排除EEM和EPC間歇性路由協定擺動故障

目錄

簡介

本文描述如何對具有EEM和EPC的Cisco IOS® XE中的間歇性路由協定擺動和BFD擺動進行故障排除。

必要條件

需求

建議熟悉用於故障排除的平台的嵌入式事件管理器(EEM)和嵌入式資料包捕獲(EPC)以及Wireshark的具體資訊。此外，建議熟悉路由協定和雙向轉發檢測(BFD)的基本hello和keepalive功能。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題概述

間歇性路由協定抖動是生產網路中的常見問題，但由於其不可預測性，難以對其進行即時故障排除。EEM能夠在系統日誌字串觸發資料捕獲時，自動執行資料收集。使用EEM和EPC，資料包捕獲資料可以從鄰接的兩端收集，以便在進行翻動之前隔離潛在的資料包丟失。

間歇性路由協定跳變的性質是它們總是由於hello或keepalive超時而引起的（除非這是明顯的物理問題，如會出現在日誌中的鏈路跳變）。 因此，這就是本檔案中的邏輯所涵蓋的內容。

故障排除方法

確定路由協定擺動發生時間的最重要的事情是，在出現問題時，兩台裝置是否傳送和接收了hello資料包或keepalive資料包。此疑難排解方法涉及在循環緩衝區上使用連續的EPC，直到發生翻動，此時EEM使用相關的系統日誌字串觸發一組命令運行，其中一個命令會停止EPC。循環緩衝區選項允許EPC繼續捕獲新資料包，同時覆蓋緩衝區中最舊的資料包，這可確保捕獲事件且緩衝區不會預先填充和停止。然後，可以將分組捕獲資料與翻動的時間戳相關聯，以確定在事件之前兩端是否傳送和接收了必要的分組。

此問題最常見於通過中間網路（如網際網路服務提供商[ISP]）形成鄰接關係的裝置，但是同樣的方法也適用於任何間歇性路由協定擺動情況，無論具體的拓撲細節如何。如果鄰居裝置由第三方管理，並且無法訪問，也可以執行相同操作。在這類情況下，本文檔中描述的故障排除方法可應用於僅可訪問的一個裝置，以證明它在翻動之前是否傳送和接收了所需的資料包。確認此情況後，資料可顯示給管理鄰居的一方，以便在需要時進一步在另一端進行疑難排解。

組態概觀

本節提供一組配置模板，可用於設定此自動資料捕獲。根據需要修改IP地址、介面名稱和檔名。

ACL配置模板

在大多數情況下，源自路由鄰接兩端介面IP地址的唯一流量是路由控制流量本身。因此，允許從本地介面IP地址和鄰居IP地址到任何目的地的流量的ACL會滿足任何路由協定以及BFD的要求。如果需要額外的篩選條件，那麼也可以指定基於路由通訊協定或BFD模式的相關目的地IP。在配置模式下定義ACL引數：

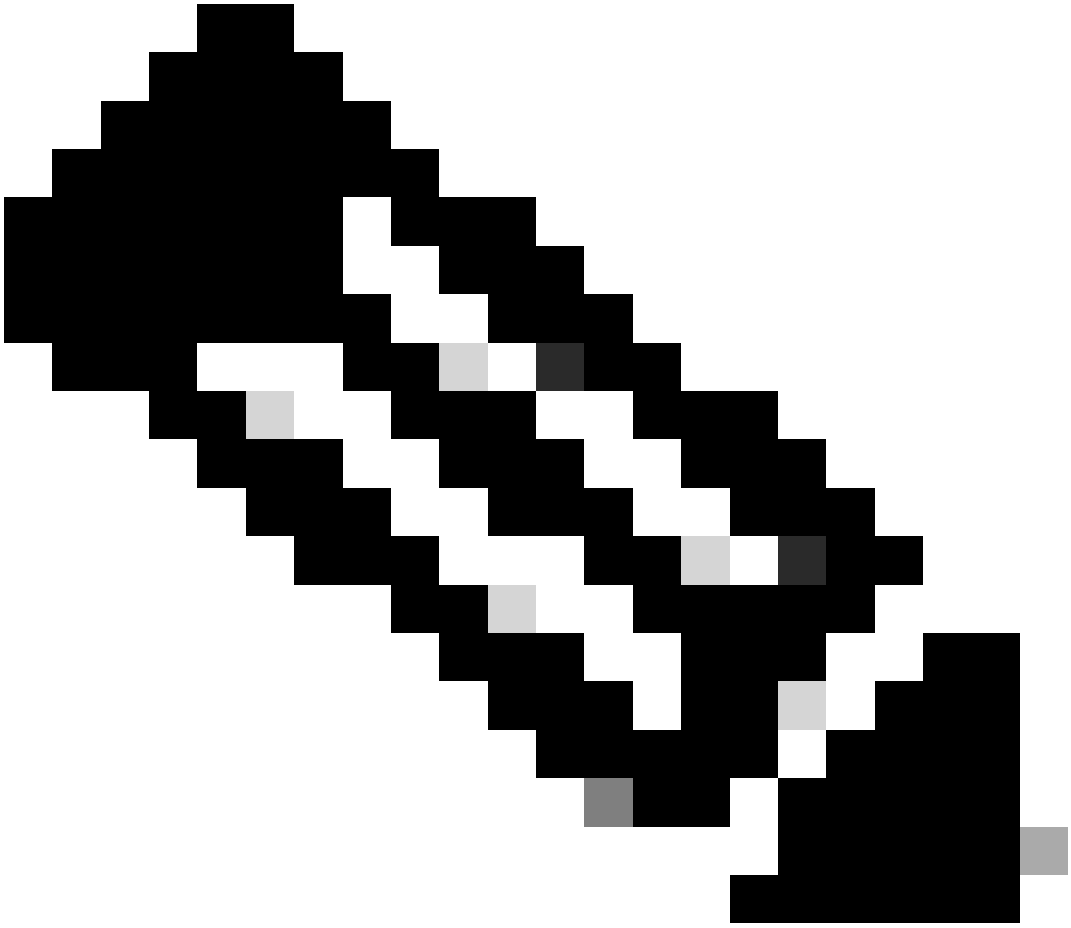
```
config t

ip access-list extended
```

```
permit ip host

 any permit ip host

  any end
```

