Resolución de problemas de inestabilidad de protocolo de ruteo intermitente con EEM y EPC

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Descripción general del problema
  - Metodología de Troubleshooting
- Información general sobre configuración
  - Plantilla de configuración de ACL
  - Plantilla de parámetros EPC
  - Plantilla de configuración de EEM
- Troubleshooting de Intermitent Routing Protocol Flaps
  - Ejemplo: EIGRP
    - Topología
    - Configuración
    - Análisis
  - OSPF
  - BGP
- Resolución de problemas de inestabilidad BFD intermitente
  - Topología
  - Ejemplo: modo de eco BFD
    - Configuración
    - Análisis
  - Modo asíncrono BFD

Introducción

Este documento describe cómo resolver problemas de inestabilidad de protocolo de ruteo intermitente y inestabilidad BFD en Cisco IOS® XE con EEM y EPC.

Prerequisites

Requirements

Se recomienda estar familiarizado con las características específicas de Embedded Event Manager (EEM) y Embedded Packet Capture (EPC) para las plataformas involucradas en la resolución de problemas, así como Wireshark. Además, se recomienda estar familiarizado con las funciones básicas de saludo y keepalive para protocolos de routing y detección de reenvío

bidireccional (BFD).

Componentes Utilizados

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.

Descripción general del problema

Los flaps del protocolo de ruteo intermitente son un problema común en las redes de producción, pero debido a su naturaleza impredecible, pueden ser difíciles de resolver en tiempo real. EEM proporciona la capacidad de automatizar la recopilación de datos mediante la activación de la captura de datos con cadenas de syslog cuando se producen los flaps. Con EEM y EPC, los datos de captura de paquetes se pueden recopilar de ambos extremos de la adyacencia para aislar la pérdida potencial de paquetes antes del momento de la inestabilidad.

La naturaleza de los flaps del protocolo de ruteo intermitente es que siempre se deben a un tiempo de espera hello o keepalive (a menos que sea un problema físico claro como flaps de link que aparecería en los logs). Por lo tanto, esto es lo que trata la lógica de este documento.

Metodología de Troubleshooting

Lo más importante para determinar cuándo ocurre una inestabilidad del protocolo de ruteo es si los paquetes de saludo o paquetes keepalive fueron enviados y recibidos en ambos dispositivos en el momento del problema. Este método de solución de problemas implica el uso de un EPC continuo en un búfer circular hasta que se produce la inestabilidad, momento en el cual EEM utiliza la cadena de syslog relevante para activar un conjunto de comandos para ejecutar, uno de los cuales detiene el EPC. La opción de memoria intermedia circular permite que el EPC continúe capturando nuevos paquetes mientras sobrescribe los paquetes más antiguos en la memoria intermedia, lo que garantiza que se capture el evento y que la memoria intermedia no se llene ni se detenga de antemano. Los datos de captura de paquetes se pueden correlacionar con la marca de tiempo de la inestabilidad para determinar si los paquetes necesarios se enviaron y recibieron en ambos extremos antes del evento.

Este problema ocurre más comúnmente para los dispositivos que forman una adyacencia sobre una red intermedia como un Proveedor de Servicios de Internet (ISP), pero la misma metodología se puede aplicar para cualquier escenario de inestabilidad del protocolo de ruteo intermitente sin importar los detalles específicos de la topología. Lo mismo se puede hacer en los casos en que el dispositivo vecino es administrado por un tercero y no se puede acceder a él. En tales casos, el método de resolución de problemas descrito en este documento se puede aplicar solamente al dispositivo al que se puede acceder para probar si envió y recibió los paquetes requeridos antes de la inestabilidad. Cuando esto se confirma, los datos se pueden mostrar a la parte que administra el vecino para resolver problemas en el otro extremo si es necesario.

Información general sobre configuración

Esta sección proporciona un conjunto de plantillas de configuración que se pueden utilizar para configurar esta captura de datos automatizada. Modifique las direcciones IP, los nombres de interfaz y los nombres de archivo según sea necesario.

Plantilla de configuración de ACL

En la mayoría de los casos, el único tráfico originado en la dirección IP de la interfaz en ambos extremos de una adyacencia de ruteo es el tráfico de control de ruteo en sí. Como tal, una ACL que permite el tráfico desde la dirección IP de la interfaz local y la dirección IP del vecino a cualquier destino cubre el requisito de cualquier protocolo de ruteo, así como BFD. Si se necesita un filtro adicional, también se puede especificar la IP de destino relevante basada en el protocolo de ruteo o el modo BFD. Defina los parámetros ACL en el modo de configuración:

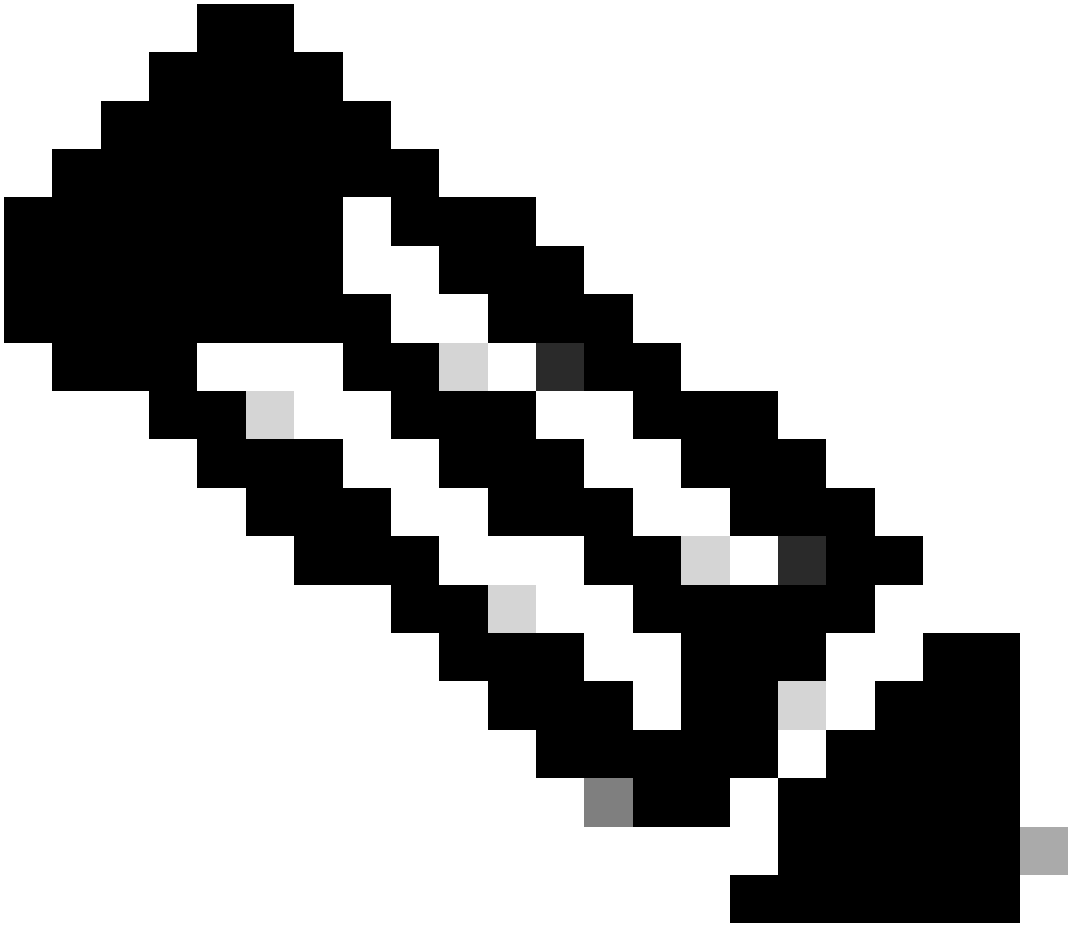
```
config t

ip access-list extended




      permit ip host




       any permit ip host




        any end
```

Plantilla de parámetros EPC

Los parámetros EPC se crean a partir del modo exec de privilegio, no del modo de configuración.

