Configuración y verificación de BFD en switches Nexus 9000

Contenido

Introducción

Este documento describe cómo configurar y verificar las sesiones de detección de reenvío bidireccional (BFD) en los switches basados en Cisco Nexus NXOS®.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Detección de reenvío bidireccional (BFD)
- Software Nexus NX-OS.

- Protocolos de routing: ruta de acceso más corta primero (OSPF), protocolo de gateway fronterizo (BGP) y protocolo de routing de gateway interior mejorado (EIGRP).

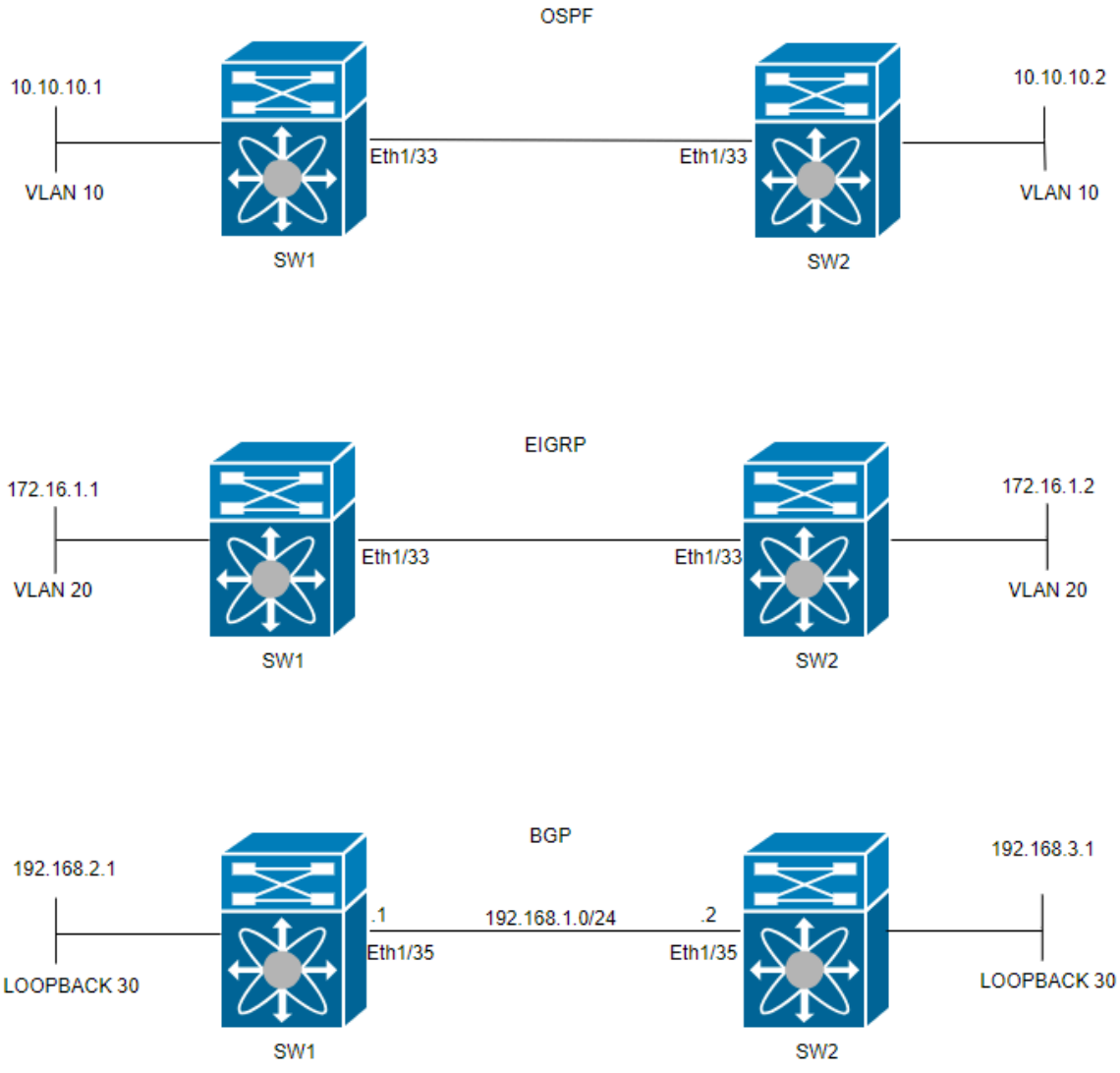
Componentes Utilizados

La información de este documento se basa en Cisco Nexus 9000 con NXOS versión 10.3(4a).M.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configurar