EPC引數模板

EPC引數是在特權exec模式而非配置模式下建立的。請務必檢查特定於平台的配置指南，以確定對EPC是否有任何限制。為所需介面建立引數，並將其與要過濾所需流量的ACL相關聯：

- monitor capture <EPC name> interface <interface> both
- monitor capture <EPC name> access-list <ACL name>
- monitor capture <EPC name>緩衝區大小5循環



附註：在某些軟體版本中，本地生成的流量在介面級EPC中不可見。在這些情況下，可以更改捕獲引數以捕獲CPU上的兩個流量方向：

- monitor capture <EPC name> control-plane both
- monitor capture <EPC name> access-list <ACL name>
- monitor capture <EPC name>緩衝區大小5循環

配置後，啟動EPC:

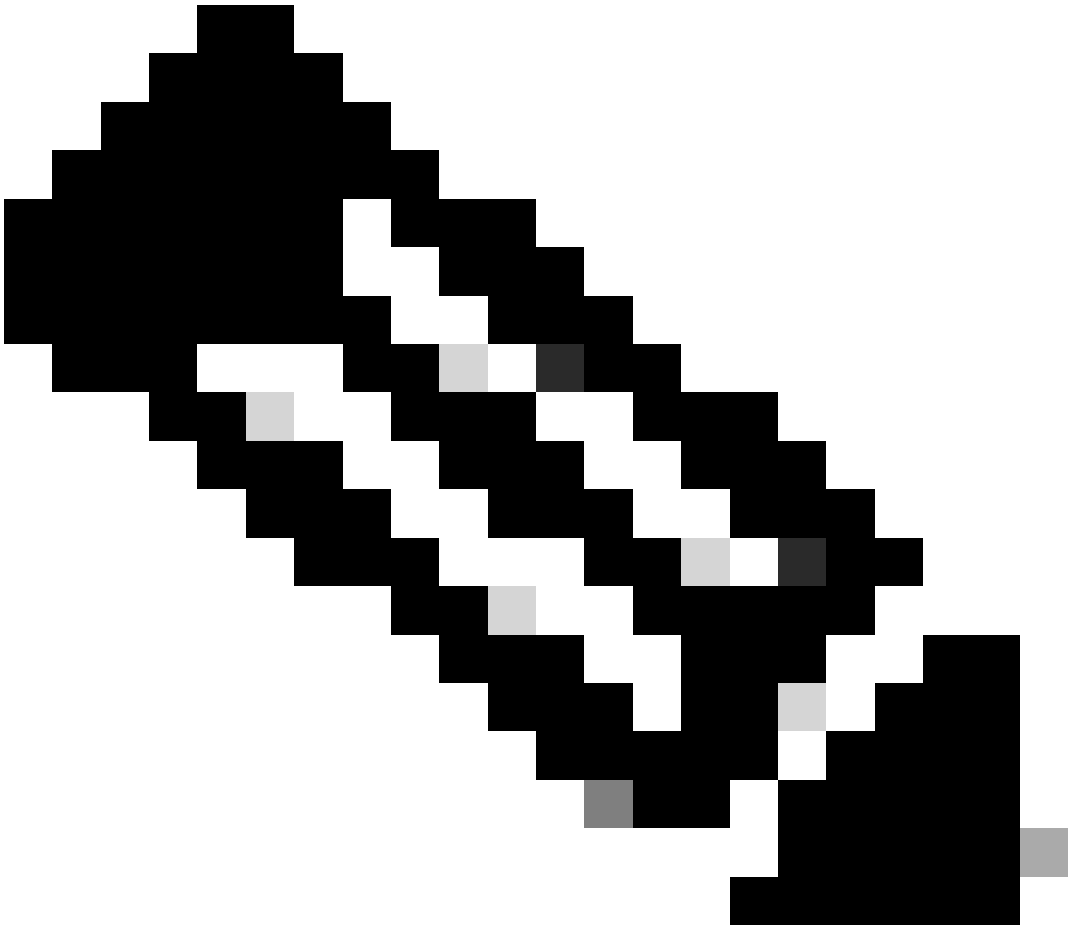
- monitor capture <EPC name>啟動

EEM設定為在翻動發生時停止捕獲。

若要確保兩個方向都擷取封包，請檢查擷取緩衝區：

```
show monitor capture
```

```
buffer brief
```



附註：Catalyst交換平台（例如Cat9k和Cat3k）要求先停止擷取，才能檢視緩衝區。要確認捕獲正常工作，請使用monitor capture stop命令停止捕獲，檢視緩衝區，然後再次啟動它以收集資料。

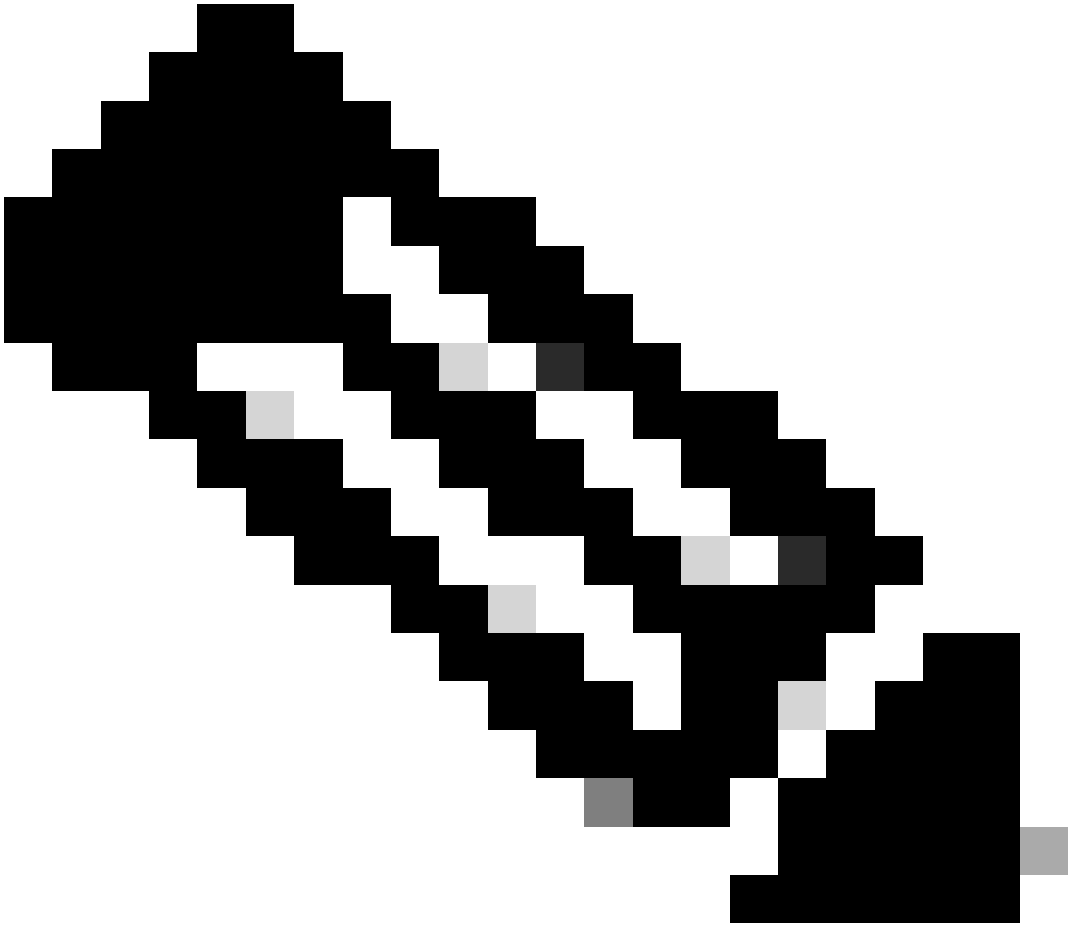
EEM配置模板

EEM的主要用途是停止資料包捕獲，並將其與系統日誌緩衝區一起儲存。還可以包括其他命令來檢查其他因素，例如CPU、介面丟棄或平台特定的資源利用率和丟棄計數器。在配置模式下建立