Asegúrese de consultar las guías de configuración específicas de la plataforma para determinar si hay alguna restricción con EPC. Cree los parámetros para la interfaz deseada y asóciela con la ACL para filtrar el tráfico deseado:

- monitor capture <EPC name> interface <interface> both
- monitor capture <EPC name> access-list <ACL name>
- monitor capture <EPC name> buffer size 5 circular



> Nota: En algunas versiones de software, el tráfico generado localmente no es visible con un EPC de nivel de interfaz. En estos escenarios, los parámetros de captura se pueden cambiar para capturar ambas direcciones del tráfico en la CPU:

- monitor capture <EPC name> control-plane both
- monitor capture <EPC name> access-list <ACL name>
- monitor capture <EPC name> buffer size 5 circular

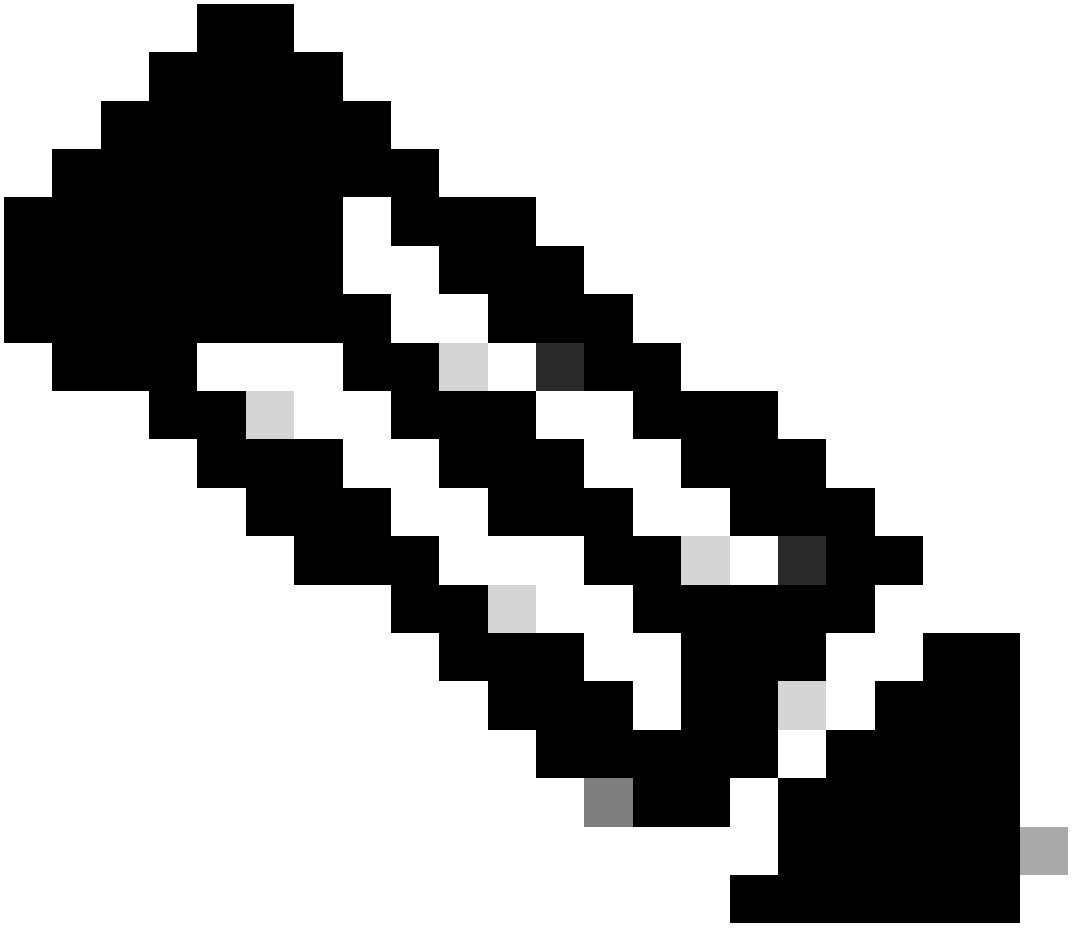
Una vez configurado, inicie el EPC:

- monitor capture <EPC name> start

El EEM está configurado para detener la captura cuando se produce la inestabilidad.

Para asegurarse de que los paquetes se capturan en ambas direcciones, verifique el buffer de captura:

```
show monitor capture

      buffer brief
```



Nota: Las plataformas de switching Catalyst (como Cat9k y Cat3k) requieren que se detenga la captura antes de que se pueda ver el búfer. Para confirmar que la captura funciona, detenga la captura con el comando monitor capture stop, vea el búfer y, a continuación, vuelva a iniciarlo para recopilar datos.

