




Guía del usuario del sistema Dell™ PowerConnect™ 5324

[Introducción](#)
[Descripción del hardware](#)
[Instalación del dispositivo PowerConnect](#)
[Inicio y configuración del dispositivo](#)
[Utilización del administrador del conmutador Dell OpenManage](#)
[Configuración de la información del sistema](#)
[Configuración de la información del dispositivo](#)
[Visualización de las estadísticas](#)
[Configuración de QoS](#)
[Especificaciones del dispositivo](#)
[Glosario](#)

Notas, avisos y precauciones

-  **NOTA:** Una NOTA proporciona información importante que le ayuda a utilizar su equipo de la mejor manera posible.
 -  **AVISO:** Un AVISO indica la posibilidad de daños en el hardware o pérdida de datos, y le explica cómo evitar el problema.
 -  **PRECAUCIÓN:** Una PRECAUCIÓN indica un posible daño material, lesión corporal o muerte.
-

La información contenida en este documento puede modificarse sin aviso previo.
© 2003 - 2007 Dell Inc. Todos los derechos reservados.

Queda prohibida su reproducción en cualquier medio sin la autorización por escrito de Dell Corporation.

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* y *Windows* son marcas comerciales registradas de Microsoft Corporation.

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.

Mayo 2007

[Regresar a la página de contenido](#)

Inicio y configuración del dispositivo

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Configuración del terminal](#)
- [Inicio del dispositivo](#)
- [Descripción general de la configuración](#)
- [Configuración inicial](#)
- [Nombre de usuario](#)
- [Cadenas de comunidad SNMP](#)
- [Configuración avanzada](#)
- [Recuperación de una dirección IP desde un servidor DHCP](#)
- [Recepción de una dirección IP desde un servidor BOOTP](#)
- [Configuración de contraseñas y gestión de la seguridad](#)
- [Configuración de contraseñas de seguridad](#)
- [Procedimientos de inicio](#)

Tras efectuar todas las conexiones externas, debe conectar un terminal al dispositivo para poder configurar el dispositivo y para otros procedimientos. Para la configuración inicial, se lleva a cabo la configuración de dispositivo estándar.


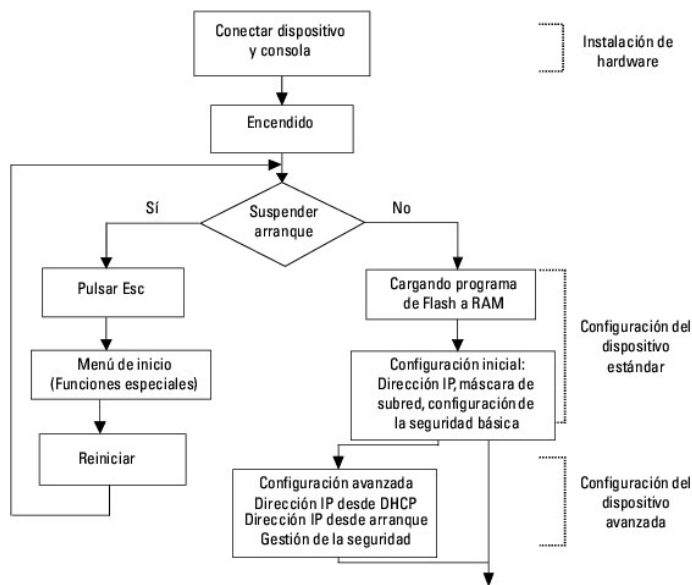
 **NOTA:** Antes de continuar, lea las notas de la versión de este producto. Las notas de la versión se pueden descargar del sitio web www.support.dell.com.

Ilustración 4-12. Esquema de instalación y configuración




Configuración del terminal

Para configurar el dispositivo, el terminal debe ejecutar software de emulación de terminal.


Asegúrese de que el software de emulación de terminal se configura de la manera siguiente:

1. Seleccione el puerto serie adecuado (puerto serie 1 o puerto serie 2) para conectarlo a la consola.
2. Establezca la velocidad de los de datos en 9600 baudios.

3. Establezca el formato de los datos en 8 bits de datos, 1 bit de parada y ninguna paridad.
4. Establezca el control de flujo en **ninguno**.
5. En **Properties** (Propiedades), seleccione el modo **VT100 for Emulation** (VT100 para emulación).
6. Seleccione **Terminal keys** (Teclas de terminal) para las teclas **Function** (Función), **Arrow** (Flecha) y **Ctrl**. Asegúrese de que configura **Terminal keys** (Teclas de terminal) (no **Windows keys** [Teclas de Windows]).

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

Inicio del dispositivo

 **NOTA:** Se supone que la información de inicio es la siguiente:

- o El dispositivo se suministra con una configuración predeterminada.
- o El dispositivo no se configura con un nombre de usuario y una contraseña predeterminados.

Para iniciar el dispositivo, realice los siguientes pasos:

1. Asegúrese de que el puerto serie del dispositivo esté conectado a un terminal ASCII, o al conector serie de un sistema de sobremesa que ejecute software de emulación de terminal.
2. Localice un enchufe de CA.
3. Apague el enchufe de CA.
4. Conecte el dispositivo al enchufe de CA. Consulte el apartado "[Conexión de un dispositivo a un suministro de energía](#)".
5. Encienda el enchufe de CA.

Si se enciende la alimentación con el terminal local ya conectado, el dispositivo pasa por una autoprueba de encendido (POST). POST se ejecuta cada vez que el dispositivo se inicia y comprueba los componentes de hardware para determinar si el dispositivo está completamente operativo antes de iniciarse por completo. Si se detecta un problema grave, el flujo del programa se detiene. Si POST finaliza correctamente, se carga una imagen ejecutable válida en la RAM. Los mensajes de POST se muestran en el terminal e indican si la prueba ha finalizado con éxito o no.

1. Asegúrese de que el cable ASCII esté conectado al terminal, y de que los parámetros de emulación de software estén configurados correctamente.
2. Conecte el suministro de energía al dispositivo.
3. Encienda el dispositivo.
4. Mientras se inicia el dispositivo, la prueba de inicio efectúa en primer lugar un recuento de la memoria disponible del dispositivo y, a continuación, prosigue con el inicio. En la pantalla que figura a continuación se muestra un ejemplo de la POST que se puede ver en el terminal:

```
----- Performing the Power-On Self Test (POST) -----
```

```
UART Channel Loopback Test.....PASS
```

```
Testing the System SDRAM.....PASS
```

```
Boot1 Checksum Test.....PASS
```

```
Boot2 Checksum Test.....PASS
```

```
Flash Image Validation Test.....PASS
```

```
BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28
```

Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

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

Preparing to decompress...

El proceso de inicio dura aproximadamente 90 segundos.

El mensaje de autoinicio que aparece al final de la POST (véanse las últimas líneas) indica que no se ha encontrado ningún problema durante el inicio.

Durante el inicio se puede utilizar el menú **Startup** (Inicio) para ejecutar procedimientos especiales. Para entrar en el menú **Startup** (Inicio), pulse <Esc> o <Intro> en los dos segundos siguientes a la aparición del mensaje de autoinicio.

Si no interrumpe el inicio del sistema pulsando <Esc> ni <Intro>, el proceso continúa descomprimiendo y cargando el código en la RAM. El código se inicia ejecutándose desde la RAM y se muestra una lista numerada de los puertos del sistema y sus estados (activo o inactivo).

En la pantalla que se muestra continuación figura un ejemplo de configuración. Algunos elementos, como direcciones, versiones y fechas, pueden diferir para cada dispositivo.

Decompressing SW from image-2

78c000

OK

Running from RAM...

*** Running SW Ver. 1.0.0.15 Date 03-Mar-2004 Time 10:41:14 ***

HW version is 00.01.07

Base Mac address is: 00:00:07:77:77:77

Dram size is : 64M bytes

Dram first block size is : 40960K bytes

Dram first PTR is : 0x1800000

Flash size is: 16M

Device configuration:

Pretera based system

Slot 1 - Neyland24 HW Rev. 0.1

Tapi Version: v1.2.9

Core Version: v1.2.9

01-Jan-2000 01:01:32 %INIT-I-InitCompleted: Initialization task is completed

console> 01-Jan-2000 01:01:35 %LINK-W-Down: g1

01-Jan-2000 01:01:35 %LINK-W-Down: g2

01-Jan-2000 01:01:35 %LINK-W-Down: g3

01-Jan-2000 01:01:35 %LINK-W-Down: g4

01-Jan-2000 01:01:35 %LINK-W-Down: g5

01-Jan-2000 01:01:35 %LINK-W-Down: g6

01-Jan-2000 01:01:35 %LINK-W-Down: g7

01-Jan-2000 01:01:35 %LINK-W-Down: g8

01-Jan-2000 01:01:35 %LINK-W-Down: g9

01-Jan-2000 01:01:35 %LINK-W-Down: g10

01-Jan-2000 01:01:35 %LINK-W-Down: g11

01-Jan-2000 01:01:35 %LINK-W-Down: g12

01-Jan-2000 01:01:35 %LINK-W-Down: g13

01-Jan-2000 01:01:36 %LINK-W-Down: g14

01-Jan-2000 01:01:36 %LINK-W-Down: g15

01-Jan-2000 01:01:36 %LINK-W-Down: g16

01-Jan-2000 01:01:36 %LINK-W-Down: g17

01-Jan-2000 01:01:36 %LINK-W-Down: g18

01-Jan-2000 01:01:36 %LINK-W-Down: g19

01-Jan-2000 01:01:36 %LINK-W-Down: g20

01-Jan-2000 01:01:36 %LINK-W-Down: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g22

01-Jan-2000 01:01:36 %LINK-I-Up: vlan 3000

01-Jan-2000 01:01:36 %LINK-I-Up: vlan 1

01-Jan-2000 01:01:36 %LINK-I-Up: g1

01-Jan-2000 01:01:36 %LINK-I-Up: g13

01-Jan-2000 01:01:36 %LINK-I-Up: g14

01-Jan-2000 01:01:36 %LINK-I-Up: g19

01-Jan-2000 01:01:36 %LINK-I-Up: g20

01-Jan-2000 01:01:36 %LINK-I-Up: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g23

01-Jan-2000 01:01:36 %LINK-W-Down: g24

```
01-Jan-2000 01:01:36 %LINK-W-Down: chl

01-Jan-2000 01:01:36 %LINK-I-Up: vlan 1000

01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 added to chl

01-Jan-2000 01:01:36 %LINK-I-Up: g22

01-Jan-2000 01:01:36 %LINK-I-Up: g23

01-Jan-2000 01:01:36 %LINK-I-Up: g24

01-Jan-2000 01:01:36 %LINK-I-Up: chl

01-Jan-2000 01:01:36 %LINK-W-Down: g1

01-Jan-2000 01:03:42 %INIT-I-Startup: Cold Startup
```

```
console>
```

Después de que el dispositivo se inicie correctamente, se muestra un aviso del sistema (`console>`) que se utiliza para configurar el dispositivo. No obstante, antes de configurar el dispositivo, compruebe que la versión de software instalada en el dispositivo sea la última. En caso contrario, descargue e instale la última versión. Para obtener más información sobre la descarga de la última versión, consulte el apartado ["Descarga de software"](#).

Descripción general de la configuración

Antes de asignar una dirección IP estática al dispositivo, debe obtener la siguiente información:

- 1 Una dirección IP específica que ha sido asignada al dispositivo para que se configure.
- 1 Ruta predeterminada.
- 1 Máscara de red para esta red.

Hay dos tipos de configuración:


- 1 **Configuración inicial:** consta de funciones de configuración con consideraciones de seguridad básica.
- 1 **Configuración avanzada:** consta de la configuración IP dinámica y más consideraciones de seguridad avanzadas.




NOTA: Después de realizar cualquier cambio en la configuración, debe guardarse la configuración nueva antes de reiniciar. Para guardar la configuración, escriba:

```
console# copy running-config startup-config
```

Configuración inicial

 **NOTA:** Antes de continuar, lea las notas de la versión de este producto. Las notas de la versión se pueden descargar del sitio web Dell Support en la dirección support.dell.com.

 **NOTA:** La configuración inicial utiliza las siguientes suposiciones:

- o El dispositivo PowerConnect no se ha configurado nunca antes y se encuentra en el mismo estado que cuando lo recibí.
- o El dispositivo PowerConnect se ha iniciado correctamente.
- o Se ha establecido la conexión serie y la petición de consola se muestra en la pantalla de un dispositivo de terminal VT100. (Pulse la tecla <Intro> varias veces para comprobar que la petición se muestra correctamente).
- o El dispositivo no se configura con un nombre de usuario y una contraseña predeterminados.

La configuración inicial del dispositivo se realiza mediante el puerto de la consola. Después de la configuración inicial, el dispositivo se puede gestionar desde el puerto serie ya conectado o de manera remota mediante una interfaz definida durante la configuración inicial.

La configuración inicial se compone de lo siguiente:

- 1 Establecer 'admin' como nombre de usuario y 'dell' como contraseña con el nivel 15 de privilegio superior.
- 1 Configurar la dirección IP estática y la puerta de enlace predeterminada.
- 1 Configurar la cadena de comunidad de lectura/escritura SNMP.
- 1 Asignar la dirección IP asignada por el servidor DHCP.

Antes de aplicar el proceso de configuración inicial al dispositivo PowerConnect, hay que obtener la siguiente información del administrador de red:

- 1 La dirección IP que hay que asignar a una VLAN a través de la cual se gestiona el dispositivo.
- 1 La máscara de subred IP de la red.
- 1 La dirección IP de la puerta de acceso predeterminada.
- 1 La comunidad SNMP.

Dirección IP estática y máscara de subred

Se puede configurar una dirección IP en cualquier interfaz, incluida una VLAN, un LAG y un puerto físico. Tras especificar el comando de configuración, se recomienda comprobar si ya se ha configurado algún puerto con la dirección IP; para ello, escriba el comando **show ip interface**.


Importante: Si una dirección IP se configura en un LAG o en un puerto físico (por ejemplo, g10), dicha interfaz se elimina de VLAN 1.

Configuración de direccionamiento estático

Para gestionar el dispositivo desde una red remota debe configurar una ruta estática, que es una dirección IP a la que se envían los paquetes cuando no se encuentra ninguna entrada en las tablas del dispositivo. La dirección IP configurada debe pertenecer a la misma subred que una de las interfaces IP del dispositivo.

Para configurar una ruta estática, escriba el comando en el indicador del sistema tal como se muestra en el ejemplo de configuración siguiente, en el que 100.1.1.1 (máscara 24) es la estación de gestión específica, y 100.1.1.10 es la ruta estática que funciona como la puerta de enlace predeterminada.

Asignación de direcciones IP estáticas en una interfaz en banda

 **NOTA:** En este ejemplo se tiene en cuenta los siguientes supuestos:

- o La dirección IP que hay que asignar a la interfaz VLAN del dispositivo PowerConnect es 192.168.1.123
- o La máscara de subred IP de la red es 255.255.255.0
- o La dirección IP de la ruta predeterminada es 192.168.1.1
- o La cadena de la comunidad de lectura/escritura SNMP es "private"


```

console> enable

console# configure

console(config)# username admin password dell level 15

console(config)# interface vlan 1

console (config-if) # ip address 192.168.1.123 /24

console(config-if)# exit

console(config)# ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

console(config)# exit

console#

```

Comprobación de la dirección IP y la dirección de puerta de enlace predeterminada

Asegúrese de que la dirección IP y la puerta de enlace predeterminada se asignan correctamente mediante la ejecución del siguiente comando y la visualización de su salida de texto:


Comando

```
console# show ip interface vlan 1
```

Salida


Gateway IP Address	Activity status	
-----	-----	
192.168.1.1	Active	
IP address	Interface	Type

-----	-----	-----
192.168.1.123 /24	vlan 1	Static

 **NOTA:** Se recomienda que descargue la revisión más reciente de la documentación del usuario en el sitio web Dell Support en la dirección support.dell.com.

Nombre de usuario

Para gestionar el dispositivo remotamente, por ejemplo, a través de SSH, Telnet o la interfaz web, hay que configurar un nombre de usuario. Para obtener el control administrativo completo del dispositivo, hay que especificar el privilegio más alto (15).

 **NOTA:** Sólo se permite gestionar el dispositivo a través de la interfaz de navegador web al administrador (superusuario) que disponga del nivel de privilegio más alto (15).

Para obtener más información sobre el nivel de privilegio, consulte la publicación "CLI Reference Guide" (Guía de referencia CLI).

El nombre de usuario configurado se escribe como nombre de inicio de sesión para las sesiones de gestión remotas. Para configurar el nombre de usuario y el nivel de privilegio, escriba el comando en el indicador del sistema, tal como se muestra en el ejemplo de configuración:


```
console> enable
console# configure
console(config)# username admin password abc level 15
```

Cadenas de comunidad SNMP

El SNMP (Simple Network Management Protocol, Protocolo simple de administración de redes) proporciona un método para administrar dispositivos en una red. Los dispositivos compatibles con SNMP ejecutan un software local (agente). Los agentes SNMP mantienen una lista de variables utilizadas para administrar el dispositivo. Las variables se definen en la MIB (Management Information Base, Base de datos de información de administración). La MIB presenta las variables controladas por el agente. El agente SNMP define el formato de especificación de la MIB, así como el formato utilizado para obtener acceso a la información por la red. Las cadenas de acceso y de comunidad SNMP controlan los derechos de acceso al agente SNMP.

El dispositivo es compatible con SNMP y contiene un agente SNMP que admite un conjunto de variables MIB estándar y privadas. Los desarrolladores de estaciones de gestión requieren la estructura exacta del árbol de MIB y reciben la información completa de las MIB privadas antes de poder gestionar las MIB.

Todos los parámetros pueden gestionarse desde cualquier plataforma de gestión SNMP, excepto la dirección IP de la estación de gestión SNMP, el nombre de comunidad y los derechos de acceso. Si no existen cadenas de comunidad, se desactiva el acceso de administración SNMP al dispositivo.

 **NOTA:** El dispositivo se proporciona con las cadenas de comunidad sin configurar. El dispositivo admite SNMPv1 y SNMPv2. En esta sección se describen los parámetros de configuración de SNMPv1/v2.

En la pantalla siguiente se muestra la configuración predeterminada del dispositivo:

Console# show snmp		
Community-String	Community-Access	IP address
-----	-----	-----
Traps are enabled.		

Authentication trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
System Contact:		
System Location:		

Durante el procedimiento de configuración inicial, la cadena de comunidad, el acceso de comunidad y la dirección IP se pueden establecer a través del terminal local.

Las opciones de configuración SNMP son:

- 1 Cadena de comunidad.
 - o **Sólo lectura:** Indica que los miembros de la comunidad pueden ver la información de configuración, pero no pueden cambiarla.
 - o **Lectura/Escritura:** Indica que los miembros de la comunidad pueden ver y modificar la información de configuración.
 - o **Super:** Indica que los miembros de la comunidad tienen acceso de administrador.
- 1 Dirección IP configurable. Si una dirección IP no está configurada, todos los miembros de la comunidad con el mismo nombre de comunidad disponen de los mismos derechos de acceso.

Generalmente se utilizan dos cadenas de comunidad para el dispositivo: una (comunidad pública) con acceso de sólo lectura y la otra (comunidad privada) con acceso de lectura-escritura. La cadena pública permite a las estaciones de gestión autorizadas recuperar objetos MIB, mientras que la cadena privada permite a las estaciones de gestión no autorizadas recuperar y modificar objetos MIB.

Durante la configuración inicial, es recomendable configurar el dispositivo en función de los requisitos del administrador de red, de acuerdo con la utilización de una estación de gestión basada en SNMP.

Configuración de SNMP

Para configurar las cadenas de comunidad y la dirección IP de la estación SNMP para las tablas del enrutador del dispositivo general, realice los siguientes pasos.

1. En el indicador de la consola, escriba el comando **Enable**. La línea de comandos se muestra como #.
2. Introduzca el comando **configure** y pulse <Intro>.
3. En el modo de configuración, escriba el comando de configuración de SNMP con los parámetros, incluido el nombre de comunidad (privada), el derecho de acceso de comunidad (lectura y escritura) y la dirección IP, tal como se muestra en el ejemplo siguiente:

```
console# configure
```

```
config(config)# snmp-server community private rw 11.1.1.2
```

Visualización de las tablas de comunidad SNMP

Para ver las tablas de comunidad y la dirección IP de la estación SNMP:

1. En el indicador de la consola, escriba el comando **exit**. La línea de comandos se muestra como #.
2. En el modo Privileged Exec, escriba el comando show tal como se muestra en el siguiente ejemplo:

Los parámetros configurados permiten efectuar una configuración más amplia del dispositivo desde cualquier ubicación remota.

Console# show snmp		
Community-String	Community-Access	IP address
-----	-----	-----
private	read write	11.1.1.2
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
System Contact:		
System Location:		

Configuración avanzada

En esta sección se proporciona información sobre la asignación dinámica de direcciones IP y la gestión de la seguridad basada en el mecanismo de autenticación, autorización y contabilidad (AAA), e incluye los temas siguientes:

- 1 Configuración de direcciones IP a través de DHCP
- 1 Configuración de direcciones IP a través de BOOTP
- 1 Configuración de contraseñas y gestión de la seguridad

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

Recuperación de una dirección IP desde un servidor DHCP

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

1. Seleccione y conecte un puerto cualquiera a un servidor DHCP o a una subred que disponga de uno, para poder recuperar la dirección IP.
2. Escriba los comandos siguientes para utilizar el puerto seleccionado para la recepción de la dirección IP. En el ejemplo siguiente, los comandos se basan en el tipo de puerto utilizado para la configuración.
 - 1 Asignación de direcciones IP dinámicas:

```
console# configure
```

```
console(config)# interface ethernet g1
```

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

```
console(config-if)# exit
```

```
console(config)#
```

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

```
console# configure
```

```
console(config)# interface ethernet vlan 1
```


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


```
console(config-if)# exit
```

```
console(config)#
```

- Para verificar la dirección IP, escriba el comando `show ip interface` en el indicador del sistema, tal como se muestra en el ejemplo siguiente.

Console# show ip interface		
Gateway IP Address	Activity status	
-----	-----	
10.7.1.1	Active	
IP address	Interface	Type
-----	-----	-----
10.7.1.192/24	vlan 1	Static
10.7.2.192/24	VLAN 2	DHCP

 **NOTA:** No es necesario suprimir la configuración del dispositivo para recuperar una dirección IP del servidor DHCP.

 **NOTA:** Cuando copie archivos de configuración, evite utilizar un archivo de configuración que contenga una instrucción para habilitar DHCP en una interfaz que se conecte al mismo servidor DHCP, o que contenga una configuración idéntica. En esta instancia, el dispositivo recupera el nuevo archivo de configuración y arranca desde el mismo. A continuación, el dispositivo habilita DHCP, tal como se indica en el nuevo archivo de configuración, y DHCP le da instrucciones para que recargue de nuevo el mismo archivo.


Recepción de una dirección IP desde un servidor BOOTP

Se admite el protocolo BOOTP estándar que permite al dispositivo descargar automáticamente su configuración de sistema principal IP desde cualquier servidor BOOTP estándar en la red. En este caso, el dispositivo actúa como un cliente BOOTP.

Para recuperar una dirección IP desde un servidor BOOTP:

1. Seleccione y conecte un puerto cualquiera a un servidor BOOTP o a una subred que disponga de uno, para poder recuperar la dirección IP.
2. En el indicador del sistema escriba el comando **delete startup configuration** para suprimir de la flash la configuración de inicio.

El dispositivo se reinicia sin configuración alguna y 60 segundos después empieza a emitir solicitudes BOOTP. El dispositivo recibe la dirección IP automáticamente.

 **NOTA:** Cuando comienza el reinicio del dispositivo, cualquier entrada que se efectúe en el terminal ASCII o mediante el teclado cancela, automáticamente, el proceso de BOOTP antes de que finalice y el dispositivo no recibe ninguna dirección IP del servidor BOOTP.

En el ejemplo siguiente se ilustra el proceso:

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

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

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

*****

/* the switch reboots */
```

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

En este punto, el dispositivo está configurado con una dirección IP.

Configuración de contraseñas y gestión de la seguridad


La seguridad del sistema se maneja a través del mecanismo de autenticación, autorización y contabilidad (AAA) que gestiona los derechos de acceso de usuarios, privilegios y métodos de gestión. El método AAA utiliza bases de datos de usuarios tanto locales como remotas. El cifrado de datos se lleva a cabo a través del mecanismo SSH.


El sistema se entrega sin que se haya configurado la contraseña predeterminada. Todas las contraseñas están definidas por el usuario. Si se pierde una contraseña definida por el usuario, puede invocarse un procedimiento de recuperación de contraseña desde el menú **Startup** (Inicio). El procedimiento sólo puede aplicarse al terminal local y permite un sólo acceso al dispositivo desde éste sin que deba escribirse ninguna contraseña.

Configuración de contraseñas de seguridad

Es posible configurar las contraseñas de seguridad para los servicios siguientes:

- 1 Terminal
- 1 Telnet
- 1 SSH
- 1 HTTP
- 1 HTTPS

 **NOTA:** Las contraseñas están definidas por el usuario.

 **NOTA:** Al crear un nombre de usuario, la prioridad predeterminada es 1, que otorga acceso pero no derechos de configuración. Debe establecerse una prioridad de 15 para otorgar acceso y derechos de configuración del dispositivo. Aunque es posible asignar el nivel de privilegio 15 a los nombres de usuario sin definir ninguna contraseña, es recomendable asignar siempre una contraseña. Si no se especifica ninguna contraseña, los usuarios privilegiados pueden acceder a la interfaz web sin contraseña.

Configuración de una contraseña inicial de terminal

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

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password george
```

- 1 Cuando se conecte inicialmente a un dispositivo a través de una sesión de terminal, escriba `george` cuando se le pida la contraseña.
- 1 Cuando cambie el modo de un dispositivo a "enable", escriba `george` cuando se le pida la contraseña.

Configuración de una contraseña inicial Telnet

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

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
```

- 1 Cuando se conecte inicialmente a un dispositivo a través de una sesión Telnet, escriba `bob` cuando se le pida la contraseña.
- 1 Cuando cambie el modo de un dispositivo a "enable", escriba `bob`.

Configuración de una contraseña inicial SSH

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

```
console(config)# aaa authentication login defaultline
```

```
console(config)# aaa authentication enable defaultline
```

```
console(config)# line ssh
```

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

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

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

- 1 Cuando se conecte inicialmente a un dispositivo a través de una sesión SSH, escriba `jones` cuando se le pida la contraseña.
- 1 Cuando cambie el modo de un dispositivo a "enable", escriba `jones`.

Configuración de una contraseña inicial HTTP

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

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

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


Configuración de una contraseña inicial HTTPS

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

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

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


Escriba los comandos siguientes una vez cuando configure la utilización de una sesión de terminal, Telnet o SSH para poder utilizar una sesión HTTPS.

 **NOTA:** En el navegador web habilite SSL 2.0 o posterior para que el contenido de la página se pueda visualizar.

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

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

Al habilitar inicialmente una sesión HTTP o HTTPS, escriba `admin` como nombre de usuario y `user1` como contraseña.

 **NOTA:** Los servicios http y https requieren el acceso de nivel 15 y conectarse directamente al acceso de nivel de configuración.

Procedimientos de inicio

Procedimientos del menú de inicio

Los procedimientos que se invocan en el menú Startup (Inicio) cubren la descarga de software, el manejo de la memoria flash y la recuperación de la contraseña. Los procedimientos de diagnóstico sólo los debe utilizar el personal de asistencia técnica y no se explican en este documento.

Se puede entrar en el menú Startup (Inicio) cuando se inicia el dispositivo. Para ello el usuario tiene que realizar una acción inmediatamente después de la prueba POST.

Para entrar en el menú de Startup (Inicio):

1. Encienda el dispositivo y espere a que aparezca el mensaje de inicio automático.

```
*****
```

```
***** SYSTEM RESET *****
```

```
*****
```

```
----- Performing the Power-On Self Test (POST) -----
```

```
UART Channel Loopback Test.....PASS
```

```
Testing the System SDRAM.....PASS
```

```
Boot1 Checksum Test.....PASS
```

```
Boot2 Checksum Test.....PASS
```

```
Flash Image Validation Test.....PASS
```

```
BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28
```

```
Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.
```

```
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.
```

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

Preparing to decompress...

2. Cuando aparezca el mensaje de inicio automático, pulse <Intro> para ir al menú Startup (Inicio). Los procedimientos del menú Startup (Inicio) se pueden realizar utilizando el terminal ASCII o Windows HyperTerminal.

[1] Download Software

[2] Erase Flash File

[3] Password Recovery Procedure


[4] Enter Diagnostic Mode

[5] Set Terminal Baud-Rate

[6] Back (Atrás)

Enter your choice or press 'ESC' to exit

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

 **NOTA:** Cuando se selecciona una opción del menú Startup (Inicio), hay que tener en cuenta el tiempo de espera: si no efectúa ninguna selección en los 35 segundos siguientes (valor predeterminado), se agota el tiempo de espera del dispositivo. Este valor predeterminado se puede cambiar mediante la CLI.


Descarga de software


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

1. Desde el menú Startup (Inicio), pulse [1]. Aparecerá la siguiente indicación:

Downloading code using XMODEM

2. Si utiliza HyperTerminal, haga clic en **Transfer** (Transferir) en la barra de menús de HyperTerminal.
3. En el campo **Filename** (Nombre de archivo), introduzca la ruta de acceso del archivo que se va a descargar.
4. Asegúrese de que el protocolo Xmodem esté seleccionado en el campo **Protocol** (Protocolo).
5. Pulse **Send** (Enviar). El software se descarga.

 **NOTA:** Una vez descargado el software, el dispositivo se reinicia automáticamente.

 **NOTA:** El tiempo que tarda la descarga varía en función de la herramienta utilizada.

Borrar archivo de memoria flash

En algunos casos, la configuración del dispositivo debe borrarse. Si se borra, se deben reconfigurar todos los parámetros configurados a través de CLI, EWS o SNMP.

Borrado de la configuración del dispositivo

1. En el menú Startup (Inicio) pulse [2] en los 2 segundos posteriores para borrar el archivo de memoria flash. Aparece el siguiente mensaje:

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

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

2. Pulse Y. Aparecerá el siguiente mensaje.

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

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

```
***** Press Enter To Continue *****
```

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


Recuperación de contraseña

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

Para recuperar una contraseña perdida para el terminal local solamente:

1. En el menú Startup (Inicio), escriba 3 y pulse <Intro>.

La contraseña se suprime.

 **NOTA:** Para garantizar la seguridad del dispositivo, reconfigure las contraseñas para los métodos de administración aplicables.

Descarga del software a través de un servidor TFTP

Esta sección contiene instrucciones para descargar software del dispositivo (imágenes del sistema y inicio) a través de un servidor TFTP. El servidor TFTP se debe configurar antes de comenzar a descargar el software.

Descarga de la imagen del sistema

El dispositivo se inicia y se activa tras descomprimir la imagen del sistema del área de la memoria flash en la que se ha almacenado una copia de la imagen del sistema. Cuando se descarga una nueva imagen, se guarda en el área asignada para la otra copia de la imagen del sistema.

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

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

1. Compruebe que se haya configurado una dirección IP en uno de los puertos de dispositivo y que un comando ping ejecutado contra un servidor TFTP obtenga una respuesta satisfactoria.
2. Asegúrese de que el archivo que se va a descargar se guarde en el servidor TFTP (el archivo `zos`).
3. Escriba `show version` para comprobar qué versión de software se ejecuta actualmente en el dispositivo. A continuación se muestra un ejemplo de la información que aparece:

```
console# show version
```


[Regresar a la página de contenido](#)

Glosario

Guía del usuario del sistema Dell™ PowerConnect™ 5324

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [L](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#)

Este glosario contiene palabras técnicas clave de interés.

A

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

Aprendizaje de direcciones MAC

El aprendizaje de direcciones MAC caracteriza un puente de aprendizaje, en el que se registra la dirección MAC de origen del paquete. Los paquetes destinados para dicha dirección se reenvían sólo a la interfaz de puente en la que se encuentre ubicada dicha dirección. Los paquetes que se dirijan a direcciones desconocidas se reenvían a cada interfaz del puente. El aprendizaje de direcciones MAC minimiza el tráfico en las LAN que estén conectadas.

Archivo de configuración en ejecución

Contiene todos los comandos del archivo de inicio además de todos los comandos introducidos durante la sesión actual. Después de apagar o reiniciar el dispositivo, se pierden todos los comandos almacenados en el archivo de configuración en ejecución.

Archivo de imagen

Las imágenes del sistema se guardan en dos sectores Flash denominados imágenes (Imagen 1 e Imagen 2). La imagen activa almacena la copia activa, mientras que la otra imagen almacena una segunda copia.

Archivos de configuración de copia de seguridad

Contiene una copia de seguridad de la configuración del dispositivo. El archivo de copia de seguridad cambia cuando los archivos de configuración en ejecución o inicio se copian en el archivo de copia de seguridad.

ARP

Protocolo de resolución de direcciones. Protocolo TCP/IP que convierte direcciones IP en direcciones físicas.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Asset Tag (Etiqueta de propiedad)

Especifica la referencia de dispositivo definida por el usuario.

B

Baudio

El número de elementos de señalización transmitidos cada segundo.

BootP

Protocolo de inicio del sistema operativo Permite a una estación de trabajo descubrir su dirección IP, una dirección IP de un servidor BootP en una red, o un archivo de configuración cargado en el arranque de un dispositivo.

BPDU

Unidad de datos de protocolo de puente. Proporciona información de puente en formato de mensaje. Las BPDU se envían a través de la información del dispositivo en una configuración de árbol extensible. Los paquetes BPDU contienen información sobre puertos, direcciones, prioridades y costes de reenvío.

C

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Captura

Mensaje enviado por el protocolo SNMP que indica que se ha producido un evento del sistema.

CDB

Base de datos de configuración. Archivo que contiene información de configuración de un dispositivo.

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.

Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

CLI

Interfaz de línea de comandos. Conjunto de comandos de línea utilizados para configurar el sistema. Para obtener más información sobre cómo usar la CLI, consulte el apartado Utilización de la CLI.

Ciente DHCP

Sistema principal de Internet que utiliza DHCP para obtener parámetros de configuración como, por ejemplo, una dirección de red.

Cambio rápido

El cambio rápido ocurre cuando el estado de una interfaz cambia constantemente. Por ejemplo, un puerto STP cambia constantemente entre las acciones de escuchar, aprender o reenviar. Esto puede provocar la pérdida de tráfico.

Compensación de carga

Permite la distribución uniforme de datos o paquetes de proceso a través de los recursos de red disponibles. Por ejemplo, la compensación de carga puede distribuir los paquetes entrantes de forma uniforme a todos los servidores, o redirigirlos al siguiente servidor disponible.

Comunidades

Especifica un grupo de usuarios que retiene los mismos derechos de acceso del sistema.

Configuración de iniciación

Retiene la configuración de dispositivo exacta cuando se apaga o reanuncia el dispositivo.

Conmutador

Filtra y reenvía paquetes entre segmentos de LAN. Los conmutadores admiten cualquier tipo de protocolo de paquetes.

Consulta

Extrae información de una base de datos y presenta la información para poder utilizarla.

Contrapresión

Mecanismo utilizado con la modalidad dúplex medio que permite a un puerto no recibir un mensaje.

Control de flujo

Permite que dispositivos de velocidad inferior se comuniquen con los de velocidades superiores; es decir, el dispositivo de velocidad superior se abstiene de enviar paquetes.

CPU

Unidad central de procesamiento. La parte de un equipo que procesa la información. Las CPU constan de una unidad de control y una ALU.

D

Difusión

Método de transmisión de paquetes a todos los puertos de una red.

Difusión única

Forma de encaminamiento que transmite un paquete a un usuario.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Dominio

Grupo de equipos y dispositivos de una red que se agrupan con reglas y procedimientos comunes.

Dominio de difusión

Conjuntos de dispositivos que reciben tramas de difusión procedentes de cualquier dispositivo dentro de un conjunto designado. Los enrutadores vinculan dominios de difusión, ya que los enrutadores no reenvían tramas de difusión.

Duplicación de puertos

Supervisa y duplica el tráfico de la red reenviando copias de los paquetes entrantes y salientes de un puerto a un puerto de supervisión.

Para obtener información sobre la duplicación de puertos, consulte el apartado **Definición de sesiones de duplicación de puertos**.

E

Enlazamiento

Agregación de conexión. Optimiza la utilización de los puertos al conectar un grupo de puertos para que formen un único tronco (grupos agregados).

Enrutador

Dispositivo que conecta redes separadas. Los enrutadores reenvían paquetes entre dos o más redes. Los enrutadores funcionan al nivel de la Capa 3.

Ethernet

Ethernet se estandariza como IEEE 802.3. Ethernet es el estándar de LAN implementado más común. Admite velocidades de transferencia de datos de Mbps, compatibles con velocidades de 10, 100 ó 1000 Mbps.

EWS

Servidor web incorporado. Proporciona gestión de dispositivos a través del navegador web estándar. Los servidores web incorporados se utilizan además de una CLI o NMS, o en su lugar.

F

FFT

Tabla de avance rápido. Proporciona información sobre el reenvío de rutas. Si un paquete llega a un dispositivo con una ruta conocida, el paquete se reenvía a través de una ruta que aparezca en la FFT. Si no existe ninguna ruta conocida, la CPU reenvía el paquete y actualiza la FFT.

FIFO

Primeras entradas, primeras salidas. Proceso de colocación en cola en el que el primer paquete de la cola es el primer paquete que sale del paquete.

Fragmento

Paquetes Ethernet de tamaño inferior a los 576 bits.

G

GARP

Protocolo de registro de atributos general. Registra estaciones cliente en un dominio multidifusión.

Gigabit Ethernet

Gigabit Ethernet transmite a 1000 Mbps y es compatible con los estándares Ethernet 10/100 Mbps existentes.

GVRP

Protocolo de registro VLAN GARP. Registra estaciones cliente en una VLAN.

H

HOL

Cabecera de línea. Los paquetes se colocan en la cola. Los paquetes situados al principio de la línea se reenvían antes que los paquetes situados al final de la línea.

HTTP

Protocolo de transferencia de hipertexto. Transmite documentos HTML entre servidores y clientes de internet.

I

IC

Circuito integrado. Los circuitos integrados son pequeños dispositivos eléctricos compuestos de material semiconductor.

ICMP

Protocolo de mensajes de control de Internet. Permite a la puerta de enlace o al sistema principal de destino comunicarse con un sistema principal de origen; por ejemplo, para informar sobre un error de proceso.

IEEE

Institute of Electrical and Electronics Engineers. Organización de ingeniería que desarrolla estándares de comunicación y redes.

IEEE 802.1d

Utilizado en el protocolo de árbol extensible, el estándar IEEE 802.1d es compatible con el puente de MAC para evitar bucles de red.

IEEE 802.1p

Prioriza el tráfico de red en la subcapa de vínculo de datos/MAC.

IEEE 802.1Q

Define el funcionamiento de los puentes VLAN que permite definir, hacer funcionar y administrar VLAN dentro de las infraestructuras de LAN con puente.

IP

Internet Protocol (Protocolo de Internet). Especifica el formato de los paquetes y su método de direccionamiento. El protocolo IP direcciona los paquetes y los reenvía al puerto correcto.

IPX

IPX (Internetwork Packet eXchange). Transmite comunicaciones sin conexión.

L

LAG

Grupo agregado de conexiones. Agrega puertos o VLAN en un único puerto virtual o VLAN.

Para obtener más información sobre los LAG, consulte el apartado **Definición de la pertenencia a LAG**.

LAN

Redes de área local. Red dispuesta en una única habitación, edificio, campus u otra área geográfica limitada.

M

Máscara comodín

Especifica qué bits de dirección IP utilizan y cuáles se ignoran. Una máscara comodín de 255.255.255.255 indica que ningún bit es importante. Un comodín de 0.0.0.0 indica que todos los bits son importantes.

Por ejemplo, si la dirección IP de destino es 149.36.184.198 y la máscara comodín es 255.36.184.00, los primeros dos bits de la dirección IP se ignoran, mientras que se utilizan los dos últimos.

Máscara de subred

Se utiliza para enmascarar toda o parte de la dirección IP que se utiliza en una dirección de subred.

Mejor esfuerzo

El tráfico se asigna a la cola de prioridad más baja, y no se garantiza la entrega de los paquetes.

Modo de acceso

Especifica el método por el cual se otorga al usuario acceso al sistema.

Modo dúplex

Permite la transmisión y la recepción simultánea de datos. Existen dos tipos diferentes de modo dúplex:

- 1 **Modo dúplex completo** — Permite la comunicación bisíncrona, por ejemplo, un teléfono. Las dos partes pueden transmitir información al mismo tiempo.
- 1 **Modo dúplex medio** — Permite la comunicación asíncrona, por ejemplo, un "walkie-talkie". Sólo una parte puede transmitir datos cada vez.

MD5

Síntesis del mensaje 5. Algoritmo que genera un hash de 128 bits. MD5 es una variedad de MD4, pero con mayor seguridad. MD5 verifica la integridad de la comunicación y autentica su origen.

MDI

Interfaz dependiente de los soportes. Cable utilizado para las estaciones finales.

MDIX

Interfaz dependiente de los soportes con cable cruzado (MDIX). Cable que se utiliza con los concentradores y conmutadores.

MIB

Base de datos de información de administración. Las MIB contienen información que describe aspectos específicos de los componentes de la red.

Multicast

Transmite copias de un único paquete a varios puertos.

N

Negociación automática

Permite establecer puertos Ethernet 10/100 Mbps o 10/100/1000 Mbps para las características siguientes:

- 1 Modo dúplex/ dúplex medio
- 1 Control de flujo
- 1 Velocidad

NMS

Sistema de administración de redes. Interfaz que proporciona un método para administrar un sistema.

Nodo

Punto final de conexión de red o unión común para varias líneas de red. Los nodos pueden ser:

- 1 Procesadores
 - 1 Controladoras
 - 1 Estaciones de trabajo
-

O

OID

Identificador de objeto. SNMP lo utiliza para identificar objetos gestionados. En el paradigma de administración de redes Gestor/ Agente SNMP, cada objeto gestionado debe tener un OID que lo identifique.

P

Paquetes

Bloques de información para la transmisión en sistemas de conmutación de paquetes.

PDU

Unidad de datos de protocolo. Unidad de datos especificada en un protocolo de capas que consta de información de control de protocolo y datos de usuarios de la capa.

Perfiles de acceso

Permite a los administradores de red definir perfiles y reglas para acceder al dispositivo. El acceso a las funciones de gestión puede limitarse a grupos de usuarios, que se definen mediante los criterios siguientes:

- 1 Interfaces de entrada
- 1 Dirección IP de origen o subredes IP de origen

Perfiles de autenticación

Conjuntos de reglas que permiten el inicio de sesión y la autenticación de usuarios y aplicaciones.

PING

Sonda de paquetes Internet. Verifica si una dirección IP específica está disponible. Un paquete se envía a otra dirección IP y espera una respuesta.

Plano posterior

El BUS principal que lleva información en el dispositivo.

Protocolo

Conjunto de reglas que rige cómo los dispositivos intercambian información a través de las redes.

Protocolo de árbol extensible

Impide que se creen bucles en el tráfico de la red. El protocolo de árbol extensible (STP) proporciona topografía de árbol para cualquier disposición de puentes. STP proporciona una vía de comunicación entre las estaciones finales de una red, eliminando los bucles.

Puente

Dispositivo que conecta dos redes. Los puentes son específicos del hardware, aunque son independientes del protocolo. Los puentes funcionan en los niveles de la capa 1 y de la capa 2.

Puerto

Los puertos físicos proporcionan componentes de conexión que permiten a los microprocesadores comunicarse con los equipos periféricos.

Puerto de entrada

Puertos en los que se recibe el tráfico de la red.

Puertos combinados

Único puerto lógico con dos conexiones físicas, que incluye una conexión RJ-45 y una conexión SFP.

Puertos de entrada

Puertos desde los cuales se transmite el tráfico de la red.

Q

QoS

Calidad de servicio. QoS permite a los administradores de red decidir qué tráfico de red se reenvía y cómo se reenvía en función de las prioridades, tipos de aplicación y direcciones de origen y destino.

R

RADIUS

Servicio de usuario de acceso telefónico de autenticación remota. Método de autenticación de usuarios del sistema y de seguimiento del tiempo de conexión.

RMON

Supervisión remota. Proporciona la información de red que debe recopilarse de una única estación de trabajo.

RSTP

Protocolo de árbol extensible rápido. Detecta y utiliza topologías de red que permiten una convergencia más rápida del árbol extensible, sin crear bucles de reenvío.

S

Segmentación

Divide las LAN en segmentos de LAN separados para establecer puentes y encaminamientos. La segmentación elimina las limitaciones de la amplitud de banda de la LAN.

Servidor

Equipo central que proporciona servicios a otros equipos de una red. Entre los servicios se incluyen el almacenamiento de archivos y el acceso a aplicaciones.

Sistema final

Dispositivo de un usuario final en una red.

Sistema principal

Equipo que actúa como fuente de información o de los servicios que se ofrecen a otros equipos.

SNMP

Simple Network Management Protocol (Protocolo simple de administración de redes). Gestiona las LAN. El software basado en SNMP se comunica con los dispositivos que disponen de agentes SNMP incorporados. Los agentes SNMP recopilan información de la actividad de la red y del estado del dispositivo y la envían de vuelta a una estación de trabajo.

SNTP

Protocolo simple de tiempo de red. El protocolo SNTP garantiza una sincronización precisa del tiempo del reloj del conmutador de la red en milisegundos.

SoC

Sistema en un chip. ASIC que contiene un sistema completo. Por ejemplo, una aplicación SoC de telecomunicaciones puede contener un microprocesador, un procesador de señales digitales, RAM y ROM.

SSH

Shell seguro. Inicia una sesión en un equipo remoto a través de una red, ejecuta comandos y transfiere archivos de un equipo a otro.

Subred

Subred. Las subredes son partes de una red que comparten un componente de dirección común. En redes TCP/IP, los dispositivos que comparten un prefijo forman parte de la misma subred. Por ejemplo, todos los dispositivos con un prefijo de 157.100.100.100 forman parte de la misma subred.

T

TCP/IP

Protocolo de control de transmisiones. Permite a dos sistemas principales comunicarse e intercambiar corrientes de datos. El TCP garantiza la entrega de los paquetes y que éstos se transmitan y reciban en el orden en que se envían.

Telnet

Protocolo de emulación de terminal. Permite a los usuarios del sistema iniciar una sesión y utilizar los recursos de redes remotas.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Tormentas de difusión

Cantidad excesiva de mensajes transmitidos simultáneamente a través de una red mediante un único puerto. Las respuestas a mensajes reenviados se cargan en la red, lo que provoca una sobrecarga en los recursos de ésta o que se agote el tiempo de espera.

Para obtener información sobre las tormentas de difusión, consulte el apartado ["Definición de los parámetros del LAG"](#).

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

U

UDP

Protocolo de datos de usuario. Transmite paquetes pero no garantiza su entrega.

V

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

- 1 Ethernet 10 Mbps
- 1 Fast Ethernet 100 Mbps
- 1 Gigabit Ethernet 1000 Mbps

Versión de arranque

La versión de arranque.

VLAN

Redes de área local virtual. Subgrupos lógicos de una red de área local (LAN) creados utilizando software en lugar de una definición de solución de hardware.

VLAN agregada

Agrupar varias VLAN en una sola VLAN agregada. La agregación de VLAN permite a los enrutadores responder a las peticiones ARP de nodos ubicados en subVLAN distintas que pertenezcan a la misma superVLAN. Los enrutadores responden con su dirección MAC.

W

WAN

Redes de área extensa. Redes que cubren un área geográfica grande.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Descripción del hardware

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Configuraciones de los puertos del dispositivo](#)
- [Dimensiones físicas](#)
- [Definiciones de los LED](#)
- [Componentes de hardware](#)

Configuraciones de los puertos del dispositivo

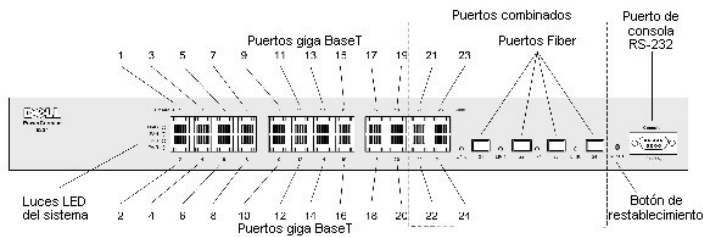
Descripción de los puertos del panel anterior del dispositivo PowerConnect 5324

El dispositivo PowerConnect 5324 se configura con los siguientes puertos:

- 1 **24 puertos de cobre:** puertos RJ-45 designados como puertos Gigabit Ethernet 10/100/1000 BaseT
- 1 **4 puertos de fibra:** designados como puertos Gigabit
- 1 **Puerto de terminal:** puerto de consola RS-232

En la siguiente ilustración se muestra el panel anterior del dispositivo PowerConnect 5324.

Ilustración 2-3. Panel anterior del dispositivo PowerConnect 5324



El panel anterior contiene los puertos 1-24, que son puertos RJ-45 de cobre, designados como 10/100/1000 Mbps y que son compatibles con los modos de dúplex medio y completo. Hay cuatro puertos de fibra SFP designados como puertos combinados 21-24. Un puerto combinado es un único puerto lógico con dos conexiones físicas. No puede haber más de una conexión física activa a la vez, de modo que los puertos de cobre o los equivalentes puertos de fibra 21-24 pueden estar activos, pero no simultáneamente. En la fila superior, los puertos se indican mediante números impares del 1 al 23 y en la fila inferior, los puertos se indican mediante números pares del 2 al 24.

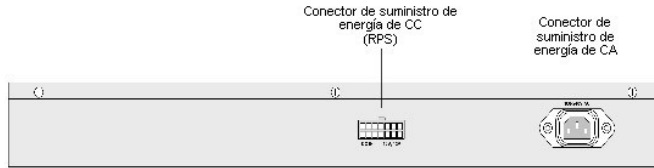
En el panel anterior hay un puerto de consola RS-232, todos los LED del dispositivo y un botón de restablecimiento que se utiliza para restablecer el dispositivo de manera manual.

El dispositivo detecta automáticamente si el cable conectado a un puerto RJ-45 es un cable cruzado o directo, y funciona de las dos maneras.

Descripción de los puertos del panel posterior del dispositivo PowerConnect

El panel posterior del dispositivo contiene los conectores de alimentación, tal como se muestra en la [Ilustración 2-4](#).

Ilustración 2-4. Panel posterior del dispositivo



En el panel posterior del dispositivo hay dos conectores para los suministros de energía. Hay un conector para el suministro de energía de CA para uso general que se puede conectar a fuentes de alimentación de 110 V o 220 V.

El conector para el suministro de energía de CC sirve para conectar un suministro de energía redundante (RPS) de modo que se active automáticamente en caso de que se produzca una interrupción del suministro de energía de CA.

Puertos del dispositivo

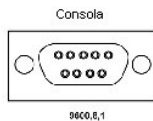
Puertos SFP

El puerto SFP (Small Form Factor Pluggable) es un transceptor modular óptico de intercambio dinámico que ofrece una gran velocidad y grado de compresión, que se designa como 1000Base-SX o LX.

Puerto de consola RS-232

Un conector DB-9 para una conexión de terminal serie que se utiliza para depurar errores, descargar software, etc. La velocidad en baudios predeterminada es de 9600 bps. La velocidad en baudios se puede configurar de 2400 bps hasta 38400 bps.

Ilustración 2-5. Puerto de la consola



Puertos combinados

Un puerto combinado es un único puerto lógico con dos conexiones físicas:

- 1 Una conexión RJ-45 para una conexión de cables de cobre de par trenzado
- 1 Una conexión SFP para varios módulos basados en fibra

No se pueden utilizar las dos conexiones físicas de un puerto combinado a la vez. Las funciones de los puertos y los controles de puerto disponibles vienen determinados por el tipo de conexión física utilizada.

El sistema detecta automáticamente los medios utilizados en un puerto combinado, y utiliza esta información en todas las operaciones e interfaces de control.

Si se dispone de un puerto RJ-45 y otro SFP, y se inserta un conector en el puerto SFP, el puerto SFP estará activo, a no ser que se inserte el conector de cobre del puerto Base-T del mismo número y tenga un vínculo.

El sistema puede pasar del puerto RJ-45 al SFP (o viceversa) sin tener que reiniciar o restablecer el sistema.

Dimensiones físicas

El dispositivo tiene las siguientes dimensiones físicas:

- 1 Altura: 44 mm (1,73 pulgadas)
 - 1 Anchura: 440 mm (17,32 pulgadas)
 - 1 Profundidad: 255 mm (10,03 pulgadas)
-

Definiciones de los LED

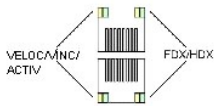
El panel anterior contiene diodos emisores de luz (LED) que indican el estado de las fuentes de alimentación, ventiladores y diagnósticos del sistema.

LED de los puertos

LED del puerto 10/100/1000 Base-T

Cada puerto 10/100/1000 Base-T tiene dos LED. En el LED de la izquierda se indica la velocidad, vínculo y actividad y en el LED de la derecha se indica el modo dúplex.

Ilustración 2-6. LED del puerto RJ-45 10/100/1000 BaseT basado en cobre



En la siguiente tabla se describen las indicaciones del LED de RJ-45:

Tabla 2-1. Indicaciones del LED del puerto RJ-45 10/100/1000 BaseT basado en cobre

LED	Color	Descripción
LED izquierdo	Verde estático	El puerto está vinculado a 1000 Mbps.
	Verde parpadeante	El puerto transmite o recibe datos a 1000 Mbps.
	Naranja estático	El puerto está vinculado a 10 ó 100 Mbps.
	Naranja parpadeante	El puerto transmite o recibe datos a 10 ó 100 Mbps.
	APAGADO	El puerto funciona en modo de dúplex medio.

LED de SFP

Cada uno de los puertos SFP tienen un LED que se indica mediante las letras LNK.

Ilustración 2-7.



LED de puerto SFP

En la siguiente tabla se describen las indicaciones del LED de puerto SFP:

Tabla 2-2. Indicaciones del LED de puerto SFP

LED	Color	Descripción
SFP	Verde estático	El puerto está actualmente en funcionamiento.
	Verde parpadeante	Actualmente el puerto transmite o recibe datos.
	APAGADO	Actualmente el puerto no funciona.

Cuando el puerto SFP está conectado, el LED de dúplex situado en el correspondiente puerto combinado de cobre es verde.

LED del sistema

Los LED del sistema, ubicados en la parte izquierda del panel anterior, proporcionan información sobre las fuentes de alimentación, ventiladores, condiciones térmicas y diagnósticos. En la [Ilustración 2-8](#) se muestran los LED del sistema.

Ilustración 2-8. LED del sistema

DIAG 
 FAN 
 RPS 
 PWR 

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

Tabla 2-3. Indicaciones de los LED del sistema

LED	Color	Descripción
Diagnósticos (DIAG)	Verde parpadeante	Actualmente el sistema ejecuta una prueba de diagnóstico.
	Verde estático	El sistema ha pasado la prueba de diagnóstico.
	Rojo estático	El sistema no ha pasado la prueba de diagnóstico.
Ventilador (FAN)	Verde estático	Los ventiladores del dispositivo funcionan normalmente.
	Rojo estático	Uno o varios ventiladores no funcionan.
Suministro de energía redundante (RPS)	Verde estático	Actualmente el suministro de energía redundante funciona.
	Rojo estático	El suministro de energía redundante no funciona.
	APAGADO	Actualmente el suministro de energía redundante no funciona.
Suministro de energía principal (PWR)	Verde estático	Actualmente el suministro de energía principal funciona normalmente.
	APAGADO	Actualmente el suministro de energía principal no funciona.
	Rojo	Se ha producido un fallo en el suministro de energía principal

Componentes de hardware

Fuentes de alimentación

El dispositivo tiene una unidad interna de suministro de energía (unidad de CA) y un conector para conectar el dispositivo a una unidad externa de suministro de energía (unidad de CC). La unidad externa ofrece redundancia y se denomina unidad de RPS. Para encender el dispositivo, sólo se necesita un suministro de energía. El funcionamiento con las dos unidades de suministro de energía se regula mediante el reparto de la carga.

En el reparto de la carga es donde los requisitos de alimentación del dispositivo se dividen entre los dos suministros de energía. Si un suministro de energía sufre una interrupción, el segundo suministro de energía sigue proporcionando alimentación a todo el dispositivo.

Los LED del suministro de energía indican el estado del suministro de energía. Para obtener más información sobre los LED, consulte el apartado ["Definiciones de los LED"](#).

Unidad de suministro de energía de CA

La unidad de suministro de energía de CA convierte 220/110 VCA estándar a 50/60 Hz en 5 VCC a 5A, 12 VCC en 3A. La unidad detecta automáticamente la especificación de voltaje disponible (110 ó 220 V) y no es necesario ninguna configuración.

La unidad de suministro de energía de CA utiliza un conector estándar de 220/110 VCA. El indicador LED se encuentra en el panel anterior e indica si la unidad de CA está conectada.

Unidad de suministro de energía de CC

Una unidad externa de suministro de energía de CC se utiliza como una unidad de suministro de energía redundante. El funcionamiento es posible con alimentación suministrada sólo desde esta unidad. Se utiliza un tipo de conector RPS600. No es necesario realizar ningún tipo de configuración. El indicador LED se encuentra en el panel anterior e indica si la unidad de CC está conectada.

Cuando el dispositivo está conectado a una fuente de energía diferente, las posibilidades de que se produzca un error en el caso de que haya una interrupción de la alimentación disminuyen.

Botón de restablecimiento

El botón de restablecimiento, situado en el panel anterior, restablece el dispositivo de manera manual.

Sistema de ventilación

El dispositivo utiliza un sistema de ventilador para enfriarse. El estado operativo de los ventiladores se puede comprobar observando los LED que indican si hay algún ventilador defectuoso. Para obtener información, consulte el apartado ["Definiciones de los LED"](#).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Instalación del dispositivo PowerConnect

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Precauciones de instalación](#)
- [Requisitos de emplazamiento](#)
- [Desembalaje](#)
- [Montaje del dispositivo](#)
- [Conexión del dispositivo](#)
- [Información sobre la asignación de patas, los cables y las conexiones de los puertos](#)
- [Configuración predeterminada del puerto](#)

Esta sección contiene información sobre el desembalaje, la ubicación, la instalación y las conexiones de cable del dispositivo.

Precauciones de instalación

PRECAUCIÓN: Antes de realizar alguno de los siguientes procedimientos, lea y siga las instrucciones de seguridad que se encuentran en la Guía de información del sistema incluida en la documentación de Dell.

PRECAUCIÓN: Siga los siguientes puntos antes de realizar los procedimientos de esta sección:

- 1 Asegúrese de que el estante o el gabinete que cubre el dispositivo esté bien fijado para evitar que sea inestable o se caiga.
 - 1 Asegúrese de que los circuitos de la fuente de energía estén bien conectados a tierra.
 - 1 Observe y siga las marcas de servicio. No manipule ningún dispositivo excepto como se explica en la documentación del sistema. Si abre o extrae cubiertas que están marcadas con un rayo dentro de un símbolo triangular puede suponer un riesgo de descarga eléctrica. Estos componentes sólo deben ser manipulados por personal cualificado del servicio técnico.
 - 1 Asegúrese de que el cable de alimentación, el cable de extensión, y, o también, el enchufe no estén dañados.
 - 1 Asegúrese de que el dispositivo no entre en contacto con el agua.
 - 1 Asegúrese de que el dispositivo no esté expuesto a radiadores y, o también, a fuentes de calor.
 - 1 Asegúrese de que las aberturas de enfriamiento no estén bloqueadas.
 - 1 No introduzca objetos extraños en el dispositivo, ya que se puede producir un incendio o una descarga eléctrica.
 - 1 Utilice el dispositivo únicamente con otros componentes aprobados.
 - 1 Deje enfriar el dispositivo antes de desmontar las cubiertas o tocar los componentes internos.
 - 1 Asegúrese de que el dispositivo no sobrecargue los circuitos de alimentación, los cables y la protección contra sobrecorriente. Para determinar si existe la posibilidad de sobrecargar los circuitos de alimentación, sume la intensidad de régimen de todos los conmutadores instalados en el mismo circuito que el dispositivo. Compare este total con el límite de intensidad del circuito.
 - 1 No instale el dispositivo en un entorno en el que la temperatura ambiente de funcionamiento pueda superar los 40°C (122°F).
 - 1 Asegúrese de no restringir el flujo de aire en la parte delantera, lateral y posterior del dispositivo.
-

Requisitos de emplazamiento

El dispositivo se puede montar en un estante estándar de 19 pulgadas o se puede colocar sobre una mesa. Antes de instalar el dispositivo, compruebe que la ubicación elegida para la instalación cumple los requisitos de emplazamiento:

- 1 **General:** asegúrese de que el suministro de energía esté correctamente instalado.
- 1 **Alimentación:** el dispositivo está instalado en un radio de 1,5 m (5 pies) de una toma de corriente de 220/110 VCA y 50/60 Hz que esté conectada a tierra y a la que se pueda acceder fácilmente.
- 1 **Distancia de separación:** hay una distancia de separación adecuada en la parte anterior que permite que el operador pueda acceder fácilmente al sistema. Deje una distancia de separación entre los cables, las conexiones de alimentación y la ventilación.
- 1 **Conexión de cables:** la conexión de cables se dispone de tal manera para poder evitar fuentes de ruido eléctrico como transmisores de radio, amplificadores de difusión, líneas de alimentación y accesorios de iluminación fluorescente.
- 1 **Requisitos ambientales:** el intervalo de temperatura ambiente de funcionamiento de la unidad es de 0 a 40°C (de 32 a 104°F) con una humedad relativa de 10% a 90%, sin condensación. Compruebe que no puede entrar ni agua ni humedad en la cubierta de la unidad.

Desembalaje


Contenido del paquete


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

- 1 El dispositivo
- 1 Un cable de alimentación de CA
- 1 Cable cruzado RS-232
- 1 Almohadillas de goma autoadhesivas
- 1 Kits de montaje en estante para instalación en estante
- 1 CD de documentación

Desembalaje del dispositivo

Para desembalar el dispositivo:

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

 **NOTA:** No se suministra ninguna correa contra descargas electrostáticas, aunque se recomienda llevar una para realizar el siguiente procedimiento.

1. Coloque el contenedor en una superficie plana y limpia, y corte todas las correas que fijan el contenedor.
2. Abra el contenedor o extraiga la parte superior del mismo.
3. Con cuidado, extraiga el dispositivo del contenedor y colóquelo en una superficie fija y limpia.
4. Extraiga todos los materiales de embalaje.
5. Examine el dispositivo para comprobar que no haya sufrido daños. Informe inmediatamente de cualquier daño.

Montaje del dispositivo


Descripción general

Los conectores de alimentación para el dispositivo se encuentran en el panel posterior. Se recomienda conectar un suministro de energía redundante (SAI), aunque es opcional. El conector de CC del SAI está situado en el panel posterior del dispositivo.

Montaje del sistema

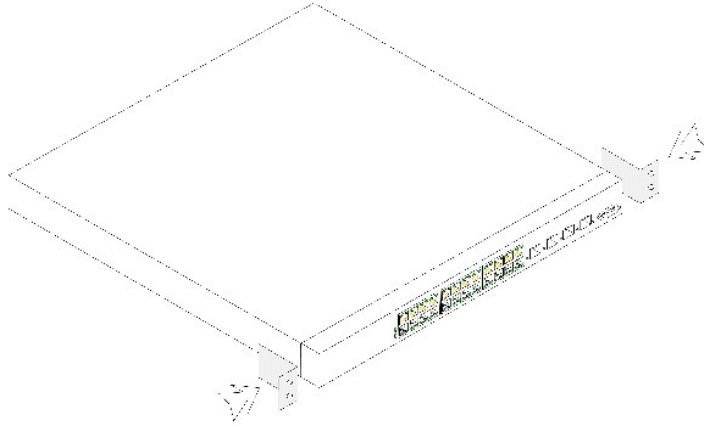
Instalación del estante del dispositivo

 **PRECAUCIÓN:** Desconecte todos los cables de la unidad antes de montar el dispositivo en un estante o gabinete.

 **PRECAUCIÓN:** Cuando se montan varios dispositivos en un estante, se deben montar de abajo arriba.

1. Coloque el soporte de montaje en estante que se proporciona en un lateral del dispositivo y asegúrese de que los agujeros de montaje del dispositivo coinciden con los agujeros de montaje del soporte de montaje en estante. En la [Ilustración 3-9](#) se muestra dónde hay que montar los soportes.

Ilustración 3-9. Soportes de montaje del estante de conexión



2. Inserte los tornillos suministrados en los agujeros de montaje en estante y apriételos con un destornillador.
3. Repita el proceso para el soporte de montaje en estante en el otro lado del dispositivo.
4. Inserte la unidad en el estante de 19 pulgadas y asegúrese de que los agujeros de montaje en estante del dispositivo coinciden con el agujero de montaje del estante.
5. Fije la unidad al estante con los tornillos del estante (no se proporcionan). Apriete el par inferior de tornillos antes que el superior. De esta manera, se asegura de que el peso de la unidad se distribuye uniformemente durante la instalación. Asegúrese de que los agujeros de ventilación no están obstruidos.

Instalación del dispositivo sin un estante

El dispositivo debe instalarse en una superficie plana si no está instalado en un estante. La superficie debe poder aguantar el peso del dispositivo y de los cables del mismo.

1. Instale las patas de goma que se proporcionan con el dispositivo.
2. Coloque el dispositivo en una superficie plana y deje 2 pulgadas (5,08 cm) de separación a ambos lados y 5 pulgadas (12,7 cm) en la parte posterior.
3. Asegúrese de que el dispositivo está correctamente ventilado.

Conexión del dispositivo

Para configurar el dispositivo, éste debe estar conectado a un terminal.

Conexión del dispositivo a un terminal

El dispositivo dispone de un puerto de consola para conectarlo a un sistema de sobremesa terminal que ejecute software de emulación de terminal para poder supervisar y configurarlo. El conector del puerto de la consola es un conector DB-9 macho, instalado como un conector DTE (Data Terminal Equipment [Equipo terminal de datos]).

Para utilizar el puerto de la consola, se necesita lo siguiente:

1. Un terminal compatible con VT100 o bien un sistema de sobremesa o portátil con un puerto serie y que ejecuta el software de emulación de terminal VT100.
1. Un cable cruzado RS-232 con un conector DB-9 hembra para el puerto de la consola y el conector adecuado para el terminal.

Para conectar un terminal al puerto de la consola del dispositivo, realice los siguientes pasos:

1. Conecte un cable cruzado RS-232 al terminal que ejecuta el software de emulación de terminal VT100.
2. Asegúrese de que el software de emulación de terminal se configura de la manera siguiente:
 - a. Seleccione el puerto serie adecuado (puerto serie 1 o puerto serie 2) para conectarlo a la consola.

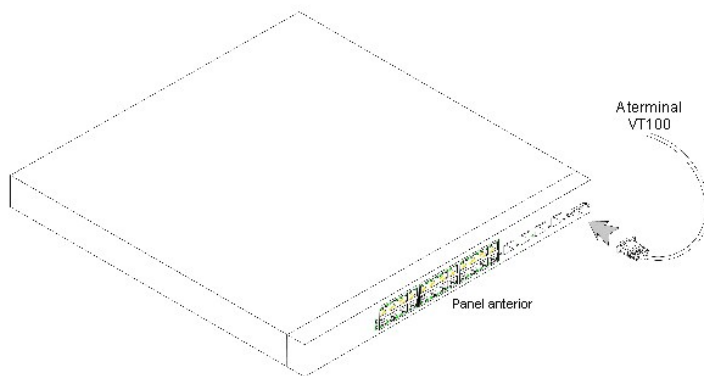
- b. Establezca la velocidad de los de datos en 9600 baudios.
- c. Establezca el formato de los datos en 8 bits de datos, 1 bit de parada y ninguna paridad.
- d. Establezca el control de flujo en ninguno.
- e. En **Properties** (Propiedades), seleccione el modo **VT100 for Emulation** (VT100 para emulación).
- f. Seleccione **Terminal keys** (Teclas de terminal) para las teclas **Function** (Función), **Arrow** (Flecha) y **Ctrl**. Asegúrese de que configura **Terminal keys** (Teclas de terminal) (no **Windows keys** [Teclas de Windows]).

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

3. Conecte el conector hembra del cable cruzado RS-232 directamente al puerto de la consola del dispositivo y apriete los tornillos cautivos de retención.

El puerto de la consola del dispositivo se encuentra en el panel anterior.

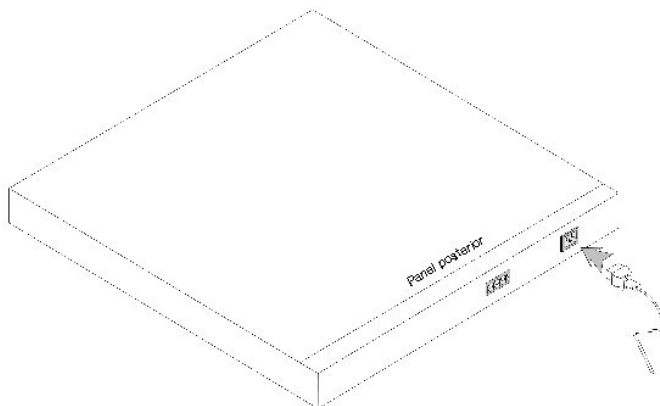
Ilustración 3-10. Conexión con el puerto de la consola del dispositivo PowerConnect 5324



Conexión de un dispositivo a un suministro de energía

1. Mediante un cable de alimentación estándar de 5 pies (1,5 m) conectado a tierra de manera segura, conecte el cable de alimentación al conector de CA que se encuentra en el panel posterior.
2. Conecte el cable de alimentación a un enchufe de corriente alterna.

Ilustración 3-11. Conexión con el conector de alimentación del dispositivo



Confirme que el dispositivo se ha conectado y funciona correctamente; para ello, examine los LED del panel anterior.

Información sobre las patas, los cables y las conexiones de los puertos

En esta sección se explican las interfaces físicas del dispositivo y también se proporciona información sobre las conexiones de los puertos. Los tipos de conectores, los puertos y los cables se resumen en la tabla Puertos, conectores y cables. Los diagnósticos de los transceptores ópticos y los cables de cobre son compatibles.

Conexiones RJ-45 para puertos 10/100/1000BaseT

Los puertos 10/100/1000BaseT son puertos de par trenzado de cobre.

Con objeto de establecer un vínculo para los puertos de par trenzado, el par de transmisión situado en un extremo del cable se tiene que conectar al par de recepción del otro extremo del cable y viceversa. Si la conexión de cables se hace de tal manera que el transmisor de un extremo se conecta al transmisor del otro extremo, y el receptor se conecta a un receptor, no se establecerá ningún vínculo.

Cuando se seleccionan los cables para conectar los puertos del dispositivo con sus extremos de conexión, hay que utilizar cables directos para conectar el dispositivo a una estación, y hay que utilizar cables cruzados para conectar un dispositivo de transmisión (conmutador o concentrador) a otro. Tanto los cables directos como los cruzados son de categoría 5.

Después de conectar un puerto, se enciende su LED de indicación de VÍNCULO.

Tabla 3-4. Puertos, conectores y cables

Conector	Puerto/Interfaz	Cable
RJ-45	Puerto 10/100/1000BaseT	Cat. 5

En la siguiente lista se muestra la asignación del número de pata de RJ-45 para los puertos 10/100/1000BaseT.

Tabla 3-5. Asignación del número de pata de RJ-45 para el puerto Ethernet 10/100/1000BaseT

Nº. de pata	Función
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Configuración predeterminada del puerto

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

Negociación automática

La negociación automática permite la detección automática de la velocidad, el modo dúplex y el control de flujo en los puertos de conmutación 10/100/1000BaseT. La negociación automática se habilita por puerto de manera predeterminada.

La negociación automática es un mecanismo establecido entre las dos partes del vínculo para permitir que un puerto comunique su velocidad de transmisión, modo dúplex y capacidades de control de flujo (de manera predeterminada el control de flujo está inhabilitado) a la otra parte. De esta manera, ambos puertos funcionan al común denominador más alto entre ellos.

Si se conecta un NIC que no admite la negociación automática o no está configurado para ella, tanto el puerto de conmutación del dispositivo como el NIC se

deben configurar manualmente con la misma velocidad y modo dúplex.

Si la estación del otro lado del vínculo intenta realizar la negociación automática con un puerto 10/100/1000BaseT del dispositivo que está configurado para dúplex completo, como resultado de la negociación automática, la estación intentará funcionar en dúplex medio.

MDI /MDIX

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

Cuando la opción MDI/MDIX (Media Dependent Interface with Crossover o Interfaz dependiente de los soportes con cable cruzado) está activada, es posible realizar la corrección automática de errores en la selección por cable, lo que hace que la distinción entre un cable directo y un cable cruzado sea irrelevante. (El cableado estándar para las estaciones terminales se conoce como MDI (Media Dependent Interface o Interfaz dependiente de los soportes), y el cableado estándar para los concentradores y conmutadores se conoce como MDIX).

Control de flujo

El dispositivo admite el control de flujo 802.3x para los puertos configurados con el modo de dúplex completo. De manera predeterminada, esta función está desactivada. Se puede activar por puerto. El mecanismo de control de flujo permite que la parte receptora indique a la parte transmisora que hay que detener la transmisión de manera temporal para evitar que el búfer se desborde.

Contrapresión

El dispositivo admite la contrapresión para los puertos configurados con el modo de dúplex medio. De manera predeterminada, esta función está desactivada. Se puede activar por puerto. El mecanismo de contrapresión impide que la parte transmisora transmita tráfico adicional de manera temporal. La parte receptora puede ocupar un vínculo de modo que ya no estará disponible para el tráfico adicional.

Configuración predeterminada del puerto de conmutación

En la siguiente tabla se ofrece la configuración predeterminada del puerto.

Tabla 3-6. Configuración predeterminada del puerto

Función	Configuración predeterminada
Velocidad y modo del puerto	Cobre 10/100/1000BaseT: negociación automática 100 dúplex completo
Estado de reenvío del puerto	Activado
Etiquetas del puerto	Sin etiquetas
Control de flujo	Apagado (desactivado en la entrada)
Contrapresión	Apagado (desactivado en la entrada)

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Introducción

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [PowerConnect 5324](#)
- [Funciones](#)
- [Documentación adicional de la CLI](#)

➡ **AVISO:** Antes de continuar, lea las notas de la versión de este producto. Las notas de la versión se pueden descargar del sitio web support.dell.com.

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

PowerConnect 5324

El dispositivo PowerConnect 5324 tiene 24 puertos Gigabit Ethernet. También hay cuatro puertos de fibra SFP designados como alternativas de los puertos combinados para los puertos Ethernet 21-24. Los puertos combinados son puertos únicos con dos conexiones físicas. Cuando uno está conectado el otro está desactivado.

En la [Ilustración 1-1](#) y la [Ilustración 1-2](#) se muestran los paneles anterior y posterior del dispositivo PowerConnect 5324.

Ilustración 1-1. Panel anterior del dispositivo PowerConnect 5324



Ilustración 1-2. Panel posterior del dispositivo PowerConnect 5324



Funciones

En esta sección se describen las funciones del dispositivo configuradas por el usuario. Para obtener una lista completa de todas las funciones actualizadas del dispositivo, consulte las notas más recientes de la versión del software.

Funciones generales

Bloqueo de la cabecera de línea

El bloqueo de cabecera de línea (HOL) hace que se produzcan retrasos en el tráfico y pérdida de trama debido a que el tráfico compite por los mismos recursos del puerto de salida. El bloqueo HOL pone en cola los paquetes, y los paquetes situados al principio de la línea se envían antes que los paquetes situados al final de la cola.

Pruebas virtuales de cable (VCT)

VCT detecta e informa sobre los problemas del cableado de conexión de cobre, como es el caso de la desconexión o los cortocircuitos de los cables.

Compatibilidad con tramas gigantes

Las tramas gigantes permiten transportar datos idénticos en menos tramas. Así se garantiza un menor coste, un tiempo de procesamiento inferior y menos interrupciones.

Para obtener información sobre la activación de las tramas gigantes, consulte la sección ["Definición de información general sobre el dispositivo"](#).

Compatibilidad con MDI /MDI X

El dispositivo admite la autodetección entre cables de red cruzados y directos.

El cableado estándar para las estaciones terminales es MDI (Media-Dependent Interface) y el cableado estándar para los concentradores y conmutadores se conoce como MDIX (Media-Dependent Interface with Crossover).

Para obtener información sobre la configuración de MDI/MDI para los puertos o LAG, consulte el apartado ["Definición de los parámetros de puerto"](#) o ["Definición de los parámetros del LAG"](#).

Compatibilidad con el control de flujo (IEEE 802.3X)

El control de flujo permite que dispositivos de menor velocidad se comuniquen con dispositivos de mayor velocidad al solicitar que el dispositivo de velocidad superior se abstenga de enviar paquetes. Las transmisiones se detienen temporalmente para evitar que se produzcan desbordamientos del búfer.

Para obtener información sobre la configuración del control de flujo para los puertos o LAG, consulte el apartado ["Definición de los parámetros de puerto"](#) o ["Definición de los parámetros del LAG"](#).

Compatibilidad con la contrapresión

En las conexiones de dúplex medio, el puerto receptor evita que se produzcan desbordamientos en el búfer ocupando el vínculo de modo que éste no esté disponible al tráfico adicional.

Para obtener información sobre la configuración de la contrapresión para los puertos o LAG, consulte el apartado ["Definición de los parámetros de puerto"](#) o ["Definición de los parámetros del LAG"](#).

Funciones compatibles con las direcciones MAC

Compatibilidad con la capacidad de las direcciones MAC

El dispositivo admite un máximo de ocho mil direcciones MAC. Además, reserva direcciones MAC específicas para que las utilice el sistema.

Autoaprendizaje de direcciones MAC

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

Caducidad automática de las direcciones MAC

Las direcciones MAC en las que no se ha recibido tráfico durante un período de tiempo determinado caducan. Esto impide que la tabla de direcciones se desborde.

Para obtener más información sobre la configuración del período de caducidad de las direcciones MAC, consulte el apartado ["Configuración de las tablas de direcciones"](#).

Entradas MAC estáticas

Las entradas MAC estáticas definidas por el usuario se almacenan en la **Tabla de direcciones**.

Para obtener más información, consulte el apartado ["Configuración de las tablas de direcciones"](#).

Conmutación basada en MAC compatible con VLAN

Los paquetes que llegan de una dirección de origen desconocida se envían al microprocesador, donde las direcciones de origen se agregan a la tabla de hardware. Los paquetes que se envían a esta dirección o desde ella se reenvían de manera más eficaz con la tabla de hardware.

Compatibilidad con la multidifusión de MAC

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

Para obtener más información, consulte el apartado ["Compatibilidad con el reenvío de multidifusión"](#).

Funciones del nivel 2

Inspección IGMP

En la inspección del protocolo de pertenencia a grupos de Internet (IGMP) se examina el contenido de las tramas IGMP cuando el dispositivo las reenvía de las estaciones de trabajo a un enrutador de multidifusión que precede en la cadena. Desde la trama, el dispositivo identifica las estaciones de trabajo configuradas para sesiones de multidifusión, y los enrutadores de multidifusión que envían tramas de multidifusión.

Para obtener más información, consulte el apartado ["Inspección IGMP"](#).

Duplicación de puertos

En la duplicación de puertos se supervisa y duplica el tráfico de red mediante el reenvío de copias de paquetes entrantes y salientes desde un puerto supervisado a un puerto de supervisión. Los usuarios especifican qué puerto de destino recibe copias de todo el tráfico que pasa a través de un puerto de origen especificado.

Para obtener más información, consulte el apartado ["Definición de sesiones de duplicación de puertos"](#).

Control de tormentas de difusión

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

Cuando se envían las tramas de nivel 2, las tramas de difusión y multidifusión se desbordan en todos los puertos de la VLAN relevante. Esto ocupa la amplitud de banda, y carga todos los nodos conectados en todos los puertos.

Para obtener más información, consulte el apartado "[Habilitación del control de tormentas](#)".

Funciones compatibles con VLAN

Compatibilidad con VLAN

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

Para obtener más información, consulte el apartado "[Configuración de VLAN](#)".

LAN virtuales (VLAN) basadas en puertos

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

Para obtener más información, consulte el apartado "[Definición de la configuración de puertos VLAN](#)".

LAN virtuales (VLAN) basadas en el protocolo IEEE802.1V

Las normas de clasificación de VLAN se definen según la identificación del protocolo de nivel de enlace de datos (nivel 2). Las VLAN basadas en protocolos aíslan el tráfico de nivel 2 de forma que se diferencie de los protocolos de nivel 3.

Para obtener más información, consulte el apartado "[Definición de los grupos de protocolos de la VLAN](#)".

Cumplimiento absoluto con el estándar de etiquetado 802.1Q VLAN

El estándar IEEE 802.1Q define una arquitectura para las LAN con puentes virtuales, los servicios proporcionados en las VLAN, y los protocolos y algoritmos que participan en la oferta de estos servicios. Un requisito importante incluido en este estándar es la posibilidad de marcar tramas con el valor de etiqueta (0-7) Class of Service (CoS) que se desee.

Compatibilidad con GVRP

El protocolo de registro VLAN GARP (GVRP) proporciona la creación dinámica de VLAN y la eliminación de VLAN de acuerdo con el estándar IEEE 802.1Q en los puertos troncales 802.1Q. Cuando se habilita el protocolo GVRP, el dispositivo registra y propaga la pertenencia a VLAN a todos los puertos que forman parte de la topología activa subyacente "[Funciones del protocolo de árbol extensible](#)".

Para obtener más información, consulte el apartado "[Configuración de GVRP](#)".

Funciones del protocolo de árbol extensible

Protocolo de árbol de expansión (STP)

El árbol extensible 802.1d es un requisito estándar de los conmutadores de nivel 2 que permite a los puentes impedir y solucionar automáticamente los bucles de reenvío de nivel 2. Los conmutadores intercambian mensajes de configuración, utilizando tramas formateadas específicamente, y activa y desactivan de manera selectiva el reenvío en los puertos.

Para obtener más información, consulte el apartado "[Configuración del protocolo de árbol extensible](#)".

Conexión rápida

La convergencia de STP puede tardar de 30 a 60 segundos. Durante este tiempo, STP detecta posibles bucles y permite que los cambios de estado se propaguen y que los dispositivos pertinentes respondan. Se considera que la espera de 30 a 60 segundos es un tiempo de respuesta demasiado largo para muchas aplicaciones. La opción Fast Link (Conexión rápida) omite este retraso y se puede utilizar en topologías de red en las que no se produce el reenvío de bucles.

Para obtener más información sobre la habilitación de Fast Link (Conexión rápida) para puertos y LAG, consulte el apartado "[Definición de la configuración del puerto STP](#)" o "[Definición de la configuración STP de LAG](#)".

Árbol extensible rápido compatible con el estándar IEEE 802.1w

El árbol extensible puede tardar entre 30 y 60 segundos para que cada sistema principal decida si sus puertos reenvían el tráfico de manera activa. El árbol extensible rápido (RSTP) detecta el uso de las topologías de red para activar una convergencia más rápida, sin crear bucles de envío.

Para obtener más información, consulte el apartado "[Configuración del árbol extensible rápido](#)".

Link Aggregation (Adición de vínculos)

Para obtener más información, consulte el apartado "[Agregado de puertos](#)".

Link Aggregation (Adición de vínculos)

Se pueden definir hasta ocho conexiones agregadas, cada una de ellas con un máximo de ocho puertos miembro, para formar un único grupo agregado de conexiones (LAG). Esto permite que haya:

- 1 Protección de tolerancia de fallos contra la interrupción de vínculos físicos
- 1 Conexiones con una amplitud de banda superior
- 1 Resolución mejorada de la amplitud de banda
- 1 Conectividad del servidor de alta amplitud de banda

LAG se compone de puertos de la misma velocidad, establecidos para que funcionen en dúplex completo.

Para obtener más información, consulte el apartado "[Definición de la pertenencia a LAG](#)".

Agregado de conexiones y LACP

LACP utiliza intercambios de igual a igual entre vínculos para determinar, de manera continua, la capacidad de adición de diferentes vínculos, y proporciona el máximo nivel de capacidad de adición posible entre un par determinado de sistemas. LACP determina, configura, enlaza y supervisa automáticamente el enlace de puertos con agregadores dentro del sistema.

Para obtener más información, consulte el apartado "[Definición de los parámetros del LACP](#)".

Funciones del nivel 3

Protocolo de resolución de direcciones (ARP)

ARP es un protocolo TCP/IP que convierte las direcciones IP en direcciones físicas. ARP determina automáticamente las direcciones MAC de próximo salto del dispositivo de los sistemas, incluidos los sistemas finales conectados directamente. Los usuarios pueden hacer prevalecer esta función y complementarla mediante la definición de entradas adicionales de la tabla ARP

Para obtener más información, consulte el apartado ["Asignación del sistema principal de dominios"](#).

TCP

Las conexiones del protocolo de control de transmisiones (TCP) están definidas entre 2 puertos por un intercambio de sincronización inicial. Los puertos TCP se identifican mediante una dirección IP y un número de puerto de 16 bits. Las secuencias de octetos se dividen en paquetes TCP, cada uno de los cuales lleva un número de secuencia.

Clientes de BootP y DHCP

El protocolo de configuración dinámica del host (DHCP) activa los parámetros adicionales de configuración para que se puedan recibir desde un servidor de red cuando el sistema se inicie. El servicio DHCP es un proceso continuo. DHCP es una ampliación de BootP.

Para obtener más información sobre DHCP, consulte el apartado ["Definición de los parámetros de interfaz IP DHCP"](#).

Funciones de QoS

Compatibilidad con la clase de servicio 802.1p

La técnica de señalización IEEE 802.1p es un estándar OSI de nivel 2 para marcar y priorizar el tráfico de red en el subnivel MAC/de vínculo de datos. El tráfico de 802.1p se clasifica y envía al destino. No se establecen ni imponen reservas o límites de amplitud de banda. Este estándar deriva de 802.1Q (VLAN). El estándar 802.1p establece ocho niveles de prioridad, similar al campo de bits IP Precedence IP Header.

Para obtener más información, consulte el apartado ["Configuración de QoS"](#).

Funciones de gestión del dispositivo

Registros de capturas y alarmas de SNMP

El sistema registra eventos con códigos de gravedad y marcas de hora. Los eventos se envían como capturas del protocolo simple de administración de redes (SNMP) a una lista de destinatarios de capturas.

Para obtener más información sobre las capturas y alarmas de SNMP, consulte el apartado ["Definición de los parámetros de SNMP"](#).

Versión 1 y 2 de SNMP

Protocolo simple de administración de redes (SNMP) a través del protocolo UDP/IP. Para controlar el acceso al sistema, se define una lista de entradas de

comunidad, cada una de las cuales se compone de una cadena de comunidad y sus privilegios de acceso. Existen tres niveles de seguridad SNMP: sólo lectura, lectura/escritura y super. Sólo un superusuario puede acceder a la tabla de comunidades.

Gestión basada en web

Gracias a la gestión basada en web, el sistema se puede gestionar desde cualquier explorador de la web. El sistema contiene un servidor web incorporado (EWS), que ejecuta páginas HTML, a través del cual el sistema se puede supervisar y configurar. El sistema convierte internamente la entrada basada en web en comandos de configuración, valores variables de la MIB y otros valores relacionados con la gestión.

Carga y descarga del archivo de configuración

La configuración del dispositivo PowerConnect se almacena en un archivo de configuración. Este archivo incluye una configuración del dispositivo específica del puerto y de todo el sistema. El sistema puede mostrar archivos de configuración en forma de recopilación de los comandos de la CLI, que se almacenan y manejan como archivos de texto.

Para obtener más información, consulte el apartado "[Gestión de archivos](#)".

TFTP (Trivial File Transfer Protocol)

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

Supervisión remota

La supervisión remota (RMON) es una ampliación del protocolo SNMP, que proporciona opciones globales de supervisión del tráfico de la red (a diferencia de SNMP, que permite la supervisión y gestión de los dispositivos de la red). RMON es una MIB estándar que define las estadísticas actuales e históricas del nivel MAC y los objetos de control, lo que permite capturar información en tiempo real a lo largo de toda la red.

Para obtener más información, consulte el apartado "[Visualización de las estadísticas de RMON](#)".

Interfaz de línea de comandos

La sintaxis y la semántica de la interfaz de línea de comandos (CLI) se ajustan tanto como es posible a las prácticas habituales del sector. CLI se compone de elementos obligatorios y opcionales. El intérprete de la CLI permite obtener comandos y palabras clave para ayudar al usuario y reducir la tarea de escribir.

Syslog

Syslog es un protocolo que permite que las notificaciones de eventos se envíen a un conjunto de servidores remotos donde se pueden almacenar, examinar y actuar en consecuencia. Se han utilizado varios mecanismos para enviar notificaciones de eventos significativos en tiempo real y guardar un registro de estos eventos para su uso posterior.

Para obtener más información sobre Syslog, consulte el apartado "[Gestión de registros](#)".

SNTP

El protocolo de tiempo de la red simple (SNTP) garantiza una sincronización precisa del tiempo del reloj del dispositivo en red en milisegundos. La sincronización del tiempo la realiza un servidor SNTP en red. Los recursos de tiempo se establecen por niveles. Estos niveles definen la distancia del reloj de referencia. Cuanto más alto sea el nivel (donde cero es el más alto), más preciso será el reloj.

Para obtener más información, consulte el apartado "[Configuración de los valores de SNTP](#)".

Traceroute

Traceroute permite descubrir cuáles eran las rutas IP a las que se reenviaban los paquetes durante el proceso de reenvío. La utilidad Traceroute de la CLI se puede ejecutar desde los modos privilegiados o de ejecución de usuario.

Funciones de seguridad

SSL

Nivel de socket seguro (SSL) es un protocolo de nivel de aplicación que permite realizar transmisiones seguras de datos de una manera privada, autenticada e íntegra. Este protocolo está basado en certificados y claves públicas y privadas.

Autenticación basada en puerto (802.1x)

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

Para obtener más información, consulte el apartado "[Configuración de la autenticación basada en puerto](#)".

Compatibilidad con el puerto bloqueado

El puerto bloqueado aumenta la seguridad de la red mediante la limitación del acceso en un puerto específico sólo para usuarios con direcciones MAC determinadas. Estas direcciones se aprenden o definen manualmente en dicho puerto. Cuando se ve una trama en un puerto bloqueado y la dirección MAC de origen de la trama no está vinculada a ese puerto, se invoca el mecanismo de protección.

Para obtener más información, consulte el apartado "[Configuración de la seguridad de los puertos](#)".

Cliente de RADIUS

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

Para obtener más información, consulte el apartado "[Configuración de parámetros globales de RADIUS](#)".

SSH

Shell seguro (SSH) es un protocolo que proporciona una conexión segura y remota a un dispositivo. La versión 1 de SSH está actualmente disponible. La función del servidor SSH permite que un cliente SSH establezca una conexión segura y codificada con un dispositivo. Esta conexión proporciona unas funciones parecidas a una conexión de telnet entrante. SSH utiliza la criptografía de claves públicas RSA para las conexiones y la autenticación del dispositivo.

TACACS+

TACACS+ proporciona seguridad centralizada para la validación de usuarios que acceden al dispositivo. TACACS+ proporciona un sistema de gestión de usuarios centralizado al mismo tiempo que mantiene la coherencia con RADIUS y otros procesos de autenticación.

Para obtener más información, consulte el apartado ["Definición de la configuración de TACACS+"](#).

Documentación adicional de la CLI

La Guía de Referencia de la CLI, que está disponible en el CD de documentación, proporciona información sobre los comandos de la CLI utilizados para configurar el dispositivo. El documento proporciona información que incluye ejemplos, pautas, valores predeterminados, sintaxis y una descripción de la CLI.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de QoS

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Visión general de la calidad de servicio \(QoS\)](#)
- [Definición de los parámetros globales de QoS](#)

En esta sección se proporciona información para poder definir y configurar los parámetros de la calidad de servicio (QoS). Para abrir la página, haga clic en [Home](#) → Quality of Service (Calidad de servicio) en la vista de árbol.

Visión general de la calidad de servicio (QoS)

La calidad de servicio (QoS) proporciona la capacidad de implementar la QoS y la colocación en cola de la prioridad dentro de una red. La QoS mejora el flujo del tráfico de red en función de las políticas, los contadores de tramas y el contexto.

Un ejemplo de implementación que requiere la QoS incluye ciertos tipos de tráfico como, por ejemplo, tráfico de voz, vídeo y de tiempo real a los que se les puede asignar una cola de prioridad alta, mientras que a otro tráfico se le puede asignar una cola de prioridad inferior. El resultado es un flujo de tráfico mejorado para el tráfico de mucha demanda.

La QoS se define mediante:

- 1 **Clasificación:** Especifica qué campos de paquetes coinciden con valores específicos. Todos aquellos paquetes que coincidan con las especificaciones definidas por el usuario, se clasifican juntos.
- 1 **Acción:** Define la gestión del tráfico, en la que los paquetes que se reenvían se basan en la información del paquete, y los valores del campo del paquete como, por ejemplo, prioridad de VLAN (VPT) y DSCP (punto de código diferenciado de servicios).

Información de clasificación de asignación de etiquetas de VPT

Las etiquetas de prioridad de VLAN se utilizan para clasificar los paquetes asignando los paquetes a una de las colas de salida. Las asignaciones de etiqueta de prioridad de VLAN a cola también las puede definir el usuario. En la tabla siguiente se muestran los detalles de los valores predeterminados de VPT a cola:

Tabla 9-92. Valores predeterminados de la tabla de asignaciones de CoS a cola

Valor de CoS	Valores de las colas de reenvío
0	q2
1	q1 (Prioridad más baja = Mejor esfuerzo)
2	q1 (Prioridad más baja = Mejor esfuerzo)
3	q2
4	q3
5	q3
6	q4 (Prioridad más alta)
7	q4 (Prioridad más alta)

Los paquetes que llegan sin etiquetar se asignan a una VPT predeterminada que se establece por puerto. La VPT asignada se utiliza para asignar el paquete a la cola de salida y como la VPT de entrada.

Los valores del DSCP se pueden asignar a las colas de prioridad. La siguiente tabla contiene la asignación de DSCP predeterminada para los valores de cola de reenvío:

Tabla 9-93. Valores predeterminados de la tabla de asignación de DSCP a colas

Valor de DSCP	Valores de las colas de reenvío
---------------	---------------------------------

0-7	q2 (Prioridad más baja)
8-15	q1
16-23	q1
24-31	q2
32-39	q3
40-47	q3
48-55	q4
55-63	q4 (Prioridad más alta)

La asignación de DSCP se habilita por sistema.

Servicios de CoS

Una vez asignados los paquetes a una cola específica, los servicios de CoS se pueden asignar a las colas. Las colas de salida se configuran con un esquema de planificación utilizando uno de los métodos siguientes:

1. **Prioridad estricta:** Garantiza que las aplicaciones sensibles al tiempo se reenvían siempre a través de una vía con mayor celeridad. Prioridad estricta permite priorizar el tráfico sensible al tiempo, importante para la empresa, en relación a aplicaciones con una sensibilidad al tiempo inferior. Por ejemplo, bajo la prioridad estricta, el tráfico de voz sobre IP se reenvía antes que el tráfico FTP o el correo electrónico (SMTP). La cola de prioridad estricta se vacía antes que el tráfico que todavía queda en las colas de reenvío.
1. **Turno rotativo ponderado:** Garantiza que una sola aplicación no domine la capacidad de reenvío del dispositivo. El turno rotativo ponderado (WRR) reenvía colas enteras en un orden de turno rotativo. Las prioridades de cola se definen mediante la longitud de la cola. Cuanto mayor sea la longitud de la cola, más alta será la prioridad de reenvío de la cola. Por ejemplo, si cuatro colas tienen ponderaciones de cola de 1, 2, 3 y 4, los paquetes que tengan la prioridad de reenvío más alta se asignan a la cola 4, y los paquetes que tengan la prioridad de reenvío más baja se asignan a la cola 1. Al proporcionar la prioridad de reenvío más alta a las colas de longitud 4, el turno rotativo ponderado procesa el tráfico de prioridad más alta y garantiza que el tráfico de prioridad más baja se reenvíe satisfactoriamente.

El esquema de planificación se habilita en todo el sistema. Las colas asignadas a la política de prioridad estricta se asignan automáticamente a la cola de prioridad más alta. De forma predeterminada, todos los valores se asignan como política estricta. Cuando se cambia a la modalidad WRR, el valor predeterminado de la ponderación es uno. Los valores de ponderación de cola pueden asignarse en cualquier orden mediante WRR. Los valores de WRR pueden asignarse a nivel de todo el sistema. El tráfico del mejor esfuerzo se asigna siempre a la primera cola. Los valores de WRR deben asignarse de forma que la cola 1 siga perteneciendo al mejor esfuerzo.

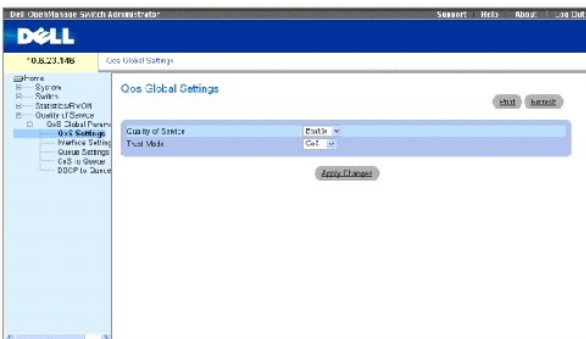
Definición de los parámetros globales de QoS

Los parámetros globales de la clase de servicio se establecen en la página CoS Global Parameter (Parámetros globales de QoS).

Configuración de los valores globales de QoS

La página QoS Global Settings (Valores globales de QoS) contiene campos para habilitar o inhabilitar QoS. Además, se puede seleccionar el modo de confianza. El modo de confianza se basa en campos predefinidos dentro del paquete para determinar la cola de salida. Para abrir la página [QoS Settings](#) (Configuración de QoS), haga clic en Quality of Service → CoS Global Parameters → CoS Settings (Calidad de servicio → Parámetros globales de QoS → Configuración de QoS) en la vista de árbol.

Ilustración 9-130. QoS Settings (Configuración de QoS)



Quality of Service (Calidad de servicio): Habilita o inhabilita la gestión del tráfico de red mediante la calidad del servicio.

Trust Mode (Modo de confianza): Determina qué campos de paquetes deben utilizarse para clasificar los paquetes que entren en el dispositivo. Cuando no se ha definido ninguna regla, el tráfico que contiene el campo de paquete predefinido (CoS o DSCP) se asigna en función de la tabla de modos de confianza pertinentes. El tráfico que no contenga ningún campo de paquete predefinido se asigna al mejor esfuerzo. Los valores posibles del campo Trust Mode (Modo de confianza) son:

CoS (Calidad de servicio): La asignación de la cola de salida se determina mediante la etiqueta de VLAN (VPT) IEEE802.1p o mediante la VPT predeterminada asignada a un puerto.

DSCP (Punto de código diferenciado de servicios): La asignación de cola de salida se determina mediante el campo DSCP.

 **NOTA:** La configuración de la confianza de interfaz suplanta a la configuración de confianza global.

Habilitación de la calidad de servicio:

1. Abra la página [QoS Settings](#) (Configuración de QoS).
2. Seleccione **Enable** (Habilitar) en el campo **CoS Mode** (Modo de QoS).
3. Haga clic en Apply Changes (Aplicar cambios).

La clase de servicio está habilitada en el dispositivo.

Habilitación de la confianza:

1. Abra la página [QoS Settings](#) (Configuración de QoS).
2. Seleccione **Trust** (Confianza) en el campo **Trust Mode** (Modo de confianza).
3. Haga clic en Apply Changes (Aplicar cambios).

La confianza se habilita en el dispositivo.

Habilitación de la confianza mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos de la página [QoS Settings](#) (Configuración de QoS).

Tabla 9-94. Comandos de la CLI para la configuración de CoS

Comando de la CLI	Descripción
<code>qos trust [cos dscp]</code>	Configura el sistema en el modo básico y el estado de "confianza".
<code>no cos trust</code>	Devuelve el estado de no confianza.

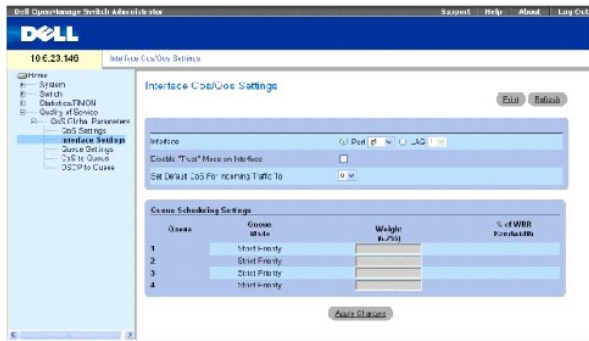
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# cos trust dscp
```

Definición de la configuración de la interfaz de QoS

La página [Interface Cos/QoS Settings](#) (Configuración de Cos/QoS de interfaz) contiene campos para definir, por interfaz, si el modo de confianza seleccionado debe activarse. La prioridad predeterminada para los paquetes sin etiquetas entrantes también se seleccionan en la página [Interface Cos/QoS Settings](#) (Configuración de Cos/QoS de interfaz), haga clic en Quality of Service → CoS Global Parameters → Interface Settings (Calidad de servicio → Parámetros globales de CoS → Configuración de la interfaz) en la vista de árbol.

Ilustración 9-131. Interface Cos/QoS Settings (Configuración de Cos/QoS de interfaz)



Interface (Interfaz): El puerto específico o el LAG que debe configurarse:

Disable "Trust" Mode on Interface (Desactivar modo de "confianza" en la interfaz): Inhabilita el modo de confianza para la interfaz seleccionada. Este valor suplanta al modo de confianza configurado en el dispositivo globalmente.

Set Default CoS For Incoming Traffic To (Establecer CoS como predeterminado para tráfico entrante en): Establece el valor predeterminado de CoS para los paquetes para los que no se haya definido ninguna etiqueta. Los valores de etiqueta de CoS posibles son 0-7. El valor predeterminado es 0.

Queue (Cola): El número de la cola.

Queue Mode (Modo de cola): Indica si la cola se encuentra en la modalidad de prioridad estricta o WRR. Esto se define en la pantalla **Queue Settings** (Configuración de colas).

- 1 SP puede configurarse en todas las colas 1 - 4.
- 1 WRR puede configurarse en todas las colas 1 - 4.
- 1 El modo SP puede configurarse en las colas 1 - 2, con WRR en las colas 3 - 4.
- 1 El modo WRR puede configurarse en las colas 1 - 2, con SP en las colas 3 - 4.

Weight (6-255) (Ponderación [6-255]): Asigna ponderaciones WRR a las colas. Este campo se habilita sólo para las colas que estén en el modo de cola WRR.

% of WRR Bandwidth (% de amplitud de banda WRR): La conversión del porcentaje de la ponderación definida en el campo **Weight (6-255)** (Ponderación [6-255]).

Asignación de la configuración de QoS/CoS para una interfaz:

1. Abra la página [Interface Cos/QoS Settings](#) (Configuración de Cos/QoS de interfaz).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de CoS se asigna a la interfaz.

Asignación de interfaces de CoS mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos de la página [Interface Cos/QoS Settings](#) (Configuración de Cos/QoS de interfaz).

Tabla 9-95. Comandos de la CLI de la interfaz de CoS

Comando de la CLI	Descripción
<code>qos trust</code>	Habilita el estado de confianza para cada puerto.
<code>qos cos <i>cos-predeterminado</i></code>	Configura el valor predeterminado de CoS del puerto.
<code>no qos trust</code>	Inhabilita el estado de confianza de cada puerto.

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

```

Console (config)# interface ethernet g5

Console (config-if)# qos trust

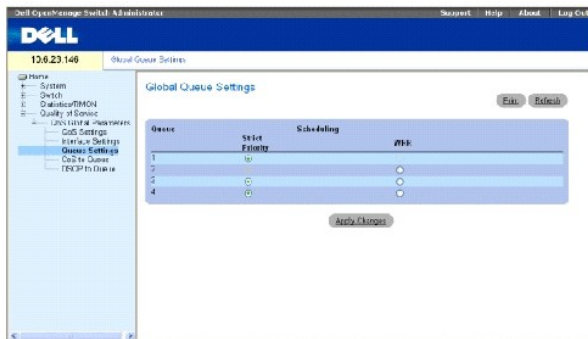
Console (config-if)# qos cos 3

```

Definición de la configuración de las colas

La página [Global Queue Setting](#) (Configuración global de las colas) contiene campos para configurar el método de planificación mediante el cual se mantienen las colas. Para abrir la página [Global Queue Setting](#) (Configuración global de las colas), haga clic en Quality of Service → CoS Global Parameters → Queue Settings (Calidad de servicio → Parámetros globales → Configuración de colas) en la vista de árbol.

Ilustración 9-132. Global Queue Setting (Configuración global de las colas)



Queues (Colas): El número de la cola.

Strict Priority (Prioridad estricta): Especifica si la planificación del tráfico se basa en la prioridad de la cola. El valor predeterminado es habilitado.

WRR (Turno rotativo ponderado): Especifica si la planificación del tráfico se basa en las ponderaciones de turno rotativo ponderado (WRR) a las colas de entrada.

Definición de la configuración de las colas

1. Abra la página [Global Queue Setting](#) (Configuración global de las colas).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de las colas se define, y el dispositivo se actualiza.

Asignación de la configuración de colas mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos de la página [Global Queue Setting](#) (Configuración global de las colas).

Tabla 9-96. Comandos de la CLI para la configuración de las colas

Comando de la CLI	Descripción
<code>wrr-queue bandwidth weight1 weight2...weight_n</code>	Asigna las ponderaciones de turno rotativo ponderado (WRR) en las colas de salida.
<code>show qos interface [ethernet número-interfaz] [queuing]</code>	Muestra los datos de la interfaz QoS.

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

```

Console (config)# wrr-queue bandwidth 10 20 30 40

Console(config)#exit

Console# exit

Console> show qos interface ethernet g1 queuing

Ethernet g1

wrr bandwidth weights and EF priority:

```

```

Console (config)# wrr-queue bandwidth 10 20 30 40

Console(config)#exit

Console# exit

Console> show qos interface ethernet g1 queuing

Ethernet g1

wrr bandwidth weights and EF priority:

```

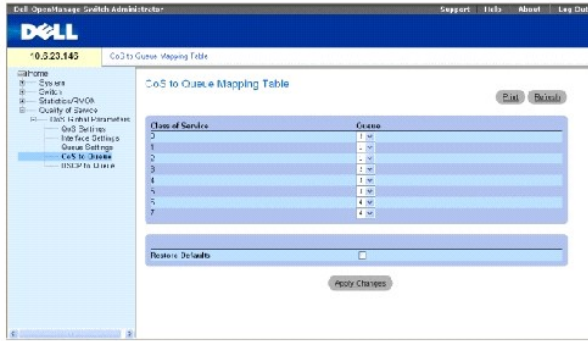
qid	weights	EF	Priority
-----	-----	-----	-----

1	125	Disable	-
2	125	Disable	-
3	125	Disable	-
4	125	Disable	-
<p>Cos queue map:</p> <p>Cos qid</p> <p>0 2</p> <p>1 1</p> <p>2 1</p> <p>3 2</p> <p>4 3</p> <p>5 3</p> <p>6 4</p> <p>47</p>			

Asignación de los valores de CoS a las colas

La página [CoS to Queue Mapping Table](#) (Tabla de asignación de CoS a colas) contiene campos para clasificar la configuración de CoS para las colas de tráfico. Para abrir la página [CoS to Queue Mapping Table](#) (Tabla de asignación de CoS a colas), haga clic en Quality of Service→ CoS Global Parameters→ CoS to Queue (Calidad de servicio→ Parámetros globales de QoS→ CoS a colas) en la vista de árbol.

Ilustración 9-133. CoS to Queue Mapping Table (Tabla de asignaciones de CoS a cola)



Class of Service (Clase de servicio): Especifica los valores de etiqueta de CoS, donde cero es la prioridad más baja y 7 es la más alta.

Queue (Cola): La cola de reenvío de tráfico a la que se asigna la prioridad de CoS. Se admiten cuatro colas de prioridad de tráfico.

Restore Defaults (Restaurar valores predeterminados): Restaura los valores predeterminados de fábrica para asignar los valores de CoS a una cola de reenvío.

Asignación de un valor de CoS a una cola

1. Abra la página [CoS to Queue Mapping Table](#) (Tabla de asignación de CoS a colas).
2. Seleccione una entrada de CoS.
3. Defina el número de cola en el campo **Queue** (Cola).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El valor de CoS se asigna a una cola, y el dispositivo se actualiza.

Asignación de los valores de CoS a las colas mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos de la página [CoS to Queue Mapping Table](#) (Tabla de asignación de CoS a colas).

Tabla 9-97. Comandos de la CLI para la configuración de CoS a colas

Comando de la CLI	Descripción
<code>wrr-queue cos-map <i>id-cola cos1...cos8</i></code>	Asigna los valores de CoS especificados a las colas de entrada.

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

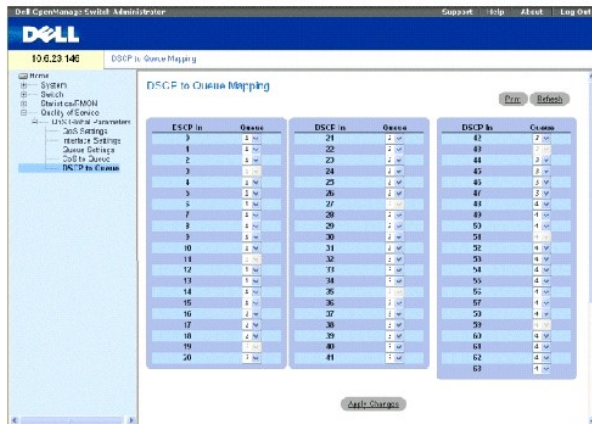
```
Console (config)# wrr-queue cos-map 4 7
```

Asignación de los valores de DSCP a las colas

La página [DSCP Mapping](#) (Asignación de DSCP) proporciona campos para definir la cola de salida a campos de DSCP específicos. Para abrir la página [DSCP Mapping](#) (Asignación de DSCP), haga clic en Quality of Service → CoS Global Parameters → DSCP Mapping (Calidad de servicio → Parámetros globales → Asignación de DSCP) en la vista de árbol.

NOTA: Para obtener la lista de la configuración predeterminada de las colas de DSCP, consulte la tabla ["Valores predeterminados de la tabla de asignación de DSCP a colas"](#).

Ilustración 9-134. DSCP Mapping (Asignación de DSCP)



DSCP In (Entrada DSCP): Los valores del campo DSCP del paquete entrante.

Queue (Cola): La cola a la que se asignan los paquetes con el valor DSCP específico. Los valores son 1-4, donde uno es el valor más bajo y cuatro es el más alto.

Asignación de un valor de DSCP y asignación de cola de prioridad:

1. Abra la página [DSCP Mapping](#) (Asignación de DSCP).
2. Seleccione un valor en la columna **DSCP In** (Entrada de DSCP).
3. Defina los campos **Queue** (Cola).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se suplanta el valor de DSCP, y al valor se asigna una cola de reenvío.

Asignación de los valores de DSCP mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos de la página [DSCP Mapping](#) (Asignación de DSCP).

Tabla 9-98. Comandos de la CLI para el valor DSCP a colas

Comando de la CLI	Descripción
<code>qos map dscp-queue lista-dscp to id-cola</code>	Modifica la asignación de DSCP a colas.

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

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

[Regresar a la página de contenido](#)

Especificaciones del dispositivo

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Especificaciones de los cables y los puertos](#)
- [Condiciones de funcionamiento](#)
- [Especificaciones físicas del dispositivo](#)
- [Especificaciones de la memoria del dispositivo](#)
- [Especificaciones de las funciones](#)

En este apéndice se incluye la información necesaria para ejecutar el dispositivo.

Especificaciones de los cables y los puertos

En esta sección se describen las especificaciones de los puertos.

Especificaciones de los puertos

En la siguiente tabla se describen los tipos de puertos del dispositivo, y además se ofrece una descripción de los tipos de puertos.

Tabla 10-99. Especificaciones de los puertos

Dispositivo	Especificación
PowerConnect 5324	<ul style="list-style-type: none">1 24 puertos GE1 4 puertos SFP1 Puerto de consola RS-232
Tipos de puerto	
RJ-45	<ul style="list-style-type: none">1 10 Base-T1 100 Base-T1 1000 Base-T
SFP	Compatible con equipos de formato reducido estándar Transceptores Gigabit Plug
Configuración de puertos	
	<ul style="list-style-type: none">1 Negociación automática para la velocidad, el modo de dúplex y el control de flujo1 Contrapresión1 Bloqueo de cabecera de línea1 MDI/MDIX automático1 Duplicación de puertos1 Control de tormentas de difusión

Condiciones de funcionamiento

En esta sección se detallan las condiciones de funcionamiento, incluidas las temperaturas de funcionamiento y la humedad.

Tabla 10-100. Condiciones de funcionamiento

Función	Especificación
Temperatura de funcionamiento	De 0 a 40 C / De 32 a 104 F
Humedad en funcionamiento	10% - 90% (sin condensación)

Especificaciones físicas del dispositivo

En esta sección se detallan las especificaciones físicas del dispositivo.

Tabla 10-101. Especificaciones físicas del dispositivo

Función	Especificación
Tamaño de la unidad	<ul style="list-style-type: none"> 19 pulgadas de ancho (aproximadamente 48 cm) 1U de alto
Ventilación	Dos ventiladores por unidad.

Especificaciones de la memoria del dispositivo

En esta sección se detallan las especificaciones de la memoria del dispositivo.

Tabla 10-102. Especificaciones de la memoria del dispositivo

Tipo de memoria	Cantidad
DRAM de la CPU	64 MB
Memoria flash	16 MB
Memoria búfer del paquete	2 Mb

Especificaciones de las funciones

VLAN

- | Compatibilidad de VLAN para el etiquetado y basado en puertos según el estándar IEEE 802.1Q
- | Se admiten hasta 4094 VLAN
- | VLAN reservadas para uso interno del sistema
- | VLAN dinámicas con compatibilidad de GVRP
- | VLAN basadas en protocolo

Calidad de servicio

- | Modo de confianza de nivel 2 (Etiquetado IEEE 802.1p)
- | Modo de confianza de nivel 3 (DSCP)
- | Turno rotativo ponderado (WRR) ajustable
- | Planificación de colas estrictas ajustable

Multidifusión de nivel 2

- | Compatibilidad con la multidifusión dinámica: hasta 256 grupos de multidifusión compatibles con la inspección IGMP o la multidifusión estática

Seguridad del dispositivo

- | Protección por contraseña para acceder al conmutador
- | Bloqueo y alerta de la dirección MAC basada en puertos
- | Autenticación remota de RADIUS para obtener acceso de administración al conmutador
- | TACACS+
- | Filtrado del acceso de administración a través de los perfiles de acceso de administración
- | Codificaciones de gestión SSH/SSL

Funciones adicionales de conmutación

- 1 Agregado de vínculos que admite hasta 8 vínculos agregados por dispositivo y hasta 8 puertos por vínculo agregado (IEEE 802.3ad)
- 1 Compatibilidad con LACP
- 1 Admite tramas gigantes de hasta 10 K
- 1 Control de tormentas de difusión
- 1 Duplicación de puertos

Gestión del dispositivo

- 1 Interfaz de gestión basada en web
- 1 Accesibilidad a la CLI a través de Telnet
- 1 Se admite SNMPv1 y SNMP v2
- 1 Se admiten 4 grupos RMON
- 1 Transferencias de firmware y archivos de configuración a través de TFTP
- 1 Imágenes duales de firmware en la placa
- 1 Se admiten varias cargas/descargas de archivos de configuración
- 1 Estadísticas para la supervisión de errores y la optimización del rendimiento
- 1 Compatibilidad con la gestión de direcciones IP BootP/DHCP
- 1 Funciones de registro remoto Syslog
- 1 Compatibilidad con SNTP
- 1 Traceroute de nivel 3
- 1 Cliente Telnet
- 1 Cliente DNS

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de la información del dispositivo

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Configuración de la seguridad de la red](#)
- [Configuración de los puertos](#)
- [Configuración de las tablas de direcciones](#)
- [Configuración de GARP](#)
- [Configuración del protocolo de árbol extensible \(STP\)](#)
- [Configuración de VLAN](#)
- [Agregado de puertos](#)
- [Compatibilidad con el reenvío de multidifusión](#)

En esta sección se proporciona toda la información general y de funcionamiento del sistema para configurar la seguridad de la red, los puertos, las tablas de direcciones, GARP, VLAN, el árbol extensible, el agregado de puertos y la compatibilidad de multidifusión.

Configuración de la seguridad de la red

El dispositivo activa la seguridad de la red a través de las listas de control de acceso y de puertos bloqueados. Para abrir la página **Network Security** (Seguridad de la red), seleccione Switch → Network Security (Commutador → Seguridad de la red).

Visión general de la seguridad de la red

En esta sección se describen las características de la seguridad de la red.

Autenticación basada en puerto (802.1x)

La autenticación basada en puerto permite la autenticación de los usuarios del sistema por puerto a través de un servidor externo. Sólo los usuarios del sistema autenticados y aprobados pueden transmitir y recibir datos. Los puertos se autentican a través del servidor RADIUS mediante el protocolo de autenticación extensible (EAP). La autenticación de los puertos incluye:

- 1 Autenticadores: Especifican el puerto que se autentica antes de permitir el acceso al sistema.
- 1 Solicitantes: Especifican el sistema principal conectado al puerto autenticado que solicita acceder a los servicios del sistema.
- 1 Servidor de autenticación: Especifica el servidor externo, por ejemplo, el servidor RADIUS que realiza la autenticación en nombre del autenticador, e indica si el usuario está autorizado para acceder a los servicios del sistema.

La autenticación basada en puerto crea dos estados de acceso:

- 1 Acceso controlado: Permite la comunicación entre el usuario y el sistema, si el usuario está autorizado.
- 1 Acceso no controlado: Permite la comunicación no controlada independientemente del estado del puerto.

Actualmente el dispositivo admite la autenticación basada en puerto a través de los servidores RADIUS.

Autenticación avanzada basada en puerto

La autenticación avanzada basada en puerto permite que varios sistemas principales se conecten a un solo puerto. La autenticación avanzada basada en puerto sólo requiere que se autorice un sistema principal para que todos los sistemas principales tengan acceso al sistema. Si el puerto no está autorizado, se negará el acceso a la red a todos los sistemas principales conectados.

La autenticación avanzada basada en puerto también permite la autenticación basada en usuario. En el dispositivo siempre hay disponibles unas VLAN

específicas, incluso si determinados puertos conectados a la VLAN no están autorizados. Por ejemplo, la tecnología de voz sobre IP no necesita la autenticación, mientras que el tráfico de datos sí que la necesita. Se pueden definir las VLAN para las que no es necesaria autorización. Las VLAN no autenticadas están disponibles para los usuarios, aunque los puertos conectados a la VLAN se definan como autorizados.

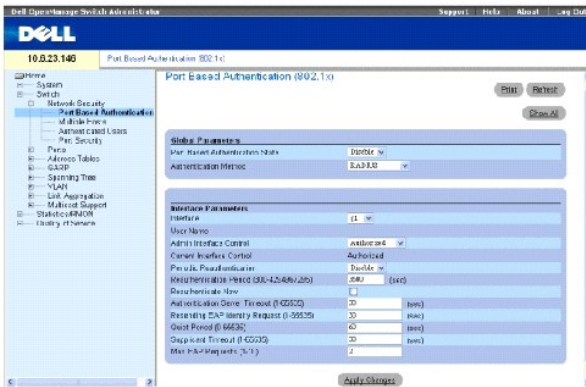
La autenticación avanzada basada en puerto se implementa en los siguientes modos:

- 1 **Modo de sistema principal único:** Sólo permite que el sistema principal autorizado acceda al puerto.
- 1 **Modo de varios sistemas principales:** Permite que varios sistemas principales se conecten a un solo puerto. Sólo hay que autorizar a un sistema principal para que todos los sistemas principales accedan a la red. Si la autenticación del sistema principal falla o se recibe un mensaje de cierre de sesión-EAPOL, se negará el acceso a la red a todos los clientes conectados.

Configuración de la autenticación basada en puerto

La página [Port Based Authentication](#) (Autenticación basada en puerto) contiene campos para configurar la autenticación basada en puerto. Para abrir la página [Port Based Authentication](#) (Autenticación basada en puerto), haga clic en Switch → Network Security → Port Based Authentication (Conmutador → Seguridad de la red → Autenticación basada en puerto).