EEM小程式：

```
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
```



附註：在Catalyst交換平台（例如Cat9k和Cat3k）上，匯出捕獲的命令略有不同。對於這些平台，請修改操作035中使用的CLI命令：

```
action 035 cli command "monitor capture

      export location bootflash:

       .pcap"
```

EEM中的速率限制值以秒為單位，指示必須經過多長時間才能再次運行EEM。在本例中，它被設定為100000秒（27.8小時），以便網路管理員有足夠的時間確定它已完成，並在再次運行之前從裝置中取出檔案。如果EEM在此速率限制期後自行再次運行，則不會收集任何新的資料包捕獲資料，因為EPC必須手動啟動。但是，新的show命令輸出被附加到文本檔案中。

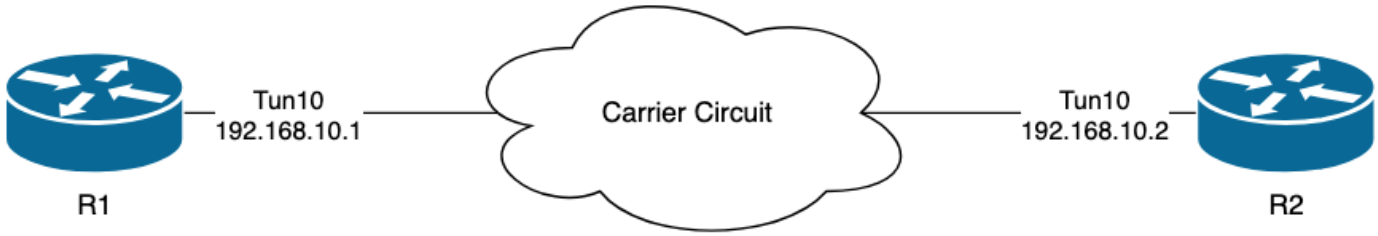
您可以根據需要修改EEM以收集平台特定的資料包丟棄資訊並獲取您的方案所需的其他功能。

排除間歇性路由協定擺動故障

示例 — EIGRP

在此示例中，所有計時器均設定為預設值（5秒hello、15秒保持時間）。

拓撲



R1上的日誌表明存在間歇性的EIGRP擺動，它們彼此相隔數小時：

```
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
```

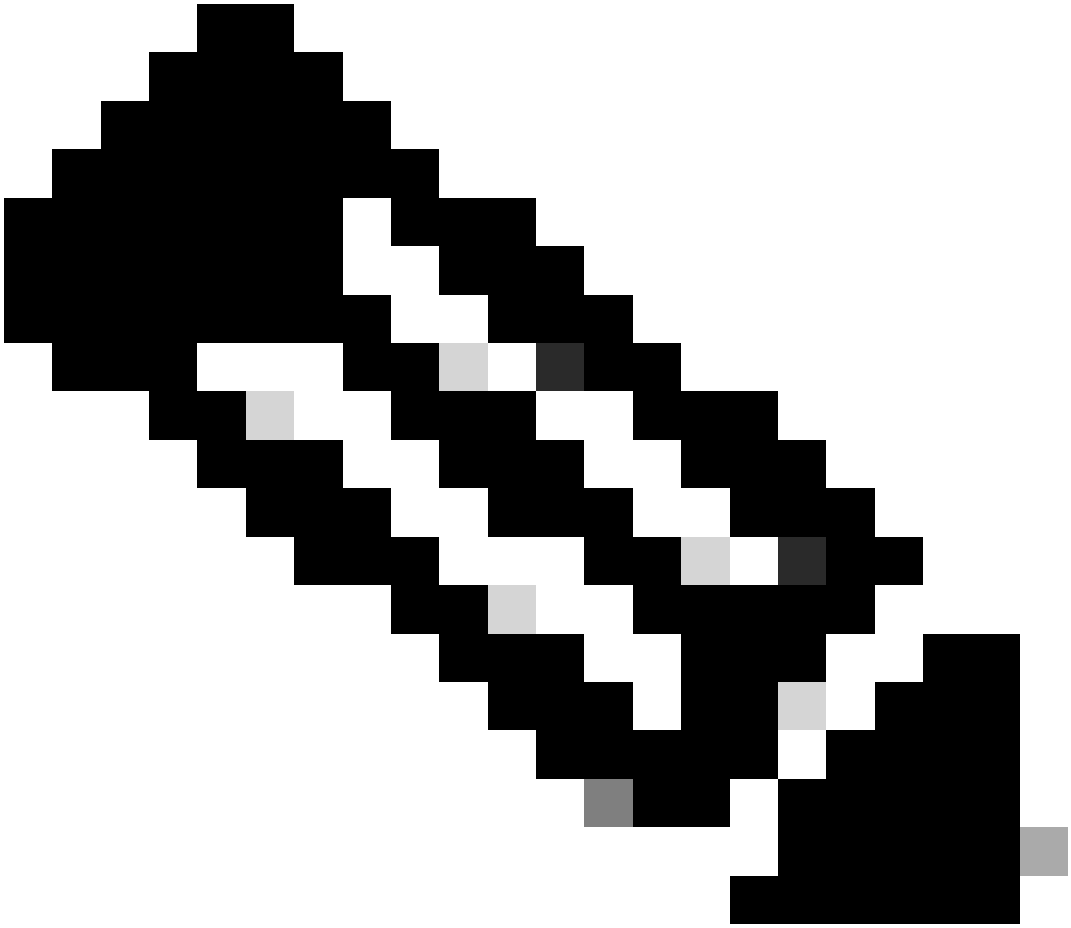
封包遺失可能發生在兩個方向；保持時間已過期表示此裝置未在保持時間內收到或處理來自對等體的hello，介面對等體已收到表示對等體已終止鄰接關係，因為它沒有在保持時間內收到或處理hello。