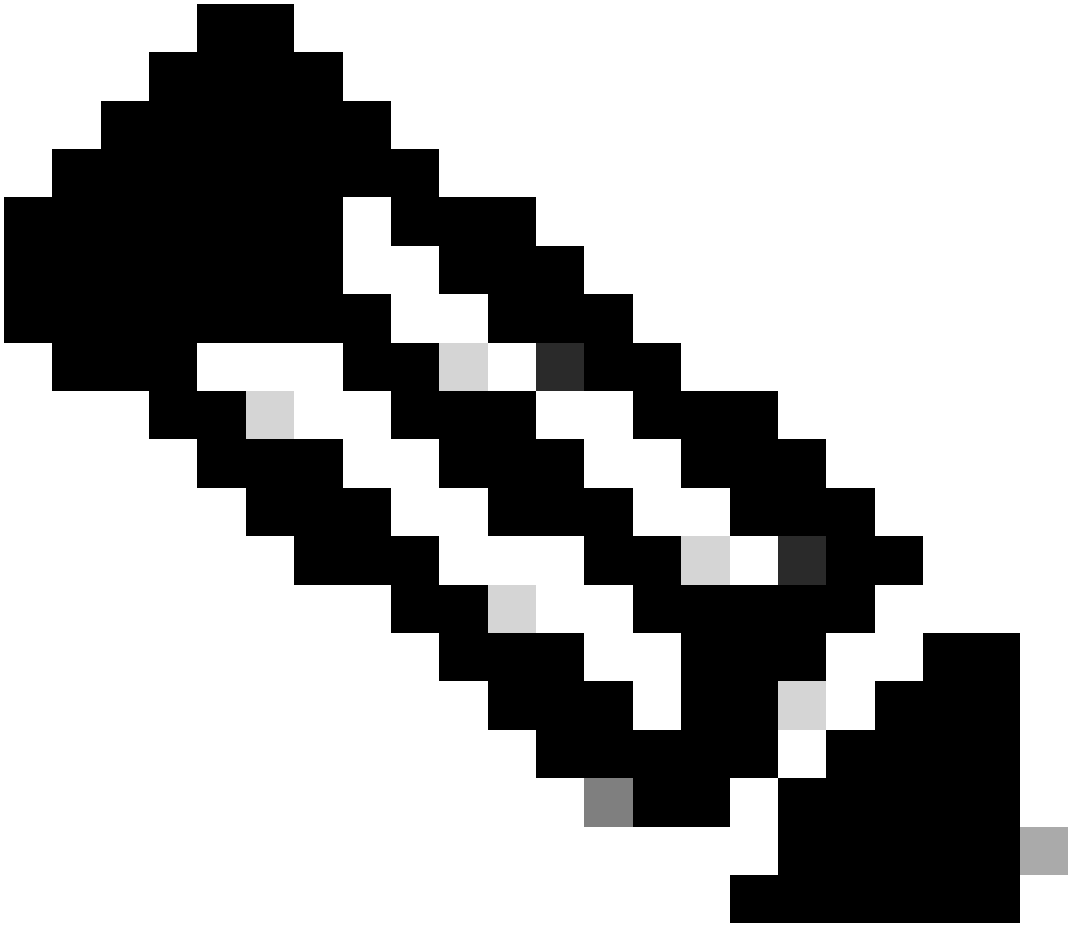
El propósito de configurar BFD es detectar y comprender las diferencias entre las configuraciones de varios protocolos de ruteo.

PASO 1: Debe habilitar la función BFD antes de poder configurar BFD en una interfaz y protocolo.