Ilustración 7-80. Port Based Authentication (Autenticación basada en puerto)



Port Based Authentication State (Estado de autenticación basada en puerto): Permite la autenticación basada en puerto del dispositivo. Los valores de campo posibles son:

Enable (Activar): Activa la autenticación basada en puerto del dispositivo.

Disable (Desactivar): Desactiva la autenticación basada en puerto del dispositivo.

Authentication Method (Método de autenticación): El método de autenticación utilizado. Los valores de campo posibles son:

None (Ninguno): No se utiliza ningún método de autenticación para autenticar el puerto.

RADIUS: La autenticación del puerto se realiza con el servidor RADIUS.

RADIUS, None (RADIUS, Ninguno): La autenticación del puerto se realiza primero con el servidor RADIUS. Si el puerto no se autentica, entonces no se utiliza ningún método de autenticación y se permite la sesión.

Interface (Interfaz): Contiene una lista de interfaces.

User Name (Nombre de usuario): El nombre de usuario tal como se configura en el servidor RADIUS.

Admin Interface Control (Control de interfaz de administración): Define el estado de autorización del puerto. Los valores de campo posibles son:

Authorized (Autorizado): Establece el estado de la interfaz en autorizado (se permite el tráfico).

Unauthorized (No autorizado): Establece el estado de la interfaz en no autorizado (se deniega el tráfico).

Auto (Automático): El estado de autorización se establece según el método de autorización.

Current Interface Control (Control de la interfaz actual): El estado de autorización del puerto actualmente configurado.

Periodic Reauthentication (Reautenticación periódica): Vuelve a autenticar el puerto seleccionado de manera periódica cuando está activado. El período de reautenticación se define en el campo **Reauthentication Period (300-4294967295)** (Período de reautenticación [300-4294967295]).

Reauthentication Period (300-4294967295) (Período de reautenticación [300-4294967295]): indica el período de tiempo en el que se vuelve a autenticar el puerto seleccionado. El valor del campo se expresa en segundos. El valor predeterminado del campo es 3600 segundos.

Reauthenticate Now (Reautenticar ahora): Si se selecciona esta opción, se permite la reautenticación inmediata del puerto.

Authentication Server Timeout (1-65535) (Tiempo de espera del servidor de autenticación [1-65535]): Define la cantidad de tiempo que pasa antes de que el dispositivo vuelva a enviar una solicitud al servidor de autenticación. El valor del campo se expresa en segundos. El valor predeterminado del campo es 30 segundos.

Resending EAP Identity Request (1-65535) (Reenvío de solicitud de identidad EAP [1-65535]): define la cantidad de tiempo que pasa antes de volver a enviar una solicitud de EAP. El valor predeterminado del campo es 30 segundos.

Quiet Period (0-65535) (Período pasivo [0-65535]): El número de segundos que el dispositivo permanece en un estado pasivo después de un intercambio de autenticación que no ha salido bien. El intervalo posible del campo es 0-65535. El valor predeterminado del campo es 60 segundos.

Supplicant Timeout (1-65535) (Tiempo de espera del solicitante [1-65535]): La cantidad de tiempo que pasa antes de que las solicitudes de EAP se reenvíen al usuario. El valor del campo se expresa en segundos. El valor predeterminado del campo es 30 segundos.

Max EAP Requests (1-10) (Nº máximo de solicitudes de EAP [1-10]): La cantidad total de solicitudes de EAP enviadas. Si no se recibe una respuesta después del período definido, se reinicia el proceso de autenticación. El valor predeterminado del campo es 2 reintentos.

Visualización de la tabla de autenticación basada en puerto

1. Muestre la página [Port Based Authentication](#) (Autenticación basada en puerto).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la [Port Based Authentication Table](#) (Tabla de autenticación basada en puerto):

Ilustración 7-81. Port Based Authentication Table (Tabla de autenticación basada en puerto)

Termination Cause (Motivo de la terminación): El motivo por el que ha finalizado la autenticación del puerto.

Copy To Checkbox (Copiar en casilla de verificación): Copia los parámetros de puerto desde un puerto a los puertos seleccionados.

Select All (Seleccionar todo): Selecciona todos los puertos de la [Tabla de autenticación basada en puerto](#).

Copia de los parámetros de la [Tabla de autenticación basada en puerto](#)

1. Abra la página [Port Based Authentication](#) (Autenticación basada en puerto).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la [Port Based Authentication Table](#) (Tabla de autenticación basada en puerto).

3. Seleccione la interfaz en el campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione una interfaz en la [Tabla de autenticación basada en puerto](#).
5. Seleccione la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que se copian los parámetros de autenticación basada en puerto.
6. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian en el puerto seleccionado de la [Tabla de autenticación basada en puerto](#), y el dispositivo se actualiza.

Habilitación de la autenticación basada en puerto mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para habilitar la autenticación basada en puerto tal como aparecen en la página [Port Based Authentication](#) (Autenticación basada en puerto).

Tabla 7-49. Comandos de la CLI para la autenticación de puertos

Comando de la CLI	Description
<code>aaa authentication dot1x default <i>método1</i> [<i>método2</i>]</code>	Especifica uno o varios métodos de autenticación, autorización y compatibilidad (AAA) para su utilización en interfaces que ejecutan IEEE 802.1X.
<code>dot1x max-req <i>recuento</i></code>	Establece el número máximo de veces que el dispositivo envía un EAP al cliente, antes de reiniciar el proceso de autenticación.
<code>dot1x re-authenticate [<i>ethernet Interfaz</i>]</code>	Inicia manualmente una reautenticación de todos los puertos habilitados para 802.1X o de un puerto específico habilitado para 802.1X.
<code>dot1x re-authentication</code>	Activa la reautenticación periódica del cliente.
<code>dot1x timeout quiet-period <i>segundos</i></code>	Establece el número de segundos que el dispositivo permanece en el estado pasivo después de un intercambio de autenticación que no ha salido bien.
<code>dot1x timeout re-authperiod <i>segundos</i></code>	Establece el número de segundos que transcurren entre los intentos de reautenticación.
<code>dot1x timeout server-timeout <i>segundos</i></code>	Establece el tiempo para la retransmisión de paquetes al servidor de autenticación.
<code>dot1x timeout supp-timeout <i>segundos</i></code>	Establece el tiempo para la retransmisión de una trama de solicitud de EAP al cliente.

<code>dot1x timeout tx-period segundos</code>	Establece el número de segundos que el dispositivo espera una respuesta a una trama de identidad/solicitud - EAP, del cliente, antes de reenviar la solicitud.
<code>show dot1x [ethernet interfaz]</code>	Muestra el estado de 802.1X para el dispositivo o para la interfaz especificada.
<code>show dot1x users [username nombreusuario]</code>	Muestra los usuarios de 802.1X para el dispositivo.

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

```

console> enable

Console# show dot1x

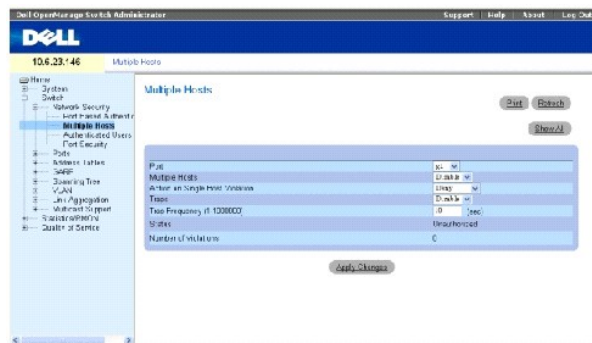
```

Interface	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
-----	-----	-----	-----	-----	-----
g1	Auto	Authorized	Ena	3600	Bob
g2	Auto	Authorized	Ena	3600	John
g3	Auto	Unauthorized	Ena	3600	Clark
g4	Force-auth	Authorized	Dis	3600	n/a

Configuración de la autenticación avanzada basada en puerto

La página [Multiple Hosts](#) (Varios sistemas principales) proporciona información para definir la configuración de la autenticación avanzada basada en puerto para puertos específicos. Para abrir la página [Multiple Hosts](#) (Varios sistemas principales), haga clic en Switch → Network Security → Multiple Hosts (Conmutador → Seguridad de la red → Varios sistemas principales).

Ilustración 7-82. Multiple Hosts (Varios sistemas principales)



Port (Puerto): El número de puerto para el que se habilita la autenticación avanzada basada en puerto.

Multiple Hosts (Varios sistemas principales): Activa o desactiva un solo sistema principal para que autorice el acceso al sistema a varios sistemas principales. Este parámetro tiene que estar activado para desactivar el filtro de entrada o utilizar la seguridad de bloqueo de puerto en el puerto seleccionado.

Action on Single Host Violation (Acción tras la infracción de un solo sistema principal): Define la acción que hay que aplicar a los paquetes que llegan en modo de un solo sistema principal, desde un sistema principal cuya dirección MAC no es la dirección MAC del cliente (solicitante). El campo **Action on Single Host Violation** (Acción tras la infracción de un solo sistema principal) sólo se puede definir si el campo **Multiple Hosts** (Varios sistemas principales) se define como **Disable** (Desactivar). Los valores de campo posibles son:

Permit (Permitir): Reenvía los paquetes de origen desconocido aunque no se obtiene la dirección MAC.

Deny (Denegar): Descarta los paquetes procedentes de un origen no obtenido. Éste es el valor predeterminado.

Shutdown (Apagar): Descarta el paquete procedente de cualquier origen no obtenido y bloquea el puerto. Los puertos permanecen bloqueados hasta que se activan o el dispositivo se restablece.

Traps (Capturas): Activa o desactiva el envío de capturas al sistema principal si se produce una infracción.

Trap Frequency (1-1000000) (Sec) (Frecuencia de las capturas [1-1000000] [seg]): Define el período de tiempo por el que se envían capturas al sistema principal. El campo **Trap Frequency (1-1000000)** (Frecuencia de las capturas [1-1000000]) sólo se puede definir si el campo **Multiple Hosts** (Varios sistemas principales) se define como **Disable** (Desactivar). El valor predeterminado es 10 segundos.

Status (Estado): El estado del sistema principal. Los valores de campo posibles son:

Unauthorized (No autorizado): Los clientes (solicitantes) tienen acceso completo al puerto.

Authorized (Autorizado): Los clientes (solicitantes) tienen acceso limitado al puerto.

No single-host (No un solo sistema principal): El campo **Multiple Hosts** (Varios sistemas principales) está activado.

Number of Violations (Número de infracciones): El número de paquetes que llegan a la interfaz en modo de sistema principal único, desde un sistema principal cuya dirección MAC no es la dirección MAC del cliente (solicitante).

Visualización de la [Tabla de varios sistemas principales](#)

1. Abra la página [Multiple Hosts](#) (Varios sistemas principales).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la [Multiple Hosts Table](#) (Tabla de varios sistemas principales):

Ilustración 7-83. Multiple Hosts Table (Tabla de varios sistemas principales)

Multiplic Hosts Table

[Refresh](#)

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations	
1	g1	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
2	g2	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
3	g3	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
4	g4	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
5	g5	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
5	g6	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
7	g7	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
9	g8	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
9	g9	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
10	g10	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
11	g11	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
12	g12	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
13	g13	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
11	g14	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
15	g15	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
16	g16	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
17	g17	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
18	g18	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
19	g19	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
20	g20	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
21	g21	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
22	g22	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
23	g23	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0
24	g24	<input type="checkbox"/>	Deny	<input type="checkbox"/>	10	Unauthorized	0

[Add Column](#)

Habilitación de varios sistemas principales mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para habilitar la autenticación avanzada basada en puerto tal como aparecen en la página [Multiple Hosts](#) (Varios sistemas principales).

Tabla 7-50. Comandos de la CLI para varios sistemas principales

Comando de la CLI	Description
<code>dot1x multiple-hosts</code>	Permite varios sistemas principales (clientes) en un puerto autorizado por 802.1X que tenga el comando de configuración de interfaces de control de puertos dot1x establecido en auto.
<code>dot1x single-host-violation {forward discard discard-shutdown} [trap segundos]</code>	Configura la acción que se debe realizar cuando una estación, cuya dirección MAC no es la dirección MAC del cliente (solicitante), intenta acceder a la interfaz.

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

```
Neyland# configure

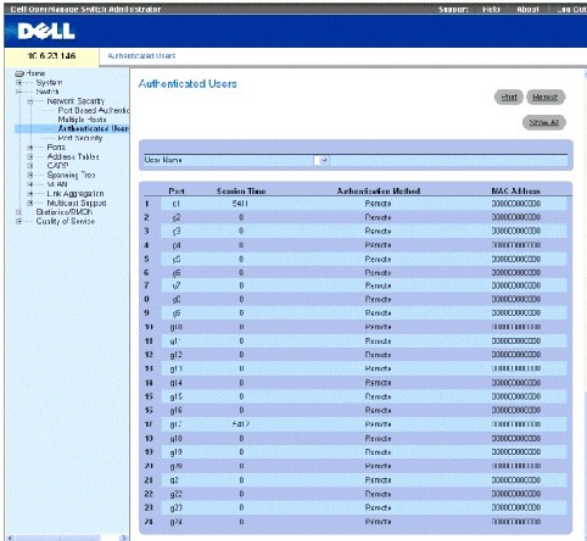
Neyland(config)# interface ethernet g1

Neyland(config-if)# dot1x multiple-hosts
```

Autenticación de usuarios

La página [Authenticated Users](#) (Usuarios autenticados) muestra las listas de acceso al puerto del usuario. Las listas de acceso del usuario se definen en la página Add User Name (Agregar nombre de usuario). Para abrir la página [Authenticated Users](#) (Usuarios autenticados), haga clic en Switch → Network Security → Authenticated Users (Commutador → Seguridad de la red → Usuarios autenticados).

Ilustración 7-84. Authenticated Users (Usuarios autenticados)



User Name (Nombre de usuario): Lista de los usuarios autorizados a través del servidor RADIUS.

Port (Puerto): Los números de puerto utilizados para la autenticación, por nombre de usuario.

Session Time (Tiempo de sesión): La cantidad de tiempo que el usuario lleva conectado al dispositivo. El formato de este campo es **Día:Hora:Segundos**, por ejemplo, 3 días: 2 horas: 4 minutos: 39 segundos.

Last Authentication (Última autenticación): La cantidad de tiempo que ha transcurrido desde que se autenticó al usuario por última vez. El formato de este campo es **Día:Hora:Minuto:Segundos**, por ejemplo, 3 días:2 horas: 4 minutos: 39 segundos.

Authentication Method (Método de autenticación): El método por el que se autenticó la última sesión. Los valores de campo posibles son:

Remote (Remoto): El usuario se ha autenticado desde un servidor remoto.

None (Ninguno): No se ha autenticado al usuario.

MAC Address (Dirección MAC): La dirección MAC del cliente (solicitante).

Visualización de la tabla de usuarios autenticados

1. Abra la página **Add User Name** (Agregar nombre de usuario).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Authenticated Users Table** (Tabla de usuarios autenticados):

Ilustración 7-85. Authenticated Users Table (Tabla de usuarios autenticados)



Autenticación de usuarios mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para autenticar usuarios tal como aparecen en la página Add User Name (Agregar nombre de usuario).

Tabla 7-51. Comandos de la CLI para agregar nombres de usuarios

Comando de la CLI	Description
<code>show dot1x users [username nombreusuario]</code>	Muestra los usuarios de 802.1X para el dispositivo.

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

console# show dot1x users					
Username	Session Time	Last Auth	Auth Method	MAC Address	Interface
-----	-----	-----	-----	-----	-----
Bob	1d3h	58m	Remote	00:08:3b:79:87:87	g1
John	8h19m	2m	None	00:08:3b:89:31:27	g2

Configuración de la seguridad de los puertos

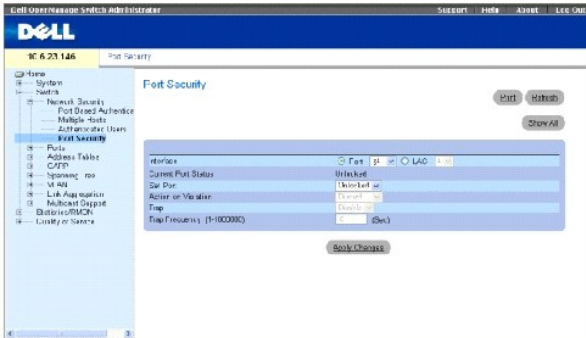
La seguridad de la red puede aumentarse limitando el acceso a un puerto específico sólo a los usuarios que dispongan de direcciones MAC específicas. Las direcciones MAC pueden obtenerse dinámicamente, hasta dicho punto, o pueden configurarse estáticamente. La seguridad de los puertos bloqueados supervisa tanto los paquetes recibidos como los obtenidos que se reciben en puertos específicos. El acceso a los puertos bloqueados está restringido a aquellos usuarios que tengan direcciones MAC específicas. Dichas direcciones se definen manualmente en el puerto o se obtienen en dicho puerto hasta el punto en que se bloquea. Cuando se recibe un paquete en un puerto bloqueado y la dirección MAC de origen del paquete no está vinculada a dicho puerto (ya sea porque se ha obtenido en un puerto distinto o bien porque resulta desconocida para el sistema), se llama al mecanismo de protección y se pueden proporcionar varias opciones. Los paquetes no autorizados que llegan a un puerto bloqueado:

- 1 Se reenvían
- 1 Se rechazan sin captura
- 1 Se rechazan con una captura
- 1 El puerto de admisión se inhabilita

La seguridad del puerto bloqueado también habilita el almacenamiento de una lista de direcciones MAC en el archivo de configuración. Esta lista puede restaurarse una vez restablecido el dispositivo.

Los puertos inhabilitados se activan desde la página [Port Parameters](#) (Parámetros de puerto), consulte el apartado ["Definición de los parámetros de puerto"](#). Para abrir la página [Port Security](#) (Seguridad del puerto), haga clic en Switch→ Network Security→ Port Security (Conmutador → Seguridad de la red → Seguridad del puerto).

Ilustración 7-86. Port Security (Seguridad del puerto)



Interface (Interfaz): El tipo de interfaz seleccionada en la que se activa el puerto bloqueado.

Port (Puerto): El tipo de interfaz seleccionada es un puerto.

LAG: El tipo de interfaz seleccionada es un LAG.

Current Port Status (Estado del puerto actual): El estado del puerto configurado actualmente.

Set Port (Establecer puerto): El puerto está bloqueado o desbloqueado. Los valores de campo posibles son:

Unlocked (Desbloqueado): Desbloquea el puerto. Éste es el valor predeterminado.

Locked (Bloqueado): Bloquea el puerto.

Action on Violation (Acción tras infracción): La acción que se aplica a los paquetes que llegan a un puerto bloqueado. Los valores de campo posibles son:

Forward (Reenviar): Reenvía los paquetes de origen desconocido aunque no se obtiene la dirección MAC.

Discard(Descartar): Descarta los paquetes procedentes de un origen no obtenido. Éste es el valor predeterminado.

Shutdown (Apagar): Descarta el paquete procedente de cualquier origen no obtenido y bloquea el puerto. Los puertos permanecen bloqueados hasta que se activan o el dispositivo se restablece.

Trap (Captura): Habilita el envío de capturas cuando se recibe un paquete en un puerto bloqueado.

Trap Frequency (1-1000000) (Frecuencia de capturas [1-1000000]): La cantidad de tiempo (en segundos) que transcurre entre las capturas. Este campo sólo se aplica a los puertos bloqueados. El valor predeterminado es 10 segundos.

Definición de un puerto bloqueado

1. Abra la página [Port Security](#) (Seguridad del puerto).
2. Seleccione un tipo de interfaz y un número.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto bloqueado se agrega a la [Port Security Table](#) (Tabla de seguridad del puerto), y el dispositivo se actualiza.

Visualización de la tabla de puertos bloqueados

1. Abra la página [Port Security](#) (Seguridad del puerto).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la [Port Security Table](#) (Tabla de seguridad del puerto):

Los puertos bloqueados también se pueden definir desde la Locked Ports Table (Tabla de puertos bloqueados) así como desde la página [Port Security](#) (Seguridad del puerto).

Ilustración 7-87. Port Security Table (Tabla de seguridad del puerto)

The screenshot shows the 'Port Security Table' interface. At the top, there is a 'Refresh' button and a 'Copy Parameters from' dropdown menu set to 'Port: g1'. Below this is a table with columns: Port, Current Port Status, Set Port, Action, Trap, Trap Frequency, and Copy to Select All. The table lists 24 ports (g1-g24) and 8 LAGs (LAG 1-8). Each row has dropdown menus for 'Current Port Status', 'Set Port', 'Action', and 'Trap'. The 'Trap Frequency' column has a numeric input field. A 'Copy to Select All' checkbox is present at the end of each row. At the bottom of the table, there is an 'Apply Changes' button.

Port	Current Port Status	Set Port	Action	Trap	Trap Frequency	Copy to Select All
1	g1 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
2	g2 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
3	g3 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
4	g4 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
5	g5 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
6	g6 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
7	g7 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
8	g8 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
9	g9 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
10	g10 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
11	g11 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
12	g12 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
13	g13 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
14	g14 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
15	g15 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
16	g16 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
17	g17 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
18	g18 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
19	g19 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
20	g20 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
21	g21 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
22	g22 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
23	g23 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
24	g24 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
Global System LAGs						
25	LAG 1 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
26	LAG 2 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
27	LAG 3 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
28	LAG 4 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
29	LAG 5 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
30	LAG 6 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
31	LAG 7 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
32	LAG 8 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>

Configuración de la seguridad de los puertos bloqueados mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar la seguridad de los puertos bloqueados tal como aparecen en la página [Port Security](#) (Seguridad del puerto).

Tabla 7-52. Comandos de la CLI para la seguridad del puerto

Comando de la CLI	Description
shutdown	Inhabilita interfaces.
set interface active { ethernet <i>interface</i> port-channel <i>port-channel-number</i> }	Reactiva una interfaz que está apagada por motivos de seguridad de los puertos.
port security [forward discard discard-shutdown] [trap <i>segundos</i>]	Bloquea la obtención de nuevas direcciones en una interfaz.
show ports security { ethernet <i>interface</i> port-channel <i>port-channel-number</i> }	Muestra el estado de bloqueo de los puertos.

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

Console # show ports security					
Port	Status	Action	Trap	Frequency	Counter
---	-----	-----	-----	-----	-----
-					-
g7	Unlocked	Discard	Enable	100	88
g8	Unlocked	Discard, Shutdown	Disable		
g3	Unlocked	-	-	-	-

Configuración de los puertos

La página Ports (Puertos) contiene enlaces a las páginas de funciones de los puertos incluidas varias funciones avanzadas como, por ejemplo, el control de tormentas y la duplicación de puertos. Para abrir la página Ports (Puertos), haga clic en Switch → Ports (Conmutador → Puertos).

Definición de los parámetros de puerto

La página [Port Configuration](#) (Configuración de puertos) contiene los campos para definir los parámetros de los puertos. Para abrir la página [Port Configuration](#) (Configuración de puertos), haga clic en Switch → Ports → Port Configuration (Conmutador → Puertos → Configuración de puertos) en la vista de árbol.

Ilustración 7-88. Port Configuration (Configuración de puertos)



Port (Puerto): El número de puerto para el que se definen los parámetros de puerto.

Description (Descripción): Una breve descripción de la interfaz como, por ejemplo, Ethernet. Este campo puede tener de 0 a 64 caracteres.

Port Type (Tipo de puerto): El tipo de puerto.

Admin Status (Estado admin): Activa o desactiva el reenvío de tráfico a través del puerto. El nuevo estado del puerto se muestra en el campo **Current Port Status** (Estado actual del puerto).

Current Port Status (Estado actual del puerto): Especifica si el puerto está actualmente operativo o no.

Re-Activate Port (Reactivar puerto): Reactiva un puerto si éste se ha desactivado a través de la opción de seguridad de puerto bloqueado.

Operational Status (Estado operativo): El estado operativo del puerto. Los valores posibles del campo son:

Suspended (Suspendido): El puerto está activo actualmente y no recibe ni transmite tráfico.

Active (Activo): El puerto está activo actualmente y recibe y transmite tráfico.

Disable (Desactivado): El puerto está actualmente desactivado y no recibe ni transmite tráfico.

Admin Speed (Velocidad admin): La velocidad configurada del puerto. El tipo de puerto determina qué opciones de configuración de velocidad hay disponibles. La velocidad admin sólo se puede designar cuando la negociación automática está desactivada en el puerto configurado.

Current Port Speed (Velocidad actual del puerto): La velocidad del puerto actualmente configurado (en bps).

Admin Duplex (Dúplex admin): El modo dúplex del puerto puede ser **Full** (Completo) o **Half** (Medio). **Full** (Completo) indica que la interfaz admite la transmisión entre el dispositivo y su compañero de vínculo en ambas direcciones simultáneamente. **Half** (Medio) indica que la interfaz admite la transmisión entre el dispositivo y el cliente en una sola dirección cada vez.

Current Duplex Mode (Modo dúplex actual): El modo dúplex del puerto actualmente configurado.

Auto Negotiation (Negociación automática): Activa la negociación automática en el puerto. La negociación automática es un protocolo entre dos partes del vínculo que permite que un puerto comunique su velocidad de transmisión, modo dúplex y capacidades de control de flujo a la otra parte.

Current Auto Negotiation (Negociación automática actual): La negociación automática actualmente configurada.

Back Pressure (Contrapresión): Habilita el modo de contrapresión en el puerto. El modo de contrapresión se utiliza con el modo dúplex medio para inhabilitar la recepción de mensajes en los puertos.

Current Back Pressure (Contrapresión actual): La configuración de contrapresión actualmente configurada.

Flow Control (Control de flujo): Habilita o inhabilita el control de flujo o habilita la negociación automática del control de flujo en el puerto. Funciona cuando el puerto está en modo de dúplex **completo**.

Current Flow Control (Control de flujo actual): La configuración actual del control de flujo.

MDI/MDIX: Permite que el dispositivo descifre entre cables cruzados y no cruzados.

Los concentradores y conmutadores se cablean deliberadamente en el sentido opuesto al cableado de las estaciones finales, de modo que cuando se conecta un concentrador o conmutador a una estación final, se puede utilizar un cable Ethernet directo y los pares coinciden correctamente. Cuando se conectan dos

concentradores/conmutadores entre sí o dos estaciones finales entre sí, se utiliza un cable cruzado para asegurar que se conecten los pares correctos. Los valores de campo posibles son:

Auto (Automático): Se utiliza para detectar automáticamente el tipo de cable.

MDI (Media Dependent Interface) MDI (Interfaz dependiente de los soportes): Se utiliza para estaciones finales.

MDIX (Media Dependent Interface with Crossover) MDIX (Interfaz dependiente de los soportes con cable cruzado): Se utiliza para concentradores y conmutadores.

Current MDI/MDIX (MDI/MDIX actual): Los valores de MDI/MDIX del dispositivo configurado actualmente.

LAG: Especifica si el puerto forma parte de un LAG.

Definición de los parámetros de puerto

1. Abra la página [Port Configuration](#) (Configuración de puertos).
2. Seleccione un puerto en el campo **Port** (Puerto).
3. Defina los campos restantes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del puerto se guardan en el dispositivo.

Modificación de los parámetros del puerto

1. Abra la página [Port Configuration](#) (Configuración de puertos).
2. Seleccione un puerto en el campo **Port** (Puerto).
3. Modifique los campos restantes.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del puerto se guardan en el dispositivo.

Visualización de la tabla de configuración de puertos:

1. Abra la página [Port Configuration](#) (Configuración de puertos).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la [Ports Configuration Table](#) (Tabla de configuración de puertos):

Ilustración 7-89. Ports Configuration Table (Tabla de configuración de puertos)

Port Configuration Table

Port	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control	MDI/MDIX	LEDs
1	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
2	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
3	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
4	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
5	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
6	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
7	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
8	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
9	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
10	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
11	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
12	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
13	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
14	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
15	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
16	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
17	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
18	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
19	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
20	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
21	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
22	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
23	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
24	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
25	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
26	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
27	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
28	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
29	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
30	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
31	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
32	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
33	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
34	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
35	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
36	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
37	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
38	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
39	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
40	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
41	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
42	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
43	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
44	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
45	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
46	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
47	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
48	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
49	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
50	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
51	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
52	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
53	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
54	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
55	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
56	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
57	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
58	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
59	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
60	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
61	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
62	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
63	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
64	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
65	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
66	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
67	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
68	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
69	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
70	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
71	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
72	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
73	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
74	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
75	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
76	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
77	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
78	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
79	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
80	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
81	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
82	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
83	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
84	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
85	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
86	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
87	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
88	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
89	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
90	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
91	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
92	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
93	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
94	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
95	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
96	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
97	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
98	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
99	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
100	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A

Configuración de los puertos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los puertos tal como aparecen en la [Ports Configuration Table](#) (Tabla de configuración de puertos).

Tabla 7-53. Comandos de la CLI para la configuración de puertos

Comando de la CLI	Descripción
<code>interface ethernet interfaz</code>	Entra en el modo de configuración de interfaz para configurar una interfaz de tipo Ethernet.
<code>description cadena</code>	Agrega una descripción a una configuración de interfaz.
<code>shutdown</code>	Inhabilita las interfaces que forman parte del contexto establecido actualmente.
<code>set interface active {ethernet interfaz port-channel número-canal-puerto}</code>	Reactiva una interfaz que está apagada por motivos de seguridad.
<code>speed bps</code>	Configura la velocidad de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
<code>autobaud</code>	Establece la línea para la detección automática de la velocidad en baudios.
<code>duplex {half full}</code>	Configura el funcionamiento dúplex completo o dúplex medio de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
<code>negotiation</code>	Habilita el funcionamiento con negociación automática para los parámetros de velocidad y dúplex de una interfaz determinada.
<code>back-pressure</code>	Habilita la contrapresión en una interfaz determinada.
<code>flowcontrol {auto on off rx tx}</code>	Configura el control de flujo en una interfaz determinada.
<code>mdi {on auto}</code>	Habilita el cable cruzado automático en una interfaz o un canal de puertos determinado.
<code>show interfaces configuration [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra el estado de la configuración de todas las interfaces configuradas.
<code>show interfaces status [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra el estado de todas las interfaces configuradas.
<code>show interfaces description [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra la descripción de todas las interfaces configuradas.

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

```

Console (config)# interface ethernet g5

Console(config-if)#description RD SW#3
    
```

```

Console (config-if)# shutdown

Console (config-if)# no shutdown

Console(config-if)# speed 100

Console (config-if)# duplex full

Console (config-if)# negotiation

Console (config-if)# back-pressure

Console (config-if)# flowcontrol on

Console (config-if)# mdix auto

Console(config-if)#exit

Console(config)#exit

Console# show interfaces configuration ethernet g5

```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
----	----	-----	-----	----	-----	-----	-----	----
g5	1G	Full	100	Enabled	On	Up	Enable	Auto
console#								

```

console# show interfaces status ethernet g5

```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	----	-----	-----	----	-----	-----	-----	----
g5	1G	Full	100	Enabled	On	Up	Disabled	on

console#								

Console# show interfaces status								
Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
---	---	-----	-----	---	-----	-----	-----	-----
g1	1G	Full	100	Auto	On	Up	Enable	On
g1	100	Full	100	Off	Off	Down	Disable	Off
g2	100	Full	1000	Off	Off	Up	Disable	On
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	---	-----	---	---	-----	-----	-----	
1	1000	Full	1000	Off	Off	Disable	Up	

Definición de los parámetros del LAG

La página [LAG Configuration](#) (Configuración de LAG) contiene campos para configurar los parámetros de los LAG configurados. El dispositivo admite hasta ocho puertos por LAG y ocho LAG por sistema.

Para obtener información sobre los LAG y la asignación de puertos a los LAG, consulte el apartado [Agregado de puertos](#).

Para abrir la página [LAG Configuration](#) (Configuración de LAG), haga clic en Switch→ Ports→ LAG Configuration (Conmutador → Puertos → Configuración de LAG) en la vista de árbol.


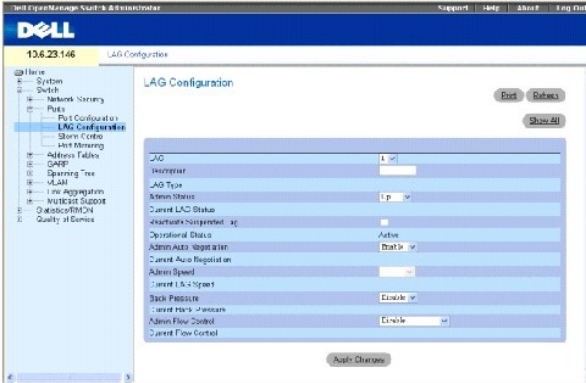
 **NOTA:** Si la configuración del puerto se modifica mientras éste es miembro de un LAG, el cambio de configuración sólo se hace efectivo una vez que se ha eliminado el puerto del LAG.

Ilustración 7-90. LAG Configuration (Configuración de LAG)



LAG: El número de LAG.

Description (Descripción): Proporciona una descripción del LAG configurado definida por el usuario. Este campo puede tener de 0 a 64 caracteres.

LAG Type (Tipo de LAG): Los tipos de puerto de que consta el LAG.

Admin Status (Estado admin): Habilita o inhabilita el reenvío de tráfico a través del LAG seleccionado.

Current LAG Status (Estado actual del LAG): Indica si el LAG está operativo actualmente.

Re-Activate Suspended LAG (Reactivar LAG suspendido): Reactiva un LAG que se había suspendido.

Operational Status (Estado operativo): Estado operativo del LAG.

Admin Auto Negotiation (Negociación automática admin): Habilita o inhabilita la negociación automática en el LAG. La negociación automática es un protocolo entre dos partes del vínculo que permite que un LAG comunique su velocidad de transmisión, modo dúplex y capacidades de control de flujo (el valor predeterminado es inhabilitado) a la otra parte.

Current Auto Negotiation (Negociación automática actual): La negociación automática actualmente configurada.

Admin Speed (Velocidad admin): La velocidad a la cual está funcionando el LAG.

Current LAG Speed (Velocidad actual del LAG): La velocidad configurada actualmente a la cual funciona el LAG.

Admin Back Pressure (Contrapresión admin): Habilita o inhabilita el modo de contrapresión en el LAG. El modo de contrapresión es eficaz en los puertos que funcionan a dúplex medio en el LAG.

Current Back Pressure (Contrapresión actual): La configuración de contrapresión actualmente configurada.

Admin Flow Control (Control de flujo admin): Habilita o inhabilita el control de flujo o habilita la negociación automática del control de flujo en el LAG. El modo de control de flujo es eficaz en los puertos que funcionan a dúplex completo en el LAG.

Current Flow Control (Control de flujo actual): La configuración del control de flujo designada por el usuario.

Definición de los parámetros del LAG

1. Abra la página [LAG Configuration](#) (Configuración de LAG).
2. Seleccione un LAG en el campo **LAG**.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG se guardan en el dispositivo.

Modificación de los parámetros de LAG

1. Abra la página [LAG Configuration](#) (Configuración de LAG).
2. Seleccione un LAG en el campo **LAG**.
3. Modifique los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG se guardan en el dispositivo.

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).

Se abre la [LAG Configuration Table](#) (Tabla de configuración de LAG):

Ilustración 7-91. LAG Configuration Table (Tabla de configuración de LAG)

LAG Configuration Table

Refresh

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Eth Port	Flow Control
1	1	Uo	Up	100	Enable	Disable	Disable
2	2	Uo	Up	100	Enable	Disable	Disable
3	3	Uo	Up	100	Enable	Disable	Disable
4	4	Uo	Up	100	Enable	Disable	Disable
5	5	Uo	Up	100	Enable	Disable	Disable
6	6	Uo	Up	100	Enable	Disable	Disable
7	7	Uo	Up	100	Enable	Disable	Disable
8	8	Uo	Up	100	Enable	Disable	Disable

Apply Changes

Configuración de LAG con comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los LAG tal como aparecen en la página [LAG Configuration](#) (Configuración de LAG).

Tabla 7-54. Comandos de la CLI para la configuración de LAG

Comando de la CLI	Description
<code>interface port-channel número-canal-puerto</code>	Entra en el modo de configuración de interfaz de un canal de puertos específico.
<code>description cadena</code>	Agrega una descripción a una configuración de interfaz.
<code>shutdown</code>	Inhabilita las interfaces que forman parte del contexto establecido actualmente.

<code>speed bps</code>	Configura la velocidad de una interfaz Ethernet determinada cuando no se utiliza la negociación automática.
<code>autobaud</code>	Establece la línea para la detección automática de la velocidad en baudios.
<code>negotiation</code>	Habilita el funcionamiento con negociación automática para los parámetros de velocidad y dúplex de una interfaz determinada.
<code>back-pressure</code>	Habilita la contrapresión en una interfaz determinada.
<code>flowcontrol { auto on off rx tx }</code>	Configura el control de flujo en una interfaz determinada.
<code>show interfaces configuration [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra el estado de la configuración de todas las interfaces configuradas.
<code>show interfaces status [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra el estado de todas las interfaces configuradas.
<code>show interfaces description [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra la descripción de todas las interfaces configuradas.
<code>show interfaces port-channel [número-canal-puerto]</code>	Muestra información de canal de puertos (qué puertos son miembros de dicho canal de puertos, y si están o no activos actualmente).

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

<pre> console(config-if)# channel-group 1 mode on console(config-if)# exit console(config)# interface range e g21-24 console(config-if)# channel-group 1 mode on console(config-if)# ex console(config)# interface ethernet g5 console(config-if)# channel-group 2 mode on console(config-if)# exit console(config)# exit </pre>	
<pre> console# show interfaces port-channel </pre>	
Channel	Ports
-----	-----
ch1	Inactive: g(21-24)
ch2	Active: g5
ch3	

ch4	
ch5	
ch6	
ch7	
ch8	
console#	

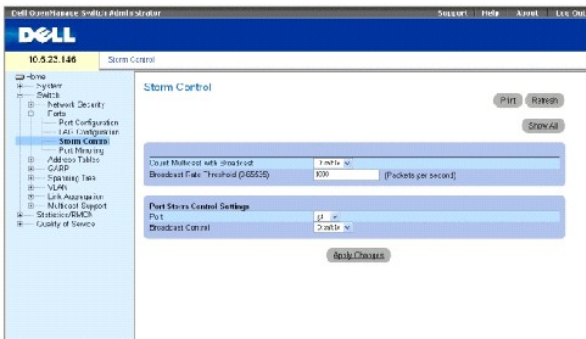
Habilitación del control de tormentas

Una tormenta de difusión es el resultado de una cantidad excesiva de mensajes transmitidos simultáneamente a través de una red mediante un único puerto. Las respuestas a mensajes reenviados se cargan en la red, lo que provoca una tensión en los recursos de ésta o que se agote el tiempo de espera.

El sistema mide la velocidad de las tramas de difusión y de multidifusión entrantes por separado en cada puerto y descarta las tramas cuando la velocidad supera un valor definido por el usuario.

La página [Storm Control](#) (Control de tormentas) proporciona los campos para habilitar y configurar el control de tormentas. Para abrir la página [Storm Control](#) (Control de tormentas), haga clic en Switch→ Ports→ Storm Control (Conmutador → Puertos → Control de tormentas) en la vista de árbol.

Ilustración 7-92. Storm Control (Control de tormentas)



Count Multicast with Broadcast (Contar multidifusión con difusión): Efectúa un recuento del tráfico de difusión y multidifusión. Los valores de campo posibles son:

- **Enable** (Activar): Efectúa un recuento del tráfico de difusión y multidifusión.
- **Disable** (Desactivar): Efectúa un recuento únicamente del tráfico de difusión.

Broadcast Rate Threshold (1-1000000) (Umbral de velocidad de difusión [1-1000000]): La velocidad máxima (paquetes por segundo) a la que se reenvían los paquetes desconocidos. El intervalo es 0-1000000. El valor predeterminado es cero. Todos los valores se redondean al valor más cercano a 64 Kbps. Si el valor del campo es inferior a 64 Kbps, el valor se redondea hasta 64 Kbps, con la excepción del valor cero.

Port (Puerto): El puerto desde el cual se habilita el control de tormentas.

Broadcast Control (Control de difusión): Habilita o inhabilita el reenvío de tipos de paquetes de difusión en el dispositivo.

Habilitación del control de tormentas en el dispositivo

1. Abra la página [Storm Control](#) (Control de tormentas).
2. Seleccione una interfaz en la que se implementará el control de tormentas.
3. Defina los campos.
4. Haga clic en **Show All** (Mostrar todo).

El control de tormentas está habilitado en el dispositivo.

Modificación de los parámetros del puerto de control de tormentas

1. Abra la página [Storm Control](#) (Control de tormentas).
2. Modifique los campos.
3. Haga clic en **Show All** (Mostrar todo).

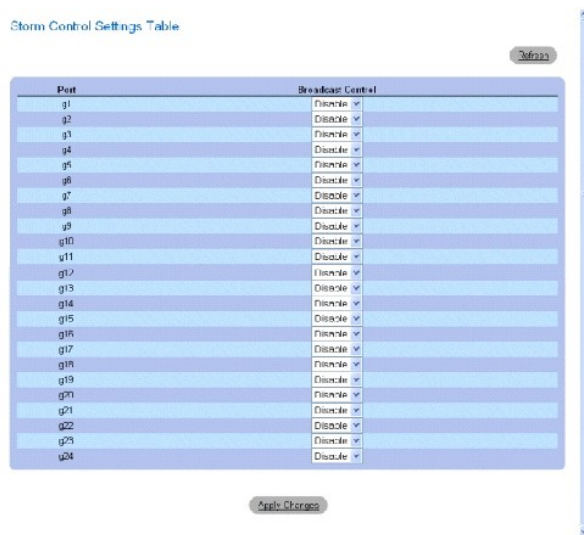
Los parámetros del puerto de control de tormentas se guardan en el dispositivo.

Visualización de la tabla de parámetros de puerto

1. Abra la página [Storm Control](#) (Control de tormentas).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la [Storm Control Settings Table](#) (Tabla de configuración del control de tormentas):

Ilustración 7-93. Storm Control Settings Table (Tabla de configuración del control de tormentas)



Storm Control Settings Table

Port	Storm Control
g1	Disable
g2	Disable
g3	Disable
g4	Disable
g5	Disable
g6	Disable
g7	Disable
g8	Disable
g9	Disable
g10	Disable
g11	Disable
g12	Disable
g13	Disable
g14	Disable
g15	Disable
g16	Disable
g17	Disable
g18	Disable
g19	Disable
g20	Disable
g21	Disable
g22	Disable
g23	Disable
g24	Disable

Configuración del control de tormentas mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar el control de tormentas tal como se muestran en la página [Storm Control](#) (Control de tormentas).

Tabla 7-55. Comandos de la CLI para el control de tormentas

Comando de la CLI	Descripción
<code>port storm-control include-multicast</code>	Habilita al dispositivo para que pueda contar paquetes de multidifusión junto con los paquetes de difusión.
<code>port storm-control broadcast enable</code>	Habilita el control de tormentas de difusión.
<code>port storm-control broadcast rate <i>velocidad</i></code>	Configura la velocidad de difusión máxima.
<code>show ports storm-control [ethernet <i>interfaz</i>]</code>	Muestra la configuración del control de tormentas.

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

```

console> enable

console# configure

Console(config)# port storm-control include-multicast

Console(config)# port storm-control broadcast rate 8000

Console (config)# interface ethernet g1

Console(config-if)# port storm-control broadcast enable

Console(config-if)# end

Console# show ports storm-control

```

Port	Broadcast Storm control [Packets/sec]
-----	-----
g1	8000
g2	Disabled
g4	Disabled

Definición de sesiones de duplicación de puertos

La duplicación de puertos supervisa y duplica el tráfico de red mediante el reenvío de copias de paquetes entrantes y salientes desde un puerto a un puerto de supervisión.

La duplicación de puertos se configura seleccionando un puerto específico para copiar todos los paquetes y diferentes puertos desde los que se copian los paquetes. Antes de configurar la duplicación de puertos, tenga en cuenta lo siguiente:

- 1 Un puerto supervisado no puede funcionar más rápido que el puerto de supervisión.
- 1 Todos los paquetes RX/TX deben supervisarse para el mismo puerto.

Las restricciones siguientes se aplican a los puertos configurados como puertos de destino:

- 1 Los puertos no pueden estar configurados como puertos de origen.

- 1 Los puertos no pueden ser miembros de un LAG.
- 1 Las interfaces IP no se configuran en el puerto.
- 1 El GVRP no se activa en el puerto.
- 1 El puerto no es miembro de una VLAN.
- 1 Sólo se puede definir un puerto de destino.

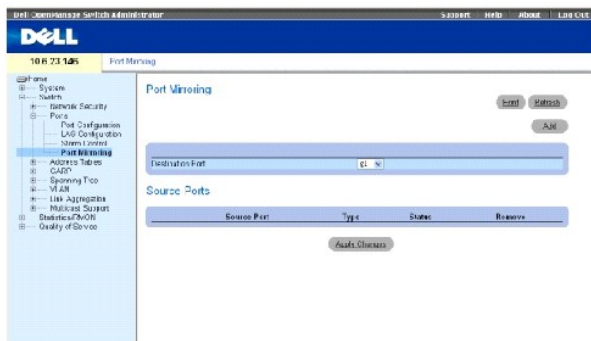
Las siguientes restricciones se aplican a los puertos configurados como puertos de origen:

- 1 Los puertos de origen no pueden ser miembros de un LAG.
- 1 Los puertos no pueden estar configurados como puertos de destino.
- 1 Todos los paquetes deben tener una etiqueta cuando se transmiten desde el puerto de destino.
- 1 Todos los paquetes RX/TX deben supervisarse para el mismo puerto.

Para abrir la página [Port Mirroring](#) (Duplicación de puertos), haga clic en **Switch**→ **Ports**→ **Port Mirroring** (Conmutador→ Puertos→ Duplicación de puertos) en la vista de árbol.

NOTA: Cuando un puerto está configurado para que sea un puerto de destino de una sesión de duplicación de puertos, se suspenden todas las operaciones de éste. Esto incluye el árbol extensible y LACP.

Ilustración 7-94. Port Mirroring (Duplicación de puertos)



Destination Port (Puerto de destino): El número de puerto en el que se copia el tráfico del puerto.

Source Port (Puerto de origen): Define el número de puerto desde el que se duplica el tráfico del puerto.

Type (Tipo): Indica si el puerto de origen es de recepción (RX), de transmisión (TX), o de las dos cosas.

Status (Estado): Indica si el puerto está supervisado actualmente (**Active**) o no está supervisado (**Ready**).

Remove (Eliminar): Si se selecciona esta opción, se elimina la sesión de duplicación de puertos.

Adición de una sesión de duplicación de puertos

- 1. Abra la página [Port Mirroring](#) (Duplicación de puertos).
- 2. Haga clic en **Agregar**.

Se abre la página **Add Source Port** (Agregar puerto de origen).

- 3. Seleccione el puerto de destino en el menú descendente **Destination Port** (Puerto de destino).

4. Seleccione el puerto de origen en el menú descendente **Source Port** (Puerto de origen).
5. Defina el campo **Type** (Tipo).
6. Haga clic en **Apply Changes** (Aplicar cambios).

Se define el nuevo puerto de origen y el dispositivo se actualiza.

Supresión de un puerto de copia desde una sesión de duplicación de puertos

1. Abra la página [Port Mirroring](#) (Duplicación de puertos).
2. Seleccione la casilla de verificación **Remove** (Eliminar).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La sesión de duplicación de puertos seleccionada se suprime y el dispositivo se actualiza.

Configuración de una sesión de duplicación de puertos mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar una sesión de duplicación de puertos tal como aparecen en la página [Port Mirroring](#) (Duplicación de puertos).

Tabla 7-56. Comandos de la CLI para la duplicación de puertos

Comando de la CLI	Descripción
<code>port monitor src-interface [rx tx]</code>	Inicia una sesión de supervisión de puertos.

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

```

Console (config)# interface ethernet g1

Console(config-if)# port monitor g8

Console# show ports monitor

```

Source Port	Destination Port	Type	Status	VLAN Tagging
-----	-----	-----	-----	-----
g8	g1	RX, TX	Active	No
g2	g8	RX, TX	Active	No
g18	g8	Rx	Active	No

Configuración de las tablas de direcciones

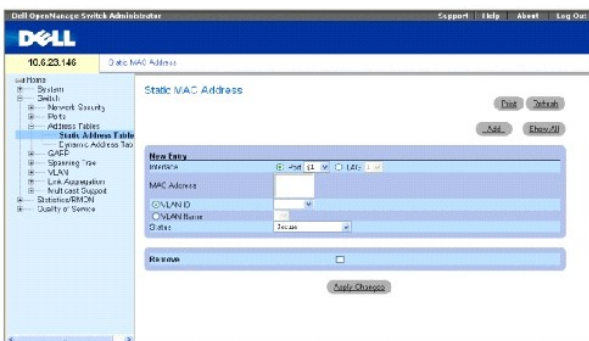
Las direcciones MAC se almacenan en bases de datos de direcciones estáticas o de direcciones dinámicas. Un paquete dirigido a un destino almacenado en una de las bases de datos se reenvía de inmediato al puerto. Las tablas de direcciones estáticas y dinámicas se pueden ordenar por interfaz, por VLAN y por tipo de interfaz. Las direcciones MAC se obtienen dinámicamente a medida que los paquetes de los orígenes llegan al dispositivo. Las direcciones también se asocian a los puertos mediante la obtención de los puertos desde la dirección de origen de la trama. Las tramas que se dirigen a una dirección MAC de destino

que no esté asociada a ningún puerto inundan todos los puertos de la VLAN relevante. Las direcciones estáticas se configuran manualmente. Para evitar que la tabla de direcciones se desborde, se borran las direcciones MAC dinámicas en las que no ha habido tráfico durante un período de tiempo determinado. Para abrir la página [Address Tables](#) (Tablas de direcciones), haga clic en **Switch**→ **Address Table** (Conmutador→ Tabla de direcciones) en la vista de árbol.

Definición de direcciones estáticas

La página [Static MAC Address](#) (Dirección MAC estática) contiene una lista de las direcciones MAC estáticas. En la página [Static MAC Address](#) (Dirección MAC estática) se pueden agregar y eliminar direcciones estáticas. Además, se pueden definir varias direcciones MAC para un solo puerto. Para abrir la página [Static MAC Address](#) (Dirección MAC estática), haga clic en **Switch**→ **Address Table**→ **Static Address** (Conmutador→ Tabla de direcciones→ Dirección estática) en la vista de árbol.

Ilustración 7-95. Static MAC Address (Dirección MAC estática)



Interface (Interfaz): El puerto o LAG específico al que se aplica la dirección MAC estática.

MAC Address (Dirección MAC): La dirección MAC indicada en la lista de direcciones estáticas actuales.

VLAN ID (ID de VLAN): El valor del ID de la VLAN conectada a la dirección MAC.

VLAN Name (Nombre de VLAN): Nombre de VLAN definido por el usuario.

Status (Estado): El estado de la dirección MAC. Los valores posibles son:

Secure (Segura): Garantiza que no se suprima una dirección MAC de puerto bloqueado.

Permanent (Permanente): La dirección MAC es permanente.

Delete on Reset (Suprimir al restablecer): La dirección MAC se suprime al restablecer el dispositivo.

Delete on Timeout (Suprimir al agotarse el tiempo de espera): La dirección MAC se suprime cuando transcurre el tiempo de espera especificado.

Remove (Eliminar): Si se selecciona esta opción, se elimina la dirección MAC de la tabla de direcciones MAC.

Adición de una dirección MAC estática

1. Abra la página [Static MAC Address](#) (Dirección MAC estática).
2. Haga clic en **Agregar**.

Se abre la página **Add Static MAC Address** (Agregar dirección MAC estática).

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

La nueva dirección estática se agrega a la tabla **Static MAC Address** (Dirección MAC estática), y el dispositivo se actualiza.

Modificación de una dirección estática de la tabla de direcciones MAC estáticas

1. Abra la página [Static MAC Address](#) (Dirección MAC estática).
2. Modifique los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección estática MAC se modifica, y el dispositivo se actualiza.

Eliminación de una dirección estática de la tabla de direcciones estáticas

1. Abra la página [Static MAC Address](#) (Dirección MAC estática).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la página **Static MAC Address Table** (Tabla de direcciones MAC estáticas).

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

La dirección estática seleccionada se suprime y el dispositivo se actualiza.

Configuración de los parámetros de direcciones estáticas mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar los parámetros de direcciones estáticas tal como aparecen en la página [Static MAC Address](#) (Dirección MAC estática).

Tabla 7-57. Comandos de la CLI para las direcciones estáticas

Comando de la CLI	Descripción
<code>bridge address dirección MAC { ethernet interfaz port-channel número-canal-puerto } [permanent delete-on-reset delete-on-timeout secure]</code>	Agrega una dirección de origen de estación de nivel MAC estática a la tabla de puentes.
<code>show bridge address-table [vlan vlan] [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra las entradas en la base de datos de reenvío de puente.

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

Console# show bridge address-table			
Aging time is 300 sec			
vlan	mac address	port	type
----	-----	----	-----

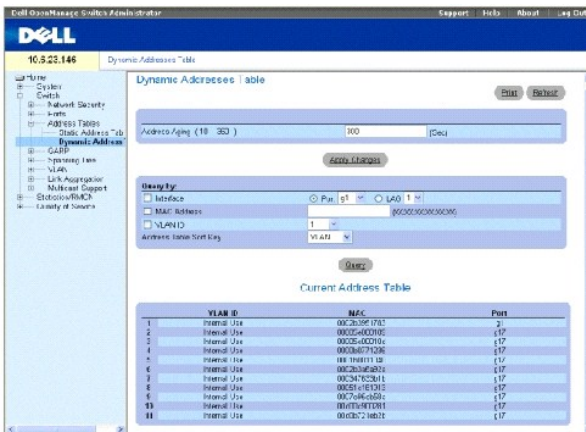
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g9	static
g8	00:10:0D:98:37:88	g8	dynamic

Visualización de direcciones dinámicas

La [Dynamic Address Table](#) (Tabla de direcciones dinámicas) contiene campos para consultar información en la tabla de direcciones dinámicas, incluido el tipo de interfaz, las direcciones MAC, la VLAN y la ordenación de las tablas. Los paquetes reenviados a una dirección almacenada en la tabla de direcciones se reenvían directamente a esos puertos. La [Dynamic Address Table](#) (Tabla de direcciones dinámicas) también contiene información sobre el tiempo de caducidad antes de que una dirección MAC dinámica se borre, e incluye parámetros para consultar y ver la lista de direcciones dinámicas. La tabla de direcciones actuales contiene parámetros de direcciones dinámicas que se utilizan para reenviar directamente los paquetes a los puertos.

Para abrir la [Dynamic Address Table](#) (Tabla de direcciones dinámicas), haga clic en **Switch** → **Address Table** → **Dynamic Addresses Table** (Conmutador → Tabla de direcciones → Tabla de direcciones dinámicas) en la vista de árbol.

Ilustración 7-96. Dynamic Address Table (Tabla de direcciones dinámicas)



Address Aging (10-360) (Caducidad de las direcciones [10-360]): Especifica la cantidad de tiempo que la dirección MAC permanece en la [Dynamic Address Table](#) (Tabla de direcciones dinámicas) antes de caducar si no se detecta tráfico desde el origen. El valor predeterminado es 300 segundos.

Interface (Interfaz): Especifica la interfaz para la que se consulta la tabla. Se puede seleccionar entre dos tipos de interfaces.

Port (Puerto): Especifica los números de puerto para los que se consulta la tabla.

LAG: Especifica el LAG para el que se consulta la tabla.

MAC Address (Dirección MAC): Especifica la dirección MAC para la que se consulta la tabla.

VLAN ID (ID de VLAN): El ID de la VLAN para el que se consulta la tabla.

Address Table Sort Key (Clave de clasificación de la tabla de direcciones): Especifica los medios por los que se ordena la tabla de direcciones.

Redefinición del tiempo de caducidad

1. Abra la [Dynamic Address Table](#) (Tabla de direcciones dinámicas).
2. Defina el campo **Aging Time** (Tiempo de caducidad).

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

El tiempo de caducidad se modifica, y el dispositivo se actualiza.

Consulta de la tabla de direcciones dinámicas

- Abra la [Dynamic Address Table](#) (Tabla de direcciones dinámicas).
- Defina el parámetro por el que se consultará la [Dynamic Address Table](#) (Tabla de direcciones dinámicas).

Las entradas se pueden consultar por **puerto**, **dirección MAC** o **ID de VLAN**.

- Haga clic en **Query** (Consultar).

Se consulta la [Tabla de direcciones dinámicas](#).

Clasificación de la tabla de direcciones dinámicas

- Abra la [Dynamic Address Table](#) (Tabla de direcciones dinámicas).
- En el menú descendente **Address Table Sort Key** (Clave de clasificación de la tabla de direcciones), seleccione si las direcciones deben clasificarse por dirección, ID de VLAN o interfaz.
- Haga clic en **Query** (Consultar).

Se clasifica la [Tabla de direcciones dinámicas](#).

Consulta y clasificación de direcciones dinámicas mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para consultar y clasificar direcciones dinámicas tal como aparecen en la [Dynamic Address Table](#) (Tabla de direcciones dinámicas).

Tabla 7-58. Comandos de la CLI para consultar y clasificar

Comando de la CLI	Description
<code>bridge aging-time segundos</code>	Establece el tiempo de caducidad de la tabla de direcciones..
<code>show bridge address-table [vlan vlan] [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra clases de entradas creadas de manera dinámica en la base de datos de reenvío de puente.

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

```

Console (config)# bridge aging-time 250

Console(config)# exit

Console# show bridge address-table

```

Aging time is 250 sec			
vlan	mac address	port	type
----	-----	----	----
1	00:60:70:4C:73:FF	g8	dynamic

1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g8	static

Configuración de GARP

El protocolo genérico de registro de atributos (GARP) es un protocolo de propósitos generales que registra cualquier información de conectividad de red o de estilo de pertenencia. GARP define un conjunto de dispositivos interesados en un atributo de red determinado, como VLAN o dirección de multidifusión.

Cuando configure GARP, tenga en cuenta lo siguiente:

- 1 El tiempo de cese debe ser igual o mayor que tres veces el tiempo de unión.
- 1 El tiempo de cese de todos debe ser mayor que el tiempo de cese.

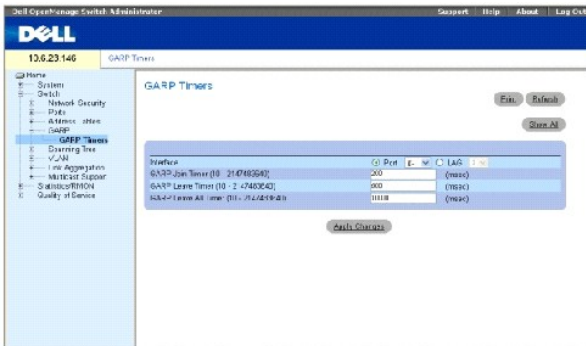
Establezca los valores del temporizador de GARP en todos los dispositivos conectados de nivel 2. Si los temporizadores de GARP se establecen de manera diferente en los dispositivos conectados de nivel 2, la aplicación GARP no funcionará correctamente.

Para abrir la página GARP, haga clic en **Switch** → **GARP** (Conmutador → GARP) en la vista de árbol.

Definición de temporizadores de GARP

La página [GARP Timers](#) (Temporizadores de GARP) contiene campos para activar GARP en el dispositivo. Para abrir la página [GARP Timers](#) (Temporizadores de GARP), haga clic en **Switch** → **GARP** → **GARP Timers** (Conmutador → GARP → Temporizadores de GARP) en la vista de árbol.

Ilustración 7-97. GARP Timers (Temporizadores de GARP)



Interface (Interfaz): Determina si se habilita en un puerto o en un LAG.

GARP Join Timer (10 - 2147483640) (Temporizador de unión GARP [10 - 2147483640]): Indica el tiempo en milisegundos en que se transmiten las PDU. Los valores posibles son 10-2147483640. El valor predeterminado es 200 ms.

GARP Leave Timer (10 - 2147483640) (Temporizador de cese GARP [10 - 2147483640]): Indica el tiempo en milisegundos durante el que el dispositivo espera antes de abandonar su estado GARP. El tiempo de cese se activa mediante un mensaje Leave All Time (Tiempo de cese de todos) enviado/recibido y se cancela mediante el mensaje Join (Unión) recibido. El tiempo de cese debe ser igual o mayor que tres veces el tiempo de unión. El valor posible del campo es 0-2147483640. El valor predeterminado es 600 ms.