組態

1.使用通道介面IP位址設定ACL，因為這些位址是hello的來源IP位址：

```
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
```



附註：顯示的配置來自R1。在R2上為相關介面和EEM的已修改檔名執行相同操作。如果需要額外的專用性，請將EIGRP組播地址為224.0.0.10的ACL配置為目標IP地址以捕獲hello資料包。

2.建立EPC並將其與介面和ACL相關聯：

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

3.啟動EPC並確認在兩個方向上都捕獲了資料包：

```
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.配置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.等待下一個翻動發生，然後使用您首選的傳輸方法從bootflash複製檔案進行分析：

```
R1#show logging

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

- 路由器上的日誌緩衝區表示發生了EIGRP翻動，並且檔案已由EEM儲存。

分析

此時，將日誌緩衝區中找到的抖動的時間與收集的資料包捕獲相關聯，以確定發生抖動時，兩端是否傳送和接收了hello資料包。由於在R1上看到接收的介面對等終止，這意味著R2必須檢測到丟失的hello，因此保持時間已過期，這是從日誌檔案中看到的情況：

```
*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
```

由於R2檢測到保持時間已過期，請確認R1在捕獲中捕獲的翻動在R1上收集之前的15秒內是否傳送了hello:

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	✓

- 捕獲顯示192.168.10.1(R1)和192.168.10.2(R2)在R2在16:51:47（資料包513）傳送的PEER-TERMINATION hello資料包之前的15秒內hello消息。
- 具體來說，資料包503、505、508和511（由綠色箭頭指示）都是由R1在此時間段傳送的hello。

下一步是確認R2是否在R1傳送的所有呼叫都被R2接收，因此必須檢查從R2收集的捕獲：

No.	Time	Source	Destination	Protocol	Length	Info	Peer Termination
498	2024-07-17 16:51:32.154320	192.168.10.1	224.0.0.10	EIGRP	98	Hello	
499	2024-07-17 16:51:34.296179	192.168.10.2	224.0.0.10	EIGRP	98	Hello	
500	2024-07-17 16:51:38.573467	192.168.10.2	224.0.0.10	EIGRP	98	Hello	
501	2024-07-17 16:51:43.006794	192.168.10.2	224.0.0.10	EIGRP	98	Hello	
502	2024-07-17 16:51:47.156716	192.168.10.2	224.0.0.10	EIGRP	98	Hello	✓

```
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 224.0.0.10
v Cisco EIGRP
    Version: 2
    Opcode: Hello (5)
    Checksum: 0xdfd1 [correct]
    [Checksum Status: Good]
  > Flags: 0x00000000
    Sequence: 0
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 1
  v Parameters: Peer Termination
```

- 捕獲顯示從192.168.10.1(R1)收到的最後一個hello時間是16:51:32（以綠色箭頭表示）。 此後，接下來的15秒只顯示R2傳送的hello資料包（以紅色框表示）。 來自R1的捕獲中的資料包505、508和511不會出現在R2的捕獲中。這會導致R2檢測保持計時器已過期，並在16:51:47傳送PEER-TERMINATION hello資料包（資料包502）。