SWITCH 1	SWITCH 2
SW1(config)# feature bfd	SW2(config)# feature bfd

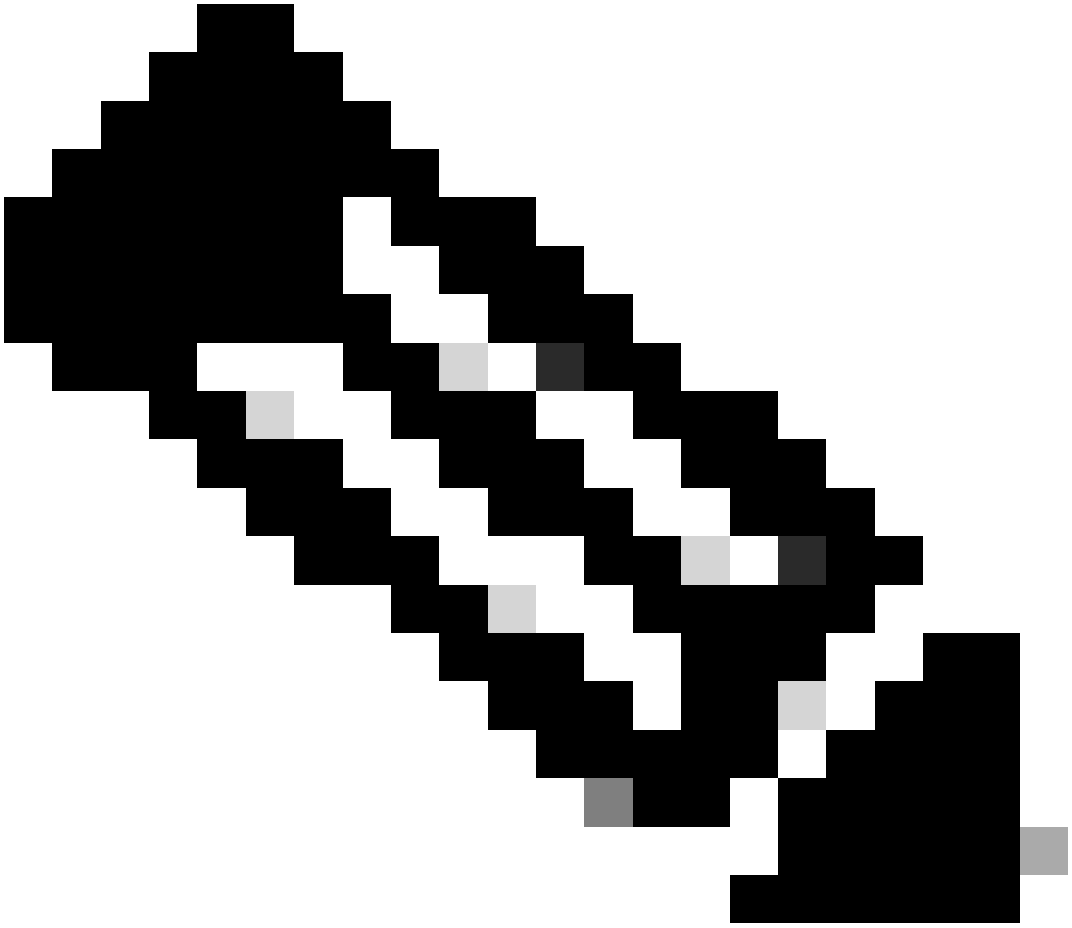
PASO 2: Configuración de Global BFD

SWITCH 1	SWITCH 2
SW1(config)# bfd interval 500 min_rx 500 multiplier 3	**SW2(config)# bfd interval 500 min_rx 500 multiplie**

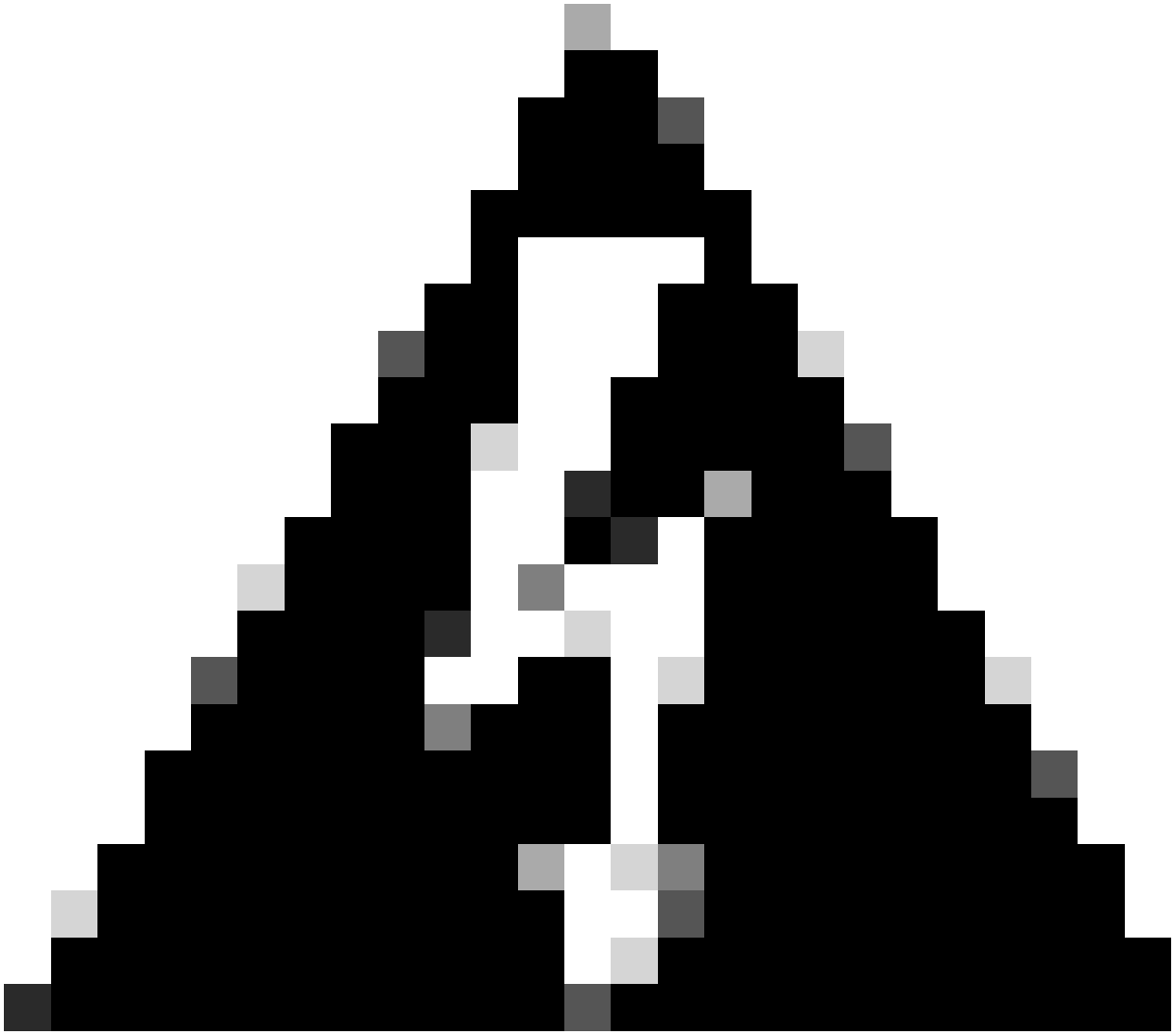


Nota: El rango min_tx y msec es de 50 a 999 milisegundos y el valor predeterminado es 50. El rango del multiplicador es de 1 a 50. El valor predeterminado del multiplicador es 3.