GARP Leave All Timer (10 - 2147483640) (Temporizador de cese de todos GARP [10 - 2147483640]): Indica el tiempo en milisegundos durante el que todos los dispositivos esperan antes de abandonar el estado GARP. El tiempo de cese de todos debe ser mayor que el tiempo de cese. El valor posible del campo es 0-2147483640. El valor predeterminado es 10000 ms.

Definición de temporizadores de GARP

1. Abra la página [GARP Timers](#) (Temporizadores de GARP).
2. Complete los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de GARP se guardan en el dispositivo.

Copia de los parámetros de la tabla de temporizadores de GARP

1. Abra la página [GARP Timers](#) (Temporizadores de GARP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **GARP Timers Table** (Tabla de temporizadores de GARP).

3. Seleccione una interfaz en el campo **Copy Parameters from** (Copiar parámetros de).
4. Seleccione una interfaz en el menú descendente **Port** (Puerto) o **LAG**.
5. Las definiciones de esta interfaz se copian en las interfaces seleccionadas. Véase el paso 6.
6. Seleccione la casilla de verificación **Copy to** (Copiar en) para definir las interfaces en las que deban copiarse las definiciones de los temporizadores de GARP, o bien haga clic en **Select All** (Seleccionar todo) para copiar las definiciones en todos los puertos o LAG.
7. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se copian a los puertos o LAG de la **GARP Timers Table** (Tabla de temporizadores de GARP), y el dispositivo se actualiza.

Definición de los temporizadores de GARP mediante los comandos de la CLI

En esta tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los temporizadores de GARP tal como aparecen en la página [GARP Timers](#) (Temporizadores de GARP).

Tabla 7-59. Comandos de la CLI para los temporizadores de GARP

Comando de la CLI	Description
<code>garp timer {join leave leaveall} valor_temporizador</code>	Establece los valores del temporizador de GARP "Join", "Leave" y "Leaveall".

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

```
console(config)# interface ethernet g1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet g1

GVRP Feature is currently Disabled on the device.
```

Maximum VLANs: 223						
Port(s)	GVRP-	Registration	Dynamic VLAN	Timers	(milliseconds)	
	Status		Creation	Join	Leave	Leave All
-----	-----	-----	-----	-----	-----	-----
gl	Disabled	Normal	Enabled	200	900	10000
console#						

Configuración del protocolo de árbol extensible

El protocolo de árbol extensible (STP) proporciona topografía de árbol para cualquier disposición de puentes. STP también proporciona una vía de comunicación entre las estaciones finales de una red, eliminando los bucles.

Los bucles se producen cuando existen rutas de acceso alternativas entre los sistemas principales. En una red extendida, los bucles pueden hacer que los puentes reenvíen tráfico indefinidamente, lo que provoca un aumento del tráfico y una disminución del rendimiento de la red.

Los dispositivos admiten los siguientes protocolos de árbol extensible:

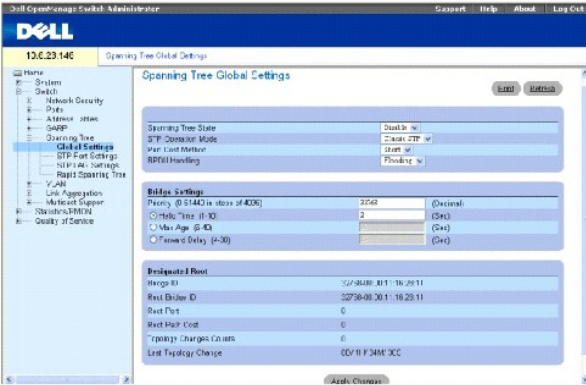
- 1 Classic STP (STP clásico): Proporciona una sola ruta de acceso entre las estaciones finales, lo que impide y elimina los bucles. Para obtener más información sobre la configuración del STP clásico, consulte el apartado "[Definición de la configuración global de STP](#)".
- 1 Rapid STP (STP rápido): Detecta y utiliza topologías de red que proporcionan una convergencia más rápida del árbol extensible sin crear bucles de reenvío. Para obtener más información sobre la configuración del STP rápido, consulte el apartado "[Configuración del árbol extensible rápido](#)".

Para abrir la página **Spanning Tree** (Árbol extensible), haga clic en **Switch**→ **Spanning Tree** (Conmutador→ Árbol extensible) en la vista de árbol.

Definición de la configuración global de STP

La página [STP Global Settings](#) (Configuración global de STP) contiene parámetros para habilitar y configurar el funcionamiento de STP en el dispositivo. Para abrir la página [STP Global Settings](#) (Configuración global de STP), haga clic en **Switch**→ **Spanning Tree**→ **Global Settings** (Conmutador→ Árbol extensible→ Configuración global) en la vista de árbol.

Ilustración 7-98. STP Global Settings (Configuración global de STP)



Spanning Tree State (Estado del árbol extensible): Habilita o inhabilita el árbol extensible en el dispositivo. Los valores de campo posibles son:

- o **Enable (Activar):** Activa el árbol extensible
- o **Disable (Desactivar):** Desactiva el árbol extensible

STP Operation Mode (Modo de funcionamiento de STP): El modo STP mediante el cual se habilita el STP en el dispositivo. Los valores de campo posibles son:

Classic STP (STP clásico): Activa el STP clásico en el dispositivo. Éste es el valor predeterminado.

Rapid STP (STP rápido): Activa el STP rápido en el dispositivo.

Port Cost Method (Método de coste de puerto): Determina el método de coste de la ruta de acceso predeterminada del árbol extensible. Los valores de campo posibles son:

Short (Breve): Especifica un intervalo de 1 a 65535 para los costes de la ruta de acceso del puerto. Éste es el valor predeterminado.

Long (Prolongado): Especifica un intervalo de 1 a 200000000 para los costes de la ruta de acceso del puerto.

BPDU Handling (Manipulación de BPDU): Determina cómo se gestionan los paquetes de BPDU cuando STP está desactivado en el puerto/ dispositivo. Las BPDU se utilizan para transmitir la información del árbol extensible. Los valores de campo posibles son:

Filtering (Filtrado): Filtra los paquetes de BPDU cuando el árbol extensible está desactivado en una interfaz.

Flooding (Desbordamiento): Desborda los paquetes de BPDU cuando el árbol extensible está desactivado en una interfaz. Éste es el valor predeterminado.

Priority (0-61440, in steps of 4096) (Prioridad [0-61440, en pasos de 4096]): Especifica el valor de prioridad del puente. Cuando los conmutadores o puentes ejecutan el STP, se asigna una prioridad a cada uno. Después de intercambiar BPDU, el conmutador con el menor valor de prioridad se transforma en el puente raíz. El valor predeterminado es 32768. El valor de prioridad del puente se proporciona en incrementos de 4096 (incrementos de 4K). Por ejemplo, 0, 4096, 8192, etc.

Hello Time (1-10): Especifica el "Hello Time" del dispositivo. El "Hello Time" indica la cantidad de tiempo en segundos durante el que se espera un puente raíz entre los mensajes de configuración. El valor predeterminado es 2 segundos.

Max Age (6-40) (Caducidad máxima [6-40]): Especifica el tiempo máximo de caducidad del dispositivo. El tiempo máximo de caducidad indica la cantidad de tiempo en segundos que espera un puente antes de enviar los mensajes de configuración. La caducidad máxima predeterminada es de 20 segundos.

Forward Delay (4-30) (Retraso de envío [4-30]): Especifica el período de retraso de envío del dispositivo. El período de retraso de envío indica la cantidad de

tiempo en segundos durante la que un puente permanece en los estados de escucha y obtención antes de reenviar paquetes. El valor predeterminado es 15 segundos.

Bridge ID (ID de puente): Identifica la prioridad del puente y la dirección MAC.

Root Bridge ID (ID de puente raíz): Identifica la prioridad del puente raíz y la dirección MAC.

Root Port (Puerto raíz): El número de puerto que ofrece la ruta de acceso de menor coste desde este puente hasta el puente raíz. Es significativo cuando el puente no es la raíz. El valor predeterminado es cero.

Root Path Cost (Coste de la ruta de acceso a la raíz): El coste de la ruta de acceso desde este puente hasta la raíz.

Topology Changes Counts (Recuentos de cambios de topología): Especifica la cantidad total de cambios de estado de STP que se han producido desde el último reinicio.

Last Topology Change (Último cambio de topología): La cantidad de tiempo que ha pasado desde que se ha inicializado o restablecido el puente, y el último cambio topográfico que se ha producido. Este tiempo aparece en formato de días, horas, minutos y segundos; por ejemplo, 0 días 1 hora 34 minutos y 38 segundos.

Definición de los parámetros globales de STP

1. Abra la página [STP Global Settings](#) (Configuración global de STP).
2. Seleccione el puerto que haya que habilitar en el menú descendente **Select a Port** (Seleccionar un puerto).
3. Seleccione **Enable** (Habilitar) en el campo **Spanning Tree State** (Estado del árbol extensible).
4. Seleccione el modo **STP** en el campo **STP Operation Mode** (Modo de funcionamiento de STP) y defina la configuración del puente.
5. Haga clic en **Apply Changes** (Aplicar cambios).

STP se habilita en el dispositivo.

Modificación de los parámetros globales de STP

1. Abra la página [STP Global Settings](#) (Configuración global de STP).
2. Defina los campos del cuadro de diálogo.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de STP se modifican, y el dispositivo se actualiza.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los parámetros globales de STP tal como aparecen en la página [STP Global Settings](#) (Configuración global de STP).

Tabla 7-60. Comandos de la CLI para los parámetros globales de STP

Comando de la CLI	Description
<code>spanning-tree</code>	Habilita la funcionalidad del árbol extensible.
<code>spanning-tree mode {stp rstp}</code>	Configura el protocolo de árbol extensible.
<code>spanning-tree priority <i>prioridad</i></code>	Configura la prioridad del árbol extensible.
<code>spanning-tree hello-time <i>segundos</i></code>	Configura el "Hello Time" del puente del árbol extensible, que es la frecuencia con la que el dispositivo transmite mensajes de saludo a otros conmutadores.
<code>spanning-tree max-age <i>segundos</i></code>	Configura la duración máxima del puente del árbol extensible.
<code>spanning-tree forward-time <i>segundos</i></code>	Configura el tiempo de reenvío del puente del árbol extensible, que es el tiempo durante el cual un puerto

	permanece en los estados de escucha y de obtención antes de pasar al estado de reenvío.
<code>show spanning-tree [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra el identificador de configuración del árbol extensible.
<code>show spanning-tree [detail] [active blockedports]</code>	Muestra información sobre la configuración del árbol extensible: información detallada, puertos activos o puertos bloqueados.

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

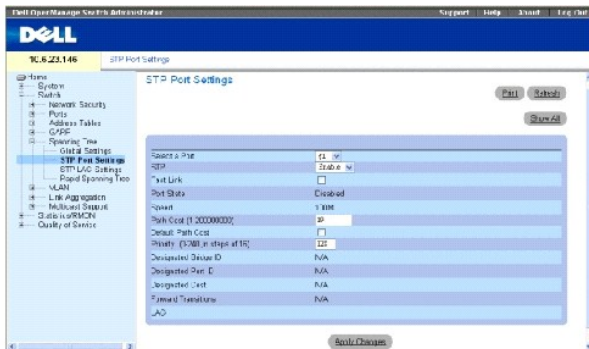
<pre> console(config)# spanning-tree console(config)# spanning-tree mode rstp console(config)# spanning-tree priority 12288 console(config)# spanning-tree hello-time 5 console(config)# spanning-tree max-age 15 console(config)# spanning-tree forward-time 25 console(config)# exit console# show spanning-tree Spanning tree enabled mode RSTP Default port cost method: short </pre>																																															
<table border="1"> <tr> <td>Root ID</td> <td>Priority</td> <td>12288</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>Address</td> <td>00:e8:00:b4:c0:00</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td colspan="7">This switch is the root</td> </tr> <tr> <td></td> <td colspan="7">Hello Time 5 sec Max Age 25 sec Forward Delay 15 sec</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>								Root ID	Priority	12288							Address	00:e8:00:b4:c0:00							This switch is the root								Hello Time 5 sec Max Age 25 sec Forward Delay 15 sec														
Root ID	Priority	12288																																													
	Address	00:e8:00:b4:c0:00																																													
	This switch is the root																																														
	Hello Time 5 sec Max Age 25 sec Forward Delay 15 sec																																														
<pre> Number of topology changes 5 last change occurred 00:05:28 ago Times: hold 1, topology change 40, notification 5 hello 5, max age 25, forward delay 15 </pre>																																															

Interfaces							
Name	State	Prio. Nbr	Cost	Sts	Role	PortFast	Type
-----	-----	-----	-----	-----	-----	-----	-----
g1	enabled	128.1	100	DSBL	Dsbl	No	P2p (STP)
g2	enabled	128.2	100	DSBL	Dsbl	No	P2p (STP)
g3	enabled	128.3	100	DSBL	Dsbl	No	P2p (STP)

Definición de la configuración del puerto STP

La página [STP Port Settings](#) (Configuración del puerto STP) contiene campos para asignar propiedades de STP a puertos individuales. Para abrir la página [STP Port Settings](#) (Configuración del puerto STP), haga clic en **Switch**→ **Spanning Tree**→ **Port Settings** (Conmutador→ Árbol extensible→ Configuración del puerto) en la vista de árbol.

Ilustración 7-99. STP Port Settings (Configuración del puerto STP)



Select a Port (Seleccionar un puerto): Puerto en el que se ha habilitado STP.

STP: Habilita o inhabilita STP en el puerto.

Fast Link (Conexión rápida): Si se selecciona esta opción, se habilita el modo de conexión rápida para el puerto. Si se activa el modo de conexión rápida para un puerto, el valor de **Port State** (Estado de puerto) pasa automáticamente al estado **Forwarding** (Reenvío) cuando se activa la conexión del puerto. El modo de conexión rápida optimiza el tiempo que tarda el protocolo STP en hacer la convergencia. La convergencia de STP puede tardar de 30 a 60 segundos en redes extensas.

Port State (Estado del puerto): El estado STP actual del puerto. Si está habilitado, el estado del puerto determina qué acción de reenvío se realiza con el tráfico. Los valores de puerto posibles son:

Disabled (Desactivado): Actualmente la conexión del puerto no está activada.

Blocking (Bloqueo): El puerto está bloqueado actualmente y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC. El bloqueo se muestra cuando se activa el STP clásico.

Listening (Escucha): El puerto está actualmente en el modo de escucha. El puerto no puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): El puerto está actualmente en el modo de obtención. El puerto no puede reenviar tráfico pero sí obtener direcciones MAC nuevas.

Forwarding (Reenvío): El puerto está actualmente en el modo de reenvío. El puerto puede reenviar tráfico y obtener direcciones MAC nuevas.

Speed (Velocidad): La velocidad del funcionamiento del puerto.

Path Cost (1-200000000) (Coste de la ruta de acceso [1-200000000]): La contribución de este puerto al coste de la ruta de acceso hasta la raíz. El coste de la ruta se puede ajustar a un valor mayor o menor, y se utiliza para reenviar tráfico cuando se redirecciona una ruta.

Default Path Cost (Coste de la ruta de acceso predeterminada): El coste de la ruta de acceso predeterminada del puerto se establece automáticamente mediante la velocidad del puerto y el método de coste de la ruta de acceso predeterminada.

Los valores predeterminados de los costes de las rutas de acceso largas son:

Ethernet - 2000000

Fast Ethernet - 200000

Gigabit Ethernet - 20000

Los valores predeterminados de los costes de las rutas de acceso cortas (los costes de las rutas de acceso cortas son los valores predeterminados) son:

Ethernet - 100

Fast Ethernet - 19

Gigabit Ethernet - 4

Priority (0-240, in steps of 16) (Prioridad [0-240, en saltos de 16]): Valor de prioridad del puerto. El valor de prioridad puede utilizarse para influir en la elección del puerto cuando un puente tiene dos puertos conectados en un bucle. El valor de prioridad está entre 0-240. Este valor se ofrece en incrementos de 16.

Designated Bridge ID (ID de puente designado): La prioridad del puente y la dirección MAC del puerto designado.

Designated Port ID (ID de puerto designado): La interfaz y la prioridad del puerto seleccionado.

Designated Cost (Coste designado): El coste del puerto que participa en la topología STP. Los puertos cuyo coste es menor tienen menos probabilidades de bloquearse si STP detecta bucles.

Forward Transitions (Transmisiones de reenvío): El número de veces que el puerto ha pasado del estado **Blocking** (Bloqueo) al estado **Forwarding** (Reenvío).

LAG: El LAG al que está conectado el puerto.

Habilitación de STP en un puerto

1. Abra la página [STP Port Settings](#) (Configuración del puerto STP).
2. Seleccione **Enabled** (Habilitado) en el campo **STP Port Status** (Estado STP de puertos).
3. Defina los campos **Fast Link** (Conexión rápida), **Path Cost** (Coste de la ruta) y **Priority** (Prioridad).
4. Haga clic en **Apply Changes** (Aplicar cambios).

STP está habilitado en el puerto.

Modificación de las propiedades de STP de puertos

1. Abra la página [STP Port Settings](#) (Configuración del puerto STP).
2. Modifique los campos **Priority** (Prioridad), **Fast Link** (Conexión rápida), **Path Cost** (Coste de la ruta) y **Fast Link** (Conexión rápida).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros STP de puertos se modifican, y el dispositivo se actualiza.

Visualización de la tabla de STP de puertos

1. Abra la página [STP Port Settings](#) (Configuración del puerto STP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la tabla **STP Port** (STP de puertos).

Definición de la configuración del puerto STP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los parámetros del puerto STP tal como aparecen en la página [STP Port Settings](#) (Configuración del puerto STP).

Tabla 7-61. Comandos de la CLI para la configuración del puerto STP

Comando de la CLI	Descripción
<code>spanning-tree disable</code>	Inhabilita el árbol extensible en un puerto específico.
<code>spanning-tree cost <i>coste</i></code>	Configura la contribución al coste del árbol extensible de un puerto.
<code>spanning-tree port-priority <i>prioridad</i></code>	Configura la prioridad del puerto.
<code>spanning-tree portfast</code>	Habilita el modo rápido de puerto.
<code>show spanning-tree [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra la configuración del árbol extensible.

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

```
console(config)# interface ethernet g5

console(config-if)# spanning-tree disable

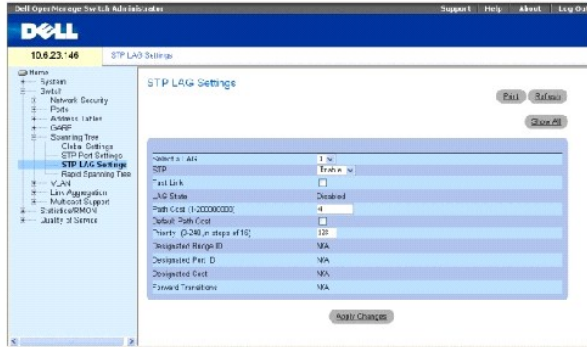
console(config-if)# spanning-tree cost 35000
```


console(config-if)# spanning-tree port-priority 96	
console(config-if)# exit	
console(config)# exit	
console# show spanning-tree ethernet g5	
Port g5 disabled	
State: disabled	Role: disabled
Port id: 96.5	Port cost: 35000
Type: P2p (configured: Auto) STP	Port Fast: No (configured: No)
Designated bridge Priority : 32768	Address: 00:e8:00:b4:c0:00
Designated port id: 96.5	Designated path cost: 19
Number of transitions to forwarding state: 0	
BPDU: sent 0, received 0	
console#	

Definición de la configuración STP de LAG

La página [STP LAG Settings](#) (Configuración STP de LAG) contiene los campos para asignar los parámetros del puerto de agregación de STP. Para abrir la página [STP LAG Settings](#) (Configuración STP de LAG), haga clic en **Switch**→ **Spanning Tree**→ **LAG Settings** (Conmutador→ Árbol extensible→ Configuración de LAG) en la vista de árbol.

Ilustración 7-100. STP LAG Settings (Configuración STP de LAG)



Select a LAG (Seleccionar un LAG): El LAG definido por el usuario. Para obtener más información, consulte el apartado "[Definición de la pertenencia a LAG](#)".

STP: Habilita o inhabilita STP en el LAG.

Fast Link (Conexión rápida): Habilita el modo de conexión rápida para el LAG. Si se habilita la conexión rápida para un LAG, el valor de **LAG State** (Estado de LAG) pasa automáticamente al estado **Forwarding** (Reenvío) cuando el LAG está activo. El modo de conexión rápida optimiza el tiempo que tarda el protocolo STP en hacer la convergencia. La convergencia de STP puede tardar de 30 a 60 segundos en redes extensas.

LAG State (Estado de LAG): El estado STP actual de un LAG. Si está habilitado, el estado de LAG determina qué acción de reenvío se realiza con el tráfico. Si el puente descubre un LAG cuyo funcionamiento es defectuoso, lo coloca en estado **Broken** (Averiado). Los posibles estados de LAG son:

Disabled (Desactivado): Actualmente la conexión del LAG no está activada.

Blocking (Bloqueo): El LAG está bloqueado y no puede utilizarse para reenviar tráfico ni para obtener direcciones MAC.

Listening (Escucha): El LAG se encuentra en el modo de escucha y no puede reenviar tráfico ni obtener direcciones MAC.

Learning (Obtención): El LAG está actualmente en el modo de obtención y no puede reenviar tráfico pero sí obtener direcciones MAC nuevas.

Forwarding (Reenvío): El LAG está actualmente en el modo de reenvío, y puede reenviar tráfico y obtener direcciones MAC nuevas.

Broken (Averiado): Actualmente, el funcionamiento del LAG es defectuoso y no puede utilizarse para reenviar tráfico.

Path Cost (1-200000000) (Coste de la ruta de acceso [1-200000000]): La cantidad con la que el LAG contribuye al coste de la ruta de acceso hasta la raíz. El coste de la ruta se puede ajustar a un valor mayor o menor, y se utiliza para reenviar tráfico cuando se redirecciona una ruta. El coste de la ruta de acceso tiene un valor de 1 a 200000000. Si el método de coste de la ruta de acceso es corto, el valor predeterminado de coste del LAG es 4. Si el método de coste de la ruta de acceso es largo, el valor predeterminado de coste del LAG es 20000.

Default Path Cost (Coste predeterminado de la ruta de acceso): Si se selecciona esta opción, el coste de la ruta de acceso del LAG vuelve a su valor predeterminado.

Priority (0-240, in steps of 16) (Prioridad [0-240, en saltos de 16]): Valor de prioridad del LAG. El valor de prioridad puede utilizarse para influir en la elección del LAG cuando un puente tiene dos puertos en bucle. El valor de la prioridad oscila entre 0-240, en incrementos de 16.

Designated Bridge ID (ID de puente designado): La prioridad del puente y la dirección MAC del puerto designado.

Designated Port ID (ID de puerto designado): La prioridad de puerto y el número de interfaz del puerto designado.

Designated Cost (Coste designado): El coste del puente designado.

Forward Transitions (Transmisiones de reenvío): El número de veces que el **LAG State** (Estado de LAG) ha pasado del estado **Blocking** (Bloqueo) al estado **Forwarding** (Reenvío).

Modificación de los parámetros STP de LAG

1. Abra la página [STP LAG Settings](#) (Configuración STP de LAG).
2. Seleccione un LAG del menú descendente **Select a LAG** (Seleccionar un LAG).
3. Modifique los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros STP de LAG se modifican, y el dispositivo se actualiza.

Definición de la configuración STP de LAG mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir la configuración STP de LAG.

Tabla 7-62. Comandos de la CLI para la configuración STP de LAG

Comando de la CLI	Descripción
<code>spanning-tree</code>	Habilita el árbol extensible.
<code>spanning-tree disable</code>	Inhabilita el árbol extensible en un LAG específico.
<code>spanning-tree priority <i>coste</i></code>	Configura la contribución al coste del árbol extensible de un LAG.
<code>spanning-tree port-priority <i>prioridad</i></code>	Configura la prioridad del puerto.
<code>show spanning-tree [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra la configuración del árbol extensible.
<code>show spanning-tree [detail] [active blockedports]</code>	Muestra información detallada del árbol extensible sobre los puertos activos o bloqueados.

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

```
console(config)# interface port-channel 1

console(config-if)# spanning-tree port-priority 16
```

Configuración del árbol extensible rápido

Aunque el árbol extensible clásico impide los bucles de reenvío de nivel 2 en una topología de red general, la convergencia puede tardar hasta 30-60 segundos. El período de convergencia se considera excesivo para muchas aplicaciones. Si la topología de red lo permite, se puede realizar una convergencia más rápida. El protocolo de árbol extensible rápido (RSTP) detecta y utiliza topologías de red que proporcionan una convergencia más rápida del árbol extensible sin crear bucles de reenvío.

RSTP tiene los siguientes estados de puerto diferentes:

- 1 Disabled (Desactivado)
- 1 Learning (Obtención)
- 1 Discarding (Descarte)
- 1 Forwarding (Reenvío)

El árbol extensible rápido está habilitado en la página [STP Global Settings](#) (Configuración global de STP). Para abrir la página [Rapid Spanning Tree \(RSTP\)](#) (Árbol extensible rápido [RSTP]), haga clic en **Switch** → **Spanning Tree** → **Rapid Spanning Tree** (Conmutador → Árbol extensible → Árbol extensible rápido) en la vista de árbol.

Ilustración 7-101. Rapid Spanning Tree (RSTP) (Árbol extensible rápido [RSTP])



Interface (Interfaz): Puerto o LAG en el que se ha habilitado el STP rápido.

Role (Rol): El rol del puerto asignado por el algoritmo de STP para proporcionar las rutas de acceso de STP. Los valores de campo posibles son:

Root (Raíz): Proporciona la ruta de acceso de menor coste para reenviar paquetes al dispositivo raíz.

Designated (Designado): El puerto o LAG a través del cual el dispositivo designado se conecta a la LAN.

Alternate (Alternativa): Proporciona una ruta de acceso alternativa al dispositivo raíz desde la interfaz raíz.

Backup (Copia de seguridad): Proporciona una ruta de acceso de copia de seguridad para la ruta de acceso del puerto designado hacia las hojas del árbol extensible. La copia de seguridad de los puertos sólo se realiza cuando los dos puertos están conectados en un bucle. También se produce cuando una LAN tiene dos o más conexiones conectadas con un segmento compartido.

Disabled (Desactivado): El puerto no participa en el árbol extensible (el puerto no tiene conexión).

Fast Link Operational Status (Estado operativo de la conexión rápida): Indica si la conexión rápida está habilitada o inhabilitada para el puerto o el LAG. Si se ha habilitado para un puerto, éste se coloca automáticamente en el estado de reenvío.

Point-to-Point Admin Status (Estado admin punto a punto): Habilita o inhabilita al dispositivo para que pueda establecer una conexión punto a punto, o bien especifica que el dispositivo establezca automáticamente una conexión punto a punto.

Para establecer comunicaciones a través de una conexión punto a punto, el PPP originario envía primero paquetes LCP (Protocolo de control de conexiones) para configurar y comprobar la conexión de los datos. Tras establecerse una conexión y una vez negociadas las capacidades opcionales en función de las necesidades del LCP, el PPP originario envía paquetes NCP (Protocolo de control de red) para seleccionar y configurar uno o más protocolos de nivel de red. Una vez configurados cada uno de los protocolos de nivel de red, ya se pueden enviar sus paquetes a través de la conexión. La conexión permanece configurada para las comunicaciones hasta que paquetes LCP o NCP explícitos cierran la conexión, o bien hasta que se genere algún evento externo. Éste es el tipo real de conexión del puerto de dispositivo. Puede ser distinto del tipo del estado administrativo.

Point-to-Point Operational Status (Estado operativo punto a punto): El estado operativo de la conexión punto a punto.

Activate Protocol Migrational Test (Activar prueba de migración de protocolo): Si se selecciona esta opción, habilita al PPP para que pueda enviar paquetes LCP (Protocolo de control de conexiones) con el fin de configurar y probar la conexión de los datos.

Habilitación de RSTP

1. Abra la página [Rapid Spanning Tree \(RSTP\)](#) (Árbol extensible rápido [RSTP]).

2. Defina los campos **Point-to-Point Admin** (Admin. punto a punto), **Point-to-Point Oper** (Oper. punto a punto) y **Activate Protocol Migration** (Activar migración de protocolo).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del STP rápido se habilitan, y el dispositivo se actualiza.

Definición de los parámetros globales de STP rápido mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir los parámetros del STP rápido tal como aparecen en la página [Rapid Spanning Tree \(RSTP\)](#) (Árbol extensible rápido [RSTP]).

Tabla 7-63. Comandos de la CLI para la configuración de RSTP

Comando de la CLI	Description
<code>spanning-tree link-type { point-to-point shared }</code>	Hace prevalecer la configuración predeterminada del tipo de conexión.
<code>spanning tree mode { stp rstp }</code>	Configura el protocolo de árbol extensible que se ejecuta actualmente.
<code>clear spanning-tree detected-protocols [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Reinicia el proceso de migración del protocolo.
<code>show spanning-tree [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra la configuración del árbol extensible.

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

```
Console (config)# interface ethernet g5

Console(config-if)# spanning-tree link-type shared
```

Configuración de VLAN

Las VLAN son subgrupos lógicos de una red de área local (LAN) creados utilizando software en lugar de una definición de solución de hardware. Combinan estaciones de usuario y dispositivos de red en un dominio único, independientemente del segmento físico de LAN al que se conecten. Las VLAN permiten que el tráfico de red fluya con mayor eficiencia dentro de subgrupos. Cuando las VLAN se administran a través de software, se reduce la cantidad de tiempo de implementación de los cambios de la red.

Las VLAN se basan en software y no se definen por atributos físicos. En consecuencia, las VLAN no tienen un número mínimo de puertos y pueden crearse por dispositivo o cualquier otra combinación de conexión lógica.

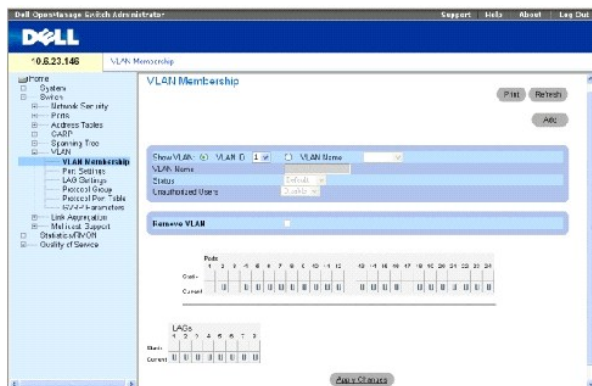
Las VLAN funcionan en el nivel 2. Dado que aíslan el tráfico dentro de la VLAN, se requiere un enrutador funcional de nivel 3 para permitir que el tráfico fluya entre ellas. Los enrutadores de nivel 3 identifican segmentos y se coordinan con las VLAN. Las VLAN son dominios de difusión y de multidifusión. El tráfico de difusión y de multidifusión sólo se transmite en la VLAN donde se genera el tráfico.

La asignación de etiquetas a VLAN proporciona un método para transferir información de la VLAN entre grupos de la VLAN. Se adjunta una etiqueta a las cabeceras de los paquetes. La etiqueta de VLAN indica a qué VLAN pertenece el paquete. Las etiquetas de VLAN se adjuntan al paquete mediante la estación final o el dispositivo de red. Las etiquetas de VLAN también contienen información de prioridad de la red VLAN. La combinación de VLAN y GVRP permite la dispersión automática de la información de VLAN. Para abrir la página **VLAN**, haga clic en **Switch** → **VLAN** (Conmutador → VLAN) en la vista de árbol.

Definición de miembros de VLAN

La página de pertenencia a VLAN contiene campos para definir los grupos de VLAN. El dispositivo admite la asignación de 4094 ID de VLAN a 256 VLAN. Todos los puertos deben tener un PVID definido. Si no se configura ningún otro valor, se utiliza el PVID de VLAN predeterminado. La VLAN número 1 es la VLAN predeterminada, y no se puede suprimir del sistema. Para abrir la página de pertenencia a VLAN, haga clic en **Switch** → **VLAN** → **VLAN Membership** (Conmutador → VLAN → Pertenencia a VLAN) en la vista de árbol.

Ilustración 7-102. Página VLAN Membership (Pertenencia a VLAN)



Show VLAN (Mostrar VLAN): Muestra una lista y visualiza información de VLAN específica de acuerdo con el ID o el nombre de VLAN.

VLAN Name (Nombre de VLAN): El nombre de la VLAN definido por el usuario.

Status (Estado): El tipo de VLAN. Los valores posibles son:

Dynamic (Dinámica): La VLAN se ha creado de manera dinámica a través de GVRP.

Static (Estática): La VLAN la ha definido el usuario.

Default (Predeterminada): La VLAN es la predeterminada.

Unauthorized Users (Usuarios no autorizados): Permite o impide que los usuarios no autorizados accedan a una VLAN.

Remove VLAN (Eliminar VLAN): Si se selecciona esta opción, se elimina la VLAN de la tabla de pertenencia a la VLAN.

Adición de nuevas VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Haga clic en **Add** (Agregar).

Se abre la página **Create New VLAN** (Crear VLAN nueva).

3. Escriba el ID de VLAN y el nombre.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva VLAN se agrega, y el dispositivo se actualiza.

Modificación de grupos de pertenencia a VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Seleccione una VLAN del menú descendente **Show VLAN** (Mostrar VLAN).
3. Modifique los campos según convenga.

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

La información de pertenencia a la VLAN se modifica, y el dispositivo se actualiza.

Supresión de grupos de pertenencia a la VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Seleccione una VLAN del campo **Show VLAN** (Mostrar VLAN).
3. Seleccione la casilla de verificación **Remove VLAN** (Eliminar VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La VLAN seleccionada se suprime y el dispositivo se actualiza.

Definición de grupos de pertenencia a la VLAN mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir grupos de pertenencia a la VLAN tal como aparecen en la página VLAN Membership (Pertenencia a la VLAN).

Tabla 7-64. Comandos de la CLI para el grupo de pertenencia a la VLAN

Comando de la CLI	Descripción
<code>vlan database</code>	Entra en el modo de (VLAN) configuración de interfaz.
<code>vlan {rango-vlan}</code>	Crea una VLAN.
<code>name cadena</code>	Agrega un nombre a una VLAN.

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

```
console(config)#vlan database

console(config-vlan)#vlan 1972

console(config-vlan)#exit

console (config)#interface vlan 1972

console (config-if)#name Marketing

console(config-if)# exit

console(config)#
```

Tabla de pertenencia a puerto de la VLAN

La tabla VLAN Port Membership (Pertenencia a puerto de la VLAN) contiene una tabla Port (Puerto) para asignar puertos a las VLAN. A los puertos se les asigna la pertenencia a la VLAN mediante la configuración de Port Control (Control de puerto). Los puertos pueden tener los valores siguientes:

Tabla 7-65. Tabla de pertenencia a puerto de la VLAN

Control de puerto	Definición
T	La interfaz es miembro de una VLAN. Todos los paquetes reenviados por la interfaz tienen etiqueta. Los paquetes contienen información de VLAN.
U	La interfaz es miembro de una VLAN. Los paquetes reenviados por la interfaz no tienen etiqueta.
F	La interfaz tiene denegada la pertenencia a una VLAN.
Blank	La interfaz no es miembro de una VLAN. Los paquetes asociados con la interfaz no se reenvían.

 **NOTA:** Los puertos que son miembros de LAG no se visualizan en la tabla de pertenencia a puerto de la VLAN.

En la VLAN Port Membership Table (Tabla de pertenencia a puerto de la VLAN) se muestran los puertos y los estados de los puertos, así como los LAG.

Asignación de los puertos a un grupo de VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Haga clic en el botón de opción **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN) y seleccione una VLAN del menú descendente.
3. Seleccione un puerto en la tabla **Port Membership** (Pertenencia al puerto) y asigne un valor al puerto.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se asigna al grupo de VLAN, y el dispositivo se actualiza.

Supresión de una VLAN

1. Abra la página VLAN Membership (Pertenencia a la VLAN).
2. Haga clic en el botón de opción **VLAN ID** (ID de VLAN) o **VLAN Name** (Nombre de VLAN) y seleccione una VLAN del menú descendente.
3. Seleccione la casilla de verificación **Remove VLAN** (Eliminar VLAN).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La VLAN seleccionada se suprime y el dispositivo se actualiza.

Asignación de puertos a grupos de VLAN mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar los puertos a los grupos de VLAN.

Tabla 7-66. Comandos de la CLI para asignar puertos a grupos de VLAN

Comando de la CLI	Descripción
<code>switchport general acceptable-frame-types tagged-only</code>	Rechaza tramas sin etiqueta en la entrada.
<code>switchport forbidden vlan {add lista-vlan remove lista-vlan}</code>	Prohíbe la adición de VLAN específicas al puerto.
<code>switchport mode { access trunk general}</code>	Configura el modo de pertenencia a la VLAN de un puerto.
<code>switchport access vlan id-vlan</code>	Configura el ID de VLAN cuando la interfaz está en modo de acceso.
<code>switchport trunk allowed vlan {add lista-vlan remove lista-vlan}</code>	Agrega o elimina VLAN de un puerto troncal.
<code>switchport trunk native vlan id-vlan</code>	Define el puerto como miembro de la VLAN especificada y el ID de VLAN como el "ID de VLAN predeterminado del puerto (PVID)".
<code>switchport general allowed vlan add lista-vlan [tagged untagged]</code>	Agrega o elimina redes VLAN de un puerto general.
<code>switchport general pvid id-vlan</code>	Configura el PVID cuando la interfaz está en modo general.

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


```
Console(config)#vlan database

Console (config-vlan)# vlan 23-25

Console(config-vlan)#exit

Console(config)# interface vlan 23

Console (config-if)# name Marketing

Console(config-if)#exit

Console(config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport access vlan 23

Console(config-if)#exit

Console (config)# interface ethernet g9

Console (config-if)# switchport mode trunk

Console (config-if)# switchport mode trunk allowed vlan add 23-25

Console(config-if)#exit

Console (config)# interface ethernet g10

Console (config-if)# switchport mode general

Console (config-if)# switchport general allowed vlan add 23,25 tagged

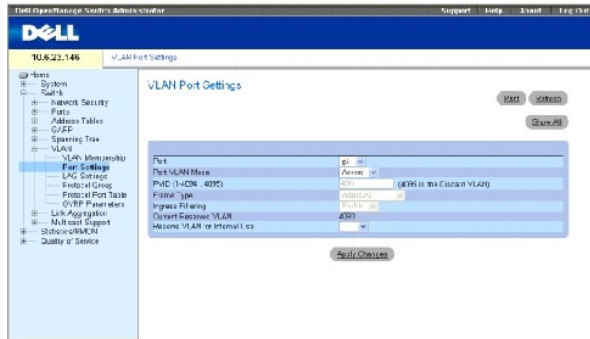
Console (config-if)# switchport general pvid 25
```

Definición de la configuración de puertos de VLAN

La página [VLAN Port Settings](#) (Configuración de puertos de VLAN) contiene campos para gestionar los puertos que forman parte de una VLAN. El ID de VLAN predeterminado de puerto (PVID) se configura en la página [VLAN Port Settings](#) (Configuración de puertos de VLAN). Todos los paquetes sin etiquetar que lleguen al dispositivo se etiquetan con los PVID de los puertos.

Para abrir la página [VLAN Port Settings](#) (Configuración de puertos de VLAN), haga clic en **Switch** → **VLAN** → **Port Settings** (Conmutador → VLAN → Configuración del puerto) en la vista de árbol.

Ilustración 7-103. VLAN Port Settings (Configuración de puertos de VLAN)



Port (Puerto): El número de puerto incluido en la VLAN.

Port VLAN Mode (Modo VLAN de puerto): El modo del puerto. Los valores posibles son:

General: El puerto pertenece a las VLAN y cada una de las VLAN está definida por el usuario como con etiqueta o sin etiqueta (modo 802.1Q completo).

Access (Acceso): El puerto pertenece a una única VLAN sin etiqueta. Cuando un puerto se encuentra en el modo de acceso, no se pueden designar los tipos de paquete que se aceptan en el puerto. No se puede habilitar/inhabilitar el filtrado de entrada en un puerto de acceso.

Trunk (Troncal): El puerto pertenece a VLAN en las que todos los puertos están etiquetados (excepto por un puerto que puede estar sin etiquetar).

PVID: Asigna un ID de VLAN a paquetes sin etiqueta. Los valores posibles son 1-4094. En el sector industrial, el valor estándar de la VLAN 4095 es definirla como la VLAN descartada. Los paquetes clasificados en la VLAN descartada se eliminan.

Frame Type (Tipo de trama): El tipo de paquete aceptado en el puerto. Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): En el puerto sólo se aceptan paquetes con etiqueta.

Admit All (Admitir todos): En el puerto se aceptan paquetes con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): Habilita o inhabilita el filtrado de entrada en el puerto. El filtrado de entrada descarta los paquetes destinados a las VLAN de las que no es miembro el LAG específico.

Current Reserve VLAN (VLAN de reserva actual): La VLAN designada actualmente por el sistema como la VLAN reservada.

Reserve VLAN for Internal Use (VLAN de reserva para uso interno): La VLAN seleccionada por el usuario para que sea la VLAN reservada si el sistema no la utiliza.

Asignación de la configuración de puertos

1. Abra la página [VLAN Port Settings](#) (Configuración de puertos de VLAN).
2. Seleccione el puerto al que hay que asignar la configuración del menú descendente **Port** (Puerto).
3. Complete los campos restantes de la página
4. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de puertos de VLAN se define, y el dispositivo se actualiza.

Visualización de la tabla de puertos de VLAN

1. Abra la página [VLAN Port Settings](#) (Configuración de puertos de VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **VLAN Port Table** (Tabla de puertos VLAN).

Asignación de puertos a grupos de VLAN mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar los puertos a los grupos de VLAN.

Tabla 7-67. Comandos de la CLI para los puertos de VLAN

Comando de la CLI	Descripción
<code>switchport mode { access trunk general }</code>	Configura un modo de pertenencia a la VLAN de puertos.
<code>switchport trunk native vlan <i>vlan-id</i></code>	Define el puerto como miembro de la VLAN especificada y el ID de VLAN como el "ID de VLAN predeterminado del puerto (PVID)".
<code>switchport general pvid <i>vlan-id</i></code>	Configura el ID de VLAN de puerto (PVID) cuando la interfaz está en modo general.
<code>switchport general allowed vlan add <i>lista-vlan</i> [tagged untagged]</code>	Agrega o elimina redes VLAN de un puerto general.
<code>switchport general acceptable-frame-types tagged-only</code>	Rechaza las tramas sin etiqueta en la entrada.
<code>switchport general ingress-filtering disable</code>	Inhabilita el filtrado de entrada del puerto.
<code>shutdown</code>	Inhabilita interfaces.
<code>set interface active { ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i> }</code>	Reactiva una interfaz que está apagada por motivos de seguridad.

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

```
Console (config)# interface range ethernet g18-20

Console (config-if)# switchport mode access

Console (config-if)# switchport general pvid 234

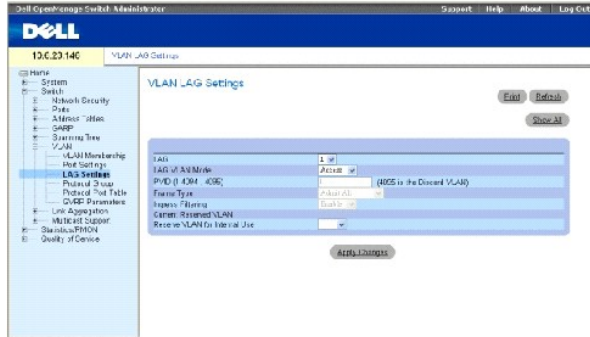
Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged

Console (config-if)# switchport general ingress-filtering disable
```

Definición de la configuración de LAG de la VLAN

En la página [VLAN LAG Setting](#) (Configuración de LAG de la VLAN) se proporcionan los parámetros para gestionar los LAGs que forman parte de una VLAN. Las VLAN pueden constar de puertos individuales o de LAG. Los paquetes sin etiquetar que entren en el dispositivo se etiquetan con el ID de LAG especificado por el PVID. Para abrir la página [VLAN LAG Setting](#) (Configuración de LAG de VLAN), haga clic en **Switch**→ **VLAN**→ **LAG Settings** (Conmutador→ VLAN→ Configuración de LAG) en la vista de árbol.

Ilustración 7-104. VLAN LAG Setting (Configuración de LAG de VLAN)



LAG: El número de LAG incluido en la VLAN.

LAG VLAN Mode (Modo VLAN de LAG): El modo de la VLAN de LAG. Los valores posibles son:

General: El LAG pertenece a las VLAN y cada una de las VLAN está definida por el usuario como con etiqueta o sin etiqueta (modo 802.1Q completo).

Access (Acceso): El LAG pertenece a una única VLAN sin etiqueta.

Trunk (Troncal): El LAG pertenece a VLAN en las que todos los puertos están etiquetados (excepto por una sola VLAN nativa opcional).

PVID: Asigna un ID de VLAN a paquetes sin etiqueta. Los valores de campo posibles son 1-4095. En el sector industrial, el valor estándar de la VLAN 4095 es definirla como la VLAN descartada. Los paquetes clasificados en esta VLAN se eliminan.

Frame Type (Tipo de trama): El tipo de paquete aceptado por el LAG. Los valores posibles son:

Admit Tag Only (Admitir sólo etiqueta): El LAG sólo acepta paquetes con etiqueta.

Admit All (Admitir todos): El LAG acepta paquetes con etiqueta y sin etiqueta.

Ingress Filtering (Filtrado de entrada): Habilita o inhabilita el filtrado de entrada por el LAG. El filtrado de entrada descarta los paquetes destinados a las VLAN de las que no es miembro el puerto específico.

Current Reserve VLAN (VLAN de reserva actual): La VLAN designada actualmente como la VLAN reservada.

Reserve VLAN for Internal Use (VLAN de reserva para uso interno): La VLAN designada como la VLAN reservada después de restablecer el dispositivo.

Asignación de la configuración de LAG de la VLAN

1. Abra la página [VLAN LAG Setting](#) (Configuración de LAG de la VLAN).
2. Seleccione un LAG en el menú descendente LAG y complete los campos de la página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros de LAG de la VLAN se definen, y el dispositivo se actualiza.

Visualización de la tabla VLAN LAG (LAG de VLAN)

1. Abra la página [VLAN LAG Setting](#) (Configuración de LAG de la VLAN).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **VLAN LAG Table** (Tabla de LAG de VLAN).

Asignación de LAG a grupos de VLAN mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar LAG a grupos de VLAN tal como aparecen en la página [VLAN LAG Setting](#) (Configuración de LAG de la VLAN).

Tabla 7-68. Comandos de la CLI para asignar LAG a VLAN

Comando de la CLI	Descripción
<code>switchport mode { access trunk general }</code>	Configura un modo de pertenencia a la VLAN de puertos.
<code>switchport trunk native vlan id-vlan</code>	Define el puerto como miembro de la VLAN especificada y el ID de VLAN como el ID de VLAN predeterminado del puerto (PVID).
<code>switchport general pvid id-vlan</code>	Configura el ID de VLAN de puerto (PVID) cuando la interfaz está en modo general.
<code>switchport general allowed vlan add lista-vlan [tagged untagged]</code>	Agrega o elimina redes VLAN de un puerto general.
<code>switchport general acceptable-frame-type tagged-only</code>	Rechaza las tramas sin etiqueta en la entrada.
<code>switchport general ingress-filtering disable</code>	Inhabilita el filtrado de entrada del puerto.

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

```
console(config)# interface port-channel 1

console(config-if)# switchport mode access

console(config-if)# switchport access vlan 2

console(config-if)# exit

console(config)# interface port-channel 2

console(config-if)# switchport mode general

console(config-if)# switchport general allowed vlan add 2-3 tagged

console(config-if)# switchport general pvid 2
```

```

console(config-if)# switchport general acceptable-frame-type tagged-only

console(config-if)# switchport general ingress-filtering disable

console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# switchport mode trunk

console (config-if)# switchport trunk native vlan 3

console(config-if)# switchport trunk allowed vlan add 2

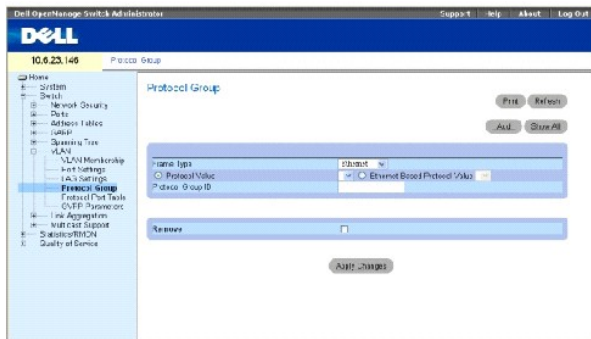
console(config-if)# exit

```

Definición de los grupos de protocolos de la VLAN

La página [Protocol Group](#) (Grupo de protocolos) proporciona los parámetros para configurar los tipos de tramas de grupos de protocolos específicos. Para abrir la página [Protocol Group](#) (Grupo de protocolos), haga clic en **Switch**→ **VLAN**→ **Protocol Group** (Conmutador→ VLAN→ Grupo de protocolos) en la vista de árbol.

Ilustración 7-105. Protocol Group (Grupo de protocolos)



Frame Type (Tipo de trama): El tipo de paquete. Los valores posibles del campo son **Ethernet**, **RFC1042** y **LLC Other** (LLC Otros).

Protocol Value (Valor del protocolo): Nombre del protocolo definido por el usuario.

Ethernet-Based Protocol Value (Valor del protocolo basado en Ethernet): El tipo de grupo de protocolos de Ethernet. Los valores posibles del campo son IP, IPX e IPv6.

Protocol Group ID (ID de grupo de protocolos): El número de ID del grupo de VLAN.

Remove (Eliminar): Si se selecciona esta opción, se elimina la asignación de tramas a grupos de protocolo, si el grupo de protocolos que se va a eliminar no está configurado en este puerto de protocolo.

Adición de un grupo de protocolos

1. Abra la página [Protocol Group](#) (Grupo de protocolos).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add Protocol to Group** (Agregar protocolo a grupo).

3. Complete los campos de esta página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El grupo de protocolos se asigna, y el dispositivo se actualiza.

Asignación de la configuración del grupo de protocolos de la VLAN

1. Abra la página [Protocol Group](#) (Grupo de protocolos).
2. Complete los campos de esta página.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del grupo de protocolos de la VLAN se definen, y el dispositivo se actualiza.

Eliminación de protocolos de la tabla de grupos de protocolos

1. Abra la página [Protocol Group](#) (Grupo de protocolos).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **Protocol Group Table** (Tabla de grupo de protocolos).

3. Seleccione **Remove** (Eliminar) para los grupos de protocolos que haya que eliminar.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se elimina el protocolo, y el dispositivo se actualiza.

Definición de grupos de protocolos de VLAN mediante los comandos de la CLI

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

Tabla 7-69. Comando de la CLI para los grupos de protocolos de VLAN

Comando de la CLI	Description
<code>map protocol <i>protocolo</i> [<i>encapsulación</i>] protocols-group <i>grupo</i></code>	Asigna un protocolo a un grupo de protocolos. Los grupos de protocolos se utilizan para la asignación de VLAN basadas en protocolo.

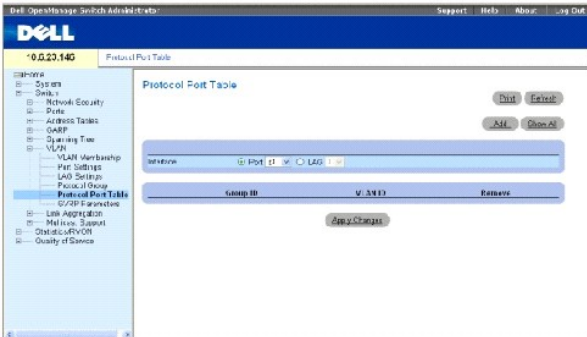
En el ejemplo siguiente se asigna un protocolo ARP de IP al grupo "213":

```
Console (config)# vlan database
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Adición de puertos de protocolo

La página [Protocol Port](#) (Puerto de protocolo) agrega interfaces a los grupos de protocolos. Para abrir la página [Protocol Port](#) (Puerto de protocolo), haga clic en **Switch**→**VLAN**→**Protocol Port** (Conmutador→VLAN→Puerto de protocolo) en la vista de árbol.

Ilustración 7-106. Protocol Port (Puerto de protocolo)



Interface (Interfaz): Número de puerto o LAG que se agrega a un grupo de protocolos.

Group ID (ID de grupo): El ID del grupo de protocolos al que se agrega la interfaz. Los ID de grupo de protocolos se definen en la tabla de grupos de protocolos.

VLAN ID (1-4095) (ID de VLAN [1-4095]): Conecta la interfaz a un ID de VLAN definido por el usuario. El ID de VLAN se define en la página [Create a New VLAN](#) (Crear nueva VLAN). Los puertos de los protocolos bien pueden conectarse a un ID de VLAN o a un nombre de VLAN.

NOTA: La VLAN 4095 es la VLAN descartada.

Adición de nuevo puerto de protocolos

NOTA: Los puertos de protocolo sólo se pueden definir en puertos definidos como General en la página [VLAN Port Settings](#) (Configuración de puertos de VLAN).

1. Abra la página [Protocol Port](#) (Puerto de protocolo).
2. Haga clic en **Add** (Agregar).

Se abre la página **Add Protocol Port** (Agregar puerto de protocolo).

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

Se agrega el nuevo grupo de protocolos de VLAN a la **Protocol Port Table** (Tabla de puertos de protocolos), y el dispositivo se actualiza.

Definición de puertos de protocolo mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen del comando de la CLI equivalente para definir los puertos de protocolo.

Tabla 7-70. Comandos de la CLI para los puertos de protocolo

Comando de la CLI	Description
<code>switchport general map protocols-group group vlan id-vlan</code>	Establece una regla de clasificación basada en protocolo.

En el ejemplo siguiente se establece una regla de clasificación basada en protocolo del grupo de protocolos 1 a la VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```


Configuración de GVRP

El protocolo de registro de VLAN GARP (GVRP) se proporciona específicamente para la distribución automática de información de pertenencia a la VLAN entre puentes con capacidad de reconocimiento de VLAN. El GVRP permite que los puentes con capacidad de reconocimiento de VLAN obtengan automáticamente las VLAN para la asignación de puertos puente sin tener que configurar individualmente cada puente y registrar la pertenencia a la VLAN.

Para garantizar el funcionamiento correcto del protocolo GVRP, se aconseja a los usuarios que fijen el número máximo de VLAN GVRP con un valor que supere significativamente la suma de:

- 1 El número de todas las VLAN estáticas, tanto las configuradas actualmente como las que se prevé que se configurarán.
- 1 El número de todas las VLAN dinámicas que participan en GVRP, tanto las configuradas actualmente (el número inicial de VLAN GVRP dinámicas es 128) como las que se prevé que se configurarán.

La página **GVRP Global Parameters** (Parámetros globales de GVRP) habilita el GVRP globalmente. GVRP también se puede habilitar en función de cada interfaz. Para abrir la página [GVRP Parameters](#) (Parámetros de GVRP), haga clic en **Switch**→**VLAN**→**GVRP Parameters** (Conmutador→VLAN→Parámetros de GVRP) en la vista de árbol.

Ilustración 7-107. GVRP Parameters (Parámetros de GVRP)



GVRP Global Status (Estado global de GVRP): Habilita o inhabilita GVRP en el dispositivo. De forma predeterminada, el GVRP está inhabilitado.

Interface (Interfaz): El puerto o LAG para el que se activa GVRP.

GVRP State (Estado de GVRP): Habilita o inhabilita GVRP en una interfaz.

Dynamic VLAN Creation (Creación de VLAN dinámica): Habilita o inhabilita la creación de VLAN a través del GVRP.

GVRP Registration (Registro de GVRP): El estado de registro del GVRP.

Habilitación de GVRP en el dispositivo

1. Abra la página **GVRP Global Parameters** (Parámetros globales de GVRP).
2. Seleccione **Enable** (Activar) en el campo **GVRP Global Status** (Estado global de GVRP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

GVRP se habilita en el dispositivo.

Habilitación del registro de VLAN a través de GVRP

1. Abra la página GVRP Global Parameters (Parámetros globales de GVRP).
2. Seleccione **Enable** (Activar) en el campo **GVRP Global Status** (Estado global de GVRP) para la interfaz pertinente.
3. Seleccione **Enable** (Activar) en el campo **GVRP Registration** (Registro de GVRP).
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se habilita el registro de VLAN GVRP en el puerto, y el dispositivo se actualiza.

Configuración de GVRP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar GVRP tal como aparecen en la página GVRP Global Parameters (Parámetros globales de GVRP).

Tabla 7-71. Comandos de la CLI para los parámetros globales de GVRP

Comando de la CLI	Descripción
<code>gvrp enable</code> (global)	Habilita el GVRP globalmente.
<code>gvrp enable</code> (interface)	Habilita el GVRP en una interfaz.
<code>gvrp vlan-creation-forbid</code>	Habilita o inhabilita la creación de VLAN dinámica.
<code>gvrp registration-forbid</code>	Extrae todas las VLAN del registro e impide la creación o el registro de VLAN dinámicas en el puerto.
<code>show gvrp configuration</code> [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]	Muestra información de la configuración de GVRP, incluidos los valores de temporizador, si la creación de GVRP y VLAN dinámicas está activada y qué puertos están ejecutando GVRP.
<code>show gvrp error-statistics</code> [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]	Muestra las estadísticas de error de GVRP.
<code>show gvrp statistics</code> [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]	Muestra las estadísticas de GVRP.
<code>clear gvrp statistics</code> [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]	Borra toda la información de estadísticas del GVRP.

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