Plantilla de configuración de EEM

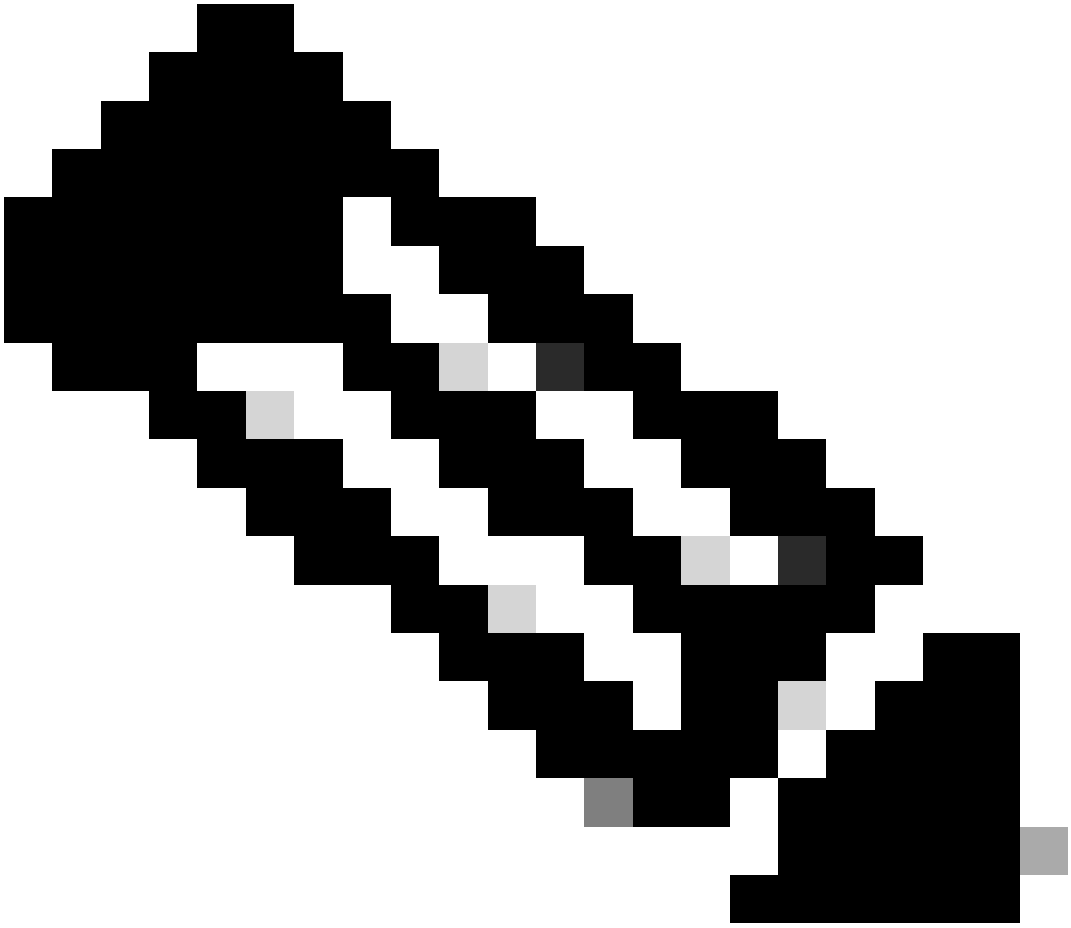
El objetivo principal del EEM es detener la captura de paquetes y guardarla junto con el búfer de syslog. Se pueden incluir comandos adicionales para verificar otros factores como la CPU, las caídas de interfaz o la utilización de recursos específicos de la plataforma y los contadores de caídas. Cree el applet EEM en el modo de configuración:

```
config t
event manager applet
```

```
authorization bypass event syslog pattern "

 " maxrun 120 ratelimit 100000 action 000 cli command "enable" action 005 cli command "show clock

  .txt" action 010 cli command "show logging | append bootflash:

   .txt" action 015 cli command "show process cpu sorted | append bootflash:

    .txt" action 020 cli command "show process cpu history | append bootflash:

     .txt" action 025 cli command "show interfaces | append bootflash:

      .txt" action 030 cli command "monitor capture

       stop" action 035 cli command "monitor capture

        export bootflash:

         .pcap" action 040 syslog msg "Saved logs to bootflash:
```

.txt and saved packet capture to bootflash:

.pcap" action 045 cli command "end" end



Nota: En las plataformas de switching Catalyst (como Cat9k y Cat3k), el comando para exportar la captura es ligeramente diferente. Para estas plataformas, modifique el comando CLI utilizado en la acción 035:

```
action 035 cli command "monitor capture

      export location bootflash:

       .pcap"
```

El valor de límite de velocidad en EEM se expresa en segundos e indica cuánto tiempo debe transcurrir antes de que EEM pueda ejecutarse de nuevo. En este ejemplo, se establece en 100000 segundos (27,8 horas) para permitir que el administrador de la red identifique que se ha completado y extraiga los archivos del dispositivo antes de volver a ejecutarse. Si el EEM se ejecuta nuevamente por sí solo después de este período límite de velocidad, no se recopilan nuevos datos de captura de paquetes, ya que el EPC debe iniciarse manualmente. Sin embargo, los nuevos resultados del comando show se agregan a los archivos de texto.

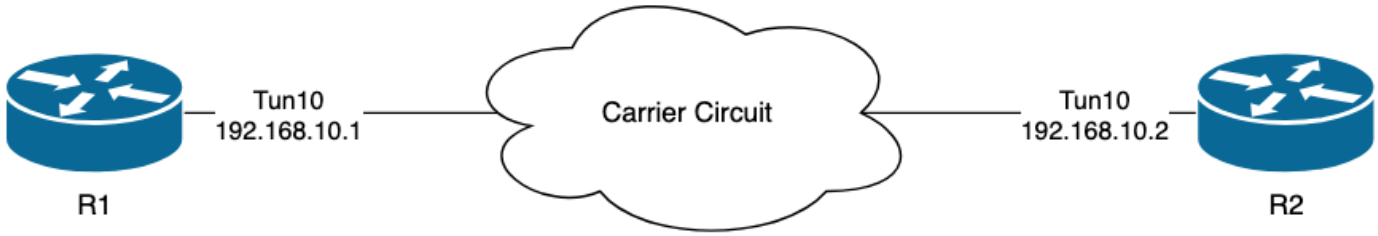
El EEM se puede modificar según sea necesario para recopilar información sobre caídas de paquetes específica de la plataforma y lograr la funcionalidad adicional necesaria para su escenario.

Troubleshooting de Intermitent Routing Protocol Flaps

Ejemplo: EIGRP

En este ejemplo, todos los temporizadores se establecen como predeterminados (saludos de 5 segundos, tiempo de espera de 15 segundos).

Topología



Los registros en R1 indican que ha habido flaps intermitentes de EIGRP que ocurrieron con varias horas de diferencia entre sí:

```
R1#show logging | i EIGRP
*Jul 16 20:45:08.019: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is down: Interf
*Jul 16 20:45:12.919: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is up: new adja
*Jul 17 10:25:42.970: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is down: holdin
*Jul 17 10:25:59.488: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is up: new adja
*Jul 17 14:39:02.970: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is down: holdin
*Jul 17 14:39:16.488: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is up: new adja
```