PASO 3: Configuración de BFD en una interfaz



Nota: Puede configurar los parámetros de sesión BFD para todas las sesiones BFD en una interfaz.



Advertencia: asegúrese de que los mensajes de redirección del Protocolo de mensajes de control de Internet (ICMP) estén deshabilitados en las interfaces habilitadas para BFD. Utilice el no ip redirects comando o el no ipv6 redirects comando en la interfaz.

SWITCH 1	SWITCH 2
SW1(config)# interface vlan 20 SW1(config-if)# bfd interval 500 min_rx 500 multiplier 3 SW1(config-if)# no ip redirects SW1(config-if)# no ipv6 redirects	SW2(config)# interface vlan 20 SW2(config-if)# bfd interval 500 min_rx 500 mul SW2(config-if)# no ip redirects SW2(config-if)# no ipv6 redirects

El modo asíncrono de BFD es como un intercambio de señales entre dos dispositivos para mantener fuerte su conexión. La configura en ambos dispositivos y, una vez activada, comienzan a enviarse mensajes especiales entre sí a una hora establecida. Estos mensajes tienen algunos ajustes importantes, como la frecuencia con la que se envían y la rapidez con la que un dispositivo puede responder al otro. También hay una

configuración que decide cuántos mensajes perdidos se necesitan para que un dispositivo se dé cuenta de que puede haber un problema con la conexión.

La función de eco BFD envía paquetes de prueba a un vecino y los envía de vuelta para verificar si hay problemas sin involucrar al vecino en el reenvío de paquetes. Puede utilizar un temporizador más lento para reducir el tráfico de paquetes de control y probar el trayecto de reenvío en el sistema de vecinos sin molestar al vecino, lo que acelera la detección. Si ambos vecinos utilizan la función de eco, no hay asimetría.

Motivos de caída de Syslog BFD

- Path Down (Ruta descendente): indica que la ruta de reenvío entre los dos vecinos BFD ya no está operativa, posiblemente debido a una congestión de la red, un fallo del hardware u otros problemas.

```
2024 Apr 11 22:07:07 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519062 to neighbor 172.16.1.1
```

- Función de eco fallida: falla de la función de eco, que es una función de BFD donde se envían y reciben paquetes de eco para verificar la conectividad. Si estos paquetes no se transmiten o reciben correctamente, indica un problema.

```
2024 Apr 11 22:17:45 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519174 to neighbor 10.10.10.1
```

- Sesión Señalizada de Vecino Caída: El dispositivo vecino indica que la sesión BFD está caída, generalmente debido a la detección de un problema en ella es el final de la conexión.

```
2024 Apr 11 22:03:48 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519058 to neighbor 172.16.1.1
```

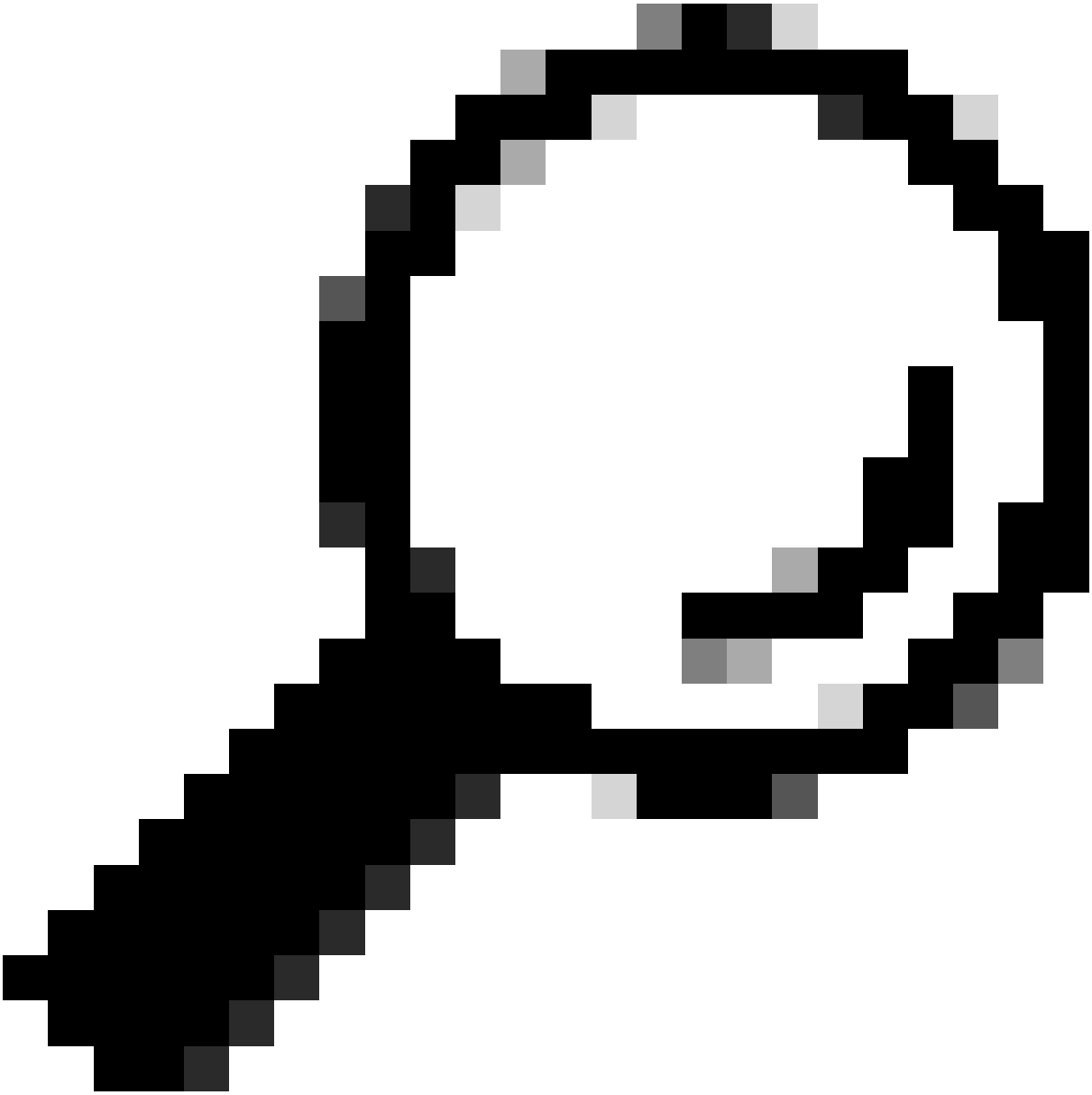
- Tiempo de detección de control vencido: se produce cuando el temporizador de detección de control se agota antes de recibir una respuesta esperada del vecino, lo que indica un posible problema con la conexión.

```
2024 Apr 11 22:19:31 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519061 to neighbor 192.168.2.1
```

