadísticas de Etherlike y especifica el tipo de estadísticas de Etherlike que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Frame Check Sequence (FCS) Errors** (Errores de secuencia de verificación de tramas [FCS]).

RMON Statistics (Estadísticas de RMON): si se activa, selecciona las estadísticas de RMON y especifica el tipo de estadísticas de RMON que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Drop Events** (Eventos descartados).

GVRP Statistics (Estadísticas de GVRP): si se activa, selecciona las estadísticas de GVRP y especifica el tipo de estadísticas de GVRP que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Join Empty - Receive** (Unir vacíos - Recibir).

Refresh Rate (Frecuencia de actualización): selecciona el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son **No Refresh** (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es **No Refresh** (No actualizar).

Visualización de las estadísticas de puerto

1. Abra la página **Ports Statistics** (Estadísticas de puerto).
2. Seleccione el puerto del que se generarán estadísticas en un gráfico.
3. Haga clic en el botón de radio asociado a las estadísticas que van a generarse en un gráfico.
4. Seleccione el tipo de estadísticas en el menú desplegable correspondiente.

5. Seleccione la frecuencia de actualización que desee en el menú desplegable **Refresh Rate** (Frecuencia de actualización).
 6. Haga clic en **Draw** (Dibujar).
- Se generan las estadísticas seleccionadas en el gráfico.

Visualización de las estadísticas de puerto mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la Guía de referencia de la CLI:

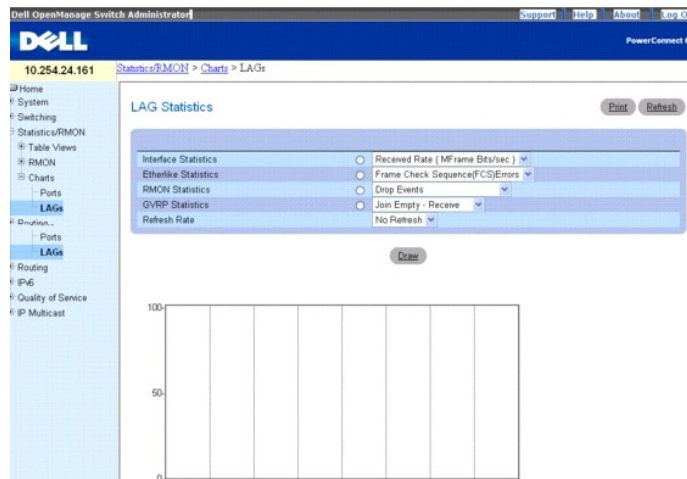
- 1 Comandos de administración del sistema
- 1 Comandos de RMON
- 1 Comandos GVRP

Estadísticas de LAG

Utilice la página **LAG Statistics** (Estadísticas de LAG) para generar estadísticas relativas a un LAG en un gráfico.

Para visualizar la página, haga clic en **Statistics/RMON** (Estadísticas/RMON) → **Charts** (Gráficos) → **LAGs** (LAG) en la vista de árbol.

Ilustración 9-20. Estadísticas de LAG



La página **LAG Statistics** (Estadísticas de LAG) contiene los campos siguientes:

Interface Statistics (Estadísticas de interfaz): si se activa, selecciona las estadísticas de interfaz y especifica el tipo de estadísticas de interfaz que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Received Rate** (Velocidad de recepción).

Etherlike Statistics (Estadísticas de Etherlike): si se activa, selecciona las estadísticas de Etherlike y especifica el tipo de estadísticas de Etherlike que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Frame Check Sequence Errors** (Errores de secuencia de verificación de tramas).

RMON Statistics (Estadísticas de RMON): si se activa, selecciona las estadísticas de RMON y especifica el tipo de estadísticas de RMON que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Drop Events** (Eventos descartados).

GVRP Statistics (Estadísticas de GVRP): si se activa, selecciona las estadísticas de GVRP y especifica el tipo de estadísticas de GVRP que va a generarse en un gráfico en el menú desplegable. El valor predeterminado es **Join Empty - Receive** (Unir vacíos - Recibir).

Refresh Rate (Frecuencia de actualización): selecciona el tiempo que transcurre antes de que se actualicen las estadísticas. Los valores posibles de este campo son **No Refresh** (No actualizar), 15, 30 y 60 segundos. El valor predeterminado es 15 segundos.

Visualización de las estadísticas de LAG

1. Abra la página **LAG Statistics** (Estadísticas de LAG).
2. Haga clic en el botón de radio asociado a las estadísticas que van a generarse en un gráfico.
3. Seleccione el tipo de estadísticas en el menú desplegable correspondiente.

4. Seleccione la frecuencia de actualización que desee en el menú desplegable **Refresh Rate** (Frecuencia de actualización).
5. Haga clic en **Draw** (Dibujar).

Se generan las estadísticas seleccionadas en el gráfico.

Visualización de las estadísticas de LAG mediante los comandos de la CLI

Para obtener información sobre los comandos de la CLI que realizan esta función, consulte los capítulos siguientes de la Guía de referencia de la CLI:

- | Comandos de administración del sistema
- | Comandos de RMON
- | Comandos GVRP

[Regresar a la página de contenido](#)