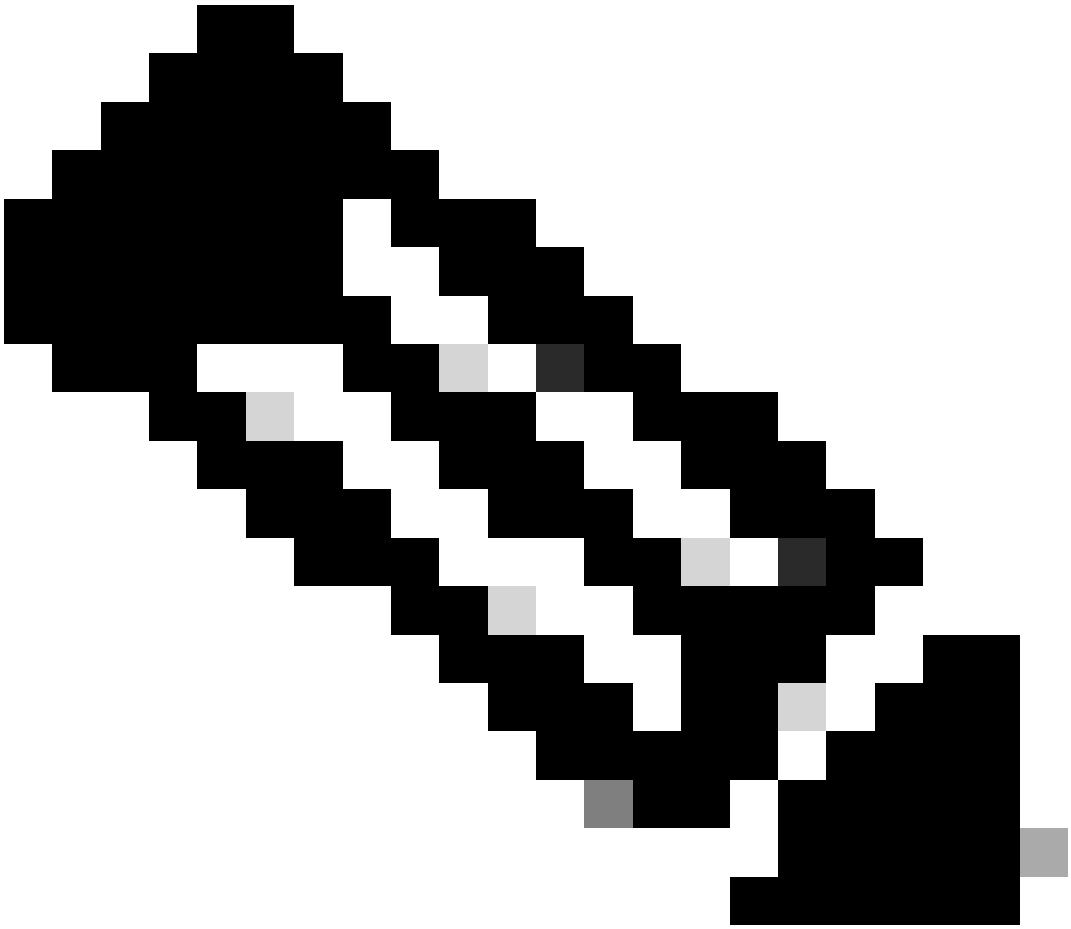
La pérdida de paquetes podría ser en ambas direcciones; el tiempo de espera vencido indica que

este dispositivo no recibió o procesó un saludo del par dentro del tiempo de espera, y la interfaz PEER-TERMINATION recibida indica que el par finalizó la adyacencia porque no recibió o procesó un saludo dentro del tiempo de espera.

Configuración

1. Configure la ACL con las direcciones IP de la interfaz de túnel, ya que éstas son las direcciones IP de origen de los saludos:

```
R1#conf t
R1(config)#ip access-list extended FLAP_CAPTURE
R1(config-ext-nacl)#permit ip host 192.168.10.1 any
R1(config-ext-nacl)#permit ip host 192.168.10.2 any
R1(config-ext-nacl)#end
```



Nota: Las configuraciones mostradas son de R1. Lo mismo se hace en R2 para las

---

interfaces relevantes y con nombres de archivo modificados para el EEM. Si se requiere especificidad adicional, configure la ACL con la dirección de multidifusión EIGRP 224.0.0.10 como la dirección IP de destino para capturar saludos.

2. Cree el EPC y asócielo a la interfaz y a la ACL:

```
R1#monitor capture CAP interface Tunnel10 both
R1#monitor capture CAP access-list FLAP_CAPTURE
R1#monitor capture CAP buffer size 5 circular
```

3. Inicie el EPC y confirme que los paquetes se capturan en ambas direcciones:

```
R1#monitor capture CAP start
R1#show monitor capture CAP buffer brief
 ----------------------------------------------------------------------------
 #   size   timestamp     source             destination      dscp    protocol
 ----------------------------------------------------------------------------
   0   74    0.000000   192.168.10.1     ->  224.0.0.10       48 CS6  EIGRP
   1   74    0.228000   192.168.10.2     ->  224.0.0.10       48 CS6  EIGRP
   2   74    4.480978   192.168.10.2     ->  224.0.0.10       48 CS6  EIGRP
   3   74    4.706024   192.168.10.1     ->  224.0.0.10       48 CS6  EIGRP
```

4. Configure el EEM:

```
R1#conf t
R1(config)#event manager applet R1_EIGRP_FLAP authorization bypass
R1(config-applet)#event syslog pattern "%DUAL-5-NBRCHANGE" maxrun 120 ratelimit 100000
R1(config-applet)#action 000 cli command "enable"
R1(config-applet)#action 005 cli command "show clock | append bootflash:R1_EIGRP_FLAP.txt"
R1(config-applet)#action 010 cli command "show logging | append bootflash:R1_EIGRP_FLAP.txt"
R1(config-applet)#action 015 cli command "show process cpu sorted | append bootflash:R1_EIGRP_FLAP.txt"
R1(config-applet)#action 020 cli command "show process cpu history | append bootflash:R1_EIGRP_FLAP.txt
R1(config-applet)#action 025 cli command "show interfaces | append bootflash:R1_EIGRP_FLAP.txt"
R1(config-applet)#action 030 cli command "monitor capture CAP stop"
R1(config-applet)#action 035 cli command "monitor capture CAP export bootflash:R1_EIGRP_CAP.pcap"
R1(config-applet)#action 040 syslog msg "Saved logs to bootflash:R1_EIGRP_FLAP.txt and saved packet cap
R1(config-applet)#action 045 cli command "end"
R1(config-applet)#end
```

5. Espere a que ocurra la siguiente inestabilidad y copie los archivos de bootflash a través de su método de transferencia preferido para el análisis:

```
R1#show logging
```

```
*Jul 17 16:51:47.154: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is down:
```

- El buffer de registro en el router indica que hubo una inestabilidad EIGRP y que EEM ha guardado los archivos.

Análisis

En este punto, correlacione el tiempo de la inestabilidad encontrada en el buffer de registro con las capturas de paquetes que se recopilaron para determinar si los paquetes de saludo se enviaron y recibieron en ambos extremos cuando ocurrió la inestabilidad. Dado que la interfaz PEER-TERMINATION recibida fue vista en R1, esto significa que R2 debe haber detectado hellos perdidos y, por lo tanto, tiempo de espera vencido, que es lo que se ve en el archivo de registro:

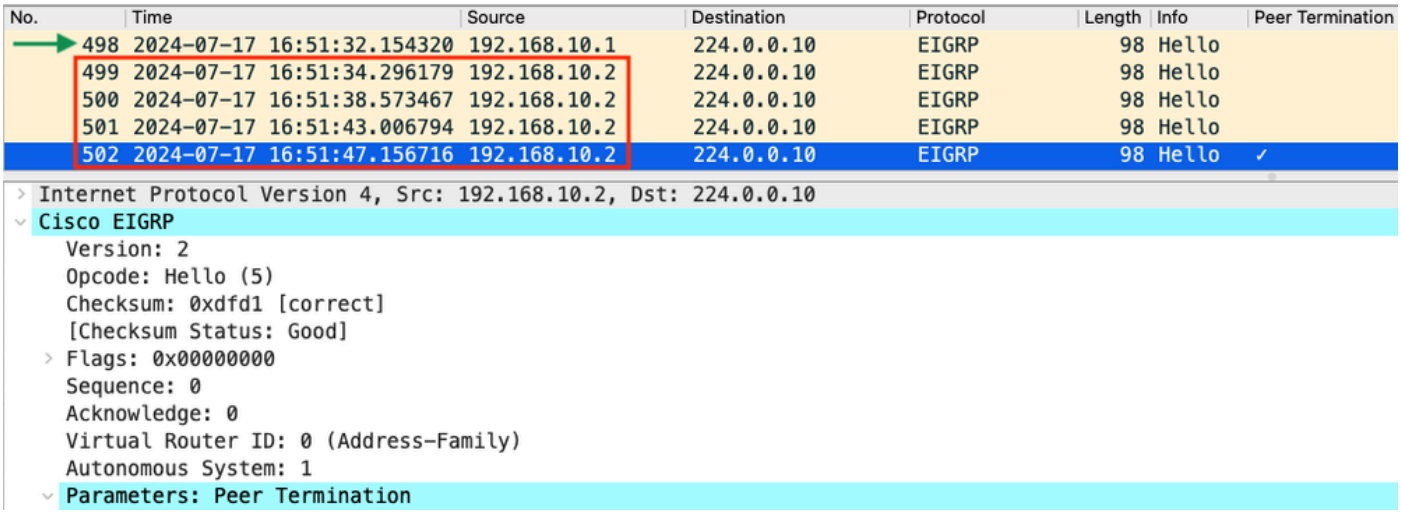
```
*Jul 17 16:51:47.156: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is down: holdin
*Jul 17 16:51:51.870: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is up: new adja
```

Debido a que R2 detectó que el tiempo de espera expiró, confirme si R1 envió saludos en los 15 segundos anteriores al flap en la captura recopilada en R1:

No.	Time	Source	Destination	Protocol	Length	Info	Peer Termination
503	2024-07-17 16:51:32.150713	192.168.10.1	224.0.0.10	EIGRP	98	Hello	
504	2024-07-17 16:51:34.293604	192.168.10.2	224.0.0.10	EIGRP	98	Hello	
505	2024-07-17 16:51:36.802191	192.168.10.1	224.0.0.10	EIGRP	98	Hello	
507	2024-07-17 16:51:38.571024	192.168.10.2	224.0.0.10	EIGRP	98	Hello	
508	2024-07-17 16:51:41.456619	192.168.10.1	224.0.0.10	EIGRP	98	Hello	
510	2024-07-17 16:51:43.004216	192.168.10.2	224.0.0.10	EIGRP	98	Hello	
511	2024-07-17 16:51:46.457320	192.168.10.1	224.0.0.10	EIGRP	98	Hello	
513	2024-07-17 16:51:47.154111	192.168.10.2	224.0.0.10	EIGRP	98	Hello	✓

- La captura muestra saludos de 192.168.10.1 (R1) y 192.168.10.2 (R2) en los 15 segundos anteriores al paquete de saludo de TERMINACIÓN DE PAR que R2 envía a las 16:51:47 (paquete 513).
- Específicamente, los paquetes 503, 505, 508 y 511 (indicados por las flechas verdes) fueron saludos enviados por R1 en este período de tiempo.

El siguiente paso es confirmar si todos los saludos enviados por R1 fueron recibidos por R2 en ese momento, por lo que se debe verificar la captura recopilada de R2:



- La captura muestra que el último saludo recibido desde 192.168.10.1 (R1) fue a las 16:51:32 (indicado por la flecha verde). Después de esto, los siguientes 15 segundos solo muestran los saludos enviados por R2 (indicados por el cuadro rojo). Los paquetes 505, 508 y 511 de la captura de R1 no aparecen en la captura de R2. Esto hace que R2 detecte el temporizador de espera caducado y envíe el paquete de saludo PEER-TERMINATION a las 16:51:47 (paquete 502).

La conclusión de estos datos es que la pérdida de paquetes está en algún lugar de la red portadora entre R1 y R2. En este caso, la pérdida estaba en la dirección de R1 a R2. Para investigar más a fondo, el portador debe estar involucrado para verificar la trayectoria en busca de caídas.

OSPF

La misma lógica se puede utilizar para resolver problemas de inestabilidad OSPF intermitente. Esta sección describe los factores clave que lo distinguen de otros protocolos de ruteo con respecto a temporizadores, filtros de direcciones IP y mensajes de registro.

- Los temporizadores predeterminados son saludos de 10 segundos y un temporizador muerto de 40 segundos. Confirme siempre los temporizadores que están en uso en su red cuando resuelva problemas de inestabilidad de temporizador muerto caducado.
- Los paquetes de saludo se originan en las direcciones IP de la interfaz. Si se necesita una especificidad ACL adicional, la dirección de destino multicast para los saludos OSPF es 224.0.0.5.
- Los mensajes de registro en los dispositivos son ligeramente diferentes. A diferencia de EIGRP, no existe el concepto de un mensaje de terminación de peer con OSPF. Más bien, el dispositivo que detecta el temporizador muerto vencido registra esto como la razón de inestabilidad y luego los saludos que envía ya no contienen el ID de router del par, lo que hace que el par se mueva al estado INIT. Cuando se vuelven a detectar los saludos, la adyacencia pasa a través hasta que alcanza el estado FULL. Por ejemplo:

R1 detecta que el temporizador muerto ha caducado:

```
R1#show logging | i OSPF
*Jul 30 15:29:14.027: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.2 on Tunnel20 from FULL to DOWN, Neighb
*Jul 30 15:32:30.278: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.2 on Tunnel20 from LOADING to FULL, Loa
*Jul 30 16:33:19.841: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.2 on Tunnel20 from FULL to DOWN, Neighb
*Jul 30 16:48:10.504: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.2 on Tunnel20 from LOADING to FULL, Loa
```

Sin embargo, R2 sólo muestra los mensajes de registro cuando OSPF vuelve a FULL. No muestra un mensaje de registro cuando el estado cambia a INIT:

```
R2#show logging | i OSPF
*Jul 30 16:32:30.279: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Tunnel20 from LOADING to FULL, Loa
*Jul 30 16:48:10.506: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Tunnel20 from LOADING to FULL, Loa
```

Para activar el EEM en ambos dispositivos, utilice "%OSPF-5-ADJCHG" como patrón de registro del sistema. Esto garantiza que el EEM se active en ambos dispositivos siempre que se desactive y vuelva a activarse. El valor de límite de velocidad configurado garantiza que no se desencadene dos veces en un breve período cuando se vean varios registros con esta cadena. La clave es confirmar si los saludos se envían y reciben en las capturas de paquetes en ambos lados.

BGP

La misma lógica se puede utilizar para resolver problemas de inestabilidad BGP intermitente. Esta sección describe los factores clave que lo distinguen de otros protocolos de ruteo con respecto a temporizadores, filtros de direcciones IP y mensajes de registro.