- Caída administrativa: la sesión de BFD es interrumpida intencionadamente por un administrador, ya sea por motivos de mantenimiento o debido a cambios en la configuración.

```
2024 Apr 11 22:13:15 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519064 to neighbor 10.10.10.1
```

Configuración de BFD en Protocolos de Ruteo



Sugerencia: Cuando BFD está habilitado en OSPF, se activa para todas las interfaces que utilizan OSPF. Las interfaces adoptan los valores configurados globalmente. Si es necesario realizar ajustes en estos valores, consulte el paso 3, 'Configuración BFD en una Interfaz'.

SWITCH 1	SWITCH 2
SW1(config)# router ospf 1	SW2(config)# router ospf 1

SW1(config-router)# bfd	SW2(config-router)# bfd

También puede habilitar BFD en la interfaz OSPF con el comandoip ospf bfd

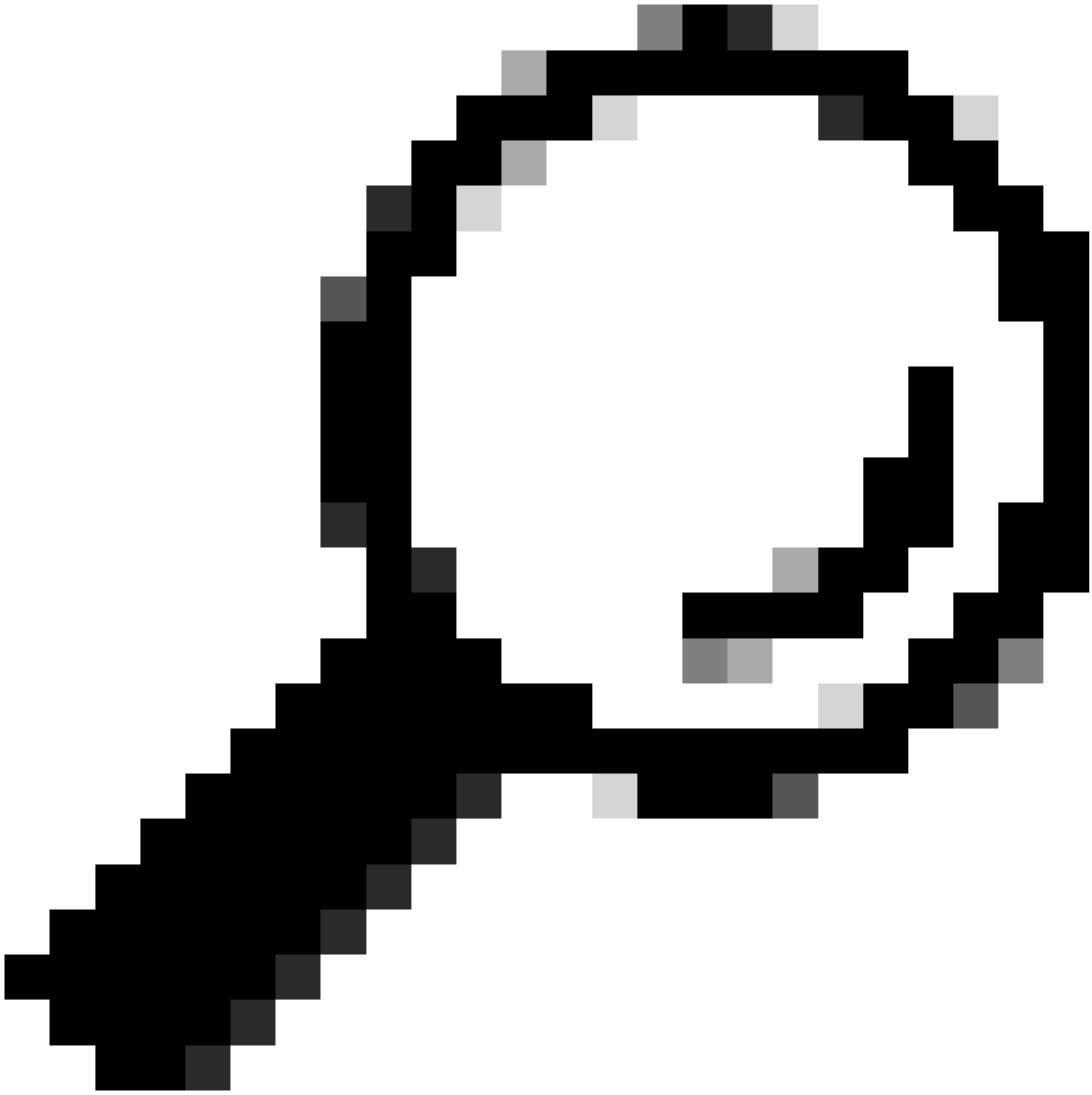
SWITCH 1	SWITCH 2
SW1(config)# interface vlan 10 SW1(config-if)# ip ospf bfd	SW2(config)# interface vlan 10 SW2(config-if)# ip ospf bfd