```

console(config)# gvrp enable

console(config)# interface ethernet g1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device.

```

Maximum VLANs: 223						
Port (s)	GVRP-Status	Registration	DynamicVLAN Creation	Timers (milliseconds) Join	Leave	Leave All
---	-----	-----	-----	-----	-----	-----
g1	Enabled	Forbidden	Disabled	200	900	10000
g2	Disabled	Normal	Enabled	200	600	10000

Agregado de puertos

El agregado de puertos optimiza la utilización de los puertos al conectar un grupo de puertos para que formen un único LAG (grupo agregado de conexiones). El agregado de puertos multiplica la amplitud de banda entre los dispositivos, aumenta la flexibilidad de los puertos y proporciona redundancia de la conexión. El dispositivo admite hasta ocho LAG y ocho puertos por LAG por sistema.

Cada LAG consta de puertos de la misma velocidad, establecida en el modo dúplex completo. Los puertos de un LAG pueden ser de diferentes tipos de soportes (UTP/Fibra, o de diferentes tipos de fibra), siempre que funcionen a la misma velocidad.

Las conexiones agregadas se pueden asignar manual o automáticamente habilitando el protocolo de control de agregado de conexiones (LACP) en las conexiones pertinentes. El dispositivo proporciona equilibrio de carga de LAG en función de las direcciones MAC de origen y de destino.

El sistema trata las conexiones agregadas como un único puerto lógico. De manera específica, la conexión agregada tiene atributos de puerto similares a un puerto no agregado, incluida la negociación automática, la velocidad, el establecimiento del modo dúplex, etc.

El dispositivo admite LAG estáticos y LAG de protocolo de control de agregado de conexiones (LACP). Los LAG de LACP negocian las conexiones de los puertos agregados con otros puertos LACP ubicados en un dispositivo distinto. Si los demás puertos de dispositivo también son puertos LACP, los dispositivos establecen un LAG entre ellos.

Hay que seguir las siguientes pautas cuando se agreguen puertos a un LAG:

- 1 No hay ninguna interfaz de nivel 3 definida en el puerto.
- 1 El puerto no pertenece a ninguna VLAN.
- 1 El puerto no pertenece a ningún otro LAG.
- 1 El puerto no es un puerto duplicado.
- 1 La prioridad 802.1p del puerto es igual a la prioridad 802.1p del LAG.
- 1 La fiabilidad de la calidad de servicio no está inhabilitada en el puerto.
- 1 GVRP no está habilitado.

 **NOTA:** Los puertos pueden configurarse como puertos de LACP sólo si no forman parte de un LAG configurado previamente

El dispositivo utiliza una función hash para determinar qué tramas se transportan en qué miembro de la conexión agregada. La función hash equilibra estadísticamente la carga de los miembros de la conexión agregada. El dispositivo considera la conexión agregada como un puerto lógico único.

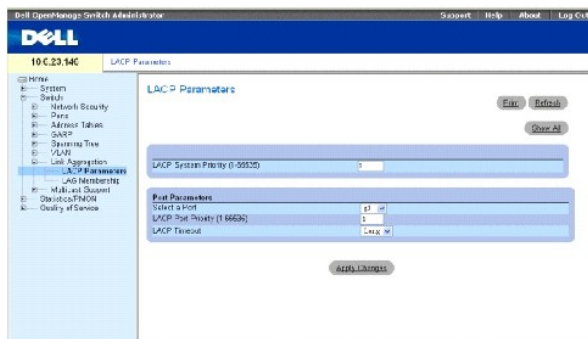
Cada conexión agregada tiene un tipo de puerto de conexión agregada, incluidos puertos Gigabit Ethernet. Los puertos sólo se pueden agregar a una conexión agregada si son el mismo tipo de puerto. Cuando los puertos se eliminan de una conexión agregada, los puertos vuelven a la configuración de puerto original. Para abrir la página **Link Aggregation** (Agregado de conexiones), haga clic en **Switch**→ **Link Aggregation** (Conmutador→ Agregado de conexiones) en la vista de árbol.

Definición de los parámetros del LACP

La página **LACP Parameters** (Parámetros de LACP) contiene campos para configurar los LAG de LACP. Los puertos agregados se pueden conectar en grupos de puertos de agregado de conexiones. Cada grupo consta de puertos con la misma velocidad.

Las conexiones agregadas se pueden configurar manualmente o establecer automáticamente habilitando el protocolo de control de agregado de conexiones (LACP) en las conexiones pertinentes. Para abrir la página [LACP Parameters](#) (Parámetros de LACP), haga clic en **Switch**→ **Link Aggregation**→ **LACP Parameters** (Conmutador→ Agregado de conexiones→ Parámetros de LACP) en la vista de árbol.

Ilustración 7-108. LACP Parameters (Parámetros de LACP)



LACP System Priority (1-65535) (Prioridad del sistema de LACP [1-65535]): El valor de prioridad de LACP para la configuración global. El rango posible es 1 - 65535. El valor predeterminado es 1.

Select a Port (Seleccionar un puerto): El número de puerto al que se asignan los valores de tiempo de espera y de prioridad.

LACP Port Priority (1-65535) (Prioridad del puerto de LACP [1-65535]): El valor de prioridad de LACP para el puerto.

LACP Timeout (Tiempo de espera de LACP): El tiempo de espera administrativo de LACP. Los valores de campo posibles son:

Short (Breve): Especifica un valor de tiempo de espera breve.

Long (Prolongado): Especifica un valor de tiempo de espera prolongado.

Definición de parámetros globales de agregado de conexiones

1. Abra la página [LACP Parameters](#) (Parámetros de LACP).
2. Complete el campo **LACP System Priority** (Prioridad del sistema de LACP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se definen, y el dispositivo se actualiza.

Definición de parámetros de puertos de agregado de conexiones

1. Abra la página [LACP Parameters](#) (Parámetros de LACP).
2. Complete los campos del área **Port Parameters** (Parámetros de puerto).
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros se definen, y el dispositivo se actualiza.

Visualización de la tabla de parámetros de LACP

1. Abra la página [LACP Parameters](#) (Parámetros de LACP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **LACP Parameters Table** (Tabla de parámetros de LACP).

Configuración de los parámetros de LACP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar parámetros de LACP tal como aparecen en la página [LACP Parameters](#) (Parámetros de LACP).

Tabla 7-72. Comandos de la CLI para los parámetros de LACP

Comando de la CLI	Descripción
<code>lACP system-priority <i>valor</i></code>	Configura la prioridad del sistema.
<code>lACP port-priority <i>valor</i></code>	Configura el valor de prioridad para los puertos físicos.
<code>lACP timeout {long short}</code>	Asigna un tiempo de espera de LACP administrativo.
<code>show lACP ethernet <i>interfaz</i> [<i>parameters</i> <i>statistics</i> <i>protocol-state</i>]</code>	Muestra información sobre LACP relativa a los puertos Ethernet.

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

```

Console (config)# lACP system-priority 120

Console (config)# interface ethernet g1

Console (config-if)# lACP port-priority 247

Console (config-if)# lACP timeout long

Console (config-if)# end

Console# show lACP ethernet g1 statistics

Port g1 LACP Statistics:

LACP PDUs sent:2

LACP PDUs received:2

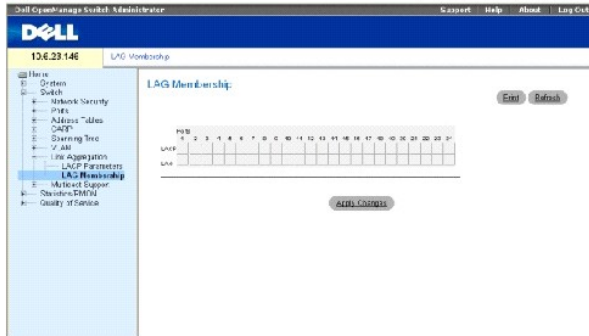
```

Definición de la pertenencia a LAG

La página [LAG Membership](#) (Pertenencia a LAG) contiene campos para asignar puertos a LAG. Los LAG pueden incluir hasta 8 puertos. Cuando se agrega un puerto a un LAG, el puerto adquiere las propiedades del LAG. Si el puerto no se puede configurar con las propiedades de LAG, se genera una captura y el puerto funciona con su configuración predeterminada.

La página [LAG Membership](#) (Pertenencia a LAG) contiene campos para asignar puertos a LAG. Para abrir la página [LAG Membership](#) (Pertenencia a LAG), haga clic en **Switch** → **Link Aggregation** → **LAG Membership** (Conmutador → Agregado de conexiones → Pertenencia a LAG) en la vista de árbol.

Ilustración 7-109. LAG Membership (Pertenencia a LAG)



LACP: Agrega el puerto a un LAG, mediante LACP.

LAG: Agrega un puerto a un LAG e indica el LAG específico al que pertenece el puerto.

Configuración de un puerto para un LAG o LACP

1. Abra la página [LAG Membership](#) (Pertenencia a LAG).
2. En la fila de LAG (la segunda fila), pulse alternando el botón en un número específico para agregar o eliminar el puerto de ese número de LAG.
3. En la fila de LACP (la primera fila), pulse alternando el botón que hay bajo el número de puerto para asignar el LACP o el LAG estático.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se agrega al LAG o LACP, y el dispositivo se actualiza.

Asignación de puertos a LAG mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para asignar puertos a LAG tal como aparecen en la página [LAG Membership](#) (Pertenencia a LAG).

Tabla 7-73. Comandos de la CLI para la pertenencia a LAG

Comando de la CLI	Descripción
<code>interface port-channel número-canal-puerto</code>	Entra en el modo de configuración de interfaz de un canal de puertos específico.
<code>channel-group número-canal-puerto mode {on auto}</code>	Asocia un puerto con un canal de puertos. Utilice la variedad no form de este comando para eliminar la configuración del grupo de canales de la interfaz.
<code>show interfaces port-channel [número-canal-puerto]</code>	Muestra información del canal de puertos.

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

```
console# config
console(config)# interface ethernet g1
console(config-if)# channel-group 1 mode on
console(config-if)# 01-Jan-2000 01:47:18 %LINK-W-Down: chl


console (config-if)#
```

Compatibilidad con el reenvío de multidifusión

El reenvío de multidifusión permite reenviar un solo paquete a varios destinos. El servicio de multidifusión de nivel 2 se basa en el conmutador de nivel 2 que recibe un solo paquete direccionado a una dirección de multidifusión específica. El reenvío de multidifusión crea copias del paquete, y transmite los paquetes a los puertos pertinentes.

El dispositivo admite:

- 1 **Forwarding L2 Multicast Packets** (Reenvío de paquetes de multidifusión de nivel 2): Habilitado de manera predeterminada, y no configurable.

 **NOTA:** El sistema admite el filtrado de multidifusión para 63 grupos de multidifusión.

- 1 **Filtering L2 Multicast Packets** (Filtrado de paquetes de multidifusión de nivel 2): Habilita el reenvío de paquetes de nivel 2 a las interfaces. Si el filtrado de multidifusión está inhabilitado, los paquetes de multidifusión se acumulan en los puertos pertinentes.

Para abrir la página **Multicast Support** (Compatibilidad con multidifusión), haga clic en **Switch** → **Multicast Support** (Conmutador → Compatibilidad con multidifusión) en la vista de árbol.

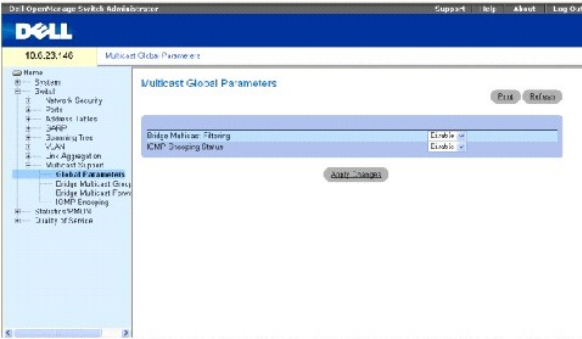
Definición de los parámetros globales de multidifusión

La conmutación de nivel 2 reenvía paquetes de multidifusión a todos los puertos de VLAN pertinentes de manera predeterminada, tratando el paquete como un paquete de transmisión de multidifusión. Aunque se trata de una acción funcional, en el sentido de que todos los puertos/nodos relevantes reciben una copia de la trama, puede resultar poco práctico puesto que los puertos/nodos pueden recibir tramas irrelevantes que sólo necesita un subconjunto de los puertos de dicha VLAN. Los filtros de reenvío de multidifusión habilitan el reenvío de paquetes de nivel 2 a los subconjuntos de los puertos, definidos en la base de datos de filtros de multidifusión.

Cuando se habilita la inspección IGMP de manera global, se programa el ASIC de conmutación para que reenvíe todos los paquetes de IGMP a la CPU. La CPU analiza los paquetes entrantes y determina qué puertos se van a unir a qué grupos de multidifusión, qué puertos tienen enrutadores de multidifusión que generan consultas de IGMP y qué protocolos enrutadores reenvían paquetes y tráfico de multidifusión. Un puerto que quiere unirse a un grupo de multidifusión específico emite un informe IGMP en el que especifica dicho grupo de multidifusión. Este proceso da como resultado la creación de la base de datos de filtrado de multidifusión.

La página [Multicast Global Parameters](#) (Parámetros globales de multidifusión) contiene campos para habilitar la inspección IGMP en el dispositivo. Para abrir la página [Multicast Global Parameters](#) (Parámetros globales de multidifusión), haga clic en **Switch** → **Multicast Support** → **Global Parameters** (Conmutador → Compatibilidad con multidifusión → Parámetros globales) en la vista de árbol.

Ilustración 7-110. Multicast Global Parameters (Parámetros globales de multidifusión)



Bridge Multicast Filtering (Filtrado de multidifusión de puente): Habilita o inhabilita el filtrado de multidifusión de puente. El valor predeterminado es Disabled (Inhabilitado). La inspección IGMP sólo se puede habilitar si el filtrado de multidifusión de puente está habilitado.

IGMP Snooping Status (Estado de inspección IGMP): Habilita o inhabilita la inspección IGMP en el dispositivo. El valor predeterminado es Disabled (Inhabilitado).

Habilitación del filtrado de multidifusión de puente en el dispositivo

1. Abra la página [Multicast Global Parameters](#) (Parámetros globales de multidifusión).
2. Seleccione **Enable** (Activar) en el campo **Bridge Multicast Filtering** (Filtrado de multidifusión de puente).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La multidifusión de puente se habilita en el dispositivo.

Habilitación de la inspección IGMP en el dispositivo

1. Abra la página [Multicast Global Parameters](#) (Parámetros globales de multidifusión).
2. Seleccione **Enable** (Activar) en el campo **IGMP Snooping Status** (Estado de inspección IGMP).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La inspección IGMP se habilita en el dispositivo.

Habilitación del reenvío de multidifusión y la inspección IGMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para habilitar el reenvío de multidifusión y la inspección IGMP tal como aparecen en la página [Multicast Global Parameters](#) (Parámetros globales de multidifusión).

Tabla 7-74. Comandos de la CLI para el reenvío de multidifusión y la inspección

Comando de la CLI	Descripción
<code>bridge multicast filtering</code>	Habilita el filtrado de direcciones de multidifusión.
<code>ip igmp snooping</code>	Habilita la inspección IGMP (protocolo de administración de grupos de Internet).

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

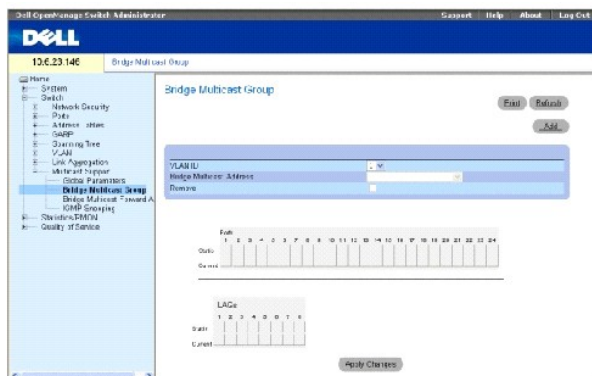
```
Console (config)# bridge multicast filtering
Console (config)# ip igmp snooping
```


Adición de miembros de dirección de multidifusión de puente

En la página [Bridge Multicast Group](#) (Grupo de multidifusión de puente) se muestran los puertos y los LAG conectados al grupo de servicio de multidifusión de las tablas **Ports** (Puertos) y **LAGs** (LAG). En las tablas de puertos y LAG también se refleja el modo en que el puerto o los LAG se han unido al grupo de multidifusión. Los puertos pueden agregarse bien a los grupos existentes o a grupos de servicio de multidifusión. La página [Bridge Multicast Group](#) (Grupo de multidifusión de puente) permite la creación de nuevos grupos de servicio de multidifusión. La página [Bridge Multicast Group](#) (Grupo de multidifusión de puente) también asigna puertos a un grupo específico de direcciones de servicio de multidifusión.

Para abrir la página **Bridge Multicast Group** (Grupo de multidifusión de puente), haga clic en **Switch**→ **Multicast Support**→ **Bridge Multicast Address** (Conmutador→ Compatibilidad con multidifusión→ Dirección de multidifusión de puente) en la vista de árbol.

Ilustración 7-111. Bridge Multicast Group (Grupo de multidifusión de puente)



VLAN ID (ID de VLAN): Identifica una VLAN y contiene información sobre la dirección de grupo de multidifusión.

Bridge Multicast Address (Dirección de multidifusión de puente): Identifica la dirección MAC/IP del grupo de multidifusión.

Remove (Eliminar): Si se selecciona esta opción, se elimina una dirección de multidifusión de puente.

Ports (Puertos): El puerto que se puede agregar a un servicio de multidifusión.

LAGs (LAG): Los LAG que se pueden agregar a un servicio de multidifusión.

La siguiente tabla contiene los valores de gestión de los miembros de LAG y el puerto IGMP:

Tabla 7-75. Valores de control de la tabla de los miembros de LAG/puerto IGMP

Control de puerto	Definición
D	El puerto/LAG se ha unido al grupo de multidifusión dinámicamente en la fila <i>Current</i> (Actual).
S	Conecta el puerto al grupo de multidifusión como miembro estático en la fila <i>Static</i> (Estático) El puerto/LAG se ha unido al grupo de multidifusión estáticamente en la fila <i>Current</i> (Actual).
F	Prohibido.
Blank	El puerto no está conectado a un grupo de multidifusión.

Adición de direcciones de multidifusión de puente

1. Abra la página [Bridge Multicast Group](#) (Grupo de multidifusión de puente).
2. Haga clic en **Add** (Agregar).

Se abre la página [Add Bridge Multicast Group](#) (Agregar grupo de multidifusión de puente):

Ilustración 7-112. Add Bridge Multicast Group (Agregar grupo de multidifusión de puente)

The screenshot shows the 'Add Bridge Multicast Group' configuration interface. It includes a title bar, a page indicator, and several input fields for configuring a multicast group. The 'VLAN ID' is set to 1. There are buttons for 'GO' next to the IP and MAC address fields. Below the input fields are two tables for selecting ports and LAGs, and an 'Apply Changes' button at the bottom.

3. Defina los campos **VLAN ID** (ID de VLAN) y **New Bridge Multicast Address** (Nueva dirección de multidifusión de puente).
4. Conmute un puerto a la posición **S** para que éste se pueda unir al grupo de multidifusión seleccionado.
5. Conmute un puerto a la posición **F** para prohibir que se puedan agregar direcciones de multidifusión específicas a un puerto específico.
6. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección de multidifusión se asigna al grupo de multidifusión, y el dispositivo se actualiza.

Definición de puertos para que reciban el servicio de multidifusión

1. Abra la página [Bridge Multicast Group](#) (Grupo de multidifusión de puente).
2. Defina los campos **VLAN ID** (ID de VLAN) y **Bridge Multicast Address** (Dirección de multidifusión de puente).
3. Conmute un puerto a la posición **S** para que éste se pueda unir al grupo de multidifusión seleccionado.
4. Conmute un puerto a la posición **F** para prohibir que se puedan agregar direcciones de multidifusión específicas a un puerto específico.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto se asigna al grupo de multidifusión, y el dispositivo se actualiza.

Asignación de LAG para que reciban el servicio de multidifusión

1. Abra la página [Bridge Multicast Group](#) (Grupo de multidifusión de puente).
2. Defina los campos **VLAN ID** (ID de VLAN) y **Bridge Multicast Address** (Dirección de multidifusión de puente).
3. Conmute el LAG a la posición **S** para que éste se pueda unir al grupo de multidifusión seleccionado.
4. Conmute el LAG a la posición **F** para prohibir que se puedan agregar direcciones de multidifusión específicas a un puerto específico.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El LAG se asigna al grupo de multidifusión, y el dispositivo se actualiza.

Administración de miembros de servicio de multidifusión mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes administrar miembros del servicio de multidifusión tal como aparecen en la página [Bridge Multicast Group](#) (Grupo de multidifusión de puente).

Tabla 7-76. Comandos de la CLI para los miembros del servicio de multidifusión

Comando de la CLI	Descripción
<code>bridge multicast address { dirección-multidifusión-mac dirección-multidifusión-ip }</code>	Registra las direcciones de multidifusión de nivel MAC en la tabla de direcciones y agrega puertos estáticos al grupo.
<code>bridge multicast forbidden address { dirección-multidifusión-mac dirección-multidifusión-IP } [add remove] { ethernet lista-interfaz port-channel lista-número-canal-puerto }</code>	Prohíbe la adición de una dirección de multidifusión específica a puertos específicos. Use la variedad no form de este comando para volver al valor predeterminado.
<code>show bridge multicast address-table [vlan id-vlan] [address dirección-multidifusión-mac dirección-multidifusión-ip] [format ip mac]</code>	Muestra la información de la tabla de direcciones MAC de multidifusión.

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

```

Console> enable

Console# config

console(config)#vlan database

console(config-if)#vlan 8

console(config-if)# exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

console(config)#interface vlan 8

console(config-if)# exit

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1,g2

Console(config-if)# exit

Console(config)#exit

Console# show bridge multicast address-table

```

Vlan	MAC Address	Type	Ports
----	-----	----	-----
1	0100.5e02.0203	static	g1, g2

19	0100.5e02.0208	static	g1-8
19	0100.5e02.0208	dynamic	g9-11
Forbidden ports for multicast addresses:			
Vlan	MAC Address	Ports	
----	-----	-----	
1	0100.5e02.0203	g8	
19	0100.5e02.0208	g8	
Console # show bridge multicast address-table format ip			
Vlan	IP Address	Type	Ports
----	-----	-----	-----
1	224-239.130 2.2.3	static	g1, g2
19	224-239.130 2.2.8	static	g1-8
19	224-239.130 2.2.8	dynamic	g9-11
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	-----	-----	
1	224-239.130 2.2.3	g8	
19	224-239.130 2.2.8	g8	

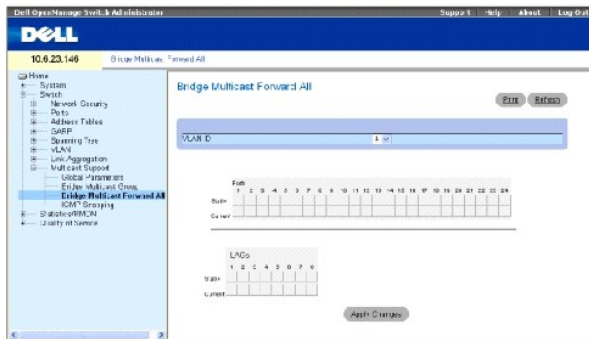
Asignación de parámetros de multidifusión "reenviar todos"

La página [Bridge Multicast Forward All](#) (Multidifusión de puente "reenviar todos") contiene campos para conectar puertos o LAG a un dispositivo conectado a un enrutador/conmutador de multidifusión adyacente. Una vez habilitada la inspección IGMP, los paquetes de multidifusión se reenvían al puerto o VLAN correspondiente.

Para abrir la página [Bridge Multicast Forward All](#) (Multidifusión de puente "reenviar todos"), haga clic en **Switch** → **Multicast Support** → **Bridge Multicast** → **Bridge Multicast Forward All**

(Conmutador → Compatibilidad con multidifusión → Multidifusión de puente → Multidifusión de puente "reenviar todos") en la vista de árbol.

Ilustración 7-113. Bridge Multicast Forward All (Multidifusión de puente "reenviar todos")



VLAN ID (ID de VLAN): Identifica una VLAN.

Ports (Puertos): Los puertos que se puede agregar a un servicio de multidifusión.

LAGs (LAG): Los LAG que se pueden agregar a un servicio de multidifusión.

La [Bridge Multicast Forward All Router/Port Control Settings Table](#) (Tabla de configuración de configuración de control de puerto/enrutador de multidifusión de puente "reenviar todo").

Tabla 7-77. Tabla de configuración de configuración de control de puerto/enrutador de multidifusión de puente "reenviar todos"

Control de puerto	Definición
D	Conecta el puerto al conmutador o enrutador de multidifusión como un puerto dinámico.
S	Conecta el puerto al conmutador o enrutador de multidifusión como un puerto estático.
F	Prohibido.
Blank	El puerto no está conectado a un conmutador o enrutador de multidifusión.

Conecta un puerto a un conmutador o direccionador de multidifusión

1. Abra la página [Bridge Multicast Forward All](#) (Multidifusión de puente "reenviar todos").
2. Defina el campo **VLAN ID** (ID de VLAN).
3. Seleccione un puerto en la tabla **Port Membership** (Pertenencia al puerto) y asigne un valor al puerto.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El puerto está conectado al conmutador o enrutador de multidifusión.

Conecta un LAG a un conmutador o direccionador de multidifusión

1. Abra la página [Bridge Multicast Forward All](#) (Multidifusión de puente "reenviar todos").
2. Defina el campo **VLAN ID** (ID de VLAN).
3. Seleccione un puerto en la tabla **Port Membership** (Pertenencia al puerto) y asigne un valor al LAG.

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

El LAG está conectado al conmutador o enrutador de multidifusión.

Administración de LAG y puertos conectados a enrutadores de multidifusión mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para administrar los LAG y puertos conectados a enrutadores de multidifusión tal como aparecen en la página [Bridge Multicast Forward All](#) (Multidifusión de puente "reenviar todos").

Tabla 7-78. Comandos de la CLI para gestionar LAG y puertos conectados a enrutadores de multidifusión

Comando de la CLI	Descripción
<code>show bridge multicast filtering id-vlan</code>	Muestra la configuración de filtro de multidifusión.
<code>no bridge multicast forbidden forward-all</code>	Inhabilita el reenvío de paquetes de multidifusión en un puerto.
<code>bridge multicast forward-all {add remove} {ethernet lista-interfaz port-channel lista-número-canal-puerto}</code>	Habilita el reenvío de todos los paquetes de multidifusión en un puerto. Use la variedad no form de este comando para volver al valor predeterminado.

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

```
console(config)#vlan database

console(config-if)#vlan 8

console(config-vlan)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

Console (config-if)# exit

console(config)#interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# interface VLAN 1

Console (config-if)# bridge multicast forward-all add ethernet g8
```

```

Console(config-if)# end

Console# show bridge multicast filtering 1

```

Filtering: Enabled		
VLAN:	Forward-All	
Port	Static	Status
-----	-----	-----
g1	Forbidden	Filter
g2	Forward	Forward(s)
g3	-	Forward(d)

Inspección IGMP

La página [IGMP Snooping](#) (Inspección IGMP) contiene campos para agregar miembros de IGMP. Para abrir la página [IGMP Snooping](#) (Inspección IGMP), haga clic en **Switch** → **Multicast Support** → **IGMP Snooping** (Conmutador → Compatibilidad con multidifusión → Inspección IGMP) en la vista de árbol.

Ilustración 7-114. IGMP Snooping (Inspección IGMP)



VLAN ID (ID de VLAN): Especifica el ID de VLAN.

IGMP Snooping Status (Estado de inspección IGMP): Habilita o inhabilita la inspección IGMP en la VLAN.

Auto Learn (Obtención automática): Habilita o inhabilita la obtención automática en el dispositivo.

Host Timeout (1-2147483647) (Tiempo de espera de sistema principal [1-2147483647]): El tiempo que transcurre antes de que caduque una entrada de

inspección IGMP. El valor predeterminado es 260 segundos.

Multicast Router Timeout (1-2147483647) (Tiempo de espera del enrutador de multidifusión [1-2147483647]): El tiempo que transcurre antes que caduque una entrada del enrutador de multidifusión. El valor predeterminado es 300 segundos.

Leave Timeout (0-2147483647) (Tiempo de espera de cese [0-2147483647]): El tiempo en segundos que transcurre después que se recibe un mensaje de cese del puerto hasta que la entrada caduca. **User-defined** (Definido por el usuario) permite al usuario establecer un período de tiempo de espera e **Immediate Leave** (Cese inmediato) especifica un período de tiempo de espera inmediato. El tiempo de espera predeterminado es 10 segundos.

Habilitación de la inspección IGMP en el dispositivo

1. Abra la página [IGMP Snooping](#) (Inspección IGMP).
2. Seleccione el ID de VLAN del dispositivo en el que sea necesario habilitar la inspección IGMP.
3. Seleccione **Enable** (Activar) en el campo **IGMP Snooping Status** (Estado de inspección IGMP).
4. Complete los campos de esta página.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La inspección IGMP se habilita en el dispositivo.

Visualización de la tabla de inspección IGMP

1. Abra la página [IGMP Snooping](#) (Inspección IGMP).
2. Haga clic en **Show All** (Mostrar todo).

Se abre la **IGMP Snooping Table** (Tabla de inspección IGMP).

Configuración de la inspección IGMP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para configurar [IGMP Snooping](#) (Inspección IGMP) en el dispositivo:

Tabla 7-79. Comandos de la CLI para la inspección IGMP

Comando de la CLI	Descripción
<code>ip igmp snooping</code>	Habilita la inspección IGMP (protocolo de administración de grupos de Internet).
<code>ip igmp snooping mrouter learn-pim-dvmrp</code>	Habilita la obtención automática de los puertos de enrutador de multidifusión en el contexto de una VLAN específica.
<code>ip igmp snooping host-time-out tiempo-espera</code>	Configura el tiempo de espera del sistema principal.
<code>ip igmp snooping mrouter-time-out tiempo-espera</code>	Configura el tiempo de espera del enrutador de multidifusión.
<code>ip igmp snooping leave-time-out {tiempo-espera cese-inmediato}</code>	Configura el tiempo de espera de cese.
<code>show ip igmp snooping groups [vlan ID-VLAN] [address dirección-multidifusión-IP]</code>	Muestra los grupos de multidifusión obtenidos por la inspección IGMP.
<code>show ip igmp snooping interface id-vlan</code>	Muestra la configuración de inspección IGMP
<code>show ip igmp snooping mrouter [interface id-vlan]</code>	Muestra información sobre las interfaces de enrutador obtenidas dinámicamente.

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

```
Console> enable

Console# config
```



```
Console (config)# ip igmp snooping

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp

Console (config-if)# ip igmp snooping host-time-out 300

Console (config-if)# ip igmp snooping mrouter-time-out 200

Console (config-if)# exit

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console(config)#exit

Console # show ip igmp snooping groups

Vlan IP Address Querier Ports
-----
1 224-239.130|2.2.3 Yes g1, g2

19 224-239.130|2.2.8 Yes g9-11

Console # show ip igmp snooping interface 1

IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1

IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 60 sec
```

IGMP mrouter timeout is 200 sec

Automatic learning of multicast router ports is enabled

Console # show ip igmp snooping mrouter

VLAN	Ports
----	-----
1	g1

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración de la información del sistema

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Definición de la información general del dispositivo](#)
- [Configuración de los valores de SNMP](#)
- [Gestión de registros](#)
- [Definición de las direcciones IP del dispositivo](#)
- [Ejecución de los diagnósticos de los cables](#)
- [Gestión de la seguridad del dispositivo](#)
- [Definición de los parámetros de SNMP](#)
- [Gestión de archivos](#)
- [Definición de la configuración avanzada](#)

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

Ilustración 6-15. System (Sistema)



Definición de la información general del dispositivo

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

Visualización de la página de activos

La página [Asset](#) (Activo) contiene parámetros para configurar información general del dispositivo, incluido el nombre, la ubicación y el contacto del sistema, la dirección MAC del sistema, el ID de objetos del sistema, la fecha, la hora y el tiempo de actividad del sistema. Para abrir la página [Asset](#) (Activo) haga clic en System → General → Asset (Sistema → General → Activo) en la vista de árbol.

Ilustración 6-16. Asset (Activo)



System Name (0-160 Characters) (Nombre del sistema [0 - 160 caracteres]): determina el nombre del dispositivo definido por el usuario.

System Contact (0-160 Characters) (Contacto del sistema [0 - 160 caracteres]): especifica el nombre de la persona de contacto.

System Location (0-160 Characters) (Ubicación del sistema [0 - 160 caracteres]): especifica la ubicación en la que se ejecuta actualmente el sistema.

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

Sys Object ID (ID de los objetos del sistema): especifica la identificación de autorización del proveedor correspondiente al sistema de gestión de red contenida en la entidad.

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

Asset Tag (0-16 Characters) (Etiqueta de activo [0 - 16 caracteres]): especifica la referencia al dispositivo definida por el usuario.

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

Date (MM/DD/YY) (Fecha [MM/DD/AA]): especifica la fecha actual. El formato es el de mes, día y año, por ejemplo, 11/10/02 corresponde a 10 de noviembre de 2002.

Time (HH:MM:SS) (Hora [HH:MM:SS]): especifica la hora. El formato es el de horas, minutos y segundos, por ejemplo, 20:12:03 corresponde a las ocho y doce minutos, tres segundos de la noche.

System Up Time (Tiempo de actividad del sistema): especifica el tiempo transcurrido desde el último restablecimiento del dispositivo. La hora del sistema tiene el formato siguiente: días, horas, minutos y segundos. Por ejemplo, 41 días, 2 horas, 22 minutos y 15 segundos.

Definición de la información del sistema:

1. Abra la página [Asset](#) (Activo).
2. Defina los campos pertinentes.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Los parámetros del sistema se definen, y el dispositivo se actualiza.

Inicio de una sesión Telnet:

1. Abra la página [Asset](#) (Activo).
2. Haga clic en **Telnet**.

Se ha iniciado una sesión Telnet.

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

En la siguiente tabla se resumen los comandos equivalentes de la CLI para ver y configurar campos que se visualizan en la página [Asset](#) (Activo).

Tabla 6-11. Comandos de la CLI del activo

Comando de la CLI	Description
<code>hostname nombre</code>	Especifica o modifica el nombre del sistema principal del dispositivo.
<code>snmp-server contact text</code>	Configura un contacto del sistema.
<code>snmp-server location text</code>	Especifica la información sobre dónde se ubica el dispositivo.
<code>show clock [detail]</code>	Muestra la hora y fecha del reloj del sistema.
<code>show system id</code>	Muestra la información de la etiqueta de servicio.
<code>show system</code>	Muestra información del sistema.
<code>asset-tag</code>	Establece la etiqueta del activo del dispositivo.

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

```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_York

Console(config)#exit

Console# exit

Console (config)# asset-tag lqwepot

Console> clock set 13:32:00 7 Dec 2004

Console> show clock

13:32:00 (UTC+0) Dec 7 2004

No time source
```

DELL Switch# show system		
System Description:		Ethernet Routing Switch

System Up Time (days, hour:min:sec):		0,00:04:17
System Contact:		epk
System Name:		DELL Switch
System Location:		R&D
System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324		
Power Supply	Status	
-----	-----	
Main	OK	
Redundant	OK	
FAN	Status	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

Definición de la configuración de la hora del sistema

La página [Time Synchronization](#) (Sincronización de la hora) contiene campos para definir los parámetros de la hora del sistema para el reloj del hardware y para el reloj de SNTP externo. Si la hora del sistema utiliza un reloj de SNTP externo y este reloj falla, la hora del sistema utiliza el reloj del hardware local. El horario de verano se puede activar en el dispositivo. A continuación, se facilita una lista del período del horario de verano en determinados países:

- 1 Albania: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Alemania: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Armenia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Australia: desde finales de octubre hasta finales de marzo.
- 1 Australia - Tazmania: desde principios de octubre hasta finales de marzo.
- 1 Austria: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Bahamas: desde abril hasta octubre, en combinación con el horario de verano de los EE.UU.

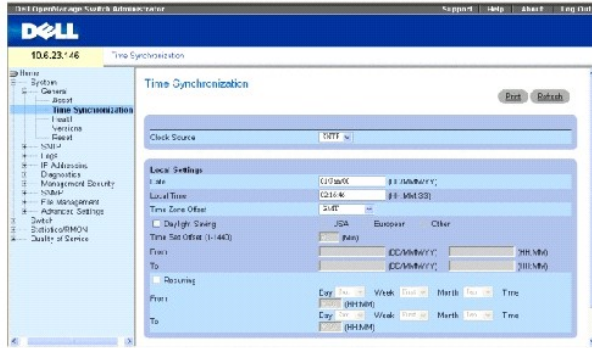
- 1 Bélgica: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Bielorrusia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Brasil: desde el tercer domingo de octubre hasta el tercer sábado de marzo. Durante el período del horario de verano, los relojes de Brasil se adelantan una hora en la mayor parte del Sudeste del país.
- 1 Canadá: desde el primer domingo de abril hasta el último domingo de octubre. El horario de verano está normalmente regulado por los gobiernos territoriales y provinciales. Pueden haber excepciones en determinados municipios.
- 1 Chile: la Isla de Pascua, desde el 9 de marzo hasta el 12 de octubre. El primer domingo de marzo o después del 9 de marzo.
- 1 China: China no tiene horario de verano.
- 1 Chipre: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Cuba: desde el último domingo de marzo hasta el último domingo de octubre.
- 1 Dinamarca: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Egipto: desde el último viernes de abril hasta el último jueves de septiembre.
- 1 España: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Estados Unidos de América: desde el primer domingo de abril a las 02:00 de la madrugada hasta el último domingo de octubre a las 02:00 de la madrugada.
- 1 Estonia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Finlandia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Francia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Grecia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Hungría: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 India: India no tiene horario de verano.
- 1 Irán: desde el primer día de Farvardin hasta el primer día de Mehr.
- 1 Iraq: desde el 1 de abril hasta el 1 de octubre.
- 1 Irlanda: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Israel: varía cada año.
- 1 Italia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Japón: Japón no tiene horario de verano.
- 1 Jordania: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Letonia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Líbano: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Lituania: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Luxemburgo: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Macedonia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 México: desde el primer domingo de abril a las 02:00 de la madrugada hasta el último domingo de octubre a las 02:00 de la madrugada.
- 1 Moldova: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Montenegro: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Nueva Zelanda: desde el primer domingo de octubre hasta el primer domingo después del 14 de marzo.
- 1 Noruega: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Países Bajos: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Paraguay: desde el 6 de abril hasta el 7 de septiembre.
- 1 Polonia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Portugal: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Reino Unido: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 República Eslovaca: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Rumania: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Rusia: desde el 29 de marzo hasta el 25 de octubre.
- 1 Serbia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Siria: desde el 31 de marzo hasta el 30 de octubre.
- 1 Sudáfrica: Sudáfrica no tiene horario de verano.
- 1 Suecia: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Suiza: desde el último fin de semana de marzo hasta el último fin de semana de octubre.
- 1 Taiwán: Taiwán no tiene horario de verano.

- 1 Turquía: desde el último fin de semana de marzo hasta el último fin de semana de octubre.

Para obtener más información sobre el SNTP, consulte el apartado "[Configuración de los valores de SNTP](#)".

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

Ilustración 6-17. Time Synchronization (Sincronización de la hora)



Código fuente del reloj

Código fuente del reloj: el código fuente utilizado para establecer el reloj del sistema. Los valores de campo posibles son:

SNTP: especifica que la hora del sistema está establecida a través de un servidor SNTP. Para obtener más información, consulte el apartado "[Configuración de los valores de SNTP](#)".

None (Ninguno): especifica que la hora del sistema no está establecida por un código fuente externo.

Configuración local

Date (Fecha): define la fecha del sistema. El formato del campo es el de Día:Mes:Año, por ejemplo, 4 de mayo de 2050.

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

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

Hay dos tipos de valores para el horario de verano: una fecha específica en un año determinado o la misma fecha independientemente del año. En el caso de un valor específico en un determinado año, complete la zona del **Daylight Savings** (Horario de verano), y para un valor recurrente, complete la zona **Recurring** (Recurrente).

Daylight Savings (Horario de verano): activa el horario de verano (DST) en el dispositivo basado en la ubicación de los dispositivos. Los valores de campo posibles son:

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

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

Other (Otros): las definiciones de DST están especificadas por el usuario en función de la localidad del dispositivo. Si se selecciona Other (Otros), los campos **From** (Desde) y **To** (Hasta) se deben definir.

From (Desde): define la fecha en que se empieza a aplicar el DST en países que no sean EE.UU. o Europa, en el formato de DíaMesAño, en un campo y la hora en otro. Por ejemplo, el DST empieza el 25 de octubre de 2007 a las 5:00 h, de modo que los dos campos serán 25oct07 y 5:00. Los valores de campo posibles son:

Date (Fecha): fecha en la que se aplica el DST. El rango posible del campo es de 1 a 31.

Month (Mes): mes del año en que se aplica el DST. El rango posible del campo es de enero a diciembre.

Year (Año): año en el que se aplica el DST configurado.

Time (Hora): hora en que se aplica el DST. El formato del campo es Hora:Minuto, por ejemplo, 05:30.

To (Hasta): define la fecha en la que finaliza el DST en países que no sean EE.UU. o Europa (en el formato de DíaMesAño) en un campo y la hora en otro. Por ejemplo, si el DST finaliza el 23 de marzo de 2008 a las 12:00 h, los dos campos serán 23mar08 y 12:00. Los valores de campo posibles son :

Date (Fecha): fecha en la que deja de aplicarse el DST. El rango posible del campo es de 1 a 31.

Month (Mes): mes del año en que deja de aplicarse el DST. El rango posible del campo es de enero a diciembre.

Year (Año): año en el que deja de aplicarse el DST configurado.

Time (Hora): hora en que se aplica el DST. El formato del campo es Hora:Minuto, por ejemplo, 05:30.

Recurring (Recurrente): define la hora en la que se aplica el DST en países que no sean EE.UU. o Europa, en los que el DST es constante todos los años. Los valores de campo posibles son:

From (Desde): define la fecha en la que se aplica el DST cada año. Por ejemplo, el DST empieza localmente cada segundo domingo de abril a las 5:00 de la mañana. Los valores de campo posibles son:

Day (Día): día de la semana a partir del cual se aplica el DST cada año. El rango posible del campo es domingo-sábado.

Week (Semana): la semana del mes a partir de la cual se aplica el DST cada año. El rango posible del campo es de 1 a 5.

Month (Mes): el mes del año en el que el DST se aplica cada año. El rango posible del campo es de enero a diciembre.

Time (Hora): hora en la que se aplica el DST cada año. El formato del campo es Hora:Minuto, por ejemplo, 02:10.

To (Para): define la hora recurrente en la que deja de aplicarse el DST cada año. Por ejemplo, el DST finaliza localmente cada cuarto viernes de octubre a las 5:00 de la mañana. Los valores de campo posibles son:

Day (Día): el día de la semana en el que deja de aplicarse el DST cada año. El rango posible del campo es domingo-sábado.

Week (Semana): la semana del mes en la que deja de aplicarse el DST cada año. El rango posible del campo es de 1 a 5.

Month (Mes): el mes del año en el que deja de aplicarse el DST cada año. El rango posible del campo es de enero a diciembre.

Time (Hora): la hora en la que deja de aplicarse el DST cada año. El formato del campo es Hora:Minuto, por ejemplo, 05:30.

Selección del código fuente del reloj

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

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

Definición de la configuración del reloj local

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

Se aplica la configuración del reloj local.

Definición de la configuración del reloj de SNTP externo

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

Se aplica la configuración del reloj externo.

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

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

Tabla 6-12. Clock Setting CLI Commands (Comandos de la CLI para la configuración del reloj)

CLI	Description
<code>clock source {sntp}</code>	Configura un recurso de tiempo externo para el reloj del sistema.
<code>clock timezone <i>diferencia horaria</i> [<i>minutes diferencia de minutos</i>][<i>zone sigla</i>]</code>	Establece la zona horaria para mostrarla en pantalla.
<code>clock summer-time</code>	Configura el sistema de modo que el cambio al horario de verano (DST) sea automático.
<code>clock summer-time recurring {usa eu {<i>semana día mes hh:mm / semana día mes hh:mm</i>}} [<i>offset diferencia</i>] [<i>zone sigla</i>]</code>	Configura el sistema de modo que el cambio al horario de verano sea automático (de acuerdo con los estándares de EE.UU. y Europa).
<code>clock summer-time date <i>fecha mes año hh:mm / fecha mes año hh:mm</i> [<i>offset diferencia</i>] [<i>zone sigla</i>]</code>	Configura el sistema de modo que el cambio al horario de verano (DST) sea automático durante un determinado período (formato fecha/mes/año).

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

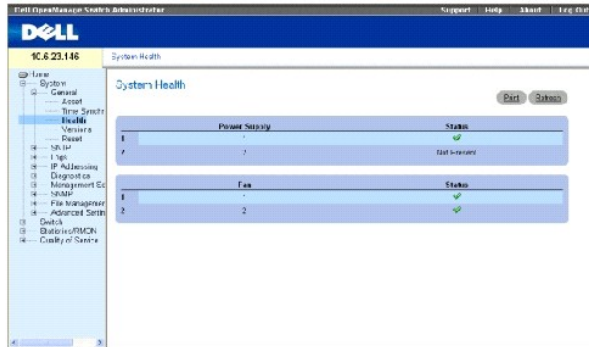
```
Console(config)# clock timezone -6 zone CST

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



Visualización de la información del estado del sistema

En la página [System Health](#) (Estado del sistema) aparece la información sobre el hardware del dispositivo físico. Para abrir la página [System Health](#) (Estado del sistema), haga clic en **System**→**General**→**Health** (Sistema → General → Estado) en la vista de árbol.

Ilustración 6-18. System Health (Estado del sistema)





Power Supply Status (Estado del suministro de energía): Estado del principal suministro de energía. Los valores de campo posibles son:

-  — El principal suministro de energía está funcionando con normalidad para la unidad especificada.
-  — El principal suministro de energía no está funcionando con normalidad para la unidad especificada.

Not Present (Inexistente): No hay suministro de energía para la unidad especificada.

Fan (Ventilador): Estado del ventilador del dispositivo. Los valores de campo posibles son:

-  — Los ventiladores funcionan con normalidad para la unidad especificada.
-  — Los ventiladores no funcionan con normalidad para la unidad especificada.

Not Present (Inexistente): No hay ventiladores para la unidad especificada.

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

En la siguiente tabla se muestra un resumen del comando de la CLI equivalente para ver los campos que se muestran en la página [System Health](#) (Estado del sistema).

Tabla 6-13. Comandos de la CLI del estado del sistema

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

DELL Switch# show system	
--------------------------	--

System Description:		Ethernet Routing Switch
System Up Time (days, hour:min:sec):		0,00:04:17
System Contact:		spk
System Name:		DELL Switch
System Location:		R&D
System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324		
Power Supply	Status	
-----	-----	
Main	OK	
Redundant	OK	
FAN	Status	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

Visualización de la página de versiones

La página [Versions](#) (Versiones) contiene información sobre las versiones de software y hardware que se ejecutan actualmente. Para abrir la página [Versions](#) (Versiones), haga clic en System→ General→ Versions (Sistema→ General→ Versiones) en la vista de árbol.

Ilustración 6-19. Versions (Versiones)



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

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

Hardware Version (Versión de hardware): las versiones actuales de hardware que se utilizan en el dispositivo.

Visualización de las versiones del dispositivo mediante la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver los campos que aparecen en la página [Versions](#) (Versiones).

Tabla 6-14. Comandos de la CLI para las versiones

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

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

```

Console> show version

SW version x.xxx (date 23-Jul-xxxx time 17:34:19)

Boot version x.xxx (date 17-Jan-xxxx time 11:48:21)

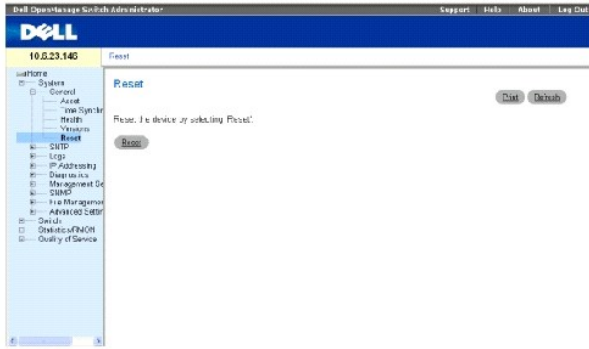
HW version x.x.x

```

Restablecimiento del dispositivo

La página [Reset](#) (Restablecimiento) permite al dispositivo restablecerse desde una ubicación remota. Para abrir la página [Reset](#) (Restablecimiento), haga clic en System→ General→ Reset (Sistema→ General→ Restablecimiento) en la vista de árbol.

Ilustración 6-20. Reset (Restablecimiento)



NOTA: guarde todos los cambios en el archivo Running Configuration (Configuración en ejecución) antes de restablecer el dispositivo. Esto evitará que la configuración actual del dispositivo se pierda. Para obtener más información sobre cómo guardar archivos de configuración, consulte el apartado "[Gestión de archivos](#)".

Restablecimiento del dispositivo

1. Abra la página [Reset](#) (Restablecimiento).
2. Haga clic en Reset (Restablecer).

Aparecerá un mensaje de confirmación.

3. Haga clic en OK (Aceptar).

Se restablecerá el dispositivo. Cuando el dispositivo esté restablecido, se le solicitará que especifique un nombre de usuario y una contraseña.

4. Escriba un nombre de usuario y una contraseña para volver a establecer la conexión con la interfaz web.

Restablecimiento del dispositivo mediante la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para realizar un restablecimiento del dispositivo a través de la CLI:

Tabla 6-15. Comando de la CLI de restablecimiento

Comando de la CLI	Descripción
reload	Recarga el sistema operativo.

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

```

Console >reload

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

Configuración de los valores de SNTP

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

El dispositivo puede hacer un sondeo de los siguientes tipos de servidores en cuanto al tiempo de servidor:

- 1 Difusión única
- 1 Cualquier difusión
- 1 Difusión

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

A continuación se muestra un ejemplo de los niveles:

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

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

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

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

Sondeo para obtener información de difusión única sobre el tiempo

El sondeo para obtener información de difusión única se utiliza para analizar un servidor cuya dirección IP se conoce. Los niveles de tiempo de T1 a T4 se utilizan para determinar la hora del servidor. Se trata del método preferido para sincronizar el cambio de hora.

Sondeo para obtener información de cualquier difusión sobre el tiempo

El sondeo para obtener información de cualquier difusión se utiliza cuando la dirección IP del servidor no se conoce. El primer servidor de cualquier difusión para devolver una respuesta se utiliza para establecer el valor de tiempo. Los niveles de tiempo T3 y T4 se utilizan para determinar la hora del servidor. La utilización de la información del tiempo de cualquier difusión para sincronizar el cambio de hora es preferible a la utilización de la información del tiempo de difusión.

Información del tiempo de difusión

La información de difusión se utiliza cuando la dirección IP del servidor es desconocida. Cuando un mensaje de difusión se envía desde un servidor SNTP, el cliente SNTP está atento a la respuesta. El cliente SNTP no envía solicitudes de información de tiempo ni recibe respuestas del servidor de difusión.

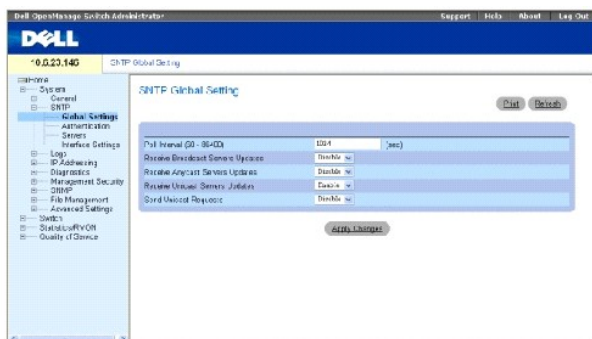
La autenticación de MD5 (Condensado de mensaje 5) protege las rutas de acceso de sincronización de cambio a los servidores SNTP. MD5 es un algoritmo que produce un hash de 128 bits. MD5 es una variedad de MD4, pero con mayor seguridad. MD5 verifica la integridad de la comunicación y autentica su origen.

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

Definición de los parámetros globales SNTP

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

Ilustración 6-21. SNTP Global Settings (Configuración global SNTP)



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

Receive Broadcast Servers Updates (Recepción de actualizaciones de servidores de difusión): realiza un sondeo de los servidores SNTP para obtener información sobre el tiempo del servidor de difusión en las interfaces seleccionadas.

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

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

Poll Unicast Servers (Sondeo de servidores de difusión única): reenvía información de difusión única SNTP al servidor SNTP cuando está activado.

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

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

Tabla 6-16. SNTP Global Parameters CLI Commands (Comandos de la CLI para la configuración global de SNTP)

Comando de la CLI	Description
<code>sntp broadcast client enable</code>	Activa los clientes de difusión SNTP
<code>sntp unicast client enable</code>	Activa los clientes predefinidos de difusión única SNTP

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

```
console> enable

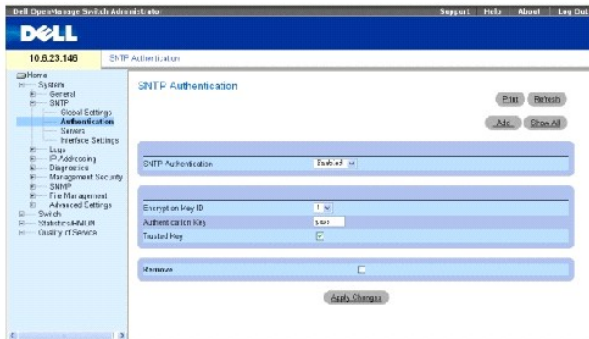
console# configure

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


Definición de los métodos de autenticación SNMP

En la página **SNTP Authentication** (Autenticación SNMP) se activa la autenticación SNMP entre el dispositivo y un servidor SNMP. El método mediante el cual se autentica el servidor SNMP también se selecciona en la página **SNTP Authentication** (Autenticación SNMP). Haga clic en **System** → **SNTP** → **Authentication** (Sistema → SNMP → Autenticación) en la vista de árbol para abrir la página **SNTP Authentication** (Autenticación SNMP).

Ilustración 6-22. SNTP Authentication (Autenticación SNMP)



SNTP Authentication (Autenticación SNMP): activa la autenticación de una sesión SNMP entre el dispositivo y un servidor SNMP cuando está activado.

Encryption Key ID (ID clave de codificación): define la identificación de la clave utilizada para autenticar el servidor SNMP y el dispositivo. El valor del campo puede tener hasta 4.294.967.295 de caracteres.

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

Trusted Key (Clave de confianza): especifica la clave de codificación utilizada para autenticar el servidor SNMP.

Remove (Retirar): elimina la clave seleccionada cuando se marca.

Adición de una clave de autenticación SNMP

1. Abra la página [SNTP Authentication](#) (Autenticación SNMP).
2. A continuación, haga clic en **Add** (Agregar).

La página [Add Authentication Key](#) (Agregar clave de autenticación) se abrirá:

Ilustración 6-23. Add Authentication Key (Agregar clave de autenticación)



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

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

Visualización de la tabla de claves de autenticación

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

La [Authentication Key Table](#) (Tabla de claves de autenticación) se abrirá:

Ilustración 6-24. Authentication Key Table (Tabla de claves de autenticación)

Encrypted Key ID	Authentication Key	Trusted Key	Remove
1	1	md5	<input checked="" type="checkbox"/>

Supresión de la clave de autenticación

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

La [Authentication Key Table](#) (Tabla de claves de autenticación) se abrirá.

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

La entrada se eliminará y el dispositivo se actualizará.

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

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

Tabla 6-17. SNTP Authentication CLI Commands (Comandos de la CLI para la autenticación SNTP)

Comando de la CLI	Description
<code>sntp authenticate</code>	Define la autenticación para el tráfico recibido del NTP (protocolo de hora de la red) desde los servidores.
<code>sntp authentication-key número md5 valor</code>	Define una clave de autenticación para SNTP.

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

```
console> enable

console# configure

xConsole(config)# sntp authentication-key 8 md5 ClkKey

Console(config)# sntp trusted-key 8

Console(config)# sntp authenticate
```

Definición de los servidores SNMP

La página [SNTP Servers](#) (Servidores SNMP) contiene información para activar servidores SNMP, así como agregar nuevos servidores SNMP. Además, la página [SNTP Servers](#) (Servidores SNMP) activa el dispositivo para solicitar y aceptar el tráfico SNMP desde un servidor. Para abrir la página [SNTP Servers](#) (Servidores SNMP), haga clic en **System** → **SNTP** → **SNTP Servers** (Sistema →SNTP → Servidores SNMP) en la *vista de árbol*.

Ilustración 6-25. SNTP Servers (Servidores SNMP)



SNTP Server (Servidor SNMP): Especifique las direcciones IP o el nombre de sistema principal de los servidores SNMP definidos por el usuario. Se pueden definir hasta ocho servidores SNMP. Este campo puede contener de 1 a 158 caracteres.

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

Encryption Key ID (ID clave de codificación): especifica la identificación clave utilizada para establecer comunicación entre el servidor SNMP y el dispositivo. El rango está establecido entre 1 y 4.294.967.295.

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

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

Secondary (secundario): el servidor de copia de seguridad proporciona información sobre SNMP.

Status Up (Estado de activación): estado del servidor SNMP operativo. Los posibles valores de los campos son:

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

Down (Desactivado): el servidor SNMP no está funcionando normalmente en la actualidad.

Unknown (Desconocido): el estado del servidor SNMP es desconocido en la actualidad.

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

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

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

Remove (Eliminar): si se selecciona esta opción, se elimina un servidor SNMP específico de la lista **SNTP Server** (Servidor SNMP).

Adición de un servidor SNMP

1. Abra la página [SNTP Servers](#) (Servidores SNMP).
2. A continuación, haga clic en **Add** (Agregar).

La página [Add SNMP Server](#) (Agregar servidor SNMP) se abrirá:

Ilustración 6-26. Add SNMP Server (Agregar servidor SNMP)

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

El servidor SNMP se agregará y el dispositivo se actualizará.

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para establecer campos que se visualizan en la página **Add SNMP Server** (Agregar servidor SNMP).

Tabla 6-18. Comandos de la CLI del servidor SNMP

Comando de la CLI	Description
<code>sntp server dirección-ip[nombre host [poll] [key keyid]</code>	Configura el dispositivo para utilizar SNMP con el fin de solicitar y aceptar el tráfico NTP desde un servidor.