- Los temporizadores predeterminados son señales de mantenimiento de 60 segundos y un tiempo de espera de 180 segundos. Confirme siempre los temporizadores que se utilizan en la red cuando solucione problemas de inestabilidad de tiempo de espera caducado.
- Los paquetes keepalive se envían mediante unidifusión entre las direcciones IP vecinas al puerto de destino TCP 179. Si se necesita una especificidad ACL adicional, permita el tráfico TCP desde las direcciones IP de origen al puerto TCP de destino 179.
- Los mensajes de registro para BGP son similares en ambos dispositivos, pero el dispositivo que detecta el vencimiento del tiempo de espera muestra que envió la notificación al vecino, mientras que el otro indica que recibió el mensaje de notificación. Por ejemplo:

R1 detecta que el tiempo de espera ha caducado y envía la notificación a R2:

```
R1#show logging | i BGP
*Jul 30 17:49:23.730: %BGP-3-NOTIFICATION: sent to neighbor 192.168.30.2 4/0 (hold time expired) 0 byte
*Jul 30 17:49:23.731: %BGP-5-NBR_RESET: Neighbor 192.168.30.2 reset (BGP Notification sent)
*Jul 30 17:49:23.732: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Down BGP Notification sent
*Jul 30 17:49:23.732: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.30.2 IPv4 Unicast topology base remove
```

R2 recibe la notificación de R1 porque R1 detectó que el tiempo de espera venció:

```
R2#show logging | i BGP
*Jul 30 17:49:23.741: %BGP-3-NOTIFICATION: received from neighbor 192.168.30.1 4/0 (hold time expired)
*Jul 30 17:49:23.741: %BGP-5-NBR_RESET: Neighbor 192.168.30.1 reset (BGP Notification received)
*Jul 30 17:49:23.749: %BGP-5-ADJCHANGE: neighbor 192.168.30.1 Down BGP Notification received
*Jul 30 17:49:23.749: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.30.1 IPv4 Unicast topology base remove
```

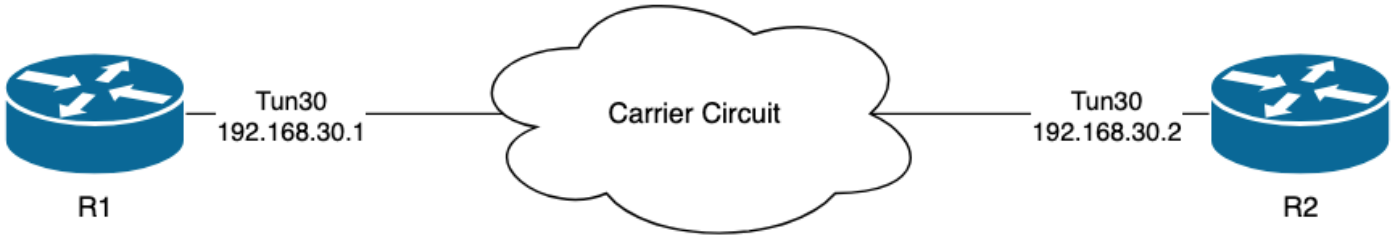
Para activar el EEM para una inestabilidad BGP, utilice "%BGP_SESSION-5-ADJCHANGE" como patrón de syslog. Cualquiera de los otros mensajes de syslog "%BGP" que también se registran después de la inestabilidad también se puede utilizar para activar el EEM.

Resolución de problemas de inestabilidad BFD intermitente

Se puede aplicar la misma metodología para resolver problemas de inestabilidad BFD intermitente, con algunas diferencias menores para aplicar al análisis. Esta sección cubre algunas funciones básicas de BFD y proporciona un ejemplo de cómo utilizar EEM y EPC para resolver problemas. Para obtener información más detallada sobre la resolución de problemas de BFD, consulte Resolución de Problemas de Detección de Reenvío Bidireccional en Cisco IOS XE.

En este ejemplo, los temporizadores BFD se configuran en 300 ms con un multiplicador de 3, lo que significa que los ecos se envían cada 300 ms, y se detecta una falla de eco cuando no se devuelven 3 paquetes de eco en una fila (igual a un tiempo de espera de 900 ms).

Topología



Ejemplo: modo de eco BFD

En el modo de eco BFD (el modo predeterminado), los paquetes de eco BFD se envían con la IP de interfaz local como origen y destino. Esto permite al vecino procesar el paquete en el plano de datos y devolverlo al dispositivo de origen. Cada eco BFD se envía con un ID de eco en el encabezado del mensaje de eco BFD. Éstos se pueden utilizar para determinar si un paquete de eco BFD enviado fue recibido de vuelta, ya que debe haber dos apariciones de cualquier paquete de eco BFD dado si fue devuelto por el vecino. Los paquetes de control BFD, que se utilizan para controlar el estado de la sesión BFD, se envían unidifusión entre las direcciones IP de la interfaz.

Los registros de R1 indican que la adyacencia BFD ha caído varias veces debido a la FALLA DE ECO, lo que significa que durante esos intervalos, R1 no recibió ni procesó 3 de sus propios