Ejemplo de configuraciones para BFD en OSPF

```
SW1# show running-config ospf !Command: show running-config ospf !Running configuration last done at: W
```

Configuración de BFD en EIGRP

```
SW1(config)# interface vlan 20 SW1(config-if)# ip eigrp 2 bfd
```



Sugerencia: Cuando BFD está habilitado bajo EIGRP, se activa para todas las interfaces que utilizan EIGRP. Las interfaces adoptan los valores configurados globalmente. Si es necesario realizar ajustes en estos valores, consulte el paso 3, 'Configuración BFD en una Interfaz'.

SWITCH 1	SWITCH 2
SW1(config)# router eigrp 2 SW1(config-router)# bfd	SW2(config)# router eigrp 2 SW2(config-router)# bfd

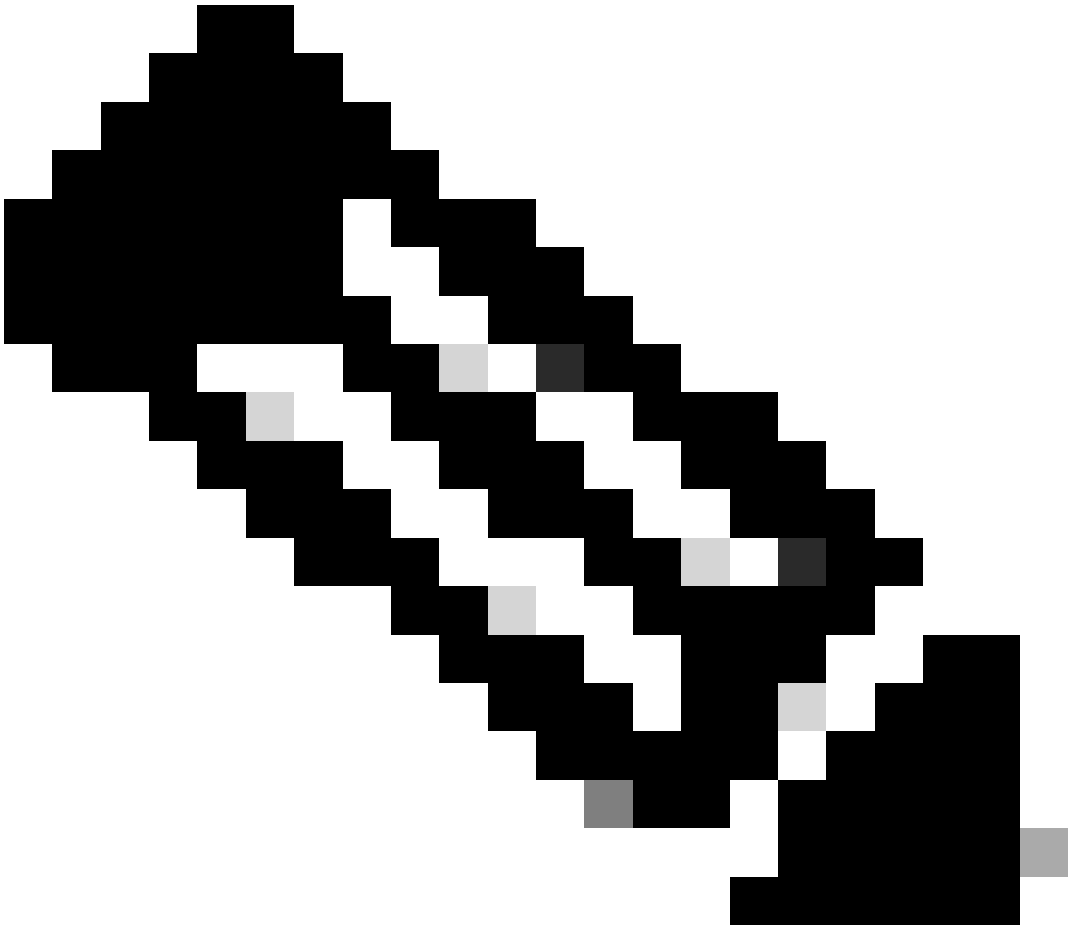
También puede habilitar BFD bajo una interfaz EIGRP con el comandoip eigrp instance-tag bfd