從這些資料可以得出結論，資料包丟失位於R1和R2之間的運營商網路中。在這種情況下，丟失位於R1到R2之間的方向。為了進一步調查，需要讓運營商參與檢查路徑是否存在丟包。

OSPF

使用相同的邏輯可以排除間歇性OSPF擺動故障。本節介紹這些關鍵因素，這些因素在計時器、IP地址過濾器和日誌消息方面區別於其他路由協定。

- 預設計時器是10秒hello和40秒dead計時器。對失效計時器過期襟翼進行故障排除時，請始終確認網路中正在使用的計時器。
- Hello資料包源自介面IP地址。如果需要額外的ACL特異性，則OSPF hello的組播目的地址是224.0.0.5。
- 裝置上的日誌消息略有不同。與EIGRP相反，OSPF沒有對等終止消息的概念。相反，檢測到失效計時器的裝置會將此記錄為翻動原因，然後其傳送的hello不再包含對等體的路由器ID，這將導致對等體移動到INIT狀態。當再次檢測到hello時，鄰接關係會轉換，直到達到FULL狀態。舉例來說：

R1檢測到失效計時器已過期：

```
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, Neighbo
*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, Neighbo
*Jul 30 16:48:10.504: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.2 on Tunnel20 from LOADING to FULL, Loa
```

但是，R2隻在OSPF回到FULL時顯示日誌消息。當狀態更改為INIT時，不會顯示日誌消息：

```
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
```

要在兩台裝置上觸發EEM，請使用「%OSPF-5-ADJCHG」作為系統日誌模式。這可確保只要關閉並恢復運行，兩台裝置上的EEM都會觸發。配置的raterlimit值可確保當看到多個帶有此字串的日誌時，不會在短時間內觸發兩次。關鍵是確認兩端的資料包捕獲中是否傳送和接收hello資料包。

BGP

同樣的邏輯也可用於對間歇性BGP擺動進行故障排除。本節介紹這些關鍵因素，這些因素在計時器、IP地址過濾器和日誌消息方面區別於其他路由協定。

- 預設計時器是60秒的keepalive和180秒的保持時間。在排除保留時間到期的襟翼故障時，請始終確認網路中正在使用的計時器。
- Keepalive資料包在鄰居IP地址之間單播傳送到TCP目標埠179。如果需要其他ACL特殊性，請允許從源IP地址到目標TCP埠179的TCP流量。
- 兩台裝置上的BGP日誌消息看起來相似，但檢測保持時間過期的裝置顯示它向鄰居傳送了通知，而另一台裝置則表示它收到了通知消息。舉例來說：

R1檢測到保留時間已過期，並將通知傳送到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收到來自R1的通知，因為R1檢測到保留時間已過期：

```
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
```

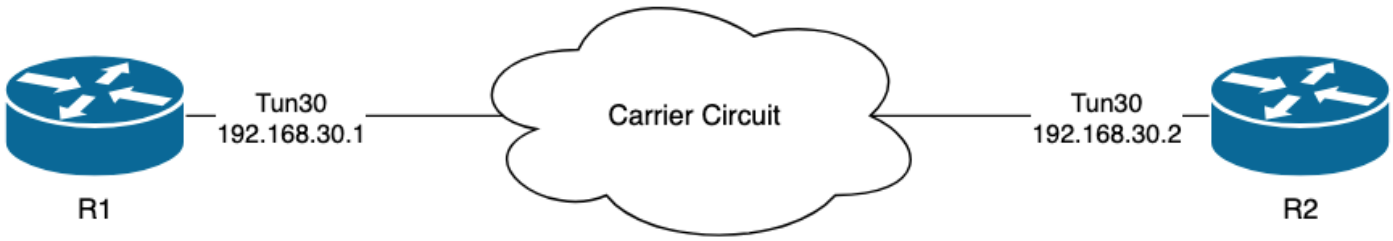
要觸發BGP擺動的EEM，請使用「%BGP_SESSION-5-ADJCHANGE」作為系統日誌模式。在翻動後還記錄的任何其他「%BGP」系統日誌消息也可用於觸發EEM。

對間歇性BFD襟翼進行故障排除

同樣的方法也可用於對間歇性BFD襟翼進行故障排除，但有些細微的差異可用於分析。本節介紹一些基本的BFD功能，並舉例說明如何使用EEM和EPC進行故障排除。如需更多詳細的BFD疑難排解資訊，請參閱對Cisco IOS XE中的雙向轉送檢測進行疑難排解。