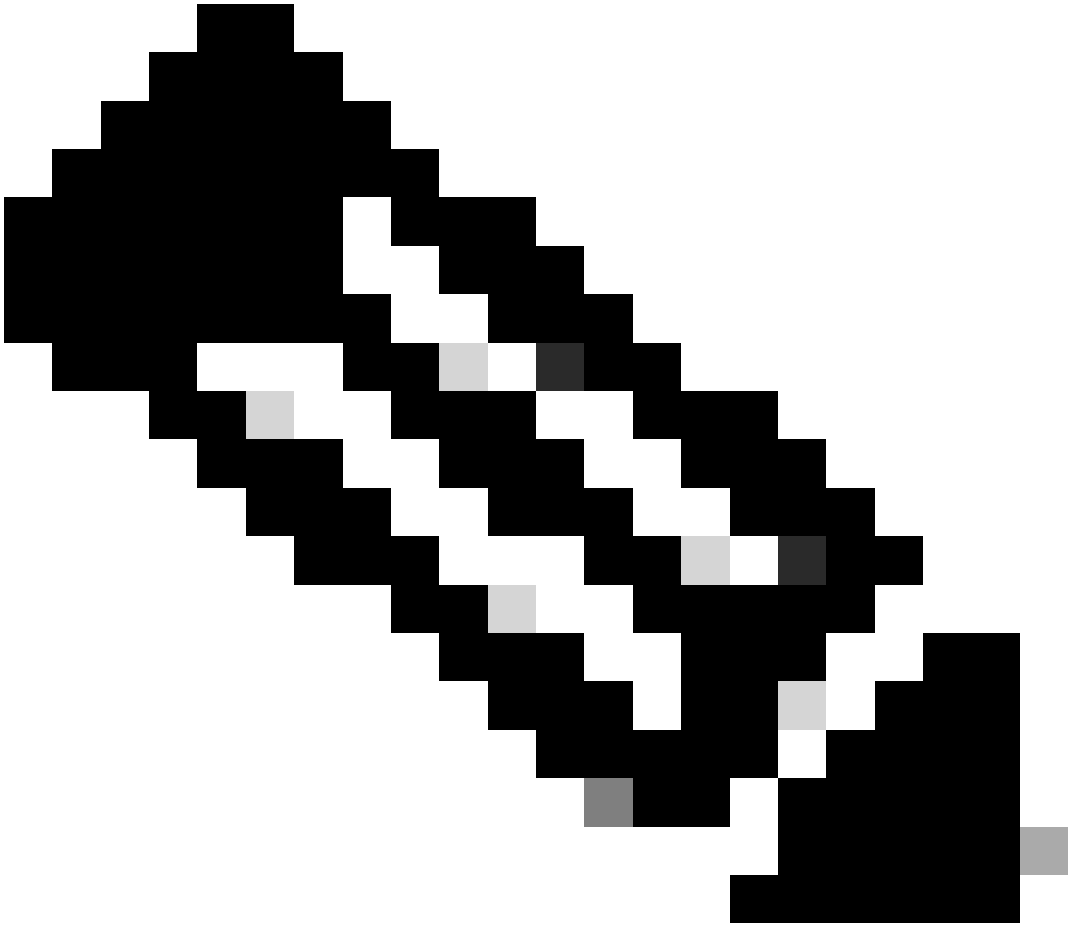
paquetes de eco de vuelta de R2.

```
R1#show logging | i BFD
*Jul 18 13:41:09.007: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going Down R
*Jul 18 13:41:09.009: %BGP-5-NBR_RESET: Neighbor 192.168.30.2 reset (BFD adjacency down)
*Jul 18 13:41:09.010: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Down BFD adjacency down
*Jul 18 13:41:09.010: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.30.2 IPv4 Unicast topology base remove
*Jul 18 13:41:09.010: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed,  ld:4097 neigh proc
*Jul 18 13:41:13.335: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4097 handle:1 is going UP
*Jul 18 13:41:18.576: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 192.168.30.2 proc
*Jul 18 13:41:19.351: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4097 handle:1 is going UP
*Jul 18 15:44:08.360: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going Down R
*Jul 18 15:44:08.362: %BGP-5-NBR_RESET: Neighbor 192.168.30.2 reset (BFD adjacency down)
*Jul 18 15:44:08.363: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Down BFD adjacency down
*Jul 18 15:44:08.363: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.30.2 IPv4 Unicast topology base remove
*Jul 18 15:44:08.363: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed,  ld:4097 neigh proc
*Jul 18 15:44:14.416: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4097 handle:1 is going UP
*Jul 18 15:44:14.418: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed,  ld:4097 neigh proc
*Jul 18 15:44:18.315: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 192.168.30.2 proc
```

Configuración

1. Configure la ACL con las direcciones IP de la interfaz de túnel, ya que éstas son las direcciones IP de origen de los paquetes de eco BFD y los paquetes de control:

```
R1#conf t
R1(config)#ip access-list extended FLAP_CAPTURE
R1(config-ext-nacl)#permit ip host 192.168.30.1 any
R1(config-ext-nacl)#permit ip host 192.168.30.2 any
```



Nota: Las configuraciones mostradas son de R1. Lo mismo se hace en R2 para las interfaces relevantes y con nombres de archivo modificados para el EEM. Si se requiere especificidad adicional, configure la ACL para UDP con los puertos de destino 3785 (paquetes de eco) y 3784 (paquetes de control).

2. Cree el EPC y asócielo a la interfaz y a la ACL:

```
R1#monitor capture CAP interface Tunnel30 both
R1#monitor capture CAP access-list FLAP_CAPTURE
R1#monitor capture CAP buffer size 5 circular
```

3. Inicie el EPC y confirme que los paquetes se capturan en ambas direcciones:

```
R1#monitor capture CAP start
```

```
R1#show monitor capture CAP buff brief
 ----------------------------------------------------------------------------
 #   size   timestamp     source             destination      dscp    protocol
 ----------------------------------------------------------------------------
   0   54    0.000000   192.168.30.2     ->  192.168.30.2     48 CS6  UDP
   1   54    0.000000   192.168.30.2     ->  192.168.30.2     48 CS6  UDP
   2   54    0.005005   192.168.30.1     ->  192.168.30.1     48 CS6  UDP
   3   54    0.005997   192.168.30.1     ->  192.168.30.1     48 CS6  UDP
```

4. Configure el EEM:

```
R1#conf t
R1(config)#event manager applet R1_BFD_FLAP authorization bypass
R1(config-applet)#event syslog pattern "%BFDFSM-6-BFD_SESS_DOWN" maxrun 120 ratelimit 100000
R1(config-applet)#action 000 cli command "enable"
R1(config-applet)#action 005 cli command "show clock | append bootflash:R1_BFD_FLAP.txt"
R1(config-applet)#action 010 cli command "show logging | append bootflash:R1_BFD_FLAP.txt"
R1(config-applet)#action 015 cli command "show process cpu sorted | append bootflash:R1_BFD_FLAP.txt"
R1(config-applet)#action 020 cli command "show process cpu history | append bootflash:R1_BFD_FLAP.txt"
R1(config-applet)#action 025 cli command "show interfaces | append bootflash:R1_BFD_FLAP.txt"
R1(config-applet)#action 030 cli command "monitor capture CAP stop"
R1(config-applet)#action 035 cli command "monitor capture CAP export bootflash:R1_BFD_CAP.pcap"
R1(config-applet)#action 040 syslog msg "Saved logs to bootflash:R1_BFD_FLAP.txt and saved packet captu
R1(config-applet)#action 045 cli command "end"
R1(config-applet)#end
```

5. Espere a que ocurra la siguiente inestabilidad y copie los archivos de bootflash a través de su método de transferencia preferido para el análisis:

```
R1#show logging

*Jul 18 19:09:47.482: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going
```

- El buffer de registro indica que hubo una inestabilidad BFD a las 19:09:47, y los archivos han sido guardados por el EEM.

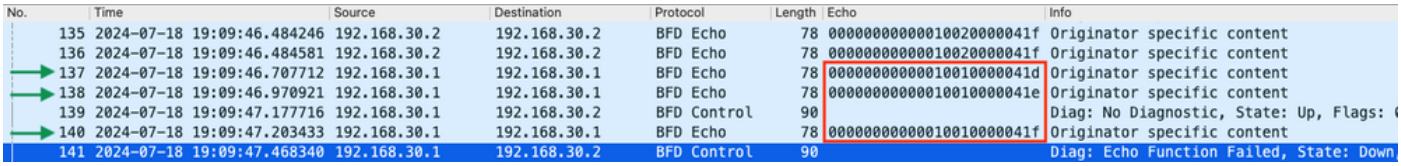
Análisis

En este punto, correlacione el tiempo de la inestabilidad encontrada en el buffer de registro con

las capturas de paquetes que se recopilaron para determinar si los ecos BFD se enviaron y recibieron en ambos extremos cuando ocurrió el problema. Dado que el motivo de inestabilidad en R1 es ECHO FAILURE, esto significa que también habría enviado un paquete de control a R2 para terminar la sesión BFD, y esto se refleja en el archivo de registro recopilado de R2 donde se ve el motivo de caída de BFD RX DOWN:

```
*Jul 18 19:09:47.468: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4098 handle:2,is going Down R
*Jul 18 19:09:47.470: %BGP-5-NBR_RESET: Neighbor 192.168.30.1 reset (BFD adjacency down)
*Jul 18 19:09:47.471: %BGP-5-ADJCHANGE: neighbor 192.168.30.1 Down BFD adjacency down
*Jul 18 19:09:47.471: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.30.1 IPv4 Unicast topology base remove
*Jul 18 19:09:47.471: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed,  ld:4098 neigh proc
```