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

```
console> enable

console# configure

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

Visualización de la tabla de servidores SNMP

1. Abra la página [SNTP Servers](#) (Servidores SNMP).
2. Haga clic en **Show All** (Mostrar todos).

La [SNTP Servers Table](#) (Tabla de servidores SNMP) se abrirá:

Ilustración 6-27. SNMP Servers Table (Tabla de servidores SNMP)

SNTP Server	Poll Interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Reserve
15.1.220	Disabled	1	Secondary	In Progress	Mon, 1 Jun '00 00:00:00 UTC	0	0	<input type="checkbox"/>

Modificación de un servidor SNTP

1. Abra la página [SNTP Servers](#) (servidores SNTP).
2. Haga clic en **Show All** (Mostrar todo).

La [SNTP Servers Table](#) (Tabla de servidores SNTP) se abrirá.

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

La información del servidor SNTP se actualizará.

Supresión del servidor SNTP

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

La [SNTP Servers Table](#) (Tabla de servidores SNTP) se abrirá.

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

La entrada se eliminará y el dispositivo se actualizará.

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

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

Tabla 6-19. SNTP Server CLI Commands (Comandos de la CLI del servidor SNTP)

Comando de la CLI	Description
<code>sntp server dirección IP nombre del sistema principal [poll] [ID clave]</code>	Configura el dispositivo para utilizar SNTP con el fin de solicitar y aceptar el tráfico NTP desde un servidor.

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

```
console> enable

console# configure

Console(config)# sntp server 100.1.1.1 poll key 10

Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8

Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)
```

Unicast servers:					
Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
-----	-----	-----	-----	-----	-----
176.1.1.8	Primary	Up	AFE252C1.6DBDDFF2	7.33	117.79
176.1.8.179	Secondary	Unknown	AFE21789.643287C9	8.98	189.19
Anycast server:					
Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
-----	-----	-----	-----	-----	-----
VLAN 119	Secondary	Up	19:53:21.789 PDT Feb 19 2002	7.19	119.89
Broadcast:					
Interface	IP address	Last response			
-----	-----	-----			
176.1.1.8	Primary	AFE252C1.6DBDDFF2			
176.1.8.179	Secondary	AFE21789.643287C9			

Definición de las interfaces SNTP

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

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

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

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

Remove (Eliminar): si se selecciona esta opción, se elimina SNTP desde una interfaz específica.

Adición de una interfaz SNTP

1. Abra la página **SNTP Broadcast Interface Table** (Tabla de interfaces de difusión SNTP).
2. A continuación, haga clic en **Add** (Agregar).

La página **Add SNTP Interface** (Agregar interfaz SNTP) se abrirá:

Ilustración 6-28. Add SNTP Interface Page (Agregar interfaz SNTP)



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

La interfaz SNTP se agregará y el dispositivo se actualizará.

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

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

Tabla 6-20. SNTP Broadcast CLI Commands (Comandos de la CLI de difusión SNTP)

Comando de la CLI	Description
<code>sntp client enable</code>	Activa el cliente de SNTP (protocolo de hora de la red simple) en una interfaz.
<code>show sntp configuration</code>	Muestra la configuración de SNTP (protocolo de hora de la red simple).

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

Console# show sntp configuration
Polling interval: 7200 seconds.
MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9
Unicast Clients Polling: Enabled.

Server	Polling	Encryption Key
-----	-----	-----
176.1.1.8	Enabled	9
176.1.8.179	Disabled	Disabled
Broadcast Clients: Enabled		
Broadcast Clients Poll: Enabled		
Broadcast Interfaces: g1, g3		

Gestión de registros

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

La página **Logs** (Registros) contiene enlaces con diferentes páginas de registros.

Definición de los parámetros globales de registro

Los registros del sistema activan la visualización de eventos del dispositivo en tiempo real, y la grabación de los eventos para una utilización posterior. Los registros del sistema graban y gestionan eventos, e incluyen informes de los errores o mensajes informativos.

Los mensajes sobre eventos tienen un formato único, como el formato de mensajes SYSLOG RFC recomendado para todos los informes de error. Por ejemplo, Syslog y los mensajes de informe del dispositivo local tienen asignados un código de gravedad e incluyen un mensaje mnemotécnico, que identifica la aplicación de origen que genera el mensaje. Permite filtrar los mensajes en función de su urgencia o relevancia. La gravedad de cada mensaje determina el conjunto de dispositivos de registro de eventos que se envía por registro de eventos.

La siguiente tabla contiene los niveles de gravedad del registro:

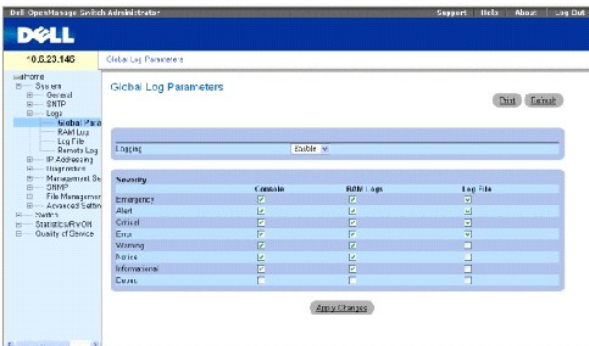
Tabla 6-21. Log Severity Levels (Niveles de gravedad del registro)

Tipo de gravedad	Nivel de gravedad	Descripción
Emergency (Emergencia)	0	El sistema no funciona.
Alert (Alerta)	1	El sistema necesita atención inmediata.
Critical (Grave)	2	El sistema se encuentra en estado crítico.
Error	3	Se ha producido un error en el sistema.
Warning (Advertencia)	4	Se ha visualizado una advertencia en el sistema.
Notice (Aviso)	5	El sistema funciona de forma adecuada pero se ha visualizado una nota.
Informational (Informativa)	6	Proporciona información sobre el dispositivo.
Debug (Depurar)	7	Proporciona información detallada sobre el registro. Si se produce un error de depuración, póngase en contacto con el soporte técnico en línea de Dell.

La página [Global Log Parameters](#) (Parámetros de registro globales) contiene campos para definir en qué registros se han grabado determinados eventos. Contiene campos para activar los registros globalmente y parámetros para definir los parámetros de los registros. Los mensajes de registros Severity

(Gravedad) se enumeran desde el nivel de gravedad más alto al más bajo. Para abrir la página [Global Log Parameters](#) (Parámetros de registro globales) haga clic en System→ Logs→ Global Parameters (Sistema→ Registros→ Parámetros globales) en la vista de árbol.

Ilustración 6-29. Global Log Parameters (Parámetros de registro globales)



Logging (Registro): activa los registros globales del dispositivo para la caché, el archivo y los registros del servidor. Los registros de la consola están activados por defecto.

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

Emergency (Emergencia): el nivel de advertencia superior. Si el dispositivo está desactivado o no funciona adecuadamente, se guarda un mensaje de registro de emergencia en la ubicación especificada del registro.

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

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


Error (Error): se ha producido un error en el dispositivo, por ejemplo, si un puerto está fuera de línea.

Warning (Advertencia): el nivel más bajo de una advertencia sobre el dispositivo. El dispositivo funciona pero se ha producido un problema operativo.

Notice (Aviso): proporciona información sobre el dispositivo.

Informational (Informativo): proporciona información sobre el dispositivo.

Debug (Depurar): proporciona mensajes de depuración de errores.

 **NOTA:** cuando un nivel de gravedad se selecciona, todas las opciones de niveles de gravedad que hay por encima de la selección se seleccionan automáticamente.

La página [Global Log Parameters](#) (Parámetros de registro globales) también contiene casillas de verificación que corresponden a un sistema de registro distinto:

Console (Consola): nivel de gravedad mínimo desde el cual se envían los registros a la consola.

RAM Logs (Registros RAM): nivel de gravedad mínimo desde el cual los registros se envían al archivo de registro guardado en la RAM (caché).

Log File (Archivo de registro): nivel de gravedad mínimo desde el cual los registros se envían al archivo de registro guardado en la memoria flash.

Activación de registros:

1. Abra la [página Global Log Parameters](#) (Parámetros de registro globales).
2. Seleccione **Enable** (Activar) en la lista desplegable **Logging** (Registro).
3. Seleccione el tipo de registro y la gravedad del registro en las casillas de verificación de **Global Log Parameters** (Parámetros de registro globales).
4. Haga clic en **Apply Changes** (Aplicar cambios).

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

Activación de registros mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Global Log Parameters](#) (**Parámetros de registro globales**).

Tabla 6-22. Global Log Parameters CLI Commands (Comandos de la CLI para los parámetros de registro globales)

Comando de la CLI	Description
logging on	Activa el registro de mensajes de error.
logging {ip-address hostname} [port port] [severity level] [facility facility] [description text]	Registra los mensajes en un servidor de registro del sistema. Si desea obtener una lista de los niveles de gravedad, consulte el apartado " Log Severity Levels " (Niveles de gravedad de registro).
logging console level	Limita los mensajes registrados en la consola según la gravedad.
logging buffered level	Limita los mensajes de registro del sistema que se muestran desde un búfer (RAM) interno según la gravedad.
logging file level	Limita los mensajes de registro del sistema que se envían al archivo de registro según la gravedad.
clear logging	Borra los registros.
clear logging file	Borra los mensajes del archivo de registro.

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

```
Console(config)#logging on

Console (config)# logging console errors

Console (config)# logging buffered debugging

Console (config)# logging file alerts

Console (config)# clear logging

Console(config)#exit

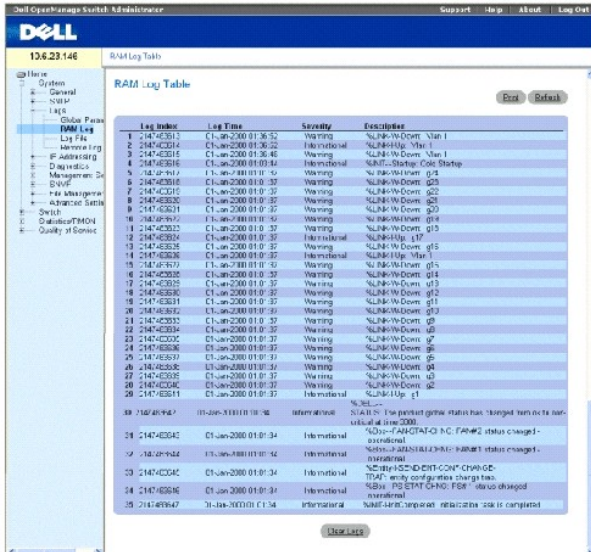
Console# clear logging file

Clear Logging File [y/n]y
```

Visualización de la tabla de registros RAM

La [RAM Log Table](#) (Tabla de registros RAM) contiene información acerca de las entradas de registro guardadas en la RAM, incluida la hora en la que se introdujo el registro, la gravedad del registro y una descripción de éste. Para abrir la [RAM Log Table](#) (Tabla de registros RAM), haga clic en System→ Logs→ RAM Log (Sistema→ Registros→ Registro RAM) en la vista de árbol.

Ilustración 6-30. RAM Log Table (Tabla de registros RAM)



Log Index (Índice de registros): número de registros en la [RAM Log Table](#) (Tabla de registros RAM).

Log Time (Hora de registro): especifica la hora en la que el se ha introducido el registro en la [RAM Log Table](#) (Tabla de registros RAM).

Severity (Gravedad): especifica la gravedad del registro.

Description (Descripción): descripción del registro definido por el usuario.

Eliminación de la información del registro:

1. Abra la [RAM Log Table](#) (Tabla de registros RAM).
2. Haga clic en Clear Log (Borrar registro).

La información sobre el registro se eliminará de la [RAM Log Table](#) (Tabla de registros RAM) y el dispositivo se actualizará.

Visualización y borrado de la tabla de registros mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para ver y borrar los campos que se muestran en la [RAM Log Table](#) (Tabla de registros RAM).

Tabla 6-23. RAM Log Table CLI Commands (Comandos de la CLI para la tabla de registros RAM)

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

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

```

> show logging
> clear logging
  
```

```
console# show logging
```

```
Logging is enabled.
```

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

```
Buffer Logging: Level info. Buffer Messages: 26 Logged, 26 Displayed, 200 Max.
```

```
File Logging: Level error. File Messages: 157 Logged, 26 Dropped.
```

```
1 messages were not logged
```

```
01-Jan-2000 01:03:42 :%INIT-I-Startup: Cold Startup
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g24
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g23
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g22
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g21
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g20
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g19
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g18
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g17
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g13
```

```
1-Jan-2000 01:01:36 :%LINK-W-Down: g2
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g1
```

```
01-Jan-2000 01:01:32 :%INIT-I-InitCompleted: Initialization task is completed
```

```
Console # clear logging
```

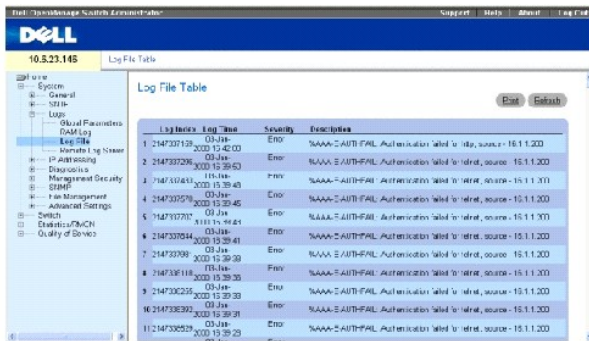
```
clear logging buffer [y/n]?
```

Console#

Visualización de la tabla de archivos de registro

La [Log File Table](#) (Tabla de archivos de registro) contiene información sobre las entradas de registro guardadas para el archivo de registro en la memoria flash, incluida la hora en la que se introdujo el registro, la gravedad del registro y una descripción del mensaje de registro. Para abrir la [Log File Table](#) (Tabla de archivos de registro), haga clic en System→ Logs→ Log File (Sistema→ Registros→ Archivo de registro) en la vista de árbol.

Ilustración 6-31. Log File Table (Tabla de archivos de registro)



Log Index (Índice de registro): número de registro en la [Log File Table](#) (Tabla de archivos de registro).

Log Time (Hora de registro): especifica la hora en la que el registro se introdujo en la [Log File Table](#) (Tabla de archivos de registro).

Severity (Gravedad): especifica la gravedad del registro.

Description (Descripción): texto del mensaje de registro.

Visualización de la tabla de archivos de registro mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para ver y configurar campos que se visualizan en la [Log File Table](#) (Tabla de archivos de registro).

Tabla 6-24. Log File Table CLI Commands (Comandos de la CLI para la tabla de archivos de registro)

Comando de la CLI	Description
show logging file	Muestra el estado de registro y los mensajes Syslog almacenados en el archivo de registro.
clear logging file	Borra mensajes del archivo de registro.

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

```
Console # show logging file

Logging is enabled.

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

```
Buffer Logging: Level info. Buffer Messages: 62 Logged, 62 Displayed, 200 Max.

File Logging: Level debug. File Messages: 11 Logged, 51 Dropped.

SysLog server 12.1.1.2 Logging: warning. Messages: 14 Dropped.

SysLog server 1.1.1.1 Logging: info. Messages: 0 Dropped.

1 messages were not logged

01-Jan-2000 01:12:01 :%COPY-W-TRAP: The copy operation was completed successfully

01-Jan-2000 01:11:49 :%LINK-I-Up: g21

01-Jan-2000 01:11:49 :%2SWPHY-I-CHNGCOMBOMEDIA: Media changed from copper media
to fiber media (1000BASE-SX) on port g21.

01-Jan-2000 01:11:48 :%2SWPHY-I-CHNGCOMBOMEDIA: Media changed from fiber media to copper media on port g21.

01-Jan-2000 01:11:48 :%LINK-W-Down: g21

01-Jan-2000 01:11:46 :%LINK-I-Up: g19

01-Jan-2000 01:11:42 :%LINK-W-Down: g14

01-Jan-2000 01:11:41 :%LINK-I-Up: g14

01-Jan-2000 01:11:36 :%LINK-W-Down: g9

01-Jan-2000 01:11:35 :%LINK-I-Up: g1

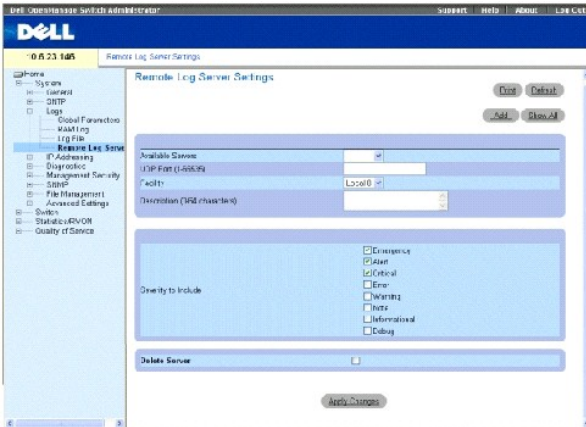
01-Jan-2000 01:11:34 :%LINK-W-Down: g1

console#
```

Configuración de la página de configuración del servidor de registros remoto

La página [Remote Log Server Settings](#) (Configuración del servidor de registros remoto) contiene campos para ver y configurar los servidores de registro disponibles. Además, se pueden definir nuevos servidores de registro y la gravedad de los registros se puede enviar a cada servidor. Para abrir la página [Remote Log Server Settings](#) (Configuración del servidor de registros remoto), haga clic en System→ Logs→ Remote Log Server (Sistema→Registros→ Servidor de registros remoto) en la vista de árbol.

Ilustración 6-32. Remote Log Server Settings (Configuración del servidor de registros remoto)



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

UDP Port (1-65535) (Puerto UDP [1-65535]): puerto UDP al que se envían los registros para el servidor seleccionado. El rango posible es 1 - 65535. El valor predeterminado es 514.

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

Local 0 - Local 7.

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

Delete Server (Suprimir servidor): suprime el servidor actualmente seleccionado de la lista Available Servers (Servidores disponibles) cuando esté seleccionado.

La página [Remote Log Server Settings](#) (Configuración del servidor de registros remoto) también contiene una lista de gravedad. Las definiciones de gravedad son las mismas que las de la página [Global Log Parameters](#) (Parámetros de registro globales).

Envío de registros a un servidor:

1. Abra la página [Remote Log Server Settings](#) (Configuración del servidor de registros remoto).
2. Seleccione un servidor de la lista desplegable **Available Servers** (Servidores disponibles).
3. Defina los campos.
4. Seleccione la gravedad de registro en la opción **Severity** (Gravedad) para incluir las casillas de verificación.
5. Haga clic en **Apply Changes** (Aplicar cambios).

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

Definición de un nuevo servidor:

1. Abra la página [Remote Log Server Settings](#) (Configuración del servidor de registros remoto).
2. Haga clic en **Add** (Agregar).

La página [Add a Log Server](#) (Agregar un servidor de registros) se abrirá:

Ilustración 6-33. Add a Log Server (Agregar un servidor de registros)

Add a Log Server Refresh

New Log Server IP Address [X.X.X.X]
UDP Port (1-65535) 514
Facility Local7
Description (0-64 characters)

Severity to include
 Emergency
 Alert
 Critical
 Error
 Warning
 Note
 Information
 Debug

Apply Changes

New Log Server IP Address (Nueva dirección IP del servidor de registros): define la dirección IP del nuevo servidor de registros.

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

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

Visualización de la tabla de servidores de registros remotos:

1. Abra la página [Remote Log Server Settings](#) (Configuración del servidor de registros remotos).
2. Haga clic en **Show All** (Mostrar todo).

La página [Remote Log Servers Table](#) (Tabla de servidores de registros remotos) se abrirá:

Ilustración 6-34. Remote Log Servers Table (Tabla de servidores de registros remotos)

Remote Log Servers Table Refresh

Servers	UDP Port	Facility	Description	Minimum Severity	Remove
---------	----------	----------	-------------	------------------	--------

Apply Changes

Eliminación de un servidor de registros de la página Log Server Table (Tabla de servidores de registros):

1. Abra la página [Remote Log Server Settings](#) (Configuración del servidor de registros remoto).
2. Haga clic en **Show All** (Mostrar todo).

La página [Remote Log Servers Table](#) (Tabla de servidores de registros remotos) se abrirá.

3. Seleccione una entrada de la [Remote Log Servers Table](#) (Tabla de servidores de registros remotos).
4. Seleccione la casilla de verificación **Remove** (Eliminar) para eliminar los servidores.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada [Remote Log Servers Table](#) (Tabla de servidores de registros remotos) se eliminará y el dispositivo se actualizará.

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

En la siguiente tabla se muestra un resumen del comando de la CLI equivalente para funcionar con registros de servidores remotos.

Tabla 6-25. Remote Log Server CLI Commands (Comandos de la CLI para el servidor de registros remoto)

Comando de la CLI	Description
<code>logging</code> (<i>dirección IP</i> <i>nombre del sistema principal</i>) [<i>port puerto</i>] [<i>severity nivel</i>] [<i>facility instalación</i>] <i>description texto</i>	Registra los mensajes en un servidor de remoto.
<code>no logging</code>	Suprime un servidor de Syslog.
<code>show logging</code>	Muestra el estado del registro y los mensajes Syslog.

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

```
console> enable

console# configure

console (config) # logging 10.1.1.1 severity critical

Console # show logging

Logging is enabled.

Console Logging: Level debug. Console Messages: 5 Dropped.

Buffer Logging: Level debug. Buffer Messages: 16 Logged, 16 Displayed, 200 Max.

File Logging: Level error. File Messages: 0 Logged, 209 Dropped.

SysLog server 31.1.1.2 Logging: error. Messages: 22 Dropped.

SysLog server 5.2.2.2 Logging: info. Messages: 0 Dropped.

SysLog server 10.2.2.2 Logging: critical. Messages: 21 Dropped.

SysLog server 10.1.1.1 Logging: critical. Messages: 0 Dropped.

1 messages were not logged

03-Mar-2004 12:02:03 :%LINK-I-Up: g1

03-Mar-2004 12:02:01 :%LINK-W-Down: g2
```

Definición de las direcciones IP del dispositivo

La página IP Addressing (Direccionamiento IP) contiene vínculos para asignar direcciones IP de la puerta de enlace predeterminada y de interfaz, y definir parámetros de ARP y DHCP de las interfaces. Para abrir la página IP Addressing (Direccionamiento IP), haga clic en System → IP Addressing (Sistema → Direccionamiento IP) en la vista de árbol.

Definición de las puertas de enlace predeterminadas

La página **Default Gateway** (Puerta de enlace predeterminada) contiene campos para asignar dispositivos de puerta de enlace. Los paquetes se reenvían a la IP predeterminada cuando las tramas se reenvían a una red remota. La dirección IP configurada debe pertenecer a la misma subred de dirección IP de una de las interfaces IP. Para abrir la página **Default Gateway** (Puerta de enlace predeterminada), haga clic en System → IP Addressing → Default Gateway (Sistema → Direccionamiento IP → Puerta de enlace predeterminada) en la vista de árbol.

La página **Default Gateway** (Puerta de enlace predeterminada) contiene los siguientes campos:

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

Remove (Eliminar): elimina los dispositivos de la puerta de enlace de la lista desplegable **Default Gateway** (Puerta de enlace predeterminada) cuando estén seleccionados.

Selección de un dispositivo de puerta de enlace:

1. Abra la página **Default Gateway** (Puerta de enlace predeterminada).
2. Seleccione una dirección IP en la lista **Default Gateway** (Puerta de enlace predeterminada).
3. Seleccione la casilla de verificación **Active** (Activa).
4. Haga clic en **Apply Changes** (Aplicar cambios).

El dispositivo de la puerta de enlace se seleccionará y se actualizará.

Eliminación de un dispositivo de puerta de enlace predeterminada:

1. Abra la página **Default Gateway** (Puerta de enlace predeterminada).
2. Seleccione la casilla de verificación **Remove** (Eliminar) para eliminar las puertas de enlace predeterminadas.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada de la puerta de enlace predeterminada se eliminará y el dispositivo se actualizará.

Definición de los dispositivos de puertas de enlace mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página **Default Gateway** (Puerta de enlace predeterminada).

Tabla 6-26. Default Gateway CLI Commands (Comandos de la CLI para la puerta de enlace predeterminada)

Comando de la CLI	Description
<code>ip default-gateway dirección-ip</code>	Define una puerta de enlace predeterminada.
<code>no ip default-gateway</code>	Elimina una puerta de enlace predeterminada.

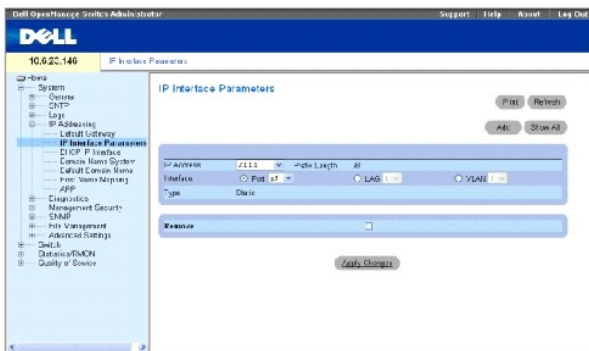
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console(config)#ip default-gateway 196.210.10.1  
  
Console (config)# no ip default-gateway
```

Definición de las interfaces IP

La página [IP Interface Parameters](#) (Parámetros de las interfaces IP) contiene campos para asignar parámetros IP a las interfaces. Para abrir la página [IP Interface Parameters](#) (Parámetros de las interfaces IP), haga clic en **System** → **IP Addressing** → **Interface Parameters** (Sistema → Direccionamiento IP → Parámetros de las interfaces) en la vista de árbol.

Ilustración 6-35. IP Interface Parameters (Parámetros de las interfaces IP)



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

Prefix Length (Longitud del prefijo): número de bits que componen el prefijo de la dirección IP de origen o la máscara de red de la dirección IP de origen.

Interface (Interfaz): tipo de interfaz para la que está definida la dirección IP. Seleccione **Port** (Puerto), **LAG** o **VLAN**.

Para obtener más información, consulte el apartado "[Configuring VLANs](#)" (Configuración de las VLAN).

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

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

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

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

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

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

Adición de una interfaz IP

1. Abra la página [IP Interface Parameters](#) (Parámetros de interfaz IP).
2. Haga clic en **Add** (Agregar).

La página [Add a Static Interface](#) (Agregar una interfaz estática) se abrirá:

Ilustración 6-36. Add a Static Interface (Agregar una interfaz estática)

The screenshot shows a configuration form titled "Add a Static IP Interface". It includes a "Refresh" button at the top right. The form has several input fields: "Source IP Address" with a placeholder "(X.X.X.X)", "Network Mask" with a placeholder "(X.X.X.X)", and "Prefix Length" with a value of "1900". Below these is an "Interface" dropdown menu currently showing "g1". There are also radio buttons for "LAG" and "VLAN". At the bottom of the form is an "Apply Changes" button.

3. Complete los campos de esta página.

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

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

La nueva interfaz se agrega y el dispositivo se actualiza.

Modificación de los parámetros de dirección IP

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

Los parámetros se modifican, y el dispositivo se actualiza.

Supresión de direcciones IP

1. Abra la página [IP Interface Parameters](#) (Parámetros de interfaz IP).
2. Haga clic en **Show All** (Mostrar todo).

La **Interface Parameters Table** (Tabla de parámetros de interfaz) se abrirá:

Ilustración 6-37. IP Interface Parameter Table (Tabla de parámetros de interfaz IP)

The screenshot shows a table titled "IP Interface Parameter Table" with a "Refresh" button at the top right. The table has five columns: "IP Address", "Prefix Length", "Interface", "Type", and "Remove". It contains three rows of data. Below the table is an "Apply Changes" button.

	IP Address	Prefix Length	Interface	Type	Remove
1	2.1.1	/8	g3	Static	<input type="checkbox"/>
2	10.1.1.1	/24	g1/2	Dynamic	<input type="checkbox"/>
3	16.1.1.3	/8	g1	Static	<input type="checkbox"/>

3. Seleccione una dirección IP y la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La dirección IP seleccionada se suprimirá y el dispositivo se actualizará.

Definición de las interfaces IP mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [IP Interface Parameters](#) (Parámetros de interfaz IP).

Tabla 6-27. IP Interface Parameters CLI Commands (Comandos de la CLI para parámetros de la interfaz IP)

Comando de la CLI	Description
<code>ip address dirección -ip {mask prefix-length}</code>	Establece una dirección IP.
<code>no ip address [dirección -ip]</code>	Elimina una dirección IP
<code>show ip interface [ethernet número de interfaz vlan id-vlan port-channel número]</code>	Muestra el estado de uso de las interfaces configuradas para IP.

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

```
Console(config)# interface vlan 1

Console (config-if)#ip address 131.108.1.27 255.255.255.0

Console (config-if)# no ip address 131.108.1.27

Console (config-if)# exitconsole# show ip interface vlan 1

Output

Gateway IP Address Activity status

-----

192.168.1.1 Active

IP address Interface Type

-----

192.168.1.123 /24 VLAN 1 Static
```

Definición de los parámetros de interfaz IP DHCP

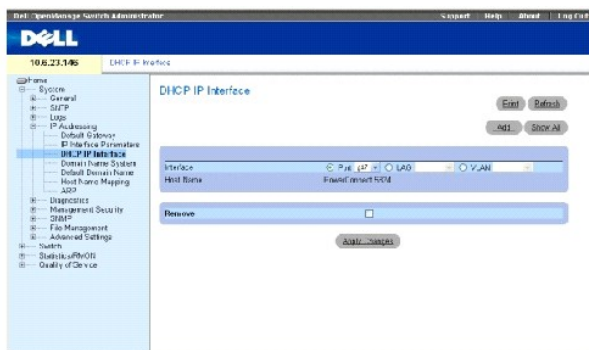
```
console# show ip interface vlan 1
```

Salida

Gateway IP Address	Activity status	
-----	-----	
192.168.1.1	Active	
IP address	Interface	Type
-----	-----	-----
192.168.1.123 /24	vlan 1	Static

La página [DHCP IP Interface](#) (Interfaz IP DHCP) contiene campos para especificar los clientes DHCP conectados al dispositivo. Haga clic en **System** → **IP Addressing** → **DHCP IP Interface** (Sistema → Direcciónamiento IP → Interfaz IP DHCP) en la vista de árbol. Para abrir la página [DHCP IP Interface](#) (Interfaz IP DHCP).

Ilustración 6-38. DHCP IP Interface (Interfaz IP DHCP)



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

Host Name (Nombre del sistema principal): nombre del sistema. Este campo puede contener hasta 20 caracteres.

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

Adición de clientes DHCP

1. Abra la página [DHCP IP Interface](#) (Interfaz IP DHCP).
2. Haga clic en **Add** (Agregar).

La página **Add DHCP IP Interface** (Agregar interfaz IP DHCP) se abrirá.

3. Complete la información en la página.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se agrega la interfaz DHCP y el dispositivo se actualiza.

Modificación de una interfaz IP DHCP

1. Abra la página [DHCP IP Interface](#) (Interfaz IP DHCP).
2. Modifique los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se modifica y el dispositivo se actualiza.

Supresión de una interfaz IP DHCP

1. Abra la página [DHCP IP Interface](#) (Interfaz IP DHCP).
2. Haga clic en **Show All** (Mostrar todo).

La **DHCP Client Table** (Tabla de clientes de DHCP) se abrirá.

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

La entrada seleccionada se suprimirá y el dispositivo se actualizará.

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

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

Tabla 6-28. DHCP IP Interface CLI Commands (Comandos de la CLI para la interfaz IP DHCP)

Comando de la CLI	Description
<code>ip address dhcp [hostname nombre del sistema principal]</code>	Para adquirir una dirección IP en una interfaz Ethernet a partir del DHCP (Protocolo de configuración de direccionamiento dinámico).

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

```
console> enable

console#config

console (config#) interface ethernet g1
```

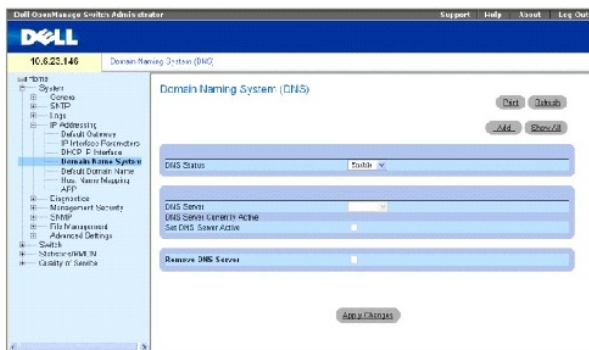
```
console (config-if)# ip address dhcp 10.0.0.1 /8
```

Configuración de sistemas de nombres de dominio

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

La página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]) contiene campos para habilitar y activar determinados servidores DNS. Para abrir la página **Domain Naming System (DNS)** (DNS [Sistema de nombres de dominio]), haga clic en **System** → **IP Addressing** → **Domain Name System** (Sistema → Direcciónamiento IP → Sistema de nombres de dominio) en la *vista de árbol*.

Ilustración 6-39. Domain Naming System (DNS) (DNS [Sistema de nombres de dominio])



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

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

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

Set DNS Server Active (Establecer como activo el servidor DNS): activa el servidor DNS seleccionado en el campo **DNS Server** (Servidor DNS).

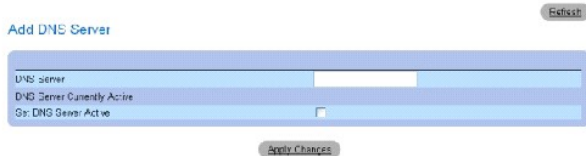
Remove DNS Server (Eliminar servidor DNS): si esta opción está seleccionada, se eliminan los servidores DNS.

Adición de un servidor DNS

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

La página **Add DNS Server** (Agregar servidor DNS) se abrirá:

Ilustración 6-40. Add DNS Server (Agregar servidor DNS)



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

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

Visualización de la tabla de servidores DNS

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

La **DNS Server Table** (Tabla de servidores DNS) se abrirá:

Ilustración 6-41. DNS Server Table (Tabla de servidores DNS)



Eliminación de servidores DNS

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

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

Configuración de los servidores DNS mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI para configurar la información del sistema del dispositivo.

Tabla 6-29. DNS Server CLI Commands (Comandos de la CLI para el servidor DNS)

Comando de la CLI	Description
ip name-server <i>dirección del servidor</i>	Establece los servidores de nombres disponibles. Se pueden establecer hasta ocho servidores de nombres.
no ip name-server <i>dirección del servidor</i>	Elimina un servidor de nombres.
ip domain-name <i>nombre</i>	Define un nombre de dominio predeterminado que el software utiliza para completar nombres de sistemas principales no calificados.
clear host { <i>nombre</i> * }	Suprime entradas de la caché de nombres de sistemas principales a direcciones.
show hosts [<i>nombre</i>]	Muestra el nombre del dominio predeterminado, la lista de sistemas principales de servidores de nombres, así como la lista de nombres y direcciones de sistemas principales estáticas y en caché.

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

```
console> enable

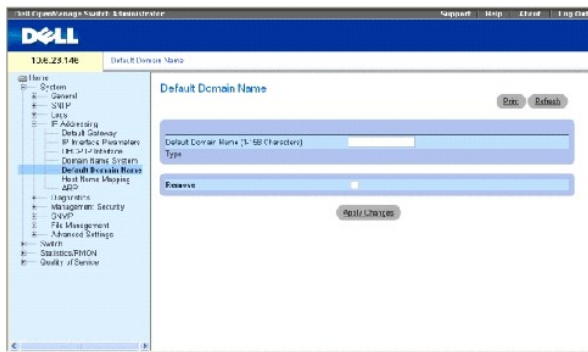
Console# configure

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

Definición de los dominios predeterminados

La página **Default Domain Name** (Nombre de dominio predeterminado) proporciona información para definir nombres de dominio DNS predeterminados. Para abrir la página **Default Domain Name** (Nombre de dominio predeterminado), haga clic en **System** → **IP Addressing** → **Default Domain Name** (Sistema → Direcciónamiento IP → Nombre de dominio predeterminado) en la *vista de árbol*.

Ilustración 6-42. Default Domain Name (Nombre de dominio predeterminado)



Default Domain Name (1-158 characters) (Nombre de dominio predeterminado [1 - 158 caracteres]): contiene un servidor de nombres de dominio DNS definido por el usuario. Cuando se selecciona, el nombre de dominio DNS es el dominio predeterminado.

Type (Tipo): tipo de dominio si el dominio se ha creado estática o dinámicamente.

Remove (Eliminar): cuando se selecciona, se elimina un dominio seleccionado.

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

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

Tabla 6-30. DNS Domain Name CLI Commands (Comandos de la CLI para el nombre de dominio DNS)

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

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

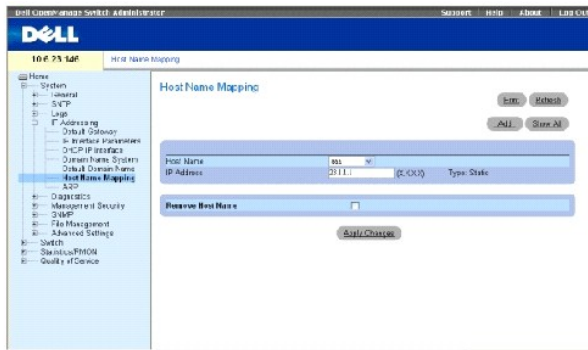
```
console> enable
```

```
console# configure
console (config)# ip domain-name www.dell.com
```

Asignación del sistema principal de dominios

La página **Host Name Mapping** (Asignación de nombres de sistemas principales) proporciona parámetros para asignar direcciones IP de nombres de sistemas principales estáticas. La página **Host Name Mapping** (Asignación de nombres de sistemas principales) proporciona hasta ocho direcciones IP por sistema principal. Para abrir la página **Host Name Mapping** (Asignación de nombres de sistemas principales), haga clic en **System**→ **IP Addressing**→ **Host Name Mapping** (Sistema→ Direcciónamiento IP→ Asignación de nombres de sistemas principales).

Ilustración 6-43. Host Name Mapping (Asignación de nombres de sistemas principales)



Host Name (Nombre de sistema principal): contiene una lista de nombres de sistemas principales. Los nombres de sistemas principales están definidos en la página **Add Host Name Mapping** (Agregar asignación de nombres de sistemas principales). Cada sistema principal proporciona hasta ocho direcciones IP. Los valores de campo del campo **Host Name** (Nombre del sistema principal) son:

IP Address (X.X.X.X) (Dirección IP [X.X.X.X]): proporciona hasta ocho direcciones IP que están asignadas al nombre del sistema principal especificado.

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

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

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

Remove Host Name Mapping (Eliminar asignación de nombres de sistemas principales): cuando se marca, elimina la asignación de sistemas principales DNS.

Adición de nombres de dominios de sistemas principales

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

La página **Add Host Name Mapping** (Agregar asignación de nombres de sistemas principales) se abrirá:

Ilustración 6-44. Add Host Name Mapping (Agregar asignación de nombres de sistemas principales)



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

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

Visualización de la tabla de asignación de nombres de sistemas principales

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

La **Hosts Name Mapping Table** (Tabla de asignación de nombres de sistemas principales) se abrirá:

Ilustración 6-45. Hosts Name Mapping Table (Tabla de asignación de nombres de sistemas principales)

Hosts Name Mapping Table

Host Name	IP Address	Remove
1 asa	23.1.1.1	<input type="checkbox"/>
2 www.com	23.1.1.1	<input type="checkbox"/>

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

1. Abra la página **Host Name Mapping** (Asignación de nombres de sistemas principales).
2. Haga clic en **Show All** (Mostrar todo)
3. La **Host Mapping Table** (Tabla de asignación de sistemas principales) se abrirá.
4. Seleccione una entrada de la **Host Mapping Table (Tabla de asignación de sistemas principales)**.
5. Marque la casilla de verificación **Remove** (Eliminar).
6. Haga clic en **Apply Changes** (Aplicar cambios).

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

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

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

Tabla 6-31. Domain Host Name CLI Commands (Comandos de la CLI para los nombres de los sistemas principales del dominio)

Comando de la CLI	Descripción
ip host name <i>dirección1</i> [<i>dirección2</i> ... <i>dirección8</i>]	Define la asignación estática de nombres de sistemas principales a direcciones en la caché de los sistemas principales.
no ip host name	Elimina la asignación de nombres a direcciones.
clear host { <i>nombre</i> * }	Suprime entradas de la caché de nombres de sistemas principales a direcciones.
show hosts [<i>nombre</i>]	Muestra el nombre del dominio predeterminado, la lista de sistemas principales de servidores de nombres, así como la lista de nombres y direcciones de sistemas principales estáticas y en caché.

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

```
console# enable
```

```
console# configure
```

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

Configuración de ARP

El protocolo de resolución de direcciones (ARP) es un protocolo TCP/IP que convierte las direcciones IP en direcciones físicas. Las entradas estáticas se pueden definir en la **ARP Table** (Tabla de ARP). Cuando se definen las entradas estáticas, se especifica una entrada permanente y se utiliza para convertir las direcciones IP en direcciones MAC. Si desea abrir la página [ARP Settings](#) (Configuración de ARP), haga clic en System→ IP Addressing→ ARP (Sistema→ Direcciónamiento IP→ ARP) en la vista de árbol.

Ilustración 6-46. ARP Settings (Configuración de ARP)



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

ARP Entry Age Out (1-4000000) (Caducidad de entrada de ARP [1-4000000]): para todos los dispositivos, el tiempo (segundos) que pasa entre las peticiones de ARP sobre una entrada de la tabla de ARP. Después de este período, la entrada se elimina de la tabla. El intervalo es 1 - 4000000, donde cero indica que las entradas nunca se borran de la caché. El valor predeterminado es 60.000 segundos.

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

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

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

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

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

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

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

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

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

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

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

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

Remove ARP Entry (Eliminar entrada de ARP): cuando se selecciona, se elimina una entrada de ARP.

Adición de una entrada en la tabla de ARP estática:

1. Abra la página [ARP Settings](#) (Configuración de ARP).
2. Haga clic en **Add** (Agregar).

La página **Add ARP Entry** (Agregar entrada de ARP) se abrirá:

Ilustración 6-47. Página Add ARP Entry (Agregar entrada de ARP)

The screenshot shows the 'Add ARP Entry' configuration page. At the top left is the title 'Add ARP Entry' and a 'Refresh' button. Below is a form with three rows: 'Interface' with a dropdown menu showing 'g1', 'IP Address' with a text input field containing '0.0.0.0' and a '(?)' icon, and 'MAC Address' with a text input field containing '000000000000'. At the bottom of the form is an 'Apply Changes' button.

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

La entrada de la **ARP Table** (Tabla de ARP) se agregará y el dispositivo se actualizará.

Visualización de la tabla de ARP

1. Abra la página [ARP Settings](#) (Configuración de ARP).
2. Haga clic en **Show All** (Mostrar todo).

La **ARP Table** (Tabla de ARP) se abrirá:

Ilustración 6-48. Página ARP Table (Tabla de ARP)

The screenshot shows the 'ARP Table' page. At the top left is the title 'ARP Table' and a 'Refresh' button. Below is a table with the following data:

	Interface	IP Address	MAC Address	Status	Remove
1	g1	15.1.1.200	0002b3951783	Dynamic	<input type="checkbox"/>
2	g7	10.6.23.129	00026e00010d	Dynamic	<input type="checkbox"/>

At the bottom of the table is an 'Apply Changes' button.

Supresión de una entrada de la tabla de ARP

1. Abra la página [ARP Settings](#) (Configuración de ARP).
2. Haga clic en **Show All** (Mostrar todo).

La página **ARP Table** (Tabla de ARP) se abrirá.

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

La entrada seleccionada de la **ARP Table** (Tabla de ARP) se borrará y el dispositivo se actualizará.

Configuración de ARP mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [ARP Settings \(Configuración de ARP\)](#).

Tabla 6-32. ARP Settings CLI Commands (Comandos de la CLI para la configuración de ARP)

Comando de la CLI	Description
<code>arp direc_ip direc_hw { ethernet número de interfaz vlan id-vlan port-channel número }</code>	Agrega una entrada permanente en la caché de ARP.
<code>arp timeout segundos</code>	Configura el tiempo que una entrada permanece en la caché de ARP.
<code>clear arp-cache</code>	Suprime todas las entradas dinámicas de la caché de ARP.
<code>show arp</code>	Muestra entradas en la ARP Table (Tabla de ARP).
<code>no arp</code>	Elimina una entrada de ARP de la ARP Table (Tabla de ARP).

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

```

Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

Console(config)#exit

Console# arp timeout 12000

Console# show arp

ARP timeout: 80000 Seconds

```

Interface	IP address	HW address	Status
-----	-----	-----	-----
g1	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
g2	10.7.1.135	00:50:22:00:2A:A4	Static

Ejecución de los diagnósticos de los cables

La página **Diagnostics** (Diagnósticos) contiene vínculos a páginas para realizar pruebas virtuales de cables en cables de cobre y de fibra óptica. Para abrir la página **Diagnostics** (Diagnósticos), haga clic en **System**→ **Diagnostics** (Sistema→ Diagnósticos) en la vista de árbol.

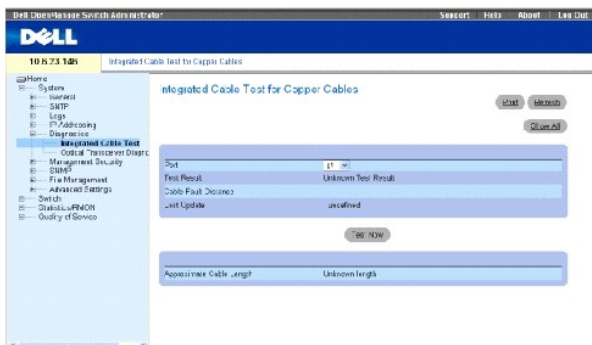
Visualización de los diagnósticos de los cables de cobre

La página [Integrated Cable Test for Copper Cables](#) (Prueba de cables integrados para cables de cobre) contiene campos para realizar pruebas de los cables de cobre. Las pruebas de cables proporcionan información sobre dónde se producen errores en el cable, la última vez que se realizó una prueba de cable, y el tipo de error de cable que se produjo. En las pruebas se utiliza la tecnología de reflectometría de dominio temporal (TDR) para probar la calidad y las

características de un cable de cobre conectado a un puerto. Se pueden probar cables de hasta 120 metros de longitud. Los cables se prueban cuando los puertos están inactivos, con la excepción de la prueba de longitud aproximada del cable.

Para abrir la página [Integrated Cable Test for Copper Cables](#) (Prueba de cables integrados para cables de cobre), haga clic en **System**→ **Diagnostics**→ **Integrated Cable Test** (Sistema→ Diagnósticos→ Prueba de cables integrados) en la vista de árbol.

Ilustración 6-49. Integrated Cable Test for Copper Cables (Prueba de cables integrados para los cables de cobre)



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

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

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

Open Cable (Cable abierto): el cable está conectado sólo por un extremo.

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

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

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

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

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

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

Ejecución de una prueba de cable

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

La prueba de cables de cobre se efectuará y los resultados se mostrarán en la página [Integrated Cable Test for Copper Cables](#) (Prueba de cables integrados para cables de cobre).

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

1. Abra la página [Integrated Cable Test for Copper Cables](#) (Prueba de cables integrados para cables de cobre).
2. Haga clic en **Show All** (Mostrar todo).

La **Virtual Cable Test Results Table** (Tabla de resultados de la prueba de cable virtual) se abrirá.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para realizar las pruebas de cables de cobre.

Tabla 6-33. Copper Cable Test CLI Commands (Comandos de la CLI para la prueba de cables de cobre)

Comando de la CLI	Description
<code>test copper-port tdr [interfaz]</code>	Realiza las pruebas VCT.
<code>show copper-port tdr [interfaz]</code>	Muestra los resultados de las últimas pruebas VCT realizadas en los puertos.
<code>show copper-port cable-length [interfaz]</code>	Muestra la longitud estimada del cable de cobre conectado a un puerto.

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


```
console> enable

Console# test copper-port tdr g3

Cable is open at 100 meters.

Console> show copper-ports tdr
```

Port	Result	Length [meters]	Date
----	-----	-----	----
g1	OK		
g2	Short	50	13:32:00 15 January 2004
g3	Test has not been performed		
g4	Open	64	13:32:00 15 January 2004
g5	Fiber	-	-

 **NOTA:** La longitud del cable que se devuelve es una aproximación en intervalos de hasta 50 metros, 50m - 80m, 80m - 110m, 110m - 120m o más de 120m. La desviación puede ser de hasta 20 metros.

Visualización de los diagnósticos del transceptor óptico

La página [Optical Transceiver Diagnostics](#) (Diagnósticos del transceptor óptico) contiene campos para realizar pruebas en cables de fibra óptica. Para abrir la página [Optical Transceiver Diagnostics](#) (Diagnósticos del transceptor óptico), haga clic en **System**→ **Diagnostics**→ **Optical Transceiver Diagnostics** (Sistema→ Diagnósticos→ Diagnósticos del transceptor óptico) en la vista de árbol.


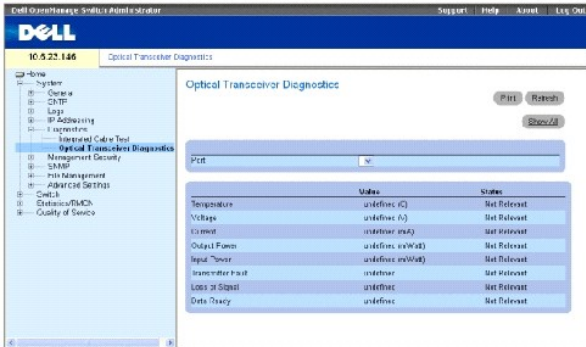
 **NOTA:** los diagnósticos del transceptor óptico sólo se pueden realizar cuando el vínculo está presente.

Ilustración 6-50. Optical Transceiver Diagnostics (Diagnósticos del transceptor óptico)



Port (Puerto): el puerto al cual está conectado el cable de fibra.

Temperature (Temperatura): temperatura (en grados centígrados) a la que funciona el cable.

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

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

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

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

Transmitter Fault (Fallo del transmisor): indica si se ha producido un error durante la transmisión.

Loss of Signal (Pérdida de señal): indica si se ha producido una pérdida de señal en el cable.

Data Ready (Datos preparados): el transceptor se ha encendido y los datos están preparados.

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

1. Abra la página [Optical Transceiver Diagnostics](#) (Diagnósticos del transceptor óptico).
2. Haga clic en **Show All** (Mostrar todo).

La prueba se ejecutará y la **Virtual Cable Test Results Table** (Tabla de resultados de la prueba virtual de cable) se abrirá.

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

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para realizar las pruebas de cables de fibra óptica.

Tabla 6-34. **Fiber Optic Cable Test CLI Commands (Comandos de la CLI para la prueba de cables de fibra óptica)**

Comando de la CLI	Description
show fiber-ports optical-transceiver [<i>interfaz</i>][<i>detailed</i>]	Muestra los diagnósticos del transceptor óptico.

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

```
console> enable

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

Port	Temp	Voltage	Current	Power		TX	LOS
				Output	Input		
	(C)	(Volt)	(mA)	(mWatt)	(mWatt)	Fault	
g1	W	OK	E	OK	OK	OK	OK
g2	OK	OK	OK	OK	OK	E	OK
g3	Copper						

Temp - Internally measured transceiver temperature.

Voltage - Internally measured supply voltage.

Current - Measured TX bias current.

Output Power - Measured TX output power.


Input Power - Measured RX received power.

Tx Fault - Transmitter fault

LOS - Loss of signal


La **Optical Transceiver Diagnostics Table** (Tabla de diagnósticos del transceptor óptico) contiene las siguientes columnas:

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

 **NOTA:** Los transceptores Finisair no son compatibles con las pruebas de diagnóstico de fallo de los transmisores.

- 1 **LOS:** pérdida de señal.
- 1 **Data Ready** (Datos preparados): el transceptor tiene energía archivada y los datos están preparados.

1 N/A (N/D): no disponible, N/S (no compatible), W (advertencia), E (error).

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

Gestión de la seguridad del dispositivo

La página **Management Security** (Seguridad de gestión) proporciona acceso a las páginas de seguridad que contienen campos para establecer parámetros de seguridad para la seguridad de puertos, métodos de gestión de dispositivos, usuarios y servidores. Si desea abrir la página **Management Security** (Seguridad de gestión), haga clic en **System**→**Management Security** (Sistema→Seguridad de gestión) en la vista de árbol.

Definición de los perfiles de acceso

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

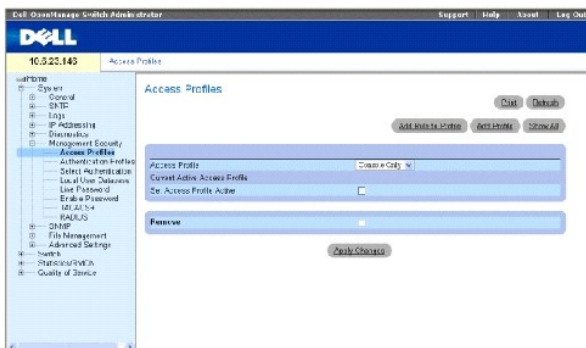
El acceso de gestión se puede definir aparte para cada tipo de método de acceso de gestión, incluidos la web (HTTP), la web segura (HTTPS), Telnet, Telnet segura y SNMP.

El acceso a diferentes métodos de administración puede variar entre los grupos de usuarios. Por ejemplo, el Grupo de usuarios 1 puede acceder al dispositivo sólo a través de una sesión HTTPS, mientras que el Grupo de usuarios 2 puede acceder al dispositivo a través de las sesiones HTTPS y Telnet.

Las listas de acceso de gestión contienen las reglas que determinan cuáles son los usuarios que pueden gestionar el dispositivo, y mediante qué métodos. También se puede bloquear a usuarios para impedir que accedan al dispositivo.

La página **Access Profiles** (Perfiles de acceso) contiene campos para configurar las listas de gestión y aplicarlas a determinadas interfaces. Para abrir la página **Access Profiles** (Perfiles de acceso), haga clic en **System**→**Management Security**→**Access Profiles** (Sistema→Seguridad de gestión→Perfiles de acceso) en la vista de árbol.

Ilustración 6-51. Access Profiles (Perfiles de acceso)



Access Profile (Perfil de acceso): listas de perfiles de acceso definidos por el usuario. La lista **Access Profile** (Perfil de acceso) contiene un valor predeterminado de la **Console List** (Lista de consolas), a la que se agregan perfiles de acceso definidos por el usuario. Si se selecciona **Console Only** (Sólo consola) como el nombre **Access Profile** (Perfil de acceso), se desconecta la sesión, y se activa el acceso al dispositivo sólo desde la consola.

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

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

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

Activación de un perfil

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

El perfil de acceso se activará.

Adición de un perfil de acceso

Las reglas hacen la función de filtros para determinar la prioridad de las reglas, el método de gestión del dispositivo, el tipo de interfaz, la máscara de red y la dirección IP de origen, así como la acción del acceso de gestión del dispositivo. Se pueden bloquear o permitir el acceso de gestión a los usuarios. La prioridad de las reglas establece el orden de su aplicación en un perfil.

Definición de las reglas para un perfil de acceso:

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

La página **Add An Access Profile** (Agregar un perfil de acceso) se abrirá:

Ilustración 6-52. Página Add An Access Profile (Agregar un perfil de acceso)

The screenshot shows the 'Add an Access Profile' configuration page. It features a 'Refresh' button at the top right. The main form area contains several fields: 'Access Profile Name' (a text input field), 'Rule Priority (1-65535)' (a text input field), 'Management Method' (a dropdown menu currently set to 'All'), 'Interface' (a checkbox), 'Source IP Address' (a text input field with '(0.0.0.0)' as a placeholder), 'Network Mask' (a text input field with '(0.0.0.0)' as a placeholder), 'Prefix Length' (a text input field with '/0/0' as a placeholder), and 'Action' (a dropdown menu currently set to 'Permit'). At the bottom of the form is an 'Apply Changes' button.

Access Profile Name (1-32 Characters) (Nombre de perfil de acceso [1 - 32 caracteres]): nombre definido por el usuario para el perfil de acceso.

Rule Priority (1-65535) (Prioridad de reglas [1-65535]): prioridad de las reglas. Cuando el paquete coincide con una regla, se otorga o se niega a los grupos de usuarios el acceso de administración del dispositivo. El orden de las reglas se establece mediante la definición de un número de regla en la **Profile Rules Table** (Tabla de reglas de perfil). El número de regla es vital para que los paquetes coincidan con las reglas, puesto que los paquetes coinciden con la primera regla a la que se ajusten. Las prioridades de las reglas se asignan en la **Tabla de reglas de perfil**.

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

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

NOTA: La asignación de un perfil de acceso a una interfaz deniega el acceso a través de otras interfaces. Si un perfil de acceso no se asigna a ninguna interfaz, se puede acceder al dispositivo a través de todas las interfaces.

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

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

Prefix Length (Longitud del prefijo): número de bits que componen el prefijo de la dirección IP de origen o máscara de red de la dirección IP de origen.

Action (Acción): define si se debe permitir o denegar el acceso de gestión a la interfaz definida.

3. Defina el campo **Access Profile Name** (Nombre del perfil de acceso).
4. Defina los campos pertinentes.
5. Haga clic en **Apply Changes** (Aplicar cambios).

El nuevo perfil de acceso se agregará y el dispositivo se actualizará.

Adición de reglas al perfil de acceso

NOTA: La primera regla debe estar definida para empezar a relacionar el tráfico a los perfiles de acceso.

1. Abra la página **Access Profiles** (Perfiles de acceso).
2. Haga clic en **Add Profile to Rule** (Agregar perfil a la regla).

La página **Add An Access Profile Rule** (Agregar una regla de perfil de acceso) se abrirá:

Ilustración 6-53. Add An Access Profile Rule (Agregar una regla de perfil de acceso)

Cancel

Access Profile Name Console Only

Priority (1-65535)

Management Method All

Interfaces

Port LAG VLAN

Exclude IP Address

Source IP Address (XXX.X) Network Mask (XXXX)

Prefix Length (M)

Action Permit

Apply Changes

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

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

Visualización de la tabla de reglas del perfil:

NOTA: el orden en el que aparecen las reglas en la tabla de reglas del perfil es importante. Los paquetes se corresponden con la primera regla, que cumple con los criterios de ésta.

1. Abra la página [Access Profiles](#) (Perfiles de acceso).
2. Haga clic en **Show All** (Mostrar todo).

La página **Profile Rules Table** (Tabla de reglas de perfil) se abrirá:

Ilustración 6-54. Página Profile Rules Table (Tabla de reglas de perfil)

Default

Profile Rules Table

Access Profile Name: Console Only

Priority	Interface	Management Method	Source IP Address	Prefix Length	Action	Remove
1		all		32	Deny	<input type="checkbox"/>

Apply Changes

Eliminación de una regla

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

La **Profile Rules Table** (Tabla de reglas de perfil) se abrirá.

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

La regla seleccionada se suprimirá y el dispositivo se actualizará.

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

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Access Profiles](#) (Perfiles de acceso).

Tabla 6-35. Access Profiles CLI Commands (Comandos de la CLI para perfiles de acceso)

Comando de la CLI	Description
<code>management access-list nombre</code>	Define una lista de acceso para la administración e introduce el contexto de la lista de acceso para la configuración.
<code>permit [ethernet número de interfaz vlan id-vlan port-channel número] [service servicio]</code>	Establece condiciones de generación de permisos de puerto para la lista de acceso de administración.
<code>permit ip-source dirección-ip [mask mask longitud-prefijo] [ethernet número de interfaz vlan id-vlan port-channel número] [service servicio]</code>	Establece condiciones de generación de permisos de puerto para la lista de acceso a la administración y el método de administración seleccionado.
<code>deny [ethernet número de interfaz vlan id-vlan port-channel número] [service servicio]</code>	Establece condiciones de denegación de puerto para la lista de acceso de administración y el método de administración seleccionado.
<code>deny ip-source dirección-ip [mask mask longitud-prefijo] [ethernet número de interfaz vlan id-vlan port-channel número] [service servicio]</code>	Establece condiciones de denegación de puerto para la lista de acceso de administración y el método de administración seleccionado.
<code>management access-class { console-only nombre }</code>	Define qué lista de acceso se utiliza como conexiones de administración activas.
<code>show management access-list [nombre]</code>	Muestra las listas de acceso de administración activas.
<code>show management access-class</code>	Muestra información sobre la clase de acceso de administración.

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

```

Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# deny ethernet g2

```

```
Console (config-macl)# deny ethernet g10

Console (config-macl)# exit

Console (config)# management access-class mlist

Console(config)#exit

Console# show management access-list

mlist
-----

permit ethernet g1

permit ethernet g9

! (Note: all other access implicitly denied)

Console> show management access-class

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

Definición de los perfiles de autenticación

La página [Authentication Profiles](#) (Perfiles de autenticación) contiene campos para seleccionar el método de autenticación del usuario en el dispositivo. La autenticación del usuario se lleva a cabo:

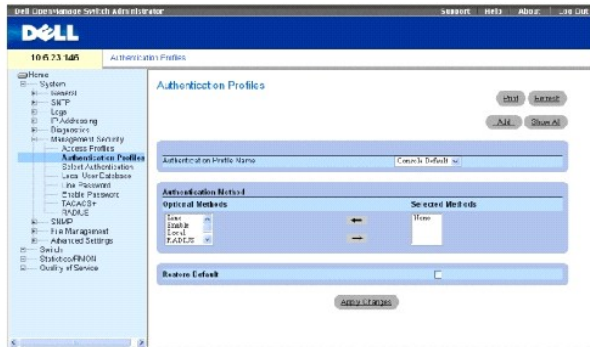
- 1 Localmente
- 1 A través de un servidor externo

La autenticación del usuario también se puede establecer en None (Ninguna).

La autenticación de usuarios se produce en el orden en el que se seleccionan los métodos. Por ejemplo, si las opciones de Local y RADIUS están seleccionadas, el usuario se autenticará primero localmente. Si la base de datos del usuario local está vacía, el usuario se autenticará a través del servidor RADIUS.

Si se produce un error durante la autenticación, se utiliza el siguiente método seleccionado. Para abrir la página [Authentication Profiles](#) (Perfiles de autenticación), haga clic en System→ Management Security→ Authentication Profiles (Sistema→ Seguridad de gestión→ Perfiles de autenticación) en la vista de árbol.

Ilustración 6-55. Authentication Profiles (Perfiles de autenticación)



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

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

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

Local (Local): la autenticación de usuarios se realiza en el dispositivo. Éste comprueba el nombre de usuario y la contraseña para llevar a cabo la autenticación.

RADIUS (RADIUS): la autenticación de usuarios se realiza en el servidor RADIUS. Para obtener más información, consulte el apartado "[Configuración de parámetros globales de RADIUS](#)."

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

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

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

Restore Default (Restaurar valor predeterminado): restaura el método de autenticación de usuarios predeterminado en el dispositivo.

Selección de un perfil de autenticación:

1. Abra la página [Authentication Profiles](#) (Perfiles de autenticación).
2. Seleccione un perfil en el campo **Authentication Profile Name** (Nombre de perfil de autenticación).
3. Seleccione el método de autenticación mediante el uso de las flechas de navegación.
4. Haga clic en **Apply Changes** (Aplicar cambios).

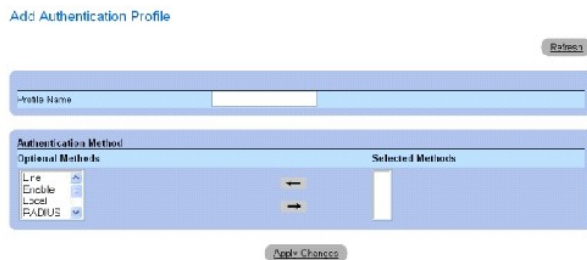
El perfil de autenticación del usuario se actualiza en el dispositivo.

Adición de un perfil de autenticación:

1. Abra la página [Authentication Profiles](#) (Perfiles de autenticación).
2. A continuación, haga clic en **Add** (Agregar).

La página **Add Authentication Method Profile Name** (Agregar nombre del perfil del método de autenticación) se abrirá:

Ilustración 6-56.



Página Add Authentication Profile (Agregar perfil de autenticación)

3. Configure el perfil.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El perfil de autenticación se actualizará en el dispositivo.

Visualización de la página de muestra de todos los perfiles de autenticación:

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

La página **Authentication Profile** (Perfil de autenticación) se abrirá:

Ilustración 6-57. Authentication Profiles (Perfiles de autenticación)



Supresión de un perfil de autenticación:

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

La página **Authentication Profile** (Perfil de autenticación) se abrirá.

3. Seleccione un perfil de autenticación.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El perfil de autenticación seleccionado se suprimirá.

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

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Authentication Profiles](#) (Perfiles de autenticación).

Tabla 6-36. Authentication Profile CLI Commands (Comandos de la CLI para el perfil de autenticación)

Comando de la CLI	Description
-------------------	-------------

<code>aaa authentication login { default nombre-lista } método1 [método2]</code>	Configura la autenticación de inicio de sesión.
<code>no aaa authentication login { default nombre-lista }</code>	Elimina un perfil de autenticación de inicio de sesión.