SWITCH 1	SWITCH 2
SW1(config)# interface vlan 20 SW1(config-if)# ip eigrp 2 bfd	SW2(config)# interface vlan 20 SW2(config-if)# ip eigrp 2 bfd

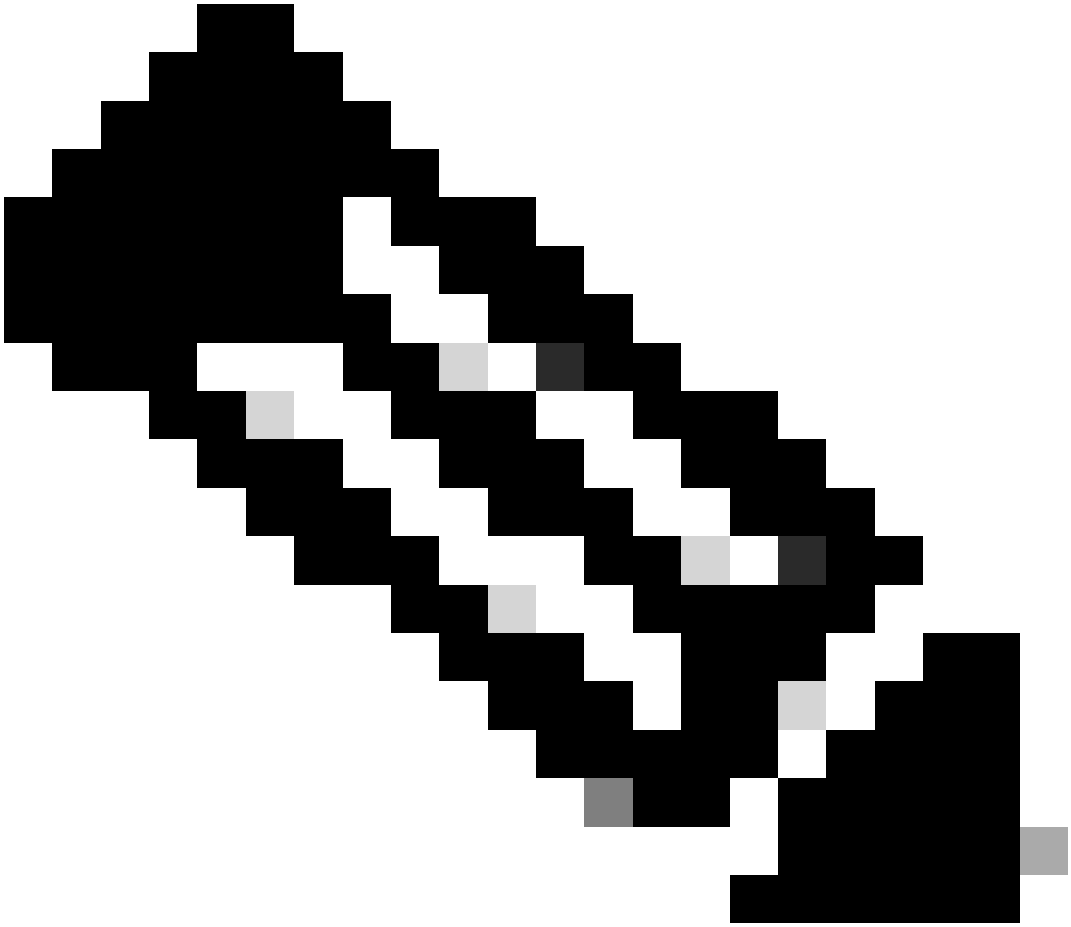
Ejemplo de configuraciones para BFD en EIGRP

```
SW1# show running-config eigrp !Command: show running-config eigrp !Running configuration last done at:
```

Configuración de BFD en BGP



Nota: La función update source facilita que las sesiones BGP utilicen la dirección IP primaria de una interfaz designada como dirección local durante el establecimiento de una sesión BGP con un vecino. Además, permite que BGP se registre como cliente con BFD.



Nota: Al configurar sesiones BFD en el dispositivo, la especificación de 'multihop' o 'single hop' determina el tipo de sesión. Si no se proporciona ninguna palabra clave, el tipo de sesión predeterminado es 'single hop' cuando el par está conectado directamente. Si el par no está conectado, el tipo de sesión predeterminado es 'multisalto'.