在本示例中，BFD計時器設定為300ms，乘數為3，這意味著每300ms傳送一次回波，並且當一行中未返回3個回波資料包時（等於900ms保持時間）檢測到回波故障。

拓撲



示例 — BFD Echo Mode

在BFD回應模式（預設模式）下，BFD回應封包會透過本機介面IP作為來源和目的地來傳送。這允許鄰居在資料平面中處理封包並將其傳回來源裝置。每個BFD回聲與BFD回聲消息報頭中的回聲ID一起傳送。這些引數可用於確定已傳送的BFD回顯資料包是否被接收回，因為如果任何給定的BFD回顯資料包確實由鄰居返回，則其必須出現兩次。用於在介面IP地址之間單播傳送用於控制BFD會話狀態的BFD控制資料包。

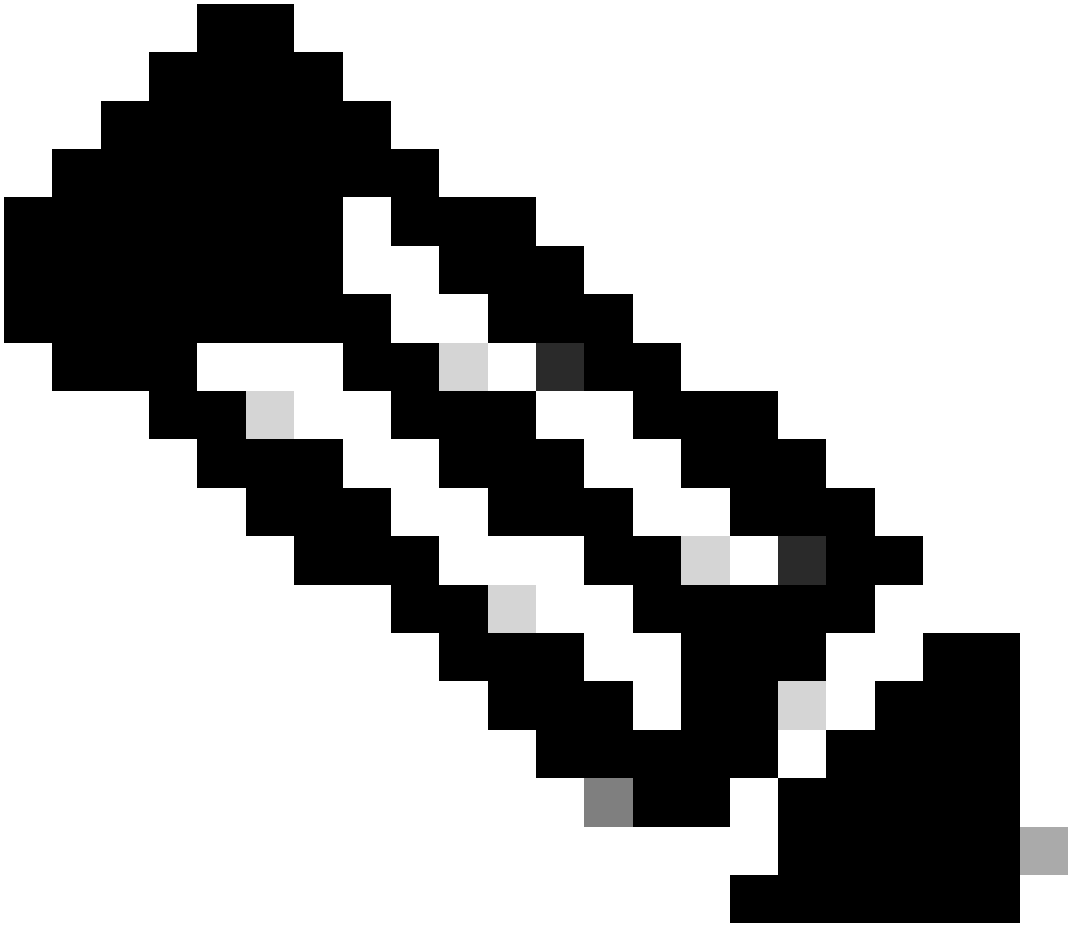
來自R1的日誌表明BFD鄰接因回聲故障而多次中斷，這意味著在這些間隔期間，R1沒有從R2接收或處理自己的回聲資料包3。

```
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
```

組態

1.使用通道介面IP位址設定ACL，因為這些位址是BFD回應封包和控制封包的來源IP位址：

```
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
```



附註：顯示的配置來自R1。在R2上為相關介面和EEM的已修改檔名執行相同操作。如果需要其他特殊性，請為目的地連線埠3785（回應封包）和3784（控制封包）的UDP設定ACL。