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

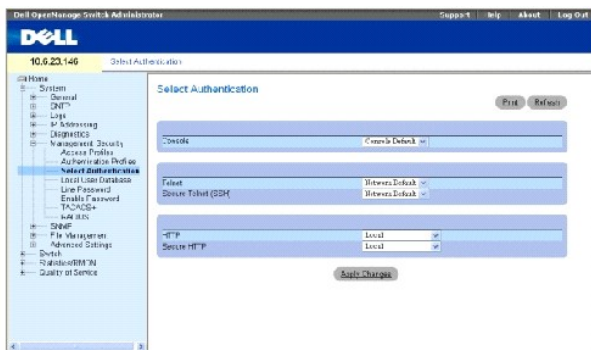
```
Console (config)# aaa authentication login default radius local enable none

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

Asignación de perfiles de autenticación

Cuando los perfiles de autenticación estén definidos, se podrán aplicar a los métodos de acceso de gestión. Por ejemplo, los usuarios de la consola se pueden autenticar mediante la Lista 1 de métodos de autenticación, mientras que los usuarios de Telnet se autentican mediante la Lista 2 de métodos de autenticación. Para abrir la página [Select Authentication](#) (Seleccionar autenticación), haga clic en System→ Management Security→ Select Authentication (Sistema→ Seguridad de gestión→ Seleccionar autenticación) en la vista de árbol.

Ilustración 6-58. Select Authentication (Seleccionar autenticación)



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

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

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

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

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

Local (Local): la autenticación se realiza localmente.

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

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

Aplicación de una lista de autenticación a sesiones de consola

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

Las sesiones de la consola están asignadas a una lista de autenticación.

Aplicación de un perfil de autenticación a sesiones de Telnet

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

Las sesiones de Telnet están asignadas a una lista de autenticación.

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

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

Las sesiones de Telnet segura (SSH) están asignadas a un perfil de autenticación.

Asignación de sesiones de HTTP a una secuencia de autenticación

1. Abra la página [Select Authentication](#) (Seleccionar autenticación).
2. Seleccione una secuencia de autenticación en el campo **HTTP**.
3. Haga clic en **Apply Changes** (Aplicar cambios).

Se asigna una secuencia de autenticación a sesiones de HTTP.

Asignación de sesiones de HTTP seguro a una secuencia de autenticación

1. Abra la página [Select Authentication](#) (Seleccionar autenticación).
2. Seleccione una secuencia de autenticación en el campo **Secure HTTP** (HTTP seguro).
3. Haga clic en **Apply Changes** (Aplicar cambios).

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

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

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Select Authentication](#) (Seleccionar autenticación).

Tabla 6-37. Select Authentication CLI Commands (Seleccionar comandos de la CLI para la autenticación)

Comando de la CLI	Description
<code>enable authentication [default nombre-lista]</code>	Especifica la lista de métodos de autenticación cuando se accede a un nivel superior de privilegio desde un Telnet o una consola remotos.
<code>login authentication [default nombre-lista]</code>	Especifica la lista de métodos de autenticación de inicio de sesión para un Telnet o consola remotos.
<code>ip http authentication método1 [método2]</code>	Especifica métodos de autenticación para servidores HTTP.
<code>ip https authentication método1</code>	Especifica métodos de autenticación para servidores HTTPS.

[método2]

show authentication methods

Muestra información sobre los métodos de autenticación.

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

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

Console (config-line)# login authentication default

Console (config-line)# exit

Console (config)# ip http authentication radius local

Console (config)# ip https authentication radius local

Console(config)#exit

Console# show authentication methods

Login Authentication Method Lists

-----

Default: Radius, Local, Line

Console_Login: Line, None

Enable Authentication Method Lists

-----

Default: Radius, Enable

Console_Enable: Enable, None

Line Login Method List Enable Method List

-----
```

```
Console Console_Login Console_Enable

Telnet Default Default

SSH Default Default

HTTP: Radius, local

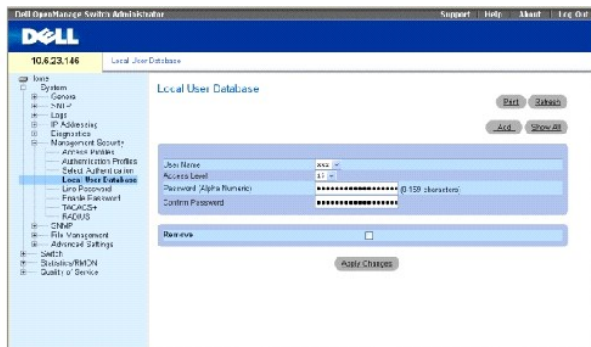
HTTPS: Radius, local

Dot1x: Radius
```

Definición de las bases de datos de usuarios locales

La página [Local User Database](#) (Base de datos de usuarios locales) contiene campos para definir usuarios, contraseñas y niveles de acceso. Para abrir la página [Local User Database](#) (Base de datos de usuarios locales), haga clic en System > Management Security > Local User Database (Sistema > Seguridad de gestión > Base de datos de usuarios locales) en la vista de árbol.

Ilustración 6-59. Local User Database (Base de datos de usuarios locales)



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

Access Level (Nivel de acceso): nivel de acceso de los usuarios. El nivel de acceso de los usuarios más bajo es el 1, y el más alto es el 15.

Password (0-159 Characters) (Contraseña [0 - 159 caracteres]): contraseña definida por el usuario. Las contraseñas de las bases de datos de usuarios locales pueden tener un máximo de 159 caracteres.

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

Remove (Eliminar): si esta opción está seleccionada, se eliminan usuarios de la lista **User Name** (Nombre de usuario).

Asignación de derechos de acceso a un usuario:

1. Abra la página [Local User Database](#) (Base de datos de usuarios locales).
2. Seleccione un usuario en el campo **User Name** (Nombre de usuario).

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

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

Definición de un nuevo usuario:

1. Abra la página [Local User Database](#) (Base de datos de usuarios locales).
2. Haga clic en **Add** (Agregar).

La página **Add User** (Agregar usuario) se abrirá:

Ilustración 6-60. Add User (Agregar usuario)

Attribute	Value
User Name (Alpha Numeric)	<input type="text"/> (12 characters)
Access Level (1-16)	1
Password (Alpha Numeric)	<input type="text"/> (0-128 characters)
Confirm Password	<input type="text"/>

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

Se define el nuevo usuario, y el dispositivo se actualiza.

Visualización de la tabla de usuarios locales:

1. Abra la página [Local User Database](#) (Base de datos de usuarios locales).
2. Haga clic en **Show All** (Mostrar todo).

La Local User Table (Tabla de usuarios locales) se abrirá:

Ilustración 6-61. Página Local User Table (Tabla de usuarios locales)

	User Name	Access Level	Remove
1	XXXX	15	<input checked="" type="checkbox"/>

Supresión de usuarios:

1. Abra la página [Local User Database](#) (Base de datos de usuarios locales).
2. Haga clic en **Show All** (Mostrar todo).

La **Local User Table** (Tabla de usuarios locales) se abrirá.

3. Seleccione un **nombre de usuario**.
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El usuario seleccionado se suprimirá y el dispositivo se actualizará.

Asignación de usuarios mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Local User Database](#) (Bases de datos de usuarios locales).

Tabla 6-38. Local User Database CLI Commands (Comandos de la CLI para bases de datos de usuarios)

Comando de la CLI	Description
<code>username nombre [password contraseña] [level nivel] [encrypted]</code>	Establece un sistema de autenticación basado en el nombre de usuario.

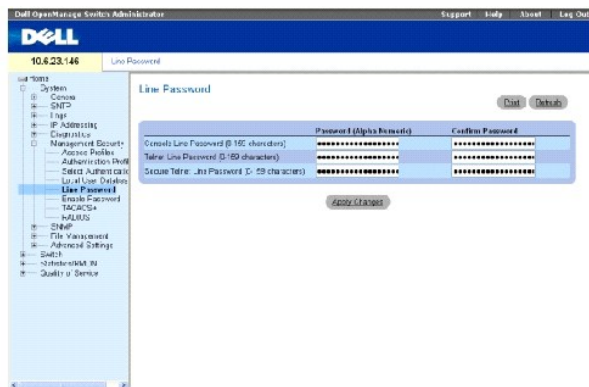
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config)# username bob password lee level 15
```

Definición de las contraseñas de línea

La página [Line Password](#) (Contraseña de línea) contiene campos para definir contraseñas de línea para métodos de gestión. Si desea abrir la página [Line Password](#) (Contraseña de línea), haga clic en System → Management Security → Line Passwords (Sistema → Seguridad de gestión → Contraseñas de línea) en la vista de árbol.

Ilustración 6-62. Line Password (Contraseña de línea)



Line Password for Console/Telnet/Secure Telnet (0-159 Characters) (Contraseña de línea para consola/Telnet/Telnet segura [0 - 159 caracteres]): la contraseña de línea para acceder al dispositivo a través de una sesión de consola, Telnet o Telnet segura. Las contraseñas pueden contener un máximo de 159 caracteres.

Confirm Password (Confirmar contraseña): confirma la nueva contraseña de línea. La contraseña se muestra como *****.

Definición de las contraseñas de línea para sesiones de consola

1. Abra la página [Line Password](#) (Contraseña de línea)
2. Defina el campo **Line Password for Console** (Contraseña de línea para consola).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La contraseña de línea para sesiones de consola se definirá y el dispositivo se actualizará.

Definición de las contraseñas de línea para sesiones de Telnet

1. Abra la página [Line Password](#) (Contraseña de línea).
2. Defina la contraseña de línea para el campo Telnet.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La contraseña de línea para las sesiones de Telnet se definirá y el dispositivo se actualizará.

Definición de las contraseñas de línea para sesiones de Telnet segura

1. Abra la página [Line Password](#) (Contraseña de línea).
2. Defina el campo **Line Password for Secure Telnet** (Contraseña de línea para Telnet segura).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La contraseña de línea para sesiones de Telnet segura se definirá y el dispositivo se actualizará.

Asignación de contraseñas de línea mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Line Password](#) (Contraseña de línea).

Tabla 6-39. Line Password CLI Commands (Comandos de la CLI para la contraseña de línea)

Comando de la CLI	Description
<code>password contraseña [encrypted]</code>	Especifica una contraseña en una línea.

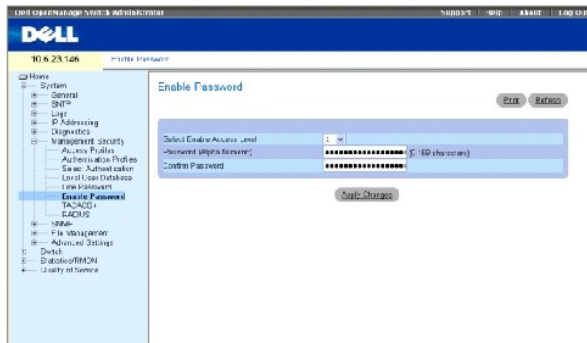
A continuación se muestra un ejemplo de los comandos de la CLI:

```
Console (config-line)# password dell
```

Definición de la contraseña de activación

En la página [Modify Enable Password](#) (Modificar contraseña de activación) se establece una contraseña local para controlar el acceso a la configuración normal, de privilegios y global. Para abrir la página [Modify Enable Password](#) (Modificar contraseña de activación), haga clic en System → Management Security → Enable Passwords (Sistema → Seguridad de gestión → Contraseña de activación) en la vista de árbol.

Ilustración 6-63. Modify Enable Password (Modificar contraseña de activación)



Select Enable Access Level (Seleccionar nivel de acceso de activación): nivel de acceso asociado a la contraseña de activación. Los valores de campo posibles son 1-15.

Password (0-159 Characters) (Contraseña [0 - 159 caracteres]): la contraseña de activación configurada actualmente. Las contraseñas de activación pueden contener un máximo de 159 caracteres.

Confirm Password (Contraseña de activación): confirma la nueva contraseña de activación. La contraseña se muestra como *****.

Definición de una nueva contraseña de activación:

1. Abra la página [Modify Enable Password](#) (Modificar contraseña de activación).
2. Defina los campos pertinentes.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La nueva contraseña de activación se definirá y el dispositivo se actualizará.

Asignación de contraseñas de activación mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Modify Enable Password](#) (Modificar contraseña de activación).

Tabla 6-40. Modify Enable Password CLI Commands (Comandos de la CLI para modificar la contraseña de activación)

Comando de la CLI	Description
<code>enable password [level nivel] password [encrypted]</code>	Establece una contraseña local para controlar el acceso a niveles de privilegio y usuario.
<code>show users accounts</code>	Muestra información sobre la base de datos de usuarios local.

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

```
Console (config)# enable password level 15 secret

Console# show users accounts

Username      Privilege
-----
secret        15
```

Definición de la configuración de TACACS+

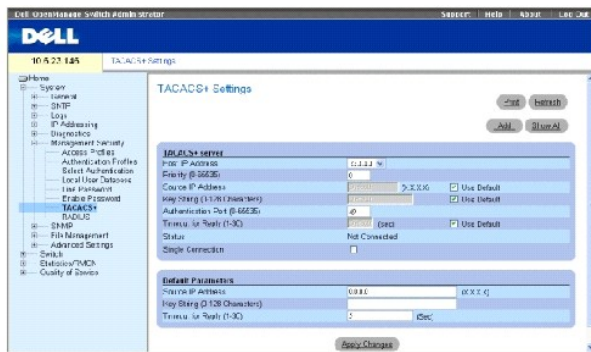
Los dispositivos proporcionan asistencia de Sistema de Control de Acceso al Controlador de Acceso a la Terminal (TACACS+) al cliente. TACACS+ proporciona seguridad centralizada para la validación de usuarios que acceden al dispositivo.

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

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

El protocolo TACACS+ garantiza la integridad de la red a través de intercambios de protocolo codificado entre el dispositivo y el servidor TACACS+. Para abrir la página [TACACS+ Settings](#) (Configuración de TACACS+), haga clic en **System** → **Management Security** → **TACACS+** (Sistema → Seguridad de gestión → TACACS+) en la vista de árbol.

Ilustración 6-64. TACACS+ Settings (Configuración de TACACS+)



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

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

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

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

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

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

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

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

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

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

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

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

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

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

Adición de un servidor TACACS+

1. Abra la página [TACACS+ Settings](#) (**Configuración de TACACS+**).
2. A continuación, haga clic en **Add** (Agregar).

La página [Add TACACS+ Host](#) (Agregar sistema principal de TACACS+) se abrirá:

Ilustración 6-65. Add TACACS+ Host (Agregar sistema principal de TACACS+)

Add TACACS+ Host Refresh

Host IP Address	<input type="text"/>	px.x.x.x
Priority (0-25535)	<input type="text"/>	
Source IP Address	<input type="text"/>	px.x.x.x <input type="checkbox"/> Use Default
Key String (1-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Authentication Port (0-25535)	<input type="text"/>	
Timeout for Reply (1-30)	<input type="text"/>	30 <input type="checkbox"/> Use Default
Single Connection	<input type="checkbox"/>	

Apply Changes

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

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

Visualización de la [Tabla de TACACS+](#)

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

La [TACACS+ Table](#) (Tabla de TACACS+) se abrirá:

Ilustración 6-66. TACACS+ Table (Tabla de TACACS+)

TACACS+ Table Refresh

	Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Remove
1	23.1.1.1	0	Default	40	Default	<input type="checkbox"/>	Not Connected	<input type="checkbox"/>

Apply Changes

Eliminación de un servidor TACACS+

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

La [TACACS+ Table](#) (Tabla de TACACS+) se abrirá.

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

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

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

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [TACACS+ Settings](#) (Configuración de TACACS+).

Tabla 6-41. TACACS+ CLI Commands (Comandos de la CLI para TACACS+)

Comando de la CLI	Description
TACACS-server host (<i>dirección IP</i> <i>nombre del sistema principal</i>) [single-connection] [port <i>puerto-número</i>] [timeout <i>tiempo de espera</i>] [key <i>clave-cadena</i>] [source <i>origen</i>] [priority <i>prioridad</i>]	Especifica un sistema principal de TACACS+.
no TACACS-server host (<i>dirección IP</i> <i>nombre de sistema principal</i>)	Suprime un sistema principal de TACACS+.
tacacs-server key <i>cadena-clave</i>	Especifica la autenticación y la clave de codificación para todas las comunicaciones de TACACS+ entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con la codificación utilizada en el daemon de TACACS+. (Intervalo: de 0 a 128 caracteres.)
tacacs-server timeout <i>tiempo de espera</i>	Especifica el valor del tiempo de espera en segundos. (Intervalo: de 1 a 30.)
tacacs-server source-ip <i>source</i>	Especifica la dirección IP de origen. (Intervalo: dirección IP válida.)
show TACACS [<i>dirección IP</i>]	Muestra la configuración y las estadísticas para un servidor TACACS+.

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

Console# show tacacs						
Router Configuration						

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority

12.1.1.2	Not Connected	49	Yes	1	12.1.1.1	1
Global values						

TimeOut : 5						

Router Configuration					

Source IP : 0.0.0.0					
console#					

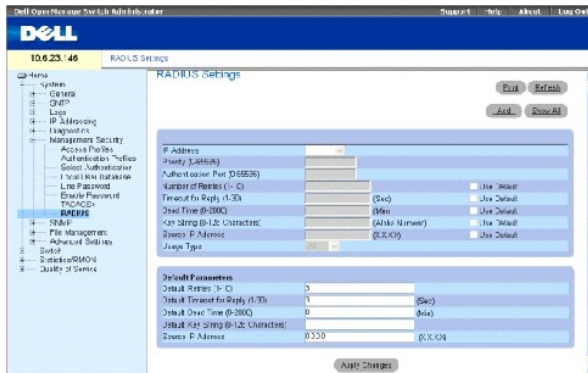
Configuración de parámetros globales de RADIUS

Los servidores de servicio de usuario de marcación de entrada de autorización remota (RADIUS) proporcionan seguridad adicional a las redes. Los servidores RADIUS proporcionan un método de autenticación centralizado para:

- 1 Acceso a Telnet
- 1 Acceso a web
- 1 Acceso de consola a dispositivo

Para abrir la página [RADIUS Settings](#) (Configuración RADIUS), haga clic en System → Management Security → RADIUS (Sistema → Seguridad de gestión → RADIUS) en la vista de árbol.

Ilustración 6-67. RADIUS Settings (Configuración de RADIUS)



IP Address (Dirección IP): lista de direcciones IP del servidor de autenticación.

Priority (1-65535) (Prioridad [1-65535]): especifica la prioridad del servidor. Los posibles valores son 1-65535, donde 1 es el valor más alto. Se utiliza para configurar el orden en el que se consulta a los servidores.

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

Number of Retries (1-10) (Número de reintentos [0 - 1]): especifica el número de solicitudes transmitidas que se envían al servidor RADIUS antes de que se produzca un fallo. Los valores posibles de campo son del 1 al 10. Tres es el valor predeterminado.

Timeout for Reply (1-30) (Tiempo de espera para respuesta [1 - 30]): especifica el tiempo (en segundos) que espera del dispositivo para recibir una respuesta del servidor RADIUS antes de volver a intentar consultar o cambiar al siguiente servidor. Los valores posibles del campo son del 1 al 30. El valor predeterminado es 3.


Dead Time (0-2000) (Tiempo muerto [0 - 2000]): especifica el tiempo (en segundos) durante el cual no se envían peticiones de servicio a un servidor RADIUS. El intervalo es 0-2000.

Key String (1-128 Characters) (Cadena de clave [1-128 caracteres]): especifica la cadena de clave utilizada para autenticar y codificar todas las comunicaciones de RADIUS entre el dispositivo y el servidor RADIUS. Esta clave está codificada.

Source IP Address (Dirección IP de origen): especifica la dirección IP de origen que se utiliza para establecer la comunicación con servidores RADIUS.

Los siguientes campos establecen los valores predeterminados de RADIUS:

Default Timeout for Reply (1-30) (Tiempo de espera predeterminado para respuesta [1 - 30]): especifica el tiempo predeterminado (en segundos) que el dispositivo espera para recibir una respuesta del servidor RADIUS antes de que se agote el tiempo.

 **NOTA:** si los valores de los tiempos de espera, reintentos o tiempos muertos determinados del sistema principal no están especificados, los valores globales (predeterminados) se aplican a cada sistema principal.

Default Retries (1-10) (Reintentos predeterminados [1 - 10]): especifica el número predeterminado de peticiones transmitidas que se envían al servidor RADIUS antes de que se produzca un fallo.

Default Dead Time (0-2000) (Tiempo muerto predeterminado [0-2000]): especifica el tiempo predeterminado (en segundos) durante el cual no se envían peticiones de servicio a un servidor RADIUS. El intervalo es 0-2000.

Default Key String (1-128 Characters) (Cadena de clave predeterminada [1 - 128 caracteres]): especifica la cadena de clave predeterminada utilizada para autenticar y codificar todas las comunicaciones de RADIUS entre el dispositivo y el servidor RADIUS. Esta clave está codificada.

Source IP Address (Dirección IP de origen): especifica la dirección IP de origen que se utiliza para establecer la comunicación con servidores RADIUS.

Usage Type (Tipo de utilización): especifica el tipo de utilización del servidor. Puede ser uno de los siguientes valores: inicio de sesión, 802.1x o todos. Si no está especificado, se toma de forma predeterminada para todos.

Definición de los parámetros de RADIUS:

1. Abra la página [RADIUS Settings](#) (Configuración de RADIUS).
2. Defina los campos.
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración de RADIUS está actualizada para el dispositivo.

Adición de un servidor RADIUS:

1. Abra la página [RADIUS Settings](#) (Configuración de RADIUS).
2. A continuación, haga clic en **Add** (Agregar).

La página **Add RADIUS Server** (Agregar servidor RADIUS) se abrirá:

Ilustración 6-68. Página Add RADIUS Server (Agregar servidor RADIUS)

Acid RADIUS Server Refresh

IP Address	<input type="text" value="192.168.1.100"/>	(X.X.X.X)
Priority ID (65535)	<input type="text" value="0"/>	
Authentication Port (65535)	<input type="text" value="1812"/>	
Number of Retries (1/0)	<input type="text" value="3"/>	<input checked="" type="checkbox"/> Use Default
Timeout for Reply (1/0)	<input type="text" value="5"/>	(Sec) <input checked="" type="checkbox"/> Use Default
Dead time (1/0)	<input type="text" value="30"/>	(Min) <input checked="" type="checkbox"/> Use Default
Key String (0-120 Characters)	<input type="text" value=""/>	(Alpha numeric) <input type="checkbox"/> Use Default
Source IP Address	<input type="text" value="192.168.1.100"/>	(X.X.X.X) <input checked="" type="checkbox"/> Use Default
Usage Type	<input type="text" value="All"/>	

Apply Changes

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

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

Visualización de la lista de servidores RADIUS:

1. Abra la página [RADIUS Settings](#) (Configuración de RADIUS).
2. Haga clic en **Show All** (Mostrar todo).

La página [Show all RADIUS Servers](#) (Mostrar todos los servidores RADIUS) se abrirá:

Ilustración 6-69. Show all RADIUS Servers (Mostrar todos los servidores RADIUS)

RADIUS Servers List Refresh

IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Usage Type	Remove
------------	----------	---------------------	-------------------	-------------------	-----------	-------------------	------------	--------

Apply Changes

Modificación de la configuración del servidor RADIUS:

1. Abra la página [RADIUS Settings](#) (Configuración de RADIUS).
2. Haga clic en **Show All** (Mostrar todo).

La página [RADIUS Servers List](#) (Lista de servidores RADIUS) se abrirá.

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

La configuración del servidor RADIUS se modifica, y el dispositivo se actualiza.

Supresión de un servidor RADIUS de la lista de servidores RADIUS:

1. Abra la página [RADIUS Settings](#) (Configuración de RADIUS).
2. Haga clic en **Show All** (Mostrar todo).

La página [RADIUS Servers List](#) (Lista de servidores RADIUS) se abrirá.

3. Seleccione un servidor RADIUS en la [RADIUS Servers List](#) (Lista de servidores RADIUS).
4. Seleccione la casilla de verificación **Remove** (Eliminar).
5. Haga clic en **Apply Changes** (Aplicar cambios).

El servidor RADIUS se eliminará de la RADIUS Servers List (Lista de servidores RADIUS).

Definición de los servidores RADIUS mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [RADIUS Settings](#) (Configuración de RADIUS).

Tabla 6-42. RADIUS Settings CLI Commands (Comandos de la CLI para la configuración de RADIUS)

Comando de la CLI	Description
<code>radius-server timeout</code> timeout	Establece el intervalo predeterminado para el cual un dispositivo espera la respuesta del sistema principal de un servidor.
<code>radius-server retransmit</code> <i>reintentos</i>	Especifica el número predeterminado de veces que el software busca la lista de sistemas principales de servidores RADIUS.
<code>radius-server deadtime</code> <i>tiempo muerto</i>	Configura servidores predeterminados no disponibles que deben omitirse.
<code>radius-server key</code> [<i>cadena-clave</i>]	Establece la autenticación predeterminada y la clave de codificación para todas las comunicaciones de RADIUS entre el dispositivo y el entorno de RADIUS.
<code>radius-server host</code> { <i>dirección IP</i> <i>nombre del sistema principal</i> } [<code>auth-port</code> <i>número puerto-aut</i>] [<code>timeout</code> <i>tiempo de espera</i>] [<code>retransmit</code> <i>reintentos</i>] [<code>deadtime</code> <i>tiempo muerto</i>] [<code>key</code> <i>tecla-cadena</i>] [<code>source</code> <i>origen</i>] [<code>priority</code> <i>prioridad</i>] [<code>usage</code> <i>tipo</i>]	Especifica el sistema principal de un servidor RADIUS y cualquier configuración no predeterminada.
<code>show radius-servers</code>	Muestra la configuración del servidor RADIUS.

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

```

Console (config)# radius-server timeout 5

Console(config)#radius-server retransmit 5

Console (config)# radius-server deadtime 10

Console (config)# radius-server key dell-server

Console (config)# radius-server host 196.210.100.1 auth-port 1645 timeout 20

```

```

Console# show radius-servers

```

Port								
IP address	Auth	Acct	TimeOut	Retransmit	Deadtime	Source IP	Priority	Usage
-----	----	----	-----	-----	-----	-----	-----	-----
33.1.1.1	1812	1813	6	4	10	0.0.0.0	0	All
172.16.1.2	1645	1646	11	8	Global	Global	2	All
Global values								

```
-----  
  
TimeOut: 5  
  
Retransmit: 5  
  
Deadtime: 10  
  
Source IP: 0.0.0.0
```

Definición de los parámetros de SNMP

El SNMP (Simple Network Management Protocol, Protocolo simple de administración de red) proporciona un método para administrar dispositivos en una red. Los dispositivos compatibles con SNMP ejecutan un software local (agente).

Los agentes SNMP mantienen una lista de variables que se utilizan para administrar el dispositivo. Las variables se definen en la MIB (Management Information Base, Base de datos de información de administración). La MIB contiene las variables controladas por el agente. El protocolo SNMP define el formato de especificación de la MIB, así como el formato utilizado para acceder a la información a través de la red.

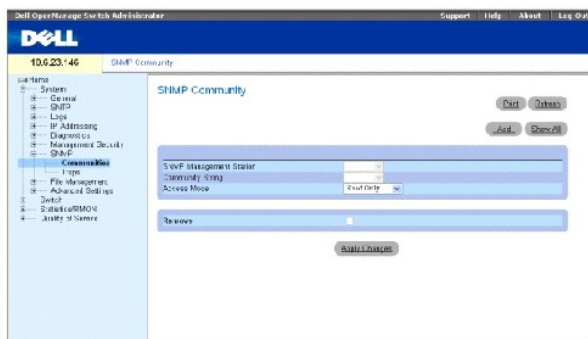
Las cadenas de acceso controlan los derechos de acceso al agente SNMP. Para comunicarse con el dispositivo, el servidor Web integrado (Embedded Web Server) debe enviar una cadena de comunidad válida para la autenticación. Para abrir la página SNMP, haga clic en System → SNMP (Sistema → SNMP) en la vista de árbol.

Esta sección contiene información para gestionar la configuración de SNMP.

Definición de las comunidades

Los derechos de acceso están gestionados mediante la definición de comunidades en la **Community Table** (Tabla de comunidades). Cuando se cambian los nombres de las comunidades, los derechos de acceso también cambian. Para abrir la página [SNMP Community](#) (Comunidad de SNMP), haga clic en System → SNMP → Communities (Sistema → SNMP → Comunidades) en la vista de árbol.

Ilustración 6-70. SNMP Community (Comunidad de SNMP)



SNMP Management Station (Management Station de SNMP): una lista de direcciones IP de la Management Station.

Community String (Cadena de comunidad): funciona como una contraseña y se utiliza para autenticar la Management Station seleccionada para el dispositivo.

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

Read Only (Sólo lectura): el acceso de gestión está restringido a sólo lectura para todas las MIB excepto la tabla de comunidades, para la que no hay acceso.

Read Write (Lectura / escritura): el acceso de gestión es de lectura y escritura para todas las MIB excepto la tabla de comunidades, para la que no hay acceso.

SNMP Admin (Administración de SNMP): el acceso de gestión es de lectura y escritura para todas las MIB, incluida la tabla de comunidades.

Remove (Eliminar): si esta opción está seleccionada, se elimina una comunidad.

Definición de una nueva comunidad

1. Abra la página [SNMP Community](#) (Comunidad SNMP).
2. A continuación, haga clic en **Add** (Agregar).

La página **Add SNMP Community** (Agregar comunidad de SNMP) se abrirá:

Ilustración 6-71. Add SNMP Community (Agregar comunidad de SNMP)



3. Seleccione una de las siguientes opciones:

Management Station (Management Station): define una comunidad de SNMP para una determinada Management Station. (Un valor de 0.0.0.0 especifica todas las Management Stations).

All (Todas): define una comunidad de SNMP para todas las Management Stations.

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

La comunidad nueva se guarda, y el dispositivo se actualiza.

Visualización de todas las comunidades

1. Abra la página [SNMP Community](#) (Comunidad SNMP).
2. Haga clic en **Show All** (Mostrar todo).

La [Community Table](#) (Tabla de comunidades) se abrirá:

Ilustración 6-72. Community Table (Tabla de comunidades)



Supresión de comunidades

1. Abra la página [SNMP Community](#) (Comunidad SNMP).
2. Haga clic en **Show All** (Mostrar todo).

La [Community Table](#) (Tabla de comunidades) se abrirá.

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

La entrada de la comunidad seleccionada se suprimirá y el dispositivo se actualizará.

Configuración de comunidades mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [SNMP Community](#) (Comunidad SNMP).

Tabla 6-43. SNMP Community CLI Commands (Comandos de la CLI para la comunidad de SNMP)

Comando de la CLI	Description
<code>snmp-server community <i>cadena</i> [ro rw su] [<i>dirección-ip</i>]</code>	Configura la cadena de acceso a la comunidad para permitir el acceso al protocolo SNMP.
<code>snmp-server host {<i>dirección-ip</i> <i>nombre host</i>} <i>cadena-comunidad</i> [1 2]</code>	Determina el tipo de captura enviada al destinatario seleccionado.
<code>show snmp</code>	Comprueba el estado de las comunicaciones de SNMP.

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

console(config)# snmp-server community public_1 su 1.1.1.1		
console(config)# snmp-server community public_2 rw 2.2.2.2		
console(config)# snmp-server community public_3 ro 3.3.3.3		
console(config)# snmp-server host 1.1.1.1 public_1 1		
console(config)# snmp-server host 2.2.2.2 public_2 2		
console(config)#		
console# show snmp		
Community-String	Community-Access	IP address

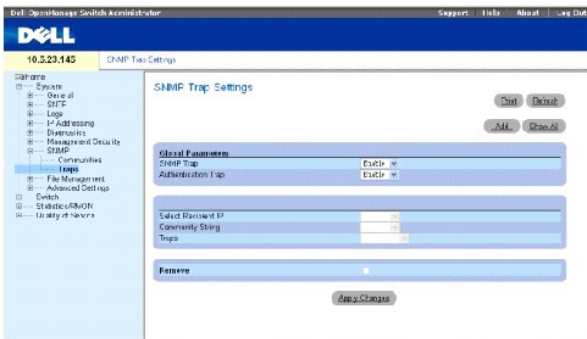
public_1	super	1.1.1.1

public_2	readwrite	2.2.2.2
public_3	readonly	3.3.3.3
Traps are enabled.		
Authentication-failure trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
-----	-----	-----
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 345 6789		
System Location: 1234 5678		
console#		

Definición de las capturas

Desde la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP), el usuario puede activar o desactivar el dispositivo para enviar capturas o notificaciones de SNMP. Para abrir la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP), haga clic en System → SNMP → Traps (Sistema → SNMP → Capturas) en la vista de árbol.

Ilustración 6-73. SNMP Trap Settings (Configuración de capturas de SNMP)



SNMP Trap (Captura SNMP): activa el envío de capturas de SNMP o notificaciones de SNMP del dispositivo a los destinatarios de captura definidos.

Authentication Trap (Captura de autenticación): activa el envío de capturas de SNMP cuando falla la autenticación para definir los destinatarios.

Select Recipient IP (Seleccionar IP de destinatario): especifica la dirección IP a la que se envían las capturas.

Community String (Cadena de comunidad): identifica la cadena de comunidad del gestor de capturas.

Traps (Capturas): determina el tipo de captura enviada al destinatario seleccionado. Los valores de campo posibles son:

SNMP V1: se envían las capturas de SNMP de la versión 1.

SNMP V2c: se envían las capturas de SNMP de la versión 2.

Remove (Eliminar): si esta opción está seleccionada, se eliminan entradas de la **Trap Manager Table** (Tabla de gestores de capturas).

Activación de capturas de SNMP en el dispositivo

1. Abra la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP).
2. Seleccione **Enable** (Activar) en la lista desplegable **SNMP Trap** (Captura de SNMP).
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se activan las capturas de SNMP en el dispositivo.

Activación de capturas de autenticación en el dispositivo

1. Abra la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP).
2. Seleccione **Enable** (Activar) en la lista desplegable **Authentication Trap** (Captura de autenticación).
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Las capturas de autenticación se activarán en el dispositivo.

Adición de un nuevo destinatario de capturas:

1. Abra la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP).
2. Haga clic en **Add** (Agregar).

La página [Add Trap Receiver/Manager](#) (Agregar receptor/gestor de capturas) se abrirá:

Ilustración 6-74. Add Trap Receiver/Manager (Agregar receptor/gestor de capturas)

The screenshot shows a web form titled "Add Trap Recipient". At the top right is a "Back" button. The form has three input fields: "Recipient IP Address" with a placeholder "(X.X.X.X)", "Community String (1-20 Characters)", and "Trap Enable" with a dropdown menu currently showing "SNMPV1". Below the form is an "Apply Changes" button.

3. Defina los campos. La configuración de 0.0.0.0 significa "Todas", y las capturas se difunden.
4. Haga clic en **Apply Changes** (Aplicar cambios).

Se agrega el administrador / destinatario de capturas, y el dispositivo se actualiza.

Visualización de la tabla de gestores de capturas

La **Trap Managers Table** (Tabla de gestores de capturas) contiene campos para configurar los tipos de captura.

1. Abra la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP).
2. Haga clic en **Show All** (Mostrar todo).

La página [Trap Managers Table](#) (Tabla de gestores de capturas) se abrirá:

Ilustración 6-75. Trap Managers Table (Tabla de gestores de capturas)

Recipient IP	Trap	Community String	Remove
--------------	------	------------------	--------

Supresión de una entrada de la tabla del administrador de capturas

1. Abra la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP).
2. Haga clic en **Show All** (Mostrar todo).

La página [Trap Managers Table](#) (Tabla de gestores de capturas) se abrirá.

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

El gestor de capturas seleccionado se suprimirá y el dispositivo se actualizará.

Configuración de capturas mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [SNMP Trap Settings](#) (Configuración de capturas de SNMP).

Tabla 6-44. SNMP Trap Settings CLI Commands (Comandos de la CLI para la configuración de capturas de SNMP)

Comando de la CLI	Description
<code>snmp-server enable traps</code>	Activa el dispositivo para enviar capturas o notificaciones de SNMP.
<code>snmp-server trap authentication</code>	Activa el dispositivo para enviar capturas de SNMP cuando falla la autenticación.
<code>snmp-server host <i>direc-host cadena-comunidad</i> [1 2]</code>	Determina el tipo de captura enviado al destinatario seleccionado.
<code>show snmp</code>	Muestra el estado de las comunicaciones de SNMP.

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

```
console(config)# snmp-server community public_1 su 1.1.1.1
console(config)# snmp-server community public_2 rw 2.2.2.2
```

console(config)# snmp-server community public_3 ro 3.3.3.3		
console(config)# snmp-server host 1.1.1.1 public_1 1		
console(config)# snmp-server host 2.2.2.2 public_2 2		
console(config)# snmp-server enable traps		
console(config)# snmp-server trap authentication		
console(config)#		
console# show snmp		
Community-String		
Community-Access		
IP address		

public_1	super	1.1.1.1
public_2	readwrite	2.2.2.2
public_3	readonly	3.3.3.3
Traps are enabled.		
Authentication-failure trap is enabled.		
Trap-Rec-Address		
Trap-Rec-Community		
Version		

-		
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 345 6789		
System Location: 1234 5678		
console#		

Gestión de archivos

La página File Management (Gestión de archivos) contiene campos para gestionar el software del dispositivo, los archivos de imagen y los archivos de configuración. Los archivos se pueden descargar de un servidor TFTP.

Visión general de la gestión de archivos

La estructura del archivo de configuración consiste en los siguientes archivos de configuración:

- 1 Startup Configuration File (Archivo de configuración de inicio): contiene los comandos necesarios para reconfigurar el dispositivo con la misma configuración que cuando el dispositivo se apaga o reinicia. El archivo de inicio se crea copiando los comandos de configuración del archivo de configuración en ejecución o del archivo de configuración de copia de seguridad.
- 1 Running Configuration File (Archivo de configuración en ejecución): contiene todos los comandos del archivo de inicio, así como todos los comandos especificados durante la sesión actual. Después de apagar o reiniciar el dispositivo, se pierden todos los comandos almacenados en el archivo de configuración en ejecución. Durante el proceso de inicio, todos los comandos del archivo de inicio se copian en el archivo de configuración en ejecución y se aplican al dispositivo. Durante la sesión, todos los comandos nuevos que se han especificado se agregan a los comandos ya existentes del archivo de configuración en ejecución en el archivo de configuración de inicio. La próxima vez que se reinicie el dispositivo, los comandos se vuelven a copiar en el archivo de configuración en ejecución desde el archivo de configuración de inicio.
- 1 Backup Configuration File (Archivo de configuración de copia de seguridad): contiene una copia de seguridad de la configuración del dispositivo. El archivo de copia de seguridad se genera cuando los archivos de configuración en ejecución o de inicio se copian en el archivo de copia de seguridad. Los comandos copiados en el archivo reemplazan a los comandos existentes guardados en el archivo de copia de seguridad. El contenido del archivo de copia de seguridad puede copiarse en el archivo de configuración en ejecución o en el archivo de configuración de inicio.
- 1 Image files (Archivos de imagen): las imágenes del archivo del sistema se guardan en dos archivos Flash llamados imágenes (Imagen 1 e Imagen 2). La imagen activa almacena la copia activa, mientras que la otra imagen almacena una segunda copia. El dispositivo se inicia y se ejecuta desde la imagen activa. Si la imagen activa está dañada, el sistema se inicia automáticamente desde la imagen no activa. Se trata de una función de seguridad contra fallos que se producen durante el proceso de actualización del software.

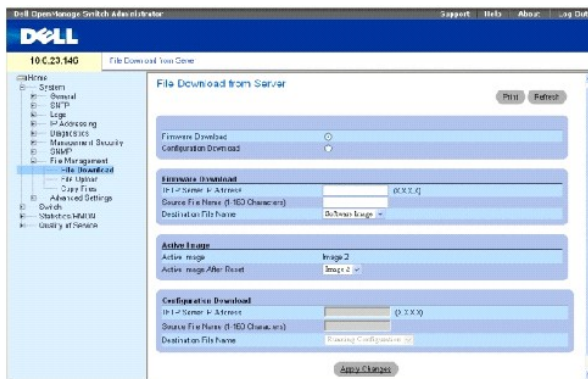
Para abrir la página File Management (Gestión de archivos), haga clic en System → File Management (Sistema → Gestión de archivos) en la vista de árbol. La página File Management (Gestión de archivos) contiene vínculos a:

- 1 File Download (Descarga de archivos)
- 1 File Upload (Carga de archivos)
- 1 Copy Files (Copia de archivos)

Descarga de archivos

La página [File Download From Server](#) (Descarga de archivos desde el servidor) contiene campos para descargar archivos de imagen del sistema y de configuración del servidor TFTP al dispositivo. Para abrir la página [File Download From Server](#) (Descarga de archivos del servidor) haga clic en System → File Management → File Download (Sistema → Gestión de archivos → Descarga de archivos) en la vista de árbol.

Ilustración 6-76. File Download From Server (Descarga de archivos del servidor)



Firmware Download (Descarga de firmware): archivo de firmware se ha descargado. Si se selecciona **Firmware Download** (Descarga de firmware), los campos de **Configuration Download** (Descarga de configuración) aparecen atenuados.

Configuration Download (Descarga de configuración): el archivo de configuración se ha descargado. Si la opción **Configuration Download** (Descarga de configuración) está seleccionada, los campos de **Firmware Download** (Descarga de firmware) aparecen atenuados.

Firmware Download TFTP Server IP Address (Dirección IP del servidor TFTP de descarga de firmware): dirección IP del servidor TFTP desde el cual se descargan los archivos.

Firmware Download Source File Name (Nombre del archivo de origen de descarga de firmware): especifica el archivo que se va a descargar.

Firmware Download Destination File (Archivo de destino de descarga de firmware): tipo de archivo de destino en el que se descarga el archivo. Los valores de campo posibles son:

Software Image (Imagen del software): descarga el archivo de imagen.

Boot Code (Código de arranque): descarga el archivo de arranque.

Active Image (Imagen activa): archivo de imagen que está actualmente activo.

Active Image After Reset (Imagen activa después del restablecimiento): el archivo de imagen que está activo tras restablecer el dispositivo.

Configuration Download File TFTP Server IP Address (Dirección IP del servidor TFTP del archivo de descarga de configuración): dirección IP del servidor TFTP desde la que se descargan los archivos de configuración.

Configuration Download File Source File Name (Nombre del archivo de origen de descarga de configuración): especifica los archivos de configuración que se van a descargar.

Configuration Download File Destination (Destino del archivo de descarga de configuración): archivo de destino en el que se descarga el archivo de configuración. Los valores de campo posibles son:

Running Configuration (Configuración en ejecución): descarga comandos en el archivo de configuración en ejecución.


Startup Configuration (Configuración de inicio): descarga el archivo de configuración de inicio y lo sobrescribe.

Backup Configuration (Configuración de copia de seguridad): descarga el archivo de configuración de copia de seguridad y lo sobrescribe.

Descarga de archivos:

1. Abra la página [File Download From Server](#) (Descarga de archivos del servidor).
2. Defina el tipo de archivo que desee descargar.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El software se descarga en el dispositivo.

 **NOTA:** para activar el archivo de imagen seleccionado, restablezca el dispositivo. Para obtener información sobre el restablecimiento del dispositivo, consulte el apartado "[Restablecimiento del dispositivo](#)".

Descarga de archivos mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [File Download From Server](#) (Descarga de archivos del servidor).

Tabla 6-45. File Download CLI Commands (Comandos de la CLI para la descarga de archivos)

Comando de la CLI	Description
<code>copy url-origen url-destino [snmp]</code>	Copia un archivo de un origen en un destino.

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

```

console# copy running-config tftp://11.1.1.2/pp.txt

NOTA: Cada "!" indica que diez paquetes se han transferido
correctamente.

Accessing file 'file1' on 172.16.101.101.

Loading file1 from
172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

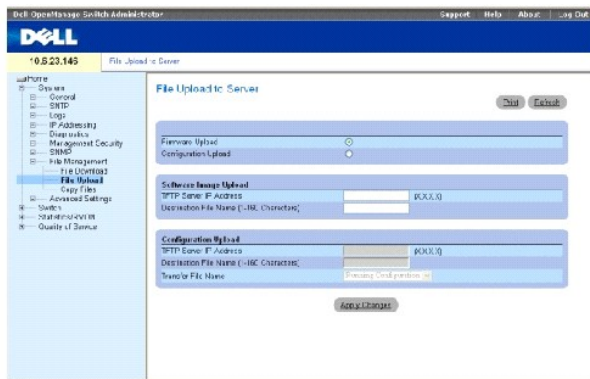
Copy took 0:01:11 [hh:mm:ss]

```

Carga de archivos

La página [File Upload to Server](#) (Carga de archivos al servidor) contiene campos para cargar el software del servidor TFTP al dispositivo. El archivo de imagen también se puede cargar desde la página [File Upload to Server](#) (Carga de archivos en el servidor). Para abrir la página [File Upload to Server](#) (Carga de archivos al servidor), haga clic en System → File Management → File Upload (Sistema → Gestión de archivos → Carga de archivos) en la vista de árbol.

Ilustración 6-77. File Upload to Server (Carga de archivos al servidor)



Firmware Upload (Carga de firmware): el archivo de firmware se ha cargado. Si la opción **Firmware Upload** (Carga de firmware) está seleccionada, los campos de **Configuration Upload** (Carga de configuración) aparecen atenuados.

Configuration Upload (Carga de configuración): el archivo de configuración se ha cargado. Si la opción **Configuration Upload** (Carga de configuración) está seleccionada, los campos de **Software Image Upload** (Carga de la imagen del software) aparecen atenuados.

Software Image Upload TFTP Server IP Address (Dirección IP del servidor TFTP de carga de imágenes de software): dirección IP del servidor TFTP en el que se carga la imagen del software.

Software Image Upload Destination (Destino de carga de imagen de software): especifica la ruta de acceso del archivo de imagen de software en la que se carga el archivo.

Configuration Upload TFTP Server IP Address (Dirección IP del servidor TFTP de carga de configuración): dirección IP del servidor TFTP en el que se carga el archivo de configuración.

Configuration Upload Destination (Destino de carga de configuración): especifica la ruta de acceso del archivo de configuración en la que se carga el archivo.

Configuration Upload Transfer file name (Nombre del archivo de transferencia de carga de configuración): archivo de software en el que se carga la configuración. Los valores de campo posibles son:

Running Configuration (Configuración en ejecución): carga el archivo de configuración en ejecución.

Startup Configuration (Configuración de inicio): carga el archivo de configuración de inicio.

Backup Configuration (Configuración de copia de seguridad): carga el archivo de configuración de copia de seguridad.

Carga de archivos

1. Abra la página [File Upload to Server](#) (Carga de archivos al servidor).
2. Defina el tipo de archivo que desee cargar.
3. Defina los campos.
4. Haga clic en **Apply Changes** (Aplicar cambios).

El software se carga en el dispositivo.

Carga de archivos mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [File Upload to Server](#) (Carga de archivos al servidor).

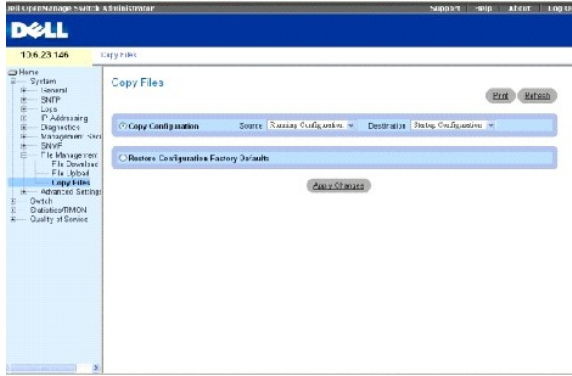
Tabla 6-46. File Upload CLI Commands (Comandos de la CLI para la carga de archivos)

Comando de la CLI	Description
<code>copy url-origen url-destino [snmp]</code>	Copia un archivo de un origen en un destino.

Copia de archivos

Los archivos se pueden copiar y suprimir en la página [Copy Files](#) (Copia de archivos). Para abrir la página [Copy Files](#) (Copia de archivos), haga clic en System→ File Management→ Copy Files (Sistema→ Gestión de archivos→ Copia de archivos) en la vista de árbol.

Ilustración 6-78. Copy Files (Copia de archivos)



Copy Configuration (Configuración de la copia): si esta opción está seleccionada, se copian los archivos de configuración en ejecución, configuración de inicio o configuración de copia de seguridad. Los valores de campo posibles son:

Source (Origen): copia los archivos de configuración en ejecución, configuración de inicio o configuración de copia de seguridad.

Destination (Destino): archivo en el que se copian los archivos de configuración en ejecución, configuración de inicio o configuración de copia de seguridad.

Restore Configuration Factory Defaults (Restaurar valores predeterminados de configuración de fábrica): si esta opción está seleccionada, se especifica que los archivos predeterminados de configuración de fábrica se deben restablecer. Si no está seleccionada, se mantienen los valores actuales de configuración.

Copia de archivos

1. Abra la página [Copy Files](#) (Copia de archivos).
2. Defina los campos **Source** (Origen) y **Destination** (Destino).
3. Haga clic en **Apply Changes** (Aplicar cambios).

El archivo se copiará y el dispositivo se actualizará.

Restauración de la configuración predeterminada de fábrica de la empresa

1. Abra la página [Copy Files](#) (Copia de archivos).
2. Haga clic en **Restore Company Factory Defaults** (Restaurar valores predeterminados de fábrica de la empresa).
3. Haga clic en **Apply Changes** (Aplicar cambios).

La configuración predeterminada de fábrica de la empresa se restaurará y el dispositivo se actualizará.

Copia y supresión de archivos mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [Copy Files](#) (Copia de archivos).

Tabla 6-47. Copy Files CLI Commands (Comandos de la CLI para la copia de archivos)

Comando de la CLI	Description
<code>copy url-fuente url-destino [snmp]</code>	Copia un archivo de un origen en un destino.
<code>delete startup-config</code>	Suprime el archivo de configuración de inicio.

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

```

Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101.

Loading file1 from
172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]

Console# delete startup-config

console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded

```

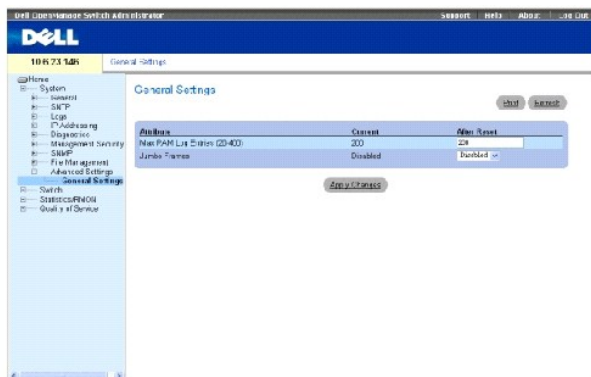
Definición de la configuración avanzada

La página **Advanced Settings** (Configuración avanzada) contiene un enlace para configurar los valores generales. Utilice la configuración avanzada para establecer diversos atributos globales para el dispositivo. Los cambios realizados en estos atributos sólo se aplican después de restablecer el dispositivo. Para abrir la página **Advanced Settings** (Configuración avanzada), haga clic en System → Advanced Settings (Sistema → Configuración avanzada) en la vista de árbol.

Configuración de parámetros generales de ajuste del dispositivo

La página **General Settings** (Configuración general) proporciona información para definir los parámetros generales del dispositivo. Para abrir la página **General Settings** (Configuración general), haga clic en System → Advanced Settings → General (Sistema → Configuración avanzada → General) en la vista de árbol.

Ilustración 6-79. General Settings (Configuración general)



Attribute (Atributo): atributo de configuración general.

Current (Actual): valor configurado actualmente.

After Reset (Después del restablecimiento): el valor futuro (después del restablecimiento). Al especificar un valor en la columna After Reset (Después del restablecimiento), la memoria se asigna a la tabla de campos.

Max RAM Log Entries (20-400) (Entradas máximas de registros RAM): número máximo de entradas de registros RAM. Cuando ya no caben más entradas de registro, el registro se borra y el archivo de registro se reinicia.

Jumbo Frames (Tramas gigantes): activa o desactiva la función de tramas gigantes. La opción de Jumbo Frames (Tramas gigantes) activa el transporte de datos idénticos en menos tramas. De este modo se garantiza un menor coste, un tiempo de procesamiento inferior y menos interrupciones.

Visualización del contador de entradas de registros RAM mediante los comandos de la CLI

En la siguiente tabla se resumen los comandos de la CLI equivalentes para configurar los campos que se visualizan en la página [General Settings](#) (Configuración general).

Tabla 6-48. General Settings CLI Commands (Comandos de la CLI para la configuración general)

Comando de la CLI	Description
<code>logging buffered size <i>número</i></code>	Establece el número de mensajes del registro del sistema almacenados en el búfer interno (RAM).
<code>port jumbo-frame</code>	Activa las tramas gigantes para el dispositivo.

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

```
Console (config)# logging buffered size 300
```

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Guía del usuario del sistema Dell™ PowerConnect™ 5324



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



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



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

La información contenida en este documento puede modificarse sin aviso previo.
© 2003 - 2004 Dell Inc. Todos los derechos reservados.

Queda prohibida su reproducción en cualquier medio sin la autorización por escrito de Dell Corporation.

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* y *Windows* son marcas comerciales registradas de Microsoft Corporation.

Este documento puede incluir otras comerciales y nombres comerciales para referirse a las entidades que son propietarias de los mismos o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Abril de 2004 Rev. A00

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Utilización del administrador del conmutador Dell OpenManage

Guía del usuario del sistema Dell™ PowerConnect™ 5324

- [Descripción de la interfaz](#)
- [Utilización de los botones del administrador del conmutador](#)
- [Inicio de la aplicación](#)
- [Acceso al dispositivo mediante la CLI](#)
- [Utilización de la CLI](#)

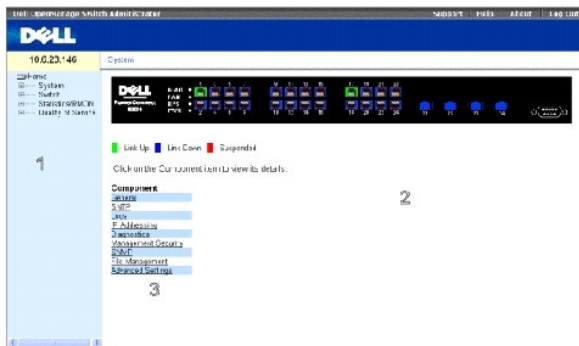
En esta sección se ofrece una introducción a la interfaz para el usuario.

Descripción de la interfaz

La página principal contiene las siguientes vistas:

- 1 Vista de árbol: situada en la parte izquierda de la página principal, la vista de árbol proporciona una vista ampliable de las funciones y sus componentes.
- 1 Vista de dispositivo: situada en la parte derecha de la página principal, la vista de dispositivo proporciona una vista del dispositivo, un área de información o tabla, e instrucciones de configuración.

Ilustración 5-13. Componentes del administrador del conmutador



En la [Tabla 5-7](#) aparecen los componentes de la interfaz con sus correspondientes números.

Tabla 5-7. Componentes de la interfaz

Componente	Nombre
1	La vista de árbol contiene una lista de las diferentes funciones del dispositivo. Las ramas de la vista de árbol se pueden expandir para ver todos los componentes de una determinada función, o se pueden retraer para ocultar los componentes de la función. Si se arrastra la barra vertical a la derecha, se puede expandir el área del árbol para ver el nombre completo de un componente.
2	La vista de dispositivo proporciona información sobre los puertos del dispositivo, el estado y la configuración actuales, información sobre la tabla, y los componentes de las funciones. Según la opción seleccionada, el área situada en la parte inferior de la vista de dispositivo muestra más información sobre el dispositivo y/o los cuadros de diálogo para configurar los parámetros.
3	La lista de componentes contiene una lista de los componentes de las funciones. Los componentes también se pueden ver ampliando una función en la vista de árbol.
4	Los botones de información proporcionan acceso a información sobre el dispositivo así como acceso a la página Dell Support. Para obtener más información, consulte el apartado " Botones de información ".

Representación del dispositivo

La página principal de PowerConnect contiene una representación gráfica del panel anterior del dispositivo.

Ilustración 5-14. Indicadores de los LED de los puertos



■ Link Up ■ Link Down ■ Disabled

El color del puerto indica si un puerto específico está actualmente activo. Los puertos pueden ser de los siguientes colores:

Tabla 5-8. Indicadores de los LED

Componente	Nombre
Indicadores de los puertos	
Verde	El puerto está actualmente activo.
Rojo	Se ha producido un error en el puerto.
Azul	El puerto está actualmente desactivado.

NOTA: Los LED de los puertos no se reflejan en el panel anterior del dispositivo PowerConnect en el administrador del conmutador PowerConnect OpenManage. El estado de los LED sólo se puede determinar visualizando el propio dispositivo. Para obtener información sobre los LED, consulte el apartado "[Definiciones de los LED](#)".

Utilización de los botones del administrador del conmutador

En esta sección se describen los botones que se encuentran en la interfaz del administrador del conmutador OpenManage.

Botones de información

Los botones de información proporcionan acceso a la asistencia y la ayuda en línea, además de información sobre las interfaces del administrador del conmutador OpenManage.

Tabla 5-9. Botones de información

Botón	Descripción
Support (Asistencia técnica)	Abre la página Dell Support que se encuentra en support.dell.com .
Help (Ayuda)	Ayuda en línea que contiene información para ayudarle a configurar y gestionar el dispositivo. Las páginas de ayuda en línea enlazan directamente con la página que está abierta actualmente. Por ejemplo, si la página IP Addressing (Direccionamiento IP) está abierta, el tema de ayuda de esa página se abre cuando se hace clic en Help (Ayuda).
About (Acerca de)	Contiene el número de versión y compilación así como información de copyright de Dell.
Log Out (Salir)	Sale de la aplicación y cierra la ventana del explorador.

Botones de gestión del dispositivo

Los botones de gestión del dispositivo proporcionan un método sencillo para configurar la información del dispositivo, e incluyen lo siguiente:

Tabla 5-10. Botones de gestión del dispositivo

Botón	Descripción
Apply Changes (Aplicar cambios)	Aplica los cambios al dispositivo.


Add (Agregar)	Agrega información a las tablas o cuadros de diálogo.
Telnet	Inicia una sesión de Telnet
Query (Consulta)	Hace consultas en las tablas.
Show All (Mostrar todos)	Muestra las tablas de dispositivos.
Left arrow/Right arrow (Flecha izquierda/Flecha derecha)	Desplaza información entre las listas.
Refresh (Actualizar)	Actualiza la información sobre el dispositivo.
Reset All Counters (Restablecer todos los contadores)	Pone a cero los contadores de estadísticas.
Print (Imprimir)	Imprime la página Network Management System (Sistema de gestión de redes) y, o también, la información de la tabla.
Show Neighbors Info (Mostrar la información de adyacentes)	Muestra la Neighbors List (Lista de adyacentes) de la página Neighbors Table (Tabla de adyacentes).
Draw (Trazar)	Crea gráficas de estadísticas al momento.


Inicio de la aplicación

1. Abra un explorador de la web.
2. Escriba la dirección IP del dispositivo (tal como se define en la CLI) en la barra de direcciones y pulse <Intro>.

Para obtener información sobre la asignación de una dirección IP a un dispositivo, consulte el apartado "Dirección IP estática y máscara de subred".

3. Cuando se abra la ventana **Enter Network Password** (Escriba la contraseña de red), escriba un nombre de usuario y una contraseña.

 **NOTA:** El dispositivo no está configurado con una contraseña predeterminada, y se puede configurar sin introducir ninguna contraseña. Para obtener información sobre la recuperación de una contraseña perdida, consulte el apartado "Recuperación de contraseña".

 **NOTA:** Las contraseñas distinguen entre mayúsculas y minúsculas y son alfanuméricas.


4. Haga clic en **OK** (Aceptar).

Se abrirá la página principal del **Administrador del conmutador Dell PowerConnect OpenManage™**.

Acceso al dispositivo mediante la CLI


El dispositivo se puede gestionar a través de una conexión directa con el puerto de consola o a través de una conexión Telnet. Utilizar la CLI es parecido a especificar comandos en un sistema Linux. Si el acceso es a través de una conexión Telnet, asegúrese de que el dispositivo tiene una dirección IP definida y que la estación de trabajo que se utiliza para acceder al dispositivo está conectada al dispositivo antes de empezar a usar los comandos de la CLI.

Para obtener información sobre la configuración de una dirección IP inicial, consulte el apartado "Dirección IP estática y máscara de subred".

 **NOTA:** Asegúrese de que el cliente está cargado antes de utilizar la CLI.

Conexión de la consola

1. Encienda el dispositivo y espere hasta que se haya iniciado completamente.
2. Cuando aparezca la petición `console>`, escriba `enable` y pulse <Intro>.
3. Configure el dispositivo y especifique los comandos necesarios para realizar las tareas requeridas.
4. Cuando haya acabado, salga de la sesión con el comando `quit` o `exit`.

 **NOTA:** Si un usuario diferente se conecta al sistema en el modo de comando Privileged EXEC, el usuario actual se desconecta y el nuevo usuario inicia sesión.

Conexión Telnet

Telnet es un protocolo TCP/IP de emulación de terminal. Los terminales ASCII se pueden conectar de manera virtual al dispositivo local mediante una red de protocolo TCP/IP. Telnet es una alternativa a un terminal de conexión local cuando sea necesario realizar un inicio de sesión remoto.

El dispositivo admite hasta cuatro sesiones simultáneas de Telnet. Se pueden utilizar todos los comandos de la CLI en una sesión de telnet.

Para iniciar una sesión de Telnet:

1. Seleccione Inicio > Ejecutar.

Se abre la ventana **Run** (Ejecutar).

2. En la ventana **Run** (Ejecutar), escriba `Telnet <dirección IP>` en el campo **Open** (Abrir).
3. Haga clic en **OK** (Aceptar) para iniciar la sesión de Telnet.

Utilización de la CLI

En esta sección se ofrece información para utilizar la CLI.

Visión general del modo de comando

La CLI está dividida en dos modos de comando. Cada uno de los modos de comando tiene un conjunto de comandos específicos. Si se introduce un signo de interrogación en la petición de consola, se muestra una lista de los comandos disponibles para ese determinado modo de comando.

En cada modo, se utiliza un comando específico para navegar de un modo de comando a otro.

Durante el inicio de la sesión de la CLI, el modo de la CLI es el modo User EXEC o modo de ejecución de usuario. En el modo User EXEC sólo hay disponibles un subconjunto limitado de comandos. Este nivel se reserva para tareas que no cambian la configuración de la consola y se utiliza para acceder a subsistemas de configuración como la CLI. Para pasar al siguiente nivel, el modo Privileged EXEC o modo de ejecución privilegiado, es necesaria una contraseña (si está configurada).

El modo Privileged EXEC proporciona acceso a la configuración global del dispositivo. Para realizar configuraciones globales específicas dentro del dispositivo, pase al siguiente nivel, el modo Global Configuration o modo de configuración global. No es necesaria ninguna contraseña.


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

El modo Interface Configuration o modo de configuración de interfaz configura el dispositivo en el nivel de interfaz física. Los comandos de interfaz que requieren subcomandos tienen otro nivel denominado modo Subinterface Configuration o modo de configuración de subinterfaz. No es necesaria ninguna contraseña.

Modo User EXEC

Después de conectarse al dispositivo, se activa el modo de comando User EXEC. La petición de nivel de usuario está formada por el nombre del sistema principal seguido del paréntesis angular (>). Por ejemplo,

```
console>
```

 **NOTA:** El nombre del sistema principal predeterminado es console a no ser que se haya modificado durante la configuración inicial.

Los comandos User EXEC permiten conectarse con dispositivos remotos, cambiar la configuración del terminal de manera temporal, realizar pruebas básicas y

enumerar la información del sistema.

Para obtener una lista de los comandos User EXEC, introduzca un signo de interrogación en la petición de comando.

Modo Privileged EXEC

El acceso privilegiado se puede proteger para impedir el acceso no autorizado y asegurar los parámetros de funcionamiento. Las contraseñas aparecen en la pantalla con el formato ***** y distinguen entre mayúsculas y minúsculas.

Para acceder y ver una lista de los comandos del modo Privileged EXEC:

1. En la petición escriba `enable` y pulse <Intro>.
2. Cuando aparezca una petición de contraseña, introduzca la contraseña y pulse <Intro>.

La petición del modo Privileged EXEC aparece como el nombre de sistema principal del dispositivo seguido del símbolo #. Por ejemplo,

```
console#
```

Para obtener una lista de los comandos Privileged EXEC, escriba un signo de interrogación en la petición de comando y pulse <Intro>.

Para pasar del modo Privileged EXEC al modo User EXEC utilice uno de los siguientes comandos: `disable`, `exit/end` o <Ctrl><Z>.

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

```
console> enable
```

```
Enter Password: *****
```

```
console#
```

```
console# disable
```

```
console>
```

Utilice el comando `exit` para volver a un modo anterior. Por ejemplo, para pasar del modo Interface Configuration al modo Global Configuration, y del modo Global Configuration al modo Privileged EXEC.

Modo Global Configuration

Los comandos de configuración global se aplican a las características del sistema en vez de a una interfaz o protocolo específico.

Para acceder al modo Global Configuration, en la petición del modo Privileged EXEC, escriba `configure` y pulse <Intro>. El modo Global Configuration aparece como el nombre del sistema principal del dispositivo seguido de (config) y el símbolo de la almohadilla #.