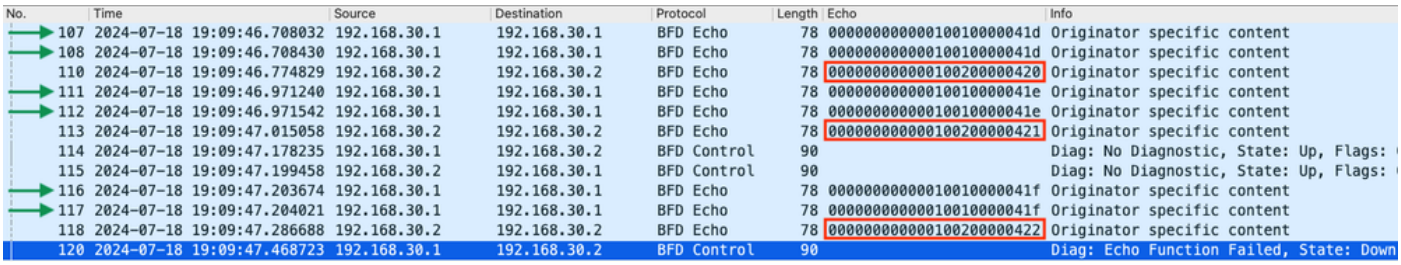
Debido a que R1 detectó una FALLA DE ECO, verifique la captura de paquetes recopilada en R1 para ver si envió y recibió ecos BFD en los 900 ms antes de la inestabilidad.



No.	Time	Source	Destination	Protocol	Length	Echo	Info
135	2024-07-18 19:09:46.484246	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000001002000041f	Originator specific content
136	2024-07-18 19:09:46.484581	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000001002000041f	Originator specific content
137	2024-07-18 19:09:46.707712	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041d	Originator specific content
138	2024-07-18 19:09:46.970921	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041e	Originator specific content
139	2024-07-18 19:09:47.177716	192.168.30.1	192.168.30.2	BFD Control	90		Diag: No Diagnostic, State: Up, Flags:
140	2024-07-18 19:09:47.203433	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041f	Originator specific content
141	2024-07-18 19:09:47.468340	192.168.30.1	192.168.30.2	BFD Control	90		Diag: Echo Function Failed, State: Down

- La captura muestra que R1 envió activamente paquetes de eco BFD hasta el momento de la inestabilidad, pero R2 no los devolvió, por lo que R1 envía un paquete de control para terminar la sesión a las 19:09:47.468.
- Esto se evidencia por el hecho de que los paquetes 137, 138 y 140 (indicados por las flechas verdes) solo se ven una vez en la captura, lo que se puede determinar a partir de los ID de eco de BFD (en el cuadro rojo). Si se hubieran devuelto los ecos, habría una segunda copia de cada uno de esos paquetes con el mismo ID de eco BFD. El campo de identificación IP del encabezado IP (no representado aquí) también se puede utilizar para verificar esto.
- Esta captura también muestra que no se recibieron ecos de BFD de R2 después del paquete 136, lo que es otra indicación de pérdida de paquetes en la dirección de R2 a R1.

El siguiente paso es confirmar si todos los paquetes de eco BFD enviados por R1 fueron recibidos y devueltos por R2, por lo que se debe verificar la captura recopilada de R2:



No.	Time	Source	Destination	Protocol	Length	Echo	Info
107	2024-07-18 19:09:46.708032	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041d	Originator specific content
108	2024-07-18 19:09:46.708430	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041d	Originator specific content
110	2024-07-18 19:09:46.774829	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000001002000000420	Originator specific content
111	2024-07-18 19:09:46.971240	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041e	Originator specific content
112	2024-07-18 19:09:46.971542	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041e	Originator specific content
113	2024-07-18 19:09:47.015058	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000001002000000421	Originator specific content
114	2024-07-18 19:09:47.178235	192.168.30.1	192.168.30.2	BFD Control	90		Diag: No Diagnostic, State: Up, Flags:
115	2024-07-18 19:09:47.199458	192.168.30.2	192.168.30.1	BFD Control	90		Diag: No Diagnostic, State: Up, Flags:
116	2024-07-18 19:09:47.203674	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041f	Originator specific content
117	2024-07-18 19:09:47.204021	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000001001000041f	Originator specific content
118	2024-07-18 19:09:47.286688	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000001002000000422	Originator specific content
120	2024-07-18 19:09:47.468723	192.168.30.1	192.168.30.2	BFD Control	90		Diag: Echo Function Failed, State: Down

- Esta captura muestra que todos los ecos BFD enviados por R1 fueron recibidos y devueltos por R2 (indicados con flechas verdes); Los paquetes 107 y 108 son el mismo eco BFD, los paquetes 111 y 112 son el mismo eco BFD y los paquetes 116 y 117 son el mismo eco BFD.

- Esta captura también muestra que R2 envió activamente paquetes de eco (indicados con cuadros rojos) que no se ven en la captura en R1, lo que indica aún más la pérdida de paquetes entre los dispositivos en la dirección de R2 a R1.

La conclusión de estos datos es que la pérdida de paquetes está en algún lugar de la red portadora entre R1 y R2, y todas las pruebas en este punto indican que la dirección de la pérdida es de R2 a R1. Para investigar más a fondo, el portador debe estar involucrado para verificar la trayectoria en busca de caídas.

Modo asíncrono BFD

Se puede aplicar el mismo método cuando el modo asíncrono BFD está en uso (función de eco inhabilitada), y la configuración EEM y EPC se pueden mantener iguales. La diferencia en el modo asíncrono es que los dispositivos envían paquetes de control BFD de unidifusión entre sí como señales de mantenimiento, análogas a una adyacencia de protocolo de ruteo típica. Esto significa que sólo se envían paquetes del puerto UDP 3784. En este escenario, BFD permanece en el estado activo mientras se reciba un paquete BFD del vecino dentro del intervalo requerido. Cuando esto no sucede, el motivo de la falla es DETECT TIMER EXPIRED y el router envía un paquete de control al par para desactivar la sesión.

Para analizar las capturas en el dispositivo que detectaron la falla, busque los paquetes BFD de unidifusión recibidos del par durante el tiempo justo antes de la inestabilidad. Por ejemplo, si el intervalo TX se establece en 300 ms con un multiplicador de 3, entonces si no hay paquetes BFD recibidos en los 900 ms previos a la inestabilidad, esto indica una posible pérdida de paquetes. En la captura obtenida del vecino a través del EEM, verifique esta misma ventana de tiempo; si los paquetes se enviaron durante ese tiempo, entonces confirma que hay una pérdida en algún lugar entre los dispositivos.

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).