2.建立EPC並將其與介面和ACL相關聯：

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

3.啟動EPC並確認在兩個方向上都捕獲了資料包：

```
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.配置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.等待下一個翻動發生，然後使用您首選的傳輸方法從bootflash複製檔案進行分析：

```
R1#show logging
```

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

- 日誌緩衝區指示在19:09:47出現BFD翻動，並且檔案已由EEM儲存。

分析

此時，將日誌緩衝區中找到的翻頁的時間與收集的資料包捕獲相關聯，以便確定出現問題時兩端是否傳送和接收BFD回波。由於R1上的擺動原因為ECHO FAILURE，這意味著它會向R2傳送控制資料包以終止BFD會話，這反映在從R2收集到的日誌檔案中，該檔案顯示BFD關閉原因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
```

由於R1檢測到回聲故障，因此請檢查R1上收集的資料包捕獲，看它是否在翻動之前的900毫秒內傳送和接收BFD回聲。

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	0000000000000100200000041f	Originator specific content
136	2024-07-18 19:09:46.484581	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000000100200000041f	Originator specific content
137	2024-07-18 19:09:46.707712	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000000100100000041d	Originator specific content
138	2024-07-18 19:09:46.970921	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000000100100000041e	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	0000000000000100100000041f	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

- 捕獲顯示，R1一直主動傳送BFD回應資料包，直到發生翻動時為止，但R2未返回這些資料包，因此R1傳送控制資料包，在19:09:47.468終止會話。
- 這一點從以下事實中明顯可見：資料包137、138和140（由綠色箭頭指示）在捕獲中僅出現一次，這可以通過BFD回應ID（在紅色方框中）確定。 如果已返回回應，則具有相同BFD回應ID的每個資料包都有第二份副本。IP報頭中的IP Identification（IP標識）欄位也可用於驗證這一點。
- 此捕獲還顯示，在資料包136之後沒有從R2收到BFD回波，這是在R2到R1的方向上資料包丟失的另一個指示。

下一步是確認R1傳送的所有BFD回應資料包是否都已接收並由R2返回，因此必須檢查從R2收集的捕獲：

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	0000000000000100100000041d	Originator specific content
108	2024-07-18 19:09:46.708430	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000000100100000041d	Originator specific content
110	2024-07-18 19:09:46.774829	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000000100200000420	Originator specific content
111	2024-07-18 19:09:46.971240	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000000100100000041e	Originator specific content
112	2024-07-18 19:09:46.971542	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000000100100000041e	Originator specific content
113	2024-07-18 19:09:47.015058	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000000100200000421	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	0000000000000100100000041f	Originator specific content
117	2024-07-18 19:09:47.204021	192.168.30.1	192.168.30.1	BFD Echo	78	0000000000000100100000041f	Originator specific content
118	2024-07-18 19:09:47.286688	192.168.30.2	192.168.30.2	BFD Echo	78	0000000000000100200000422	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

- 此捕獲顯示R1傳送的所有BFD回聲都由R2接收並返回（用綠色箭頭指示）；資料包107和108是相同的BFD回應，資料包111和112是相同的BFD回應，資料包116和117是相同的BFD回應。
- 此捕獲還顯示R2主動傳送了在R1的捕獲中看不到的回應資料包（以紅色方框表示），進一步表明從R2到R1的方向上裝置之間的資料包丟失。

從資料分析可知，丟包率在R1與R2之間的載波網路中，此時所有的證據都表明，丟包率在R2與R1之間。為了進一步深入研究，需要讓載波參與路由過程，檢查丟包率。

BFD非同步模式

當使用BFD非同步模式（回聲功能被禁用）時，可以使用相同的方法，並且可以保持EEM和EPC配置相同。非同步模式的區別在於，裝置將單播BFD控制資料包作為keepalive（類似於典型的路由協定鄰接關係）相互傳送。這表示只傳送了UDP連線埠3784封包。在此案例中，只要BFD封包在所需的間隔內從鄰居收到，BFD就會保持運行狀態。如果沒有發生這種情況，故障原因為DETECT

TIMER EXPIRED，然後路由器向對等裝置傳送控制資料包以關閉會話。

要分析檢測到故障的裝置上的捕獲，請查詢在到達翻動之前的時間從對等裝置接收的單播BFD資料包。例如，如果使用3的乘數將TX間隔設定為300ms，那麼如果在翻動之前的900ms中沒有收到BFD資料包，則這表示潛在的資料包丟失。在通過EEM從鄰居收集的捕獲中，選中此相同的時間視窗；如果資料包是在該時間段傳送的，則確認裝置之間的某個位置有丟失。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。