SWITCH 1	SWITCH 2
SW1(config)# router bgp 65001 SW1(config-router)# address-family ipv4 unicast SW1(config-router)# neighbor 192.168.3.1 SW1(config-router-neighbor)# bfd multihop SW1(config-router-neighbor)# update-source loopback30	SW2(config)# router bgp 65002 SW2(config-router)# address-family ipv4 unicast SW2(config-router)# neighbor 192.168.2.1 SW2(config-router-neighbor)# bfd multihop SW2(config-router-neighbor)# update-source loopbac

Ejemplo de Configuraciones para BFD en BGP

```
SW1# show running-config bgp !Command: show running-config bgp !Running configuration last done at: Thu
```

Verificación

Después de configurar BFD y asociarlo con un protocolo como OSPF, EIGRP o BGP, los vecinos BFD deben identificarse automáticamente.
Para confirmarlo, utilice el comando:

```
show bfd neighbors
```

En el switch 1

```
 SW1# show bfd neighbors OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf Type BSID 172.16.1.1
```

En el switch 2

```
SW2# show bfd neighbors OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf Type BSID 172.16.1.2
```

Para confirmar esto y obtener un resultado detallado, utilice el comando:

```
SW1# show bfd neighbors interface lo30 details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vr
```

```
SW2# show bfd neighbors interface vlan 20 details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
```

Verificar Usando Detalles De Sesión

```
SW1# sh bfd clients Client : Number of sessions bgp : 1 ospf : 1 eigrp : 1 SW1# show system internal bf
```

Verificar mediante lista de acceso

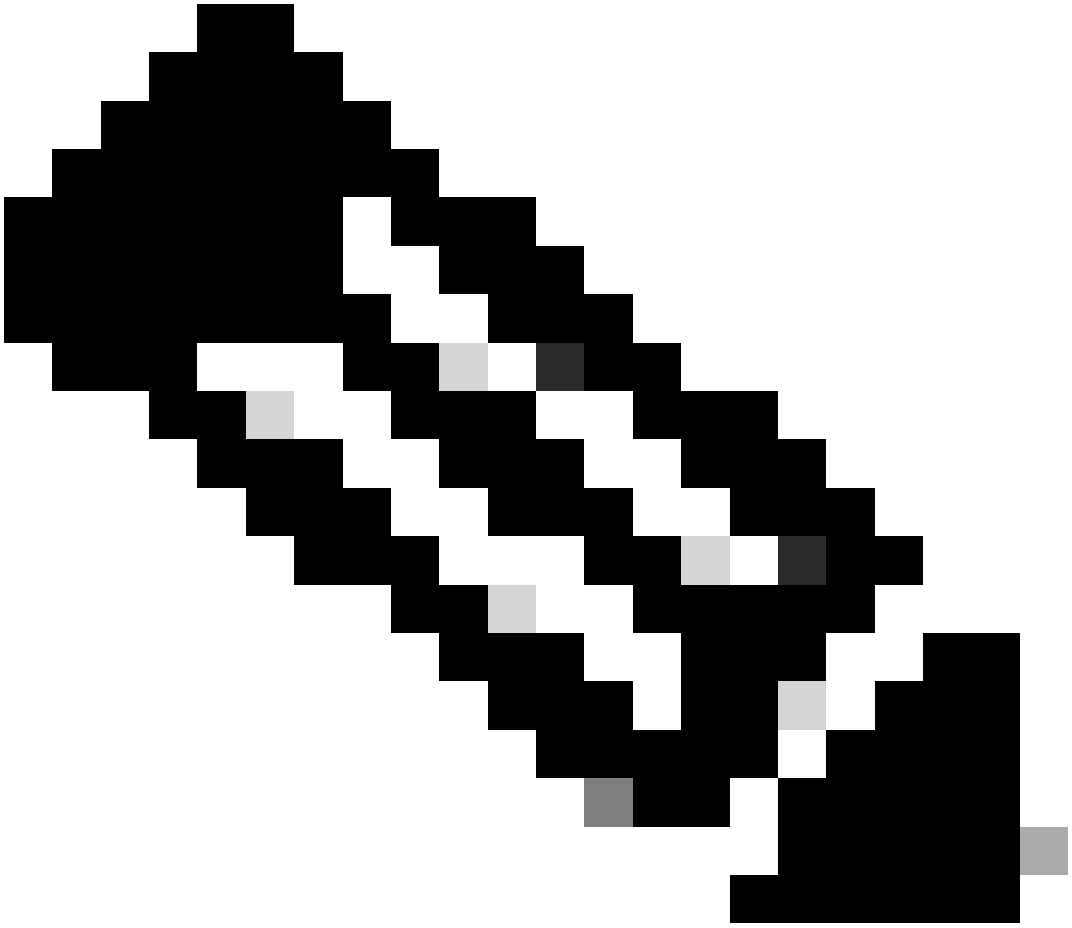
```
SW2# show system internal access-list vlan 10 input statistics slot 1 ======= INSTANCE 0x0 ----------
```

Verificar con Ethanalyzer

Un enfoque alternativo es ejecutar una captura de paquetes, filtrando específicamente para el puerto UDP 3785.

```
SW1# ethanalyzer local interface inband display-filter "udp.port==3785" limit-captured-frames 0 Capturi
```

Se espera la presencia de direcciones IP de origen y destino idénticas en los paquetes capturados del protocolo BFD Echo, ya que estos paquetes Echo se originan desde el propio switch local.



Nota: En ausencia de la sentencia 'no bfd echo' bajo la interfaz, la captura revela paquetes con la dirección IP de origen local y la dirección IP de destino vecina, junto con la observación del control BFD

```
SW2# ethanalyzer local interface inband display-filter "ip.addr==192.168.2.1" limit-captured-frames 0 C
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).