```
console(config)#
```

Para obtener una lista de los comandos Global Configuration, introduzca un signo de interrogación en la petición de comando.

Para volver del modo Global Configuration al modo Privileged EXEC, escriba el comando `exit` o utilice el comando `<Ctrl><Z>`.

En el ejemplo siguiente se muestra cómo acceder al modo Global Configuration y volver al modo Privileged EXEC:

```
console#  
  
console#configure  
  
console(config)#exit  
  
console#
```

Modo Interface Configuration

Los comandos de configuración de la interfaz modifican la configuración específica de la interfaz IP, incluido el grupo de puentes, la descripción, etc.

Modo VLAN Database

El modo VLAN contiene los comandos para crear y configurar una VLAN como un todo, por ejemplo, para crear una VLAN y aplicarle una dirección IP. A continuación se muestra un ejemplo de la petición del modo VLAN:

```
Console # vlan database  
  
Console (config-vlan)#
```

Modo Port Channel

El modo Port Channel o modo de canal de puertos contiene los comandos para configurar grupos de agregación de enlaces (LAG). A continuación se muestra un ejemplo de la petición del modo Port Channel:

```
Console(config)#interface port-channel 1  
  
Console(config-if)#
```

Modo Interface

El modo Interface o modo de interfaz contiene comandos que configuran la interfaz. El comando del modo Global Configuration `interface ethernet` se utiliza para entrar en el modo de configuración de interfaz. A continuación se muestra un ejemplo de la petición del modo Interface:

```
console> enable
```

```
console# configure
```

```
console(config)# interface ethernet g18
```

```
console (config-if)#
```

Lista de acceso de administración

El modo Management Access List o modo de lista de acceso de administración contiene comandos para definir las listas de acceso de administración. El comando del modo Global Configuration management access-list se utiliza para entrar en el modo Management Access List Configuration.

En el siguiente ejemplo se muestra cómo crear una lista de acceso denominada "m1ist", configurar dos interfaces de gestión ethernet g1 y ethernet g9, y convertir la lista de acceso en la lista activa:

```
Console (config)# management access-list m1ist
```

```
Console (config-macl)# permit ethernet g1
```

```
Console (config-macl)# permit ethernet g9
```

```
Console (config-macl)# exit
```

```
Console (config)# management access-class m1ist
```

Clave pública SSH

El modo SSH Public Key o modo de clave pública SSH contiene comandos para especificar manualmente otras claves públicas SSH del dispositivo.

El comando del modo Global Configuration crypto key pubkey-chain ssh se utiliza para entrar en el modo SSH Public Key-chain Configuration.

En el siguiente ejemplo se muestra cómo entrar en el modo de configuración de cadena de clave pública SSH:

```
Console(config)# crypto key pubkey-chain ssh
```

```
Console(config-pubkey-chain)#
```

Ejemplos de la CLI

Los comandos de la CLI se proporcionan como ejemplos de configuración. Para obtener una descripción completa de los comandos de la CLI, incluidos ejemplos, consulte la publicación "CLI Reference Guide" (Guía de referencia CLI) que se incluye en el CD de documentación.

[Regresar a la página de contenido](#)


[Regresar a la página de contenido](#)

Visualización de las estadísticas

Guía del usuario del sistema Dell PowerConnect 5324

- [Visualización de tablas](#)
- [Visualización de las estadísticas de RMON](#)
- [Visualización de gráficos](#)

La página Statistics (Estadísticas) contiene información de dispositivo para la utilización de la interfaz, GVRP, Etherlike, RMON y el dispositivo. Para abrir la página Statistics (Estadísticas), haga clic en Statistics (Estadísticas) en la vista de árbol.

 **NOTA:** Los comandos de la CLI no están disponibles para todas las páginas Statistics (Estadísticas).

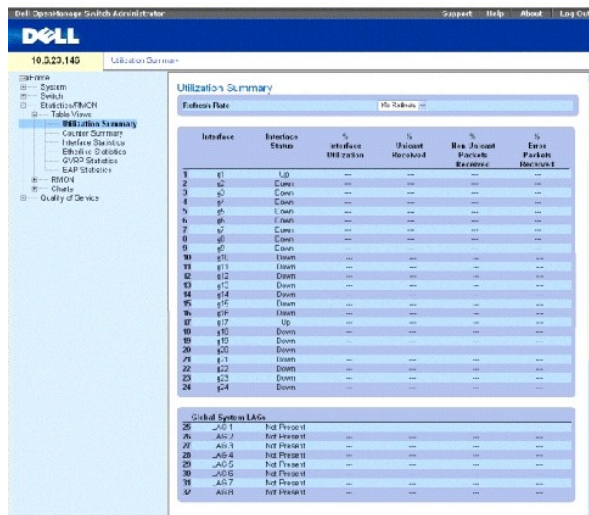
Visualización de tablas

La página Table Views (Vistas de tabla) contiene enlaces para visualizar estadísticas en un formato de gráfico. Para abrir la página, haga clic en Statistics→Table (Estadísticas → Tabla) en la vista de árbol.

Visualización del resumen de utilización

La página [Utilization Summary](#) (Resumen de utilización) contiene estadísticas para la utilización de la interfaz. Para abrir la página, haga clic en Statistics→Table Views→Utilization Summary (Estadísticas→Vistas de tabla→Resumen de utilización) en la vista de árbol.

Ilustración 8-115. Utilization Summary (Resumen de utilización)



Interface	Interface Status	% Interface Utilization	% Packet Headset	% Max. Jumbo Frames	% Error Packet Headset
1	e1	Up	---	---	---
2	e2	Down	---	---	---
3	e3	Down	---	---	---
4	e4	Down	---	---	---
5	e5	Down	---	---	---
6	e6	Down	---	---	---
7	e7	Down	---	---	---
8	e8	Down	---	---	---
9	e9	Down	---	---	---
10	e10	Down	---	---	---
11	e11	Down	---	---	---
12	e12	Down	---	---	---
13	e13	Down	---	---	---
14	e14	Down	---	---	---
15	e15	Down	---	---	---
16	e16	Down	---	---	---
17	e17	Up	---	---	---
18	e18	Down	---	---	---
19	e19	Down	---	---	---
20	e20	Down	---	---	---
21	e21	Down	---	---	---
22	e22	Down	---	---	---
23	e23	Down	---	---	---
24	e24	Down	---	---	---

Global System LAGs	LAG Status	LAG Type	LAG Mode	LAG State
25	_AG-1	Not Present	---	---
26	_AG-2	Not Present	---	---
27	_AG-3	Not Present	---	---
28	_AG-4	Not Present	---	---
29	_AG-5	Not Present	---	---
30	_AG-6	Not Present	---	---
31	_AG-7	Not Present	---	---
32	_AG-8	Not Present	---	---

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Interface (Interfaz): El número de la interfaz.

Interface Status (Estado de la interfaz): El estado de la interfaz.

% Interface Utilization (% de utilización de la interfaz): El porcentaje de utilización de la interfaz de red en función del modo dúplex de la interfaz. El rango de esta lectura está comprendido entre 0 y 200 %. La lectura máxima de 200% en una conexión de dúplex completo indica que el flujo de datos que pasa por la interfaz utiliza el 100% de la amplitud de banda de las conexiones de entrada y salida. La lectura máxima en una conexión de dúplex medio es del 100%.

% Unicast Received (% de paquetes de difusión única recibidos): El porcentaje de paquetes de difusión única recibidos en la interfaz.

% Non Unicast Packets Received (% de paquetes recibidos sin difusión única): El porcentaje de paquetes sin difusión única recibidos en la interfaz.

% Error Packets Received (% de paquetes con errores recibidos): El número de paquetes con errores recibidos en la interfaz.

Global System LAG (LAG de sistema global): El rendimiento del LAG/tronco actual.

Visualización del resumen de contador

La página [Counter Summary](#) (Resumen de contador) contiene estadísticas para la utilización del puerto en sumas numéricas en lugar de porcentajes. Para abrir la página [Counter Summary](#) (Resumen de contador), haga clic en **Statistics/RMON** → **Table Views** → **Counter Summary** (Estadísticas/RMON → Vistas de tabla → Resumen de contador) en la vista de árbol.

Ilustración 8-116. Counter Summary (Resumen de contador)

The screenshot shows the Dell OpenManage Enterprise interface. The main content area is titled "Counter Summary" and displays a table of interface statistics. The table has columns for "Port/Name", "Status", "Received Packets", "Transmit Packets", "Received Bytes", "Transmit Bytes", and "Provisioned Error". The table lists various interfaces such as Et 0, Et 1, Et 2, Et 3, Et 4, Et 5, Et 6, Et 7, Et 8, Et 9, Et 10, Et 11, Et 12, Et 13, Et 14, Et 15, Et 16, Et 17, Et 18, Et 19, Et 20, Et 21, Et 22, Et 23, Et 24, and Global System LAGs. The "Received Packets" and "Transmit Packets" columns show values for each interface, while the "Received Bytes" and "Transmit Bytes" columns show values in bytes. The "Provisioned Error" column shows the number of errors for each interface.

Port/Name	Status	Received Packets	Transmit Packets	Received Bytes	Transmit Bytes	Provisioned Error
Et 0	Up	127	257	0	1300	0
Et 1	Down	0	0	0	0	0
Et 2	Down	0	0	0	0	0
Et 3	Down	0	0	0	0	0
Et 4	Down	0	0	0	0	0
Et 5	Down	0	0	0	0	0
Et 6	Down	0	0	0	0	0
Et 7	Down	0	0	0	0	0
Et 8	Down	0	0	0	0	0
Et 9	Down	0	0	0	0	0
Et 10	Down	0	0	0	0	0
Et 11	Down	0	0	0	0	0
Et 12	Down	0	0	0	0	0
Et 13	Down	0	0	0	0	0
Et 14	Down	0	0	0	0	0
Et 15	Down	0	0	0	0	0
Et 16	Down	0	0	0	0	0
Et 17	Up	5200	6386	330 000	5	0
Et 18	Down	0	0	0	0	0
Et 19	Down	0	0	0	0	0
Et 20	Down	0	0	0	0	0
Et 21	Down	0	0	0	0	0
Et 22	Down	0	0	0	0	0
Et 23	Down	0	0	0	0	0
Et 24	Down	0	0	0	0	0
Global System LAGs						
LAG 1	Not Disrupt	0	0	0	0	0
LAG 2	Not Disrupt	0	0	0	0	0
LAG 3	Not Disrupt	0	0	0	0	0
LAG 4	Not Disrupt	0	0	0	0	0
LAG 5	Not Disrupt	0	0	0	0	0
LAG 6	Not Disrupt	0	0	0	0	0
LAG 7	Not Disrupt	0	0	0	0	0
LAG 8	Not Disrupt	0	0	0	0	0

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Interface (Interfaz): El número de la interfaz.

Interface Status (Estado de la interfaz): El estado de la interfaz.

Received Unicast Packets (Paquetes de difusión única recibidos): El número de paquetes de difusión única recibidos en la interfaz.

Received Non Unicast Packets (Paquetes recibidos sin difusión única): El número de paquetes sin difusión única recibidos en la interfaz.

Transmit Unicast Packets (Paquetes de difusión única transmitidos): Número de paquetes de difusión única transmitidos desde la interfaz.

Transmit Non Unicast Packets (Paquetes sin difusión única transmitidos): Número de paquetes sin difusión única transmitidos desde la interfaz.

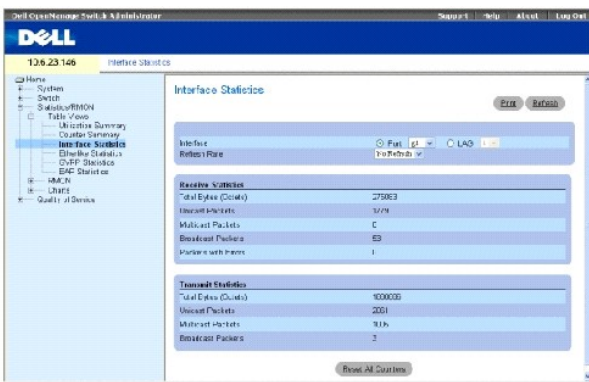
Received Errors (Errores recibidos): El número de paquetes con errores recibidos en la interfaz.

Global System LAG (LAG de sistema global): El rendimiento del LAG/tronco actual.

Visualización de las estadísticas de la interfaz

La página [Interface Statistics](#) (Estadísticas de interfaz) contiene las estadísticas de los paquetes recibidos y transmitidos. Los campos para los paquetes recibidos y transmitidos son exactamente iguales. Para abrir la página [Interface Statistics](#) (Estadísticas de interfaz), haga clic en **Statistics/RMON**→ **Table Views**→ **Interface Statistics** (Estadísticas/RMON→ Vistas de tabla→ Estadísticas de interfaz) en la vista de árbol.

Ilustración 8-117. Interface Statistics (Estadísticas de interfaz)



Interface (Interfaz): Especifica si se muestran las estadísticas para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Estadísticas de recepción

Total Bytes (Octets) (Total de bytes [octetos]): Cantidad de octetos recibidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única recibidos): El número de paquetes de difusión única recibidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): Cantidad de paquetes de multidifusión recibidos en la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): Cantidad de paquetes de difusión recibidos en la interfaz seleccionada.

Packets with Errors (Paquetes con errores): El número de paquetes con errores recibidos de la interfaz seleccionada.

Estadísticas de transmisión

Total Bytes (Octets) (Total de bytes [octetos]): Número de octetos transmitidos en la interfaz seleccionada.

Unicast Packets (Paquetes de difusión única): Número de paquetes de difusión única transmitidos en la interfaz seleccionada.

Multicast Packets (Paquetes de multidifusión): Número de paquetes de multidifusión transmitidos en la interfaz seleccionada.

Broadcast Packets (Paquetes de difusión): Número de paquetes de difusión transmitidos en la interfaz seleccionada.

Packets with Errors (Paquetes con errores): El número de paquetes con errores recibidos de la interfaz seleccionada.

Visualización de las estadísticas de interfaz

1. Abra la página [Interface Statistics](#) (Estadísticas de interfaz).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de interfaz.

Restablecimiento de los contadores de las estadísticas de la interfaz

1. Abra la página [Interface Statistics](#) (Estadísticas de interfaz).
2. Haga clic en el botón **Reset All Counters** (Restablecer todos los contadores).

Se restablecen los contadores de las estadísticas de interfaz.

Visualización de las estadísticas de la interfaz mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de la interfaz.

Tabla 8-80. Comandos de la CLI para ver las estadísticas de la interfaz

Comando de la CLI	Descripción
<code>show interfaces counters [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra la pantalla de tráfico desde el punto de vista de una interfaz física.

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

```
Console> enable
Console# show interfaces counters
```

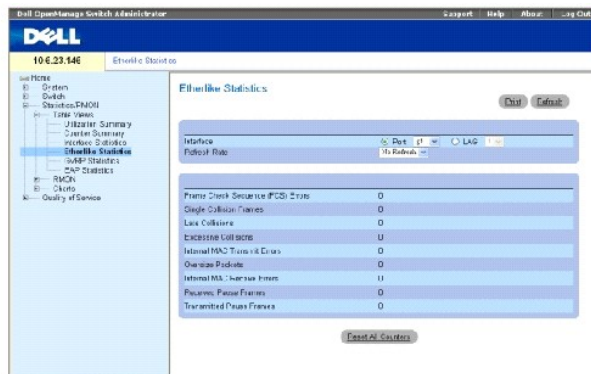
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
g1	183892	1289	987	8
g2	0	0	0	0
g3	123899	1788	373	19

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
g4	9188	9	8	0
g5	0	0	0	0
g6	8789	27	8	0
Ch	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-----	-----	-----	-----	-----
1	27889	928	0	78
Ch	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
1	23739	882	0	122

Visualización de las estadísticas de Etherlike

La página [Etherlike Statistics](#) (Estadísticas de Etherlike) contiene las estadísticas de la interfaz. Para abrir la página [Etherlike Statistics](#) (Estadísticas de Etherlike), haga clic en **Statistics/RMON**→ **Table Views**→ **Etherlike Statistics** (Estadísticas/RMON→ Vistas de tabla→ Estadísticas de Etherlike) en la vista de árbol.

Ilustración 8-118. Etherlike Statistics (Estadísticas de Etherlike)



Interface (Interfaz): Especifica si se muestran las estadísticas para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Frame Check Sequence (FCS) Errors (Errores de secuencia de comprobación de tramas [FCS]): Número de errores FCS recibidos en la interfaz seleccionada.

Single Collision Frames (Tramas de colisión única): Número de tramas de colisión única recibidas en la interfaz seleccionada.

Multiple Collision Frames (Tramas de colisión múltiple): Número de tramas de colisión múltiple recibidas en la interfaz seleccionada.

Single Quality Error (SQE) Test Errors (Errores de prueba de calidad única [SQE]): Número de errores de prueba SQE recibidos en la interfaz seleccionada.

Deferred Transmissions (Transmisiones diferidas): Número de transmisiones diferidas en la interfaz seleccionada.

Late Collisions (Colisiones tardías): Número de conexiones tardías recibidas en la interfaz seleccionada. **Excessive Collisions** (Colisiones excesivas): Número de colisiones excesivas recibidas en la interfaz seleccionada.

Internal MAC Transmit Errors (Errores de transmisión MAC internos): Número de errores de transmisión MAC internos en la interfaz seleccionada.

Carrier Sense Errors (Errores de detección de comunicación): Número de errores de detección de comunicación en la interfaz seleccionada.

Oversize Packets (Paquetes demasiado grandes): Número de errores de paquetes demasiado grandes en la interfaz seleccionada.

Internal MAC Receive Errors (Errores de recepción MAC internos): Número de errores MAC internos en la interfaz seleccionada.

Single Quality Errors (SQE) Test Errors (Errores de prueba de calidad única [SQE]): Indica el número de errores de prueba SQE recibidos en la interfaz seleccionada.

Receive Pause Frames (Tramas de pausa recibidas): Número de errores de pausa recibidos en la interfaz seleccionada.

Transmitted Paused Frames (Tramas de pausa transmitidas): Número de errores de pausa transmitidos en la interfaz seleccionada.

Visualización de las estadísticas de Etherlike para una interfaz

1. Abra la página [Etherlike Statistics](#) (Estadísticas de Etherlike).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de Etherlike de la interfaz.

Restablecimiento de las estadísticas de Etherlike

1. Abra la página [Etherlike Statistics](#) (Estadísticas de Etherlike).
2. Haga clic en el botón **Reset All Counters** (Restablecer todos los contadores).

Se restablecen las estadísticas de Etherlike.

Visualización de las estadísticas Etherlike mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de Etherlike.

Tabla 8-81. Comandos de la CLI para ver las estadísticas de Etherlike

Comando de la CLI	Descripción
<code>show interfaces counters [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra la pantalla de tráfico desde el punto de vista de una interfaz física.

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

```

Console> enable

Console# show interfaces counters ethernet g1

```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-----	-----	-----	-----	-----
g1	183892	1289	987	8

```


```

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
g1	9188	9	8	0

```


```

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0

Visualización de las estadísticas de GVRP

La página [GVRP Statistics](#) (Estadísticas de GVRP) contiene estadísticas del dispositivo de GVRP. Para abrir la página, haga clic en **Statistics/RMON**→ **Table Views**→ **GVRP Statistics** (Estadísticas/RMON→ Vistas de tabla→ Estadísticas de GVRP) en la vista de árbol.

Ilustración 8-119. GVRP Statistics (Estadísticas de interfaz)



Interface (Interfaz): Especifica si se muestran las estadísticas para un puerto o un LAG.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Join Empty (Unir vacíos): Muestra las estadísticas de Join Empty (Unir vacíos) de GVRP del dispositivo.

Empty (Vacíos): Muestra las estadísticas de Empty (Vacíos) de GVRP del dispositivo.

Leave Empty (Dejar vacío): Muestra las estadísticas de Leave Empty (Dejar vacío) de GVRP del dispositivo.

Join In (Unir): Muestra las estadísticas de Join In (Unir) de GVRP del dispositivo.

Leave In (Dejar): Muestra las estadísticas de Leave In (Dejar) de GVRP del dispositivo.

Leave All (Dejar todos): Muestra las estadísticas de Leave All (Dejar todos) de GVRP del dispositivo.

Invalid Protocol ID (ID de protocolo no válido): Estadísticas de IP de protocolo no válido GVRP del dispositivo.

Invalid Attribute Type (Tipo de atributo no válido): Estadísticas de ID de atributo no válido GVRP del dispositivo.

Invalid Attribute Value (Valor del atributo no válido): Estadísticas de valor del atributo no válido GVRP del dispositivo.

Invalid Attribute Length (Longitud de atributo no válida): Estadísticas de longitud de atributo no válida GVRP del dispositivo.

Invalid Events (Eventos no válidos): Estadísticas de eventos no válidos de GVRP del dispositivo.

Visualización de las estadísticas de GVRP para un puerto

1. Abra la página [GVRP Statistics](#) (Estadísticas de GVRP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de GVRP de la interfaz.

Restablecimiento de las estadísticas de GVRP

1. Abra la página [GVRP Statistics](#) (Estadísticas de GVRP).
2. Haga clic en el botón **Reset All Counters** (Restablecer todos los contadores).

Se restablecen los contadores de GVRP.

Visualización de las estadísticas de GVRP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de GVRP.

Tabla 8-82. Comandos de la CLI para ver las estadísticas de GVRP

Comando de la CLI	Descripción
<code>show gvrp statistics [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra las estadísticas de GVRP.
<code>show gvrp error-statistics [ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>]</code>	Muestra las estadísticas de error de GVRP.

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

```
:
Console# show gvrp statistics

GVRP statistics:
-----
rJE : Join Empty Received      rJIn : Join In Received
rEmp : Empty Received          rLIn : Leave In Received
rLE : Leave Empty Received     rLA : Leave All Received
```


sJE : Join Empty Sent						sJIn : Join In Sent						
sEmp : Empty Sent						sLIn : Leave In Sent						
sLE : Leave Empty Sent						sLA : Leave All Sent						
Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
----	----	-----	-----	-----	----	----	----	-----	-----	-----	----	----
g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

Console# show gvrp error-statistics					
GVRP error statistics:					

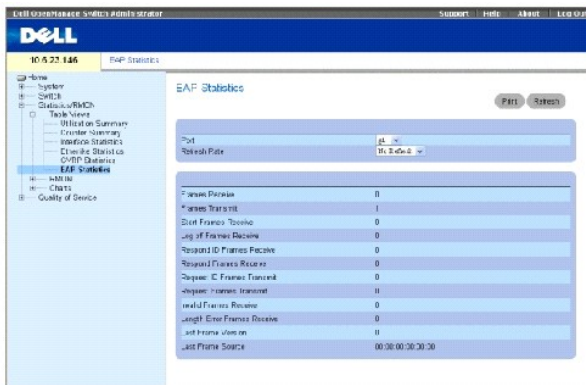
Legend:					
INVPROT : Invalid Protocol Id			INVPLEN : Invalid PDU Length		
INVATYP : Invalid Attribute Type			INVALEN : Invalid Attribute Length		
INVAVAL : Invalid Attribute Value			INVEVENT : Invalid Event		
Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT

g1	0	0	0	0	0
g2	0	0	0	0	0
g3	0	0	0	0	0
g4	0	0	0	0	0
g5	0	0	0	0	0
g6	0	0	0	0	0
g7	0	0	0	0	0
g8	0	0	0	0	0

Visualización de estadísticas de EAP

La página [EAP Statistics](#) (Estadísticas de EAP) contiene información sobre los paquetes EAP recibidos en un puerto específico. Para obtener más información sobre EAP, consulte el apartado "[Autenticación basada en puertos \(802.1x\)](#)". Para abrir la página [EAP Statistics](#) (Estadísticas de EAP), haga clic en Statistics/RMON > Table Views > EAP Statistics (Estadísticas de EAP) > Vistas de tabla > Estadísticas de EAP en la vista de árbol.

Ilustración 8-120. EAP Statistics (Estadísticas de EAP)



Port (Puerto): El puerto que se sondea para obtener las estadísticas.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas de la interfaz se actualicen.

Frames Receive (Tramas recibidas): El número de tramas de EAPOL válidas recibidas en el puerto.

Frames Transmit (Tramas transmitidas): El número de tramas EAPOL válidas transmitidas a través del puerto.

Start Frames Receive (Tramas de inicio recibidas): El número de tramas de EAPOL de inicio recibidas en el puerto.

Log off Frames Receive (Tramas de cierre de sesión recibidas): El número de tramas de cierre de sesión de EAPOL que se han recibido en el puerto.

Respond ID Frames Receive (Tramas de ID de respuesta recibidas): El número de tramas de respuesta/ID de EAPOL que se han recibido en el puerto.

Respond Frames Receive (Tramas de respuesta recibidas): El número de tramas de respuesta de EAP válidas recibidas en el puerto.

Request ID Frames Transmit (Tramas de ID de solicitud transmitidas): El número de tramas de ID de solicitud de EAP transmitidas a través del puerto.

Request Frames Transmit (Tramas de solicitud transmitidas): El número de tramas de solicitud de EAP transmitidas a través del puerto.

Invalid Frames Receive (Tramas no válidas no recibidas): El número de tramas de EAPOL no reconocidas recibidas en este puerto.

Length Error Frames Receive (Tramas con longitud errónea recibidas): El número de tramas de EAPOL con una longitud de cuerpo de paquete no válida recibidas en este puerto.

Last Frame Version (Versión de la última trama): El número de versión del protocolo que va unido a la trama de EAPOL que se haya recibido más recientemente.

Last Frame Source (Origen de la última trama): La dirección MAC de origen que va unida a la trama de EAPOL que se haya recibido más recientemente.

Visualización de las estadísticas de EAP para un puerto

1. Abra la página [EAP Statistics](#) (Estadísticas de EAP).
2. Seleccione una interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de EAP de la interfaz.

Restablecimiento de las estadísticas de EAP

1. Abra la página [EAP Statistics](#) (Estadísticas de EAP).
2. Haga clic en Reset All Counters (Restablecer todos los contadores) para restablecer el contador.

Se restablecen las estadísticas de EAP.

Visualización de las estadísticas de EAP mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de EAP.

Tabla 8-83. Comandos de la CLI para ver las estadísticas de EAP

Comando de la CLI	Descripción
<code>show dot1x statistics ethernet <i>interfaz</i></code>	Muestra las estadísticas 802.1X de la interfaz especificada.

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

```
Switch# show dot1x statistics ethernet gl
```

```
EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

Visualización de las estadísticas de RMON

La supervisión remota (RMON) contiene vínculos para ver información de red desde una ubicación remota. Para abrir la página **RMON**, haga clic en **Statistics/RMON** → **RMON**(Estadísticas/RMON → RMON) en la vista de árbol.

Visualización del grupo de estadísticas de RMON

La página [RMON Statistics](#) (Estadísticas de RMON) contiene campos para ver información sobre la utilización del dispositivo y los errores producidos en el mismo. Para abrir la página [RMON Statistics](#) (Estadísticas de RMON), haga clic en **Statistics/RMON** → **RMON** → **Statistics** (Estadísticas/RMON → RMON → Estadísticas), en la vista de árbol.

Ilustración 8-121. RMON Statistics (Estadísticas de RMON)

RMON Statistics	
Interface	0/10/0/0
Refresh Rate	10 Seconds
Drop Events	0
Received Bytes (Octets)	27751
Received Packets	1318
Broadcast Packets Received	65
Multicast Packets Received	0
CRC/Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	11
Frames of 64 Bytes	1159
Frames of 65 to 127 Bytes	361
Frames of 128 to 255 Bytes	24
Frames of 256 to 511 Bytes	11
Frames of 512 to 1023 Bytes	230
Frames of 1024 to 1518 Bytes	0

Interface (Interfaz): Especifica el puerto o LAG para el que se muestran las estadísticas.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas se actualicen.

Drop Events (Eventos descartados): Número de eventos descartados que se han producido en la interfaz desde que se actualizó por última vez el dispositivo.

Received Bytes (Octets) (Bytes recibidos [octetos]): Número de octetos recibidos en la interfaz desde que se actualizó por última vez el dispositivo. Este número incluye paquetes erróneos y octetos FCS, pero excluye los bits de la trama.

Received Packets (Paquetes recibidos): Número de paquetes recibidos en la interfaz, incluidos los paquetes erróneos y los paquetes de difusión, desde que se actualizó por última vez el dispositivo.

Broadcast Packets Received (Paquetes de difusión recibidos): Número de paquetes de difusión correctos recibidos en la interfaz desde que se actualizó por última vez el dispositivo. Este número no incluye los paquetes de multidifusión.

Multicast Packets Received (Paquetes de multidifusión recibidos): Número de paquetes de multidifusión correctos recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

CRC & Align Errors (Errores de alineación y de CRC): Número de errores de alineación y de CRC que se han producido en la interfaz desde que se actualizó por última vez el dispositivo.

Undersize Packets (Paquetes demasiado pequeños): Número de paquetes demasiado pequeños (inferiores a los 64 octetos) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Oversize Packets (Paquetes demasiado grandes): Número de paquetes demasiado grandes (superiores a los 1.518 octetos) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Fragments (Fragmentos): Número de fragmentos (paquetes de menos de 64 octetos, excluidos los bits de trama e incluidos los octetos FCS) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Jabbers: Número de jabbers (paquetes de más de 1.518 octetos) recibidos en la interfaz desde que se actualizó por última vez el dispositivo.

Collisions (Colisiones): Número de colisiones recibidas en la interfaz desde que se actualizó por última vez el dispositivo.

Frames of xx Bytes (Tramas de xx bytes): Número de tramas de xx bytes recibidas en la interfaz desde que se actualizó por última vez el dispositivo.

Visualización de las estadísticas de la interfaz

1. Abra la página [RMON Statistics](#) (Estadísticas de RMON).
2. Seleccione un tipo y un número de interfaz en el campo **Interface** (Interfaz).

Se visualizan las estadísticas de interfaz.

Visualización de las estadísticas de RMON mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de RMON.

Tabla 8-84. Comandos de la CLI para ver las estadísticas de RMON

Comando de la CLI	Descripción
<code>show rmon statistics {ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>}</code>	Muestra las estadísticas de Ethernet de RMON.

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

```
console> enable
```

```
console> enable

Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

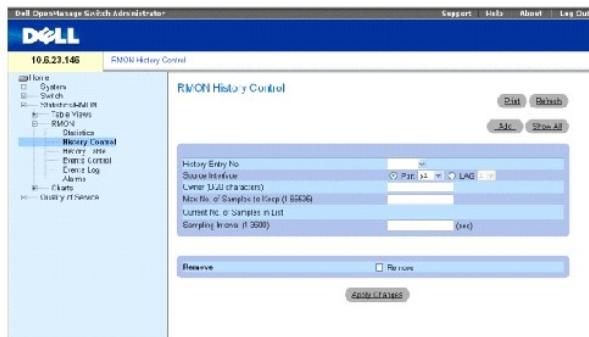
128 to 255 Octets: 0 256 to 511 Octets: 0
```

512 to 1023 Octets: 491 1024 to 1518 Octets: 389

Visualización de estadísticas del control del historial de RMON

La página [RMON History Control](#) (Control del historial de RMON) contiene información acerca de muestras de datos obtenidos desde los puertos. Por ejemplo, las muestras pueden incluir definiciones de interfaz o periodos de encuesta. Para abrir la página [RMON History Control](#) (Control del historial de RMON), haga clic en **Statistics/RMON→ History Control** (Estadísticas/RMON→ Control del historial) en la vista de árbol.

Ilustración 8-122. RMON History Control (Control del historial de RMON)



History Entry No. (Nº de entrada del historial): Número de entrada para la página **History Control Table** (Tabla de control del historial).

Source Interface (Interfaz de origen): El puerto o LAG desde los que se han obtenido las muestras del historial.

Owner (0-20 characters) (Propietario [0-20 caracteres]): La estación de RMON o usuario que ha solicitado la información de RMON.

Max No. of Samples to Keep (1-65535) (Número máximo de muestras que se deben conservar [1-65535]): Número de muestras que se van a guardar. El valor predeterminado es 50.

Current No. of Samples in List (Número actual de muestras en la lista): Indica el número actual de muestras obtenidas.

Sampling Interval (1-3600) (Intervalo de muestreo [1-3600]): Indica el tiempo, transcurrido en segundos, que se tarda en obtener los muestreos desde los puertos. Los valores posibles están comprendidos entre 1 y 3.600 segundos. El valor predeterminado es 1800 segundos (30 minutos).

Remove (Eliminar): Si se selecciona esta opción, se elimina la entrada **History Control Table** (Tabla de control del historial).

Adición de una entrada de control del historial

1. Abra la página [RMON History Control](#) (Control del historial de RMON).
2. Haga clic en **Add** (Agregar).

La página **Add History Entry** (Agregar entrada del historial) se abrirá.

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

La entrada se agrega a la **History Control Table** (Tabla de control del historial).

Modificación de una entrada de la tabla de control del historial

1. Abra la página [RMON History Control](#) (Control del historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).
3. Modifique los campos según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

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

Supresión de una entrada de la tabla de control del historial

1. Abra la página [RMON History Control](#) (Control del historial de RMON).
2. Seleccione una entrada en el campo **History Entry No.** (Nº de entrada del historial).
3. Pulse en **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada seleccionada de la tabla se borrará y el dispositivo se actualizará.

Visualización del control del historial de RMON mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas de GVRP.

Tabla 8-85. Comandos de la CLI para ver el historial de RMON

Comando de la CLI	Descripción
<code>rmon collection history índice [owner nombrepropietario buckets número-bucket] [interval segundos]</code>	Activa y configura RMON en una interfaz.
<code>show rmon collection history [ethernet interfaz port-channel número-canal-puerto]</code>	Muestra las estadísticas del historial de recopilación de RMON.

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

```
Console(config)# interface ethernet g8

Console (config-if)# rmon collection history 1 interval 2400

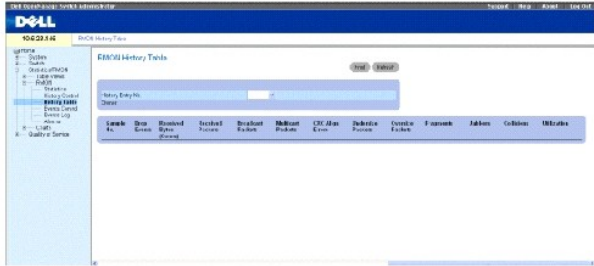
Console (config-if)# exit

Console(config)#exit
```

Visualización de la tabla del historial de RMON

La tabla [RMON History Table](#) (Tabla del historial de RMON) contiene muestreos estadísticos de red específicos de la interfaz. Cada entrada de la tabla representa a todos los valores del contador compilados durante una única muestra. Para abrir la tabla [RMON History Table](#) (Tabla del historial de RMON), haga clic en **Statistics/RMON→RMON→History Table** (Estadísticas/RMON→RMON→Tabla del historial) en la vista de árbol.

Ilustración 8-123. RMON History Table (Tabla del historial de RMON)



Sample No. (Nº de muestra): Indica la muestra específica que refleja la información de la tabla.

Drop Events (Eventos descartados): El número de paquetes descartados debido a la falta de recursos de red durante el intervalo de muestreo. Es posible que no represente la cantidad exacta de paquetes descartados, en cambio se ha detectado el número de veces que se han descartado paquetes.

Received Bytes (Octets) (Bytes recibidos [octetos]): El número de octetos de datos, incluidos los paquetes erróneos, recibidos en la red.

Received Packets (Paquetes recibidos): El número de paquetes recibidos durante el intervalo de muestreo.

Broadcast Packets (Paquetes de difusión): El número de paquetes de difusión correctos recibidos durante el intervalo de muestreo.

Multicast Packets (Paquetes de multidifusión): El número de paquetes de multidifusión correctos recibidos durante el intervalo de muestreo.

CRC Align Errors (Errores de alineación de CRC): El número de paquetes recibidos durante la sesión de muestreo con una longitud de 64-1518 octetos, una secuencia de comprobación de tramas (FCS) y con un número entero de octetos, o una FCS errónea con un número no integral de octetos.

Undersize Packets (Paquetes demasiado pequeños): El número de paquetes recibidos de menos de 64 octetos de longitud durante la sesión de muestreo.

Oversize Packets (Paquetes demasiado grandes): El número de paquetes recibidos de más de 1.518 octetos de longitud durante la sesión de muestreo.

Fragments (Fragmentos): El número de paquetes recibidos de menos de 64 octetos de longitud y que han tenido una FCS durante la sesión de muestreo.

Jabbers: El número de paquetes recibidos de más de 1.518 octetos de longitud y que han tenido una FCS durante la sesión de muestreo.

Collisions (Colisiones): Realiza una estimación del número total de colisiones de paquetes producidas durante la sesión de muestreo. Las colisiones se detectan cuando los puertos repetidores detectan dos o más estaciones que transmiten simultáneamente.

Utilization (Utilización): Realiza una estimación de la utilización de la red del nivel físico principal en una interfaz durante la sesión de muestreo. El valor se refleja en porcentajes con dos decimales.

Visualización de las estadísticas para una entrada específica del historial

1. Abra la página [RMON History Table](#) (Tabla del historial de RMON).
2. Seleccione una entrada en el campo **History Table No.** (Nº de entrada del historial).

Las estadísticas de entrada se muestran en la RMON History Table (Tabla del historial de RMON).

Visualización del control del historial de RMON mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver el historial de RMON.

Tabla 8-86. Comandos de la CLI para ver el control del historial de RMON

Comando de la CLI	Descripción
<code>show rmon history index { throughput errors other } [period segundos]</code>	Muestra el historial de las estadísticas de Ethernet de RMON.

A continuación se muestra un ejemplo de los comandos de la CLI para visualizar las estadísticas de Ethernet de RMON sobre la producción en el índice 1:.

```

console> enable

Console# show rmon history 1 throughput

```

: 1		Owner: CLI			
Interface: gl		Interval: 1800			
Requested samples: 50		Granted samples: 50			
Maximum table size: 500					
Time	Octets	Packets	Broadcast	Multicast	%
-----	-----	-----	-----	-----	-----
Jan 18 2004 21:57:00	303595962	357568	3289	7287	19.98%
Jan 18 2004 21:57:30	287696304	275686	2789	2789	20.17%

Definición de los eventos de RMON del dispositivo

La página [RMON Events Control](#) (Control de eventos de RMON) contiene campos para definir eventos de RMON. Para abrir la página [RMON Events Control](#) (Control de eventos de RMON), haga clic en **Statistics/RMON→ RMON→ Events Control** (Estadísticas/RMON→ RMON Control de eventos) en la vista de árbol.

Ilustración 8-124. RMON Events Control (Control de eventos de RMON)



Event Entry (Entrada de eventos): El evento.

Community (Comunidad): Comunidad a la que pertenece el evento.

Description (Descripción): La descripción del evento definido por el usuario.

Type (Tipo): Describe el tipo de evento. Los valores posibles son:

Log (Registro): El tipo de evento es una entrada de registro.

Trap (Captura): El tipo de evento es una captura.

Log and Trap (Registro y captura): El tipo de evento es una entrada de registro y una captura.

None (Ninguno): No hay ningún evento.

Time (Hora): Hora en que se produjo el evento. Por ejemplo, la fecha 29 de marzo de 2004, a las 11:00 de la mañana se visualiza como 29/03/2004 11:00:00.

Owner (Propietario): El dispositivo o usuario que ha definido el evento.

Remove (Eliminar): Si se selecciona esta opción, se elimina el evento de la tabla de eventos de RMON.

Adición de un evento de RMON

1. Abra la página [RMON Events Control](#) (Control de eventos de RMON).
2. Haga clic en **Add** (Agregar).

La página **Add an Event Entry** (Agregar una entrada de evento) se abrirá.

3. Complete la información en el cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

La entrada **Event Table** (Tabla de eventos) se agrega y el dispositivo se actualiza.

Modificación de un evento de RMON

1. Abra la página [RMON Events Control](#) (Control de eventos de RMON).

2. Seleccione una entrada de la **Event Table** (Tabla de eventos).
3. Modifique los campos del cuadro de diálogo y haga clic en **Apply Changes** (Aplicar cambios).

La entrada **Event Table** (Tabla de eventos) se modifica y el dispositivo se actualiza.


Supresión de las entradas de eventos de RMON

1. Abra la página [RMON Events Control](#) (Control de eventos de RMON).
2. Haga clic en **Show All** (Mostrar todo).

La página **Events Table** (Tabla de eventos) se abrirá.

3. Seleccione **Remove** (Eliminar) para eliminar los eventos que desee y, a continuación, haga clic en **Apply Changes** (Aplicar cambios).

La entrada seleccionada de la tabla se borrará y el dispositivo se actualizará.

 **NOTA:** Se puede eliminar una única entrada de evento desde la página **RMON Events Control** (Control de eventos de RMON) seleccionando la casilla de verificación **Remove** (Eliminar) de la página.

Definición de los eventos del dispositivo mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir eventos del dispositivo.

Tabla 8-87. Comandos de la CLI para ver la definición de los eventos del dispositivo

Comando de la CLI	Descripción
<code>rmon event tipo indice [community texto] [description texto] [owner nombre]</code>	Configura los eventos de RMON.
<code>show rmon events</code>	Muestra la tabla de eventos de RMON.

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

```

console> enable

console# config

console (config)# rmon event 1 log

console(config)# exit

Console# show rmon events

```

Index	Description	Type	Community	Owner	Last time sent
-----	-----	-----	-----	-----	-----
1	Errors	Log		CLI	Jan 18 2002 23:58:17

Visualización de la tabla del registro de eventos de RMON

La página [RMON Events Log](#) (Registro de eventos de RMON) contiene una lista de eventos de RMON. Para abrir la página [RMON Events Log](#) (Registro de eventos de RMON), haga clic en **Statistics/RMON→RMON→Events** (Estadísticas/RMON→RMON Eventos) en la vista de árbol.

Ilustración 8-125. RMON Events Log (Registro de eventos de RMON)



Event (Evento): El número de entrada de RMON Events Log (Registro de eventos de RMON).

Log No. (Nº de registro): El número de registro.

Log Time (Tiempo de registro): Hora en la que se ha especificado la entrada del registro.

Description (Descripción): Describe la entrada del registro.

Definición de los eventos del dispositivo mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir eventos del dispositivo.

Tabla 8-88. Comandos de la CLI para ver la definición de los eventos del dispositivo

Comando de la CLI	Descripción
<code>show rmon log [evento]</code>	Muestra la tabla de registros de RMON.

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

```

console> enable

console# config

console (config)# rmon event 1 log

```

```
console(config)# exit
```

```
Console# show rmon log
```

```
Maximum table size: 500
```

Event	Description	Time
-----	-----	-----
1	Errors	Jan 18 2002 23:48:19
1	Errors	Jan 18 2002 23:58:17
2	High Broadcast	Jan 18 2002 23:59:48

```
Console# show rmon log
```

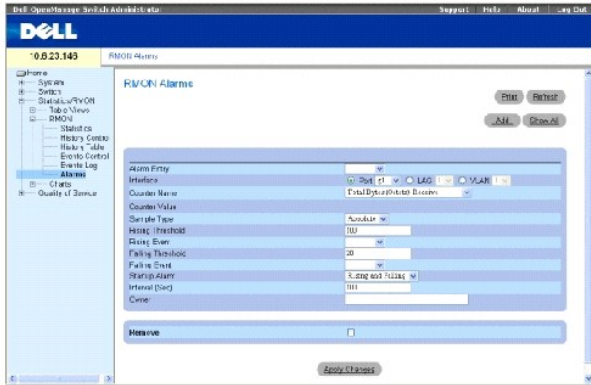
```
Maximum table size: 500 (800 after reset)
```

Event	Description	Time
-----	-----	-----
1	Errors	Jan 18 2002 23:48:19
1	Errors	Jan 18 2002 23:58:17
2	High Broadcast	Jan 18 2002 23:59:48

Definición de alarmas del dispositivo de RMON

La página [RMON Alarms](#) (Alarmas de RMON) contiene campos para establecer alarmas de red. Las alarmas de la red se activan cuando se detecta un problema en la red o un evento. Los umbrales superiores e inferiores generan eventos. Para abrir la página [RMON Alarms](#) (Alarmas de RMON), haga clic en [Statistics/RMON](#) → [RMON](#) → [Alarms](#) (Estadísticas/RMON → RMON → Alarmas) en la vista de árbol.

Ilustración 8-126. RMON Alarms (Alarmas de RMON)



Alarm Entry (Entrada de alarma): Indica una alarma específica.

Interface (Interfaz): La interfaz para la que se muestran las estadísticas de RMON.

Counter Name (Nombre del contador): La variable MIB seleccionada.

Counter Value (Valor del contador): El valor de la variable MIB seleccionada.

Sample Type (Tipo de muestra): Especifica el método de muestreo para la variable seleccionada y compara el valor con los umbrales. Los valores de campo posibles son:

Delta (Delta): Resta el último valor muestreado del valor actual. La diferencia de los valores se compara con el umbral.

Absolute (Absoluto): Compara los valores directamente con los umbrales al finalizar el intervalo de muestreo.

Rising Threshold (Umbral superior): El valor del contador superior que activa la alarma del umbral superior. El umbral superior aparece en la parte superior de las barras de gráficos. Se asigna un color a cada una de las variables supervisadas.

Rising /Falling Event (Evento superior/inferior): El mecanismo que notifica las alarmas (LOG [registro], TRAP [captura] o una combinación de ambas). Cuando se selecciona LOG (registro), no hay ningún mecanismo de almacenamiento en el dispositivo ni en el sistema de administración. Sin embargo, si el dispositivo no se restablece, permanece en la tabla de registros del dispositivo. Si TRAP (captura) se selecciona, se genera una captura SNMP y se notifica a través del mecanismo general de la captura. La captura se puede guardar con el mismo mecanismo.

Falling Threshold (Umbral inferior): El umbral inferior aparece gráficamente en la parte inferior de las barras de gráficos. El umbral inferior aparece gráficamente en la parte inferior de las barras de gráficos. Se asigna un color a cada una de las variables supervisadas.

Startup Alarm (Alarma de inicio): El activador que hace funcionar la alarma. El umbral superior se define cuando se atraviesa el umbral desde uno con un valor bajo hasta un umbral con un valor más alto.

Interval (sec) (Intervalo [s.]): El intervalo de tiempo entre las alarmas.

Owner (Propietario): El dispositivo o usuario que ha definido la alarma.

Remove (Eliminar): Si se selecciona esta opción, se elimina una alarma de RMON.

Adición de una entrada de la tabla de alarmas

1. Abra la página RMON Alarms (Alarmas de RMON).
2. Haga clic en **Add** (Agregar).

La página **Add an Alarm Entry** (Agregar una entrada de alarma) se abrirá.

Ilustración 8-127. Página **Add an Alarm Entry** (Agregar una entrada de alarma)

Alarm Entry	1
Interface	Part 9 LAG VLAN
Counter Name	Total Bytes (Clerk) Perceive
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100
Overcr	

3. Seleccione una interfaz.
4. Complete los campos del cuadro de diálogo.
5. Haga clic en **Apply Changes** (Aplicar cambios).

La alarma de RMON se agrega y el dispositivo se actualiza.

Modificación de una entrada de la tabla de alarmas

1. Abra la página [RMON Alarms](#) (Alarmas de RMON).
2. Seleccione una entrada en el menú descendente **Alarm Entry** (Entrada de alarma).
3. Modifique los campos del diálogo según convenga.
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada se modifica y el dispositivo se actualiza.

Visualización de la tabla de alarmas

1. Abra la página [RMON Alarms](#) (Alarmas de RMON).
2. Haga clic en **Show All** (Mostrar todo).

La página **Alarms Table** (Tabla de alarmas) se abrirá.

Supresión de una entrada de la tabla de alarmas

1. Abra la página [RMON Alarms](#) (Alarmas de RMON).
2. Seleccione una entrada en el menú descendente **Alarm Entry** (Entrada de alarma).
3. Seleccione la casilla de verificación **Remove** (Eliminar).
4. Haga clic en **Apply Changes** (Aplicar cambios).

La entrada seleccionada se suprimirá y el dispositivo se actualizará.

Definición de las alarmas del dispositivo mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para definir alarmas del dispositivo.

Tabla 8-89. Comandos de la CLI para ver las alarmas del dispositivo

Comando de la CLI	Descripción
<code>rmon alarm índice variable intervalo umbral_sup umbral_inf evento_sup evento_inf [tipo tipo] [startup dirección] [owner nombre]</code>	Configura las condiciones de alarma de RMON.
<code>show rmon alarm-table</code>	Muestra el resumen de la tabla de alarmas.
<code>show rmon alarm</code>	Muestra la configuración de las alarmas de RMON.

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

```

console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table

```

Index	OID	Owner
-----	-----	-----
1	1.3.6.1.2.1.2.2.1.1 0.1	CLI
2	1.3.6.1.2.1.2.2.1.1 0.1	Manager
3	1.3.6.1.2.1.2.2.1.1 0.9	CLI

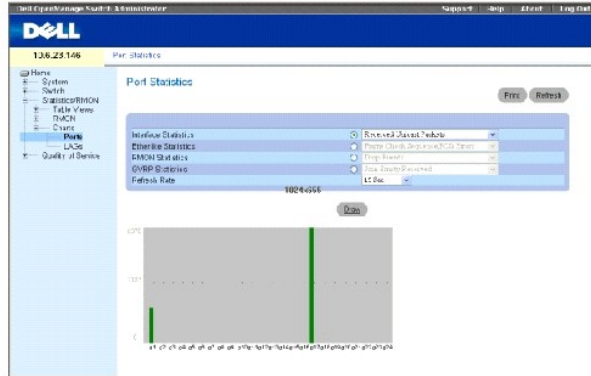
Visualización de gráficos

La página [Charts](#) (Gráficos) contiene enlaces para mostrar estadísticas en formato de gráfico. Para abrir la página, haga clic en [Statistics](#)→ [Charts](#) (Estadísticas→ Gráficos) en la vista de árbol.

Visualización de las estadísticas del puerto

La página [Port Statistics](#) (Estadísticas de puerto) contiene campos para abrir estadísticas en formato de gráfico para los elementos de un puerto. Para abrir la página [Port Statistics](#) (Estadísticas de puerto), haga clic en [Statistics](#)→ [Charts](#)→ [Ports](#) (Estadísticas→ Gráficos→ Puertos) en la vista de árbol.

Ilustración 8-128. Port Statistics (Estadísticas de puerto)



Interface Statistics (Estadísticas de interfaz): Selecciona el tipo de estadísticas de interfaz que se debe abrir.

Etherlike Statistics (Estadísticas de Etherlike): Selecciona el tipo de estadísticas de Etherlike que se va a abrir.

RMON Statistics (Estadísticas de RMON): Selecciona el tipo de estadísticas de RMON que se va a abrir.

GVRP Statistics (Estadísticas de GVRP): Selecciona el tipo de estadísticas de GVRP que se va a abrir.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas se actualicen.

Visualización de las estadísticas de puerto

1. Abra la página [Port Statistics](#) (Estadísticas de puerto).
2. Seleccione el tipo de estadísticas que se debe abrir.
3. Seleccione la frecuencia de actualización deseada en el menú descendente Refresh Rate (Frecuencia de actualización).
4. Haga clic en Draw (Dibujar).

Se muestra el gráfico de la estadística seleccionada.

Visualización de las estadísticas de puerto mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas del puerto.

Tabla 8-90. Comandos de la CLI para ver las estadísticas de puerto

Comando de la CLI	Descripción
<code>show interfaces counters {ethernet interfaz port-channel número-canal-puerto}</code>	Muestra la pantalla de tráfico desde el punto de vista de una interfaz física.
<code>show rmon statistics {ethernet interfaz port-channel número-canal-puerto}</code>	Muestra las estadísticas de Ethernet de RMON.
<code>show gvrp statistics {ethernet interfaz port-channel número-canal-puerto}</code>	Muestra las estadísticas de GVRP.
<code>show gvrp error-statistics {ethernet interfaz port-channel número-canal-puerto}</code>	Muestra las estadísticas de error de GVRP.

```
Console# show interfaces description ethernet g1
```

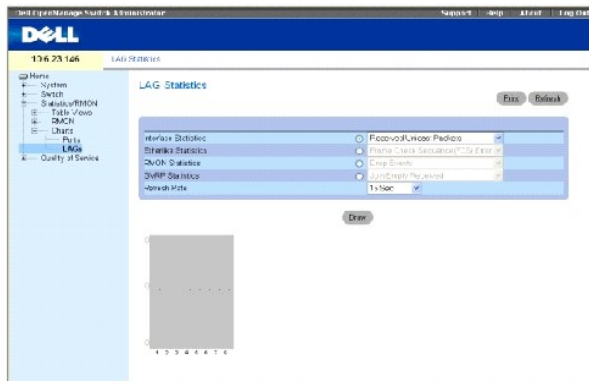
Port	Description

g1	Management_port
g2	R&D_port
g3	Finance_port
Ch	Description
1	Output

Visualización de las estadísticas de LAG

La página [LAG Statistics](#) (Estadísticas de LAG) contiene campos para abrir estadísticas en formato de gráfico para los LAG. Para abrir la página [LAG Statistics](#) (Estadísticas de LAG), haga clic en **Statistics**→ **Charts**→ **LAGs** (Estadísticas→ Gráficos→ LAG) en la vista de árbol.

Ilustración 8-129. LAG Statistics (Estadísticas de LAG)



Interface Statistics (Estadísticas de interfaz): Selecciona el tipo de estadísticas de interfaz que se debe abrir.

Etherlike Statistics (Estadísticas de Etherlike): Selecciona el tipo de estadísticas de Etherlike que se va a abrir.

RMON Statistics (Estadísticas de RMON): Selecciona el tipo de estadísticas de RMON que se va a abrir.

GVRP Statistics (Estadísticas de GVRP): Selecciona el tipo de estadísticas de GVRP que se va a abrir.

Refresh Rate (Frecuencia de actualización): Tiempo que transcurre antes de que las estadísticas se actualicen.

Visualización de las estadísticas de LAG

1. Abra la página [LAG Statistics](#) (Estadísticas de LAG).
2. Seleccione el tipo de estadísticas que se debe abrir.

3. Seleccione la frecuencia de actualización deseada en el menú descendente **Refresh Rate** (Frecuencia de actualización).
4. Haga clic en **Draw** (Dibujar).

Se muestra el gráfico de la estadística seleccionada.

Visualización de las estadísticas de LAG mediante los comandos de la CLI

En la siguiente tabla se muestra un resumen de los comandos de la CLI equivalentes para ver las estadísticas del LAG.

Tabla 8-91. Comandos de la CLI para ver las estadísticas de LAG

Comando de la CLI	Descripción
<code>show interfaces counters {ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>}</code>	Muestra la pantalla de tráfico desde el punto de vista de una interfaz física.
<code>show rmon statistics {ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>}</code>	Muestra las estadísticas de Ethernet de RMON.
<code>show gvrp statistics {ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>}</code>	Muestra las estadísticas de GVRP.
<code>show gvrp error-statistics {ethernet <i>interfaz</i> port-channel <i>número-canal-puerto</i>}</code>	Muestra las estadísticas de error de GVRP.

```

Console# show gvrp statistics
-----
GVRP statistics:
-----
rJE : Join Empty Received      rJIn : Join In Received
rEmp : Empty Received          rLIn : Leave In Received
rLE : Leave Empty Received     rLA : Leave All Received
sJE : Join Empty Sent          sJIn : Join In Sent
sEmp : Empty Sent              sLIn : Leave In Sent
sLE : Leave Empty Sent         sLA : Leave All Sent
-----
Port  rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp  sLIn  sLE  sLA
-----
g1    0    0    0    0    0    0    0    0    0    0    0    0
g2    0    0    0    0    0    0    0    0    0    0    0    0

```

g3	0	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0	0

[Regresar a la página de contenido](#)